САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
РЕГИОНАЛЬНАЯ ИНФОРМАТИКА

Сборник трудов

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Выпуск 12

Санкт-Петербург
2023

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
РЕГИОНАЛЬНАЯ ИНФОРМАТИКА

Сборник трудов

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Выпуск 12

Санкт-Петербург
2023

УДК (002:681):338.98

Р32

Региональная информатика и информационная безопасность.
Р32 Сборник трудов. Выпуск 12 / СПОИСУ. – СПб., 2023. – 421 с.
ISBN 978-5-00182-088-8

В сборник включены статьи участников Санкт-Петербургской международной конференции «Региональная информатика» и Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России», проведенных при поддержке Правительства Санкт-Петербурга, объединенных в рубрики: Государственная политика в сфере информатизации и информационной безопасности; Информационно-психологические и правовые аспекты информационной безопасности; Информационная безопасность; Телекоммуникационные сети и технологии; Информационные технологии в экономике и критических инфраструктурах; Информационные технологии на транспорте; Информационные технологии управления объектами морской техники и морской инфраструктуры, Киберфизические и геоинформационные системы; Подготовка кадров в области обеспечения информационной безопасности; Молодежная научная школа «интеллектуальные безопасные информационные системы и технологии».

Сборник статей предназначен для широкого круга руководителей и специалистов органов государственной власти и местного самоуправления, промышленности, науки, образования, бизнеса, аспирантов и студентов высших учебных заведений, специализирующихся в вопросах информатизации, связи, информационной безопасности и защиты информации.

УДК (002:681):338.98

Редакционная коллегия: *Б.Я. Советов, Р.М. Юсупов, В.В. Касаткин*
Компьютерная верстка: *А.С. Михайлова*
Дизайн: *Н.С. Михайлов*

Публикуется в авторской редакции

Подписано в печать 21.10.2023. Формат 60x84⅛. Бумага офсетная.
Печать – ризография. Усл. печ. л. 49. Тираж 400 экз. Заказ № 1310
Отпечатано в ООО «ИПЦ «Измайловский»
190005, Санкт-Петербург, Измайловский пр., 18-д

ISBN 978-5-00182-088-8

ST. PETERSBURG INTERREGIONAL CONFERENCE
INFORMATION SECURITY OF RUSSIAN REGIONS

ST. PETERSBURG INTERNATONAL CONFERENCE
REGIONAL INFORMATICS

Proceedings

REGIONAL INFORMATICS AND INFORMATION SECURITY

The Issue No 12

St. Petersburg
2023

ГОСУДАРСТВЕННАЯ ПОЛИТИКА В СФЕРЕ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 332.1

СТРАТЕГИЯ РАЗВИТИЯ СЕТИ МНОГОФУНКЦИОНАЛЬНЫХ ЦЕНТРОВ В САНКТ-ПЕТЕРБУРГЕ

Смирнова Юлия Леонидовна[1], Токарева Любовь Сергеевна[1], Александров Максим Михайлович[2], Розова Алла Юрьевна[2], Минаев Николай Николаевич[3], Крылатов Александр Юрьевич[4]

[1] Комитет по информатизации и связи
Смольный проезд, 1, Санкт-Петербург, 191060, Россия
[2] СПб ГКУ «Многофункциональный центр предоставления государственных и муниципальных услуг»
Красного Текстильщика ул., 10-12, Санкт-Петербург, 191124, Россия
[3] СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Транспортный пер., 6, лит. А, пом. 7Н8Н, Санкт-Петербург, 191040, Россия
[4] Санкт-Петербургский государственный университет,
Петергоф, Университетский пр., 35, Санкт-Петербург, 198504, Россия
e-mails: kis@gov.spb.ru, m.alexandrov@mfcspb.ru, a.rozova@mfcspb.ru, n.minaev@iac.spb.ru, a.krylatov@spbu.ru

Аннотация. Доклад посвящен разработке стратегии развития сети многофункциональных центров (МФЦ) в Санкт-Петербурге на период до 2027 года. Содержит методические подходы и аналитические материалы к разработке системы предоставления населению социально значимых сервисов, в том числе государственных услуг, в объективно и обоснованно выбранных локациях. Разработаны инструменты анализа пространственных данных для оценки мест расположения МФЦ с точки зрения близости к наиболее интенсивным местам возникновения спроса и экономической целесообразности.

Ключевые слова: государственные услуги; многофункциональные центры; стратегия развития сети; клиентоцентричность; количество обращений заявителей; окна приема и выдачи документов (окна МФЦ); места возникновения спроса на услуги; территориальные единицы высокой связности.

MULTIFUNCTIONAL CENTER NETWORK DEVELOPMENT STRATEGY IN SAINT PETERSBURG

Smirnova Yulia[1], Tokareva Lyubov[1], Aleksandrov Maxim[2], Rozova Alla[2], Minaev Nikolay[3], Krylatov Alexander[4]

[1] Committee on Informatization and Communications
1 Smolny passage, St. Petersburg, 191060, Russia
[2] SPb GKU «Multifunctional Center for the Provision of State and municipal services»
10-12 Krasnaya Tekstilshchik str., St. Petersburg, 191124, Russia
[3] St. Petersburg State Unitary Enterprise «St. Petersburg Information and Analytical Center»
6 Transport lane, lit. A, pom. 7N8N, St. Petersburg, 191040, Russia
[4] Saint Petersburg State University,
35 University Ave., Peterhof, St. Petersburg, 198504, Russia
e-mails: kis@gov.spb.ru, m.alexandrov@mfcspb.ru, a.rozova@mfcspb.ru, n.minaev@iac.spb.ru, a.krylatov@spbu.ru

Abstract. The report is devoted to the development of a strategy for the development of a network of multifunctional centers (MFC) in St. Petersburg for the period up to 2027. Contains methodological approaches and analytical materials to the development of a system for providing socially significant services to the population, including public services, in objectively and reasonably selected locations. Tools for analyzing spatial data have been developed to assess the locations of the MFC in terms of proximity to the most intensive places of demand and economic feasibility.

Keywords: public services; multifunctional centers; network development strategy; customer centrism; number of applicants' requests; windows for receiving and issuing documents (MFC windows); places of demand for services; territorial units of high connectivity.

Одно из направлений стратегии социально-экономического развития Санкт-Петербурга до 2035 года – повышение эффективности предоставления государственных услуг и прозрачности государственного управления. Развитие данного направления осуществляется в том числе путем расширения перечня государственных услуг, а также предоставления гражданам и организациям государственных услуг с использованием современных информационных технологий.

Клиентоцентричный подход предполагает, что государство выстраивает свою деятельность таким образом, чтобы эффективно отвечать на запросы человека, предлагать ему качественные и востребованные услуги и сервисы. Идеальной является такая ситуация, когда человек для решения любого жизненного вопроса получает наилучшее возможное решение «здесь и сейчас» и в удобной для него форме [2].

Для населения необходимыми признаются два варианта взаимодействия с государством: электронный формат и очный формат – то есть инстанция, куда человек может обратиться очно, получить услугу, проконсультироваться, при необходимости, оставить жалобу [1, 3]. В качестве очного канала взаимодействия населения с государством выступают многофункциональные центры.

Санкт-Петербург ставит перед собой цель создания в МФЦ общественно-деловых пространств по предоставлению жителям современных и технологичных государственных и негосударственных сервисов, основанных на принципах клиентоцентричности.

В том числе, в рамках федерального проекта «Цифровое государственное управление» перед МФЦ поставлено несколько задач, одна из которых – к 2030 году стать единственным каналом очного взаимодействия по государственным услугам.

Несмотря на очевидные преимущества электронной формы взаимодействия с государством, население все еще сталкивается с рядом барьеров к более активному использованию цифровых решений: это и недостаточная цифровая грамотность пользователей, и сложность в самостоятельном освоении услуг, и неуверенность в безопасности хранения персональных данных.

Следовательно, для обеспечения клиентского равенства необходимо не только сохранить существующую сеть МФЦ, но и продолжать ее развивать, а, следовательно, создать такую систему очного предоставления государственных услуг и сервисов, которая обеспечит их максимальную доступность и высокое качество.

В основу Стратегии развития сети МФЦ Санкт-Петербурга (далее – Стратегия) заложен анализ статистических показателей деятельности за предшествующий период и расчет прогнозных значений количества обращений заявителей на период до 2027 года.

Научное обоснование Стратегии включает в себя разработку инструментов анализа пространственных данных для оценки мест расположения МФЦ с точки зрения их близости к наиболее интенсивным местам возникновения спроса и экономической целесообразности мероприятий.

Стратегия основывается на следующих факторах, оказывающих влияние на прогноз количества очных обращений в МФЦ:

- динамика численности населения Санкт-Петербурга;
- динамика очных обращений в МФЦ, приходящихся на 1 жителя;
- увеличение количества услуг;
- среднее время обслуживания одного очного обращения в МФЦ;
- фонд рабочего времени одного окна приема и выдачи документов.

Прогноз численности населения по районам Санкт-Петербурга и по городу в целом до 2027 года подготовлен на средствах Интегрированной системы информационно-аналитического обеспечения деятельности исполнительных органов государственной власти Санкт-Петербурга». Прогнозирование демографических показателей выполнено на основе заданных экспертных сценариев (базового, целевого, консервативного), отражающих динамику показателей рождаемости, смертности и миграционного прироста в прогнозируемом периоде, методом передвижки возрастов. В расчет прогнозного количества обращений на период 2023–2027 годов принят целевой сценарий прогноза численности населения.

Поскольку ежегодно количество обращений в МФЦ превышает численность населения, на основании анализа фактических данных за предшествующий период рассчитаны коэффициенты посещаемости, то есть количество обращений в МФЦ на 1 жителя [5].

Следующим фактором, влияющим на прогнозное значение количества обращений, является количество оказываемых МФЦ услуг [5]. В расчетах учтено, что к 2030 году 100% обращений из органов власти должно быть переведено в МФЦ. На основании анализа статистических данных за предыдущие 3 года построена трендовая модель перераспределения обращений, поданных через МФЦ, и посредством электронной формы, до 2027 года. Ожидаемо, что увеличение доли электронного способа подачи обращений быстрее коснется массовых социально значимых услуг за счет реализации всех региональных социально значимых услуг на федеральном портале государственных услуг в 2024 году.

Прогнозное значение количества обращений к 2027 году рассчитано в четырех вариантах, учитывающих различные сценарии влияния факторов.

Для определения необходимого количества окон МФЦ, позволяющего удовлетворить потребность в приеме потенциального количества обращений, спрогнозировано среднее время обслуживания одного обращения и фонд рабочего времени одного окна МФЦ в год [5].

На основании полученных значений спрогнозировано необходимое количество окон МФЦ в 2027 году, которое распределено по районам города и по годам. 4 варианта значений количества окон смоделированы по 4 вариантам прогнозных значений количества обращений.

Очередным шагом в разработке Стратегии стало определение приоритета качественных характеристик МФЦ. Для получения необходимой информации применен метод «парных сравнений» Луиса Терстоуна, и проведено анкетирование посетителей и работников по месту нахождения МФЦ. Участникам анкетирования было предложено выбрать наиболее приоритетные для них характеристики центров: посетителям – с точки зрения комфортности посещения, работникам – в контексте работы.

Как показал опрос, для посетителей наиболее важным является удобство расположения МФЦ, на втором месте – хорошее состояние помещений и наличие функциональных зон. Для работников, напротив, в приоритете состояние помещений, а удобство расположения – на втором месте. На третьем и четвертом местах, соответственно, «дополнительные сервисы» и «количество окон приема», что позволяет определить оснащение дополнительными сервисами зоной роста МФЦ на ближайшую перспективу.

По итогам сведений о приоритетности характеристик рассчитан индекс комфортности для каждого центра и сформирована «Карта комфортности сети МФЦ», которая определяет перечень действующих МФЦ, соответствующих требованиям, а также фиксирует перечень «проблемных» центров, расположенных в труднодоступных местах и/или эксплуатационно-неблагополучных помещениях.

Для обоснования выбора предпочтительных (оптимальных) мест расположения МФЦ проведено исследование на предмет доступности центров и близости расположения к наиболее интенсивным местам спроса. Исследована задача поиска оптимального расположения точек присутствия МФЦ, как задача условной оптимизации с учетом всех предъявляемых к каждому отдельному центру требований.

За основу приняты следующие требования:

– на каждые 5 тыс. жителей района, в котором располагается МФЦ, предусматривается не менее одного окна приема и выдачи документов [4];

– каждый МФЦ предусматривает возможность обслуживания граждан в радиусе 3 км по дорогам общего пользования, с учетом естественных препятствий: водных преград, автомагистралей, железнодорожных путей и т.д.

При построении перспективной схемы размещения использованы данные о числе проживающих, работающих, перемещающихся и обслуживаемых граждан в местах проживания, приложения труда, транспортного и коммерческого обслуживания.

Исследована задача оптимизации топологии сети МФЦ, как задача кластерного анализа с учетом методики построения оптимальной схемы размещения МФЦ [6].

Применение графовых методов кластеризации территории позволило выявить территориальные единицы высокой связности, удовлетворяющие требованию задачи.

В результате исследования получены следующие методологически обоснованные данные:

– координаты всех узлов улично-дорожной сети, находящихся в границах территориальных единиц высокой связности;

– координаты объектов формирования спроса на услуги МФЦ;

– данные о потенциальном спросе на услуги МФЦ в каждом объекте формирования спроса;

– координаты наилучших мест размещения МФЦ, рассчитанные как центроиды внутри единиц высокой связности.

В настоящее время формируется информация об отклонении текущих местоположений МФЦ от «идеальных» точек и оценивается их доступность для граждан. После обработки данных об экономически целесообразном числе окон в потенциальном МФЦ при его расположении в центроиде спроса и с учетом требования одного окна на каждые 5 тыс. жителей, будет сформирована перспективная схема размещения МФЦ Санкт-Петербурга, внедрение которой позволит осуществить качественное улучшение взаимодействия органов власти с гражданским обществом на принципах клиентоцентричности, что, несомненно, повысит удовлетворенность жителей деятельностью Правительства Санкт-Петербурга и обеспечит рост доверия населения к власти.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 27.07.2010 № 210-ФЗ (ред. от 31.07.2023) «Об организации предоставления государственных и муниципальных услуг» // Собрание законодательства Российской Федерации. – 2010. – № 31. – Ст. 4179.
2. Закон Санкт-Петербурга от 19.12.2018 № 771-164 (ред. от 21.12.2022) «О стратегии социально-экономического развития Санкт-Петербурга на период до 2035 года» // Официальный интернет-портал правовой информации (www.pravo.gov.ru). – 2018. – № 7800201812250015.

3. Указ Президента Российской Федерации от 07.05.2012 № 601 «Об основных направлениях совершенствования системы государственного управления» // Собрание законодательства Российской Федерации. – 2012. – № 19. – Ст. 2338.
4. Постановление Правительства Российской Федерации от 22.12.2012 № 1376 (ред. от 28.12.2022) «Об утверждении Правил организации деятельности многофункциональных центров предоставления государственных и муниципальных услуг» // Собрание законодательства Российской Федерации. – 2012. – № 53 (Часть II). – Ст. 7932.
5. «Методика мониторинга осуществления многофункциональными центрами предоставления государственных и муниципальных услуг отдельных функций в соответствии с Федеральным законом от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», утвержденная статс-секретарем – заместителем Министра экономического развития Российской Федерации А.И.Херсонцевым 22.12.2022 г.
6. Ahmadi-Javid A., Seyedi P., Syam S. (2017) A survey of healthcare facility location. Computers & Operations Research, 79, 223-263.

УДК 004.056

О ПОДГОТОВКЕ СТРАТЕГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИСПОЛНИТЕЛЬНЫХ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ САНКТ-ПЕТЕРБУРГА

Сиденко Александр Иванович
Комитет по информатизации и связи
Смольный проезд, 1, Санкт-Петербург, 191060, Россия

Аннотация. Раскрывается содержание Стратегии информационной безопасности исполнительных органов государственной власти (ИОГВ) Санкт-Петербурга: нормативная база; цели, объекты защиты, структура системы защиты информации, защищенные сети, показатели состояния, защищенности, функционирования, стратегия дальнейшего развития информационной инфраструктуры ИОГВ. Обсуждается содержание дорожной карты и результаты реализации стратегии дорожной карты в государственных бюджетных учреждениях Санкт-Петербурга.

Ключевые слова: стратегия информационной безопасности ИОГВ Санкт-Петербурга; системы защиты информации; информационная инфраструктура ИОГВ; дорожная карта.

ON PREPARATION OF INFORMATION SECURITY STRATEGY OF EXECUTIVE BODIES OF STATE POWER OF ST. PETERSBURG

Sidenko Aleksandr
Committee on Informatization and Communications
1 Smolny passage, St. Petersburg, 191060, Russia
e-mail: kis@gov.spb.ru

Abstract. The connection between the information security strategy of the executive bodies of the state government (EBSP) of St. Petersburg and the national security strategy of the Russian Federation and other regulatory legal acts is disclosed. The goals of the strategy, objects of protection, information protection in state information systems, the secure corporate network of the EBSP of St. Petersburg, indicators of the state of security and the strategy for the further development of the information infrastructure of the EBSP are considered. The content of the roadmap and the results of the implementation of the roadmap strategy in state budgetary institutions of St. Petersburg are being discussed.

Key words: information security strategy of the EBSP of St. Petersburg; information infrastructure of the EBSP; information security system; secure corporate network of EBSP; road map.

1.Связь Стратегии информационной безопасности исполнительных органов государственной власти Санкт-Петербурга с стратегией национальной безопасности Российской Федерации и иными нормативными правовыми актами

Правовой основой обеспечения информационной безопасности являются положения Конституции Российской Федерации, федеральных законов, Указов Президента Российской Федерации, постановлений и распоряжений Правительства Российской Федерации, нормативных правовых актов законодательства Российской Федерации, нормативных и руководящих документов ФСТЭК России и ФСБ России по вопросам защиты информации.

При подготовке стратегии информационной безопасности исполнительных органов государственной власти Санкт-Петербурга (далее – Стратегия) были учтены следующие документы:

1) Конституция Российской Федерации.

2) Федеральный закон от 01.04.2020 № 98-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам предупреждения и ликвидации чрезвычайных ситуаций».

3) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

4) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

5) Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

6) Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по защите информации».

7) Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации».

8) Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных».

9) Постановление Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».

10) Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

11) Приказ ФСЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

12) Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

13) Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах: персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

14) ГОСТ Р ИСО/МЭК 15408-2002 «Информационные технологии. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий».

15) ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования».

16) ГОСТ Р 51583-2014 Национальный стандарт Российской Федерации «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

17) ГОСТ Р 59547-2001 «Защита информации. Мониторинг информационной безопасности. Общие положения».

18) ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания».

19) ГОСТ 34.602-2020 Межгосударственный стандарт «Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

20) ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности».

21) ГОСТ Р ИСО 22301-2021. Национальный стандарт Российской Федерации. Надежность в технике. Системы менеджмента непрерывности деятельности. Требования.

22) Концепция информационной безопасности исполнительных органов государственной власти Санкт-Петербурга, утвержденная от 20.02.2023 Губернатором Санкт-Петербурга А.Д. Бегловым.

2. Единая мультисервисная телекоммуникационная сеть исполнительных органов государственной власти Санкт-Петербурга; защищенная корпоративная сеть исполнительных органов государственной власти Санкт-Петербурга; система защиты информации ГИС; объекты защиты; информационные технологии ГИС

Исполнительные органы государственной власти Санкт-Петербурга (далее – ИОГВ) объедены в одну выделенную общую сеть передачи данных - единую многофункциональную телекоммуникационную сеть (далее – ЕМТС) [1]. Для обеспечения защиты информации от раскрытия и модификации при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны объектов информатизации, на базе ЕМТС создана защищенная корпоративная сеть ИОГВ [2]. (далее – ЗКС ИОГВ) в которой применяются сертифицированные по требованиям безопасности средства криптографической защиты информации не ниже класса КС2.

В целях исполнения Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных утвержденного Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» необходимо применять организационные и технические меры защиты информации посредством создания системы (подсистемы) защиты информации государственной информационной системы (далее – ГИС).

Система защиты информации предназначена для защиты информации, содержащейся в ГИС, от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

Целями создания системы защиты информации ГИС являются:

– предотвращение несанкционированного доступа к информации, обрабатываемой в ГИС и подлежащей защите;

– своевременное обнаружение фактов нарушения защиты информации;

– предупреждение возможности неблагоприятных последствий нарушения свойств информации;

– недопущение воздействия на основные технические средства и системы обработки информации, в результате которого нарушается функционирование ГИС;

– постоянный контроль за обеспечением уровня защищенности информации, обрабатываемой в ГИС и подлежащей защите.

В перечень объектов защиты ГИС входит:

– информация, обрабатываемая в ГИС и подлежащая защите,

– комплекс технических средств ГИС,

– применяемые в ГИС информационные технологии,

– применяемое в ГИС программное обеспечение,

– программные и программно-аппаратные средства защиты информации ГИС.

В ГИС применяются следующие информационные технологии [3]:

– система на основе тонкого клиента,

– веб-приложения,

– виртуальная инфраструктура,

– облачные технологии,

– физические каналы передачи данных,

– программное обеспечение,

– интернет-технологии,

– мобильные технические средства (съемные машинные носители информации).

3. *Операционный процесс воздействия угроз безопасности информации* Визуализация типового операционного процесса воздействия угроз безопасности информации на объектах информатизации ИОГВ и подведомственных учреждений приведена на рис. 1.

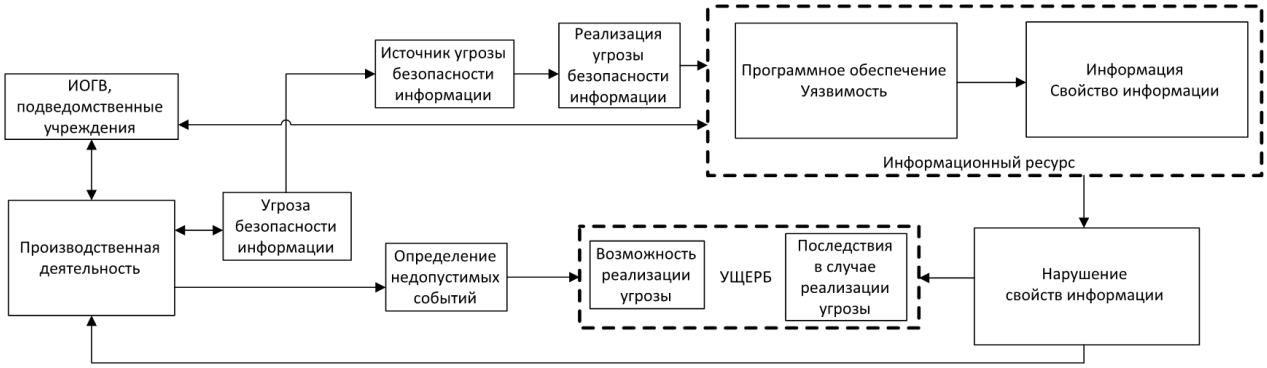


Рис. 1 - Визуализация типового операционного процесса воздействия угроз безопасности информации

4. Назначение автоматизированной системы «Центр оперативного управления информационной безопасностью», Ведомственного центра государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, показатели их состояния и функционирования, стратегия дальнейшего развития

При рассмотрении комплексной защиты информации в ИОГВ в качестве основных типов угроз безопасности информации [4] рассматриваются угрозы безопасности информации, связанные с:

– преднамеренными действиями внешнего нарушителя;

– преднамеренными и непреднамеренными действиями внутреннего нарушителя;

– применением методов социальной инженерии;

– уничтожением или блокированием информации вредоносным программным обеспечением;

– передачей информации по каналам связи;

– использованием нарушителем уязвимостей и недекларированных возможностей программного обеспечения (далее – ПО);

– нарушением функционирования средств, реализующих технологии искусственного интеллекта;

– нарушениями предоставления облачных услуг;
– техногенными источниками.

Нейтрализация таких угроз безопасности информации осуществляется посредством устранения источников угроз, ослабления степени влияния уязвимостей, а также посредством минимизации последствий, возникающих в результате реализации угроз безопасности информации. Снижение вероятности реализации угроз безопасности в ИОГВ обеспечивается в том числе посредством эксплуатации автоматизированной системы «Центр оперативного управления информационной безопасностью» государственной информационной системы Санкт-Петербурга «Аппаратно-программный комплекс «Безопасный город» (далее – АС ЦОУ).

АС ЦОУ позволяет решать такие задачи как:

– централизованное управление средствами защиты информации ИОГВ;
– обеспечение информационно-аналитической деятельности ИОГВ в области защиты информации;
– защищенное информационное взаимодействие информационных систем ИОГВ и их Пользователей;
– автоматизация процессов сбора и первичный анализ информации от существующих систем защиты информации ИОГВ;
– мониторинг информационной безопасности, оценка состояния и повышения уровня защищенности ГИС ИОГВ;
– централизованное получение обновлений базы данных сигнатур вредоносного ПО, распространение этих обновлений на серверы, размещенные в ИОГВ;
– предотвращение передачи персональных данных за пределы контролируемой зоны ИОГВ;
– анализ исходного кода информационных систем ИОГВ на наличие уязвимостей.

Учитывая положения стратегии национальной безопасности Российской Федерации, утвержденную Указом Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации», геополитическую ситуацию, возникновение новых и развивающихся угроз безопасности информации, направленных на государственные информационные ресурсы ИОГВ, привело к необходимости повышения уровня готовности служб мониторинга информационной безопасности.

В рамках предотвращения деструктивного информационно-технического воздействия на государственные информационные ресурсы ИОГВ, включая объекты критической информационной инфраструктуры Российской Федерации и развития системы прогнозирования, выявления и предупреждения угроз информационной безопасности Российской Федерации, определения их источников, оперативной ликвидации последствий реализации таких угроз, Распоряжением Комитета по информатизации и связи от 30.06.2022 № 130-Р «О создании ведомственного центра государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы исполнительных органов власти Санкт-Петербурга» на базе подведомственного предприятия СПб ГУП «СПб ИАЦ» создан Ведомственный центр государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (далее – Ведомственный центр). Ведомственный центр задействует возможности АС ЦОУ в целях мониторинга информационной безопасности.

Ведомственный центр позволяет решать такие задачи как:

– обнаружение, предупреждение и ликвидация последствий компьютерных атак, направленных на контролируемые информационные ресурсы;
– проведение мероприятий по установлению причин инцидентов информационной безопасности, вызванных компьютерными атаками на контролируемые информационные ресурсы ИОГВ;
– сбор и анализ данных о состоянии информационной безопасности контролируемых информационных ресурсов ИОГВ;
– осуществление взаимодействия с Национальным координационным центром по компьютерным инцидентам;
– информирование в зоне ответственности заинтересованных лиц по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак.

5. Сведения по организации новых подключений к ЗКС ИОГВ

За 2023 год увеличено количество подключенных объектов информатизации ИОГВ и подведомственных учреждений, пользователей ГИС к ЗКС ИОГВ, а именно подключено:

– объектов информатизации посредством программно-аппаратных комплексов средств криптографической защиты информации (далее – СКЗИ) – 554 шт. (ЗАСТАВА-150 – 233 шт., VipNet Coordinator HW – 321 шт);
– пользователей посредством СКЗИ в программном исполнении VipNet Client – 131 шт.;
– пользователей посредством СКЗИ в программном исполнении КриптоПро Ngate – 1204 шт.

Общее количество используемых СКЗИ в ЗКС:

– программно-аппаратных комплексов – 3938 шт. (ЗАСТАВА-150 – 2366 шт. VipNet Coordinator HW – 1572 шт.);
– в программном исполнении VipNet Client – 5263 шт.;
– в программном исполнении КриптоПро Ngate – 1204 шт.

6. Квантовое шифрование

В рамках ЗКС ИОГВ рассматривается внедрение квантовой криптографической системы выработки и распределения криптографических ключей с использованием квантовых каналов связи и специальных протоколов посредством продукта ViPNet Quandor.

Основными особенностями данной системы являются:

– отсутствие асимметричных криптографических механизмов;

– автоматическая выработка и распределение криптографических ключей полностью исключает влияние человека и решает проблему доверенной доставки криптографических ключей;

– обеспечение стойкости к атакам, возможным при реализации эффективного квантового компьютера;

– невозможность перехвата передаваемой информации без ее изменения;

– защита от компрометации администратором защищенной сети, во время эксплуатации системы к используемым криптографическим ключам нет доступа извне.

7. Показатели атак, уязвимостей в информационной инфраструктуре ИОГВ

Ведомственным центром и службами мониторинга, входящими в его состав, за 2023 год зафиксировано:

– 12 404 863 события информационной безопасности;

– 159 702 попытки компьютерной атаки на ГИС;

– 151 717 компьютерных атак на информационную инфраструктуру ИОГВ из числа которых - 9 723 атаки высокого уровня.

При этом стоит отметить, что проведенные компьютерные атаки не имели серьезных последствий для информационной инфраструктуры ИОГВ.

За 2023 не было зафиксировано утечек персональных данных граждан, связанных с негативным воздействием на портальные решения ГИС. Уровень защищенности городских сервисов значительно повышен за счет внедрения современных отечественных средств защиты веб-порталов.

Количество ложных срабатываний средств защиты информации, осложняющих эксплуатацию сервисов гражданами, снижено на 93% (со 130 до 10 в месяц).

Сведения по наиболее частым уязвимостям приведены в таблице 1.

Таблица 1

Сведения по наиболее частым уязвимостям

№	Тип уязвимости	Количество	Уровень	Группа
1	Удаленное выполнение кода	126	Критический	Использование устаревшего ПО
2	Повышение привилегий	17	Критический	Использование уязвимого ПО
3	Разглашение информации (SWEET32)	452	Высокий	Использование устаревших алгоритмов шифрования
4	Удаленное выполнение кода, связанное с Windows SMB	184	Высокий	Использование уязвимого ПО
5	Учетная запись	146	Высокий	Использование слабых паролей и паролей «По умолчанию»
6	Перехват сессии	59	Высокий	Использование устаревшего ПО
7	Перехват TNS-соединения	57	Высокий	Использование уязвимого ПО
8	Уязвимость протокола удаленного рабочего стола	51	Высокий	Использование устаревшего ПО

Общая доля уязвимостей по их группам приведена на рис.2.

8. Показатели защищенности

По результатам работ по оценке уровня (состояния) защищенности [5] и верификации недопустимых событий в информационной инфраструктуре ИОГВ [6] работниками СПб ГУП «СПб ИАЦ» установлен средний уровень защищенности.

В ходе работ были обнаружены открытые элементы информационных систем ИОГВ с исходными кодами, что впоследствии могло быть использовано для изучения внутренней структуры приложений и подготовки атак на такие информационные системы. Среди которых обнаружены отладочные сценарии, раскрывающие сервисные учетные записи и сведения о структуре и используемых компонентах. Осуществляется некорректная обработка данных, отображаемых на страницах веб-приложений, позволяющая проводить атаки на пользователей информационных систем ИОГВ путем внедрения произвольного JavaScript-кода.

Также отсутствует режим «песочницы» для пользователей, при проверке поступивших подозрительных писем по электронной корпоративной почте.

Рис. 2 - Общая доля уязвимостей по их группам

В связи с чем для повышения уровня защищенности информационной инфраструктуры ИОГВ дополнительные меры по:

– проведению смены аутентификаторов учетных записей ПО, установленного на административных узлах сети;

– проведению отработки выполнения мер по противодействию компьютерным атакам на объекты информационной инфраструктуры ИОГВ, восстановлению их работоспособности и устранению последствий возможных инцидентов информационной безопасности;

– организации дежурства инженеров и иного технического персонала, ответственных за обеспечение функционирования объектов информационной инфраструктуры ИОГВ;

– обеспечению фильтрации трафика прикладного уровня с применением средств межсетевого экранирования уровня приложений (web application firewall), установленных в режим противодействия компьютерным атакам;

– созданию отдельного электронного почтового адреса, на который пользователи информационных систем ИОГВ могут пересылать письма с подозрением на вредоносное содержание (ссылку или вложение);

– обеспечению блокировки трафика, поступающего из программных средств анонимного веб-серфинга.

Кроме всего прочего выявлена необходимость в разработке типовых решений в отношении минимальных технических характеристик и оснащения необходимым программным обеспечением в том числе средствами защиты информации автоматизированных рабочих мест пользователей (далее – АРМ Пользователя) под определенные классы защищенности для работы в ГИС.

9. Киберучения

В целях обеспечения информационной безопасности информационной инфраструктуры ИОГВ в условиях проведения целенаправленных компьютерных атак, в марте 2023 года были проведены киберучения ООО «СОЛАР СЕКЬЮРИТИ» на базе киберполигона «Солар Кибермир».

Киберучения были организованы с целью оценки и улучшения существующих навыков участников проводить расследование инцидентов информационной безопасности, проверки готовности к отражению масштабных целенаправленных компьютерных атак в соответствии со сценарием учений.

В киберучениях участвовали работники:

– СПб ГУП «СПб ИАЦ»;

– Комитета имущественных отношений Санкт-Петербурга;

– Комитета государственной службы и кадровой политики Администрации Губернатора Санкт-Петербурга;

– Комитета по транспорту.

Согласно сценарию учений, злоумышленник произвел атаку на типовую информационную инфраструктуру. Выполнив разведку внешнего сетевого периметра и обнаружив определенный открытый сетевой порт, злоумышленник произвел компрометацию локальной учетной записи путем перебора паролей. Следующим шагом злоумышленника была компрометация учетной записи администратора домена методом снятия дампа памяти процесса на скомпрометированном ранее сервере. Вследствие чего злоумышленник произвел перемещение на контроллер домена используя системную утилиту и выполнил закрепление в информационной инфраструктуре,

создав задачу планировщика заданий. Для сокрытия следов компрометации злоумышленник произвел удаление журналов на скомпрометированном контроллере домена.

В рамках расследования сценария атаки участники должны были восстановить цепочку атак и заполнить отчет о расследовании инцидента. Отчет заполнялся индивидуально каждым участником киберучений. В отчете указывались техники и тактики злоумышленника, а также выявленные индикаторы компрометации, указывающие на несанкционированный доступ к конкретной информационной системе в информационной инфраструктуре.

Основными целями и задачами киберучения являлись:

– обнаружение и классификация участниками кибератак с использованием различных подходов и инструментов;

– определение участниками используемых в сценарии тактик и техник злоумышленника;

– применение участниками навыков по мониторингу информационной безопасности;

– применение участниками навыков по расследованию инцидентов информационной безопасности.

В итоговом отчете о проведении киберучений для ИОГВ были сформированы рекомендации по дальнейшей подготовке и профессиональному развитию специалистов ИОГВ.

В октябре 2023 года также проводились киберучения, но уже на базе киберполигона Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича.

В киберучениях участвовали работники:

– Комитета имущественных отношений Санкт-Петербурга;

– Комитета государственной службы и кадровой политики Администрации Губернатора Санкт-Петербурга;

– Комитета по транспорту;

– Комитета финансов;

– Администрации Выборгского района Санкт-Петербурга.

10. Показатели по импортозамещению

В существующей информационной инфраструктуре ИОГВ осуществлен полный перевод на использование отечественных средств защиты информации [5], справочно-правовых систем и систем электронного документооборота.

На данный момент в рамках реализации импортозамещения уже осуществлен перевод [6]:

12 086 шт. АРМ Пользователей ИОГВ на использование отечественных технических средств (Aquaris, Ramec, Depo, Kraftway, RDW, ГРАВИТОН, iRU) из их общего числа в 41 124 шт.;

24 482 шт. системного программного обеспечения (Базальт рабочая станция, Astra Linux Common Edition, Astra Linux Special Edition) из их общего числа в 64 305 шт.

23 207 шт. текстовых редакторов (МойОфис Профессиональный, SmetaWizard, Р-7 Офис), из их общего числа в 56 936 шт.

1 678 шт. средств проведения видеоконференцсвязи из их общего числа в 1 696 шт.

11. Реакция ИОГВ на уход с рынка иностранных технических средств и программного обеспечения

В текущих условиях эксплуатации в ИОГВ иностранного технического оборудования и ПО:

возникают сложности на фоне отсутствия технической поддержки или неисполнения гарантийных обязательств производителем;

по-прежнему отсутствует полноценная отечественная замена платформе виртуализации VMware с поддержкой миграции на нее;

отсутствует возможность миграции данных конфигурации с большей части используемого сетевого оборудования в информационной инфраструктуре ИОГВ на отечественные аналоги не осуществляя перевод информационных систем в длительный режим регламентных работ;

– обновление свободно распространяемого ПО осуществляется не из доверенного отечественного репозитория, в связи с чем не подтверждается отсутствие недекларированных возможностей, вероятно присутствующих в исходном коде свободно распространяемого ПО.

12. Об основных целях Стратегии

В рамках реализации Концепции информационной безопасности ИОГВ определены приоритетные направления в области информационной безопасности [7]. В связи с этим пути достижения требуемого уровня защищенности информации при повседневной деятельности ИОГВ определены в Стратегии.

Для формирования единой политики обеспечения информационной безопасности, достижения требуемого уровня защищенности информационных ресурсов ИОГВ, оперативного реагирования на возникающие угрозы и негативные тенденции, в рамках Стратегии предлагается рассмотреть систему обеспечения информационной безопасности (далее – СОИБ), представляющую собой комплекс мер и средств, направленных на выявление, противодействие и ликвидацию угроз безопасности информации.

Создание СОИБ направлено на достижение требуемого уровня доверия к компонентам, участвующим в информационном взаимодействии.

В результате построения СОИБ, по отношению к объектам защиты предлагается создать условия, исключающие возможность любых несанкционированных действий с ними.

Требуемый уровень безопасности объектов защиты ИОГВ предлагается достичь посредством:

– локализации информационных ресурсов в части разделения информационных систем ИОГВ на сегменты;

– учета всех субъектов информационных отношений и всех объектов защиты;

– конфигурации и настроек ПО, технических средств информационных систем ИОГВ в соответствии с требованиями по защите информации;

– целостности всех элементов объектов информатизации ИОГВ и их окружения;

– подконтрольности всех действий с объектами защиты;

– документированности всех событий, влияющих на безопасность информации;

– обеспечения постоянного мониторинга событий информационной безопасности, позволяя оперативно противодействовать внешним нарушителям и деструктивным воздействиям с их стороны на информационную инфраструктуру ИОГВ.

В рамках внедрения системы мониторинга информационной безопасности [8] (далее – СМИБ) предлагается взять за основу созданный Ведомственный центр.

В процессе мониторинга информационной безопасности Ведомственный центр осуществляет:

– анализ событий информационной безопасности и иных данных мониторинга информационной безопасности;

– контроль (анализ) защищенности информации;

– анализ и оценку функционирования систем защиты информации информационных систем ИОГВ;

– периодический анализ изменения угроз безопасности информации в информационных системах ИОГВ, возникающих в ходе их эксплуатации.

В основных подходах эксплуатации СМИБ рассматриваются:

– любые события, которые могут повлиять на безопасность информационных систем ИОГВ и их регистрацию всеми источниками (средствами защиты информации, системным программным обеспечением);

– контроль эффективности мер защиты информации и внесение своевременных изменений в обеспечение информационной безопасности информационных системах ИОГВ осуществляемого в числе прочего на основе анализа данных о событиях информационной безопасности.

Для координации и контроля действий по реализации Стратегии, в составе СМИБ, на основе соответствующих подразделений ИОГВ, необходимо сформировать систему управления информационной безопасностью (далее – СУИБ).

Основу СУИБ должна составлять организационная база, которая обеспечивает единую вертикаль управления всеми механизмами информационной безопасности из СМИБ, на всех жизненных циклах создания, передачи, обработки и хранения объектов защиты и эксплуатации.

Основной целью СУИБ является предотвращение нарушений свойств информации.

Основными задачами СУИБ являются:

– совершенствование политики в области информационной безопасности при создании и внедрении информационных систем ИОГВ;

– обеспечение соответствия мер и средств защиты информации в информационных системах ИОГВ положениям нормативных документов по защите информации;

– координация деятельности по защите информации;

– обеспечение полноты, достоверности и оперативности получения информации;

– защита от вмешательства в процесс функционирования информационных систем ИОГВ посторонними лицами;

– совершенствование системы защиты информации, ее организации, методов предотвращения реализации угроз безопасности информации, в том числе посредством дополнительных организационных и технических мер по защите информации в информационных системах ИОГВ;

– регистрация событий, влияющих на безопасность информации;

– обеспечение подконтрольности и подотчетности выполнения всех операций, совершаемых в информационных системах ИОГВ;

– анализ рисков реализации угроз безопасности информации, оценка возможного ущерба, предотвращение последствий нарушения информационной безопасности;

– создание условий для минимизации, локализации и максимально возможного возмещения ущерба в условиях реализованных угроз безопасности информации.

Учитывая вышеизложенные подходы к построению информационной безопасности, в ИОГВ сформирован проект дорожной карты развития информационной безопасности в отношении отдельных компонентов информационной инфраструктуры ИОГВ.

13. Основные тезисы из дорожной карты

Основные задачи, которые предлагается рассмотреть, в рамках подготовки дорожной карты по построению информационной безопасности к Стратегии заключаются в:

– проведении анализа зараженности информационной инфраструктуры ИОГВ по поиску индикаторов компрометации (IoC);

– запуске централизованного процесса установки обновлений системного ПО в информационной инфраструктуре ИОГВ;

– вводе централизованной аутентификации администраторов при доступе к интерфейсам управления на всем сетевом оборудовании;

– переводе все АРМ Пользователей в единый домен;

– внедрении централизованной системы создания/изменения учетных записей пользователей;

– внедрении процессов безопасной разработки ПО;

– обеспечении дополнительной защиты веб-приложений (от DDOS-атак, SQL-инъекций) различными современными средствами защиты информации;

– автоматизации процессов реагирования на инциденты информационной безопасности;

– внедрении системы контроля передвижения корпоративной информации в рамках почтового трафика ИОГВ;

– внедрении средств контроля привилегированных пользователей информационных систем ИОГВ;

– рассмотрении возможности внедрения инфраструктуры управления виртуальными рабочими столами пользователей по технологии VDI.

Проект дорожной карты по построению информационной безопасности на 2023-2025 года приведен в таблице 2.

Таблица 2

Проект дорожной карты по построению информационной безопасности на 2023-2025 года

Наименование компонента	**Период**		
	2023 год	**2024 год**	**2025 год**
Периметр информационной инфраструктуры	Провести настройку функций защиты сетевого и телекоммуникационного оборудования от атак, связанных с подменой MAC, IP-адресов и DHCP-сервера	Реализовать сегментирование и ограничить межсегментный трафик в локальной сети ИОГВ. Обеспечить дополнительную защиту веб-приложений (от DDOS-атак, SQL-инъекций)	Модернизировать систему защиты каналов связи. Рассмотреть возможность в условиях действующего законодательства Российской Федерации реализацию программы выявления уязвимостей в программных сервисах информационных систем и информационных ресурсах ИОГВ с привлечением внешних специалистов
Внутренние системы	Провести анализ зараженности информационной инфраструктуры ИОГВ по поиску индикаторов компрометации (IoC). Запустить автоматизированный процесс установки обновлений системного программного обеспечения	На почтовых системах ИОГВ, настроить расширение аутентификации электронной почты (SPF), политику DMARK и методов e-mail аутентификации DKIM	Внедрить процессы безопасной разработки программного обеспечения и контроля уязвимостей. Автоматизировать и централизовать управление учетными записями и правами доступа пользователей
Администраторы	Использовать централизованную аутентификацию администраторов при доступе к интерфейсам управления на всем сетевом оборудовании	Ограничить список протоколов управления. Не использовать незащищенные протоколы управления (telnet)	Внедрить систему контроля и отслеживания действий привилегированных пользователей, включая сотрудников аутсорсинговых организаций и внешних подрядчиков

Автоматизированные рабочие места пользователей	Ввести все АРМ Пользователей в домен, автоматически устанавливать обновления на них	Модернизировать систему защиты от несанкционированного доступа (подключить клиентское программное обеспечение серверов и АРМ Пользователей в единый центр управления)	Ввести контроль устранения уязвимостей, выявленных в результате контроля защищенности. Внедрить систему предотвращения утечек информации, блокировки передачи конфиденциальных документов. Рассмотреть возможность внедрения инфраструктуры управления виртуальными рабочими столами пользователей по технологии VDI.
Персонал	Провести киберучения с привлечением профильных специалистов	Организовать работы по формированию навыков и повышению осведомленности работников ИОГВ в сфере информационной безопасности	Разработать портал по повышению осведомленности работников ИОГВ в сфере информационной безопасности
Управление инфраструктурой	Настроить максимальный уровень журналирования на серверном оборудовании, доменах и в системных приложениях. Ввести круглосуточный режим функционирования Ведомственного центра	Внедрить систему мониторинга внешней среды на предмет выявления угроз безопасности информации. Автоматизировать процессы реагирования на компьютерные инциденты	Ввести практику проведения расследований по фактам инцидентов информационной безопасности
Административная часть объекта информатизации	Назначить ответственных, актуализировать и утвердить основные организационно-распорядительные документы	Проводить периодическую актуализацию организационно-распорядительных документов в соответствие с вводимыми мерами, а также обучение ответственных по вопросам информационной безопасности	Провести контроль состояния защищенности и аттестацию автоматизированных рабочих мест пользователей и серверной части государственных информационных систем Санкт-Петербурга

14. Результаты от реализации стратегии дорожной карты в государственных бюджетных учреждениях Санкт-Петербурга

Реализация планируемых подходов в обеспечении информационной безопасности в рамках реализации Стратегии в подведомственных бюджетных учреждениях ИОГВ (далее – ГБУ) позволит:

– централизовать решения по принимаемым мерам защиты информации;

– принимать единые подходы при выборе средств защиты информации и системного ПО;

– реализовать централизованную загрузку пакетов обновлений для системного ПО;

– организовывать проведение тестов на проникновение в информационную инфраструктуру ГБУ извне посредством развертывания программных агентов средства контроля защищенности информации;

– внедрить единую систему контроля учетных записей ГБУ в сфере здравоохранения и образования;

– завести почтовый трафик ГБУ в рамки эксплуатации системы контроля продвижения корпоративной информации в целях обеспечения защиты персональных данных от их раскрытия;

– повысить отказоустойчивость эксплуатируемых технических средств в информационной инфраструктуре ГБУ в рамках реализации импортозамещения, в связи с возможным отсутствием технической поддержки и неисполнения гарантийных обязательств.

Успешная реализация Стратегии требует непрерывного мониторинга и анализа угроз безопасности информации, актуализации и обновления различных политик и процедур информационной безопасности. Также

очень важным фактором является внедрение современных технологий и инструментов для обеспечения информационной безопасности в ИОГВ. Реализация Стратегии не только способствует защите информации и информационных систем ИОГВ, но и укрепляет доверие граждан к деятельности ИОГВ. Только таким комплексным подходом в текущих условиях можно повысить безопасность информации и защиту информационной инфраструктуры ИОГВ от угроз безопасности информации.

СПИСОК ЛИТЕРАТУРЫ

1. Распоряжение Администрации Санкт-Петербурга от 19.02.2002 № 227-ра «О создании единой мультисервисной телекоммуникационной сети исполнительных органов государственной власти Санкт-Петербурга».
2. Постановление Правительства Санкт-Петербурга от 25.08.2016 № 759 «О государственной информационной системе Санкт-Петербурга «Аппаратно-программный комплекс «Безопасный город».
3. Банк данных угроз безопасности информации (bdu.fstec.ru).
4. Методический документ «Методика оценки угроз безопасности информации» утвержден ФСТЭК России от 05.02.2021.
5. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».
6. Распоряжение Правительства Российской Федерации от 22.06.2022 № 1661-р.
7. Концепция информационной безопасности исполнительных органов государственной власти Санкт-Петербурга (утверждена от 20.02.2023 Губернатором Санкт-Петербурга А.Д. Бегловым).
8. ГОСТ Р 59547-2001 «Защита информации. Мониторинг информационной безопасности. Общие положения».

УДК 323.21

ПОДХОД К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ В РЕГИОНАЛЬНЫХ ЦЕНТРОВ УПРАВЛЕНИЯ

Ильин Николай Иванович[1], Пухов Геннадий Георгиевич[2], Антипина Елена Александровна[3]
[1]Управление информационных систем Службы специальной связи и информации ФСО России
Старая пл., 4, Москва, 103132, Россия
[2] ООО «Геонавигатор»
20-я Линия, 5-7, корп. 2, лит. Б, Санкт-Петербург, 199026, Россия
[3] ООО «Институт государственно-частного планирования»
Невский пр., 22-24, литер А, пом. 82Н, Санкт-Петербург, 191186, Россия
e-mails: fso@gov.ru, info@geonavigator.net, info@pppinstitute.ru

Аннотация. Предлагается изменить сложившуюся систему стратегического планирования на региональном уровне и возложить функции стратегического планирования на созданную систему региональных центров управления регионами, интегрировав ее в систему распределенных ситуационных центров, что позволит повысить качество и эффективность стратегического планирования в субъектах Российской Федерации и обеспечить требуемый уровень защиты информации в этой важной государственной информационной системе.

Ключевые слова: государственная политика в сфере стратегического планирования; территориальное планирование; социально-экономическое развитие федеральных округов и макрорегионов; система распределенных ситуационных центров; система стратегического планирования на региональном уровне; защита информации.

APPROACH TO INFORMATION SECURITY IN REGIONAL CONTROL CENTERS

Ilyin Nikolay[1], Pukhov Gennady[2], Antipina Elena[3]
[1] Department of Information Systems of the Special Communications and Information Service of the FSO of Russia
4 Staraya Square, 4, Moscow, 103132, Russia
[2] Geonavigator LLC
20th Line, 5-7, bldg. 2, lit. B, St. Petersburg, 199026, Russia
[3] LLC «Institute of Public-Private Planning»
22-24 Nevsky pr., letter A, room 82N, St. Petersburg, 191186, Russia
e-mails: fso@gov.ru, info@geonavigator.net, info@pppinstitute.ru

Abstract. It is proposed to change the existing strategic planning system at the regional level and assign strategic planning functions to the created system of regional regional management centers, integrating it into the system of distributed situation centers, which will improve the quality and effectiveness of strategic planning in the constituent entities of the Russian Federation and ensure the required level of information protection in this important state information system.

Keywords: state policy in the field of strategic planning; territorial planning; socio-economic development of federal districts and macro-regions; system of distributed situational centers; strategic planning system at the regional level; data protection.

В 2021 году Президентом Российской Федерации были утверждены «Основы государственной политики в сфере стратегического планирования Российской Федерации» [1], которыми определены цели, задачи и основные

направления государственной политики в сфере стратегического планирования, а также механизмы реализации этой политики и обеспечения стратегического планирования исходя из неразрывной взаимосвязи и взаимозависимости социально-экономического развития и национальной безопасности.

Современные научные исследования проблем, снижающих эффективность регионального стратегирования, доказывающие необходимость его совершенствования, определили следующие недостатки при проведении планирования:

– отсутствие конкретных критериев отбора разработчиков стратегий (в методических документах прописаны лишь возможные группы разработчиков, но не определены параметры выбора представителей от каждой группы);

– недостаточная проработка распределения функций и механизмов взаимодействия между представителями из разных групп разработчиков на каждом этапе процедуры подготовки стратегии;

– отсутствие определенного перечня целевых показателей, используемых для оценки социально-экономического развития муниципальных образований;

– отсутствие четко сформулированных методик оценки эффективности разработки и реализации стратегий социально-экономического развития муниципальных образований.

В соответствии с Постановление Правительства РФ от 26 мая 2021 г. N 786 «О системе управления государственными программами Российской Федерации» [2] с 2022 года осуществляется трансформация института госпрограмм Российской Федерации и переход на новые подходы к их разработке и реализации, включая изменение системы целеполагания, структуры и содержания, формирование новой системы управления по следующим направлениям:

–усиление координации документов стратегического планирования на всех уровнях государственного управления и местного самоуправления, повышение качества проработки в них устойчивых трендов изменения социально-экономического пространства;

–совершенствование структуры и механизмов реализации стратегий социально-экономического развития федеральных округов и макрорегионов;

–гармонизация регулирования диспропорций развития социального и экономического пространства регионов страны;

–дифференцирование стимулов развития конкурентных возможностей каждого региона (макрорегиона) страны с учетом его типологических особенностей.

Перспективными направления совершенствования процессов территориального планирования, реализация которых необходима для обеспечения согласованности процессов и документов территориального и стратегического планирования следует считать:

1)Строгое соблюдение основополагающих принципов стратегического планирования

2)Строгое соблюдение последовательности планирования. Процессы стратегического планирования должен предшествовать территориальному планированию.

3)Необходимость разработки комплекса документов не только стратегического, но и среднесрочного и краткосрочного характера, содержащих конкретные задачи, мероприятия, механизмы их реализации.

4)Необходимость выполнение принципов разработки отраслевых стратегических документов: принцип межотраслевой сбалансированности, принцип пространственной определенности, принцип последовательности планирования, принцип сквозного анализа.

В «Основах государственной политики в сфере стратегического планирования Российской Федерации» предусмотрено формирование единого цифрового информационного пространства в интересах стратегического управления в Российской Федерации с использованием существующих государственных информационных систем (ГИС) и информационных ресурсов органов власти, а также инфраструктуры, которая обеспечивает их взаимодействие.

В силу произошедших изменений политико-экономического характера в 2023 году совершенно иначе выглядит целый ряд проблем и вопросов современного экономического развития России. При этом значительная часть вызовов и угроз, стоящих перед российской экономикой, является не столько следствием санкционного давления со стороны недружественных стран, сколько результатом накопленных на протяжении последнего 35-летнего периода внутренних ограничений развития. В этих условиях необходимо ускорить имплементацию инструментов стратегического планирования в процесс формирования экономической политики России и запустить новый цикл стратегического планирования в 2024 году и тем самым вывести государственное управление на новый качественный уровень (Материалы парламентских слушаний на тему «Новые подходы к стратегическому планированию в Российской Федерации: вопросы регионального развития», Москва 2022 г.).

В соответствии с изложенным предлагается изменить сложившуюся систему стратегического планирования на региональном уровне и возложить функции стратегического планирования на созданную систему региональных центров управления (центров регионального управления).

В настоящее время Центр управления регионом (ЦУР) являются проектным офисом – единым центром мониторинга, в который поступают и оперативно отрабатываются проблемные вопросы жителей по всем направлениям, связанным с жизнью региона. Кроме того, в нем формируются аналитические материалы, характеризующие социально-экономическую ситуацию в регионе, и вырабатываются предложения по дальнейшему развитию. По сути, федеральное типовое решение для ЦУР пока выглядит как вырезанная из ситуационного центра подсистема.

С 2013 года по настоящее время была создана и эффективно работает «Система распределенных ситуационных центров», которая решает широкий перечень задач государственного управления федерального и регионального уровня, в то числе и задачи стратегического планирования. В данной системе наиболее надежно по сравнению с другими Государственными информационными система создана и функционирует система защиты информации. (Ильин, Н. И. Ситуационные центры [Текст] : опыт, состояние, тенденции развития / Н. И. Ильин, Н. Н. Демидов, Е. В. Новикова. – Москва : МедиаПресс, 2011. – 334 с. : цв. ил.; 24 см.; ISBN 978-5-902750-18-5 (в пер.).

Считаем целесообразным сложившуюся систему региональных центров управления регионами интегрировать в Систему распределенных ситуационных центров РФ с дополнением следующих функций:

–формирование концепции социально-экономического развития субъекта РФ;

–определение перечня и содержания критериев социально-экономического развития субъекта РФ;

–определение системы взаимосвязанных методик и моделей для расчета критериев социально-экономического развития субъекта РФ;

–определение структуры, формирование основных разделов и дорожной карты стратегии социально-экономического развития субъекта РФ;

–участие в мониторинге и контроле реализации основных положений стратегии социально-экономического развития в субъекте РФ.

С целью повышения качества функционирования нового облика системы стратегического планирования в регионах предлагается развернуть полноценные региональные центры управления в РАНХиГС и ее 47 филиалах, которые также должны быть включены в единую систему стратегического планирования регионов РФ.

Реализация изложенного подхода позволит существенно повысить качество и эффективность стратегического планирования в субъектах Российской Федерации и одновременно сохранить требуемый уровень защиты информации в этой важной Государственной информационной системе.

СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента РФ от 8 ноября 2021 г. N 633 «Основы государственной политики в сфере стратегического планирования Российской Федерации».
2. Постановление Правительства РФ от 26 мая 2021 г. N 786 «О системе управления государственными программами Российской Федерации».
3. Материалы парламентских слушаний на тему «Новые подходы к стратегическому планированию в Российской Федерации: вопросы регионального развития», Москва 2022 г.
4. Ильин, Н. И. Ситуационные центры [Текст] : опыт, состояние, тенденции развития / Н. И. Ильин, Н. Н. Демидов, Е. В. Новикова. - Москва : МедиаПресс, 2011. - 334 с. : цв. ил.; 24 см.; ISBN 978-5-902750-18-5 (в пер.)

УДК 656.61

ПЕРСПЕКТИВЫ РАЗВИТИЯ СПУТНИКОВЫХ И ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЙ СВЯЗИ ДЛЯ ПРОМЫШЛЕННЫХ ПОТРЕБИТЕЛЕЙ В АРКТИЧЕСКОЙ ЗОНЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Митько Арсений Валерьевич[1], Сидоров Владимир Константинович[2]
[1]Арктическая общественная академия наук
Искровский пр., 22, офис 175, Санкт-Петербург, Россия, 193168
[1]Всероссийский научно-исследовательской институт метрологии им. Д. И. Менделеева
Московский пр., 19, Санкт-Петербург, Россия, 190005
[1]Северо-Западный институт управления РАНХ и ГС
Средний проспект В. О., 57/43, Санкт-Петербург, Россия, 199178
[2]Санкт-Петербургский университет ГПС МЧС России
Московский пр., 149, Санкт-Петербург, Россия, 196105
e-mails: arseny73@yandex.ru, hamradio-spb@yandex.ru

Аннотация. Рассматриваются актуальные вопросы обеспечения бесперебойной, надежной связью добывающих предприятий, расположенных в малонаселенных и малоосвоенных районах Крайнего Севера.

Ключевые слова: Крайний Север; месторождения; добывающие предприятия; волоконно-оптическая связь; спутниковая связь; информация; телекоммуникация; инфраструктура; удаленные; малонаселенные территории; коренные малочисленные народы Севера.

PROSPECTS FOR THE DEVELOPMENT OF SATELLITE AND FIBER-OPTIC COMMUNICATION LINES FOR INDUSTRIAL CONSUMERS IN THE ARCTIC ZONE OF THE RUSSIAN FEDERATION

Mitko Arseny[1], Sidorov Vladimir[2]
[1]Arctic Public Academy of Sciences
22 Iskrovskij Av., office 175, St. Petersburg, Russia, 193168
[1]D. I. Mendeleev All-Russian research institute of metrology
19 Moskovskij Av., St. Petersburg, Russia, 190005
[1]Northwestern Institute of Management RANE and PA
57/43 Sredny Av. V. I., St. Petersburg, Russia, 199178
[2]Saint-Petersburg university of State fire service of EMERCOM of Russia
149 Moskovskij Av., St. Petersburg, Russia, 196105
e-mails: arseny73@yandex.ru, hamradio-spb@yandex.ru

Abstract. The current issues of ensuring uninterrupted, reliable communication of mining enterprises located in sparsely populated and underdeveloped areas of the Far North are considered.

Keywords: Far North; deposits; mining enterprises; fiber-optic communication; satellite communication; information; telecommunications; infrastructure; remote; sparsely populated territories; indigenous peoples of the North.

Для быстрой передачи больших потоков информации на значительные расстояния самой совершенной физической средой является оптическое волокно (ОВ). В настоящее время на основе использования волоконно-оптических кабелей (ВОК) различного конструктивного исполнения прокладываются сотни и тысячи километров волоконно-оптических линий связи (ВОЛС).

ВОЛС по сравнению с электрическими проводными сетями имеют значительно бóльшую пропускную способность, меньшее энергопотребление, высокую помехозащищенность, небольшие габаритно-массовые характеристики ОВ.

Естественными негативными свойствами ОВ, как и любой физической среды, являются оптические потери и затухание передаваемой энергии, но существенно меньшие, чем в РРС и космической связи. Выпускаемое в настоящее время отечественными и зарубежными производителями промышленное оптическое волокно имеет затухание порядка 0,2–0,3 дБ на длине волны 1,55 мкм в расчете на один километр. Малое затухание и дисперсия позволяют строить участки ВОЛС без ретрансляции протяженностью до 100 км и более.

ВОЛС имеют многочисленные преимущества перед другими способами передачи информации, однако обладают также существенными недостатками из-за дороговизны прецизионного монтажного оборудования и надежности лазерных источников излучения.

Многие из недостатков вероятнее всего будут нивелированы с появлением новых технологий. Низкие температуры в зимний период, снег и образующиеся наледи, требующие специальных методов защиты волоконно-оптических кабелей от обрыва при их прокладке воздушным способом на опорах (например, линий электропередач); наличие огромного количества водных преград и вечная мерзлота при прокладке волоконно-оптического кабеля в грунте, требующие существенных экономических затрат, также затрудняют развитие ВОЛС на Крайнем Севере по сравнению с радиорелейной связью (РРС) и космической связью. Тем не менее срок эксплуатации ВОЛС до 25 лет делает оптическую связь привлекательной по соотношению цены и качества [1].

ВОЛС в силу особенностей распространения электромагнитной энергии в ОВ, конструктивного многослойного исполнения оптического кабеля и способа прокладки линии связи, обладают повышенной защищенностью. Однако большие расстояния между участками ретрансляции в ВОЛС (более 100 км) требуют генерации световых импульсов значительной мощности. В свою очередь высокие мощности входного светового потока создают значительное по величине рассеяние на ближайших к передатчикам и ретрансляторам участках, которые могут служить каналами утечки информации [2].

ВОЛС можно подразделить на локальные и распределенные участки. Локальные участки включают в себя модуляторы, оптические передатчики, приемники и регенераторы. Локальные участки ввиду ограниченной области их расположения наиболее защищены от несанкционированного съема информации. Распределенные участки — это волоконно-оптические тракты, которые обладают большой протяженностью и, соответственно, наименьшей защищенностью от несанкционированного доступа (НСД) [3].

Следует отметить, что защитные оболочки и элементы конструкции ВОК ослабляют боковое излучение до величин, существенно меньших квантового предела обнаружения оптического излучения. Таким образом, оптические кабели в отличие от радиочастотных обладают нулевой контролируемой зоной и перехват информации при НСД возможен только при нарушении целостности внешней защитной оболочки кабеля и непосредственном доступе аппаратуры перехвата к оптическим волокнам.

В настоящее время разработана и широко используется измерительная аппаратура (оптические рефлектометры), позволяющая не только определять с высокой точностью величину полных потерь в ВОЛС, но и распределение потерь вдоль неё.

Оптический рефлектометр используется как стабилизированный источник излучения, измеритель оптической мощности и затухания оптического сигнала в процессе прокладки, эксплуатации и ремонта ВОЛС. Применение этого прибора позволяет установить общие параметры работающей ВОЛС. В настоящее время возможно одновременное использование в ОВ несущего информацию оптического сигнала и рефлектометра.

ВОЛС прокладывается на мачтах или в грунте вдоль трубопроводов, автомобильных или железных дорог. При этом нарушение целостности кабеля возможно: в результате несанкционированного доступа к линии связи, в результате аварии, обрыва кабеля из-за падения опоры или сдвига грунтов, недопустимого изгиба кабеля, действия грызунов и др. [4].

Повышение защищенности ВОЛС от грызунов, природных катаклизмов, действий злоумышленников и других нештатных воздействий особенно актуально в суровых условиях вечной мерзлоты и больших пространств малонаселенных районов Крайнего Севера.

Необходимость создания надежно защищенных ВОК, их практического внедрения и эффективного использования в ВОЛС с применением различных методов защиты информации является актуальной проблемой и постоянным насущным требованием к сохранению передаваемых сведений различного характера, составляющих личную, коммерческую и др. тайны [5].

Спутниковая связь имеет ряд своих преимуществ над РРС и ВОЛС, т. к. обеспечивает значительно более широкий охват территории и не зависит в такой степени от дорогостоящей наземной телекоммуникационной инфраструктуры.

Спутниковая связь — оптимальное техническое решение на удаленных и малонаселенных территориях Крайнего Севера. Кроме того, она позволяет обеспечить связью морские суда, кочевья оленеводов, геологические партии, а также объединить внутренние коммуникации связи населенных пунктов, государственных учреждений и добывающих предприятий.

Телекоммуникационный и информационный ресурс российского рынка практически полностью обеспечивается геостационарными спутниками ФГУП «Космическая связь» («Экспресс») и ОАО «Газпром космические системы» («Ямал»).

Спутниковая связь востребована на Крайнем Севере для телефонной и факсимильной связи, широкополосного Интернета, трансляции видеоконференций, приема теле- и радиопрограмм и др. Крупные территориально-распределенные добывающие компании в настоящее время широко используют спутниковые системы технологии VSAT2.

Существенное достоинство данной технологии — независимость от наличия местных интернет-провайдеров. Для осуществления связи с использованием технологии VSAT необходима только электроэнергия и прямая видимость на спутник.

ФГУП «Космическая связь» обеспечивает услуги спутниковой связи и телевидения с помощью геостационарной орбитальной группировки системы спутниковой связи и вещания «Экспресс», состоящей в настоящее время из 8 космических аппаратов (КА), работающих на орбите.

Система спутниковой связи и вещания ФГУП «Космическая связь» также включает в себя:

- орбитальную группировку из спутников серии «Экспресс» и наземный комплекс
- управления спутниками;
- телекоммуникационный центр и наземную инфраструктуру в составе 400 станций спутниковой связи;
- центр спутникового телевидения, обеспечивающий трансляцию теле- и радиопрограмм.

ОАО «Газпром космические системы» обеспечивает услуги спутниковой связи и телевидения с помощью геостационарной орбитальной группировки системы спутниковой связи и вещания «Ямал», состоящей в настоящее время из 5 КА.

Система спутниковой связи и вещания ОАО «Газпром космические системы» также включает в себя:

- орбитальную группировку из спутников «Ямал-202», «Ямал-300К», «Ямал-402», «Ямал-401» и наземный комплекс управления спутниками;
- телекоммуникационный центр и наземную инфраструктуру в составе 400 станций спутниковой связи;
- центр спутникового телевидения, обеспечивающий трансляцию теле- и радиопрограмм.

Через орбитальную спутниковую группировку «Ямал» ведется вещание более 200 каналов телевидения и 100 радиоканалов. Количество наземных станций спутниковой связи, функционирующих через спутники «Ямал» на территории России в районах Крайнего Севера, превысило 7,5 тысяч. Организованы каналы телемеханики в составе подвижных комплексов для проведения ремонтных и аварийно-восстановительных работ, организуется пионерная связь на новых объектах добывающих предприятий и т. д.

Российские системы спутниковой связи и вещания работают, в основном, в C- и Ku-диапазонах. В последние годы происходит переход спутниковой связи технологии VSAT на более высокочастотный Ka-диапазон, при котором антенны имеют существенно меньшие размеры [6].

Несмотря на низкий угол места, зависимость космического сигнала от погодных условий, необходимость подбирать место установки или увеличивать высоту установки антенны и др. проблемы, космические технологии связи находят широкое применение в заполярных районах Крайнего Севера. Снижение стоимости аренды каналов и оборудования даст возможность ее широкого распространения. Например, неприхотливость и простота установки оборудования технологии VSAT позволяют снижать затраты на развертывание клиентского терминала. Малые размеры рефлектора — до Ø 0,75 м позволяют не бояться северных штормовых ветров, а достаточно высокие уровни приема передаваемого сигнала позволяют обеспечить качественный канал связи.

В настоящее время наблюдается тенденция перехода от тяжелых спутников на геостационарных орбитах к орбитальным группировкам малых КА на средних и низких орбитах [7].

АО «Спутниковая система «Гонец»« предоставляет услуги связи в глобальном масштабе. Российская многофункциональная система персональной спутниковой связи (МСПСС) построена на базе низкоорбитальных космических аппаратов «Гонец». Типичными сферами применения МСПСС «Гонец-Д1М» являются сбор и передача координатно-временной информации ГЛОНАСС со средств транспорта; сбор и передача информации датчиков со стационарных или подвижных объектов в труднодоступных районах (например, мониторинг буровых вышек, метеорологических станций, трубопроводов и т. п.); персональная связь с абонентами в труднодоступных регионах; передача конфиденциальной информации между удалёнными абонентами. Услуги на базе системы оказываются в глобальном масштабе. Спутниковая система «Гонец» применяется в транспортной, нефтегазовой, рыбопромысловой отраслях. Спутники системы «Гонец» также используются для передачи сигнала ЭРА-ГЛОНАСС в районах, не покрытых наземными сетями связи.

Активное в последние годы развитие добывающих отраслей в Арктической зоне, на российском участке шельфа Ледовитого океана и в целом на Крайнем Севере накладывает на телекоммуникационные компании дополнительные обязательства по обеспечению различными видами и услугами связи добывающих предприятий, осуществляющих свою деятельность в этих районах.

Влияние экстремальных природно-климатических условий Крайнего Севера на эксплуатацию оборудования сетей и предоставление услуг, естественно, проявляется в увеличении их стоимости. Тем не менее, у населения городов и поселков, расположенных на Крайнем Севере, наиболее востребован широкополосный доступ в Интернет, несмотря на то, что интернет-трафик отличается более высокой ценой по сравнению с европейской частью страны. По мере увеличения количества разрабатываемых месторождений, а также увеличения персонала производственных объектов и роста населения спрос на услуги мобильной связи у юридических и физических лиц на Крайнем Севере из года в год растет.

Учитывая высокие темпы совершенствования и достаточно высокую сменяемость информационных технологий, наиболее экономически эффективным становится не просто оказывать услуги или предоставлять в аренду каналы связи, а предоставлять комплекс информационно-сервисных услуг. Сегодня реализация наиболее эффективной экономической модели лежит в развитии транспортной инфраструктуры связи, в активном продвижении широкополосного доступа в Интернет и других новациях.

Связь и телекоммуникационные услуги наиболее востребованы добывающими предприятиями, коренным населением, населением отдаленных населенных пунктов районов Крайнего Севера и являются эффективным экономическим направлением развития информационно-телекоммуникационной инфраструктуры в рамках устранения «цифрового неравенства».

СПИСОК ЛИТЕРАТУРЫ

1. Воронов А. А., Алехин И. Н. Прогнозирование срока службы оптических кабелей связи, эксплуатирующихся в условиях низких температур // Известия Самарского научного центра Российской академии наук. 2014. Т. 16. № 4 (3). С. 516–519.
2. Кузяков Б. А. Повышение уровня безопасности передачи информации по комбинированным оптическим линиям в наземных и бортовых системах телекоммуникаций // T-Comm — Телекоммуникации и транспорт, 2012. № 8. С. 43–46.
3. Гришачев В. В., Кабашкин В. Н., Фролов А. Д. Физические принципы формирования каналов утечки информации в волоконно-оптических линиях связи // Информационное противодействие угрозам терроризма, 2005. № 3. С. 74–76.
4. Гурлев И. В. Экологические проблемы при прокладке волоконно-оптической линии связи в грунте на Крайнем Севере // Интернет-журнал «Науковедение», 2016. Т. 8. № 6. 10 с. [Электронный ресурс]. URL: http://naukovedenie.ru/PDF/ 69EVN616.pdf (дата обращения: 30.08.2023).
5. Румянцев К. Е., Хайров И. Е. Передача конфиденциальной информации по волоконно-оптическим линиям связи, защищенная от несанкционированного доступа // Информационное противодействие угрозам терроризма, 2003. № 1, С. 72–79.
6. Гурлев И. В. Методы и способы обеспечения безопасности информации, передаваемой по спутниковой сети технологии VSAT // Интернет-журнал «Науковедение». 2017. Т. 9. № 3. 9 с. [Электронный ресурс]. URL: http://naukovedenie.ru/PDF/85EVN317.pdf (дата обращения: 30.08.2023).
7. Тестодиев Н. А., Кузовков А. В. Перспективы и приоритеты развития информационных спутниковых систем // Исследования наукограда, 2017. Т. 1. № 1 (19). С. 7–10.

УДК 004.056

НОРМАТИВНО-ПРАВОВОЕ И МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ПО ОБНАРУЖЕНИЮ, ПРЕДУПРЕЖДЕНИЮ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ И РЕАГИРОВАНИЮ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ

Сторожик Виктор Сергеевич
Арктический и антарктический научно-исследовательский институт
Беринга ул., 38, Санкт-Петербург, 199397, Россия
e-mail: vsstorozhik@aari.ru

Аннотация. Рассматриваются нормативные правовые акты, методические документы и национальные стандарты, определяющие основные направления реализации государственной политики по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и реагированию на компьютерные инциденты.

Ключевые слова: автоматизированная система управления; безопасность; защищенность; значимый объект; информационный ресурс; информационно-телекоммуникационная сеть; информационная система; компьютерная атака; компьютерный инцидент; критическая информационная инфраструктура; ликвидация последствий; обнаружение; предупреждение; реагирование; система; субъект; угроза; устойчивость; уязвимость.

REGULATORY AND METHODOLOGICAL SUPPORT FOR THE IMPLEMENTATION OF THE STATE POLICY ON DETECTING, PREVENTING AND ELIMINATING THE CONSEQUENCES OF COMPUTER ATTACKS ON THE INFORMATION RESOURCES OF THE RUSSIAN FEDERATION AND RESPONDING TO COMPUTER INCIDENTS

Storozhik Viktor
Arctic and Antarctic Research Institute
38 Bering St., St. Petersburg, 199397, Russia
e-mail: vsstorozhik@aari.ru

Abstract. The normative legal acts, methodological documents and national standards defining the main directions of implementation of the state policy on detection, prevention and elimination of consequences of computer attacks on information resources of the Russian Federation and response to computer incidents are considered.

Keywords: automated control system; security; security; significant object; information resource; information and telecommunication network; information system; computer attack; computer incident; critical information infrastructure; elimination of consequences; detection; warning; response; system; subject; threat; stability; vulnerability.

Введение. Доктрина информационной безопасности Российской Федерации к основным национальным интересам в информационной сфере относит обеспечение устойчивого и бесперебойного функционирования критической информационной инфраструктуры Российской Федерации (КИИ) в условиях проведения компьютерных атак [1].

Стратегия национальной безопасности Российской Федерации указывает, что использование иностранных информационных технологий и телекоммуникационного оборудования повышает уязвимость российский информационных ресурсов, включая объекты КИИ, к воздействию из-за рубежа и ставит задачу повышения защищенности и устойчивости функционирования информационной инфраструктуры [2].

В докладе Президента Российской Федерации «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства» на заседании Совета Безопасности Российской Федерации 20 мая 2022 г. отмечено: «Количество кибератак на российскую информационную инфраструктуру все последние годы постоянно растёт – именно все последние годы, ну а с началом специальной военной операции на Донбассе, на Украине вызовы в этой сфере стали ещё более острыми и серьёзными, более масштабными. По сути, против России развязана настоящая агрессия, война в информационном пространстве» [3].

В рамках реализации требований Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [4] Указом Президента Российской Федерации от 22 декабря 2017 г. № 620 на Федеральную службу безопасности Российской Федерации (ФСБ России) возложены функции федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) [5, 6].

В развитии ГосСОПКА можно выделить следующие этапы:

1 этап. В начале 2000-х годов были созданы и отработаны технологии и механизмы информационного взаимодействия при реагировании на компьютерные атаки (КА), компьютерные инциденты (КИ) и угрозы безопасности в отношении защищаемых информационных ресурсов (ИР).

2 этап. В 2011 году был создан Центр реагирования на компьютерные инциденты в органах государственной власти, на который были возложены функции национального CERT (англ. Computer Emergency Response Team**)** и на базе которого выстраивалась система организации взаимодействия с защищаемыми ИР.

3 этап. В январе 2013 года было принято решение о создании ГосСОПКА [7], в соответствии с которым были закреплены входящие в зону ответственности ИР: информационные системы (ИС) и информационно-телекоммуникационные сети (ИТКС), находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом, а также определены основные задачи ГосСОПКА: прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации (ИБ); обеспечение взаимодействия владельцев ИР, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий КА; осуществление контроля степени защищенности КИИ от компьютерных атак; установление причин КИ, связанных с функционированием ИР.

В Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации [8] определены назначение, функции и принципы создания ГосСОПКА, а также виды обеспечения, необходимые для ее создания и функционирования.

Основным назначением ГосСОПКА является обеспечение защищенности ИР от КА и их штатного функционирования в условиях возникновения КИ, вызванных КА.

Основные функции ГосСОПКА:

а) выявление признаков проведения КА, определение их источников, методов, способов и средств осуществления и направленности, а также разработка методов и средств обнаружения, предупреждения и ликвидации последствий КА;

б) формирование и поддержание в актуальном состоянии информации о защищаемых субъектами ГосСОПКА ИР;

в) прогнозирование ситуации в области обеспечения ИБ, включая выявленные и прогнозируемые угрозы и их оценку;

г) организация и осуществление взаимодействия с правоохранительными органами и другими государственными органами, владельцами ИР, операторами связи, интернет-провайдерами и иными заинтересованными организациями на национальном и международном уровнях в области обнаружения КА и установления их источников;

д) организация и проведение научных исследований в сфере разработки и применения средств и методов ГосСОПКА;

е) осуществление мероприятий по подготовке и повышению квалификации кадров ГосСОПКА;

ж) сбор и анализ информации о КА и вызванных ими КИ в отношении защищаемых ИР, а также о КИ в ИС и ИТКС других стран, с которыми взаимодействуют владельцы ИР;

з) осуществление мероприятий по оперативному реагированию на компьютерные атаки и вызванные ими компьютерные инциденты, а также по ликвидации их последствий;

и) выявление, сбор и анализ сведений об уязвимостях программного обеспечения и оборудования;

к) мониторинг степени защищенности ИР на всех этапах их жизненного цикла, а также разработка методических рекомендаций по их защите от КА;

м) организация и осуществление антивирусной защиты;

н) совершенствование оперативно-тактического взаимодействия сил и средств ГосСОПКА.

Основой организационно-технической составляющей ГосСОПКА являются центры, организованные по ведомственному и территориальному принципам.

К основным задачам центров ГосСОПКА относятся:

а) обнаружение, предупреждение и ликвидация последствий КА, направленных на контролируемые ИР;

б) проведение мероприятий по оценке степени защищенности контролируемых ИР;

в) проведение мероприятий по установлению причин КИ, вызванных КА на контролируемые ИР;

г) сбор и анализ данных о состоянии ИБ в контролируемых ИР;

д) осуществление взаимодействия между центрами ГосСОПКА;

е) информирование заинтересованных лиц и субъектов ГосСОПКА по вопросам обнаружения, предупреждения и ликвидации последствий КА.

Центры ГосСОПКА подразделяются на:

– главный центр, региональные центры, территориальные центры, которые создаются силами ФСБ России и обеспечивает защиту ИР органов государственной власти Российской Федерации (в том числе ФСБ России) и органов государственной власти субъектов Российской Федерации;

– центры органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации (ведомственные центры), которые создаются заинтересованными органами государственной власти, а зоной ответственности таких центров являются принадлежащие органам государственной власти ИР. Также ведомственные центры могут создаваться и эксплуатироваться в интересах

органов государственной власти организациями, осуществляющими лицензируемую деятельность в области защиты информации. Функционирование ведомственного центра обеспечивается органом государственной власти, создавшим этот центр;

– корпоративные центры могут создаваться государственными корпорациями, операторами связи и другими организациями, осуществляющими лицензируемую деятельность в области защиты информации. Функционирование корпоративного центра обеспечивается организацией, создавшей такой центр.

Центры ГосСОПКА организуют и проводят мероприятия по оценке степени защищенности КИИ от КА.

Для осуществления деятельности центра ГосСОПКА орган государственной власти (организация), создавший (создавшая) центр должна отвечать необходимым условиям:

– иметь лицензии ФСБ России и ФСТЭК России на услуги по мониторингу ИБ средств и систем информатизации;

– заключить соглашение о взаимодействии с ФСБ России;

– иметь согласованное и утвержденное в установленном порядке Положение о центре ГосСОПКА;

– иметь согласованный и утвержденный в установленном порядке Регламент деятельности центра ГосСОПКА;

– иметь согласованные и утвержденные, в установленном порядке Штатное расписание и должностные инструкции сотрудников центра ГосСОПКА.

4 этап. Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [4] было уточнено и дополнено понятие ИР: ИС, ИТКС и автоматизированные системы управления (АСУ), находящиеся на территории Российской Федерации, в дипломатических представительствах и (или) консульских учреждениях Российской Федерации, а перед ФСБ России была поставлена задача совершенствования ГосСОПКА, в том числе – создание национального координационного центра по КИ (НКЦКИ).

В качестве субъектов КИИ рассматриваются государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым принадлежат объекты КИИ, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие ИС, ИТКС, АСУ или сетей (операторы связи) [4].

В качестве объектов КИИ рассматриваются ИС, ИТКС, АСУ, принадлежащие субъекту КИИ на праве собственности, аренды или ином законном основании [4].

Значимыми объектами КИИ являются объекты, функционирующие в сферах здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, энергетики, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической, химической промышленности и топливно-энергетического комплекса, которым присвоена одна из категорий значимости и которые включены в реестр значимых объектов КИИ, [4, 10-13].

В соответствии с требованиями статьи 10 Федерального закона от 26 июля 2017 г. № 187-ФЗ [4] субъект КИИ обязан создать систему безопасности значимого объекта КИИ в соответствии с требованиями приказов ФСТЭК России № 235 и № 239 [14, 15] и обеспечить ее функционирование.

Система безопасности значимого объекта КИИ должна обеспечивать решение следующих основных задач:

1. Предотвращение нарушения конфиденциальности, целостности и доступности информации значимого объекта КИИ.

2. Недопущение воздействия на технические средства обработки информации.

3. Восстановление функционирования значимого объекта КИИ (создание и хранение резервных копий информации).

4. Непрерывное взаимодействие с ГосСОПКА.

Статьей 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ субъектам КИИ предоставлено право [4]:

1) получать от ФСБ России, информацию, необходимую для обеспечения безопасности значимых объектов КИИ, в том числе об угрозах безопасности обрабатываемой информации и уязвимости программного обеспечения, оборудования и технологий, используемых на таких объектах;

2) в порядке, установленном ФСБ России, получать от ФСБ России информацию о средствах и способах проведения КА, а также о методах их предупреждения и обнаружения;

3) при наличии согласия ФСБ России, за свой счет приобретать, арендовать, устанавливать и обслуживать средства, предназначенные для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ.

В рамках правоотношений с ФСБ России субъекты КИИ обязаны [4]:

1) незамедлительно информировать о КИ ФСБ России в установленном порядке;

2) оказывать содействие должностным лицам ФСБ России в обнаружении, предупреждении и ликвидации последствий КА, установлении причин и условий возникновения КИ;

3) в случае установки на объектах КИИ средств, предназначенных для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ, обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств, их сохранность;

4) реагировать на КИ в порядке, утвержденном ФСБ России, принимать меры по ликвидации последствий КА.

ГосСОПКА на данном этапе представляет собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ [4].

К силам ГосСОПКА относятся:

1) подразделения и должностные лица ФСБ России;

2) НКЦКИ;

3) подразделения и должностные лица субъектов КИИ, которые принимают участие в обнаружении, предупреждении и ликвидации последствий КА и в реагировании на КИ.

Средствами ГосСОПКА являются технические, программные, программно-аппаратные и иные средства для:

– обнаружения (в том числе для поиска признаков КА в сетях электросвязи, используемых для организации взаимодействия объектов КИИ);

– предупреждения КА;

– ликвидации последствий КА;

– обмена информацией, необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий КА;

– криптографические средства защиты информации;

– реагирования на КИ.

Во исполнение требований Указов Президента Российской Федерации от 15 января 2013 г. № 31 и от 20 декабря 2017 г. № 620 ГосСОПКА предназначена для решения следующих основных задач [5, 7]:

1) прогнозирование ситуации в области обеспечения ИБ;

2) обеспечение взаимодействия владельцев ИР, операторов связи и иных субъектов, осуществляющих деятельность по защите информации, по вопросам ГосСОПКА;

3) осуществление контроля степени защищенности ИР от КА;

4) установление причин КИ, связанных с функционированием ИР.

На ФСБ России возлагаются следующие полномочия [5, 6]:

а) обеспечение и контроль функционирования ГосСОПКА;

б) формирование и реализация в пределах своих полномочий государственной научно-технической политики в области обнаружения, предупреждения и ликвидации последствий КА на ИР;

в) разработка методических рекомендаций:

– по обнаружению компьютерных атак на ИР;

– по предупреждению и установлению причин КИ, связанных с функционированием ИР, а также по ликвидации последствий этих КИ.

В рамках полномочий ФСБ России в области обеспечения безопасности КИИ разработан ряд нормативных правовых актов [16-21] и методических документов:

1. Приказом ФСБ России от 27 августа 2018 г. № 366 утверждено Положение о Национальном координационном центре по компьютерным инцидентам [16], в соответствии с которым НКЦКИ предназначен для решения задачи обеспечения координации деятельности субъектов КИИ по вопросам обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ.

Для выполнения поставленной задачи НКЦКИ осуществляет следующие функции:

1.1. Координирует мероприятия по реагированию на КИ и непосредственно участвует в таких мероприятиях.

1.2. Организует и осуществляет обмен информацией о КИ между субъектами КИИ, а также между субъектами КИИ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на КИ, в том числе посредством использования технической инфраструктуры НКЦКИ, предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного взаимодействия с субъектами КИИ, а также с иными не являющимися субъектами КИИ органами и организациями, в том числе иностранными и международными.

1.3. Осуществляет методическое обеспечение деятельности субъектов КИИ по вопросам обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ.

1.4. Участвует в обнаружении, предупреждении и ликвидации последствий КА.

1.5. Обеспечивает своевременное доведение до субъектов КИИ информации о средствах и способах проведения КА и о методах их предупреждения и обнаружения.

1.6. Осуществляет сбор, хранение и анализ информации о КИ и КА, а также анализ эффективности мероприятий по обнаружению, предупреждению и ликвидации последствий КА и реагированию на КИ.

1.7. Осуществляет эксплуатацию, обеспечение функционирования и развитие технической инфраструктуры НКЦКИ.

1.8. Организует получение информации, представляемой в соответствии с законодательством Российской Федерации в ГосСОПКА субъектами КИИ и ФСТЭК России, а также информации, которая может представляться иными не являющимися субъектами КИИ органами и организациями, в том числе иностранными и международными.

1.9. Определяет необходимые для организации взаимодействия форматы представления информации о КИ в ГосСОПКА и доводит их до субъектов КИИ.

1.10. Определяет состав технических параметров КИ, указываемых при представлении информации в ГосСОПКА, и доводит его до субъектов КИИ.

НКЦКИ в пределах своей компетенции имеет право:

а) направлять в рамках своих полномочий уведомления и запросы субъектам КИИ, а также иным не являющимся субъектами КИИ органам и организациям, в том числе иностранным и международным;

б) отказывать в предоставлении информации о КИ, связанных с функционированием объектов КИИ, по запросам органа иностранного государства или международной организации, не обладающих полномочиями направлять такой запрос, а также в случаях, когда предоставление такой информации создает угрозу безопасности Российской Федерации;

в) создавать рабочие группы из представителей субъектов КИИ по согласованию с их руководством для решения вопросов, отнесенных к компетенции НКЦКИ;

г) привлекать к реагированию на КИ организации и экспертов;

д) распространять и публиковать информационные и справочные материалы, участвовать в работе научно-технических конференций, симпозиумов, совещаний, выставок, в том числе международных, по вопросам, отнесенным к компетенции НКЦКИ;

е) заключать от своего имени соглашения о сотрудничестве в области обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ.

НКЦКИ возглавляет директор, которым является заместитель руководителя Научно-технической службы — начальник Центра защиты информации и специальной связи ФСБ России.

2. Приказом ФСБ России от 24 июля 2018 г. № 367 утверждены Перечень информации, представляемой в ГосСОПКА (Перечень) и Порядок представления информации в ГосСОПКА [17].

Перечень включает:

2.1. Информацию, содержащуюся в реестре значимых объектов КИИ.

2.2. Информацию об отсутствии необходимости присвоения объекту КИИ одной из категорий значимости.

2.3. Информацию об исключении объекта КИИ из реестра значимых объектов КИИ, а также об изменении категории его значимости.

2.4. Информацию по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов КИИ о нарушении требований по обеспечению безопасности значимых объектов КИИ, в результате которого создаются предпосылки возникновения КИ.

2.5. Информацию о КИ, связанных с функционированием объектов КИИ (дата, время, место нахождения или географическое местоположение объекта КИИ, на котором произошел КИ; наличие причинно-следственной связи между КИ и КА; связь с другими КИ (при наличии); состав технических параметров КИ; последствия КИ).

2.6. Иную информацию в области обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ, предоставляемую субъектами КИИ и иными не являющимися субъектами КИИ органами и организациями, в том числе иностранными и международными.

Информация, указанная в пунктах 2.1 – 2.4 Перечня представляется ФСТЭК России в НКЦКИ не реже раза в месяц и не позднее месячного срока с момента изменения соответствующих сведений об объекте КИИ.

Информация, указанная в пункте 2.5 Перечня представляется субъектом КИИ в НКЦКИ в соответствии с определенными НКЦКИ форматами с использованием технической инфраструктуры НКЦКИ. В случае отсутствия подключения к технической инфраструктуре НКЦКИ информация направляется посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте.

Срок представления указанной информации субъектом КИИ в НКЦКИ не позднее 24 часов с момента обнаружения КИ. Уведомление от НКЦКИ о получении информации направляется субъекту КИИ не позднее 24 часов с момента ее получения.

Информация, указанная в пункте 2.6 Перечня, представляется в ГосСОПКА (НКЦКИ) перечисленными выше способами в сроки, достаточные для своевременного проведения мероприятий по обнаружению, предупреждению и ликвидации последствий КА и реагированию на КИ.

3. Приказом ФСБ России от 24 июля 2018 г. № 368 утверждены Порядок обмена информацией о КИ между субъектами КИИ, между субъектами КИИ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями,

осуществляющими деятельность в области реагирования на КИ, и Порядок получения субъектами КИИ информации о средствах и способах проведения КА и о методах их предупреждения и обнаружения [18].

3.1. При проведении мероприятий по реагированию на КИ, связанные с функционированием объектов КИИ, субъекты КИИ осуществляют обмен информацией о таких КИ с другими субъектами КИИ в целях минимизации последствий КИ и предотвращения КИ на других объектах КИИ. Субъекты КИИ вправе самостоятельно определять круг субъектов КИИ, с которыми осуществляется такой обмен. Обмен информацией о КИ осуществляется в сроки, достаточные для своевременного проведения мероприятий по обнаружению, предупреждению и ликвидации последствий КА и реагированию на КИ. Обмен информацией осуществляется субъектами КИИ путем взаимного направления уведомлений в соответствии с форматами, определенными НКЦКИ, а также запросов, уточняющих представляемую информацию, посредством почтовой, факсимильной, электронной или телефонной связи (при возможности — с использованием технической инфраструктуры НКЦКИ). Одновременно с направлением информации о КИ в рамках обмена субъекты КИИ информируют об этом НКЦКИ.

Обмен информацией о КИ с иностранными (международными) организациями осуществляется НКЦКИ, за исключением случаев, когда обмен субъекта КИИ такой информацией напрямую с иностранной (международной) организацией предусмотрен международным договором Российской Федерации.

В случае необходимости осуществления обмена информацией о КИ с иностранной (международной) организацией субъект КИИ направляет в НКЦКИ обращение, содержащее обоснование необходимости обмена этой информацией с приложением составляющей предмет обмена информации. НКЦКИ незамедлительно информирует субъект КИИ о получении его обращения.

НКЦКИ в течение 24 часов после получения обращения рассматривает информацию о КИ. В случае принятия решения о передаче этой информации в иностранную (международную) организацию, незамедлительно направляет ее адресату, о чем одновременно информируется субъект КИИ, направивший обращение. При принятии НКЦКИ решения об отказе в передаче информации о КИ иностранной (международной) организации субъект КИИ, направивший обращение, информируется об этом в течение 24 часов. При получении ответа от иностранной (международной) организации НКЦКИ в течение 12 часов направляет данный ответ субъекту КИИ, направившему обращение.

В случае если обмен информацией о КИ, связанных с функционированием объектов КИИ, напрямую с иностранной (международной) организацией предусмотрен международным договором Российской Федерации, субъекты КИИ также направляют такую информацию в НКЦКИ с указанием реквизитов международного договора Российской Федерации. В случае получения субъектом КИИ информации о КИ, связанном с функционированием объекта КИИ, инициативно направленной иностранной (международной) организацией, субъект КИИ направляет полученную информацию в НКЦКИ не позднее 24 часов с момента получения такой информации.

3.2. Субъекты КИИ получают информацию о средствах и способах проведения КА и о методах их предупреждения и обнаружения путем:

3.2.1. Обращения к официальному сайту в ИТКС «Интернет» по адресу: http://cert.gov.ru.

3.2.2. Направления запросов в НКЦКИ с использованием технической инфраструктуры НКЦКИ либо, при отсутствии подключения к ней, посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте по адресу: http://cert.gov.ru. Ответ субъекту КИИ предоставляется в пятидневный срок с момента получения такого запроса.

3.2.3. Направления обращений в ФСБ России.

3.2.4. Направления запросов другим субъектам КИИ, иностранным (международным) организациям, если такой запрос не содержит сведений о КИ, связанных с функционированием объектов КИИ.

НКЦКИ осуществляет направление субъектам КИИ информации о средствах и способах проведения КА и о методах их предупреждения и обнаружения с учетом особенностей функционирования объектов КИИ посредством использования технической инфраструктуры НКЦКИ. В случае отсутствия у субъекта КИИ подключения к технической инфраструктуре НКЦКИ, информация направляется посредством почтовой, факсимильной или электронной связи. Направление информации о средствах и способах проведения КА и о методах их предупреждения и обнаружения субъекту КИИ осуществляется в срок не позднее 24 часов с момента получения НКЦКИ такой информации.

4. Приказом ФСБ России от 6 мая 2019 г. № 196 утверждены Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ (средства ГосСОПКА) [19]:

4.1. В средствах ГосСОПКА должна быть исключена возможность удаленного управления со стороны лиц, не являющихся работниками субъекта КИИ и (или) работниками привлекаемой в соответствии с законодательством Российской Федерации субъектом КИИ организации, осуществляющей лицензируемую деятельность в области защиты информации.

4.2. В средствах ГосСОПКА должна быть исключена возможность несанкционированной передачи обрабатываемой информации лицам, не являющимся работниками субъекта КИИ и (или) работниками привлекаемой субъектом КИИ организации, осуществляющей лицензируемую деятельность в области защиты информации.

4.3. Средства ГосСОПКА должны иметь возможность модернизации российскими организациями, не находящимися под прямым или косвенным контролем иностранных физических лиц и (или) юридических лиц.

4.4. Средства ГосСОПКА должны быть обеспечены гарантийной и технической поддержкой российскими организациями, не находящимися под прямым или косвенным контролем иностранных физических лиц и (или) юридических лиц.

4.5. Работа средств ГосСОПКА не должна приводить к нарушениям функционирования информационных ресурсов (должно быть исключено влияние на достижение целей и функционирование объектов КИИ).

4.6. В средствах ГосСОПКА должны быть реализованы функции безопасности, обеспечивающие:

- идентификацию и аутентификацию пользователей;
- разграничение прав доступа к информации и функциям;
- регистрацию событий информационной безопасности;
- обновление программных компонентов и служебных баз данных;
- резервирование и восстановление своей работоспособности;
- синхронизацию системного времени и корректировку временных значений;
- контроль целостности программного обеспечения.

5. Приказом ФСБ России от 19 июня 2019 г. № 281 утверждены Порядок и Технические условия установки и эксплуатации средств предназначенных, для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ, за исключением средств, предназначенных для поиска признаков КА в сетях электросвязи, используемых для организации взаимодействия объектов КИИ [20].

Для согласования установки средств субъект КИИ не позднее чем за 45 календарных дней до даты планируемой установки направляет в ФСБ России структурно-функциональную схему подключения средств к ИС, ИТКС, АСУ, а также сведения:

- об устанавливаемых средствах (наименование, предназначение, версия (при наличии);
- о местах установки средств;
- о лицах, ответственных за эксплуатацию средств;
- о контролируемых средствами объектах КИИ.

ФСБ России в срок до 45 календарных дней с даты поступления рассматривает представленные сведения на предмет отсутствия или наличия оснований для отказа в согласовании установки средств. По результатам рассмотрения ФСБ России направляет субъекту КИИ уведомление о согласовании или об отказе в согласовании установки средств.

Изменение структурно-функциональной схемы подключения средств к ИС, ИТКС, АСУ, состава установленных средств и (или) мест их установки осуществляется субъектом КИИ по согласованию с ФСБ России.

При изменении иной информации субъект КИИ информирует ФСБ России в течение 5 календарных дней со дня ее изменения.

Установка, настройка, проверка работоспособности и подключение средств к ИР проводятся субъектом КИИ и (или) привлекаемой субъектом КИИ организацией, осуществляющей лицензируемую деятельность в области защиты информации, и осуществляются в соответствии с эксплуатационной документацией на данные средства. При этом установка средств не должна нарушать функционирование объекта КИИ. Субъект КИИ после приема в эксплуатацию средств информирует об этом НКЦКИ в течение 5 календарных дней.

В целях непрерывного взаимодействия с ГосСОПКА субъект КИИ обеспечивает круглосуточную и бесперебойную работу средств.

Эксплуатация и техническое обслуживание средств осуществляется субъектом КИИ и (или) привлекаемой субъектом КИИ организацией, осуществляющей лицензируемую деятельность в области защиты информации, в соответствии с эксплуатационной документацией на данные средства.

6. Приказом ФСБ России от 19 июня 2019 г. № 282 утвержден Порядок информирования ФСБ России о КИ, реагирования на них, принятии мер по ликвидации последствий КА, проведенных в отношении значимых объектов КИИ [21].

Субъекты КИИ обязаны информировать ФСБ России обо всех КИ, связанных с функционированием принадлежащих им объектов КИИ, путем направления информации в НКЦКИ с использованием технической инфраструктуры НКЦКИ либо, при отсутствии подключения к ней, посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте.

Информация о КИ, связанном с функционированием значимого объекта КИИ, направляется субъектом КИИ в НКЦКИ в срок не позднее 3 часов с момента обнаружения КИ, а в отношении иных объектов КИИ – в срок не позднее 24 часов с момента его обнаружения.

Для подготовки к реагированию на КИ и принятию мер по ликвидации последствий КА субъектом КИИ в срок до 90 календарных дней со дня включения данного объекта в реестр значимых объектов КИИ разрабатывается план реагирования на КИ и принятия мер по ликвидации последствий КА (План), содержащий:

– технические характеристики и состав значимых объектов КИИ;

– события (условия), при наступлении которых начинается реализация предусмотренных Планом мероприятий;

– мероприятия, проводимые в ходе реагирования на КИ и принятия мер по ликвидации последствий КА, а также время, отводимое на их реализацию;

– описание состава подразделений и должностных лиц субъекта КИИ, ответственных за проведение мероприятий.

Разработанный План утверждается руководителем субъекта КИИ (индивидуальным предпринимателем — субъектом КИИ). Копия утвержденного Плана в срок до 7 календарных дней со дня утверждения направляется в НКЦКИ.

При необходимости в План включаются:

– условия привлечения подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА;

– порядок проведения субъектом КИИ мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА в отношении значимых объектов КИИ совместно с привлекаемыми подразделениями и должностными лицами ФСБ России.

В указанном случае проект Плана разрабатывается субъектом КИИ при методическом обеспечении НКЦКИ и до его утверждения направляется на согласование в ФСБ России. ФСБ России рассматривает проект Плана в срок до 30 календарных дней и по результатам рассмотрения согласовывает его или возвращает без согласования для доработки.

Субъект КИИ не реже одного раза в год организует и проводит тренировки по отработке мероприятий Плана. Объем и содержание тренировки определяются субъектом КИИ с учетом мероприятий, содержащихся в Плане. Организация и проведение тренировок возлагаются на подразделения и должностных лиц субъекта КИИ, ответственных за проведение мероприятий по реагированию на КИ и принятие мер по ликвидации последствий КА. При необходимости по результатам тренировок в План вносятся изменения.

Субъект КИИ в ходе реагирования на КИ и принятия мер по ликвидации последствий КА осуществляет:

– анализ КИ (включая определение очередности реагирования на них), установление их связи с КА;

– проведение мероприятий в соответствии с Планом;

– определение в соответствии с Планом необходимости привлечения к реагированию на КИ и принятию мер по ликвидации последствий КА подразделений и должностных лиц ФСБ России.

Перед принятием мер по ликвидации последствий КА субъект КИИ определяет:

– состав подразделений и должностных лиц субъекта КИИ, ответственных за проведение мероприятий по реагированию на КИ и принятие мер по ликвидации последствий КА, и их задачи в рамках принимаемых мер;

– перечень средств, необходимых для принятия мер по ликвидации последствий КА;

– очередность значимых объектов КИИ (их структурных элементов), в отношении которых будут приниматься меры по ликвидации последствий КА;

– перечень мер по восстановлению функционирования значимого объекта КИИ.

– В ходе ликвидации последствий КА субъектом КИИ принимаются меры по восстановлению функционирования и проверке работоспособности значимого объекта КИИ.

– О результатах мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА субъект КИИ информирует НКЦКИ в срок не позднее 48 часов после завершения таких мероприятий.

7. Требования к подразделениям и должностным лицам субъекта ГосСОПКА.

Методический документ определяет основные задачи подразделений и должностных лиц субъекта ГосСОПКА, требования к кадровому обеспечению и деятельности центров ГосСОПКА. Распределяет роли сотрудников центра ГосСОПКА по линиям реагирования. Выделяет классы центров ГосСОПКА в зависимости от объема функций, выполняемых центром самостоятельно.

8. Методические рекомендации по созданию ведомственных и корпоративных центров ГосСОПКА.

9. Типовой Регламент информационного взаимодействия.

Определяет режимы и порядок взаимодействия подразделений ФСБ России с другими организациями. Устанавливает функции подразделений, формы информационного взаимодействия, типы передаваемых сообщений и их виды. Определяет требования к функциональным возможностям и характеристикам технических средств, необходимых для решения задач центров ГосСОПКА.

10. Методические рекомендации по обнаружению КА на ИР.

Определяют порядок действий по обнаружению атак, классифицируют атаки и дают рекомендации по повышению уровня защищенности объектов атаки.

11. Методические рекомендации по установлению причин и ликвидации последствий КИ, связанных с функционированием ИР.

Определяют порядок и основные задачи при реагировании на КИ. Устанавливают классы КИ.

12. Методические рекомендации по проведению мероприятий по оценке степени защищенности от КА.

Определяют основные задачи, порядок и этапы проведения мероприятий по оценке степени защищенности. Устанавливают порядок оценки возможностей злоумышленника при проведении КА.

Таким образом, субъект КИИ для выполнения требований по организации взаимодействия с ГосСОПКА (НКЦКИ) должен разработать и утвердить следующие организационно-распорядительные документы:

а) приказ о назначении ответственных должностных лиц;

б) должностные инструкции для ответственных лиц;

в) регламент выявления КИ и реагирования на них;

г) план реагирования на КИ и принятия мер по ликвидации последствий КА;

д) регламент взаимодействия с НКЦКИ;

е) форма карточки КИ;

ж) журнал учета КИ.

В соответствии с частью 5 статьи 6 Федерального закона от 26 июля 2017 г. N 187-ФЗ [4] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) в рамках своих полномочий [22] утвердило Порядок установки и эксплуатации средств, предназначенных для поиска признаков КА в сетях электросвязи, используемых для организации взаимодействия объектов КИИ (Порядок), и Технические условия установки и эксплуатации средств, предназначенных для поиска признаков КА в сетях электросвязи, используемых для организации взаимодействия объектов КИИ (Технические условия) [23].

Порядок определяет требования к установке и эксплуатации средств, предназначенных для поиска признаков КА в сетях электросвязи, используемых для организации взаимодействия объектов КИИ, а также регулирует процедуру взаимодействия ФСБ России, Минцифры России и операторов связи.

Необходимость и места установки средств поиска КА на сети электросвязи, обеспечивающей взаимодействие объектов КИИ, определяются ФСБ России (ответственными лицами ГосСОПКА) на основании оценки безопасности КИИ. Установку в сетях электросвязи средств поиска КА организует ФСБ России. Установка средств поиска КА, их подключение к сетям электросвязи и каналам связи проводятся ФСБ России (ответственными лицами ГосСОПКА) или Организацией (в случае привлечения) и оператором связи в срок не более 60 рабочих дней со дня согласования ФСБ России схем установки, если иной срок не согласован ФСБ России. Прием в эксплуатацию установленных средств поиска КА осуществляется комиссией, назначенной оператором связи из представителей ФСБ России (ответственных лиц ГосСОПКА), Организации (в случае привлечения) и оператора связи. По результатам приемки оформляется Акт приемки. Эксплуатация средств поиска КА осуществляется ФСБ России (ответственными лицами ГосСОПКА). Непрерывность функционирования в круглосуточном режиме и сохранность средств поиска атак обеспечиваются оператором связи самостоятельно путем соблюдения Технических условий.

Для организации взаимодействия с ГосСОПКА оператор связи определяет ответственных лиц.

Техническое обслуживание установленных средств поиска атак проводится ответственными лицами ГосСОПКА или Организацией (в случае привлечения).

Технические условия, разработаны с учетом требований к средствам поиска КА в ГосСОПКА, установленных приказом ФСБ России от 6 мая 2019 г. № 196 [19].

5 этап. Указом Президента Российской Федерации от 1 мая 2022 г. № 250 постановлено:

– руководителям федеральных органов исполнительной власти, высших исполнительных органов государственной власти субъектов Российской Федерации, государственных фондов, государственных корпораций (компаний) и иных организаций, созданных на основании федеральных законов, стратегических предприятий, стратегических акционерных обществ и системообразующих организаций российской экономики, юридических лиц, являющихся субъектами критической информационной инфраструктуры Российской Федерации (органы (организации) возложить на заместителя руководителя органа (организации) полномочия по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий КА и реагированию на КИ;

– создать в органе (организации) структурное подразделение, осуществляющее функции по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий КА и реагированию на КИ, либо возложить данные функции на существующее структурное подразделение;

– принимать в случае необходимости решения о привлечении организаций к осуществлению мероприятий по обнаружению, предупреждению и ликвидации последствий КА и реагированию на КИ. При этом могут привлекаться исключительно организации, являющиеся аккредитованными центрами ГосСОПКА;

ФСБ России организовать аккредитацию центров ГосСОПКА;

ФСБ России определить переходный период, в течение которого допускается осуществлять мероприятия по обнаружению, предупреждению и ликвидации последствий КА и реагированию на КИ в интересах органов (организаций) на основании заключенных с ФСБ России (НКЦКИ) соглашений о сотрудничестве (взаимодействии) [24].

Во исполнение Указа Президента Федерации от 1 мая 2022 г. № 250:

– определен 3-годичный переходный период, в течение которого допускается осуществлять мероприятия по обнаружению, предупреждению и ликвидации последствий КА и реагированию на КИ в интересах органов (организаций) на основании заключенных с ФСБ России (НКЦКЦИ) соглашений о сотрудничестве [25];

– утверждены требования о защите информации, содержащейся в государственных ИС, с использованием шифровальных (криптографических) средств [26];

– утвержден порядок осуществления мониторинга защищенности ИР [27].

– 20 июня 2023 г. началось публичное обсуждение изменений в Указ Президента Российской Федерации от 1 мая 2022 г. № 250, которые предусматривают [28]:

– информировать ФСБ России о КИ и КА, связанных с функционированием ИР органов (организаций);

– определить порядок аккредитации центров ГосСОПКА и требования к ним, осуществлять контроль за деятельностью аккредитованных центров ГосСОПКА;

– определить порядок информирования ФСБ России о КИ и КА, связанных с функционированием ИР органов (организаций);

– определить порядок, технические условия установки и эксплуатации в ИР органов (организаций) средств, предназначенных для поиска признаков КА, и организовать их установку.

ФСБ России в настоящее время разрабатываются проекты:

положения об аккредитации центров ГосСОПКА;

требований к центрам ГосСОПКА и порядка контроля за деятельностью аккредитованных центров ГосСОПКА;

порядка информирования ФСБ России о КИ и КА, связанных с функционированием ИР органов (организаций);

порядка, технических условий установки и эксплуатации в ИР органов (организаций) средств, предназначенных для поиска признаков КА.

Положение об аккредитации центров ГосСОПКА будет определять:

а) порядок и сроки подачи заявки на аккредитацию;

б) порядок и сроки формирования аттестационной комиссии;

в) критерии, по которым будет проводиться аккредитация;

г) порядок и содержание этапов проведения проверок в ходе аккредитации;

д) порядок выдачи аттестата аккредитации и срок его действия;

е) порядок приостановки действия аккредитации центра ГосСОПКА;

ж) порядок прекращения действия аккредитации центра ГосСОПКА.

Требования к центрам ГосСОПКА будут определять:

а) задачи и функции центров ГосСОПКА;

б) требования к персоналу центров ГосСОПКА (уровень образования, компетенции);

в) классы центров ГосСОПКА (по видам деятельности и наборам функций;

г) требования к деятельности центров ГосСОПКА;

д) требования к составу центров ГосСОПКА.

В 2022 году Федеральным агентством по техническому регулированию и метрологии утверждены и введены в действие национальные стандарты в области обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ [29-34]:

ГОСТ Р 59709-2022 Защита информации. Управление компьютерными инцидентами. Термины и определения.

ГОСТ Р 59710-2022 Защита информации. Управление компьютерными инцидентами. Общие положения.

ГОСТ Р 59711-2022 Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами.

ГОСТ Р 59712-2022 Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты.

ГОСТ Р 59548-2022 Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации.

ГОСТ Р 70262.1-2022 Защита информации. Идентификация и аутентификация. Уровни доверия идентификации.

Федеральным законом от 14 июля 2022 г. № 266-ФЗ [35] статья 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» дополнена частью 12 с 1 сентября 2022 г. [36], которая обязывает оператора персональных данных в порядке, определенном ФСБ России, обеспечивать взаимодействие с ГосСОПКА, включая информирование его о КИ, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

Приказом ФСБ России от 13 февраля 2023 г. № 77 утвержден порядок взаимодействия операторов с ГосСОПКА, включая информирование ФСБ России о КИ, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных [37].

Порядок взаимного обмена информацией о КИ, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных, между ФСБ России и Роскомнадзором в настоящее время представлен проектом совместного приказа Роскомнадзора и ФСБ России и проходит общественное обсуждение.

Заключение. Выполнение требований нормативных правовых актов Российской Федерации, национальных стандартов, нормативных правовых актов и методических документов ФСБ России, ФСТЭК России и Минцифры России, определяющих основные направления реализации государственной политики по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и реагированию на компьютерные инциденты, создает субъектам КИИ и операторам персональных данных условия для обеспечение защищенности информационных ресурсов от компьютерных атак и обеспечения их штатного функционирования в условиях возникновения компьютерных инцидентов, вызванных целевыми компьютерными атаками. Руководители и должностные лица органов (организаций), включая субъекты КИИ, допустившие нарушение указанных требований в области обеспечения безопасности защищаемых информационных ресурсов, несут административную и уголовную ответственность в соответствии с законодательством Российской Федерации [38, 39].

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646).
2. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 2 июля 2021 г. № 400).
3. «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства» : доклад Президента Российской Федерации В. В. Путина 20 мая 2022 г. на заседании Совета Безопасности Российской Федерации.
4. «О безопасности критической информационной инфраструктуры Российской Федерации»: Федеральный закон от 26 июля 2017 г. № 187-ФЗ.
5. «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» : Указ Президента Российской Федерации от 20 декабря 2017 г. № 620.
6. Положение о Федеральной службе безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 11 августа 2003 г. № 960 «Вопросы Федеральной службы безопасности Российской Федерации»).
7. «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (выписка) : Указ Президента Российской Федерации от 15 января 2013 г. № 31.
8. Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утверждена Президентом Российской Федерации 12 декабря 2014 г. № К 1274).
9. «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085» : Указ Президента Российской Федерации от 25 ноября 2017 г. № 569.
10. «Вопросы Федеральной службе по техническому и экспортному контролю» : Положение о Федеральной службе по техническому и экспортному контролю, утв. Указом Президента Российской Федерации от 16 августа 2004 г. № 1085..
11. «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений (в редакции Постановлений Правительства Российской Федерации от 13 апреля 2019 г. № 452, от 24 декабря 2021 г. № 2431, от 19 августа 2022 г. № 1463, от 20 декабря 2022 г. № 2360) : Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127.
12. «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» : Приказ ФСТЭК России от 6 декабря 2017 г. № 227.
13. «О внесении изменений в Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденный приказом Федеральной службы по техническому и экспортному контролю от 6 декабря 2017 г. № 227» : Приказ ФСТЭК России от 10.02.2022 г. № 26.
14. «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» : Приказ ФСТЭК России от 21 декабря 2017 г. № 235.
15. «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» : Приказ ФСТЭК России от 25 декабря 2017 г. № 239.
16. «Об утверждении Положения о Национальном координационном центре по компьютерным инцидентам» : Приказ ФСБ России от 27 августа 2018 г. № 366.
17. «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» : Приказ ФСБ России от 24 июля 2018 г. № 367.
18. «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» : Приказ ФСБ России от 24 июля 2018 г. № 368.
19. «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» : Приказ ФСБ России от 6 мая 2019 г. № 196.
20. «Об утверждении Порядка, технических условий установки и эксплуатации средств предназначенных, для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации» : Приказ ФСБ России от 19 июня 2019 г. № 281.
21. «Об утверждении порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятии мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» : Приказ ФСБ России от 19 июня 2019 г. № 282.
22. Положение о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации (утв. постановлением Правительства Российской Федерации от 2 июня 2008 г. № 418).

23. «Об утверждении Порядка и Технических условий установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации» : Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 17 марта 2020 г. № 114.
24. «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» : Указ Президента Российской Федерации от 1 мая 2022 г. № 250.
25. «Об определении переходного периода, предусмотренного подпунктом «б» пункта 5 Указа Президента Российской Федерации от 1 мая 2022 г. № 250» : Приказ ФСБ России от 1 ноября 2022 г. № 543.
26. «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств» : Приказ ФСБ России от 24 октября 2022 г. № 524.
27. «Об утверждении порядка осуществления мониторинга защищенности информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным корпорациям (компаниям), иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами критической информационной инфраструктуры Российской Федерации» : Приказ ФСБ России от 11 мая 2023 г. № 213.
28. Проект «О внесении изменений в Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». [Электронный ресурс]. URL: https://regulation.gov.ru/projects#npa=139316.
29. ГОСТ Р 59709-2022. Защита информации. Управление компьютерными инцидентами. Термины и определения. М.: ФГБУ «РСТ», 2022.
30. ГОСТ Р 59710-2022. Защита информации. Управление компьютерными инцидентами. Общие положения. Введен в действие: 01.02.2023. М. : ФГБУ «РСТ», 2022. 16 с.
31. ГОСТ Р 59711-2022. Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами. Введен в действие: 01.02.2023. М. : ФГБУ «РСТ», 2022. 28 с.
32. ГОСТ Р 59712-2022. Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты. Введен в действие: 01.02.2023. М. : ФГБУ «РСТ», 2022. 20 с.
33. ГОСТ Р 59548-2022. Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации. Введен в действие: 02.01.2022. М. : ФГБУ «РСТ», 2022. 70 с.
34. ГОСТ Р 70262.1-2022. Защита информации. Идентификация и аутентификация. Уровни доверия идентификации. Введен в действие: 01.01.2023. М. : ФГБУ «РСТ», 2022. 24 с.
35. «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности» : Федеральный закон от 14 июля 2022 г. № 266-ФЗ.
36. «О персональных данных» (с изменениями и дополнениями) : Федеральный закон от 27 июля 2006 г. № 152-ФЗ.
37. «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных» : Приказ ФСБ России от 13.02.2023. № 77.
38. «Уголовный кодекс Российской Федерации» (с изменениями и дополнениями) : Федеральный закон от 13.06.1996. № 63-ФЗ.
39. «Кодекс Российской Федерации об административных правонарушениях» (с изменениями и дополнениями) : Федеральный закон от 30.12.2001. № 95-ФЗ.

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИЕ И ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 004.056:51(075.8)

О НЕКОТОРЫХ МАТЕМАТИЧЕСКИХ МЕТОДАХ, ПРИМЕНЯЕМЫХ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Воронов Сергей Алексеевич, Ефимова Анна Борисовна, Примакин Алексей Иванович
Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: voronov-sci@mail.ru, abefimova020770@mail.ru, a.primakin@mail.ru

Аннотация. В статье представлены некоторые математические методы, применяемые в области защиты информации, в частности, в современной криптографии. Несколько подробней рассмотрены особенности математической функции — эллиптической кривой, в силу ее применения в технологии криптовалют.

Ключевые слова: математические методы; эллиптические кривые; криптосистемы на эллиптических кривых.

ON SOME MATHEMATICAL METHODS USED IN THE FIELD OF INFORMATION PROTECTION

Voronov Sergey, Efimova Anna, Primakin Alexey
St. Petersburg Military Order of Zhukov Institute of National Guard Troops of the Russian Federation
1 Pilot Pilyutova St., St. Petersburg, 198206, Russia
e-mail: voronov-sci@mail.ru, abefimova020770@mail.ru, a.primakin@mail.ru

Abstract. The article presents some mathematical methods used in the field of information protection, in particular, in modern cryptography. The features of a mathematical function — an elliptic curve, due to its application in cryptocurrency technology, are considered in several details.

Keywords: mathematical methods; elliptic curves; cryptosystems on elliptic curves.

Введение. В основе технологий защиты информации, в первую очередь — криптографических средств защиты информации, лежат совокупности математических методов и алгоритмов, обеспечивающие ее конфиденциальность, целостность, аутентификацию, безопасность от атак противника. Основной составляющей криптографической защиты являются криптоалгоритмы, построенные на преобразовании информации и на использовании приватных ключей. При этом необходимо учитывать принцип, утверждающий, что надежность криптоалгоритма не зависит от секретности самого криптоалгоритма, о обеспечивается только секретностью приватного ключа. В связи с этим, параметр, определяющий качество криптоалгоритма, его криптографическая стойкость, т.е. устойчивость к попыткам противника получить приватный ключ [1].

Для обеспечения криптографической стойкости необходимо провести математическую формализацию задачи и создать математические модели исследуемых процессов.

В современной литературе по криптографии представлены различные подходы к построению математических моделей и процессов [2, 3]. Математика, которая в них представлена, касается разделов теории чисел, алгебраических основ криптографии, алгебраической геометрии. Рассматриваются детерминированная и вероятностная модели независимых биграмм, марковски зависимых букв и т.п.

Широко известно, что исторически в криптографии существуют два типа преобразований — замены и перестановки символов, а все остальные криптографические алгоритмы представлены комбинацией этих двух типов. В работе [3] приводятся некоторые одноалфавитные и многоалфавитные (исторические) шифры замены и их криптоанализ. Представлены шифры, не распространяющие искажений типа замены знаков; шифры, не распространяющие искажений типа пропуска знаков; шифры, не распространяющие искажений типа вставки знаков. Приводятся необходимые и достаточные условия данных шифров [4].

В последнее время широкое распространение получили технологии криптовалют, в основе которых также лежат криптографические несимметричные алгоритмы, а соответственно, используемые в них математические методы и алгоритмы.

Прежде всего, термин «криптовалюта» (англ. «*cryptocurrency*») переводится в буквальном смысле как виртуальная валюта, защищенная криптографией. В широком научном плане криптовалюта — это цифровые счетные единицы, учет которых децентрализован. Принцип децентрализации напрямую связан с технологией блокчейна. Помимо этого, в криптовалютах используются публичные и приватные ключи для перевода валюты от одного (физического или юридического) лица другому, и для перевода криптовалюты каждый раз требуется криптографическая подпись.

Синтез этих технологий позволяет определить понятие «криптовалюта», как децентрализованная виртуальная валюта, основанная на математических принципах пиринговыми виртуальными валютами с открытым исходным кодом, у которых нет центрального администратора и отсутствуют централизованный контроль или надзор [5].

Отсутствие контроля и надзора делает привлекательным данную сферу экономики для киберпреступности и криминального использования виртуальной валюты.

Вопросы, связанные с особенностями и алгоритмами формирования и применения криптовалют, результаты проведенного анализа возникающих при этом проблем, авторский опыт практического применения биткоинов, как универсального платежного средства, представлен в работе [6].

С учетом актуальности данного направления, представляет интерес рассмотрение алгоритмов применения математического инструментария в ассиметричных криптографических системах, формирующих основу технологии криптовалют, с точки зрения обеспечения ими высокого уровня криптографической стойкости.

Криптовалюта (биткоин) использует в своей системе защиты популярные и надёжные криптографические решения, а именно, криптографию на эллиптических кривых (*Elliptic curve cryptography*, ECC). В основе ее находится математическая функция — эллиптическая кривая [7].

Данная функция применяется сегодня во многих криптосистемах, на которых базируются современные информационные и веб технологии (PGP, SSH, TLS), в том числе биткойны и другие криптовалюты.

Ранее, почти все алгоритмы с публичным ключом основывались на RSA, DSA и DH, альтернативных криптосистемах на основе модулярной арифметики. Логика применяемых алгоритмов, в этом случае, объяснима и понятна многим, а грубые реализации пишутся довольно просто. В то время, как основы ECC всё ещё являются для большинства людей загадкой.

По этой причине в данной статье рассмотрим основы мира криптографии на эллиптических кривых и попытаемся объяснить почему ECC считают безопасной и обладающей высокой криптографической стойкостью.

В частности, рассмотрим эллиптические кривые над вещественными числами и над конечными полями.

Опишем математически эллиптическую кривую, как множество точек, связанных уравнением (1):

$$y^2 = x^3 + ax + b \qquad (1)$$

где для исключения особых кривых необходимо выполнить условие: $4a^3 + 27b^2 \neq 0$.

Приведённое выше уравнение называется обычной формулировкой Вейерштрасса для эллиптических кривых [8].

В зависимости от значений a и b эллиптические кривые могут принимать на плоскости разные формы, что представлено на рис. 1. Как можно легко увидеть и проверить, эллиптические кривые симметричны относительно оси X.

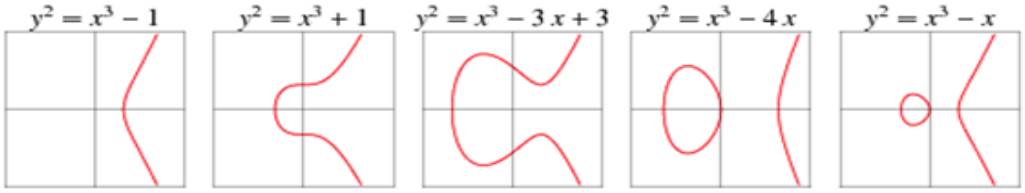


Рис. 1. Эллиптические кривые в зависимости от значений параметров *a* и *b*

Рассмотрим две точки $P, Q \in \alpha$. Их суммой называется точка $R \in \alpha$, которая в простейшем случае определяется следующим образом: проведем прямую через *P* и *Q* — она пересечет кривую α в единственной точке, которую назовем *R*. Поменяв координату точки –*R* на противоположную по знаку, мы получим точку *R*, которую и будем называть суммой *P* и *Q*, то есть $P + Q = R$. Геометрическая схема нахождения точки *R*, как суммы двух точек на эллиптической кривой представлена на рис. 2.

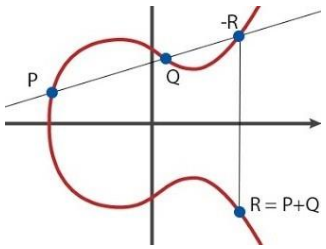


Рис. 2. Геометрические построения для получения суммы двух точек на эллиптических кривых

Примеры и особенности сложения точек на эллиптических кривых представлены в работе [9].

Необходимо отметить, что это операция именно вводится нами, т.к. если по законам алгебры будем складывать соответствующие координаты точек, то получим совершенно другую точку с координатами $D(x_1 + x_2, y_1 + y_2)$, которая, не совпадает ни с R, ни с –R и даже не лежит на кривой α.

Если рассмотреть случай, когда две точки имеют координаты P(a, b) и Q(a, -b), то проходящая через них прямая будет параллельна оси ординат, что представлено на рис. 3 (третий график). Третье пересечение с кривой α в данном случае отсутствует (выше обозначалось, как — R).

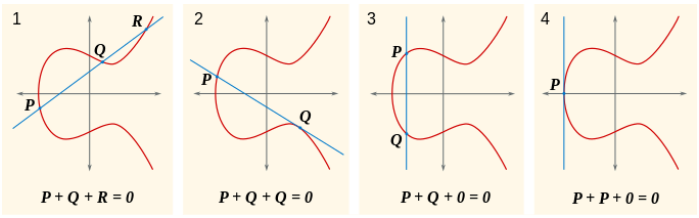


Рис. 3. Результаты сложения точек на эллиптических кривых

Для исключения этой ситуации, искусственно вводится «точка в бесконечности» (*point of infinity*), обозначаемую как 0 (см. Рис. 3), т.е. когда отсутствует пересечение с кривой α, то: $P + Q = 0$.

Интересно проанализировать случай, когда точка складывается сама с собой (точка Q на втором графике рис. 3). В данной ситуации проводится «касательная к функции в точке» Q и отмечается точка пересечения относительно оси Y.

Введем операцию умножения точки на некоторое натуральное число. В результате получается новая точка $K = Gk$, т.е. $K = G + G + \cdots + G$ (G складываем k раз). Графическое представление операции на рис. 4.

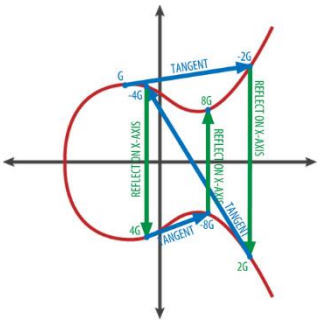


Рис. 4. Геометрические построения для получения результата операции умножения точки на натуральное число на эллиптических кривых

Рассмотрим эллиптические кривые над конечными полями. В этом случае используется точно такая же кривая, только рассматриваемая над некоторым конечным полем (2):

$$F_p = Z/Z_p = \{0, 1, \dots, p-1\}, \quad (2)$$

где p — простое число. То есть математическое описание эллиптической кривой над конечными полями представлено уравнением (3):

$$y^2 mod\ p = x^3 + ax + b(mod\ p). \quad (3)$$

Все ранее рассмотренные свойства характерные для этой функции, а именно: сложение, умножение, «точка в бесконечности» остаются в силе. Если начертить данную функцию, то напоминать привычную эллиптическую кривую она будет лишь отдаленно, да и понятие «касательной к функции в точке» в этом случае теряет всякий смысл. Как пример, на рис. 5 представлена функция $y^2 = x^3 + 7$ для p = 17.

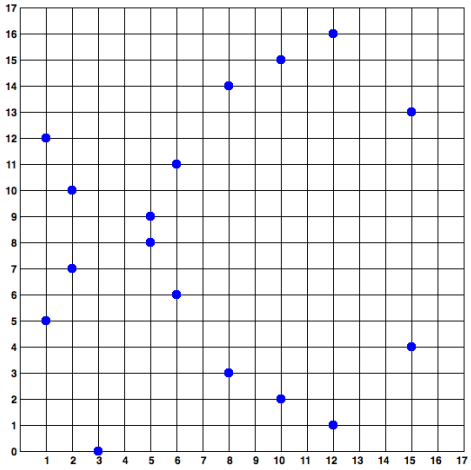


Рис. 5. Геометрическое представление функции $y^2 = x^3 + 7$ для p = 17

Для p = 59 функция $y^2 = x^3 + 7$ представлена на рис. 6 [10].

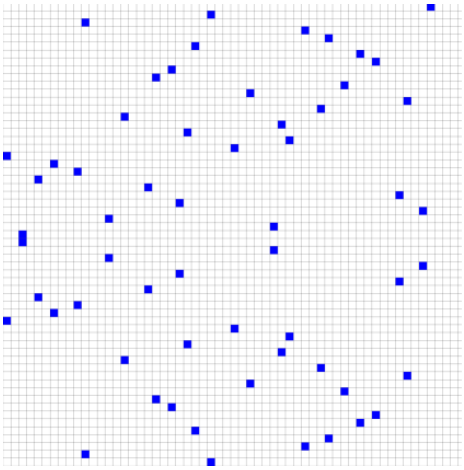


Рис. 6. Геометрическое представление функции $y^2 = x^3 + 7$ для p = 59

Если говорить конкретнее о Bitcoin, в нем используется алгоритм цифровой подписи с использованием эллиптической кривой SECP256k1 [11]. Она имеет вид $y^2 = x^3 + 7$ и рассматривается над полем F_p, где p — очень большое простое число, а именно (4):

$$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1 \quad (4)$$

Так же для SECP256k1 определена так называемая *base point*, она же *generator point* — это просто точка, как правило, обозначаемая как *G*, лежащая на данной кривой. Она необходима для создания публичного ключа.

В ассиметричной криптографии, как известно, помимо публичного (открытого) ключа применяется «приватный» (секретный) ключ. Термин этот довольно общий и в различных алгоритмах электронной подписи могут использоваться различные типы приватных ключей.

В технологии Bitcoin приватный ключ — это некоторое натуральное 256 битное число, т.е. самое обычное целое число от 1 до 2^{256}. Технически, даже число 123456 будет являться корректным приватным ключом. Но злоумышленник может легко подобрать (методом перебора) подобный приватный ключ.

Если задать *k* –приватный ключ, *G* — *base point*, тогда публичный ключ $K = Gk$. То есть, фактически, публичный ключ — это некоторая точка, лежащая на кривой SECP256k1.

Два важных обстоятельства. Прежде всего, операция получения публичного ключа определена однозначно, а именно, конкретному приватному ключу всегда соответствует один единственный публичный ключ. Второй нюанс, обратная операция является вычислительно трудной и, в общем случае, получить приватный ключ из публичного можно только полным перебором первого.

Заключение. Применение математической функции — эллиптической кривой в асимметричной криптография, которая является основой таких цифровых технологий, как электронная подпись и криптовалюта, позволяет экономить биты и гарантированно определяет основные необходимые характеристики приватных и

публичных ключей: криптостойкость и обеспечение целостности передаваемой информации, укрепляет доверие участников системы в подлинности осуществляемых операций.

СПИСОК ЛИТЕРАТУРЫ

1. Васильева И. Н., Локнов А. И., Примакин А. И. Криптографическая защита информации : учеб. пособие. СПб. : СПбУ МВД России, 2023. 120 с.
2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. М. : Гелиос АРВ, 2005. 480 с.
3. Рацеев С. М. Математические методы защиты информации : электронное учеб. пособие. Ульяновск: УлГУ, 2018. [Электронный ресурс]. URL: https://www.labirint.ru/books/848777/ (дата обращения: 20.07.2023).
4. Бабаш А. В., Глухов М. М., Шанкин Г. П. О преобразованиях множества слов в конечном алфавите, не размножающих искажений. // Дискретная математика. 1997. Т. 9. № 3. С. 3-19.
5. Васильева И. Н., Локнов А. И., Примакин А. И., Родин В. Н. Технологии криптовалют : [монография]. СПб. : СПбУ МВД России, 2023. 158 с.
6. Локнов А. И., Примакин А. И., Хлебников А. М. Особенности и алгоритмы формирования и применения криптовалют // Региональная информатика и информационная безопасность : сб. трудов. Вып. 8. СПб. : СПОИСУ, 2020. С. 151-154.
7. Математика биткойна простым языком [Электронный ресурс]. URL: https://mou43-samara.ru/education/kakie-matematicheskie-zadachi-reshaet-majning (дата обращения: 20.07.2023).
8. Болотов А. А., Гашков С. Б., Фролов А. Б. Элементарное введение в эллиптическую криптографию. Книга 2. Протоколы криптографии на эллиптических кривых. Ленанд. 2020. 376 с.
9. Примеры сложения точек на эллиптических кривых. [Электронный ресурс]. URL: https://studopedia.ru/3_100400_algoritm-vichisleniya-tochek-ellipticheskoy-krivoy.html (дата обращения: 20.07.2023).
10. Mistry N. An Introduction to Bitcoin, Elliptic Curves and the Mathematics of ECDSA [Электронный ресурс]. URL: https://raw.githubusercontent.com/bellaj/Bitcoin_Ethereum_docs/6bffb47afae6a2a70903a26d215484cf8ff03859/ecdsa_bitcoin.pdf (дата обращения: 20.07.2023).
11. Савчук С. Б., Шильцова Т. А., Хинько В. А. Принцип создания криптовалюты на базе эллиптических кривых и аспекты продвижения биткоина // Научный вестник Южного института менеджмента. 2018. № 3. С. 83-87.

УДК 000.00

БЕЗОПАСНОСТЬ ЖИЗНЕННЫХ ИНТЕРЕСОВ ЛИЧНОСТИ, ОБЩЕТСВА, ГОСУДАРСТВА В АСПЕКТЕ СОХРАНЕНИЯ БАЛАНСА НАЦИОНАЛЬНЫХ ИНТЕРЕСОВ И ИНТЕРЕСОВ ЛИЧНОЧТИ

Громова Ольга Владимировна
Фонд поддержки героико-патриотического воспитания молодежи
Черкасова ул., 4, Санкт-Петербург, 198052, Россия
e-mail: fund_shpey@mail.ru

Аннотация. В последние несколько десятилетий не прекращается дискуссия о том, чьи интересы первостепенны: интересы личности или государственные интересы. Общественный дискурс возник не на пустом месте, а в результате смены идеологии с коллективной на индивидуалистическую. К сегодняшнему дню, нарратив о преобладании интересов личности над всеми остальными, многократно дискредитирован и давно себя изжил. Однако российское общество получило важный для себя опыт, необходимый для поиска баланса между интересами государства и личности каждого в государстве. Общественный консенсус — это и есть справедливые приоритеты: в какие-то периоды своего развития и жизни, обществу требуется поставить «во главу угла» укрепление государственности, предпочитая их перед развитием культурных и гуманистических ценностей. В иные времена, общество признает более значимыми интересы личности, отводя на второй план не только безопасность, но и государственное развитие, включая науку, промышленность и технологии. Рассматривая вопросы первостепенности ценностей в тот или иной период развития общественных отношений, в том числе правовых отношений, остановимся неутихающей дискуссии о балансе жизненно важных интересов личности, общества и государства в свете закона «О безопасности».

Ключевые слова: баланс интересов; национальные интересы; национальная безопасность.

THE SECURITY OF THE VITAL INTERESTS OF THE INDIVIDUAL, THE COMMUNITY, THE STATE IN THE ASPECT OF MAINTAINING THE BALANCE OF NATIONAL INTERESTS AND PERSONAL INTERESTS

Gromova Olga
Foundation for the Support of Heroic and Patriotic Education of Youth
Cherkasova str. 4, St. Petersburg, 198052, Russia
e-mail: fund_shpey@mail.ru

Absrtact. In the last few decades, there has been a constant discussion about whose interests are paramount: the interests of the individual or the interests of the state. Public discourse did not arise from scratch, but as a result of the change of ideology from collective to individualistic. To date, the narrative about the predominance of the interests of the individual over all others has been discredited many times and has long outlived itself. However, Russian society has gained important experience for itself, which is necessary to find a balance between the interests of the state and the personality of

everyone in the state. Public consensus is just priorities: at some periods of its development and life, society needs to put the strengthening of statehood «at the forefront», preferring them over the development of cultural and humanistic values. At other times, society recognizes the interests of the individual as more important, taking into account not only security, but also state development, including science, industry and technology. Considering the issues of the primacy of values in one or another period of the development of public relations, including legal relations, we will focus on many years of relentless discussion about the balance of vital interests of the individual, society and the state in the light of the law «On Security».

Keywords: balance of interests; national interests; national security.

Введение. Система законодательства «О безопасности» раскрывается в Конституции РФ, Доктринах, Стратегиях, Законах федерального и регионального уровня.

Правовая основа о безопасности весьма разветвленная и охватывает различные сферы общественной жизни: информационную, демографическую, экономическую, культурную, национальную, нравственную и иные. В частности, Стратегия национальной безопасности, утвержденная Указом Президента РФ от 02.07.2021 № 400, статья 25, содержит обширный перечень стратегических национальных приоритетов, безопасность которых гарантирована государством. И на первом месте стоит:

«1) сбережение народа России, развитие человеческого потенциала, повышение качества жизни и благосостояния граждан;»

И только на втором:

«2) защита конституционного строя, суверенитета, независимости, государственной и территориальной целостности Российской Федерации, укрепление обороны страны;

3) поддержание гражданского мира и согласия в стране, укрепление законности, искоренение коррупции, защита граждан и всех форм собственности от противоправных посягательств, развитие механизмов взаимодействия государства и гражданского общества.

Стратегия, это в большой степени, декларативный документ, нежели обязывающий, однако дающий полное представление о ценности и первоочередности жизненных интересов народа и личности.

Такая первостепенность представляется важной именно в тот момент жизни человека или общества, когда государственные органы и организации, пользуясь своими властно-распорядительными полномочиями, позволяют себе злоупотреблять делегированной им властью и ущемлять права человека, вторгаясь и ограничивая его жизненные интересы.

Законом № 309-ФЗ от 28.12.2010 г. «О безопасности» не раскрывается правовой статус личности в отношениях, регулируемых законом, она находится в составе охраняемых прав и даже не первым пунктом.

Таким образом, актуальной является проблема поиска баланса между интересами национальной безопасности и жизненно важными интересами личности.

Сочетание и взаимодействие жизненно важных интересов субъектов права, является движущей силой развития страны, как в социально-экономическом плане, духовно-культурном и политическом планах, так и в плане суверенности и безопасности. Понятие национальные интересы имеют свою структуру и определяются правовой наукой следующим образом:

– интересы личности состоят в обеспечении конституционных прав и свобод, физической безопасности, повышения качества и уровня жизни, физического, духовного и интеллектуального развития, реализации творческих сил, духовных запросов и материальных потребностей. А именно, решение демографических проблем, снижение бедности, улучшение жилищных условий, повышение уровня образования и медобслуживания и многое другое с чем каждый человек сталкивается ежедневно в процессе жизни.

– интересы общества включают в себя упорядочение демократии и гражданского общества, достижение и поддержание общественного согласия, повышение созидательной активности населения и духовное развитие всех социальных и этнических групп, сохранение и развитие народных традиций, культурно-духовных ценностей.

– интересы государства состоят в защите конституционного строя, суверенитета и территориальной целостности, в установлении политической, экономической и социальной стабильности, в безусловном исполнении законов и поддержании правопорядка, в развитии международного сотрудничества на основе партнерства.

Эволюция доктрины безопасности.

История изменения отношения законодателя к вопросам безопасности, раскрывается при сравнении системы действующих правовых актов «О безопасности» с их предшественниками, уже утратившими силу.

Доктрина о безопасности в новой России появилась в 1992 года и с того времени претерпела существенные изменения. В целом, любая доктрина — это документ декларативный и получает свою конкретизацию в законах и подзаконных актах. поэтому может меняться в зависимости от ситуации в стране и в обществе, степени решенности поставленных ею целей и задач.

Начиная с 2009-2010 года начался процесс смещения правового акцента с «защиты интересов личности» к «езащите национальных интересов» с преобладанием интересов государства и повышения роли государственной власти в использование мер обеспечения безопасности.

Так, принципами и объектами безопасности в законе № 2446-1 от 26.06.2008 года устанавливается:

«Безопасность — состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Жизненно важные интересы — совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

К основным объектам безопасности относятся: личность — ее права и свободы; общество — его материальные и духовные ценности; государство — его конституционный строй, суверенитет и территориальная целостность»

Как справедливо отмечают Феоктистов и Зернов [25], пришедший ему на смену Федеральный закон от 28.12. 2010 г. № 390-ФЗ «О безопасности» широко использует категорию «безопасность», но не содержит ее общего понятия, не знает легально оформленного, явного определения соответствующего феномена. Предметом регулирования настоящего федерального закона выступают основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством РФ, полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления в области безопасности, а также статус Совета Безопасности Российской Федерации — ст. 1 Федерального закона.

При этом в п. 41. Стратегии прямо указано, что гарантируемая безопасность личности находится в прямой зависимости от государства: «Обеспечению государственной и общественной безопасности способствует реализация мер, направленных на усиление роли государства как гаранта безопасности личности и прав собственности, повышение эффективности деятельности правоохранительных органов и специальных служб по защите основ конституционного строя Российской Федерации, прав и свобод человека и гражданина, совершенствование единой государственной системы профилактики преступности, обеспечение реализации принципа неотвратимости наказания за совершение преступления, а также на формирование в обществе атмосферы нетерпимости к противоправной деятельности».

В этой связи закономерно возникает вопрос о степени защищенности личности от злоупотреблений правом со стороны государственных органов.

Из современной «Стратегии национальной безопасности», равно как и Федерального закона «О безопасности» изъято прямое упоминание принципа «соблюдения баланса жизненно важных интересов личности, общества и государства».

В юридической литературе отмечается, что баланс интересов представляет собой особое правовое состояние, которое обеспечивает оптимальный режим жизнедеятельности государства, общества и личности. При этом должен выражаться учет и соотношение наиболее значимых интересов субъектов общества в целях создания надлежащих благоприятных условий их реализации и обеспечения гарантий.

Как верно отмечает Холодная Е.В. [21], одной из задач правового регулирования является создание благоприятных условий для обеспечения компромисса законных прав и интересов различных субъектов.

Существует три концепции поиска баланса интересов: в первой — приоритет всегда остается за личностью (приоритет естественных прав), второй — приоритет государственных интересов (главенство публичного права), третий — узаконенное справедливое соотношение конституционно-гарантированных прав и обязанностей сторон — собственной баланс интересов.

Баланс — не синоним равенства, это оптимальное соотношение интересов субъектов, где права обременены обязанностями, а возможности — ответственностью.

Важной задачей развития общества и сохранение его безопасности, является учет, согласование и сбалансированность многообразия государственных, социальных и личных интересов; выработки системы воздействия на интересы и обеспечения условий для их реализации. Государство выражает всеобщие интересы нации, общество в свою очередь является выразителем социальных и частных интересов. По утверждению Гегеля, государство оказывается благоустроенным и само в себе сильным, если частные интересы граждан соединяются с его общими интересами.

И это верно, так как любой дисбаланс, особенно закрепленный в праве, превращается в угрозу национальной безопасности.

Механизмы обеспечения баланса интересов и способы достижения.

Какими же способами может быть достигнут такой консенсус?

Главным средством, приводящим в действие механизм согласования интересов различных уровней, является политическая деятельность государства, а также институтов, входящих в политическую систему общества.

Помимо развитой судебной системы, повышение правосознания, расширение законодательной базы, расширение экономической автономии человека и иных инструментов, справедливость баланса гарантирует также развитость гражданского общества, которое расширяет представленность интересов личности перед государственной властью.

Одним из механизмов достижения правового консенсуса, являются общественные палаты, общественные наблюдательные комиссии, общественные советы. К методам установления юридического консенсуса относятся методы работы таких общественных институтов: общественный контроль, проведение общественной экспертизы, участие в работе государственных органов и т. д.

Согласно закону об общественной палате [19] «Общественная палата призвана обеспечить согласование общественно значимых интересов граждан РФ, общественных объединений, иных некоммерческих организаций, органов государственной власти и органов местного самоуправления для решения наиболее важных вопросов экономического и социального развития, обеспечения национальной безопасности, защиты прав и свобод граждан РФ, конституционного строя РФ и демократических принципов развития гражданского общества в РФ <…>«.

Основной целью Общественной палаты является осуществления общественного контроля за деятельностью Правительства РФ, федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ и органов местного самоуправления [19]. Общественная палата РФ располагает своей нормативно-правовой базой, своими полномочиями, специфичными функциями, сотрудничает с международным сообществом. Кроме того, имеется тенденция к образованию подобных структур во всех субъектах РФ.

К способам обеспечения баланса интересов личности и государства [26], как справедливо отмечает К. А. Бабаджанян, относятся:

1) ограничение и самоограничение, как со стороны власти, государства, так и со стороны личности, гражданина;
2) взаимная ответственность государства и личности;
3) правосудие как способ обеспечения баланса интересов государства и личности;
4) максимальный учет на законодательном и правотворческом уровне объективных потребностей, запросов, ожиданий общества;
5) легитимность и справедливость власти;
6) сочетание методов убеждения и принуждения в системе государственного управления;
7) развитие отношений социального партнерства и сотрудничества между государством и личностью на основе общих целей и задач;
8) преодоление государственного патернализма и расширение экономической и политической свободы личности;
9) сокращение чрезмерного социального расслоения общества на «очень богатых» и «очень бедных», поиск социального мира и согласия между указанными слоями населения;
10) борьба с коррупцией, бюрократией и чиновничьим произволом;
11) развитое правосознание, признание и понимание взаимного равенства и свободы, взаимной ответственности личности и государства.

Развитость системы правовых актов о безопасности

Как отмечает Шахов В.В. [27], возможность ведения успешной политики в условиях многообразия интересов предполагает высокоразвитую способность кооперации усилий, взаимодействие между носителями разных интересов и политических ориентации, восприятие многообразия как данности, а не как препятствия. Это качество политической культуры вырастает из взаимной информированности людей.

В принципе, малейшие нюансы в механизме регулирования общественных отношений, должны находить отражение в соответствующей правовой терминологии, получать юридическое толкование.

Проявление правовой культуры отражен в уровне законотворчества и разветвленности законодательства, отражает реальную способность правовой системы влиять на общественные отношения и человеческое поведение, четко фиксировать назревшие социальные потребности и проблемы и предлагать новые правовые средства их разрешения. При этом весьма важным оказывается способность действующей правовой системы учитывать и согласовывать интересы разных социальных групп, ведь если правовой механизм нарушает интересы части населения страны, он перестает рассматриваться в качестве приемлемого для всех членов общества средства регуляции общественных отношений, реализация его норм неизбежно вызывает сопротивление других социальных групп, порядок все больше поддерживается мерами насилия, что не уменьшает, а лишь увеличивает количество и сложность социальных проблем.

Этот общеправовой тезис возвращает нас к нашей теме и значимости консенсуса, как одного из аспектов безопасности.

Заключение. Необходимость повышения правовой культуры человека, как гражданина, как члена общества, как индивида, преследует основную цель — понимание и полное осознание того объема прав и свобод, которое не только декларировано в Основным законе Российской Федерации, но и гарантировано разветвленной системой законов, а также прямо поддерживается государственной политикой по формированию гражданского общества, в частности Общественной палаты РФ.

Мы рассмотрели всю иерархию понятия интересов, раскрыли также понятие баланса интересов и необходимости поиска консенсуса между национальными интересами и интересами личности, определили

механизмы его достижения, сделали вывод о том, что национальная безопасность только крепнет, когда найден баланс и ни одна из сторон не ощущает ущемление своих интересов, то есть внутриструктурных угроз.

СПИСОК ЛИТЕРАТУРЫ

1. Конституция Российской Федерации.
2. «Об утверждении Концепции национальной безопасности Российской Федерации» : Указ Президента РФ от 17.12.1997 г. № 1300 (ред. От 10.01.2000).
3. «О Концепции национальной безопасности Российской Федерации» : Указ Президента РФ от 10.01.2000 г. № 24.
4. «О Стратегии национальной безопасности Российской Федерации до 2020 года» : Указ Президента РФ от 12.05.2009 г. № 537 (ред. от 01.07.2014).
5. «О Стратегии национальной безопасности Российской Федерации» : Указ Президента РФ от 31.12.2015 г. № 683.
6. «Об утверждении Доктрины информационной безопасности Российской Федерации» : Указ Президента РФ от 05.12.2016 г. № 646.
7. «О Стратегии развития информационного общества в Российской Федерации на 2017–2030» : Указ Президента РФ от 09.05.2017 г. № 203.
8. «О Стратегии национальной безопасности Российской Федерации» : Указ Президента РФ от 02.07.2021 г. № 400.
9. «О безопасности» : Закон РФ от 05.03.1992 г № 2446-1 (ред. от 26.06.2008).
10. «О безопасности» : Федеральный закон № 390-ФЗ от 28.12.2010 г.
11. «О противодействии терроризму» : Федеральный закон от 06.03.2006 г. № 35-ФЗ (ред. от 10.07.2023).
12. «О противодействии экстремистской деятельности» : Федеральный закон от 25.07.2002 г. № 114-ФЗ (ред. от 28.12.2022).
13. «О противодействии коррупции» : Федеральный закон от 25.12.2008 г. № 273-ФЗ (ред. от 10.07.2023).
14. «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» : Указ Президента РФ от 09.11.2022 г. № 809.
15. «Об утверждении Основ государственной культурной политики» : Указ Президента РФ от 24.12.2014 г. № 808 (ред. от 25.01.2023).
16. «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» : Указ Президента Российской Федерации от 7 мая 2018 г. № 204.
17. «О национальных целях развития Российской Федерации на период до 2030 года» : Указ Президента РФ от 21 июля 2020 г. № 474.
18. «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» : Указ Президента РФ от 13.05.2017 г. № 208
19. «Об Общественной палате Российской Федерации» : Федеральный закон от 04.04.2005 г. № 32-ФЗ (ред. от 13.06.2023).
20. Туранин В. Ю. Национальные интересы: подходы к определению понятия; «Российская юстиция // СПС «Консультант Плюс». 2021, № 1.
21. Холодная Е. В. О правовом принципе баланса интересов личности, общества и государства // Вестник Саратовской государственной юридической академии 2018. № 3 (122). С. 116-121.
22. Адзиев Х. Г., Гасанов Н. Н. Что такое «национальное согласие», или об опасности омонимии в политологии. Дагестанский государственный педагогический университет (Работа выполнена в рамках гранта Российского гуманитарного научного фонда 09-03-00816а/Р. Статья поступила в редакцию 19.07.2009 г), 2009.
23. Куричев А. А. Основные проблемы ограничения прав человека в современном государстве в целях противодействия экстремизму и терроризму. С. 17-22. URL: https://elar.urfu.ru/bitstream/10995/60551/1/978-5-7996-2407-1_02_04.pdf (дата обращения: 30.06.2023).
24. Маникин Д. Н. Защита прав личности — приоритетная тактическая цель уголовного процесса Российской Федерации / Пермский филиал Санкт-Петербургского ИВЭСЭП, г. Пермь // Историческая и социально-образовательная мысль. 2016. Т. 8 № 5/1, С. 109-116.
25. Феоктистов А. В., Зернов И. В. Эволюция развития законодательства о национальной безопасности в российской федерации // Электронный научный журнал «Наука. Общество. Государство». 2023. Т. 11, № 1. http://esj.pnzgu.ru
26. Бабаджанян К. А. Взаимная ответственность личности и государства как основа гармонизации взаимоотношений между ними (теоретико-правовой аспект) : диссертация к. ю. н.. Саратов : Саратовская государственная юридическая академия, 2013.
27. Политология : курс лекций / Шахов В. В. [и др.]. Московский Университет МВД РФ им. В. Я. Кикотя. URL: https://studfile.net/preview/16409179/page:15/ (дата обращения: 30.06.2023).
28. Командирова Т. Г. Правовые гарантии безопасности личности в России // Вестник Саратовской государственной юридической академии, 2013. № 3 (92). С. 51-54.
29. Грецова Е. Е. Ограничения прав и свобод человека в интересах обеспечения общественной безопасности и противодействия терроризму. URL: https://www.sovremennoepravo.ru/ (дата обращения: 30.06.2023).

УДК 004.056.53

ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ КОГНИТИВНЫХ ВОЙН

Губин Александр Николаевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, Санкт-Петербург, 193232, Россия
e-mail: gan50_60@mail.ru

Аннотация. В статье рассматриваются вопросы определения значений оценки коэффициента информационной безопасности для различных групп населения в условиях когнитивной агрессии. Для расчета коэффициента информационной безопасности с учетом степени лояльности населения используется модель Бирнбаума. Приведен пример расчета значений коэффициента информационной безопасности.

Ключевые слова: информационная безопасность; когнитивная агрессия; энтропийная сложность; модель Бирнбаума.

ASSESSMENT OF INFORMATION SECURITY IN CONDITIONS OF COGNITIVE WARS

Gubin Alexander
St. Petersburg State University of Telecommunications. prof. M. A. Bonch-Bruevich
22 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mail: gan50_60@mail.ru

Abstract. The article deals with the issues of determining the values of the assessment of the information security coefficient for various groups of the population in terms of cognitive aggression. To calculate the information security coefficient, taking into account the degree of population loyalty, the Birnbaum model is used. An example of calculating the values of the information security coefficient is given.

Keywords: information security; cognitive aggression; entropy complexity; Binbaum model.

Введение. Под когнитивной войной понимают нетрадиционную форму ведения войны, которая использует кибернетические инструменты для изменения познавательных процессов противника, эксплуатирует предубеждения, рефлексивные суждения, а также провоцирует искажения мышления [1].

Целью когнитивной войны является переформатирование сознания противника в свою пользу всеми доступными, в том числе невоенными способами, что, как правило, провоцируете негативные последствия этих действий, как на индивидуальном, так и на коллективном уровнях.

Согласно аналитикам НАТО, когнитивная война имеет универсальный охват, начиная с отдельных лиц и заканчивая государственными и интернациональными организациями. Ее поле деятельности глобально и обеспечивает захват контроля над людьми, как гражданскими, так и военными.

Достижения целей когнитивной войны обеспечивается информационным воздействием на противника, причем способы информационного воздействия могут быть достаточно разнообразными от формирования ложных сведений до организации анонимных утечек компрометирующих данных оппозиционным группам населения.

Положения «Концепции информационной безопасности Российской Федерации» [2] определяют следующие способы воздействия угроз на объекты информационной безопасности Российской Федерации:

– манипулирование информацией (дезинформация, сокрытие или искажение информации);

– использование средств массовой информации с позиций, противоречащих интересам граждан, организаций и государства.

Для обеспечения надлежащей информационной защиты населения от когнитивной агрессии необходима организация мониторинга информационных потоков с целью принятия решения об активизации механизмов противодействия элементам когнитивной агрессии.

В основном к таким механизмам относятся:

1. Полная изоляция объектов воздействия (населения) от информационных воздействий.
2. Замена потоков вредоносной составляющей информационных потоков на информацию, способствующую стабилизации общества.
3. Частичное изменение содержания информационных потоков когнитивной агрессии с целью противодействия форматированию сознания масс и стабилизации общества.

Выбор механизма защиты населения от когнитивной агрессии можно поставить в зависимость от значения вычисляемого ниже коэффициента информационной безопасности.

Постановка задачи. Объектами воздействия когнитивной агрессии являются все слои общества государства противника. Любое общество подвержено явлению стратификации. Под стратификацией обычно понимают некую систему, присущую любому обществу и определяющую дифференциацию всех членов общества.

С точки зрения информационной безопасности в любом обществе можно выделить наличие следующих групп.

1. Часть населения, активно поддерживающая воздействия поражающих факторов когнитивной агрессии и противостоящая политике государства.
2. Часть населения, критически оценивающая факторы воздействия, как когнитивной агрессии, так и системы, обеспечивающей информационную безопасность.
3. Часть населения, практически неподверженная действию поражающих факторов когнитивной агрессии и поддерживающая политику государства.

Соответствующие значения оценки состава данных групп населения можно определить как (1):

$$p_1 = \frac{n_1}{n_0},\ p_1 = \frac{n_2}{n_0},\ p_1 = \frac{n_3}{n_0}, \quad (1)$$

где n_1, n_2, n_3 — количество населения в каждой из групп, а $n_0=n_1+n_2+n_3$ — общее количество населения в зоне когнитивной агрессии.

На население воздействует информационный поток, общую структуру которого можно представить в виде совокупности информации, непосредственно блокирующей враждебные данные, обозначим вероятностную оценку доли этой части потока как $p_{и1}$, и информации решающей задачи общего информирования населения, эту часть информации обозначим как $p_{и2}$. Очевидно, что $p_{и1}+p_{и2}=1$.

Анализ вероятности приема информации противодействующей когнитивной агрессии в различных слоях общества показывает, что та часть населения, которая активно поддерживает воздействия поражающих факторов

когнитивной агрессии, обычно характеризуется низким значением вероятности приема полезной информации, обозначим это значение как $p_{п1}$.

Во второй части населения, критически оценивающей факторы воздействия, как когнитивной агрессии, так и системы обеспечивающей информационную безопасность, вероятность приема полезной информации принимает обычно средние значения — $p_{п2}$.

В третьей части населения, практически неподверженной действию поражающих факторов когнитивной агрессии и поддерживающей политику государства, вероятность приема полезной информации принимает обычно наиболее высокие значения — $p_{п3}$.

Определение значений количественных характеристик в рассматриваемых группах населения требует дополнительных социальных исследований в регионах, подвергающихся воздействиям когнитивной агрессии.

Для указанных исходных данных необходимо определить значения коэффициента информационной безопасности для каждой группы населения.

Оценка значений коэффициента информационной безопасности для различных групп населения.

Под значением коэффициента информационной безопасности, в данном случае, будем понимать вероятностную оценку события, определяющего факт усвоения полезной информации, в каждой из групп населения.

Рассматривая возможные варианты поведения представителей различных групп населения под воздействием информационного потока, можно отметить аналогию между представителями групп населения и обучающимися, для которых проводится проверка знаний тестированием. В обоих случаях с некоторой вероятностью осуществляется выбор. В случае обучения выбирается вариант ответа, в случае когнитивной агрессии выбирается (формируется) стереотип поведения, соответствующий принятой и усвоенной части информационного потока, действие которого противостоит когнитивной агрессии.

Вероятность успешной сдачи всего теста (значение функции успеха) обычно моделируется логистической функцией от разницы значений параметров уровня подготовки тестируемого и сложностью тестовой единицы. Математическая форма модели в данном случае получила наименование модели Раша [3] и имеет следующий вид (2):

$$P\{x_j = 1\} = \frac{e^{\theta_j - \delta_i}}{1 + e^{\theta_j - \delta_i}}, \quad (2)$$

где $P\{x_i = 1\}$ - вероятность успешной сдачи теста (функция успеха), θ_j–уровень подготовки j-го обучаемого, δ_i – сложность i-ой тестовой единицы.

Для рассматриваемого случая, сложность задания δ следует рассматривать как энтропийную оценку сложности потока информации, воздействующего на все группы населения (одно задание для всех групп населения) (3):

$$\delta = p_{и1} \cdot log \frac{1}{p_{и1}} + p_{и2} \cdot log \frac{1}{p_{и2}}. \quad (3)$$

В качестве уровня подготовки θ_j используем этропийную оценку способности населения к приему информационного потока. Тогда для каждой группы населения можно определить (4):

$$\theta_1 = p_{п1} \cdot log \frac{1}{p_{п1}} + (1 - p_{п1)} \cdot \log(\frac{1}{(1 - p_{п1})},$$

$$\theta_2 = p_{п2} \cdot log \frac{1}{p_{п2}} + (1 - p_{п2)} \cdot \log(\frac{1}{(1 - p_{п2})}, \quad (4)$$

$$\theta_3 = p_{п3} \cdot log \frac{1}{p_{п3}} + (1 - p_{п3)} \cdot log(\frac{1}{(1 - p_{п3})}.$$

Для учета уровня лояльности групп населения, мотивированных к действиям в поддержку государственной политики используем трехпараметрическую модель А. Бирнбаума [4] (5):

$$P\{x_j = 1\} = c_i + (1 - c_i)\frac{e^{\alpha_i(\theta_j - \delta_i)}}{1 + e^{\alpha_i(\theta_j - \delta_i)}}, \quad (5)$$

где c_i – коэффициент, учитывающий возможность угадывания правильного ответа; α_i - коэффициент, определяющий дифференцирующее свойство модели.

В нашем случае, в качестве c_i будем использовать коэффициент лояльности для каждой группы населения.

Коэффициент лояльности представляет собой оценку способности населения к восприятию положительной информации и активным действиям, которые предписываются государственной властью. Значение коэффициента для каждой группы населения определим как (6):

$$c_i = \frac{p_{пi}}{1+p_{пi}}, \text{ i=1, 2, 3.} \quad (6)$$

Значение коэффициента α выберем равным единице.

Таким образом, значение коэффициента информационной безопасности для каждой из групп населения с учетом ранее изложенного, можно определить согласно следующему выражению (7):

$$K_{ИБi} = c_i + (1 - c_i)\frac{e^{(\theta_i - \delta)}}{1+e^{(\theta_i - \delta)}}, i=1, 2, 3. \quad (7)$$

Пример. Рассмотрим пример формирования значений коэффициента информационной безопасности для следующих условий.

На население со структурой p_1=0,1, p_2=0,7, p_3=0,2 воздействует информационный поток, который характеризуется параметрами $p_{1и}$=0,6 и $p_{2и}$=0,4. Характеристики, отражающие возможности восприятия информации, позволяющей противостоять когнитивной агрессии, имеют следующий вид.

$$p_{п1}=0,1,\ p_{п2}=0,3,\ p_{п3}=0,6. \quad (8)$$

Значение коэффициента дифференциации α=1.

Необходимо определить значение коэффициента информационной безопасности для каждой группы населения.

Решение. Энтропийная оценка сложности потока информации составляет: δ=0,6·(-log 0,6) +0,4·(-log 0,4)=0,97095.

Энтропийная оценка уровня подготовки населения к восприятию информационного потока для каждой группы определяется как (9):

$$\theta_1 = 0,1 \cdot (-\log 0,1) + 0,9 \cdot (-\log 0,9) = 0,63117,$$
$$\theta_2 = 0,3 \cdot (-\log 0,3) + 0,7 \cdot (-\log 0,7) = 0,88585, \quad (9)$$
$$\theta_3 = 0,6 \cdot (-\log 0,6) + 0,4 \cdot (-\log 0,4) = 0,61905.$$

Значения коэффициентов лояльности для каждой группы населения вычисляются согласно следующим выражениям (10):

$$c_1 = \frac{p_{п1}}{1 + p_{п1}} = 0,0909,$$
$$c_2 = \frac{p_{п2}}{1+p_{п2}} = 0,23077, \quad (10)$$
$$c_3 = \frac{p_{п3}}{1 + p_{п3}} = 0,375.$$

Соответственно, значения коэффициента информационной безопасности для каждой группы общества определится следующим образом (11):

$$K_{ИБ1} = 0,0909 + (1 - 0,0909)\frac{e^{(0,63117-0,97095)}}{1 + e^{(0,63117-0,97095)}} = 0,46908,$$
$$K_{ИБ2} = 0,23077 + (1 - 0,23077)\frac{e^{(0,88585-0,97095)}}{1+e^{(0,88585-0,97095)}} = 0,59903, \quad (11)$$
$$K_{ИБ3} = 0,375 + (1 - 0,375)\frac{e^{(0,61905-0,97095)}}{1 + e^{(0,61905-0,97095)}} = 0,63308.$$

Заключение. Предложенная методика позволяет определить количественные оценки значений коэффициента информационной безопасности для различных групп населения. При вычислении коэффициента учитывается как структура общества, так и структура информационного потока, который должен противодействовать влиянию поражающих факторов когнитивной агрессии. Полученные значения коэффициента информационной безопасности могут быть использованы для анализа состояний различных групп общества с точки зрения информационной безопасности в условиях когнитивной войны.

СПИСОК ЛИТЕРАТУРЫ

1. Claverie B., Cluzel F. The Cognitive Warfare Concept [Электронный ресурс]. URL: https://www.innovationhub-act.org/sites/default/files/2022-02/CW%20article%20Claverie%20du%20Cluzel%20final_0.pdf (дата обращения: 28.08.2022).
2. Концепция информационной безопасности Российской Федерации : Проект. Совет безопасности Российской Федерации. Межведомственная комиссия по информационной безопасности [Электронный ресурс]. URL: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/4d900a096c2bf5b9c325763f0045a87f (Дата обращения: 10.04.2023).
3. Райт Б. Д. Решение задач измерения с помощью модели Раша // Журнал педагогических измерений. 1977. № 14 (2). С. 97-116.
4. Нейман Ю. М., Хлебников В. А. Введение в теорию моделирования и параметризации педагогических тестов. М. : Прометей, 2000, 169 с.

УДК 004.056.5

К ВОПРОСУ О ПРАКТИЧЕСКИХ РЕКОМЕНДАЦИЯХ ПО ИДЕНТИФИКАЦИИ ТЕЛЕФОННЫХ МОШЕННИЧЕСТВ

Локнов Алексей Игоревич, Бизин Роман Владимирович
Санкт-Петербургский университет МВД России
Лётчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
emails: info_for_aleksey@mail.ru, roma.bizin.01@mail.ru

Аннотация. Рассматривается явление телефонного мошенничества в эпоху цифровых технологий. Использование мошенниками звонков и мессенджеров для обмана и получения доступа к личным данным и деньгам. Рассмотрены предупреждающие знаки и способы борьбы с мошенниками.

Ключевые слова: информационная безопасность; телефонное мошенничество; цифровые технологии; звонки;мессенджеры;предупреждающие знаки;борьба с мошенниками.

TO THE QUESTION OF PRACTICAL RECOMMENDATIONS FOR THE IDENTIFICATION OF TELEPHONE FRAUDS

Loknov Alexey, Bizin Roman
Saint Petersburg University of the Ministry of internal Affairs of the Russian Federation
1, Pilyutov's pilot St., St. Petersburg, 198206, Russia
emails: info_for_aleksey@mail.ru, roma.bizin.01@mail.ru

Absrtact. The article deals with the phenomenon of telephone fraud in the digital age. Fraudsters use calls and instant messengers to deceive and gain access to personal data and money. Warning signs and ways to deal with scammers are considered.

Keywords: information security; telephone fraud; digital technologies; calls; instant messengers; warning signs; fight against fraudsters.

Введение. Наше общество вступило в эпоху цифровых технологий, но телефон остается ключевым оружием в арсенале мошенников. В 2022 году телефонное мошенничество заняло 90% среди основных схем кибермошенников, а россияне потеряли около 14,2 млрд рублей из-за них. Для обмана мошенники используют мессенджеры (40 %), звонки с помощью DEF-номеров (20 %) и подмену номера (20 %) [1].

После того, как вы ответите на звонок, телефонные мошенники используют ложные обещания, коммерческие предложения и ложные угрозы, чтобы узнать информацию, которую они могут использовать для кражи денег или личных данных (или того и другого).

Благодаря развитию технологий мошенникам всё проще заниматься незаконной деятельностью. С помощью автоматических дозвонов сомнительные операторы могут совершать миллионы звонков. Легкодоступные инструменты спуфинга могут заставить идентификатор вызывающего абонента отображать подлинный государственный номер или номер, который кажется местным, чтобы увеличить шансы на ответ [2].

Будь то живые или автоматизированные звонки, мошенники часто изображают из себя представителей государственных органов или знакомых технических, туристических, розничных или финансовых компаний, предположительно звонящих с ценной информацией. Это могут быть как «хорошие» новости (Вы имеете право на большой денежный приз), так и «плохие» (Вы должны заплатить налоги или проблема со счетом кредитной карты). При этом мошенники уверяют, что какой бы ни была проблема, ее можно решить, если, скажем, просто предоставить свои паспортные данные, данные банковской карты или сделать немедленный платеж.

Телефонные мошенники также могут выдавать себя за сборщиков благотворительных средств или даже за родственников, играя на щедрости, чтобы заставить перевести деньги.

Предупреждающие знаки:

1. Звонки от людей, утверждающих, что они работают в каком-либо государственном органе, коммунальном предприятии или крупной фирме. Эти организации будут редко звонить, если только они связались и другими способами или связались с ними вы.

2. Звонки от благотворительных организаций по сбору средств, особенно во время праздников и после стихийных бедствий.

3. Звонки, рекламирующие продукты или услуги с преимуществами, которые звучат слишком хорошо, чтобы быть правдой. Распространенные мошеннические предложения включают бесплатные пробные версии продуктов, денежные призы, дешевые туристические пакеты, медицинские услуги, предварительно одобренные кредиты, сокращение долга и инвестиции с низким уровнем риска и высокой доходностью.

4. Автоматический звонок по продажам от компании, с которой вы никак не связывались ранее. Этот автоматический звонок и почти всегда является мошенничеством.

Есть несколько причин, почему не стоит перезванивать на незнакомые номера. Например, самый безопасный сценарий — когда звонок совершается автоматически, чтобы проверить активность номера. В таком разговоре вы не получите никакой полезной информации, но мошенники будут знать, что этот номер действующий и готовы связываться с ним [3].

Часто при обратном звонке пользователи сталкиваются с приветливыми операторами колл-центров, которые задают множество вопросов и намеренно затягивают разговор. В таких случаях разговор происходит по платной телефонной линии, и могут списываться значительные суммы за время разговора.

Способы борьбы с мошенниками:

1. Блокировка мошенников:

Самый простой и очевидный способ. Он работает только в том случае, если есть номер мошенника.

– Откройте приложение «Телефон».
– Перейдите в раздел «Контакты».
– Выберите соответствующий номер и нажмите «Заблокировать абонента» (обычно эта функция находится внизу экрана или в меню).

2. Проверка номеров:

Контакты телефонных мошенников и спамеров обычно быстро распространяются в Интернете. Существуют специальные сервисы, которые собирают отзывы пользователей о конкретных номерах. Необходимо выбрать предпочитаемый веб-сайт, ввести интересующий номер и прочитать, что другие люди пишут о нем.

3. Загрузить приложение для борьбы со спамом и мошенниками

На сегодняшний день на рынке технологий существует множество программ, предназначенных для борьбы с назойливыми звонками от спамеров и мошенников. Однако необходимо осторожно подходить к выбору такого приложения, поскольку некоторые из них могут запрашивать доступ к номеру и телефонной книге, после чего контакты попадают в общую базу данных. Как эти данные будут использоваться, остается открытым вопросом.

Тем не менее, такие программы обладают обширными базами данных спам-номеров и могут автоматически определять информацию о звонящем во время входящего вызова.

4. Подключить справочник организаций

На смартфонах тысячи, а, может быть, даже миллионы пользователей устанавливают приложение «2ГИС» [4]. Однако, многие не знают о функции «Определитель номера».

Эту опцию можно включить в настройках телефона. В случае с iPhone необходимо следовать этим шагам:

1. Откройте «Настройки».
2. Выберите «Телефон».
3. Найдите «Блокировка и идентификация вызовов».
4. Включите опцию «2ГИС».

Теперь, когда вам поступит входящий вызов, вы будете видеть название организации, которая звонит. Можно быть уверенным в точности информации, поскольку у «2ГИС» огромные базы данных городских и мобильных номеров. Следует, однако, учесть, что программа определяет контакты лишь легальных и честных организаций, а не спамеров и мошенников. Все же, в борьбе все средства хороши.

5. Воспользоваться функциями операторов

Многие операторы предлагают своим абонентам возможности для блокировки спама. Чаще всего эти опции являются платными, но они довольно эффективны.

Заключение. Телефонное мошенничество остается серьезной проблемой в эпоху цифровых технологий. Мошенники используют различные методы, включая мессенджеры, подмену номеров и звонки с DEF-номеров, чтобы обмануть людей и получить доступ к их деньгам и личным данным. Для борьбы с мошенниками рекомендуется блокировать и проверять подозрительные номера, использовать специальные приложения для борьбы со спамом, а также воспользоваться функциями операторов. Важно быть бдительными, не отвечать на звонки с незнакомых номеров и не раскрывать личную информацию по телефону.

СПИСОК ЛИТЕРАТУРЫ

1. RSpectr : портал об информационных технологиях, связи и массовых коммуникациях. [Электронный ресурс] URL: https://clck.ru/34pYZA (дата обращения: 26.06.2023).
2. Научная электронная библиотека «КиберЛенинка». [Электронный ресурс] URL: https://cyberleninka.ru/article/n/mehanizm-hischeniy-denezhnyh-sredstv-sovershaemyh-s-ispolzovaniem-tehnologiy-ip-telefonii-i-programm-podmeny-nomerov (дата обращения: 26.06.2023).
3. Хабр : русскоязычный веб-сайт в формате системы тематических коллективных блогов (именуемых хабами) с элементами новостного сайта, созданный для публикации новостей, аналитических статей, мыслей, связанных с информационными технологиями, бизнесом и интернетом. [Электронный ресурс] URL: https://habr.com/ru/articles/657403/ (дата обращения: 26.06.2023).
4. «3ДНьюс» : независимое российское онлайн-издание, посвященное цифровым технологиям. [Электронный ресурс] URL: https://3dnews.ru/1039682/telefonniy-blokpost-obzor-prilogeniy-dlya-zashchiti-ot-moshennicheskih-i-spamzvonkov (дата обращения: 26.06.2023).

УДК 327.8

СТРАТЕГИЧЕСКИЕ ЦЕЛИ И СРЕДСТВА СОВРЕМЕННОЙ ИНФОРМАЦИОННОЙ ВОЙНЫ ЗАПАДА ПРОТИВ РОССИЦЙСКОЙ ФЕДЕРАЦИИ: ПОЛИТОЛОГИЧЕСКИЙ АНАЛИЗ

Шевцов Владимир Сергеевич
Российский Государственный гуманитарный университет,
Каширское шоссе, 4, корп. 2, Домодедово, 142000, Россия
e-mails: speziell@mail.ru

Аннотация. В публикации уточнено соотношение понятий «информационная война» и «информационное противоборство», обозначены стратегические цели, политические задачи, средства и направления современной информационной войны, осуществляемой США и их союзниками против Российской Федерации.

Ключевые слова: информационная война; информационное противоборство; стратегические цели и задачи; средства информационной войны; направления подрывных действий.

STRATEGIC GOALS AND MEANS OF THE MODERN INFORMATION WAR OF THE WEST AGAINST THE RUSSIAN FEDERATION: POLITICAL ANALYSIS

Shevtsov Vladimir
Russian State University for the Humanities,
4/2 Kashirskoe highway, St. Domodedovo, 142000, Russia
e-mails: speziell@mail.ru

Absrtact. The publication clarifies the relationship between the concepts of «information war» and «information warfare» and outlines the strategic goals, political objectives, means and directions of the modern information war carried out by the United States and its allies against the Russian Federation.

Key words: information warfare, information warfare, strategic goals and objectives, means of information warfare, areas of subversive actions.

Введение. В контексте политологического анализа стратегических целей и средств информационной войны, следует оговориться, что понятие «война» используется в переносном значении, поскольку в прямой постановке вопроса она предполагает вооруженное столкновение. В указанном значении под «войной» понимается крайняя, наиболее острая или масштабная форма противоборства, где предпринимаемые противником действия можно оценивать, как враждебные. Эти обстоятельства дают полагать, что в аспекте проводимого анализа информационная война рассматривается как наиболее опасная и масштабная конфликтная форма информационного противоборства.

В аспекте обостряющейся геополитической обстановки следует указать, что наиболее враждебные действия в информационной сфере против Российской Федерации исходят от США и их союзников, проводником деструктивной политики которых сегодня выступает преступный военно-политический режим Украины. Все это диктует необходимость более глубокого изучения внешнеполитических устремлений США, чтобы предметно разобраться в геополитических целях осуществляемой ими информационной войны.

Проанализировав все Стратегии Национальной Безопасности США XXI века (от: 12.2000 г.; 09.2002 г.; 03.2006 г.; 04.2010 г.; 02.2015 г., 12.2017., 01.2018., 01.2019 г.)., установлено общее концептуальное сходство документов, поскольку в различных вариациях фигурирует одни и те же геополитические цели — сохранение за собой статуса ключевого лидера (гегемона) и недопущение появления государств (коалиций стран и иных сил), способных составить им в этом реальную конкуренцию.

Вразрез их устремлениям идет политика России, которая достаточно активно реализует энергетические проекты и иные экономические проекты в странах, традиционно входящих в сферу влияния США. Указанные обстоятельства, в сочетании с достижениями нашего государства в области укрепления безопасности, создают условия, в которых лидерство официального Вашингтона выглядит уже не столь очевидным. Помимо этого, обозначенный Российской Федерацией и поддержанный многими другими государствами вектор на построение полицентричного мира, был расценен США как имперские амбиции, призванные пересмотреть сложившийся миропорядок при их главенствующей роли.

Во всеуслышание об экспансивных устремлениях американцев президентом России В.В. Путиным впервые открыто было сказано еще в 2007 г., в формате международного дискурса по вопросам политики и безопасности [1]. Однако ошибочно полагать, что ранее информационного противоборства между нашими государствами не было. Так, еще в 1998 г. корпорацией РЭНД, осуществляющей стратегические исследования по заказу правительства США, в отчете MR-964-OSD указано на важность экстраполяции информационного противоборства за пределы военного и государственных уровней [2]. В числе приоритетных указывалась необходимость активного воздействия на сферы жизнедеятельности общества потенциального противника, особенно экономическую. При этом подчеркивалось, что подобная политика может осуществляться не один год.

В ключе указанных событий, небезосновательно можно утверждать, что действия США в отношении Российской Федерации, являются развитием ключевых тезисов, представленных в этом Отчете.

В то же время, декларируемые Западом приоритеты демократии и мира, не позволяют осуществлять неприкрытые акты агрессии в отношении России. Именно поэтому важной политической целью современной информационной войны против неё является поиск (создание) условий для информационной инверсии собственных враждебных намерений в миротворческие, а наших защитных — в акты агрессии не просто против Украины, а против «всего цивилизованного мира», апологетом которого себя считают США. В совокупности, подобного рода информационная политика и давала им «мотивированные» основания для расширения военной инфраструктуры к границам Российской Федерации, закономерным итогом чего стала специальная военная операция, призванная превентивными мерами устранить актуализировавшиеся угрозы.

В аспекте реализуемой США и их союзниками информационной войны против Российской Федерации также преследуется определенные стратегические / геополитические цели. Как минимум — блокирование развития всех сфер жизнедеятельности нашего государства до тех пор, пока наши органы власти не откажутся от реализации самостоятельной внешней и внутренней политики. Как максимум — создание информационных условий для управляемого разрушения России, при котором будут нивелированы оборонительные функции государства.

Декомпозиция геополитических целей позволяет определить реализуемые США информационными средствами задачи, которые условно можно дифференцировать по следующим направлениям: политико-идеологические (ввиду отсутствия государственной идеологии его преимущественно рассматривают в аспекте духовно-культурной сферы, науки и образования); политико-экономические; политико-правовые; военно-политические и политико-кадровые.

Политико-идеологическое направление предполагает «западнизацию» сознания населения с перспективой внедрения либеральной модели (идеологии) управления российским обществом. Такой подход призван исключить перспективы появления государственной консолидирующей общество идеологии, а также утрате институтами власти многих регулирующих функций, которые перейдут под контроль западных структур. Тут важно понимать, что в нынешних условиях, даже при поддержке специальной военной операции значительным числом населения, происходит отток молодежи из страны, сознание которой излишне либерализовано. Сопутствующим этому является размывание (подмена) традиционных для России ценностей и национальной самоидентичности, фальсификация истории и блокирование потенциала развития. Подобные действия способны привести к разобщению общества, в том числе и путем внутреннего противопоставления, децентрализации власти с перспективой дальнейшего управляемого дробления российского государства и его ресурсной базы, что укладывается в характер геополитических устремлений США.

В контексте *политико-правового* направления решаются задачи ослабления суверенитета России через углубление приоритета международного права над национальным. В условиях, когда подконтрольные США и их союзникам инстанции принимают политически ангажированные решения, законность которых Российская Федерация может не признавать в соответствии с действующим законодательством, ей наносится имиджевый ущерб. Государства, входящие в пул Западных стран и «сочувствующих Украине» активно инвестируют в создание и расширение в России псевдодемократических структур, призванных осуществлять контроль не только деятельности государственных органов, но и силовых ведомств. Сегодня, в свете законодательных ограничений функционала многих из них, эта угроза может показаться не столь очевидной, но в 2024 г. предстоят выборы Президента Российской Федерации и акты политико-правого нигилизма могут повториться. Тем более этому способствует снижение реальных доходов населения, инфляция и удорожание импорта.

В области *политико-экономического* направления превалируют ограничительные (санкционные) меры, специфика воздействия которых сводится к планомерному давлению на Россию в экономической сфере и истощению возможностей её развития. Отметим, что на данный момент Евросоюз начал работу над двенадцатым пакетом санкций против России [3], что еще сильнее снижает инвестиционную привлекательность Российской Федерации и не способствует удержанию инвестиций в стране. В свою очередь, блокирование доступа к элементам мировой финансово-экономической информационной инфраструктуры осуществляется поэтапно, распределено и с сознательно нечетко формулируемыми целями воздействия, что стагнирует отечественный сегмент еще больше и делает неясными перспективы его развития. Вводимые Западом под патронажем США «полумеры» создают ситуацию, в которой России сложно однозначно прогнозировать дальнейший характер сотрудничества с ними, отчасти продолжая надеяться, что украинский кризис разрешится и взаимоотношения снова стабилизируются. Как следствие из этого, неясность целесообразия развития альтернативных конкурентных финансовых структур (например, должного развития за рубежом не получила платежная система «Мир», под сомнением анонсированное создание в 2025 г. платежной системы «BRICS Pay» и ряд других) [4]. По сути, поддерживаемая неопределенность выступает средством сдерживания нашего потенциала развития.

Известно, что война является продолжением политики. В свете сказанного значительное внимание отводится *военно-политическим* устремлениям США. Отметим, что именно в этой области наиболее ярко прослеживается специфика информационной войны, поскольку США решают свои геополитические задачи посредством манипулятивной подмены ролей ключевых политических акторов. В частности, собственные наступательные

агрессивные (враждебные) действия позиционируются как оборонительно-сдерживающие, а защитные меры России как ревизионистские и угрожающие демократическим режимам. В совокупности указанные обстоятельства позволяют мотивировать расширение инфраструктуры НАТО к границам Российской Федерации и инспирировать все новые конфликты. Так, в свете украинских событий поступает информация об обострении ситуации в Сирии и Приднестровье, горячим очагом стал Нагорных Карабах, а оппозиция в Грузии призывает к открытию второго фронта против России. Всё это делается исключительно для усиления давления на российские органы власти с целью вынудить их подчиниться экспансивным устремлениям США в ущерб национальным интересам и выстраиваемому внешнеполитическому курсу. Инспирируя конфликты, вина за которые возлагается на Российскую Федерацию, США находят адекватно воспринимаемые среди своих союзников основания для выхода из ограничивающих их договоров, фактически втягивая Россию в новую гонку вооружений и вынуждая увеличивать расходы на безопасность, тем самым замедляя темпы экономического развития.

Проводится информационно-подрывная работа в отношении наших союзников по Организации Договора о коллективной безопасности, Шанхайской организации сотрудничества, Содружеству Независимых государств и др., с целью устранения в них пророссийских вектора и последующего вовлечения государств в структуры НАТО. В подтверждении этого можно привести информацию разведывательно-аналитической компании «Stratfor», которая указала, что «Вашингтон будет предлагать экономические стимулы и гарантии безопасности странам, которые более прочно находятся на орбите Москвы, чтобы попытаться преодолеть их зависимость от России», а также усилит военное присутствие в граничащих с Россией районах [5]. В контексте приграничных территорий следует сказать, что значительно расширяется военная и информационная инфраструктура НАТО. Так, например, Центр передового опыта в Латвии (NATO Strategic Communications Centre of Excellence) уже является двадцатым по счету. Был создан Центр кибербезопасности НАТО в Эстонии, под протекторатом США действует Центр энергетической безопасности в Литве и др. [6], которые причастны к кибератакам на российскую информационную инфраструктуру.

Указанные обстоятельства вскрывают истинную цель США в рамках реализации военно-политических (специальных) задач — сформировать чувство страха перед искусственно созданной российской угрозой, которое обеспечит консолидацию Запада (так называемое трансатлантическое единство) и поспособствует дезинтеграции России в системе международных отношений, будет поддерживать уверенность европейских стран в правильности саморазрушительной политики поддержки Украины.

Относительно самостоятельным, но, в то же время одним из ключевых направлением действий, является политико-кадровое. В рамках его США реализуется активная политика, направленная на внедрение в управленческие структуры экономического, политического, военного и иных сегментов Российской Федерации лиц, идейно разделяющих политику Запада. Условно можно выделить три таких способа:

– содействие (лоббирование) в постановке на конкретную должность специалиста, чьи устремления отвечают интересам и потребностям Запада или рекрутирование уже назначенного. В данном случае сотрудник мотивирован на конкретную деструктивную деятельность (наносится прямой ущерб);

– продвижение управленческих кадров, некомпетентных в конкретной сфере деятельности («за былые заслуги»). У таких лиц может присутствовать мотивация к работе, но отсутствовать понимание того, что совершаемые действия не соответствуют интересам государства (опосредованный ущерб от некомпетентных действий или бездействия);

– рекрутирование конкретного лица и сопровождение его на протяжении всего трудового цикла от обучения до окончания периода заинтересованности в нем (прямой и / или опосредованный ущерб). Субъект может понимать деструктивность собственных действий, а может и обладать искаженным представлением о своей работе (деятельности). Оно может возникнуть вследствие того, что обучение, а также привитие норм, ценностей, приоритетов развития личности и государства проходило за рубежом и понятие «национальное» не сформировано (девальвировано, подменено).

Заключение. Стратегические цели и средства информационной войны стран Запада в отношении России преимущественно подчинены геополитическим устремлениям США и призваны обеспечить им мировое доминирование, формируемое недопущением появления в мире сопоставимого по возможностям центра силы. В условиях активизации Российской Федерацией внешней политики и вынужденного наращивания ею своего военного потенциала, наиболее приоритетной целью информационной войны против неё будет создание условий обрушения государственности, с последующей расконсервацией и введением внешнего управления над ресурсоемкими регионами. Частные задачи направлены: в рамках политико-идеологического направления — на разобщение нации; политико-правового — на разрушение системы управления; политико-экономического — на стагнацию развития; военно-политического — на сковывание и последующее разрушение оборонительного (защитного) потенциала; политико-кадрового — на переподчинение внешнему управлению. Применяемые информационные средства будут варьироваться от введения ограничений на доступ к важной информационной инфраструктуре до стремления латентно подчинить медийные ресурсы России собственным целям и интересам (особенно востребованные у молодежи Интернет-ресурсы). Средства воздействия могут быть применены как в отношении общества и масс (через пропаганду, манипулирование и др.), так и субъектов специализированного

сознания, к числу которых относят политическую, экономическую, военную элиту и др. Особое внимание следует уделять политико-кадровому направлению обеспечения безопасности. Это продиктовано тем, что от профессионального уровня должностных лиц и их ориентации на реализацию национально-государственных интересов, во многом будет зависеть будущее Российской Федерации.

СПИСОК ЛИТЕРАТУРЫ

1. Выступление и дискуссия на Мюнхенской конференции по вопросам политики безопасности [Электронный ресурс]. URL: http://www.kremlin.ru/ events/ president/transcripts/24034 (дата обращения 12.09.2023).
2. Strategic Information Warfare Rising [Электронный ресурс]. URL: https://www.rand.org/pubs/ monograph_reports/ MR964.html (дата обращения 12.09.2023).
3. ЕС начал работу над 12-м пакетом санкций против России, сообщил МИД Польши [Электронный ресурс]. URL: https://ria.ru/ 20230623/sanktsii-1879950272.html (дата обращения 12.09.2023).
4. Уйти от доллара: БРИКС ударит по США криптой. [Электронный ресурс]. URL: https://www.gazeta.ru/business/2020/01/16 (дата обращения 12.09.2023).
5. The U.S. Zeroes in on Russia's Borderlands [Электронный ресурс]. URL: https://worldview.stratfor.com/article/us-zeroes-russias-borderlands (дата обращения 12.09.2023).
6. Don North — US/NATO Embrace Psy-ops and Info-War [Электронный ресурс]. URL: https://consortiumnews.com/2015/09/02/usnato-embrace-psy-ops-and-info-war (дата обращения 12.09.2023).

УДК 004.056

ПРАВОВАЯ, ЭКОНОМИЧЕСКАЯ И ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ И ГОСУДАРСТВА В ГЛОБАЛЬНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Шилков Владимир Ильич
Уральский федеральный университет имени первого Президента России Б. Н. Ельцина
Мира ул., 19, Екатеринбург, 620002, Россия
e-mail: shilkov-urfu@yandex.ru

Аннотация. В статье обсуждаются правовые, экономические и информационно-психологические проблемы деструктивного информационном воздействия. Приведены сведения о мотивах, психологических особенностях злоумышленников, об инструментах информационно-психологического воздействия и видах противоправных действий, направленных на подрыв системы информационной безопасности. Названы основные виды информационно-психологических угроз для различных социальных групп населения. Приведены сведения о структурных особенностях глобального информационного пространства. Обозначены правовые проблемы централизованного управления глобальным информационным пространством.

Ключевые слова: информационная безопасность; деструктивное воздействие; угрозы; аддикции; глобальное информационное пространство.

LEGAL, ECONOMIC, INFORMATIONAL AND PSYCHOLOGICAL SECURITY OF THE INDIVIDUAL AND THE STATE IN THE GLOBAL INFORMATION SPACE

Shilkov Vladimir
Ural Federal University, named after the First President of Russia B.N. Yeltsin
19 Mira St., Yekaterinburg, 620002, Russia
e-mail: shilkov-urfu@yandex.ru

Abstract. The article discusses the legal, economic and informational-psychological problems of destructive informational influence. Information is given about the motives, psychological characteristics of intruders, tools of information and psychological influence and types of illegal actions aimed at undermining the information security system. The main types of informational and psychological threats to various social groups of the population are named. The information about the structural features of the global information space is given. The legal problems of centralized management of the global information space are outlined.

Keywords: information security; destructive impact; threats; addictions; global information space.

Введение. Активное развитие информационно-коммуникационных технологий и цифровая трансформация экономических процессов привели не только: к появлению новых видов цифровых услуг; возникновению белых, серых, черных (теневых) экономических рынков; структурной трансформации секторов экономики, но также и к новой системе социально-экономических отношений, формирующейся в глобальном информационно-экономическом пространстве. Возможности динамично развивающихся информационных технологий и средств массовых коммуникаций, которые могут управлять информационными потоками с помощью информационных фильтров, позволяют злоумышленникам, манипулируя социальными проблемами и потребностями населения, с помощью методов социальной инженерии и информационно-психологического воздействия вовлекать людей в сомнительные экономические и мошеннические проекты, в социально-опасную деятельность; распространять идеи

экстремистского характера; развязывать межличностные, социальные и межнациональные конфликты; формировать низкопробную массовую культуру; продвигать интересы определенных групп и сообществ; навязывать собственные стандарты поведения, модели потребления и восприятия информации, оказывая деструктивное воздействие в масштабах регионального, национального и глобального информационного пространства.

Актуальность исследования данного вопроса обусловлена тем, что проблема противоправного деструктивного информационно-психологического воздействия на личность, общество и государство стала одной из современных глобальных проблем мирового сообщества. Вместе с тем, авторы ряда работ обращают внимание на то, что с правовой точки зрения, дефиниция «вредоносное информационное воздействие», осуществляемое в интересах определенных политических и социальных сил и оказывающее негативное деформирующее влияние на личность, общество и информационно-психологическую среду государства, не имеет легитимного закрепления, а детальная классификации преступлений в сфере информационных технологий должна соответствовать тенденциям развития современной преступности и учитывать анализ квалификационных признаков преступлений по каждой статье уголовного кодекса. Выявление реальных информационно-психологических, экономических и правовых угроз, существующих в современном информационном пространстве часто затруднено в связи с отсутствием непосредственного контакта между объектом посягательств и злоумышленниками, ощущающими недосягаемость и безнаказанность, в связи с чем, в работе [1] отмечена целесообразность выделения понятия «цифровая среда» как части информационного пространства, компонентами которой являются информационные ресурсы, технологии и системы, участвующие в обработке информации, имеющей цифровую форму представления.

Категория «информационная безопасность личности» также требует правового сопровождения и разрешения ряда проблемных моментов, связанных с терминологией, содержанием и определением ее правого статуса. По мнению автора работы [2], юридическую проработку проблем информационной безопасности личности целесообразно вести отдельно по техническим и содержательным (смысловым) компонентам. Автор работы [3] отмечает, что несмотря на то, что информационная безопасность личности является важнейшим элементом национальной информационной безопасности, анализ специальных нормативных документов показывает, что на уровне двустороннего международно-правового сотрудничества, в ряде определений, связанных с трактовками информационной безопасности государства в целом и информационной безопасности личности, существуют определенные противоречия. В частности, определение информационной безопасности личности как состояния защищенности от внешних и внутренних угроз неоднородно и применимо преимущественно для технической сферы. Проблемы формирования системы международной информационной безопасности, по мнению авторов [4], необходимо рассматривать в контексте: возникновения новых угроз; мирового кризиса, вызванного пандемией; трансформации права и глобальной проблемы «инфодемии». Целенаправленное информационно-психологическое воздействие, осуществляемое с помощью информационно-телекоммуникационных технологий может быть направлено и на представителей различных государственных структур, на сотрудников правоохранительной сферы, а также на широкие круги населения, с целью вовлечения их в противоправную антиобщественную и антигосударственную деятельность. В оказании такого воздействия могут быть заинтересованы представители преступных сообществ и отдельных криминальных элементов, коммерческих и некоммерческих организаций, несистемных оппозиционных политических объединений.

К угрозам и противоправным действиям, направленным на подрыв системы информационной безопасности государства, следует относить действия, связанные, в том числе, с незаконным оборотом наркотических средств и цифровых валют; с социальной инженерией; с сексуальной эксплуатацией несовершеннолетних; с распространением и использованием информации, приносящей вред общественной нравственности и здоровью населения, с распространением деструктивных и экстремистских материалов. Нелегальные материалы и информация, могут распространяться, например, с помощью СМС рассылок, различных рекламных сайтов и мессенджеров.

Так, например, в соответствии со сведениями, приведенными в [5], результаты мониторинга информационного пространства Белоруссии свидетельствуют о большой вовлеченности граждан в различные интернет-сообщества деструктивного характера, и о том, что значительная часть дискуссий, имевших место в локальных белорусских телеграм-группах (чатах) в период с 1 августа по 20 октября 2020 года, была акцентирована на действиях силовых структур и содержала информацию по оперативной обстановке, в том числе сведения о перемещении подразделений и спецтехники, а также о тактических приемах силовых структур. Сотрудники государственных служб могут подвергаться информационно-психологическим атакам через традиционные средства коммуникаций и передачи информационных сообщений, к которым, в частности, могут быть отнесены средства телефонной связи и печатная продукция, включающая рекламные листки и объявления. Информационно-психологическому воздействию могут подвергаться и сотрудники силовых структур, которые в личной жизни, в большей или меньшей степени, но обращаются к инструментам социальных сетей, обеспечивающих продвижение цифрового контента. К таким инструментам, через которые может быть оказано информационно-психологическое воздействие, следует отнести, например, сайты для обмена фотографиями и видеоконтентом, микроблоги, автоматически генерируемые новостные RSS-каналы (Rich Site Summary) [6].

Цели такого воздействия могут быть связаны с попытками криминальных элементов использовать служебное положение представителей силовых структур, мотивировав их к уклонению от корректного выполнения должностных обязанностей и создав препятствия для решения поставленных перед ними оперативно-служебных задач. Деструктивное информационно-психологическое воздействие на сотрудников правоохранительной сферы может быть ориентировано на: создание у сотрудников состояния тревоги за свое будущее и искаженного ощущения реальных и вымышленных угроз; размывание чувства и гордости за свою страну. Деструктивное воздействие может быть направлено не только на изменение сознания, самовосприятия и психологического состояния отдельных сотрудников, но и на деформацию социальных отношений в коллективе, путем создания состояния групповой подавленности или конфликтности. К числу важнейших элементов системы защиты, как сотрудников государственных служб, так и пользователей социальных сетей, от угроз и деструктивного воздействия глобального информационного пространства, следует отнести психологическую устойчивость участников социальных коммуникаций.

Экономические права граждан могут нарушаться со стороны злоумышленников с преступными корыстными мотивами. К типичным экономическим угрозам в интернете, следует отнести, например, действия хакеров, направленные на кражи криптоценностей и средств, принадлежащих гражданам и хранящимся на банковских депозитах. Получение доступа к личным данным владельцев банковских вкладов могут осуществляться, например, как с помощью различных мошеннических приемов, связанных как с социальной инженерией и информационно-психологическим воздействием на потенциальных жертв, так и с помощью создания поддельных сайтов и аккаунтов. Мошеннические действия с корыстными целями могут осуществляться как с помощью похищения персональных данных, так и с помощью проведения информационно-технических атак, в результате которых, злоумышленники могут вносить фиктивные сведения об юридических лицах и индивидуальных предпринимателях даже в единые государственные реестры. Полученные данные персонального, конфиденциального и интимного характера, могут быть использованы злоумышленниками, например, для шантажа жертвы путем декларации угроз размещения этих данных в сети. Угрозы и шантаж с целью последующего получения доступа к имуществу и другим материальным ресурсам атакованного пользователя, могут быть основаны, в том числе и на использовании ложной информации, дискредитирующей и «бросающей тень» на владельца аккаунта.

Угрозы информационно-психологического воздействия со стороны злоумышленников-манипуляторов, цели которых не всегда связаны с материальной заинтересованностью, могут исходить и от людей, страдающих определенными видами психических заболеваний, либо стремящихся эксплуатировать болезненные состояния и психологические мотивы других людей. Например, такие угрозы представляют злоумышленники, эксплуатирующие болезненные состояния потенциальных жертв и стимулирующие их к игровым зависимостям (интернет-аддикции). Интернет-аддикция представляет собой форму измененного психического состояния и поведения, связанную с пагубными привычками, компьютерными и игровыми зависимостями и уходом в виртуальную реальность. Органы государственной власти и институты гражданского общества постоянно совершенствуют правовые рычаги для защиты детей и молодого поколения от тлетворного информационно-психологического влияния глобального информационного пространства. Однако, по мнению автора [7], для решения проблем интернет-аддикции необходима совместная работа многих специалистов, так как, несмотря на разрозненные, усилия психологов, юристов, медиков и педагогов, число интернет зависимых людей, часто не осознающих этой зависимости, не только не уменьшается, а постоянно увеличивается. К деструктивным молодежным субкультурам, представители которых демонстрируют признаки психических заболеваний и представляют угрозы для личности, общества и государства можно отнести: суицидальные субкультуры («группы смерти»), депрессивные, радикальные, агрессивные и девиантные сообщества; а также группы, поддерживающие вооруженные нападения злоумышленников на учащихся внутри учебных заведений. (скулшутинг) [8].

Жертвами преступников, профессионально владеющих приемами информационно-психологического воздействия могут легко стать дети и подростки, не имеющие достаточного жизненного опыта и навыков критического анализа информации. В работе [9] отмечено, что информационно-психологическими последствиями бесконтрольного доступа детей к интернету могут стать: знакомство детей с потенциально опасными людьми; нарушение нормального развития ребенка; неправильное формирование нравственных ценностей и киберзависимость. Жертвами злоумышленников, могут также стать взрослые люди, для психологического портрета которых характерны, в первую очередь, например, следующие черты: инфантильность, внушаемость, восприимчивость к воздействию на когнитивно-эмоциональную сферу; отсутствие навыков и способностей к анализу потенциальных рисков; отсутствие склонности к критическому восприятию информации; безответственные решений и стремление к достижению «легких результатов», эмоциональный тип мышления и «клиповая психология» [10]. В свою очередь, в ряде случаев, не только жертвы, попавшие в психологическую зависимость, но и их друзья и родственники могут быть вовлечены в преступные схемы, невольно став исполнителями кем-либо запрограммированных действий. Не только сами действия, нарушающие законы государства и предполагающие уголовное преследование, но и обсуждение намерений, а также и подготовка к совершения преступных действий, могут осуществляться с помощью различных психологических приемов, использующих различные информационно-коммуникационные технологии. Как правило, информационно-

психологическое воздействие ориентировано на изменение информационного статуса или личностных характеристик объекта воздействия и осуществляется с помощью определенным образом оформленной и декларируемой информации. В качестве целенаправленных методов воздействия обычно используются методы внушения, убеждения, заражения и стимулирования к подражанию.

Инструментальной основой психологического давления и доставки угроз и оскорблений до жертвы могут выступать СМС рассылки, звонки с мобильных телефонов, мгновенные сообщения и электронные письма. В связи с тем, что оскорбления, насмешки и провокации могут поступать с разных адресов электронной почты или номеров телефонов, защита от злоумышленников с помощью «черных и белых списков» не всегда является достаточно эффективной. В качестве инструментальных средств для осуществления «криминальной деятельности» могут выступать: анонимные почтовые серверы; зеркала Фейсбука, запрещенного в некоторых странах; различные сайты, на которых реализованы форумы об оружии; анонимные торговые площадки для наркобизнеса и для торговли криптовалютой.

В манипулятивный набор применяемых психотехнологий с целями психологического воздействия могут входить различные приемы и способы подачи информации с учетом социального контекста, момента и выгодного физического фона для подачи информации. К таким приемам следует отнести, например: ложь, смещение понятий, утаивание деталей и важных аспектов; искажение; компоновку тем; подтасовку фактов; манипулирование предрассудками; создание потока бессмысленной информации [11]. Современные информационно-коммуникационные инструменты позволяют злоумышленникам реализовать психотехнику, так называемого «кибербуллинга», оказывая круглосуточное давление на участников информационных коммуникаций, в частности, на сотрудников правоохранительных органов и, распространяя фейковую или компрометирующую информацию для практически неограниченной аудитории. В ряде случаев, инструментом воздействия на потенциальных жертв являются угрозы информационно-психологического воздействия и психологические атаки, использующие методы психологического травмирования пользователя, с помощью контента брутального содержания. В качестве инструментов информационно-психологического воздействия на широкий круг лиц, например, в сфере общественной деятельности, также может применяться технология, так называемого «краудсорсинга», которая позволяет с помощью информационно-технических средств вовлечь большое количество участников в процесс достижения поставленных целей, на добровольных началах или за незначительное вознаграждение. Для организации мошеннических акций, информационно-технических и информационно-психологических атак, злоумышленники также могут использовать технологии, позволяющие деанонимизировать потенциальную жертву, шантажируя владельца профиля угрозой предоставить в сеть данные о каких-либо незначительных правонарушениях, с целью его дальнейшего вовлечения в преступную деятельность.

В работе [12] отмечается необходимость решения целого ряда вопросов, связанных с проблемами идентификации владельцев социальных интернет-сетей и лиц, осуществляющих противоправную деятельность. Однако для установления ответственности за преступную деятельность, осуществляемую с помощью инструментальных возможностей сети «Интернет», необходимо определение правового статуса администраторов социальных интернет-сетей и анонимных торговых площадок. Сложность решения многих проблем правовой, экономической и информационно-психологической безопасности личности и государства обусловлена целым рядом обстоятельств, к которым относится в том числе то, что глобальное информационное пространство представляет собой открытую систему с отсутствием централизованного управления, а неоднозначность подходов мирового сообщества к оценке информационных угроз, проблемных контентов и признаков деструктивной информации создает барьеры для установления единых стандартов. Автор [2] отмечает, что на международном уровне отсутствует единство мнений относительно терминологии и наполнения понятия «информационная безопасность» и «информационная безопасность личности».

Регулирование информационных потоков в глобальном пространстве Интернета осуществляется отдельными государствами и частными компаниями на основе действующих и изменяющихся правовых и организационных мер, имеющих как разрешительный, так и запретительный характер. Отсутствие централизованного управления глобальным интернет-пространством обусловлено целым рядом правовых и имущественных обстоятельств, в соответствии с которыми, многие компоненты интернет-инфраструктуры, принадлежат крупнейшим государственным или частным телекоммуникационными компаниям. Владельцы межконтинентальных оптоволоконных линий и телефонных сетей, спутников связи, маршрутизаторов, центров обработки данных, по своему усмотрению могут сдавать в аренду сетевые ресурсы не только крупным провайдерам, но и мелким операторам, работающим с конечными потребителями, которые в свою очередь, с помощью различных экономических рычагов, касающихся размеров оплаты за предоставляемое в аренду оборудование, трафик и различные сервисы, могут ограничивать коммуникационные возможности граждан. Вместе с тем, в ряде случаев, руководствуясь своими стратегическими и оперативными интересами владельцы интернет-ресурсов могут предоставить пользователям возможность бесплатного использования пиринговых сетей.

Традиционно в структуре глобальной сети Интернет, которая представляет собой единую компьютерную сеть, обеспечивающую возможности передачи информации, выделяют 3 основных уровня: поверхностный (Surface Web); глубинный (Deep Web) и скрытый уровень (DarkNet). На долю поверхностного уровня, в котором содержится примерно 2 млрд сайтов, доступных широкому кругу пользователей, приходится не более 10 процентов

всего информационного объема глобальной сети. В отличие от поверхностного уровня, глубинный уровень Интернета, представлен множеством страниц, не индексируемых поисковыми системами. Для получения доступа к сведениям, содержащихся в базах данных, которые могут принадлежать государственным и военным структурам, компаниям, научно-исследовательским центрам, пользователь должен пройти процедуру аутентификации. На долю скрытого теневого уровня Интернета, и представленного примерно 10 тысячами сайтов, приходится примерно 0,03 % объема всей информации, содержащейся в глобальной сети.

Особое место в глобальной сети занимает теневой уровень, который существует параллельно обычному Интернету и обеспечивает анонимное информационное взаимодействие только между доверенными пользователями (пирами). В техническом плане, «DarkNet» представляет собой «теневую» одноранговую пиринговую Интернет-сеть (Overlay Network), применяются методы шифрования, нестандартные порты, протоколы, что позволяет передавать информацию анонимно и в зашифрованном виде. Анонимность при посещении сайтов, при работе с приложениями, при файлообмене и отправке почтовых сообщений, обеспечивается с помощью специального свободного и открытого программного обеспечения Tor Browser (The Onion Router). Возможности скрытых сетей по организации бесконтрольной и анонимной передачи информации являются своего рода гарантией безопасности и безнаказанности для различного рода злоумышленников и правонарушителей, позволяя им эффективно реализовывать преступные замыслы, что может способствовать формированию ощущения вседозволенности и безнаказанности при совершении противоправных действий у всех пользователей, работающих в сети «DarkNet».

По мнению автора [13], для обеспечения информационной безопасности необходимо создание единого международного правового пространства. Вместе с тем, что, несмотря на то, что в настоящее время в РФ происходит постепенное формирование информационного законодательства, законодательные инициативы носят порой разрозненный характер, а вопросы, связанные с концептуальной основой обеспечения национального информационного суверенитета, как и с обеспечением устойчивости, стабильности, защищенности, непрерывности и целостности функционирования национального сегмента сети Интернет, нуждаются в дальнейшей доработке.

По мнению автора [14], к важнейшим принципам, которые должны быть положены в основу создания системы информационной безопасности личности следует отнести принцип международного сотрудничества в сфере информационной безопасности, реализация которого предполагает международный обмен опытом и оценку эффективности мер, принятых для решения конкретных проблем. Для создания эффективных механизмов международного регулирования в условиях больших вызовов в глобальном информационном обществе необходима разработка современных моделей и новых подходов для прогнозирования перспектив развития и трансформации международных норм информационной безопасности [4]. В том случае, если мировое сообщество придет к пониманию необходимости формирования безопасного глобального виртуального пространства с помощью международных структур централизованного управления, потребуется разработка единой нормативно-правовой базы; формирование органов управления международного уровня; создание структур для предупреждения и пресечения противоправных действий; для выявления преступного контента; для расследования инцидентов и преступных сделок в глобальной сети.

Заключение. Таким образом, по результатам проведенного исследования и на основании приведенных примеров, можно сделать вывод что: проблемы, связанные с информационной безопасностью личности и государства актуальны; имеют комплексный характер и должны решаться системными методами; терминологическая база категории информационной безопасности требует постоянного правового сопровождения и актуализации; целесообразной следует считать разработку моделей информационных угроз, психологических портретов и мотивов злоумышленников, осуществляющих преступные действия с помощью современных информационных технологий; для решения проблем информационной безопасности в масштабах глобального информационного пространства необходимы усилия всего мирового сообщества.

СПИСОК ЛИТЕРАТУРЫ

1. Атагимова Э. И. Право человека на информацию: вопросы обеспечения ее достоверности в цифровом информационном пространстве // Права человека и политика права в XXI в.: перспективы и вызовы : сборник научных трудов по итогам Всероссийской научно-практической конференции с международным участием. Саратов, 2022. С. 449-465.
2. Кузьменкова Т. Н. Проблемные аспекты правового сопровождения информационной безопасности личности // Проблемы устойчивого развития регионов Республики Беларусь и сопредельных стран : сборник научных статей XI Международной научно-практической интернет-конференции / под редакцией Н. В. Маковской. Могилев, 2022. С. 71-74.
3. Бражник Т. А. Отдельные аспекты правового регулирования информационной безопасности личности // Вестник Воронежского государственного университета. Серия: Право. 2019. № 3 (38). С. 182-189.
4. Полякова Т. А., Шинкарецкая Г. Г. Проблемы формирования системы международной информационной безопасности в условиях трансформации права и новых вызовов и угроз // Право и государство: теория и практика. 2020. № 10 (190). С. 138-142.
5. Мушта А. А. Проблемные аспекты защищенности органов безопасности и правопорядка от деструктивного информационного воздействия // Деятельность правоохранительных органов на современном этапе: наука, образование, практика : сборник статей по итогам VI Международного научно-практического семинара. Минск, 2021. С. 33-35.
6. Чимаров С. Ю., Чимаров Н. С. Правовое регулирование вопросов сетевой безопасности сотрудников органов внутренних дел в контексте ведомственных нормативных правовых актов // Проблемы современного законодательства России и зарубежных стран. Материалы X Международной научно-практической конференции / отв. редакторы А. М. Бычкова, Н. В. Кешикова. Иркутск, 2021. С. 70-74.

7. Ратникова И. Г. О необходимости профилактики интернет-аддикции как вида психологической зависимости и о некоторых правовых аспектах в сфере информационной безопасности детей // Дни науки. Сборник трудов международной научно-практической конференции. В 2-х ч. / под редакцией В. И. Бакайтис, 2018. С. 319-324.
8. Смирнов А. А. Роль и функции МВД России в системе обеспечения информационно-психологической безопасности // Научный портал МВД России. 2022. № 2 (58). С. 41-49.
9. Алексеенко А. А., Иванова М. М. Обеспечение информационной безопасности учащихся при использовании интернета // Проблемы техносферной безопасности : сборник статей V международной научно-практической конференции / под редакцией М. Н. Вишняк. Барнаул, 2022. С. 101-104.
10. Виноградов М. В., Ульянина О. А. Психологические аспекты информационного воздействия на сотрудников органов внутренних дел // Психология и право. 2020. Т. 10. № 1. С. 18-29.
11. Рожков А. А., Аникеева Н. В. Психолого-педагогические условия противодействия информационно-психологическим угрозам в служебной деятельности // Морально-психологическое обеспечение деятельности органов внутренних дел: современные подходы и перспективы развития. материалы всероссийской научно-практической конференции. СПб. : Санкт-Петербургский университет МВД России, 2022. С. 30-35.
12. Рекомендации I Всероссийской научно-практической конференции «Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции (Долговские чтения)» // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции. Сборник материалов I Всероссийской научно-практической конференции. М., 2021. С. 445-451
13. Сергун П. П., Герасимов Ю. С. Информационная безопасность в Российской федерации: отдельные аспекты правового регулирования. Вестник Российской правовой академии. 2020. № 2. С. 112-117.
14. Смольяков А. А. К вопросу о защите прав и свобод человека и гражданина в контексте информационной безопасности личности // Закон. Право. Государство. 2022. № 2 (34). С. 344-350.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.451:004.056

ЦИФРОВОЙ ДВОЙНИК: ОПРЕДЕЛЕНИЕ, КЛАССИФИКАЦИЯ, СФЕРЫ ПРИМЕНЕНИЯ, ВОПРОСЫ БЕЗОПАСНОСТИ ДАННЫХ

Ананьева Варвара Яновна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия
e-mail: viaananeva@etu.ru

Аннотация. В данной статье рассматривается понятие цифрового двойника: приводится его определение, классификация. Также рассмотрены различные сферы применения, особое внимание уделяется применению цифровых двойников в медицине. Рассматривается вопрос безопасности хранения, сбора, использования данных при работе с цифровым двойником.

Ключевые слова: цифровой двойник; цифровой двойник человека; безопасность данных; защита данных; здравоохранение; медицина; цифровой двойник в здравоохранении; цифровой двойник в медицине.

DIGITAL TWIN: DEFINITION, CLASSIFICATION, APPLICATION FIELDS, DATA SECURITY ISSUES

Ananeva Varvara
Saint-Petersburg Electrotechnical University
5 Professor Popov St, St. Petersburg, 197022, Russia
e-mail: viaananeva@etu.ru

Abstract. The concept of the Digital Twin (it’s definition, classification) is considered. Various fields of application are also considered, special attention is paid to the use of Digital Twins in medicine. The issues of security of gathering, storing and using data, which is used for the work of Digital Twins of people, are also considered.

Keywords: digital twin; digital twin of human; data security; data protection; healthcare; medicine; digital twinin healthcare; digital twin in medicine.

Введение. Создание цифрового двойника (DigitalTwin, ЦД) — это непростая задача, требующая много сил и средств. ЦД создают для сложных динамических систем, которые имеют большое количество элементов, над которыми постоянно нужно осуществлять контроль, а также заниматься их управлением. В частности, ЦД позволяет сократить время создания реального физического объекта благодаря возможности моделировать различные ситуации и смотреть, как поведёт себя, в каком состоянии будет находиться объект в зависимости от различных заданных сценариев, установок. Так технология ЦД может включать в себя такие технологии, как виртуальная и дополненная реальность, Большие данные, имитационное моделирование, Промышленный интернет вещей и другие, которые позволяют следить за текущим состоянием физического объекта, имитировать и предсказывать его будущее состояние на основе текущих характеристик и «исторических» данных об изменении состояния, накопленных за период существования данного объекта или других схожих по характеристикам объектов.

ЦД (см. рис. 1) [1] — это виртуальная сущность, которая состоит из модели и процессора, который обрабатывает запросы к модели и отвечает за её адекватность (виртуальная модель и физический объект интегрируются, существует двусторонняя связь между физическим и виртуальным объектом, когда в виртуальную модель поступают данные о текущем состоянии физического объекта, а информация, полученная из виртуальной модели (прогнозы, имитации), используется для управления физическим объектом).

В соответствии с работой одних из создателей концепции ЦД Майкла Гривса и Джона Викерса [2] ЦД может быть двух типов: *ЦД-прототип* (прототип будущего цифрового двойника, который содержит всю информацию, которая необходима для создания конкретного реального физического объекта) и *ЦД-экземпляр* (возникает с появлением, созданием реального физического объекта и существует до окончания его эксплуатации). Если провести ассоциацию с программированием, то цифровой двойник-прототип — это класс с описанием его свойств (характеристик) и методов (функций). А цифровой двойник-экземпляр — это как экземпляр класса, который имеет

конкретные значения свойств, передаёт конкретные аргументы в методы. Также в классификации рассматривается *агрегированный ЦД*, который собирает, обрабатывает и анализирует данные с ЦД-экземпляров, имеющих схожую структуру.

Также существует классификация, согласно которой ЦД, в зависимости от их типа, можно разделить на: *ЦД продукта* (например, корабль, крыло самолёта), *ЦД процесса* (например, линия производства двери шкафа в цеху) и *ЦД системы* (например, завода).

ЦД имеют различные сферы применения [3, 4] (представлены на рис. 2).

Далее будет рассмотрено применение ЦД в медицине.

Цифровые двойники могут применяться не только при лечении болезней, а также для управления состоянием здоровья человека (health management), профилактики заболеваний и восстановления здоровья пациентов [4].

Рис. 1. Концепция цифрового двойника

Рис. 2. Сферы применения цифровых двойников

Человек, животное — это сложные биологические системы. Если создать цифровой двойник тела человека [5-7] или животного, можно отслеживать динамику изменения его состояния, прогнозировать и предупреждать заболевания, смотреть, как подействует на данный организм тот или иной препарат. Но к таким обследованиям человек должен быть готов, таким образом прежде чем повсеместно вводить цифровых двойников людей, их (людей) нужно подготовить психологически. Однако проблема заключается не только в создании такого двойника, но и хранении всех «исторических» данных человека, которые можно использовать для предсказания возникновения заболевания не только данного человека, но и других людей со схожими свойствами организма: данных будет очень много, а также встаёт вопрос безопасности хранения и передачи информации между двойниками-агрегаторами. Тогда, благодаря таким системам, длительность жизни людей значительно увеличится.

Использование цифровых двойников при лечении заболеваний. С помощью цифровых двойников человека можно предсказать его будущее состояние, например, после операции, проанализировать его и, если необходимо, если состояние может ухудшиться, предпринять действия во избежание риска.

Также уже сейчас проводят операции, когда хирург работает не непосредственно руками и медицинскими инструментами, а управляет роботом, которому необходимо маленькое отверстие для проведения операции, с помощью джойстика и иных средств. Усовершенствовав данную технологию, в будущем мы сможем прийти к возможности удалённых операций (удалённой хирургии), когда хирург может находиться в одном месте, а пациент в другом.

Также сами поликлиники и больницы можно рассматривать как сложные системы и превращать их в «умные производства». Необходимо следить за количеством пациентов, которые входят в здание, как их поток затем распределяется, в какое время приходит больше людей, в какое — меньше, сколько врачей работает в данный момент и сколько их всего есть, сколько человек находится в очереди к тому или иному врачу — в зависимости от различных факторов прогнозировать различные ситуации и оптимизировать процесс посещения людьми поликлиник и больниц.

Использование цифровых двойников в управлении состоянием здоровья человека (Health Management). Как уже было сказано выше, с помощью ЦД можно предсказывать будущее состояние человека на основе имеющейся информации. Также врач может, чтобы прописать лечение, предварительно испытать метод лечения на модели и при получении удовлетворительного результата назначать уже его человеку.

Также работу с цифровым двойником можно включить и в программу диспансеризации для сбора данных о человеке и составлении прогноза на основе имеющихся.

Цифровые двойники также можно применять для выявления источника стресса: на основе данных, полученных с помощью датчиков, таких как, например, умные часы, можно строить цифровые модели для управления психическим здоровьем. Было обнаружено, что что состояние некоторых органов человека зависит от эмоционального состояния, в свою очередь состояние здоровья человека также влияет на психологическое состояние человека. Обнаружение источника стресса позволяет дать рекомендации по уменьшению негативных факторов, влияющих на человека.

Цифровые двойники в планировании расписания занятий спортом. С помощью цифровых двойников можно контролировать в реальном времени состояние спортсмена, что позволяет вносить изменения в разработанный план тренировок для достижения лучшей формы спортсмена к соревнованиям.

Аналогично можно контролировать состояние здоровья обычного человека и предлагать ему различные упражнения для достижения того или иного эффекта.

Во всех рассмотренных случаях необходимо решить вопрос о безопасности хранения и использования данных людей.

Для возможности предсказания и работы ЦД-агрегаторов необходимы Большие данные, собранные от большого числа людей. Без согласия человека их взять нельзя. Но не все готовы передать данные о своём здоровье, т.к. считают, что есть вероятность утечки этих данных. Личные данные — это большая ценность, разглашать которую люди не хотят в силу различных обстоятельств. Поэтому вопрос сохранности данных, невозможности их утечки, является одним из важнейших, он блокирует дальнейшую работу с ЦД.

Обезопасить данные необходимо на следующих стадиях:

– на стадии сбора информации — если информацию вводит медицинский работник (врач, медсестра) со слов пациента или переносит информацию с бумажного носителя, у него не должно быть возможности сохранить введённую информацию у себя локально.

– на стадии хранения– данные должны храниться таким образом, чтобы напрямую с ними работать могли только отдельные пользователи по защищённому каналу.

– на стадии использования — для лечения пациента доступ к ЦД должен быть у врача и/или медсестры. Каждое обращение к данным ЦД должно сопровождаться созданием логов — кто, когда, что смотрел. Также

доступ к ЦД должен быть и у пациента. При этом для каждой роли (медицинский работник, пациент) создаётся свой интерфейс, чтобы пациент не занимался самолечением, работая с данными, которые ему выдаст ЦД.

Создав безопасных ЦД необходимо убедить пациентов, что система безопасна. Людям необходимо знать, что их данные не украдут, они не будут обнародованы, не будут использоваться в целях контроля или шантажа. Для этого в частности можно открыть доступ к логам — кто, когда и зачем работал с ЦД.

С каждым днём мы используем всё новые технологии, но не всем легко сразу к ним привыкнуть, поэтому с целью будущего ускорения работы, создания всё большего количества ЦД необходимо начать заранее рассказывать про данную технологию, про её преимущества.

Заключение. ЦД — сложная система и её безопасность играет одну из ключевых ролей. Этому вопросу необходимо уделять особое внимание, т.к. без доверия к системе сбор личной, конфиденциальной информации будет затруднён.

СПИСОКЛИТЕРАТУРЫ

1. Grieves M. Originsofthe Digital Twin Concept. Florida Institute of Technology // NASA. 2016. DOI:10.13140/RG.2.2.26367.61609.
2. Grieves M., Vickers J. Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Com-plex Systems // Transdisciplinary Perspectives on Complex Systems. Springer Cham. 2017. Pp. 85-113. DOI:10.1007/978-3-319-38756-7_4.
3. Vohra M. Digital Twin Technology. Fundamentals and Applications. USA: Scrivener Publishing and Wiley, 2023. Vohra M. Digital Twin Technology. Fundamentals and Applications. USA: Scrivener Publishing and Wiley, 2023. 272 p.
4. Jinkang Guo, Zhihan Lv. Application of Digital Twins in multiple fields // Multimedia Tools and Applications (2022) 81:26941–26967. 1202: Multimedia tools for digital twin. Springer, 2022. https://doi.org/10.1007/s11042-022-12536-5.
5. Цифровой двойник сердца // ZDRAV.EXPERT : Медтех-портал. [Электронный ресурс]. URL: https://zdrav.expert/index.php/Продукт:Цифровой_двойник_сердца (дата обращения 14.06.2023).
6. ЛЭТИ: Цифровой двойник шеи // ZDRAV.EXPERT: Медтех-портал. [Электронный ресурс]. URL: https://zdrav.expert/index.php/Продукт:ЛЭТИ:_ Цифровой_двойник_шеи (дата обращения 14.06.2023).
7. Клон в помощь: зачем ученые создают цифровые двойники сердца и легких // ИЗВЕСТИЯ iz. [Электронный ресурс]. URL: https://iz.ru/1381626/veronika-kulakova-olga-kolentcova/klon-v-pomoshch-zachem-uchenye-sozdaiut-tcifrovye-dvoiniki-serdtca-i-legkikh?ysclid=liw104q6km486241687 (дата обращения 14.06.2023).

УДК 004.082.2

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ СИСТЕМЫ ХРАНЕНИЯ ДАННЫХ С ПРИМЕНЕНИЕМ КОДОВ, ИСПРАВЛЯЮЩИХ ОШИБКИ

Архипцев Евгений Дмитриевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5 лит. Ф, Санкт-Петербург, 19702, Россия
e-mail: lokargenia@gmail.com

Аннотация. Обсуждается задача организации хранения данных, основанная на технологии RAID-массивов и кодах, исправляющих ошибки. Показано, что применяемые технологии позволяют поддерживать систему хранения данных в работоспособном состоянии при наличии отказов отдельных серверов и устройств хранения, а для защиты от потери данных в результате сбоев программного или аппаратного обеспечения используются отдельные системы резервного копирования. Рассмотрены характеристики RAID-массивов и твердотельных накопителей, как перспективных систем для хранения больших данных. Приведены схема применения кодов, исправляющих ошибки в системе хранения данных. Выполнена постановка задачи построения математической и имитационной моделей, учитывающих специфику твердотельных накопителей и позволяющих оценивать параметры систем хранения данных, использующих схемы кодирования с заданными параметрами.

Ключевые слова: система хранения данных; большие данные; RAID-массивы; твердотельные накопители; целостность данных; коды исправляющие ошибки.

ENSURING THE INTEGRITY OF THE DATA STORAGE SYSTEM WITH THE APPLICATION OF CODES, CORRECTING ERRORS

Arkhiptsev Evgeny
Saint Petersburg Electrotechnical University «LETI»
5 Professor Popov St, lit. F, St. Petersburg, 197376, Russia
e-mail: lokargenia@gmail.com

Abstract. The problem of organizing data storage based on the technology of RAID-arrays and error-correcting codes is discussed. It is shown that the technologies used make it possible to maintain the storage system in a healthy state in the presence of failures of individual servers and storage devices, and separate backup systems are used to protect against data loss due to software or hardware failures. The characteristics of RAID arrays and solid-state drives are considered as

promising systems for storing big data. The scheme of application of codes that correct errors in the data storage system is given. The task of constructing mathematical and simulation models that consider the specifics of solid-state drives and allow estimating the parameters of data storage systems using coding schemes with specified parameters is completed.

Keywords: storage system, big data; RAID; solid state drives; data integrity; error-correcting codes.

Введение. На рынке информационных услуг остается актуальным спрос на хранение данных, что является следствием развития таких направлений как аналитика данных, системы искусственного интеллекта, внедрение умной техники интернета вещей на производствах и в частном секторе. С увеличением объемов генерируемых массивов данных повышаются требования к надежности их хранения, а также доступности, производительности и энергоэффективности современных систем хранения данных (СХД) [1].

Для сохранения целостности и обеспечения доступности данных используются такие технологии как RAID — избыточные массивы независимых дисков (Redundant Array of Independent Disks) и коды исправляющие ошибки. Эти технологии позволяют поддерживать СХД в работоспособном состоянии при наличии отказов отдельных серверов и устройств хранения. Для защиты от потери данных в результате сбоев программного или аппаратного обеспечения используются отдельные системы резервного копирования.

Однако, на больших объемах обрабатываемых данных RAID-массивы становятся неэффективными — недопустимо высокие задержки пересылки данных между серверами и время отклика [2].

Появление альтернативного вида устройств хранения — твердотельных накопителей позволило значительно повысить класс систем хранения данных за счёт повышения производительности. Твердотельные накопители позволяют снизить задержку операций чтения/записи до 250 микросекунд, в то время как жёсткие магнитные диски имеют в среднем задержку 2-4 мс. С точки зрения количества операций чтения/записи в секунду твердотельные накопители превосходят производительность жёстких магнитных дисков от двух до пятнадцати раз в зависимости от сценария использования. Низкая распространенность до недавнего времени СХД, базирующихся на SDD, объясняется их более высокой стоимостью в пересчете на один гигабайт емкости [3].

Особенности СХД, базирующихся на твердотельных накопителях. Одна из важнейших характеристик систем хранения данных — это производительность, так как от неё зависит скорость обработки данных в вычислительном кластере.

С ростом вычислительных мощностей затрудняется использование систем, основанных на жёстких магнитных дисках, так как их производительность становится узким местом всей вычислительной системы. Также жёстким магнитным дискам присущи такие недостатки как плохая защита от физических воздействий (вибрации, перегрузки), высокое энергопотребление, высокий уровень шума и узкий диапазон рабочих температур.

Низкая распространённость систем хранения данных, базирующихся на твердотельных накопителях, была обусловлена их более высокой стоимостью в пересчёте на один гигабайт ёмкости, чем у жёстких магнитных дисков. Однако в настоящее время наблюдается уменьшение стоимости производства компонентов твердотельных накопителей, в связи с чем возрастает актуальность All-Flash систем хранения данных.

Наряду с упомянутыми достоинствами, твердотельные накопители также имеют и ряд недостатков:

1. Ограничение ресурса записи. Твердотельные накопители имеют ограниченный ресурс по количеству циклов записи данных. Ресурс накопителя определяется производителем и зависит от количества бит, записываемых в ячейку флэш-памяти.

2. Сложная процедура восстановления данных в случае отказа. Исходя из вышеперечисленных свойств твердотельных накопителей, можно сделать вывод что в современных системах хранения данных очень важно учитывать износ твердотельных накопителей и повышенную стоимость в пересчёте на один гигабайт ёмкости.

Характеристики SSD. Из четырех основных показателей надежности (безотказность, ремонтопригодность, долговечность и сохраняемость) два показателя — безотказности и долговечности — указываются производителями SSD дисков при изготовлении, что и обусловило выбор данных показателей для оценки СХД.

Долговечность (ресурс) каждого диска зависит от такого параметра SSD, как общий ресурс записи TBW (Total Bytes Written) и от средней интенсивности потока записи/перезаписи данных. Безотказность диска определяется таким параметром SSD, как среднее время наработки на отказ MTTF (Mean Time To Failure).

Безотказность и долговечность всей СХД определяется в зависимости от количества дисков и уровня RAID. Кроме того, представляет интерес оценка такого комплексного показателя надежности, как коэффициент готовности AR (Availability Rate), который определяется, как вероятность, что объект окажется в работоспособном состоянии в произвольный момент времени (кроме планируемых периодов, в течение которых применение объекта по назначению не предусматривается). Этот показатель включает в себя такой показатель ремонтопригодности, как среднее время восстановления системы MTTR (Mean Time to Recovery) и определяется соотношением

Системы хранения данных, использующие коды, исправляющие ошибки. Стирающие коды (англ. Erasure code) — коды, позволяющие обеспечивать доступность и целостность при помощи расширения исходных данных

избыточными, способные восстановить целые пакеты данных в случае их потери. Кодер работает с единицами данных одинакового размера, называемыми узлами. Кодер может принимать на вход несколько узлов данных и выводить несколько узлов четности (избыточных узлов). Этот процесс называется кодированием. Вместе ячейки данных и ячейки четности образуют группу кодирования. Потерянную ячейку можно восстановить, выполнив соответствующие коду вычисления над оставшимися узлами в группе; этот процесс называется декодированием.

Частные случаи кодов, исправляющих ошибки, используется в локальных системах хранения, в формах RAID-5 и RAID-6. RAID-5 использует кодирование XOR, поскольку он должен выдерживать отказ только одного диска, в то время как RAID-6 использует код Рида-Соломона с двумя ячейками четности, чтобы выдерживать до двух отказов. Размер ячейки обычно настраивается, при этом группы кодирования формируются ячейками с одинаковым смещением на каждом диске.

Общие коды, исправляющие ошибки, позволяют улучшить RAID-6 с точки зрения допустимого количества отказавших дисков, что повышает уровень отказоустойчивости. Например, в конфигурации кодирования (10+6) 16 ячеек данных и избыточности распределены по 16 дискам, что позволяет обрабатывать до шести одновременных отказов дисков. С помощью стирающих кодов организации могут внедрять системы хранения в соответствии с конкретными требованиями к целостности и доступности данных. Кроме того, стирающие коды могут позволить сократить время, необходимое для восстановления отказавшего диска, в зависимости от конфигурации кодирования. На рис. 1 представлена схема разбиения исходных данных на блоки и добавления избыточных узлов при помощи процедуры кодирования.

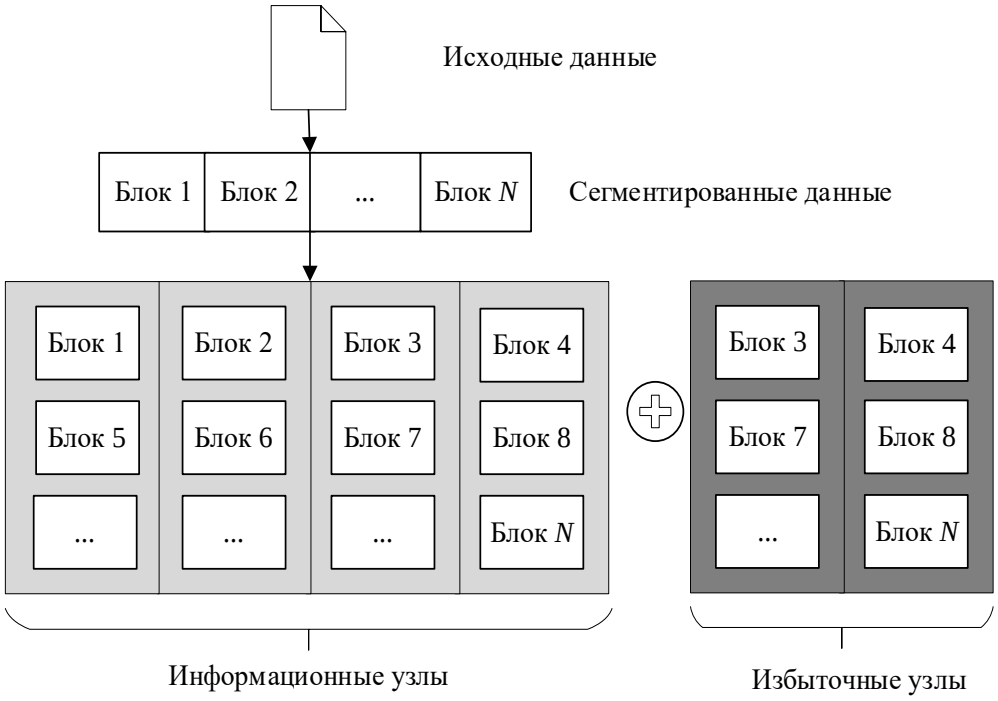


Рис. 1. Схема применения в СХД кодов, исправляющих ошибки

Для управления потенциально очень большими файлами, распределенные системы хранения обычно разделяют файлы на логические байтовые диапазоны фиксированного размера, называемые логическими блоками. Логические блоки затем сопоставляются с блоками хранения в кластере, которые отражают физическую структуру данных в кластере [4].

Простейшее отображение между логическими блоками и блоками хранения — это компоновка непрерывных блоков, при которой каждый логический блок взаимно однозначно отображается на блок хранения (рис. 2). Чтение файла с непрерывной структурой блоков эквивалентно чтению каждого блока хранения линейно по очереди.

Структура с чередованием блоков разбивает логический блок на гораздо меньшие единицы хранения, обычно называемые ячейками, и записывает повторяющиеся полосы ячеек циклически по набору блоков хранения (рис. 3).

Чтение файла с чередующейся структурой требует запроса набора блоков хранения логического блока, а затем чтения полос ячеек из набора блоков хранения. 0-1M Узел Данных 0 Блок 0 Узел Данных 1 Блок 1 Узел Данных 5 Блок 5 Узел Данных 6 Узел Данных 8 Данные Избыточность 1-2M.

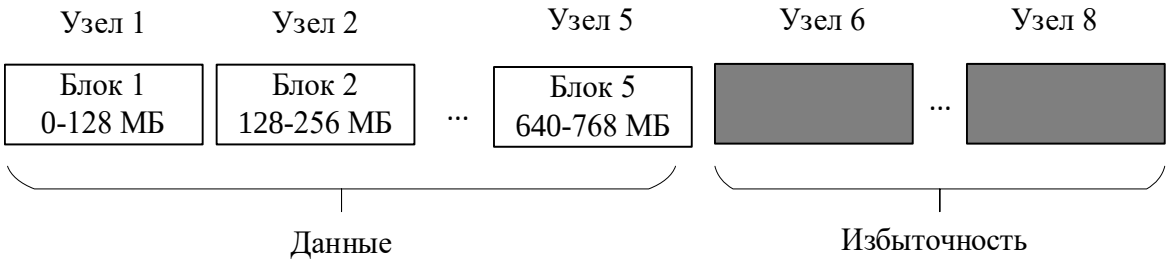


Рис. 2. Непрерывная блочная структура СХД

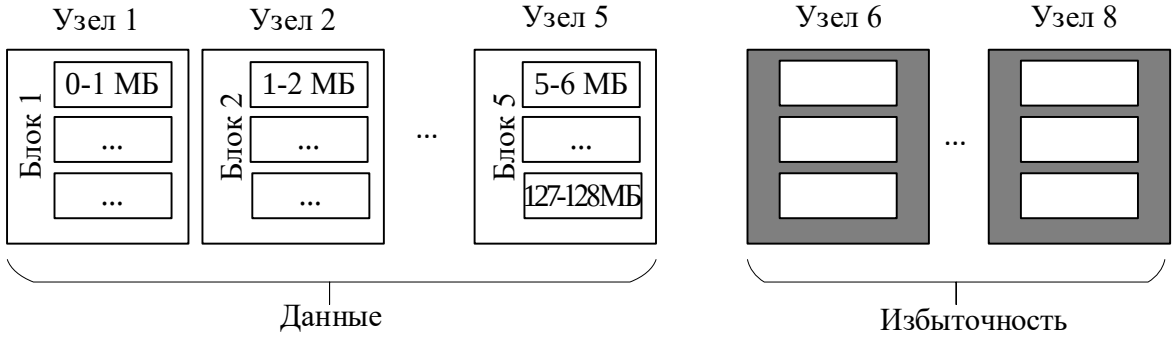


Рис. 3. Структура СХД с чередованием блоков

Постановка задачи исследования. Введены следующие допущения модели [5-8]:

1. Все устройства хранения имеют одинаковые конструктивные показатели такие как ёмкость, среднее время наработки на отказ, вероятность ошибок чтения.

2. Система хранения данных сохраняет работоспособность при отказе не более r элементов.

3. Отказавшие элементы всегда восстанавливаются совместно в рамках единого процесса восстановления.

4. Интенсивности переходов системы из состояния в состояние не зависят от времени.

Входные параметры математических моделей надёжности:

- λ — интенсивность отказов устройств хранения;
- μ — интенсивность восстановления данных для одного устройства хранения в массиве;
- ε — интенсивность ошибок чтения устройства хранения URE (от англ. Unrecoverable Read Error);
- ν — интенсивность критических ошибок программного обеспечения (ПО), управляющего массивом;
- γ — интенсивность восстановления системы из состояния потери данных (восстановление из резервной копии);
- Выходными параметрами приведённой математической моделей являются:
- $\overline{T}_{\mathrm{MTTF}}$ — среднее время наработки на отказ системы хранения данных;
- R_{AR} — стационарный коэффициент готовности;
- $\overline{T}_{\mathrm{MTTR}}$ — среднее время восстановления.

Введены в рассмотрение следующие виды отказов и ошибок устройств:

– Отказы устройств хранения. Интенсивность перехода системы из состояний i = «0» … «r» в состояние «i + 1» вследствие отказа устройства хранения обозначим за λ.

– Критические ошибки управляющего программного обеспечения. Данный вид ошибок переводит систему хранения данных из работоспособных состояний «0» … «r» в состояние «r + 1» (состояние потери данных). Обозначим интенсивность данного перехода за ν .

– Битовые ошибки чтения твердотельного накопителя. Обозначим за ε интенсивность битовых ошибок чтения твердотельного накопителя. Для вычисления данного параметра используется следующее выражение (1):

$$\varepsilon = -\mu 8 \ln V(1 - \mathrm{PUER}), \quad (1)$$

где P_{UER} — вероятность невосстанавливаемой ошибки чтения бита,

V — объём диска в битах.

Введём в рассмотрение следующие виды процессов восстановления системы:

– Восстановление системы из состояния потери данных. При отказе r+1 устройства хранения либо при критической ошибке управляющего ПО система хранения данных переходит в состояние «r+1», требующего восстановления из резервной копии, возвращающего её в полностью исправное состояние «0» . Обозначим интенсивность данного восстановления γ.

– Восстановление отказавших устройств хранения. Восстановительный процесс переводит систему из состояния i = «1»… «r» в исправное состояние «0» в соответствии с допущением 3. Обозначим интенсивность данных переходов μ. На основе приведённых выше данных построена следующая марковская цепь системы (рис. 4).

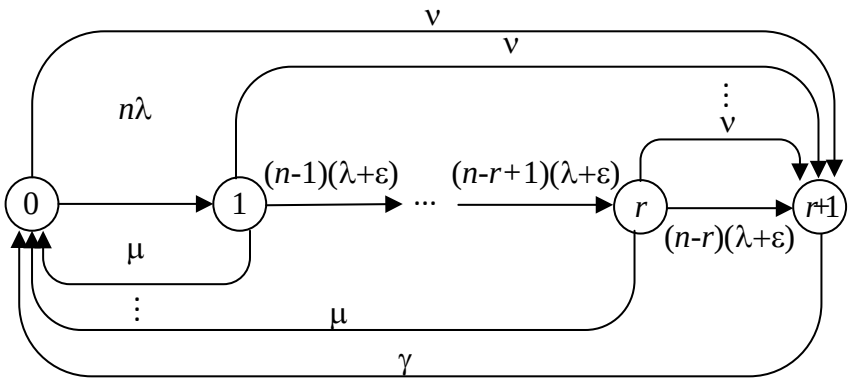


Рис. 4. Марковская модель для СХД, использующих коды исправляющие ошибки

Математическая модель на рис. 4 может быть представлена в виде системы уравнений Колмогорова-Чепмена (рис. 5):

$$\begin{cases} p_0 + p_1 + \ldots + p_r + p_{r+1} = 1; \\ -(n\lambda + \nu)\, p_0 + \mu p_1 + \ldots + \mu p_r + \gamma p_{r+1} = 0; \\ n\lambda p_0 - \left(\mu + (n-1)(\lambda+\varepsilon) + \nu\right) p_1 = 0; \\ \vdots \\ -(n-r+1)(\lambda+\varepsilon)\, p_{r-1} - \left(\mu + (n-r)(\lambda+\varepsilon) + \nu\right) p_r = 0; \\ \nu p_0 + \ldots + \nu p_{r-1} + \left((n-1)(\lambda+\varepsilon) + \nu\right) p_r - \gamma p_{r+1} = 0. \end{cases}$$

Рис. 5. Марковская модель в виде системы уравнений Колмогорова-Чепмена

Заключение. Рассмотрены архитектурные решения в области построение надёжных высокопроизводительных систем хранения данных и приведены современные тенденции в разработке систем хранения данных:

– переход с жёстких магнитных дисков на твердотельные накопители;

– развитие архитектуры программно-определённых систем хранения;

– обеспечение отказоустойчивости в системах хранения данных при помощи кодов, исправляющих ошибки.

Выполненная постановка задач и предложенная математическая модель системы хранения данных на основе марковской цепи, использующей коды, исправляющие ошибки. В построенной математической модели была учтена особенность твердотельных накопителей, влияющая на надёжность системы.

СПИСОК ЛИТЕРАТУРЫ

1. Советов Б. Я., Татарникова Т. М., Пойманова Е. Д. Модель управления масштабированием хранилища // Информационные и управляющие системы. 2020. № 5(108). С. 43-49. DOI: 10.31799/1684-8853-2020-5-43-49.
2. Татарникова Т. М., Архипцев Е. Д. Определение числа реплик распределенного хранения больших данных // Международная конференция по мягким вычислениям и измерениям. 2023. Т. 1. С. 305-308.
3. Пойманова Е. Д., Татарникова Т. М., Краева Е. В. Модель управления хранением трафика данных // Известия высших учебных заведений. Приборостроение. 2021. Т. 64. № 5. С. 370-375.
4. Татарникова Т. М., Пойманова Е. Д. Энергетическая модель процесса хранения данных // Информация и космос. 2019. № 1. С. 89-95.
5. Татарникова Т. М. Статистические методы исследования сетевого трафика // Информационно-управляющие системы. 2018. № 5 (96). С. 35-43.
6. Кутузов О. И., Татарникова Т. М. Из практики применения метода Монте-Карло // Заводская лаборатория. Диагностика материалов. 2017. Т. 83. № 3. С. 65-70.
7. Татарникова Т. М., Вольский А. В. Оценка вероятностно-временных характеристик узлов с дифференциацией трафика // Информационно-управляющие системы. 2018. № 3 (94). С. 54-60. DOI: 10.15217/issn1684-8853.2018.3.54.
8. Татарникова Т. М., Елизаров М. А. Процедура разрешения коллизий в RFID-системе // Известия высших учебных заведений. Приборостроение . 2017. Т. 60. № 2. С. 150-157. DOI: 10.17586/0021-3454-2017-60-2-150-157.

УДК 621.396.4

СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕИЯ КАК ЭФФЕКТИВНЫЙ ИНСТРУМЕНТ ПЛАНИРОВАНИЯ ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ СВЯЗИ И АВТОМАТИЗАЦИИ СИЛОВОГО ВЕДОМСТВА

Грачев Илья Борисович, Ковалев Игорь Станиславович, Пащенко Василий Владимирович
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: i.grachev@mail.gov.kz, iskova53@yandex.ru, vvpash@mail.ru

Аннотация. Планирование играет важную роль в любой организации. Эффективность управленческих решений зависит главным образом от качества информации, используемой в качестве исходных данных в процессе принятия решений. Крайне важно, чтобы системы поддержки принятия решений своевременно и точно предоставляли информацию, помогающую принимать правильные решения в том числе и непредвиденных ситуациях. В статье рассмотрены вопросы системы поддержки принятия решений и ее использование как инструмента для принятия эффективных решений при планировании технического обеспечения.

Ключевые слова: интуитивность; своевременность; система поддержки принятия решения; метод.

DECISION SUPPORT SYSTEM (DSS) AS AN EFFECTIVE TOOL FOR TECHNICAL SUPPORT PLANNING IN POWER DEPARTMENTS

Grachev Ilua, Kovalev Igory, Pashenko Vasiliy
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av., St. Petersburg, 194064, Russia
e-mails: i.grachev@mail.gov.kz, iskova53@yandex.ru, vvpash@mail.ru

Absrtact. Planning plays an important role in any organization. The effectiveness of managerial decisions depends mainly on the quality of the information used as input data in the decision-making process. It is extremely important that decision support systems provide timely and accurate information to help make the right decisions, including unforeseen situations. This article discusses the issues of the decision support system and its use as a tool for making effective decisions when planning technical support.

Key words: intuition; timeliness; decision support system; method.

Введение. Процесс принятия решений является основным моментом управленческой деятельности должностных лиц, занимающихся планированием связи и автоматизации силового ведомства.

Решения имеют разную продолжительность действия: краткосрочные решения, которые необходимо принимать каждый день (или даже несколько раз в день); долгосрочные решения, которые принимаются на несколько лет (месяцев, дней).

Должностные лица по сути являются анализаторами информации. Современный командир имеет возможность получать, хранить, обрабатывать, извлекать и отображать требуемую информацию для принятия правильного решения при планировании технического обеспечения.

Принятие неадекватных решений при планировании сложных систем (например, планирование технического обеспечения связи и автоматизации силового ведомства) может привести к увеличению сроков достижения поставленных целей задач [1].

Анализ существующей системы планирования технического обеспечения связи и автоматизации силового ведомства показал, что многие должностные лица ограничиваются шаблонными решениями, ранее применявшимися и, зачастую, в наименьшей степени подходящими для достижения основных целей.

Применение персональных вычислительных электронных машин (ПЭВМ) должностными лицами для отработки документов планирования технического обеспечения связи и автоматизации силового ведомства позволило сократить сроки отработки документов планирования, значительно повысить их качество. В тоже время стандартное программное обеспечение, установленное на ПЭВМ должностных лиц, позволяет разрабатывать далеко не все необходимые для планирования технического обеспечения связи и автоматизации документы, что значительно снижает эффективность его использования [2, 3].

Основными причинами подобного остаются: слабое знание пользователями возможностей электронного документооборота применяемого в силовом ведомстве; нежелание их изучения и использования в повседневной деятельности; недостаточно защищенность инфраструктуры связи для должностных лиц; слаборазвитое программного обеспечения для планирования технического обеспечения связи и автоматизации; нежелание должностных лиц использовать специальное программное обеспечение по организации учета вооружения и военной техники (ВВТ) по причине отсутствия актуальных данных о состоянии ВВТ.

Необходимость принятия правильного решения в допустимое время требует разработки современной системы для предоставления консультаций и помощи должностным лицам в принятии решения.

Система поддержки принятия решения (СППР) должна выполнять задачи по выбору наиболее эффективного решения из всех возможных, а также структурирование решений по выбираемым критериям (ранжирование). Она позволит обеспечивать процесс принятия решений в такой сложной среде как планирование технического обеспечения связи и автоматизации силового ведомства [4].

Следует отметить, что выбор совокупности критериев оценки является основным моментом для дальнейшего ранжирования полученных решений.

Известны следующие методы подготовки предложений в СППР:

- информационный поиск;
- поиск знаний в базах данных;
- имитационное моделирование;
- нейронные сети;
- ситуационный анализ.

Основными компонентами структуры СППР являются:

- информационное хранилище данных;
- средства извлечения, обработки и загрузки данных;
- база данных;
- система управления базами данных.

Процесс создания системы поддержки принятия решений при планировании технического обеспечения связи и автоматизации силового ведомства состоит из следующих этапов:

- анализ существующих в организации информационных потоков и процедур управления организацией;
- подготовка процедур обеспечивающих должностных лиц необходимой информацией в нужное время, в нужном месте и в нужном виде;
- настройка программных средств анализа;
- обучение должностных лиц программными средствами анализа.

Актуальность задачи повышения значений показателей обеспеченности обусловлена потребностью должностных лиц в современных СППР, в оперативном получении информации, необходимой для принятия решений.

Заключение. Решение данной задачи позволит вырабатывать правильные решения по техническому обеспечению связи и автоматизации на основе актуальной информационной базы, а также эффективно планировать техническое обеспечение связи и автоматизации силового ведомства.

СПИСОК ЛИТЕРАТУРЫ

1. Бородко А. В., Пантюхин О. И. Анализ содержания типовых стадий и задач проектирования современных центров обработки данных специального назначения // Проблемы технического обеспечения войск в современных условиях. Труды IV межвузовской научно-практической конференции : сборник. СПб.: ВАС, 2019. С. 127-131.
2. Овсянников С. Н., Пантюхин О. И., Хмелевской В. П. Организация информационного процесса в системе автоматизации управления связью // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017). VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2017. Т. 1. С. 502-507.
3. Михайличенко Н. В. Сравнительный анализ технологий построения региональных центров обработки данных // Юбилейная XV Санкт-Петербургская международная конференция «Региональная информатика 2016». СПб.: СПОИСУ, 2016. С. 102-103.
4. Котенко И. В. Теория и практика построения автоматизированных систем информационной и вычислительной поддержки процессов планирования связи на основе новых информационных технологий. СПб. : ВАС, 1998. 404 с.

УДК 004.056

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Грачев Михаил Иванович, Грачева Наталья Геннадьевна
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: mig2500@mail.ru

Аннотация. Статья посвящена вопросам информационной безопасности. В век информационных технологий происходит постоянная гонка технологий и их внедрение в жизнедеятельность человека. Электронный обмен информацией становится всё более привычной технологией, а обеспечение информационной безопасности передачи данных, остаётся актуальной задачей в работе предприятий.

Ключевые слова: информационная безопасность; обмен информацией; защищенность сети; управление; обмен данными.

ENSURING INFORMATION SECURITY OF THE ENTERPRISE

Grachev Mikhail, Gracheva Natalya
St. Petersburg University of the Ministry of internal Affairs Russia
Pilot Pilyutova Av, St. Petersburg, 198206, Russia
e-mails: mig2500@mail.ru

Abstract. The article is devoted to information security issues. In the age of information technology, there is a constant race of technologies and their introduction into human life. Electronic information exchange is becoming an increasingly common technology, and ensuring the information security of data transmission remains an urgent task in the work of enterprises.

Keywords: information security; information exchange; network security; management; data exchange.

В настоящее время в мире происходят глобальные изменения. Информационные технологии внедряются в процессы жизнедеятельности организаций и человека. Влияние информационных технологий огромно, так как они позволяют обмениваться информацией на больших расстояниях. И вопросы обеспечения информационной безопасности становятся всё более актуальной задачей.

Необходимо учесть, что к решению вопроса обеспечения информационной безопасности необходимо подходить комплексно. Комплекс мер направленных на обеспечение информационной безопасности будет состоять из решения задач по противодействию возникающим проблемам в системе управления для поддержания штатной работы организации.

Соответственно, рассматривая организацию или предприятие необходимо декомпозировать рассматриваемый объект. Рассмотрим в общем виде организацию информационной безопасности предприятия, рис. 1.

В простом виде мы можем представить прямую зависимость от квалифицированного персонала (человеческий фактор) и технического оснащения (программно-аппаратный комплекс), которым располагает предприятие.

Рис. 1. Схема зависимости ресурсов предприятия и организации информационной безопасности предприятия

На рисунке видно, что информационная безопасность будет зависеть от способности персонала по своим умениям, навыкам и квалификации обеспечивать своевременную защиту предприятия от возникающих угроз по сфере ответственности.

Способность решать задачи по противодействию несанкционированному доступу в систему управления предприятия, поддержание технических систем предприятия препятствующих их взлому имеет прямую зависимость от степени подготовки персонала или его квалификации. Квалификация должна постоянно поддерживаться за счет прохождения курсов повышения квалификации, курсов переподготовки [1-3].

В публикациях литературных источников отмечается зависимость человеческого фактора в обеспечении информационной безопасности [4, 5], даже предлагается провести анализ человеко-машинных систем их дальнейшее внедрение в жизнедеятельность человечества [6, 7].

Интерактивная карта киберугроз представлена на сайте Касперского, где в режиме реального времени представлены кибератаки [8, 9].

На рис. 1 видно, что информационная безопасность предприятия будет зависеть и от технического оснащения, которым располагает предприятие.

В современных публикациях указывается роль технического оснащения на информационную безопасность предприятия [10, 11], рассматриваются различные варианты, способствующие предотвращению негативных воздействий [12].

Техническое оснащение можно декомпозировать на аппаратную часть (серверное оборудование, мощные электронно-вычислительные машины, система контроля допуска, система видеонаблюдения и прочее оснащение), а также программное оснащение (антивирусное программное обеспечение, программы шифрования каналов передачи данных, отечественное программное обеспечение).

Для предотвращения негативного воздействия на предприятие необходимо проводить шифрование передаваемой информации. В случае если площадок предприятий много они должны располагать устройствами шифрования и дешифрования передаваемой информации.

На рис. 2 представлена примерная схема взаимодействия между площадками предприятия.

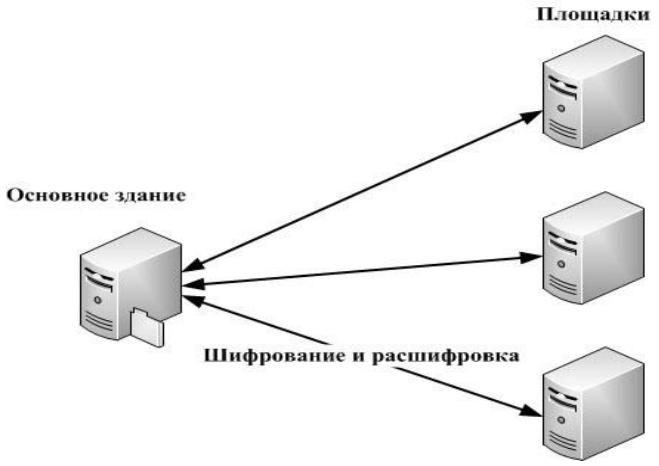


Рис. 2. Схема зависимости ресурсов предприятия и организации информационной безопасности предприятия

Важным остается переход на отечественное программное обеспечение, для снятия зависимости от иностранного программного обеспечения.

При работе в текущее время с оборудованием иностранного производства необходимо контролировать процессы обновления или отказаться от них до перехода на отечественное оборудование.

Штатная работа предприятия может быть нарушена путем внешнего воздействия, одним из них может быть кибер-атака с целью хищения данных предприятия и руководитель должен располагать моделью противодействия возникающим угрозам на предприятии [10].

Для реализации мероприятий по предупреждению срывов в работе предприятия можно воспользоваться имитационным моделированием для предварительного расчета сложных ситуаций, которые могут возникнуть в работе предприятия [13, 14].

Выводы. Анализ публикуемой литературы показал необходимость рассматривать вопросы информационной безопасности необходимо комплексно. Приоритетной задачей в настоящее время является переход на отечественное программное обеспечение и отечественное техническое обеспечение. Передача данных и информации по каналам связи должна быть защищена аппаратно-программным шифрованием, а проведение переподготовки и повышение квалификации работников предприятия, в связи с постоянным изменением руководящих документов и внедрением современных информационных технологий в работу предприятия, становится необходимостью. Применение имитационного моделирования может помочь в решении возникающих трудностей в системе управления предприятием. Предлагаемый вариант может быть дополнен другими комплексными решениями.

СПИСОК ЛИТЕРАТУРЫ

1. Бурлов В. Г., Грачев М. И., Примакин А. И. О необходимости подготовки и переподготовки квалифицированных кадров в сфере безопасности информационных технологий // Информационная безопасность регионов России (ИБРР-2017) : материалы конференции. Санкт-Петербург, 01–03 ноября 2017 г. СПб. : СПОИСУ, 2017. С. 470-472. EDN HFJEXS.
2. Бурлов В. Г., Грачев М. И., Примакин А. И. Многоуровневый подход в подготовке и переподготовке кадров в сфере безопасности информационных технологий // Региональная информатика и информационная безопасность : сборник научных трудов. Санкт-Петербург, 01–03 ноября 2017 г. Т. Вып. 3. СПб. : СПОИСУ, 2017. С. 185-189. EDN YNAEGV.
3. Воронич В. В., Грачев М. И., Локнов А. И., Примакин А. И. Подготовка и переподготовка кадров в области информационной безопасности

для правоохранительных органов // Региональная информатика и информационная безопасность : Сборник трудов. Санкт-Петербург, 26–28 октября 2016 г. Вып. 2. СПб. : СПОИСУ, 2016. С. 80-84. EDN XEYLMF.
4. Скворцов И. П. О проблеме человеческого фактора в обеспечении информационной безопасности / И. П. Скворцов, А. О. Титарев // Воздушно-космические силы. Теория и практика. 2022. № 23. С. 106-113. EDN HYFMVI.
5. Калуцкий И. В., Агафонов А. А. Роль человеческого фактора в обеспечении информационной безопасности бизнеса // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2012. № 2-2. С. 173-178. EDN RDGWMT.
6. Маркова Д. Г. Человеческий фактор в информационной безопасности // Известия Тульского государственного университета. Технические науки. 2018. № 10. С. 149-152. EDN YRBHLN.
7. Грачев М. И., Грачева Н. Г. Экономическая и информационная безопасность личности, общества и государства в сфере развития современных информационных технологий // Безопасность личности, общества и государства: теоретико-правовые аспекты : сб. научных статей XV международной научной конференции обучающихся, адъюнктов и аспирантов, проводимой в рамках II Санкт-Петербургского международного молодежного научного форума «Северная Пальмира: территория возможностей», Санкт-Петербург, 31 мая 2022 г. СПб. : Санкт-Петербургский университет МВД РФ, 2022. С. 908-913. EDN DANEIT.
8. Интерактивная карта киберугроз : [Электронный ресурс]. URL: https://cybermap.kaspersky.com/ru (дата обращения 12.06.2023).
9. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. СПб. : Издательство «Наукоемкие технологии», 2017. 546 с. ISBN 978-5-9909412-1-2. EDN ZFYEUV.
10. Трошин Д. В. Безопасность предприятия: смысл, онтология, оценка. Тверь : Тверской государственный университет, 2015. 212 с. ISBN 978-5-7609-1048-6. EDN UQUZUX.
11. Золотова В. А. Направления развития интеллектуальной информационной технологии прогнозирования состояния предприятий промышленности России в условиях неблагоприятных внешних воздействий. 2022. № 4(86). С. 71-78. DOI 10.17277/voprosy.2022.04. EDN LCDRXT.
12. Грачев М. И., Бурлов В. Г. Математическая модель для принятия решений по противодействию киберугрозам в производстве // Информационные технологии в проектировании и производстве. 2022. № 4(188). С. 22-27. DOI 10.52190/2073-2597_2022_4_22. EDN FXVJDL.
13. Грачев М. И. Имитационное моделирование процессов управления // Интеллектуальные системы в производстве. 2022. Т. 20. № 4. С. 64-71. DOI 10.22213/2410-9304-2022-4-64-71. EDN JHVVWR.
14. Грачев М. И., Бурлов В. Г., Чудаков О. Е., Примакин А. И. Имитационная модель управления образовательной организацией высшего образования // XXI век: итоги прошлого и проблемы настоящего плюс. 2021. Т. 10. № 1(53). С. 57-62. DOI 10.46548/21vek-2021-1053-0010. EDN BJCEUH.

УДК 004.056.53

ИМПОРТОЗАМЕЩЕНИЕ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПОИСК УЯЗВИМОСТЕЙ В ПРОГРАММНОМ КОДЕ

Знаменская Дарья Денисовна
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, Санкт-Петербург, 190121, Россия
e-mail: zdasha02@gmail.com

Аннотация. В данной статье представлено исследование опыта российской компании в импортозамещении решения для сферы информационной безопасности — анализатора программного кода. Автор приводит детальное, развернутое сравнение отечественного продукта с зарубежными аналогами.

Ключевые слова: информационная безопасность; импортозамещение; программное обеспечение; анализатор кода; уязвимость; ИТ-компания; аналоги.

IMPORT SUBSTITUTION IN INFORMATION SECURITY: SEARCH FOR THE VULNERABILITIES IN PROGRAM CODE

Znamenskaya Daria
Saint Petersburg State University of Aerospace Instrumentation
67 Bolshaya Morskaya St., St. Petersburg, 190121, Russia
e-mail: zdasha02@gmail.com

Abstract. In this article there is a research of the russian company’s experience in import substitution of a code analyzer for information security. The author presents a full, detailed comparison of a domestic product with foreign analogues.

Keywords: information security; import substitution; software; code analyzer; vulnerability; IT-company; analogues.

Введение. В современных реалиях, в связи с приостановкой или полным прекращением деятельности на территории Российской Федерации многих зарубежных ИТ-компаний (по данным Йельского университета, более 180 иностранных ИТ-компаний закрыли свой бизнес [1], крупнейшие из них представлены на рис. 1), как никогда остро стоит вопрос об импортозамещении программных средств.

ИТ компания	Сотрудники	Действия
Dell	100 000	приостановил продажи
IBM	345 900	приостановил продажи
HP	195 000	приостановил продажи
Accenture	624 000	полностью покинул Россию
Cisco	79 500	приостановил продажи
Oracle	132 000	приостановил продажи
Fujitsu	172 438	приостановил продажи
Amazon	1 608 000	приостановил продажи
Intel	121 100	приостановил продажи
Microsoft	181 000	приостановил новые продажи в Россию, но сохранил доступ к продуктам

Рис. 1. Крупнейшие ИТ-компании, покинувшие Россию в 2023 году [1]

Неотъемлемой частью разработки программного продукта является обеспечение информационной безопасности: защита данных и ресурсов системы. В условиях участившихся кибератак особое внимание необходимо уделять исходному коду прикладных программных решений, так как наличие уязвимостей в нем может позволить злоумышленникам похитить конфиденциальную информацию, причинить ущерб людям и техническому оборудованию или осуществить другие преступные, потенциально опасные действия [2]. В данной статье рассматривается один из отечественных анализаторов для поиска уязвимостей в коде программного обеспечения.

Solar appScreener — продукт российской компании Ростелеком-Солар, представляющий собой эффективное решение для полноценного контроля безопасности приложений [3]. Задача этого пакета программного обеспечения состоит в обнаружении недостатков кода на всех этапах цикла разработки.

Solar appScreener не только является аналогом иностранных решений (таких, как Checkmarx AST Platform от компании Checkmarx, Fortify Static Code Analyzer от компании Micro Focus и другие), но и имеет ряд весомых преимуществ:

– поддерживает наибольшее в мире количество языков программирования (36 языков и 10 форматов исполняемых файлов) [3];

– реализует бинарный анализ без исходного кода;

– осуществляет комплексный контроль информационной безопасности разрабатываемых продуктов, состоящий из статического (SAST), динамического (DAST) анализа кода и анализа состава программного обеспечения (SCA).

В таблице 1 представлено подробное сравнение Solar appScreener с двумя зарубежными аналогами.

Таблица 1

Сравнение анализаторов кода

Критерии сравнения / Продукт	Solar appScreener	Checkmarx AST Platform	Fortify Static Code Analyzer
Количество поддерживаемых языков программирования	36	25	27
Интеграция с различными средами разработки	Да	Да	Да
Сканирование бинарного кода	Да	Нет	Нет
Интеграция в SDLC (жизненный цикл разработки приложений)	Да	Да	Да
Виды анализа	SCA, SAST, DAST	SCA, SAST	SCA
Поддержка русского языка (пользовательский интерфейс, документация)	Да	Нет	Нет

Исходя из таблицы 1, можно сделать вывод, что Solar appScreener не уступает иностранным аналогам, а по отдельным критериям сравнения их превосходит.

С целью минимизировать количество ложных срабатываний и пропусков уязвимостей анализатора компания Ростелеком-Солар разработала уникальную технологию Fuzzy Logic Engine, в основу которой легла нечеткая логика. Нечеткая логика — раздел логики, в которой, в отличие от классической, вместо величин «истина» и «ложь» применяется «степень истинности», которая может принимать любое значение из бесконечного множества от 0 до 1 и задается некоторой функцией [4].

Анализатор кода Solar appScreener широко используется отечественными ИТ-компаниями. Так, например, именно этим программным средством ищут уязвимости в приложениях, создаваемых специально для автоматизации процессов сталеплавильной промышленности: производственные данные о плавке металлов относятся к коммерческой тайне, и если они попадут в руки киберпреступников, компания может понести значительные убытки. Сканирование с помощью Solar appScreener позволяет разработчикам повысить надежность приложений и устранить найденные недочеты.

Заключение. Solar appScreener является примером успешного импортозамещения зарубежных программных инструментов в сфере информационной безопасности: данное программное обеспечение сертифицировано и внесено в Единый реестр отечественного ПО [5]. На примере поиска уязвимостей в программном коде продемонстрирована важность высококачественного импортозамещения. Рекомендуется уделять повышенное внимание при разработке продуктов, призванных заменить зарубежные решения в контексте информационной безопасности, и руководствоваться опытом компании Ростелеком-Солар в отношении ее программного пакета Solar appScreener.

СПИСОК ЛИТЕРАТУРЫ

1. Бегин А. Статистика оттока ИТ-специалистов из России в 2023 году // Inclient: [сайт]. [2023]. [Электронный ресурс] URL: https://inclient.ru/outflow-it-specialists/#:~:text=Habr%202%2C%20Forbes.-,Какие%20зарубежные%20ИТ-компании%20ушли%20из%20России, после%2024%20февраля%202022%20года. (дата обращения: 23.06.2023).
2. Татарникова Т. М. Статистические методы исследования сетевого трафика // Информационно-управляющие системы. 2018. № 5 (96). С. 35-43.
3. Solar appScreener // Продукты Ростелеком-Солар : [сайт]. [2023]. [Электронный ресурс] URL: https://rt-solar.ru/products/solar_appscreener/ (дата обращения: 23.06.2023).
4. Шеври Ф., Гели Ф. Нечеткая логика // Техническая коллекция Schneider Electric: журн. 2009. [Электронный ресурс] URL: https://www.academia.edu/Техническая_коллекция_Schneider_Electric (дата посещения: 24.06.2023).
5. Реестровая запись Solar appScreener // Реестр российского программного обеспечения: [сайт]. [2023]. [Электронный ресурс] URL: https://reestr.digital.gov.ru/reestr/307469/?sphrase_id=3155775 (дата посещения: 24.06.2023).

УДК 004.056.5

ЗАЩИТА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА С ПОМОЩЬЮ ПРОГРАММНОГО ПРОДУКТА PILIGRIM

Иванов Денис Александрович, Ярош Артем Андреевич
Филиал Военного учебно-научного центра Военно-воздушных сил
«Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина
Городок 11 ул., 1, Челябинск, 454015, Россия
e-mails: prosto_deniss@mail.ru, aros32495@gmail.com

Аннотация. В статье описывается система шифрования организации защищенности процесса хранения информации электронного документооборота в условиях воздействия злоумышленника.

Ключевые слова: электронный документооборот; шифрование; система защиты; безопасность.

PROTECTION OF ELECTRONIC DOCUMENT FLOW USING THE PILIGRIM SOFTWARE PRODUCT

Ivanov Denis, Yarosh Artem
Branch of the Military Educational and Scientific Center of the Air Force
Air Force Academy named after Professor N. E. Zhukovsky and Yu. A. Gagarin
1 Town 11 St., Chelyabinsk, 454015, Russia
e-mails: prosto_deniss@mail.ru, aros32495@gmail.com

Abstract. The article describes the encryption system for organizing the security of the process of storing electronic document management information under the influence of an attacker.

Key words: electronic document management; encryption; protection system; security.

Введение. Учитывая результаты оценки эффективности существующих средств защиты информации на узлах связи ИТКС предлагается изменить порядок хранения информации.

Согласно результатам оценки, традиционный метод хранения информации на общем сервере заменяется на перспективный децентрализованный метод, при котором все автоматизированные рабочие места на узлах связи ИТКС будут участвовать в хранении данных.

С целью автоматизации процесса распределения информации между УС ИТКС и защищенного ее хранения в работе разработана программа Piligrim, в основе которой реализована технология P2P и алгоритм шифрования AES.

Программный продукт Piligrim. Программный продукт разработан в рамках данной работы, позволяет выполнить хранения данных в децентрализованной сети без применения централизованного сервера коммутации и DHCP.

Данная программа выполняет разделение файла на равные части и распространение его по оконечным устройствам внутри ЛВС. Стоит заметить, что есть возможность использования сервера безопасности и сервера DHCP при отсутствии использования статической IP адресации и в данном случае эти сервера могут обозначаться как ещё одни оконечные устройства с предоставлением своего места для хранения файлов.

Алгоритм работы. При запуске программы идет сканирование ЛВС на наличие всех АРМ сети. На всех АРМ сети должно быть запущенно данное приложение с правами суперпользователя и получая сигнал о новом объекте (открытая программа на АРМ, который раньше не учитывался для хранения данных) все АРМ участвующие в P2P обмене данных отправляют ответный сигнал для подтверждения готовности работы с данным устройством.

Интерфейс программы позволяет увидеть наличие файлов в сети и подключенных оконечных устройствах. Информация о файлах постоянно обновляется и распространяется по всей сети для предоставления актуальной информации.

При добавлении нового файла нажимаем кнопку «Добавить файл в сеть». Дальше выбираем нужный файл и идет его последовательная обработка файла.

На первом этапе идет высчитывание хеш-суммы [1] файла и запись его в файл с информацией о всех файлах сети вместе с именем. Далее идет побайтовое разделение файла на равные части. Высчитывается размер файла в байтах m. Далее идет чтение из файла по n-байт для оптимизации чтения файла 1024, 256 или 1 в зависимости от размера m.

После достижения определенного размера файл закрывается и создается новый файл, в который идет запись с момента, где остановилась программа.

После того как весь файл разделен на равные части идет шифрование всех частей по алгоритму AES. Шифрование и расшифрование при использовании данного алгоритма происходит одним и тем же сгенерированным ключом. Предварительно входные данные разбиваются на блоки по 16 байт, если полный размер не кратен 16 байтам, то данные дополняется до размера, кратного 16 байтам [3]. Блоки представляются в виде матрицы 4x4 — state. Далее происходит процедура расширения ключа и к каждому блоку state применяются операции 2-4. Итак, алгоритм состоит из следующих шагов:

1. Расширение ключа — KeyExpansion;
2. Начальный раунд — сложение state с основным ключом;
3. 9 кругов шифрования, каждый из которых состоит из преобразований:
   1.1. SubBytes;
   1.2. ShiftRows;
   1.3. MixColumns;
   1.4. AddRoundKey;
2. Финальный раунд, состоящий из преобразований:
   2.1. SubBytes;
   2.2. ShiftRows;
   2.3. AddRoundKey;

Рассмотрим подробнее каждое из представленных выше преобразований:

SubBytes — замена байтов state по таблице S-box. Каждый байт представляется в виде двух шестнадцатеричных чисел b = (x, y), где x определяется 4 старшими разрядами b, а y — 4 младшими. В таблице S-box размера 16x16 находятся значения для замены исходного байта: значение b' на пересечении строки x и столбца y S-box используется в качестве замены исходному байту.

ShiftRows — циклический сдвиг строк state. Нулевая строка остается на месте, первая смещается влево на 1 байт, вторая на 2 байта и третья на 3 соответственно

MixColumns — умножения каждого столбца state на фиксированную матрицу. Таким образом осуществляется линейное преобразование над столбцами state. Причем умножение и сложение производится по правилам, описанным выше

AddRoundKey — раундовый ключ поэлементно добавляется к state с помощью поразрядного XOR.

KeyExpansion — процедура расширения основного ключа для создания раундовых ключей, которые затем используются в раундах шифрования. Расширенный ключ состоит из 44 четырехбайтовых слов (wi): 4 слова на основной ключ и по 4 слова на 10 раундовых ключей. Таким образом, полная длина расширенного ключа составляет 1408 бит.

Операция расширения ключа использует массив Rcon и состоит из следующих действий:

Четыре слова основного ключа переносятся в первые четыре слова расширенного ключа.

Если число i без остатка делится на 4, то wi =SubBytes(RotByte(wi-1)) xor Rconi/4 . Иначе: wi = wi-4 xor wi-1.

Стоит заметить, что при искусственной избыточности, которая была достигнута во время распространения файла, файл можно восстановить даже когда выключены несколько компьютеров участвующие в хранении файла.

Так как все преобразования шифрования выполняются однозначно, то существует обратное преобразование, с помощью которого шифротекст переводится в открытый текст [9]. Обратное преобразование представляет собой последовательность инвертированных операций шифрования, выполняемых в обратном порядке:

1. Расширение ключа — KeyExpansion;
2. 9 раундов дешифрования, каждый из которых состоит из преобразований:
   2.1. AddRoundKey — суммирование state с раундовым ключом;
   2.2. InverseMixColumns — обратная перестановка столбцов state;
   2.3. InverseShiftRows — обратный циклический сдвиг столбцов state;
   2.4. SubBytes — замена байтов state по обратной таблице замен InverseS-box;
3. Финальный раунд:
   3.1. AddRoundKey;
   3.2. InverseShiftRows;
   3.3. InverseSubBytes.

Заключение. Результаты натурных испытаний программного продукта Piligrim показал его эффективность в организации защищенного процесса хранения информации в условиях воздействия злоумышленника. При выходе из строя одного или нескольких устройств, участвующих в хранении данных, данные все также можно восстановить.

При воздействии злоумышленника на одно из устройств посредством удалённого взлома возможность украсть важную информацию исключен, так как полноценного файла на устройстве нет.

СПИСОК ЛИТЕРАТУРЫ

1. Максимов М. В., Бобнев М. П., Кривицкий Б. Х. Защита от радиопомех. М.: Советское радио, 1976. 495 с.
2. Радзивский В. Г. Современная радиоэлектронная борьба. Вопросы методологии. М.: Радиотехника, 2006. 424 с.
3. Добыкин В. Д. Радиоэлектронная борьба. Силовое поражение радиоэлектронных систем. М.: Вузовская книга, 2007. 468 с.

УДК 004.056

ИСПОЛЬЗОВАНИЕ МОДИФИКАЦИЙ ДЛЯ СОЗДАНИЯ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ В КОМПЬЮТЕРНЫХ ИГРАХ

Куликов Илья Александрович, Ахрамеева Ксения Андреевна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232
e-mails: wyzzus@gmail.com, cbor@mail.ru

Аннотация. В статье рассматривается проблема защиты информации в компьютерных играх с использованием стеганографии. Рассмотрены различные типы модификаций, методы и способы их распространения через специализированные сайты-библиотеки и сервисы цифровой дистрибуции. Отмечается, что использование стеганографии в модификациях компьютерных игр предоставляет простой способ внедрения стегосистемы и расширяет возможности создания стегосистем.

Ключевые слова: стеганография; компьютерные игры; игровые модификации; стеганография в компьютерных играх.

GAME MODIFICATIONS AS A TOOL FOR CREATING STEGANOGRAPHIC SYSTEMS

Kulikov Ilya, Akhrameeva Ksenia
Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich
22 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: wyzzus@gmail.com, cbor@mail.ru

Abstract. The problem of information protection in computer games using steganography is considered. Various types of modifications, methods and ways of their distribution through specialized library sites and digital distribution services are considered. It is noted that the use of steganography in modifications of computer games provides an easy way to implement a stegosystem and expands the possibilities of creating stegosystems.

Keywords: steganography; computer games; game modifications; steganography in computer games.

Введение. Одной из наиболее важных задач для человечества была и остается защита информации. Для ее решения человек разработал множество способов защиты, в том числе и стеганографические методы защиты

информации. Стеганографические системы позволяют вложить необходимое дополнительное сообщение в некоторый объект, скрыв сам факт передачи сообщения.

Компьютерные игры, на данный момент, являются одним из наиболее популярных видов развлечений. В них сочетаются множество видов информации – визуальная, звуковая, текстовая. Сервисы цифровой дистрибуции, наподобие онлайн-магазинов и библиотек, облегчают доступ к компьютерным играм, позволяя игрокам покупать компьютерные игры без каких-либо трудностей. При этом игроки часто модифицируют игры по своему усмотрению, а сервисы цифровой дистрибуции зачастую предлагают механизмы агрегации и удобной установки пользовательских модификаций. Данные факторы делают компьютерные игры и их модификации потенциальным объектом для создания и использования стеганографических систем.

Игровые модификации. Модификация (моддинг игр) — это изменение компьютерной игры, осуществленное кем-либо, кроме ее разработчиков. Модификации могут варьироваться от небольших изменений и настроек до полной переделки и могут повысить интерес к игре и реиграбельность [1].

Моды обычно любительские и представляют собой программы, созданные фанатами игр. Они предполагают свободное распространение без оплаты [2].

Типы модификаций. У всех модификаций есть своя специфика, поэтому их принято делить на несколько категорий. Специалисты из Университета Сёдертёрна, Элеонора Хакман и Ульфрик Бьорквист, выделяют восемь основных направлений, связанных с игровыми модами [3]:

- изменение внешнего вида персонажей;
- изменение снаряжения;
- изменение параметров;
- перестановка предметов;
- улучшение графики;
- изменение локаций;
- погружение в игру;
- любая помощь в создании модов (утилиты для разработки).

Моды нередко бывают гибридными. Чем больше в них сочетаний, тем больше шансов, что мод станет масштабным аддоном или самостоятельной игрой.

Подготовка модификаций. В современном мире становится все больше игр, в которых разработчики добавляют поддержку модификаций. Примерами таких игр являются The Elder Scrolls V: Skyrim и утилита Creation Kit [4]. Данный инструмент позволяет подготавливать файлы модификаций без лишних затрат для удобной установки в саму игру. Подобные инструменты присутствуют во многих современных играх и упрощают создание игровых модификаций.

Рис. 1. Главная страница портала Nexus Mods

Распространение модификаций. Распространение модификаций может производится несколькими способами: напрямую между игроками, через специализированные сайты-библиотеки модификаций, через сервисы цифровой дистрибуции. Наиболее удобными способами являются последние два - специализированные сайты и

библиотеки дистрибьютора. Примером специализированного сайта может служить портал Nexus Mods, интерфейс которого представлен на рис. 1. На этом портале представлены десятки тысяч модификаций для популярных игр. А в качестве примера библиотеки дистрибьютора на рис. 2 представлена Мастерская Steam. Для упрощения установки оба сервиса предоставляют автоматизированные механизмы установки модификаций.

Рис. 2. Главная страница портала Мастерской Steam

Возможности стеганографии. Возможности стеганографии в модификациях к компьютерным играм сходны с теми возможностями, которые предоставляет и сама игра [5]. Отличительной чертой использования стеганографии в модификациях является относительно простой способ внедрения стегосистем. Нет необходимости модифицировать файлы самой игры, достаточно внедрить стегосистему в модификацию, а затем - установить ее в компьютерную игру на принимающей и передающей сторонах. Это позволяет снизить затраты на разработку средства передачи скрытых сообщений. При этом модификации позволяют превратить одиночную игру (без сетевого взаимодействия) в полноценную игру с кооперативными механиками, что в дальнейшем может расширить спектр возможностей создания стегосистем.

Заключение. Модификации в компьютерных играх являются очень популярным способом улучшения компьютерных игр. Они могут распространяться бесплатно, через специализированные сервисы, и устанавливаются как вручную, так и автоматизированно. Сами модификации имеют те же возможности для применения стеганографии, что и компьютерные игры, но при этом могут привносить в компьютерные игры те возможности, которые не зависят от жанра и изначальных возможностей модифицируемой игры. Данные факты делают модификации компьютерных игр отличным способом создания стеганографических систем в компьютерных играх. Однако открытым остается вопрос стегоанализа таких стегосистем.

СПИСОК ЛИТЕРАТУРЫ

1. Модификация (компьютерные игры) // Википедия. 2023 [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F_(%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B5_%D0%B8%D0%B3%D1%80%D1%8B) (дата обращения: 20.02.2023).
2. Моды для игр: что это и какие виды существуют // Настоящий хостинг картинок [Электронный ресурс]. URL: https://hostingkartinok.com/news/modyi-dlya-igr-chto-eto-i-kakie-vidyi-sushhes/ (дата обращения: 20.02.2023).
3. Игровые модификации: виды и базовый инструментарий для создания модов // Skillbox [Электронный ресурс]. URL: https://skillbox.ru/media/gamedev/igrovye-modifikatsii/ (дата обращения: 20.02.2023).
4. The Elder Scrolls Construction Set. TES5 Creation Kit // Википедия. 2023 [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/The_Elder_Scrolls_Construction_Set#TES5_Creation_Kit (дата обращения: 20.02.2023).
5. Ахрамеева К. А., Герлинг Е. Ю., Ковцур М. М., Куликов И. А. Использование стеганографии в компьютерных играх // Телекоммуникации, 2020. № 10. С. 22-26.

УДК 343

К ВОПРОСУ О НЕОБХОДИМОСТИ ПРИМЕНЕНИЯ СКАНЕРА АНАЛИЗА ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ТЕРРИТОРИАЛЬНОГО ОРГАНА МВД РОССИИ

Локнов Алексей Игоревич, Пирог Никита Викторович
Санкт-Петербургский университет МВД России
Лётчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
emails: info_for_aleksey@mail.ru, nikpirog@bk.ru

Аннотация. В статье обосновывается необходимость проведения анализа защищенность информационной инфраструктуры территориального органа МВД России. Рассматриваются основные средства анализа защищенности автоматизированных информационных систем.

Ключевые слова: анализ защищенности; кибербезопасность; уязвимость; оценка защищенности; автоматизированная информационная система.

TO THE QUESTION OF THE NEED TO USE A SCANNER FOR ANALYZING THE SECURITY OF AUTOMATED INFORMATION SYSTEMS OF A TERRITORIAL AUTHORITY MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

Loknov Alexey, Pirog Nikita
Saint Petersburg University of the Ministry of internal Affairs of the Russian Federation
1 Pilyutov's pilot St., St. Petersburg, 198206, Russia
emails: info_for_aleksey@mail.ru, nikpirog@bk.ru

Absrtact. The article substantiates the need to analyze the security of the information infrastructure of the territorial body of the Ministry of Internal Affairs of Russia. The main means of analyzing the security of automated information systems are considered.

Keywords: security analysis; cybersecurity; vulnerability; security assessment; automated information system.

Введение. Уровень защищенности – один из важнейших показателей эффективности автоматизированной информационной системы. Под понятием «защищенность» обычно подразумевается способность внедренных средств и процессов по защите информации противостоять угрозам и сохранить конфиденциальность и целостность данных.

Анализ защищенности (также называемый «оценкой защищенности») – это комплексная проверка информационной инфраструктуры на наличие возможных уязвимостей и поиск уязвимых мест в сети, включающая:

- проверку уязвимостей локальной сети [3];
- проверку на наличие вирусов [1];
- анализ надежности паролей;
- анализ необходимых обновлений безопасности операционных систем;
- анализ настроек программного обеспечения.

Говоря простыми словами, в процессе анализа защищенности проверяется безопасность различных информационных систем организации.

Даже при использовании новейших средств защиты, надлежащий контроль за безопасностью данных невозможен без выявления слабых мест, которые могут стать брешью в информационной защите территориального органа МВД России. Поэтому для реальной проверки защищенности информационных систем требуется проводить анализ защищенности внутренней ИТ-инфраструктуры территориального органа МВД России. Такой комплекс работ показывают четкую картину защищенности от угроз, помогают найти все уязвимости и сформировать стратегию по повышению уровня защищенности. Для осуществления этих мер существуют специальные средства анализа защищенности [2, 5].

Средства анализа защищенности информации осуществляют диагностику и мониторинг уязвимостей информационной систем, а также помогают составлять подробные отчеты, благодаря которым можно оперативно устранять обнаруженные недочеты без потери времени на поиск описаний обнаруженных уязвимостей.

Для осуществления анализа защищенности чаще всего используются сканеры защищенности. Основные результаты работы сканеров защищенности выражаются в отчетах с описанием найденных уязвимостей и вариантами их устранения.

Сканер обеспечивает:

- оценку эффективности мер обеспечения безопасности информационной инфраструктуры,
- проверку приложений и сервисов на наличие уязвимостей,
- оценку эффективности защитных функций ПО.

В процессе анализа защищенности сканеры могут работать в двух режимах [4]:

1) Статическое сканирование. При использовании сканера уязвимостей в режиме статического сканирования происходит пассивный анализ инфраструктуры, в процессе которого осуществляется анализ уязвимостей по косвенным признакам.

2) Динамическое сканирование. При использовании сканера уязвимостей в режиме динамического сканирования, предусматривается имитация атак потенциальных злоумышленников.

В целях проведения анализа защищенности автоматизированных информационных систем и поиска уязвимостей МВД России в соответствии с руководящими документами ФСТЭК России обязано использовать только сертифицированные средства. Таким образом, рассмотрим наиболее популярные сканеры анализа защищенности, имеющие соответствующие сертификаты:

Сканер ВС

Система комплексного анализа защищенности, обеспечивает своевременное выявление уязвимостей в информационной инфраструктуре организаций самого разного масштаба. «Сканер-ВС» позволяет проводить как специализированные тесты, так и комплексное тестирование защищенности информационных систем, сочетающие сетевые и системные проверки.

Главными преимуществами «Сканер-ВС» являются возможность развертывания в ИТ-инфраструктуре организации с поддержкой, одновременной удаленной работы пользователей, еженедельно обновляемая база уязвимостей, интуитивно понятный интерфейс, интеграция с SIEM-системами, гибкий конструктор отчетов и совместимость с отечественной ОС Astra Linux SE. Систему можно применять при проведении сертификационных и аттестационных испытаний.

«Сканер-ВС» включен в единый реестр российских программ для электронных вычислительных машин и баз данных (реестр российского ПО) в соответствии с Приказом Минкомсвязи России от 18.03.2016 г. № 23.

MaxPatrol 8

Система контроля защищенности и соответствия требованиям регулирующих органов, международных стандартов и корпоративных регламентов. Использует три модуля:

1) Pentest. Режим тестирования на проникновение, осуществляет проверки на уровне сети, а также проверки для анализа безопасности веб-приложений и системы управления базами данных.

2) Audit. Режим системного сканирования, обеспечивает контроль состояния аппаратного и программного обеспечения, выявление уязвимостей и их устранение.

3) Compliance. Режим контроля соответствия требованиям различных стандартов и законодательства.

Такой комплексный подход позволяет получать объективную оценку состояния защищенности ИТ-инфраструктуры в целом, а также отдельных подразделений, узлов и приложений для своевременного выявления уязвимостей и предотвращения угроз. MaxPatrol 8 автоматизирует процессы информационной безопасности и следит за их эффективностью, охватывая при этом все информационные ресурсы организации.

MaxPatrol VM

Система для управления уязвимостями, которая позволяет получать полные и актуальные данные о составе информационной инфраструктуры, контролировать устранение уязвимостей и отслеживать общее состояние защищенности компании.

MaxPatrol VM постоянно актуализирует сведения о состоянии IT-инфраструктуры организации, собирает наиболее полную информацию об активах, выявляет уязвимости и выстраивает процесс управления ими.

Данное решение помогает выстроить и автоматизировать управление уязвимостями с учетом значимости компонентов для рабочих процессов, охватить все системы компании, а также учитывать изменения инфраструктуры.

XSpider

Сканер уязвимостей для оценки реального состояния защищенности информационной инфраструктуры. Решение определяет компоненты сети, сканирует сетевые ресурсы на наличие уязвимостей и дает рекомендации по их устранению.

Сканирование XSpider помогает выявить:

- ошибки в веб-приложениях;
- слабые пароли;
- небезопасные беспроводные сети;
- ошибки в настройках сетевого оборудования, систем защиты периметра и баз данных.
- человеческий фактор, влияющий на информационную безопасность.

Проверку на уязвимости XSpider осуществляет автоматически по заданному расписанию. По окончанию проверок, решение выводит отчет о результатах, куда включается не только информация о найденных уязвимостях, но и ссылки на различные статьи, которые описывают обнаруженную уязвимость и дают рекомендации по ее устранению.

Заключение. В территориальном органе МВД России, использующем ведомственные автоматизированные информационные системы, необходимо регулярно проверять, насколько реализованные или используемые

механизмы защиты информации соответствуют положениям принятой в МВД России политики безопасности. Такая задача периодически возникает при изменении и обновлении компонентов автоматизированной информационной системы, изменении конфигурации операционной системы и т. п.

При этом администраторы безопасности сетей не имеют достаточно времени на проведение подобных проверок для всех узлов ведомственной сети. Поэтому специалисты отделов информационных технологий, связи и защиты информации территориальных отделов МВД России нуждаются в средствах, которые могли бы облегчить анализ защищенности используемых механизмов обеспечения информационной безопасности. Этот процесс помогают автоматизировать средства анализа защищенности, называемые, в том числе, сканерами безопасности (security scanners).

СПИСОК ЛИТЕРАТУРЫ

1. Горячев С. Н., Кобяков Н. С. Оценка состояния защищенности информационных систем от вредоносных программ // Безопасность информационных технологий. 2022. Т. 29. № 1. С. 44-56.
2. Ефимов А. О., Рогозин Е. А. О вопросах разработки программного комплекса для оценки защищенности автоматизированной системы ОВД России // Охрана, безопасность, связь. 2023. № 8-3. С. 16-20.
3. Комаричева Е. А. Анализ уязвимостей локальных сетей // Системы управления, технические системы: устойчивость, стабилизация, пути и методы исследования : материалы молодежной секции в рамках Третьей Международной научно-практической конференции, Елец, 26 апреля 2017 г. Елец : Елецкий государственный университет им. И. А. Бунина, 2017. С. 112-116.
4. Семенова А. А., Глухов Н. И. Анализ уязвимостей современных систем электронного документооборота // Информационные технологии и математическое моделирование в управлении сложными системами. 2020. № 2(7). С. 32-38.
5. Янгиров А. И. К вопросу оценки защищенности операционных систем, использующихся в автоматизированных информационных системах органов внутренних дел // Охрана, безопасность, связь. 2023. № 8-3. С. 83-90.

УДК 65.01

ОТ ДЕИНДУСТРИАЛИЗАЦИИ К РЕИНДУСТРИАЛИЗАЦИЯ ПРОМЫШЛЕННОСТИ В РАЗЛИЧНЫХ СТРАНАХ

Михайлов Николай Семёнович[1], Михайлова Анна Сергеевна[2]
[1]Санкт-Петербургский государственный университет аэрокосмического приборостроения
ул. Большая Морская, д. 67, лит. Д, Санкт-Петербург 190000, Россия
[1]Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
ул. 1-я Красноармейская, дом 1, Санкт-Петербург, 190005, Россия
e-mails: nmikhailov.ru@gmail.com, anna.mikhais@gmail.com

Аннотация. Авторами рассмотрены причины и методы реиндустриализации промышленности различных стран, а также предложены мероприятия по развитию промышленности в России.

Ключевые слова: деиндустриализация; реиндустриализация; промышленность; производство.

FROM DEINDUSTRIALIZATION TO REINDUSTRIALIZATION OF INDUSTRY IN VARIOUS COUNTRIES

Mikhailov Nikolay[1], Mikhailova Anna[2]
[1]St. Petersburg State University of Aerospace Instrumentation
st. Bolshaya Morskaya, 67, lit. D, St. Petersburg 190000, Russia
[2]Baltic State Technical University «VOENMECH» named after. D.F. Ustinova
st. 1st Krasnoarmeyskaya, building 1, St. Petersburg, 190005, Russia
e-mails: nmikhailov.ru@gmail.com, anna.mikhais@gmail.com

Abstract. The authors considered the causes and methods of reindustrialization of industry in various countries, and also proposed measures for the development of industry in Russia.

Keywords: deindustrialization; reindustrialization; industry; production.

Термин «реиндустриализация» употребляется в двух основных значениях:

1) процесс возрождения обрабатывающей промышленности;

2) государственная политика, способствующая данному процессу [1].

Развернувшийся до глобального кризиса в развитых странах в течение 30-40 лет, а в постсоветских странах - в течение 20-25 лет, современный процесс деиндустриализации, концептуально обоснованный постиндустриальным будущим капиталистического общества, привел к резкому сокращению доли промышленного производства в ВВП и промышленной занятости в разных странах.

Если в западных странах основу деиндустриализации составили экономические факторы: снижение международной конкурентоспособности и необходимость уменьшения высоких издержек трудоемких производств,

связанных с затратами на содержание дорогостоящей рабочей силы, то в постсоветских странах деиндустриализация явилась следствием либерально-рыночных реформ и носила политический характер.

В странах Запада деиндустриализация осуществлялась путем переноса производств транснациональными корпорациями за рубеж, в страны, где издержки минимизированы из-за дешевизны труда (Индию, Китай, Мексику, в новые, восточноевропейские страны ЕС).

Из европейских стран в процессах деиндустриализации лидером является Великобритания, в которой промышленность в последние 30 лет сократилась почти на 70%.

Сущностью реиндустриализации является восстановление роли промышленности как базиса развития экономики, а содержанием - восстановление, наверстывание и возрождение на новых технологических основаниях базовых отраслей индустриальных укладов, развитие высокотехнологических секторов промышленности, производств новейших технологических укладов.

Процесс реиндустриализации отражает специфику экономики страны. Поэтому он не может быть одинаковым для разных стран, в разных стратегиях развития [2].

Таблица 1.

Причины и методы реиндустриализации различных стран

№	Страна/ Континент	Причины реиндустриализации	Методы реиндустриализации
1.	США	1.Дополнительные издержки 2. Проблемы с контролем качества. 3.Преимущества локального базирования производства в стране происхождения. 4. Необходимость развития экспорта и укрепления национальных брендов. 5.Развитие инновационного производства в рамках шестого технологического уклада.	1.Возвращение промышленных производств в страну происхождения (решоринг) поближе к своим инновационным центрам и центрам НИОКР, что будет способствовать развитию исследовательского сектора и росту инновационной составляющей в промышленной продукции [2]. 2. Активное использование механизма государственно-частного партнёрства и рационального природопользования. 3.Привлечение квалифицированных кадров и рост численности занятых в промышленности. 4.Снижение стоимости энергетических ресурсов внутри США Автомобилестроение будет являться в среднесрочной и долгосрочной перспективе одним из основных секторов промышленности США [3].
2.	Европа	1.Недостаточное качество производимой продукции. 2.Низкая отдача делокализации производства. 3.Проблемы логистического характера, возникающие в результате больших расстояний между рынками сбыта в развитых странах и производителями в развивающихся экономиках.	Развитие высокотехнологичных секторов промышленности: ИТ-индустрия, телекоммуникационная техника, оптические приборы, авиастроение, космическая техника, производство новых материалов, фармацевтика, медицинское оборудование [2].
3.	Россия	1.Снижение спроса на продукцию промышленного производства. 2. Низкая рентабельность производства. 3.Дефицит ресурсного и кадрового обеспечения. 4.Несоответствие качества образования требованиям предприятий.	1.Обновление экономической системы, выбор новой модели и стратегии экономического развития. 2.Эффективное инновационное обновление традиционных секторов промышленности [1]. 3.Государственно-частное партнёрство, в рамках которого государство не только финансирует научные организации, но и разрабатывает стратегии и законы развития высокотехнологичного производства и экспорта продукции [3].

Также страны применяют бэкшоринг - деятельность переносится на родину или ниашоринг – деятельность переносится в соседнюю страну компании. В трудах российских ученых часто используется термин «Неоиндустриализация», под которым понимается вторая стадия индустриализации, заключающаяся в комплексной автоматизации производства [1].

Для всех западных экономик все более важным становится решение проблем цифровизации экономики и повышения доли высокотехнологичной продукции в общем объеме выпуска, что также является одной из важнейших причин проведения реиндустриализации [4].

В качестве аргументов в пользу реиндустриализации в США можно отметить следующие. Во-первых, обрабатывающая промышленность порождает эффекты распространения новых знаний на всю остальную экономику. Новые знания и технологии, управленческие формы, используемые в производстве новой продукции, неизбежно распространятся на другие бизнес-проекты. Во-вторых, снижение рыночной доли в отраслях, основанных на знаниях, оказывает негативный эффект на всю экономику. Так, если страна теряет аэрокосмическую отрасль, то происходит деградация всей инновационной экосистемы, что затрудняет развитие новых предприятий и генерацию новых технологий. Если утрачиваются технологические возможности в одной отрасли, то почти невозможно её возродить. Это затрудняет рост других отраслей, что ослабляет общую конкурентоспособность. В-третьих, если производство уходит за границу, то инновации обычно следуют туда же, ослабляя международную конкурентоспособность страны [3].

Исходя из вышеперечисленного, авторы предлагают следующие мероприятия по реиндустриализации промышленности в России:

1. Обеспечение квалифицированными кадрами и работа с образовательным учреждениями: популяризация рабочих специальностей, имидж профессии, единая сеть промышленно-образовательных центров.
2. Обеспечение платежеспособного спроса на продукцию промышленного производства: маркетинг, логистика, административные инструменты.
3. Повышение рентабельности производства и обеспечение ресурсами: технологии, земельные ресурсы.

СПИСОК ЛИТЕРАТУРЫ

1. Тагаров Б.Ж. Причины реиндустриализации экономики развитых стран // Экономические отношения. – 2020. – Том 10. – № 4. – С. 999-1010. – doi: 10.18334/eo.10.4.111012. URL: https://elibrary.ru/item.asp?id=44491632 (дата обращения: 04.08.2023).
2. Тараш Л.И., Голоднюк Р.А. Реиндустриализация экономики как направление промышленного развития // Вестник Института экономических исследований. 2017. №4 (8). URL: https://cyberleninka.ru/article/n/reindustrializatsiya-ekonomiki-kak-napravlenie-promyshlennogo-razvitiya (дата обращения: 04.08.2023).
3. Реиндустриализация в США и в России // Neftegaz.RU: интернет-портал. – URL: https://magazine.neftegaz.ru/articles/pervaya-strochka/674369-reindustrializatsiya-v-ssha-i-v-rossii/ (дата обращения: 04.08.2023).
4. Тагаров Б.Ж. Причины реиндустриализации экономики развитых стран // Экономические отношения. – 2020. – Том 10. – № 4. – С. 999-1010. – doi: 10.18334/eo.10.4.111012. URL: https://elibrary.ru/item.asp?id=44491632 (дата обращения: 04.08.2023).

УДК 004.855.5

АНАЛИЗ СЕТЕВОГО ТРАФИКА ПОСРЕДСТВОМ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ

Мокрецов Никита Сергеевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, лит. Ф, Санкт-Петербург, 19702, Россия
e-mail: mokrecovnikita6374@gmail.com

Аннотация. Рассматривается задача обнаружения аномального трафика, к числу которого относятся атаки и вирусы. Предлагается программный контроллер для обнаружения аномального трафика, в котором параллельно реализуются два процесса: поиск оптимальной модели искусственной нейронной сети с учетом запрашиваемых для нее гиперпараметров и нормализация данных обучающей выборки. Обучение нейронной сети происходит на основе специальных библиотек и полученного набора оптимальных гиперпараметров.

Ключевые слова: аномальный трафик; искусственная нейронная сеть; гиперпараметры нейронной сети; обучение с учителем; датасет.

NETWORK TRAFFIC ANALYSIS BY AN ARTIFICIAL NEURAL NETWORK

Mokretsov Nikita
Saint Petersburg Electrotechnical University «LETI»
5 Professor Popov St, lit. F, St. Petersburg, 197376, Russia
e-mail: mokrecovnikita6374@gmail.com

Abstract. The problem of detecting anomalous traffic, which includes attacks and viruses, is considered. A software controller proposed for detecting anomalous traffic, in which implemented two processes in parallel: searching for the optimal model of an artificial neural network, taking into account the hyperparameters requested for it, and normalizing the training sample data. The neural network was training on basis of special libraries and the resulting set of optimal hyperparameters.

Keywords: abnormal traffic; artificial neural network; neural network hyperparameters; training with a teacher; dataset.

Введение. В связи с увеличением вычислительных возможностей программно-аппаратных комплексов, в том числе в результате использования графических процессоров и распределенных архитектур вычислительных систем, стало доступным широкое применение искусственных нейронных сетей (ИНС), в том числе для анализа сетевого трафика на наличие аномальных проявлений - атак и вирусов [1].

Обращение к активному использованию ИНС обусловлен необходимостью раннего предупреждения о наличии аномального трафика и компьютерных вирусов. Методы, основанные на применении ИНС, являются сопутствующими к статистическим методам, на которых основаны современные системы обнаружения вторжений и антивирусные системы. Поскольку аномальный трафик имеет свои признаки, по которым он и может быть обнаружен, например, нехарактерное время суток, подозрительный маршрут соединения, некорректные параметры сетевых пакетов, большие объемы передаваемых данных и другие.

В статье приводится разработанный алгоритм и описание программной реализации контроллера на основе ИНС, целью которой является повышение эффективности обнаружения аномального трафика.

Постановка задачи и последовательность ее решения. Построение котроллера обнаружения аномального трафика на основе ИНС подразумевает решение ряда важных задач, таких как формирование исходного набора данных для обучения (датасета), выбор типа нейронной сети, ее гиперпараметров и тестирования ИНС.

Для обучения ИНС используются датасеты – выборки с размеченными классами аномального трафика (атаками). В отчете лаборатории Касперского [2] констатируется, что такие атаки как переполнение буфера (buffer overflow), неправильная аутентификация (brute force), SQL-инъекция, DoS-атака, XSS-атака являются наиболее распространенными. Самые популярные датасеты – NSL-KDD [3] и KYOTO 2006+ [4]. Первый датасет создан искусственно в виртуальных сетях, второй – основан на реальном сетевом трафике. Эти и другие датасеты собраны в [5].

Датасеты имеют определенную структуру, которая формируется из исходного сетевого трафика, проходящего предобработку. Предлагается использовать в качестве исходной выборки «чистый» сетевой трафик, без преобразования исходных данных в другой формат. Это позволит сократить время преобразования данных в специальный формат, особенно это актуально для высокоскоростного сетевого трафика. Следовательно, используемые данные должны быть представлены в виде pcap-файла(-ов). Соответственно, предполагается достигнуть точность обнаружения атак – 85%, что является нижней границей достигнутых результатов других исследований, но для размеченных датасетов (от 85 % до 99 %).

Таким образом, к обучению ИНС выставим следующие требования:

– Задача ИНС: классификация;
– Выборка данных: pcap-файлы;
– Типы атак (метки классов): SQL-инъекция, DoS-атака, переполнение буфера (buffer overflow), подбор паролей (brute force), XSS-атака, отсутствие атаки;
– Входные данные: csv-таблица с метками;
– Выходные данные: csv-таблица с метками;
– Точность обнаружения, в %: более 85 %.

На рис. 1 приведена функциональная модель котроллера, показывающая базовые элементы (блоки), участвующие в процессе обучения ИНС.

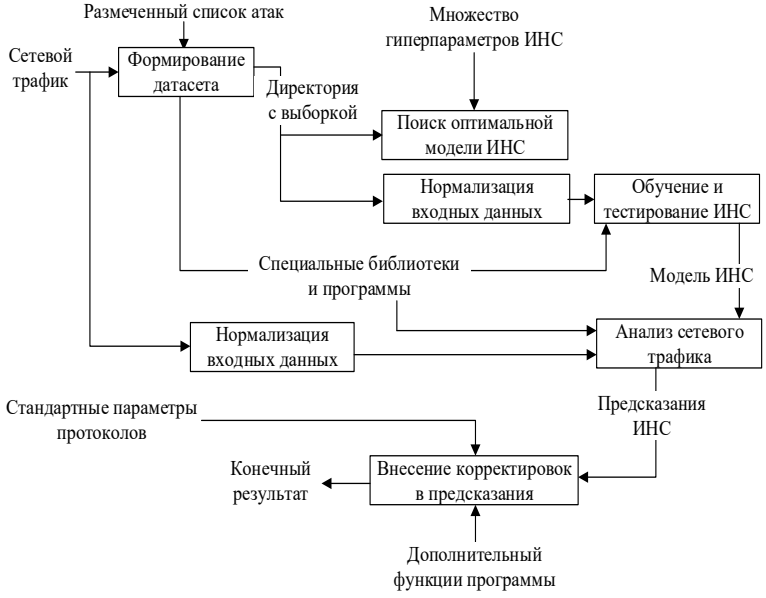


Рис. 1. Функциональная модель котроллера обнаружения аномального трафика, построенного на основе ИНС

Процесс функционирования котроллера начинается с формирования обучающей выборки ИНС. Входящий сетевой трафик на основе списка выбранных атак формируется в датасет, который сохраняется в директорию. Датасет запускает два параллельных процесса: поиск оптимальной модели ИНС с учетом запрашиваемых гиперпараметров ИНС и нормализацию данных обучающей выборки. Далее, на основе специальных библиотек и полученного набора оптимальных гиперпараметров происходит обучение ИНС. И уже обученная модель готова анализировать другие предварительно нормализованные данные, выдавая на выходе некоторые предсказания. Используя стандартные общеизвестные параметры протоколов, можно откорректировать полученные предсказания.

Обучающую выборку можно сформировать и самостоятельно, например, с помощью программы Snort [6]. Сетевой пакет, попав в Snort, последовательно проходит через декодеры, задача которых состоит в том, чтобы извлечь данные сетевого и транспортного уровней. Далее эти данные преобразуются в специальный формат, после чего к ним применяются правила. В правилах содержится информация о трафике, искомой сигнатуре, описании угрозы и как необходимо реагировать на нее [7, 8].

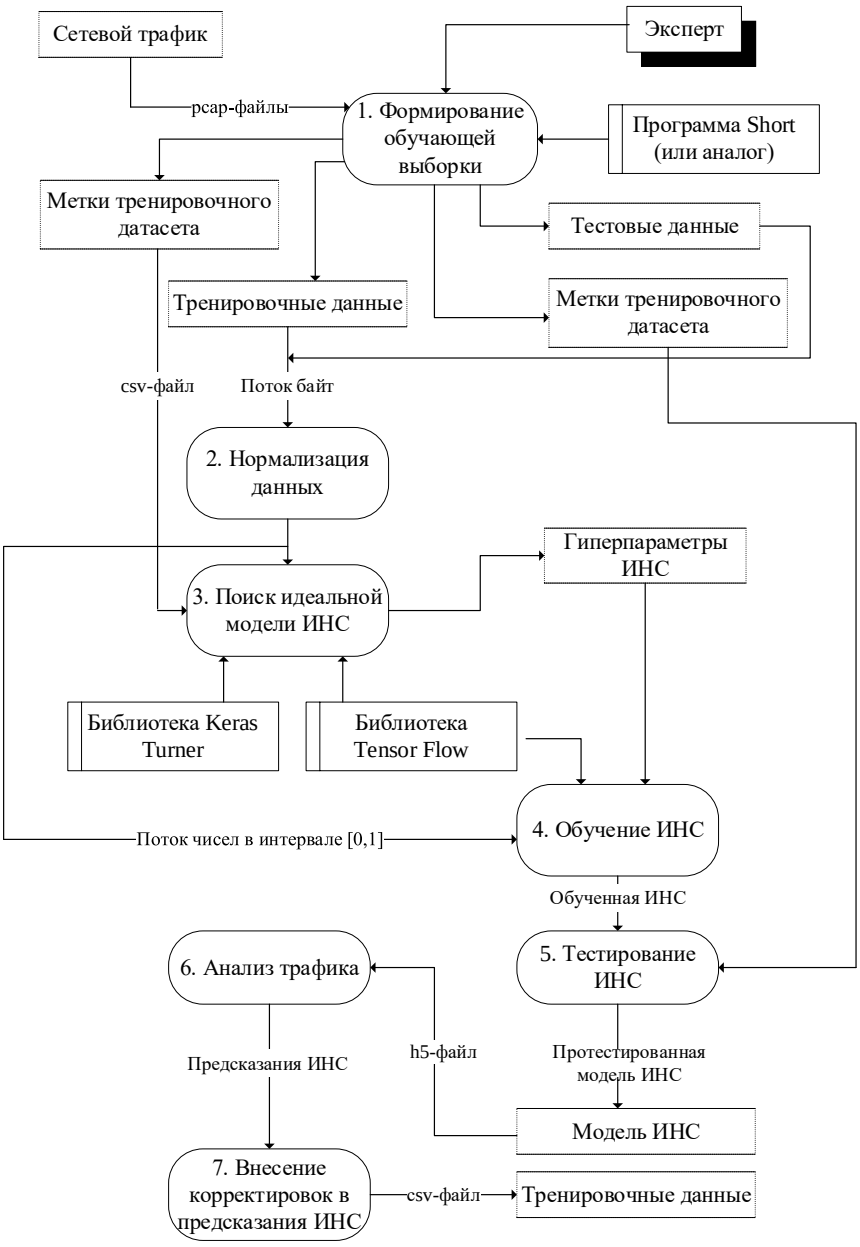


Рис. 2. Алгоритм работы котроллера обнаружения аномального трафика на основе нейросетевого метода

Сформированную выборку данных необходимо разделить на два множества: обучающее и тестовое. Для каждого множества создана таблица с метками pcap-файлов, в данной работе – csv-файлы. На рис. 2 показана

подробная схема алгоритма, реализуемого в котроллере обнаружения аномального трафика на основе нейросетевого метода. Числами показана последовательность действий.

Для обучения ИНС существуют специальные библиотеки (фреймворки). В таблице 1 приведен перечень использованных библиотек и их назначение.

Таблица 1

Используемые библиотеки

Наименование библиотеки	Назначение
TensorFlow	Работа с ИНС
Keras	Удобное использование TensorFlow
Keras Tuner	Поиск оптимальных гиперпараметров ИНС
dpkt	Работа с pcap-файлами
numpy	Работа с массивами данных
tqdm	Отслеживание прогресса выполнения задачи
csv	Работа с csv-файлами
argparse	Реализация парсера параметров запуска программы

Библиотеки TensorFlow и Keras используется для быстрого создания прототипов ИНС [9]. Для уточнения архитектуры ИНС используется библиотека Keras Tuner – определение гиперпараметров ИНС, в которые входят, например, количество слоев, их размеры, функции активации и пр.

В качестве языка программирования выбран Python, имеющий библиотеки для работы с большими данными: dpkt, numpy, tqdm, csv и argparse.

Входные данные представляют собой множество pcap-файлов, расположенных в одном каталоге. Файлы содержат сетевой трафик с классифицируемыми атаками. Выходной файл представляет собой таблицу в виде csv-файла. Структура входного файла и выходного фала повторяет таблицу 2.

Таблица 2

Структура входного и выходного файла

Название файла	Номера пакетов	Тип атаки	Название атаки
…	…	…	…

Заключение. Сложность использования искусственных нейронных сетей для обнаружения аномального трафика заключается в построении ее оптимальной архитектуры и подборе исходных данных, определяющих качество работы алгоритма обучения ИНС. Во многих исследованиях для работы с ИНС используются датасеты, но в данной работе использован «чистый» сетевой трафик.

Для построения оптимальной модели ИНС использованы библиотеки (фреймворки) TensorFlow и Keras Tuner. С их помощью удалось построить несколько моделей, показывающих высокие результаты.

Программная реализация СОА показала следующие результаты:

- котроллер способен обнаруживать атаки: «brute force», SQL-инъекция, переполнение буфера, XSS, DoS;
- обнаружение известных сетевых атак происходит в 98 % случаев;
- эксперимент по обнаружению неизвестной атаки «brute force» показало 94,7 % точности.

Полученная в экспериментах точность в 94-98 % оказалась выше ожидаемой и сравнима с результатами других исследований, где используются готовые «датасеты» с искусственными данными.

СПИСОК ЛИТЕРАТУРЫ

1. Бахарева Н. Ф., Тарасов В. Н., Шухман А. Е. Выявление атак в корпоративных сетях с помощью методов машинного обучения // Современные информационные технологии и ИТ-образование. 2018. № 3. С. 626-632.
2. Ландшафт угроз для систем промышленной автоматизации // Kaspersky Lab ICS CERT [Электронный ресурс]. URL: https://icscert.kaspersky.ru/reports/2018/03/26/threat-landscape-for-industrial-automationsystems-in-h2-2017/#_Toc508825260 (дата обращения: 20.06.2023).
3. NSL-KDD dataset // University of New Brunswick [Electronic resource]. URL: https://www.unb.ca/cic/datasets/nsl.html (дата обращения: 20.06.2023).
4. Traffic Data from Kyoto University's Honeypots [Electronic resource]. URL: http://www.takakura.com/Kyoto_data/ (дата обращения: 20.06.2023).
5. Датасеты по информационной безопасности для машинного обучения // SecurityLab.ru by Positive Technologies [Электронный ресурс]. URL: https://www.securitylab.ru/ blog/personal/Business_without_danger/345789.php (дата обращения: 20.06.2023).
6. Татарникова Т. М., Бимбетов Ф., Богданов П. Ю. Выявление аномалий сетевого трафика методом глубокого обучения // Известия СПбГЭТУ ЛЭТИ, 2021. № 4. С. 36-41.
7. Татарникова Т. М., Вольский А. В. Оценка вероятностно-временных характеристик узлов с дифференциацией трафика // Информационно-управляющие системы. 2018. № 3 (94). С. 54-60. DOI: 10.15217/issn1684-8853.2018.3.54.
8. Татарникова Т. М. Статистические методы исследования сетевого трафика // Информационно-управляющие системы. 2018. № 5 (96). С. 35-43.
9. Анчишкин А. П. Сравнительный анализ современных систем обнаружения вторжений // Colloquium-Journal. 2019. № 26 (50). С 25-27.

УДК 004.056.53

ВОЗРАСТАЮЩАЯ УГРОЗА КВАНТОВОГО ВЗЛОМА: ПОДГОТОВКА ИНФОРМАЦИОННЫХ СИСТЕМ

Степурин Константин Дмитриевич, Плеханов Егор Сергеевич
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, Санкт-Петербург, 190121, Россия
e-mails: kastian.stepurin@mail.ru, egor.plekhanov00@mail.ru

Аннотация. В статье рассматривается проблема квантового взлома, который становится все более реальной угрозой для информационных систем с развитием квантовых компьютеров. Обсуждаются технические детали квантового взлома, его потенциальные последствия для информационных систем и стратегии подготовки к этой угрозе.

Ключевые слова: квантовый взлом; информационные системы; квантовые компьютеры; криптография; безопасность данных.

THE GROWING THREAT OF QUANTUM HACKING: PREPARING INFORMATION SYSTEMS

Stepurin Konstantin, Plekhanov Egor
Saint Petersburg State University of Aerospace Instrumentation
67, Bolshaya Morskaya St, St. Petersburg, 190121 Russia
emails: kastian.stepurin@mail.ru, egor.plekhanov00@mail.ru

Abstract. The article discusses the problem of quantum hacking, which is becoming an increasingly real threat to information systems with the development of quantum computers. The technical details of quantum hacking, its potential consequences for information systems, and strategies for preparing for this threat are discussed.

Keywords: quantum hacking; information systems; quantum computers; cryptography; data security.

Введение. В современном мире, где информационные технологии играют центральную роль во многих аспектах общества, безопасность данных становится все более важной. Однако с развитием квантовых компьютеров возникает новая угроза - квантовый взлом. Это явление, которое ранее считалось лишь теоретической возможностью, теперь становится все более реальным с каждым годом.

Квантовый взлом представляет собой использование квантовых компьютеров для взлома криптографических систем, которые сегодня широко используются для защиты данных. Это становится возможным благодаря свойствам квантовых частиц, которые позволяют проводить вычисления гораздо быстрее и эффективнее, чем классические компьютер.

В этой статье рассмотрим, что такое квантовый взлом, почему он представляет собой все возрастающую угрозу для информационных систем и как мы можем подготовиться к этой угрозе.

Общее представление о квантовом взломе. Квантовый взлом — это процесс использования квантовых компьютеров для взлома криптографических систем, которые считаются безопасными для классических компьютеров. Это становится возможным благодаря принципам квантовой механики, таким как суперпозиция и запутанность [1].

Квантовые компьютеры отличаются от классических компьютеров. В то время как классические компьютеры используют биты (0 и 1) для обработки информации, квантовые компьютеры используют квантовые биты или кубиты. Кубиты могут находиться в состоянии суперпозиции, что означает, что они могут быть и 0, и 1 одновременно. Это дает квантовым компьютерам потенциально огромное преимущество в обработке информации и решении определенных задач, таких как взлом криптографических систем [2].

Однако важно отметить, что квантовые компьютеры все еще находятся в начальной стадии развития, и многие из них могут работать только при экстремально низких температурах. Кроме того, они подвержены ошибкам из-за феномена, известного как декогеренция. Но несмотря на эти проблемы, прогресс в этой области продолжается, и квантовый взлом становится все более реальной угрозой.

Почему это становится все более важной угрозой. С развитием квантовых компьютеров квантовый взлом становится все более реальной угрозой. В настоящее время большинство современных криптографических систем сосредоточены на проблемах, которые сложно решить с помощью классических компьютеров, таких как факторизация больших чисел или вычисление логарифмов в конечных полях. Однако эти проблемы могут быть эффективно решены с помощью квантовых компьютеров.

Квантовые компьютеры могут потенциально взломать эти системы, декодировав зашифрованную информацию, что может привести к серьезным последствиям, включая нарушение конфиденциальности и целостности данных. Это особенно важно для критически важных информационных систем, таких как банковские и правительственные системы, где безопасность данных имеет первостепенное значение.

В связи с этим все больше внимания уделяется разработке новых криптографических систем, устойчивых к квантовому взлому, таких как пост-квантовая криптография.

Технические детали квантового взлома. Квантовый взлом основывается на использовании квантовых алгоритмов, таких как алгоритм Шора для факторизации больших чисел и алгоритм Гровера для поиска в неструктурированной базе данных. Эти алгоритмы могут быть выполнены на квантовом компьютере существенно быстрее, чем их классические аналоги [3].

Алгоритм Шора, например, может факторизовать большое число N за время, пропорциональное $(\log N)^3$, в то время как лучший известный классический алгоритм работает за время, пропорциональное экспоненте от $(\log N)^{1/3}$. Это означает, что квантовый компьютер может факторизовать 2048-битное число за несколько часов, в то время как классическому компьютеру потребуется миллиарды лет [4].

Алгоритм Гровера позволяет искать в неструктурированной базе данных из N элементов за время, пропорциональное корню из N, в то время как классический алгоритм требует времени, пропорционального N. Это означает, что квантовый компьютер может выполнить поиск по базе данных в миллиард записей за время, примерно равное времени поиска по базе данных в тысячу записей на классическом компьютере [5].

Однако важно отметить, что эффективное использование этих алгоритмов требует квантового компьютера с большим числом кубитов и низкой ошибкой. В настоящее время такие компьютеры еще не существуют, но исследования в этом направлении активно ведутся.

Потенциальные последствия для информационных систем. Возможность квантового взлома представляет серьезную угрозу для современных информационных систем. Большинство существующих систем безопасности основаны на сложности факторизации больших чисел или дискретного логарифмирования, задач, которые могут быть эффективно решены с помощью квантовых алгоритмов.

Если квантовые компьютеры станут доступными, они могут использоваться для взлома этих систем и получения доступа к конфиденциальной информации. Это может включать в себя перехват и дешифровку зашифрованных сообщений, взлом паролей, кражу кредитной информации и другие формы кибератак.

Более того, многие из этих атак могут быть выполнены ретроспективно. Например, злоумышленник может перехватить зашифрованное сообщение сегодня и сохранить его до тех пор, пока у него не появится квантовый компьютер, способный его дешифровать. Это означает, что конфиденциальная информация, может быть, под угрозой даже если квантовые компьютеры не станут доступными в ближайшем будущем.

Примеры реальных угроз и их влияние. Хотя полноценные квантовые компьютеры, способные взломать современные криптосистемы, еще не созданы, уже существуют реальные угрозы, связанные с квантовым взломом [6].

1. Сбор и хранение зашифрованных данных: некоторые организации и государства уже начали собирать и хранить зашифрованные данные в надежде, что в будущем они смогут их дешифровать с помощью квантовых компьютеров. Это представляет угрозу для любой конфиденциальной информации, которая была передана или хранится в электронном виде.

2. Развитие квантовых технологий: несмотря на то, что квантовые компьютеры, способные взломать современные криптосистемы, еще не существуют, технологии в этой области развиваются очень быстро. Например, компания Google уже заявила о достижении «квантового превосходства», что означает, что они создали квантовый компьютер, который может решать задачи, недоступные для классических компьютеров.

3. Угроза для блокчейн технологий: блокчейн и криптовалюты, такие как Bitcoin, основаны на криптографических алгоритмах, которые могут быть взломаны с помощью квантовых компьютеров. Это может привести к крупномасштабным финансовым потерям и подорвать доверие к этим технологиям.

Все эти примеры подчеркивают важность разработки квантово-устойчивых криптосистем и других методов защиты данных.

Подготовка информационных систем. С учетом возрастающей угрозы квантового взлома, подготовка информационных систем становится все более важной задачей. Рассмотрим текущие стратегии и предложим некоторые методы для улучшения защиты от квантового взлома.

Текущие стратегии и их эффективность. Существующие стратегии защиты от квантового взлома включают в себя разработку новых криптографических алгоритмов, которые могут противостоять квантовым атакам, и использование квантовой криптографии для защиты данных.

1. Пост-квантовая криптография: это область криптографии, которая занимается разработкой криптографических алгоритмов, устойчивых к атакам с использованием квантовых компьютеров. Несмотря на то, что эта область находится в стадии активного исследования, уже существуют некоторые алгоритмы, которые считаются потенциально устойчивыми к квантовому взлому.

2. Квантовая криптография: это метод защиты информации, использующий принципы квантовой механики. Наиболее известный пример — это квантовый распределение ключей, которое позволяет двум сторонам обмениваться секретным ключом, который может быть использован для шифрования и дешифрования сообщений. Если кто-то попытается перехватить ключ, это будет немедленно заметно благодаря законам квантовой механики.

Однако, несмотря на эти усилия, существует множество проблем и вызовов, связанных с защитой информационных систем от квантового взлома.

Предложения по улучшению защиты от квантового взлома. В свете вышеупомянутых вызовов, существует несколько предложений по улучшению защиты информационных систем от квантового взлома:

1. Ранняя подготовка и образование: одним из ключевых аспектов защиты от квантового взлома является ранняя подготовка. Это включает в себя обучение и образование специалистов в области квантовой криптографии и пост-квантовой криптографии. Чем больше специалистов будет готово к приходу квантовых компьютеров, тем лучше мы сможем защитить наши информационные системы.
2. Исследование и разработка: необходимо продолжать исследования в области пост-квантовой криптографии и квантовой криптографии. Это поможет нам лучше понять возможные угрозы и разработать более эффективные методы защиты.
3. Стандартизация: важно работать над стандартизацией пост-квантовых криптографических алгоритмов. Это поможет обеспечить, что все используют одни и те же методы защиты, что упростит процесс обеспечения безопасности.
4. Регулятивные меры: правительства и регуляторы должны также играть свою роль в защите от квантового взлома. Это может включать в себя введение законов и регуляций, которые обязывают организации принимать меры по защите своих информационных систем от квантового взлома.
5. Создание квантово-устойчивых сетей: в долгосрочной перспективе, строительство квантово-устойчивых сетей может быть одним из наиболее эффективных способов защиты от квантового взлома. Это включает в себя использование квантового распределения ключей для обеспечения безопасного обмена информацией.

Эти предложения могут помочь в подготовке информационных систем к угрозе квантового взлома. Однако важно помнить, что это быстро развивающаяся область, и стратегии должны постоянно обновляться, чтобы идти в ногу с последними разработками.

Заключение. В этой статье рассмотрена угроза, которая представляет квантовый взлом для информационных систем. Рассмотрены технические детали квантового взлома, его потенциальные последствия для информационных систем, а также примеры реальных угроз и их влияние. Предложены несколько стратегий для улучшения защиты информационных систем от квантового взлома.

Важно подчеркнуть, что квантовый взлом – это быстро развивающаяся область, и стратегии защиты должны постоянно обновляться, чтобы держаться наравне с последними разработками. В свете этого, продолжение исследований в этой области имеет критическое значение.

СПИСОК ЛИТЕРАТУРЫ

1. Ван И. Современные квантовые технологии защиты информации // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2023. № 1–2.
2. Andreev A. S., Khrapov P. V. Emulators of quantum computers on qubits and on qudits // Modern information technologies and it-education. 2022. Vol. 18, № 2.
3. Фолджер Т. Квантовый взлом // В Мире Науки. 2016. № 4.
4. Nonresonant effects in the implementation of the quantum Shor algorithm / Berman G. P. [et al]. // Physical Review a: Atomic, Molecular, and Optical Physics. 2000. Vol. 61, № 4.
5. Шемякина М. А. Алгоритм моделирования квантового алгоритма гровера // Аллея Науки. 2019. Vol. 1, № 1 (28).
6. Лежинский М. В. Алгоритмы шифрования, устойчивые ко взлому в условиях квантового превосходства // Современная школа России. Вопросы модернизации. 2021. № 2-1 (35).

УДК 004.056.53

ЭКОНОМИЧЕСКИЕ ПОТЕРИ ОТ КИБЕРАТАК: МЕТОДЫ ОЦЕНКИ И МИНИМИЗАЦИИ

Степурин Константин Дмитриевич, Плеханов Егор Сергеевич
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, Санкт-Петербург, 190121, Россия
e-mails: kastian.stepurin@mail.ru, egor.plekhanov00@mail.ru

Аннотация. В статье рассматривается проблема кибератак и их влияния на экономику. Основное внимание уделяется методам оценки экономических потерь от кибератак и методам их минимизации. Представлены аналитические соотношения для оценки эффективности этих методов.

Ключевые слова: кибератаки; экономические потери; методы оценки; методы минимизации; эффективность.

ECONOMIC LOSSES FROM CYBERATTACKS: METHODS OF ASSESSMENT AND MINIMIZATION

Stepurin Konstantin, Plekhanov Egor
Saint Petersburg State University of Aerospace Instrumentation
67, Bolshaya Morskaya St, St. Petersburg, 190121 Russia
emails: kastian.stepurin@mail.ru, egor.plekhanov00@mail.ru

Abstract. The article deals with the problem of cyberattacks and their impact on the economy. The main focus is on methods for assessing economic losses from cyberattacks and methods for their minimization. Analytical relations are presented for assessing the effectiveness of these methods.

Keywords: cyberattacks; economic losses; assessment methods; minimization methods; efficiency.

Введение. В современном мире кибератаки стали значительной проблемой, влияющей на экономику многих стран. С увеличением числа цифровых систем и сетей, становится все более важным понимание того, как кибератаки могут влиять на экономическую стабильность и безопасность. Это исследование посвящено методам оценки экономических потерь от кибератак и методам их минимизации.

Целью данного исследования является анализ существующих методов оценки экономических потерь от кибератак и методов минимизации этих потерь. Важность этого исследования обусловлена необходимостью разработки эффективных стратегий и мер по снижению экономического ущерба от кибератак.

Обзор литературы. В научной литературе представлены различные подходы к оценке экономических потерь от кибератак. Одним из наиболее распространенных подходов является использование моделей риска, которые учитывают вероятность кибератаки и потенциальный ущерб от нее [1]. Эти модели обычно основываются на статистическом анализе данных о прошлых кибератаках и их последствиях. Другой подход включает в себя использование экономических моделей, которые учитывают такие факторы, как затраты на восстановление после атаки, потерю дохода и репутационные потери [2, 3].

В отношении методов минимизации экономических потерь от кибератак, существуют различные стратегии и технологии. Они включают в себя использование современных технологий шифрования, которые помогают защитить данные от несанкционированного доступа. Обучение персонала является еще одним важным аспектом, поскольку часто кибератаки происходят из-за ошибок или недостатка знаний сотрудников. Кроме того, разработка планов реагирования на инциденты может помочь организациям быстро и эффективно реагировать на кибератаки, минимизируя потенциальный ущерб.

Методы оценки экономических потерь от кибератак. Оценка экономических потерь от кибератак представляет собой сложную задачу, ставящую перед собой множество переменных. Для решения этой задачи были разработаны разнообразные методы, каждый из которых обладает своими преимуществами и недостатками.

Один из наиболее часто используемых подходов основывается на применении статистических моделей, которые строятся на основе данных о предшествующих кибератаках. Этот метод позволяет оценивать вероятность возникновения кибератаки и ее возможные последствия. Однако данный подход ограничен тем фактом, что он может быть неэффективен при оценке новых форм кибератак, отсутствующих в исторических данных.

Альтернативным подходом является применение экономических моделей, включающих такие факторы, как затраты на восстановление после атаки, прямые и косвенные потери дохода, а также репутационные риски. Данный подход, хотя и требует более сложного анализа и обработки большего объема данных, может дать более точные результаты.

Существуют и другие методы, такие как сценарное моделирование и оценка рисков киберстрахования. Сценарное моделирование предполагает создание и анализ различных гипотетических «сценариев» кибератак, что позволяет оценивать потенциальные угрозы и их возможное влияние на организацию. Оценка рисков киберстрахования — это подход, при котором страховые компании анализируют безопасность системы, историю кибератак и потенциальные угрозы для определения страховой премии [4].

Пример применения различных методов оценки можно проследить на примере кибератаки 2017 года на крупную транспортную компанию «Maersk», известную как «NotPetya». Атака привела к значительному сбою в работе компании и нарушению поставок грузов по всему миру. Для оценки экономических потерь от этой атаки, «Maersk» использовала комбинацию статистических и экономических моделей, а также сценарного моделирования. В результате, общие потери были оценены в $300 миллионов.

Таким образом, различные методы оценки экономических потерь от кибератак могут быть эффективны в разных контекстах и при различных условиях. Например, статистические модели хорошо подходят для оценки потерь от кибератак на крупные корпорации, в то время как экономические модели могут быть более эффективны при оценке потерь на малых и средних предприятиях.

Методы минимизации экономических потерь от кибератак. Минимизация экономических потерь от кибератак требует комплексного подхода, включающего в себя не только технические меры, но и организационные и правовые стратегии.

Применение стандартов кибербезопасности, таких как ISO 27001 или NIST Cybersecurity Framework, оказывается одним из наиболее эффективных методов смягчения потерь. Эти стандарты предлагают систематический подход к управлению рисками кибербезопасности, охватывающий идентификацию и классификацию активов, оценку угроз, разработку стратегий защиты и планирование реагирования на инциденты.

Обучение персонала также играет ключевую роль в снижении риска кибератак. Учитывая, что многие кибератаки основываются на социальной инженерии [5], например, фишинге, осведомленность сотрудников о основах кибербезопасности может значительно снизить вероятность успешного проникновения злоумышленников.

Кроме того, страхование от киберрисков представляет собой еще один эффективный метод смягчения потенциальных финансовых потерь от кибератак. Пакеты киберстрахования могут покрывать разнообразные виды потерь, включая потерю данных, затраты на восстановление после атаки и репутационный ущерб.

Пример использования этих подходов можно увидеть на примере компании «Target», пострадавшей от масштабной кибератаки в 2013 году. В ответ на это, «Target» внедрила ряд мер для улучшения своей кибербезопасности, включая обучение своего персонала и применение стандартов кибербезопасности [6]. Это помогло снизить риск повторных атак и минимизировать потенциальные экономические потери [7].

Заключение. В современном мире, где все больше и больше организаций и индивидуальных пользователей становятся целями кибератак, важность понимания и минимизации экономических потерь от таких атак становится все более актуальной. В этой статье мы рассмотрели различные методы оценки и минимизации экономических потерь от кибератак.

Мы обсудили различные методы оценки экономических потерь, включая прямые и косвенные затраты, а также методы оценки репутационных потерь. Мы также рассмотрели примеры применения этих методов на практике, включая случай кибератаки на компанию Target.

В области минимизации потерь мы рассмотрели различные стратегии, включая применение мер безопасности, обучение персонала, использование страхования от киберрисков и разработку планов восстановления после киберинцидентов. Мы также обсудили пример распределенной системы, которая может помочь в минимизации потерь от кибератак.

В заключение, хотя кибератаки и представляют собой серьезную угрозу для организаций всех размеров, существуют эффективные методы оценки и минимизации экономических потерь от этих атак. Понимание и применение этих методов может помочь организациям лучше защитить себя и свои активы в цифровой эпохе.

СПИСОК ЛИТЕРАТУРЫ

1. Бердюгин А. А. Разработка алгоритма оценки риска воздействия кибератак в условиях электронного банкинга // Безопасность информационных технологий. 2019. Vol. 26, № 2.
2. Дьяченко Н. В., Отакулов А. С., Акушуев Р. Т. Особенности кибератак и их свойства // E-Scio. 2019. № 7 (34).
3. Шарыпова Т. Н., Калюжная А. Н. Проблема определения ущерба в результате кибератаки // Аллея науки. 2019. Vol. 4, № 1 (28).
4. Борхаленко В. А. Механизмы страхования в управлении рисками информационной безопасности // Экономический Анализ: Теория и Практика. 2017. Vol. 16, № 2 (461).
5. Сиротский А. А. Анализ технологий социальной инженерии как потенциальной угрозы информационной и экономической безопасности в социальной сфере // Материалы Международной Научно-Технической Конференции «Системы Безопасности». 2015. № 24.
6. Хасселл Д. Почему компании нужны и CIO, и CISO // Директор Информационной Службы. 2014. № 12.
7. Советов Б. Я., Колбанёв М. О., Татарникова Т. М. Оценка вероятности эрланговского старения информации // Информационно-управляющие системы. 2013. № 6 (67). С. 25-28.

УДК 004.056.53

СПОСОБ ОБНАРУЖЕНИЯ АТАКИ НА УСТРОЙСТВА ИНТЕРНЕТА ВЕЩЕЙ

Швайко Александр Сергеевич
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, Санкт-Петербург, 190121, Россия
e-mail: sasha.shvayko2002@gmail.com

Аннотация. Для сенсорных устройств интернета вещей не всегда подходят те же самые технологии защиты данных, применяемые в проводных сетях связи. Рассматривается способ обнаружения атаки на устройства интернета вещей по аномалии – средствами анализа трафика, несущего угрозу. Способ заключается в выделении из трафика, генерируемого сенсорными устройствами интернета вещей случайной составляющей, оставшиеся после исключения основных характеристик и в которой может содержаться аномалия. Программная реализация предложенной методики может стать частью системы обнаружения вторжений для сетей интернета вещей.

Ключевые слова: сенсорные сети; аномальный трафик; безопасность данных; анализ трафика; обнаружение аномалий.

METHOD FOR DETECTING ATTACKS ON INTERNET OF THINGS DEVICES

Shvayko Aleksander
Saint Petersburg State University of Aerospace Instrumentation
67, Bolshaya Morskaya St, St. Petersburg, 190121 Russia
e-mail: sasha.shvayko2002@gmail.com

Abstract. The same data protection technologies used in wired communication networks are not always suitable for IoT sensor devices. A method for detecting an attack on Internet of Things devices based on an anomaly is considered - by means of analyzing traffic that poses a threat. The method consists in isolating from the traffic generated by sensor devices of the Internet of things a random component that remains after excluding the main characteristics and which may contain

an anomaly. A software implementation of the proposed technique can become part of an intrusion detection system for Internet of Things networks.

Keywords: sensor networks; anomalous traffic; data security; traffic analysis; anomaly detection.

Введение. Развитие технологий построения измерительных систем на основе интернета вещей (Internet of Things, IoT) является трендом современных инфокоммуникационных сетей.

Устройства IoT, как правило используют батареи в качестве источника питания, обладают низкой вычислительной мощностью, ограниченным объемом памяти [1]. Эти ограничения обусловили разработку протоколов, обеспечивающих передачу и обработку данных с минимальной вычислительной и коммуникационной нагрузкой, что делает устройства интернета вещей уязвимыми к аномальному трафику – различным атакам, реализация которых может нанести серьезный ущерб эксплуатируемому оборудованию IoT и даже физический ущерб людям [2].

Известно, что системы обнаружения вторжений (Intrusion Detection System, IDS) не увеличивают нагрузку на сенсорные устройства и поэтому могут быть использованы для своевременного обнаружение аномального трафика, генерируемого интернетом вещей [3].

IDS для IoT представляет собой программное обеспечение, которое позволяет выявить несанкционированное получение доступа или вредоносную атаку на данные и оповестить о нарушении безопасности. Методы, используемые в системах обнаружения вторжения, относятся к активным и реализуют [4]:

– поиск по сигнатуре;
– поиск по аномалии.

Поиск по сигнатуре – способ, позволяющий определить атаку по некоторому шаблону, составленному по признакам известных на данное время атак. При совпадении признаков трафика и одного из шаблонов создается оповещение о нарушении безопасности. Такой метод позволяет определять только те вторжения, которые были ранее.

Поиск по аномалии – способ, при котором система сравнивает активность трафика с некоторой моделью стандартного (корректного) поведения того или иного устройства. При отклонении от нормы система также оповестит о нарушении безопасности.

Исходя из скорости развития информационных технологий в целом и отрасли интернета вещей в частности, есть проблема быстрого устаревания систем обнаружения вторжения. IDS нуждаются в постоянных доработках и обновлениях, чтобы корректно реагировать на появление новых угроз, что в свою очередь требует больших временных и финансовых затрат.

В работе предлагается интеграция метода машинного обучения на основе самообучаемой нейронной сети в анализ трафика, генерируемого интернетом вещей. Самообучаемая нейросеть способна самостоятельно адаптироваться к обновляемой среде и оставаться актуальной на протяжении длительного времени.

Структура сети IoT. Взаимодействие Machine-to-Machine (M2M) является основой интернета вещей и подключения новых устройств в единую сеть [5]. Организация M2M взаимодействия основано на протоколе CoAP (Constrained Application Protocol). Этот протокол разработан специально для маломощных устройств, совместим с HTTP (HyperText Transfer Protocol) и реализует передачу данных с минимальными энергозатратами такими, как они есть – без модификаций и инкапсулирования [6].

Протокол CoAP является бинарным и работает поверх UDP (User Datagram Protocol – протокол пользовательских датаграмм), что позволяет работать с любым типом данных. Передача данных происходит эффективнее, так как бинарный код подразумевает короткие и маловесные пакеты – уменьшается объем, требуемый для передачи данных и появляется гибкость при работе с различными устройствами.

В общем случае, взаимодействие клиента с умным устройством интернета вещей выглядит, как на рис. 1, где подразумевается, что пакеты данных с сенсорного устройства проходят через прокси-сервер, где инкапсулируются в HTTP-пакеты.

Протокол CoAP не поддерживает режим шифрования, предусмотренный в протоколе TCP (Transmission Control Protocol – протокол управления передачей), а поддерживает более упрощенный вариант шифрования DTLS (Datagram Transport Layer Security – протокол датаграмм безопасности транспортного уровня).

Протокол DTLS может работать в одном из четырех режимов:

– NoSec – в этом режиме шифрование отключено;
– PreSharedKey – шифрование включено, добавляется список общих ключей шифрования AES (Advanced Encryption Standard – симметричный алгоритм блочного шифрования) и узлов, между которыми ведется конфиденциальный обмен данными;
– RawPublicKey – шифрование включено, используются асимметричные пары ключей с шифрованием по алгоритму AES;
– Сертификат – шифрование включено, устройство использует сертификаты X.509 с цифровыми подписями для распределения открытых ключей.

Методика анализа трафика. Модель трафика представляет собой закономерность изменения его основных характеристик во времени. В описании трафика обычно учитываются три характеристики [7]:

– тренд – описание поведения трафика во времени;

– сезонность – закономерность роста или падения объема трафика, связанных, например, с конкретным промежутком времени;

– случайная составляющая – остальные характеристики, оставшиеся после исключения основных характеристик, собственно, в которых и следует искать аномалии.

После выбора способа анализа, необходимо трафик разложить на составляющие:

– выделить тренд и сгладить исходные данные, например, при помощи скользящего окна, экспоненциального сглаживания или регрессии;

– вычесть или разделить сезонную составляющую из исходных данных, что зависит от выбранного способа;

– после удаления сезонного фактора и тренда остается случайная составляющая, которая и принимается за аномалию.

Примерами аномалий могут быть выбросы, сдвиги, изменения распределения значений, отклонения от среднего и совместные аномалии.

В качестве примера можно рассмотреть анализ трафика, основанный на циклическом алгоритме, состоящий из:

– отбора данных;
– сглаживания тренда;
– поиска возможных циклов;
– удаления трендовых компонент;
– проверки циклов;
– предсказания будущих циклов.

На этапе отбора данных определяется анализируемый временной ряд X_q (рис. 1). На рис. 1 изображен временной ряд, где по оси ординат отложен объем трафика V, а по оси абсцисс – период наблюдения T. Для дальнейшего анализа, временная шкала дискретизируется равными интервалами Δt наблюдения динамики изменения объема трафика.

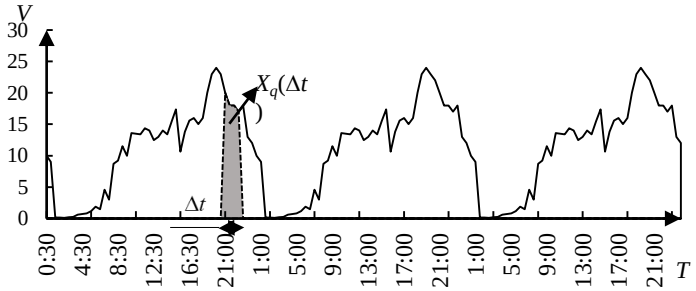


Рис. 1. Временной ряд трафика

Каждый интервал Δt содержит агрегацию данных, объем которых зафиксирован в этом интервале

$$X_q(\Delta t) = \sum_{j=1}^{R} V_j$$

где q – номер интервала (q = 1, 2, …, Q);

R – число пакетов в интервале Δt;

X_q – ряд данных.

Для сглаживания необходимо исключить одиночные выбросы – (L – 1) точку. Применяя, например, метод краткосрочной центрированной скользящей средней осуществляется переход к новому сглаженному ряду X_k , длина которого равна $N = Q - (L-1),\ k = \overline{1, N}.$

$$X_k = \frac{1}{L} \sum_{j=k}^{k+L-1} X_j .$$

После удаления случайных колебаний и выравнивания значений переходят к поиску циклов. Здесь применяется метод спектрального анализа. На графике спектра мощности (рис. 2) видны пики, образующиеся возле определенных частот. Пики указывают на возможные циклы.

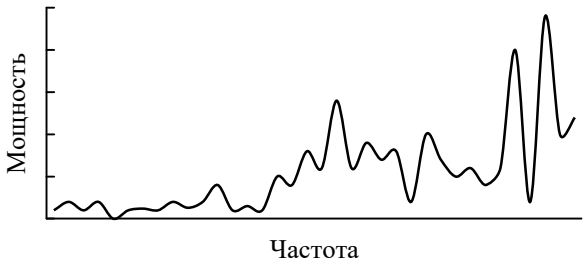


Рис. 2. Спектр мощности

Пики свидетельствует только о вероятности наличия циклов. Поэтому проводят еще несколько шагов для проверки наличия циклов. Одним из таких критериев является удаление трендовых компонентов. Применяя метод скользящей средней, удаляются силы роста в данных, а затем исходя из статистической значимости методами *F*-коэффициентов или хи-квадрат ищется отклонение от распределения спектра мощности.

Архитектура IDS интернета вещей. IDS для интернета вещей, имеет иерархическую структуру, как и сама сеть IoT – три компонентных уровня. На нижнем уровне иерархии находятся кластерные беспроводные сенсорные сети [8]. Головной узел кластера отвечает за авторизацию других членов кластера, маршрутизатор отвечает за авторизацию головных узлов кластера, а шлюз за авторизацию маршрутизаторов.

Модуль обнаружения аномального поведения установлен в каждом кластере, интеллектуальная система обнаружения сетевых атак на маршрутизаторах и шлюзах.

IoT-устройства оповещают о своем присутствии в конкретном кластере, направляя идентификатор (ID), например MAC-адрес в модуль мобильности. Модуль мобильности отвечает за регистрацию вновь прибывших в кластер устройств и удаление вышедших из кластера устройств. Любой вновь прибывший узел проходит процедуру аутентификации [9].

Модуль синхронизации представляет собой тактовый генератор – формирование временных окон (слотов) и соответственно раундов беспроводной сенсорной сети, во время которых происходит опрос IoT-устройств.

Модуль обнаружения аномального поведения реализуется программно по приведенной в статье методике анализа трафика.

На уровне сети обнаружение атак реализуется программной моделью глубокого обучения, например, нейронной сетью или случайным лесом [10].

Модуль вычисления доверия позволяет в онлайн режиме удалять скомпрометированные узлы из списка доверенных узлов, на основании которого формируется таблица маршрутизации.

Заключение. Предложенная в статье методика анализа трафика с целью поиска аномалий, несущих атаку на устройства интернета вещей, является частью системы обнаружения вторжений и реализует свои функции на нижнем уровне архитектуры интернета вещей, то есть на уровне сенсорных устройств и кластеров беспроводной сенсорной сети.

Последовательность шагов методики направлена на выделение из трафика, генерируемого сенсорными устройствами интернета вещей случайной составляющей, оставшиеся после исключения основных характеристик, в которой может содержаться аномалия.

СПИСОК ЛИТЕРАТУРЫ

1. Wang C., Lin H., & Jiang H. CANS: Towards congestion-adaptive and small stretch emergency navigation with wireless sensor networks // IEEE Transactions on Mobile Computing. 2015. Vol. 15(5). P. 1077-1089.
2. Татарникова Т.М., Богданов П.Ю., Краева Е.В. Предложения по обеспечению безопасности системы умного дома, основанные на оценке потребляемых ресурсов // Проблемы информационной безопасности. Компьютерные системы. 2020. № 4. С. 88-94.
3. Baddar S.A.-H., Merlo A., Migliardi M. Anomaly Detection in Computer Networks: A State-of-the-Art Review // Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications. 2014. vol. 5. no. 4. P. 29–64.
4. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети. Сетевые аномалии. – М.: Горячая линия – Телеком, 2013. – 220 с.
5. Bogatyrev V.A., Bogatyrev A.V., Bogatyrev S.V. Redundant Servicing of a Flow of Heterogeneous Requests Critical to the Total Waiting Time During the Multi-path Passage of a Sequence of Info-Communication Nodes,» Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2020. Vol. 12563. P. 100-112.
6. Lee Perry. Internet of Things Architects. Packt Publishing, 2018. 514 p.
7. Сахаров Д. В., Козлов Д. С. Обнаружение аномального поведения устройства IoT в сети на основе модели трафика. 2018. С. 51-55.
8. Basford P. J., Johnston S. J., Perkins C. S., Garnock-Jones T., Tso F. P., Pezaros D., Cox S. J. Performance analysis of single board computer clusters. Future Generation Computer Systems. 2020. Vol. 102. P. 278-291.
9. Dziubenko I. N. and Tatarnikova T. M. Algorithm for Solving Optimal Sensor Devices Placement Problem in Areas with Natural Obstacles. 2018 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). 2018. P. 1-5. DOI: 10.1109/WECONF.2018.8604325.
10. Татарникова Т.М., Бимбетов Ф., Богданов П.Ю. Выявление аномалий сетевого трафика методом глубокого обучения // Известия СПбГЭТУ ЛЭТИ. 2021. №4. С. 36-41.

ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И ТЕХНОЛОГИИ

УДК 004.032.26

ПРИМЕНЕНИЕ СВЕРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ РАСПОЗНАВАНИЯ ОБЪЕКТОВ БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ

Авраменко Владимир Семенович, Чичков Евгений Сергеевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного,
Тихорецкий пр-т, д. 3, Санкт-Петербург, 194064, Россия
e-mails: vsavr@yandex.ru, jen.chichckow2014@yandex.ru

Аннотация. Проведен анализ проблемы обработки данных беспилотными летательными аппаратами. Предложен вариант решения задачи распознавания объектов на основе методов машинного обучения. Рассмотрены распространённые сверточные нейронные сети, их основные характеристики, проведен сравнительный анализ. Для реализации компьютерного зрения на борту малогабаритных БПЛА рассмотрена возможность применения сети MobileNet.

Ключевые слова: беспилотный летательный аппарат; обработка данных; распознавание объектов; машинное обучение; сверточная нейронная сеть; архитектура сети.

APPLICATION OF CONVOLUTIONAL NEURAL NETWORKS FOR OBJECT RECOGNITION BY UNMANNED AERIAL VEHICLES

Avramenko Vladimir, Chichkov Evgeny
Military Academy of Communications Marshal of the Soviet Union S.M. Budyonny
Tikhoretsky Ave., 3, St. Petersburg, 194064, Russia
e-mails: vsavr@yandex.ru, jen.chichckow2014@yandex.ru

Abstract. The analysis of the problem of data processing by unmanned aerial vehicles is carried out. A variant of solving the problem of object recognition based on machine learning methods is proposed. The widespread convolutional neural networks, their main characteristics are considered, a comparative analysis is carried out. To implement computer vision on board small-size UAVs, the possibility of using the MobileNet networks is considered.

Keywords: unmanned aerial vehicle; data processing; object recognition; machine learning; convolutional neural network; network architecture.

Введение. В настоящее время активно развиваются роботизированные системы в различных областях деятельности, с их помощью значительно повышается эффективность решения широкого спектра задач, зачастую ранее трудно выполнимых. Самостоятельная разработка и производство роботизированных систем является приоритетной задачей в ведущих странах.

Наиболее активно развиваются беспилотные летательные аппараты (БПЛА) как в гражданском коммерческом секторе, таки и в военной сфере. В последних военных конфликтах роль БПЛА резко повысилась.

Под беспилотным летательным аппаратом (БПЛА) понимается летательное средство, не имеющее на своем борту экипажа. Также используется более широкое понятие − беспилотная летательная система (БПЛС), которая включает в себя:

1)БПЛА;
2)средства управления БПЛА;
3)средства связи с БПЛА;
4)дополнительное оборудование.

Основные достоинства БПЛА по сравнению с пилотируемыми летательными аппаратами следующие:

1)Высокая маневренность;
2)Простота управления;
3)Простота производства;
4)Относительно невысокая стоимость;
5)Короткие сроки обучения операторов.

В настоящее время в большинстве случаев управление одним БПЛА или роем БПЛА осуществляют операторы. Под роем БПЛА понимается объединение БПЛА в группы (в «рой») для совместного выполнения одной или нескольких задач. Такой тип организации множества БПЛА имеет ряд преимуществ по сравнению с одиночными БПЛА, основными из которых является высокая живучесть, масштабируемость и скорость выполнения задачи.

Управление БПЛА может быть ручное, автоматизированное либо автоматическое (с использованием заранее разработанных алгоритмов действий). Третий способ является наиболее предпочтительным во многих сферах (нет необходимости в подготовке операторов, низкие требования к каналу прямой и обратной связи с наземным пунктом управления и т.д.).

Как для одиночных, так и для роев БПЛА перспективным является применение методов машинного обучения и для управления БПЛА и для выполнения заданных функций, что, в свою очередь, требует решения задачи обработки данных на борту БПЛА [1].

Под обработкой данных понимаются все этапы преобразования входных данных к конечному результату, а именно: очистка, редактирование, форматирование данных, вычислительные операции и т.п. Обработка данных в системах БПЛА может осуществляться «вручную» (человеком) и с помощью наземной и (или) бортовой ЭВМ.

В автономных одиночных БПЛА и, тем более, в роях БПЛА, в которых в режиме реального времени одни БПЛА для выполнения своих функций используют данные (результаты сбора и обработки) от других БПЛА, обработка данных на борту становится безальтернативной.

Вместе с тем реализация обработки данных на борту БПЛА во многих задачах требует вычислительного устройства достаточно высокой производительности, дополнительного энергоснабжения. Для малогабаритных БПЛА эта задача является проблемной, так как ее решение путем использования высокопроизводительных процессоров влечет за собой увеличение массогабаритных характеристик.

В свою очередь, для сохранения требуемых полетных характеристик (скорость, высота, продолжительность полета) может потребоваться модернизация или замена двигателей и других конструктивных элементов.

Также следует отметить, что возможность несанкционированного доступа злоумышленников к обрабатываемой и передаваемой информации, методам и алгоритмам ее обработки с целью нарушения конфиденциальности, доступности и целостности информации требует дополнительных мер защиты.

Таким образом, возникает необходимость использования в малогабаритных БПЛА компактных экономичных вычислителей, средств математического, информационного и программного обеспечения, обеспечивающих обработку данных с требуемыми значения показателей качества и минимальными вычислительными затратами.

Одной из самых распространённых задач во многих областях применения БПЛА является задача обнаружения и распознавания (классификации) объектов различного рода (компьютерное зрение).

В настоящее время в основном эту задачу решает оператор БПЛА путем анализа видеоданных или фотографий на мониторе. Применение методов машинного обучения для решения этой задачи может существенно повысить оперативность и точность распознавания.

Для решения задач обнаружения и классификации объектов были разработаны сверточные нейронные сети (Convolution neural network, CNN). Для реализации компьютерного зрения на борту БПЛА важным становятся показатели ресурсоемкости CNN (вычислительных затрат на решение задачи распознавания, объема памяти для хранения программного обеспечения и данных, и т.д.).

Характеристики точности распознавания и ресурсоёмкости для распространенных CNN, полученные на основе анализа [2], представлены в таблице 1.

Таблица 1

Сравнение различных архитектур сверточных нейронных сетей

Название CNN	Top-1 Accuracy, % (Точность)	Количество параметров, млн	MAC, млн	Количество памяти, занимаемое на диске, Мбайт
VGG	~71	~140	30,6 – 39,2	~ 530
ResNet	~75-78	~25-60	~22,6	~ 100 – 230
Xception	~79	~30	33,48	~ 88
MobileNet	~71	~3,5-4,3	>14	~ 14 – 16

Сравнение представленных в таблице №1 CNN по показателю точности Top-1 Accuracy и показателю ресурсоёмкости MAC представлены на рис. 1.

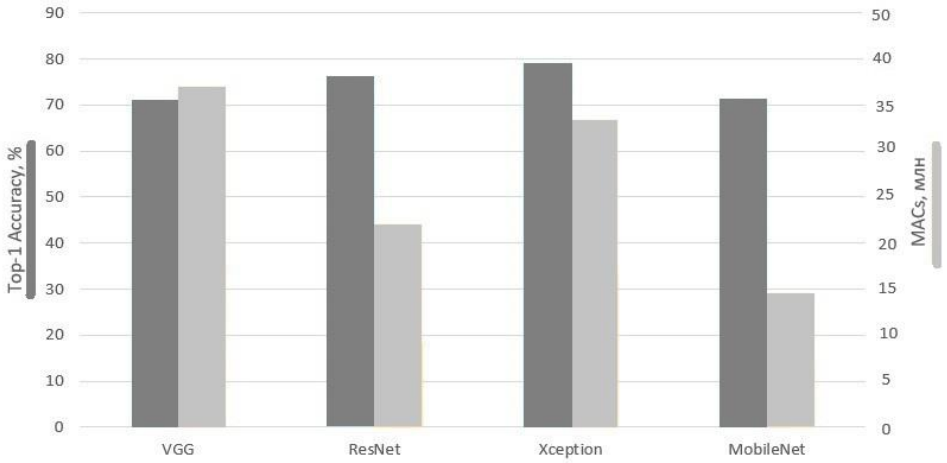


Рис. 1. Сравнение различных архитектур сверточных нейронных сетей

Для расчёта показателя эффективности $Y_{эф}$ сверточной нейронной предлагается использовать следующее выражение:

$Y_{эф} = \frac{A}{MAC}$,

где: A - Top-1 Accuracy;

MAC - количество операций сложения и накопления (млн. операций).

Сравнение CNN в графическом виде по результатам расчетов $Y_{эф}$ представлены на рис. 2. Очевидно, что наиболее эффективной по соотношению точности к вычислительным затратам является сеть MobileNet.

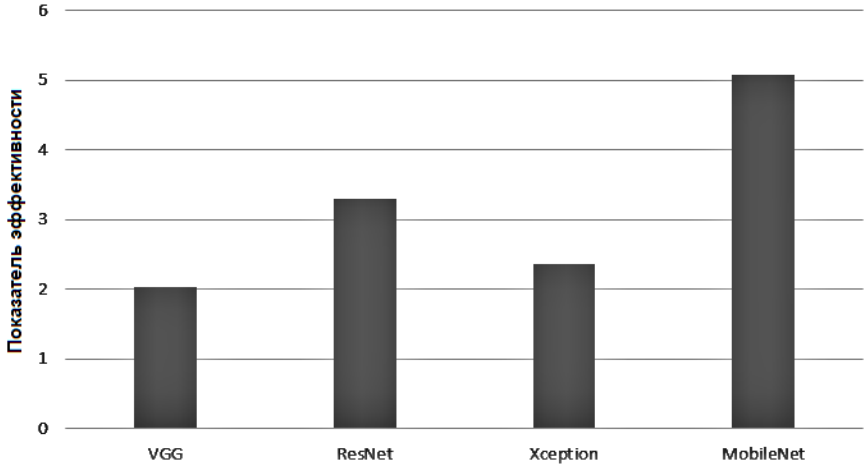


Рис. 2. Сравнение показателей эффективности для различных архитектур сверточных нейронных сетей

Архитектура сети MobileNet была разработана компанией Google [3]. Особая структура ее свертки позволяет значительно сократить объем вычислений и количество параметров. Скорость и количество потребляемой памяти пропорциональны количеству операций MAC (multiply-accumulate, умножение-накопление). MAC является мерой количества объединенных операций умножения и накопления [4].

Так, в MobileNet применяется разделимая по глубине свертка (Depthwise Separable Convolution, DSC). DSC подразумевает под собой разложение полной операции свертки на два шага, а именно на глубинную свертку (Depthwise Convolution, DWC) и точечную свертку (Pointwise Convolution, PWC) [3] (Рис. 3 и 4).

Обычная свертка представляет из себя фильтр с размерами $D_k \times D_k \times C_{in}$, где D_k — это размер ядра свёртки, а C_{in} — количество каналов, подаваемых на вход. Общая вычислительная сложность данного сверточного слоя составляет $D_k \times D_k \times C_{in} \times D_f \times D_f \times C_{out}$, где D_f — это высота и ширина слоя (пространственные размеры входного и выходного тензоров совпадают), а C_{out} — число каналов на выходе.

Идея DSC состоит в том, чтобы разложить подобный слой на depthwise-свертку, которая представляет из себя поканальный фильтр, и свёртку 1×1, называемую pointwise convolution. Суммарное количество операций необходимых для применения такого слоя равно $(D_k \times D_k + C_{out}) \times D_f \times D_f \times C_{in}$.

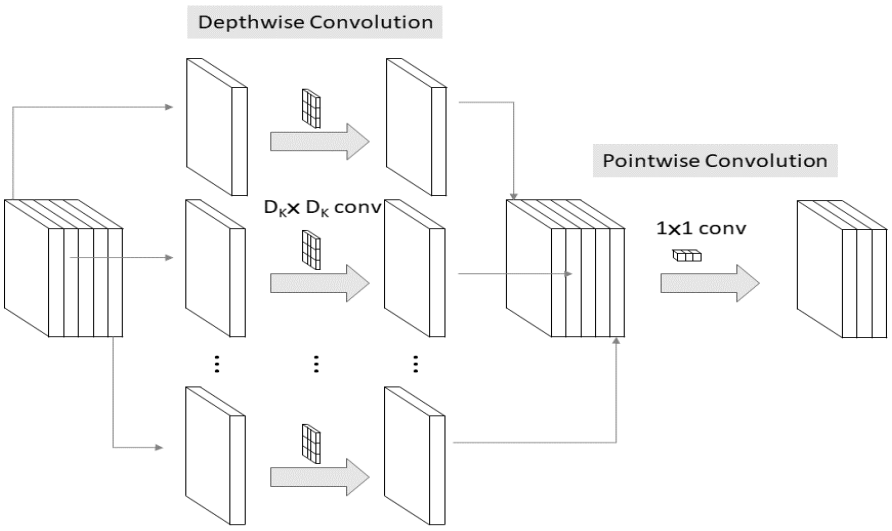


Рис. 3. Схематическое изображение глубокой разделимой свертки Depthwise Separable Convolution

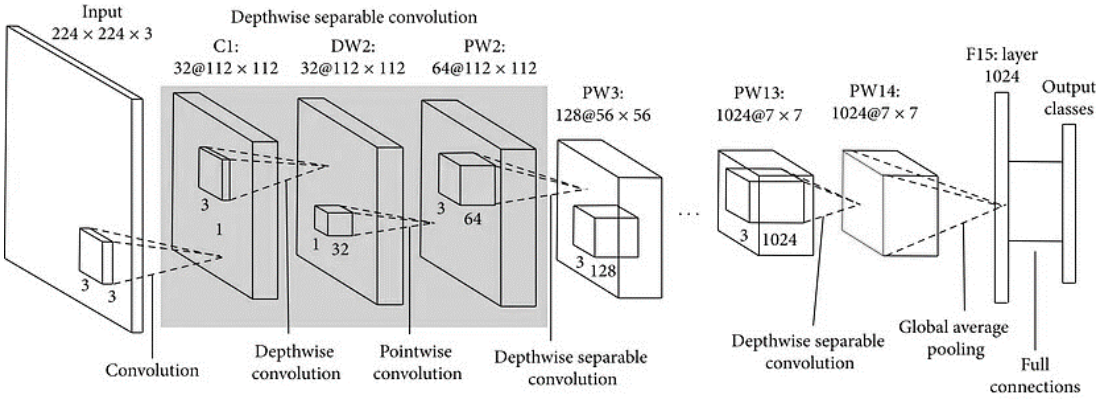


Рис. 4. Графическое представление архитектуры сверточной нейронной сети MobileNet

Для настройки сверточной сети MobileNet предусмотрен множитель ширины α, отвечающий за количество каналов в каждом слое, и множитель разрешения ρ, отвечающий за пространственные размеры входных тензоров. Оба множителя позволяют варьировать размерами сети, например, если α = 0.25, то в 4 раза уменьшается число каналов на входе каждого блока, при ρ = 0.5 высота и ширина входных карт признаков, подаваемых на вход каждому слою, будет уменьшена вдвое. С изменением α и ρ происходит изменение точности сети, в то же время эти настройки влияют на скорость работы и объем потребляемой памяти.

Вариант постановки задачи разработки модели системы распознавания объектов для малогабаритных БПЛА на основе сверточной сети MobileNet для заданного бортового вычислителя БПЛА можно сформулировать, как задачу нахождения оптимальных значений параметров сети, минимизирующих количество операций MAC при выполнении заданных требований по точности и оперативности распознавания. Такой подход обеспечивает максимальное сохранение летных и других характеристик, снизить требования к аппаратной части при разработке новых БПЛА. В зависимости от целевого назначения БПЛА возможны другие формулировки постановок задач.

Следует заметить, что при использовании методов машинного обучения большие вычислительные мощности требуются на этапе обучения, но этот этап может выполняться «на земле», например, на мобильном центре обработки данных [5]. А бортовая ЭВМ БПЛА может реализовать только задачу распознавания, не требующей существенных вычислительных ресурсов.

Одним из примеров использования технологий машинного обучения на борту БПЛА является тяжелый ударный беспилотник С-70 «Охотник». Данный аппарат способен выполнять вычисления на борту благодаря сопроцессору с элементами VLIW (Very long instruction word) и SIMD (single instruction, multiple data) архитектур [6]. Однако, С-70 «Охотник» имеет массу порядка 20 тонн, и проблема размещения вычислительного комплекса для обработки данных на борту для него не так актуальна, как для небольших БПЛА массой до 5 кг.

Заключение. Таким образом, одним из путей оперативного решения проблемы обработки данных на борту в отечественных БПЛА является разработка моделей машинного обучения на основе искусственных нейронных сетей, предназначенных для реализации на существующих отечественных и доступных зарубежных процессорах.

В частности, для решения задачи распознавания образов на борту малогабаритных БПЛА может быть использована сверточная нейронная сеть архитектуры MobileNet, адаптированная под возможности доступных аппаратных средств. Перспективным направлением развития технологий обработки данных в отечественной беспилотной авиации является создание отечественной конкурентоспособной специализированной аппаратно-программной платформы для реализации машинного обучения в малогабаритных беспилотных летательных аппаратах. В целом, развитие автоматизированных и автоматических систем управления и обработки данных на основе технологий машинного обучения в области БПЛА является многообещающим направлением повышения эффективности их применения в различных сферах деятельности.

СПИСОК ЛИТЕРАТУРЫ

1. Авраменко. В.С. Чичков Е.С. Анализ проблемы обработки данных беспилотными летательными аппаратами на основе методов машинного обучения // В сборнике: Информационная безопасность телекоммуникационных сетей. Материалы XIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2023)» 2023. С 115-117.
2. Keras Applications. [Электронный ресурс] URL:https://keras.io//api/applications (Дата обращения 02.11.2023)
3. A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, H. Adam. MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications. [Электронный ресурс] URL: https://mobilenets-efficient-convolutional-neural-networks-for-mobile-vision-applications.
4. Jiho Chang, Yoonsung Choi, Taegyoung Lee, Junhee Cho. Reducing Mac operation in convolutional neural network with sign prediction. [Электронный ресурс] URL: https://www.semanticscholar.org/org/paper/reducing-mac-operation-in-convolutional-neural-network-with-sign-prediction.
5. Михайличенко А.В. Паращук И.Б. Анализ надежности мобильных центров обработки данных: проблемы и перспективы. Перспективные направления развития отечественных информационных технологий. Материалы VIII межрегиональной научно-практической конференции. Севастопольский государственный университет. Севастополь 2022. С 66-68.
6. В России впервые показали ударный беспилотник «Охотник» с плоским соплом // Информационное агенство ТАСС [Электронный ресурс] URL:https://tass.ru/armiya-i-opk/13191513 (Дата обращения 09.06.2023).

УДК 004.056.5

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ЗАЩИТЫ ОТ PHISHING-АТАК

Бобрышов Данил Павлович, Зацепин Илья Сергеевич, Чуваев Константин Игоревич
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, лит. А, Санкт-Петербург, 190000, Россия
e-mail: danil.bobryshov@mail.ru, xiluhax@gmail.com, wizeer66@gmail.com

Аннотация. Данная статья посвящена изучению применения технологий машинного обучения и искусственного интеллекта для защиты от phishing-атак в сети Интернет. В статье рассматриваются различные подходы и методы, которые используются для защиты от несанкционированного взлома устройства, проведен анализ существующих методов обнаружения и предотвращения атак. Рассматриваются возможности использования алгоритмов технологий машинного обучения «с учителем» как способ повышения эффективности фильтров и систем анализа электронных сообщений для выявления вредоносной активности методы проверки подлинности электронного письма SPF и DKIM.

Ключевые слова: DKIM; phishing; домен; искусственный интеллект; машинное обучение.

APPLICATION OF MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE TECHNOLOGIES TO PROTECT AGAINST PHISHING ATTACKS

Bobryshov Danil, Zacepin Ilya, Chuvaev Konstantin
Saint Petersburg State University of Aerospace Instrumentation
67 Bolshaya Morskaya St., lit. A, St. Petersburg, 190000, Russia
e-mail: danil.bobryshov@mail.ru, xiluhax@gmail.com, wizeer66@gmail.com

Abstract. This article is devoted to the study of the use of machine learning and artificial intelligence technologies to protect against phishing attacks on the Internet. The article discusses various approaches and methods that are used to protect against unauthorized hacking of the device, the analysis of existing methods for detecting and preventing attacks. The possibilities of using algorithms of machine learning technologies «with a teacher» as a way to increase the effectiveness of filters and systems for analyzing electronic messages to detect malicious activity are considered. The methods of verifying the authenticity of an email are SPF and DKIM.

Keywords: DKIM; phishing; domain; artificial intelligence; machine learning.

Введение. При использовании электронных писем, социальных сетей и других онлайн-платформ, существует повышенный риск попасть под атаку phishing, которая может привести к утечке личных данных или вредоносному программному обеспечению на устройстве пользователя. Phishing-атаки являются одним из самых распространенных и опасных видов атак цифрового пространства. Они представляют собой мошеннические

попытки получить доступ к конфиденциальной информации через электронную почту, путем использования поддельных сообщений, похожих на оригинальные [1]. Хакеры отправляют подделанные электронные письма, которые выглядят как оригинальные сообщения от проверенных источников, таких как банки, социальные сети или онлайн-магазины. В таких письмах может быть содержимое, написанное с использованием официальных логотипов и дизайна компаний, что заставляет пользователя думать, что происходит взаимодействие с подлинными представителями данной организации. Обычно подобные письма предлагают клиентам выполнить какое-то действие, например, обновить свои данные или пароль, нажав на ссылку, перейдя по которой можно попасть на поддельный сайт, используя который злоумышленники взламывают устройства пользователей. В результате, хакеры могут получить доступ к личной информации жертвы, логину, паролю или банковскому счету, а иногда и интеллектуальной собственности. На рис. 1 изображён график попыток проведения несанкционированного взлома устройств.

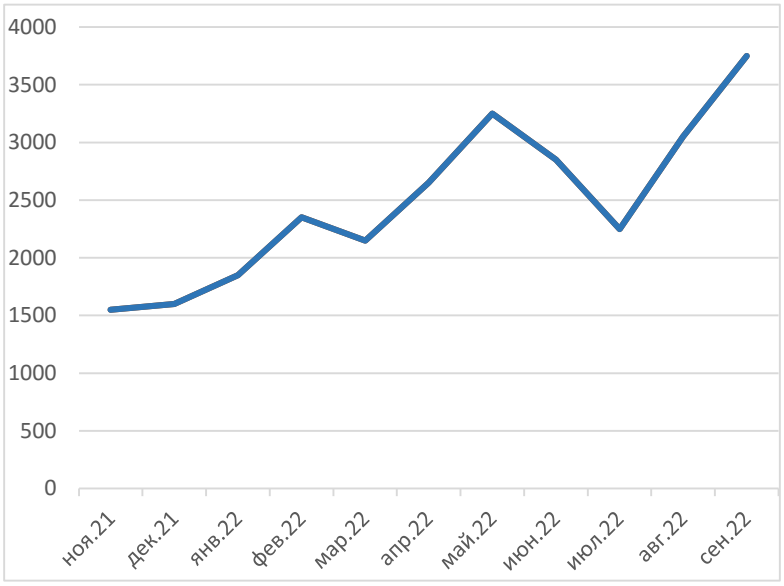


Рис. 1. Попытки Phishing-атак в России, октябрь 2021 г. — сентябрь 2022 г.

Методы защиты информационных систем от несанкционированного доступа. Существует много методов защиты от данного вида взлома. Например, для защиты своих устройств пользователи могут установить программное обеспечение, содержащее разные способы сохранения безопасности данных. Применяются различные методы анализа данных, основанные на технологиях машинного обучения и искусственного интеллекта [2-7]. Кроме того, используются технологии аутентификации отправителя, которые позволяют проверять подлинность письма посредством проверки цифровой подписи SPF (Sender Policy Framework) и DKIM (DomainKeys Identified Mail).

SPF — это метод проверки подлинности отправителя электронной почты. SPF использует часть идентификационного имени отправителя электронной почты — домена, чтобы проверить, действительно ли отправитель имеет разрешение на отправку сообщения от данного адресанта.

При получении сообщения, сервер получателя выполняет проверку, в ходе которой извлекается домен отправителя электронной почты из заголовка сообщения и выполняет проверка адресанта, в целях получения его адреса. Затем проводится проверка, является ли IP-адрес отправителя доверенным, и принимает решение о блокировке или доставке сообщения. Если адрес IP отправителя не совпадает с доменом-отправителем, то письмо не проходит аутентификацию и может быть помечено как спам. SPF запись добавляется в DNS-запись домена и содержит список допустимых IP-адресов, которые могут отправлять сообщения от этого домена. Это уменьшает вероятность спама и phishing-атак, поскольку злоумышленники не могут использовать домен для отправки поддельных сообщений, если они не имеют доступа к корректным IP-адресам. SPF является стандартной технологией, принятой как часть международных стандартов почтовой аутентификации. Использование данной технологии уменьшает риски подделки электронной почты и снижает количество спама. Среди приложений, использующих данный метод проверки, можно выделить:

1. Gmail — сервис электронной почты от Google;
2. Microsoft 365 — веб-сервис, включающий в себя электронную почту и облачное хранилище;
3. Amazon SES — сервис электронной почты, предоставляемый Amazon Web Services.

DKIM — это метод проверки подлинности отправителя электронной почты, который основывается на цифровой подписи. DKIM позволяет установить, действительно ли сообщение было отправлено от имени подлинного отправителя, а не было подделано или изменено в процессе передачи. Метод работает таким образом,

что отправитель электронной почты использует ключ шифрования для создания цифровой подписи, которая закодирована и встроена в электронное сообщение. При получении сообщения сервер получателя использует открытый ключ отправителя, чтобы расшифровать подпись и проверить, что сообщение действительно было отправлено отправителем, указанным в заголовке сообщения.

Для работы DKIM, отправитель настраивает запрос на разрешение доменного имени для своего домена, которая содержит открытый ключ шифрования. Когда получатель получает сообщение от данного домена, он извлекает открытый ключ из обратного запроса домена и использует его для проверки цифровой подписи, которая встроена в сообщение. DKIM является эффективным методом защиты от спама и phishing, так как мошенники не могут использовать ключ отправителя, чтобы создать правдоподобную цифровую подпись для своих сообщений. Проверка цифровой подписи DKIM помогает улучшить безопасность электронной переписки. На рис. 2 изображен процесс проверки письма с помощью метода DKIM.

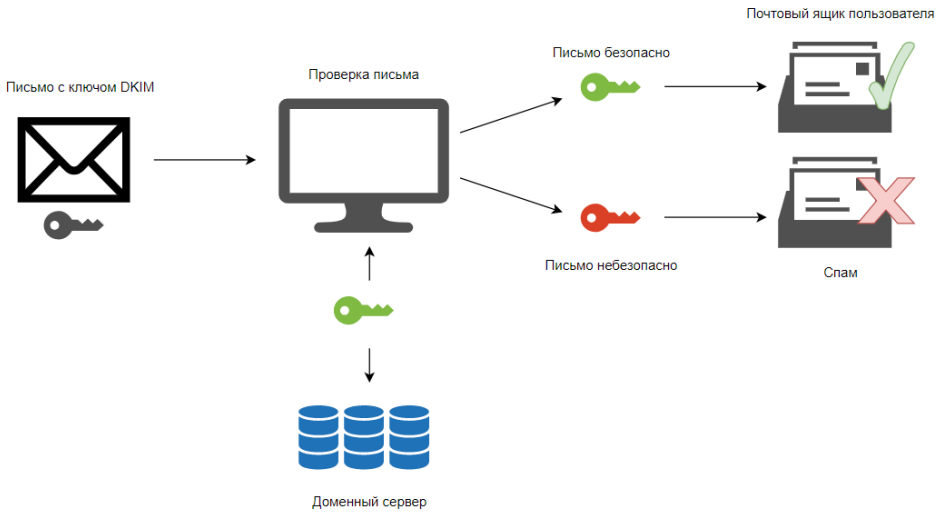


Рис. 2. Процесс работы метода DKIM

Наиболее популярных приложений и сервисы, использующие технологию DKIM:

1. Gmail — сервис электронной почты от Google;
2. Microsoft 365 — веб-сервис, включающий в себя электронную почту и облачное хранилище;
3. Amazon SES — сервис электронной почты, предоставляемый Amazon Web Services;
4. MailChimp — онлайн-сервис для отправки электронных рассылок;
5. Yahoo Mail — бесплатный сервис электронной почты.

Один из подходов, используемых для борьбы с phishing — это использование алгоритмов машинного обучения на основе обучения «с учителем». Этот метод основан на обучении алгоритма предсказывать, является ли сообщение phishing или нет, используя проверки содержания письма, домена отправителя и другие сходства с предыдущими phishing сообщениями. Для этого система использует большую базу данных, содержащую как безопасные, так и злонамеренные электронные сообщения. Эти данные используются для обучения системы, так что она может самостоятельно идентифицировать и классифицировать сообщения, сходные со входными данными. Алгоритм обучается на данных, и затем тестируется на новых, неизвестных письмах. Этот метод может быть достаточно точным, но требует большого количества данных и времени для обучения. При классификации сообщений система анализирует многие аспекты сообщения, включая заголовок, текст, вложения, язык, стиль и другие характеристики. С помощью этого анализа система строит модели, тем самым улучшая точность распознавания нежелательных сообщений и уменьшая количество ложноположительных срабатываний. Одним из преимуществ этой технологии является ее способность к обучению на основе получаемых обратных связей. Если система неправильно классифицирует сообщение, пользователь может пометить его как нежелательное, а система автоматически обновит свои данные и подкорректирует алгоритм работы. Технология обучения «с учителем» может быть использована для автоматического обнаружения и блокировки вредоносных сообщений в реальном времени, что делает его важным элементом безопасности для организаций и пользователей, которые регулярно обрабатывают множество электронной почты.

Для более простых систем, используется метод «bag-of-words», который анализирует частоту слов и фраз в сообщениях, чтобы определить, является ли сообщение вредоносным или нет. Данный подход использует методы обработки естественного языка, что позволяет извлекать из письма наиболее значимые слова и фразы, которые могут свидетельствовать о phishing атаке. Суть этого метода состоит в следующем: вся входящая информация,

например, текст сообщения, разбивается на отдельные слова, которые затем сортируются в алфавитном порядке и представляются в виде вектора чисел, где каждому слову соответствует свой код или индекс в алфавите словаря. Затем этот вектор обрабатывается специальными алгоритмами машинного обучения, которые определяют, является ли сообщение вредоносным. Важным преимуществом метода «мешок слов» является его универсальность — он может применяться для анализа любых текстовых данных, начиная от электронных писем и заканчивая новостными статьями, сообщениями в социальных сетях и т.д. Кроме того, благодаря накопленной базе данных, которая содержит информацию о ранее выявленных вредоносных сообщениях, алгоритмы машинного обучения могут непрерывно совершенствоваться и становиться все более точными и эффективными в борьбе с новыми видами угроз. Этот метод считается менее точным, чем первый подход, но может быть использован для рассмотрения сообщений, которые не были размечены с целью обучения модели, а также для обработки текстов на естественном языке на различных языках.

Байесовские классификаторы — это метод классификации данных, основанный на теореме Байеса. Он используется для определения вероятности принадлежности объектов к определенному классу на основе характеристик этих объектов. Байесовские классификаторы могут быть использованы для борьбы с phishing-атаками, анализируя содержание электронных сообщений, обнаруживая характеристики этого сообщения и ассоциируя соответствующую вероятность возможности phishing-атаки. Например, наивный байесовский алгоритм, который основывается на предположении, что каждый признак сообщения вносит свой независимый вклад в вероятность phishing атаки. Алгоритм сначала обучается на известных наборах электронных сообщений, размеченных как спам и корректные сообщения. Затем на основе этого обучения, наивный байесовский алгоритм классифицирует новые электронные сообщения на основе вероятности phishing атаки. Примерами признаков могут быть содержание сообщения, ключевые фарузы или метаданные сообщения. На основе этих признаков алгоритм определяет вероятность того, что данное электронное сообщение является phishing атакой. Байесовские классификаторы могут быть использованы как самостоятельное средство борьбы с phishing-атаками или в сочетании с другими методами. Преимущество классификаторов в их высокой скорости работы и отсутствия необходимости в большой вычислительной мощности системы.

Random Forest — это метод машинного обучения, который используется для классификации данных. Алгоритм основывается на анализе множества решений, принятых деревом решений, и создает ансамбль из множества других деревьев решений с целью уменьшения возможных ошибок. В борьбе с phishing -атаками, Random Forest может использоваться для автоматической классификации электронных писем под категорию писем злоумышленников и обычных, проверенных сообщения. Алгоритм обучения на основе Random Forest будет определять, насколько происходящее в электронном сообщении соответствует традиционным приемам phishing: указание на несуществующий счет в банке, запрос личной информации, поиск подтверждения учетной записи. Random Forest может быть настроен на распознавание определенных фраз в электронных письмах, наличие скрытых ссылок на поддельные веб-страницы или маскировку URL-адреса для перехода на несуществующий сайт. Классификация электронных сообщений может стать надежным средством борьбы с phishing-атаками, прежде чем они достигнут обычных пользователей.

Deep Learning — это вид машинного обучения, который использует искусственные нейронные сети для извлечения признаков из сложно структурированных данных. Данный метод может быть использован для борьбы с phishing-атаками путем обнаружения и классификации поддельных электронных сообщений. Для обнаружения phishing-атак, Deep Learning может быть использован при анализе текстового содержания электронных сообщений в поиске ключевых слов и фраз, а также для определения наличия в этих сообщениях вредоносных ссылок. Подобный метод близок к работе антивирусов, которые используют методы распознавания печатной речи для обнаружения вирусов. Deep Learning также может быть использован для анализа структуры электронных сообщений, например, для определения адресанта сообщения или наличия поддельных заголовков. Этот подход основан на анализе большого количества данных, которые могут быть собраны из электронных сообщений, получаемых от различных отправителей. Использование Deep Learning для борьбы с phishing-атаками может быть очень эффективным, ввиду возможности метода обработки больших объемов данных, а также функции обнаружения новых тенденций в атаках при обучении на ранее неизвестных типах атак. Deep Learning может обнаружить и устранить различные типы phishing-атак, повышая уровень защиты от несанкционированных атак.

Технологии искусственного интеллекта также могут использоваться в системах дополнительной аутентификации и фильтрации сообщений, которые могут быть отправлены на приватный электронный ящик пользователей. Системы многофакторной аутентификации могут использовать биометрические данные, такие как сканирование отпечатков пальцев или сканирование лица. Также широко используемы методы аутентификации через, например, сканирование QR-кодов и отправку одноразовых паролей. Дополнительная фильтрация сообщений может быть использована для обнаружения писем, которые могут быть phishing или содержать вредоносное программное обеспечение. Это помогает предотвратить потенциальный вред, который может быть вызван прочтением или нажатием ссылок в этих сообщениях.

Заключение. Использование технологий машинного обучения и искусственного интеллекта играет важную роль в борьбе с phishing в современном мире. Защита от Phishing-атак на сегодняшний день стала актуальной

проблемой в интернете. Применение технологий машинного обучения и искусственного интеллекта в этой области становится все более популярным и эффективным. Разработка правильных методов и алгоритмов, понимание основных концепций и технических навыков помогут обеспечить защиту данных и противостоять phishing атакам. Технологии машинного обучения «с учителем», такие как метод «bag-of-words», позволяют проверять электронные сообщения на наличие признаков взлома. Это помогает улучшить работу фильтров и систем анализа электронных сообщений для выявления вредоносной активности и защиты пользователей. В свою очередь, стандарты проверки подлинности отправителя электронной почты, такие как SPF и DKIM, используются для защиты от phishing. SPF позволяет проверять, допустимо ли использование IP-адресов отправителем для отправки электронных сообщений, а DKIM позволяет проверить, действительно ли сообщение было отправлено от подлинного отправителя. Применение технологий машинного обучения и искусственного интеллекта, в сочетании со стандартами проверки подлинности отправителя электронной почты, может значительно повысить уровень защиты системы, что в свою очередь улучшает безопасность электронной переписки и защищает пользователей от потенциальных угроз.

СПИСОК ЛИТЕРАТУРЫ

1. Mukhamadieva K. Обзор методов обнаружения фишинговых атак на основе искусственного интеллекта // Вестник ДонНУ : научный журнал. Серия Г: Технические науки, 2021. № 4. [Электронный ресурс]. URL: https://www.researchgate.net/publication/360218773_OBZOR_METODOV_OBNARUZENIA_FISINGOVYH_ATAK_NA_OSNOVE_ISKUSSTVENNOGO_INTELLEKTA (дата обращения: 24.06.2023).
2. Чуквубе Д. Защищаемся от ИИ с помощью ИИ: решения с поддержкой искусственного интеллекта для киберугроз нового поколения [Электронный ресурс]. URL: https://www.securitylab.ru/analytics/518993.php (дата обращения: 22.06.2023).
3. Maraximov A. Xudaybergenov K. Модифицированный алгоритм повышения производительности машинного обучения для обнаружения и классификации фишинговых атак // Science and innovation, 2022. № A8. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/modifitsirovannyy-algoritm-povysheniya-proizvoditelnosti-mashinnogo-obucheniya-dlya-obnaruzheniya-i-klassifikatsii-fishingovyh-atak (дата обращения: 23.06.2023).
4. Пурисов Д. И., Летникова Е. М. Машинное обучение для определения фишинговых интернет-ресурсов // Международный научный журнал «Синергия Наук», 2021. [Электронный ресурс]. URL: http://synergy-journal.ru/archive/article7459 (дата обращения: 25.06.2023).
5. Татарникова Т. М., Бимбетов Ф., Богданов П. Ю. Выявление аномалий сетевого трафика методом глубокого обучения // Известия СПбГЭТУ ЛЭТИ. 2021. № 4. С. 36-41.
6. Татарникова Т. М. Статистические методы исследования сетевого трафика // Информационно-управляющие системы. 2018. № 5(96). С. 35-43.
7. Татарникова Т. М., Журавлев А. М. Нейросетевой метод обнаружения вредоносных программ на платформе android // Программные продукты и системы. 2018. № 3. С. 543-547.

УДК004.056.5

МОДЕЛЬ БЕЗОПАСНОСТИ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА С ПОМОЩЬЮ DIRECTUM RX

Иванов Денис Александрович, Ярош Артем Андреевич

Филиал Военного учебно-научного центра Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина,
г.Челябинск, городок 11 дом 1, Челябинск, 454015, Россия
e-mails: prosto_deniss@mail.ru, aros32495@gmail.com,

Аннотация. В статье рассматривается определение следующих наборов базовых функций электронного ДКО создание документов в электронном виде. Решение о выборе той или иной СЭД должно быть основано на соответствии конкретной системы тем задачам, которые планируют с ее помощью решать. Наряду с основным и самым предсказуемым источником угроз — внешними нарушителями (злоумышленниками), угрозу могут представлять и легальные пользователи СЭД. Система защиты СЭД должна быть способна противостоять этим угрозам, защищая не только данные, хранящиеся внутри электронных документов, но и саму себя. Многофакторная аутентификация позволяет серьезно повысить защищенность системы от внешних злоумышленников. Но одним из важных средств защиты информации является резервирование. Все же для обеспечения оптимальной защиты данных потребуется применять и другие меры, выходящие за границы встроенных решений. В случае возникновения инцидентов информационной безопасности, проанализировав сохраненные данные можно будет вычислить нарушителя с помощью Directum RX. В дополнение разграничения доступа можно добавить шифрование документов для дополнительного ограничения доступа. Делаем вывод, что СЭД обладает весьма обширным и разнообразным набором встроенных средств защиты.

Ключевые слова: функции электронного ДКО; Атаки на СЭД; защиты электронного документа.

THE SECURITY MODEL OF THE ELECTRONIC DOCUMENT MANAGEMENT SYSTEM USING DIRECTUM RX

Ivanov Denis Alexandrovich, Yarosh Artem Andreevich

Branch of the Military Educational and Scientific Center of the Air Force «Air Force Academy named after Professor N. E. Zhukovsky and Yu. A. Gagarin,
Chelyabinsk, town 11 house 1, Chelyabinsk, 454015, Russia
e-mails: prosto_deniss@mail.ru, aros32495@gmail.com

Abstract. The article discusses the definition of the following sets of basic functions of electronic ATP - the creation of documents in electronic form. The decision to choose one or another EDMS should be based on the compliance of a particular system with the tasks that are planned to be solved with its help. Along with the main and most predictable source of threats — external intruders (intruders), legitimate users of the EDMS can also pose a threat. The EDMS security system must be able to withstand these threats, protecting not only the data stored inside electronic documents, but also itself. Multi-factor authentication allows you to seriously increase the security of the system from external intruders. But one of the important means of protecting information is redundancy. However, to ensure optimal data protection, other measures will need to be taken that go beyond the boundaries of embedded solutions. In the event of information security incidents, after analyzing the stored data, it will be possible to calculate the violator using Directum RX. In addition to access control, you can add document encryption to further restrict access. We conclude that the EDMS has a very extensive and diverse set of built-in protection tools.

Keywords: functions of electronic ATP; attacks on EDMS; protection of an electronic document.

Введение. Необходимая функциональность систем электронного документооборота (ДКО) формируется исходя из задач, стоящих перед автоматизацией ДКО организации.

Можно определить следующий набор базовых функций электронного ДКО: создание документов в электронном виде; создание карточки атрибутов для документа; формирование шаблонных документов, подстановкой в них переменных значений из атрибутной карточки документа; поиск атрибутной карточки документа; формирование электронного документа с использованием шаблонов на бланке организации; сохранение документов в необходимых форматах; формирование маршрутов документов и управление его перемещением; ведение журналов, классификаторов и справочников; регистрация и классификация документов; согласование документов; формирование о передвижении и исполнении документов.

Система электронного ДКО — это специальное приложение, которое обеспечивает участникам обмен электронными документами. Все системы электронного документооборота могут быть классифицированы по нескольким признакам.

Особенностью российского внутреннего электронного ДКО организации является его вертикальная направленность: электронный документ, прежде чем попасть к исполнителю, проходит ряд согласований и утверждений у вышестоящего руководства. Помимо этого, в отечественном делопроизводстве присутствуют такие неотъемлемые части, как регистрационная система, подготовка отчетов, контроль исполнения.

Очевидно, что решение о выборе той или иной СЭД должно быть основано на соответствии конкретной системы тем задачам, которые планируют с ее помощью решать. Чтобы окончательно определить, какое решение имеет смысл внедрить в работу организации необходимо руководствоваться следующими критериями: соответствие стандарту отрасли организации; соответствие целям и задачам организации; уровень технической поддержки СЭД со стороны поставщика как во время внедрения, так и в процессе эксплуатации; расширяемость СЭД в случае расширения деятельности организации; доступность документации по администрированию или изменению настроек СЭД; защита СЭД. Система должна обеспечивать защиту информации в соответствии с политикой безопасности организации; время, необходимое на восстановление СЭД после сбоев в работе; стоимость СЭД, включая стоимость покупки, лицензии, администрирования и технической поддержки [1, 2].

Современные СЭД являют собой автоматизированную информационную систему, предназначенную для обработки электронных документов, которая обеспечена комплексом средств защиты информации, программных и технических. СЭД можно разделить на четыре основные подсистемы: обработки электронных документов; обеспечения безопасности информации; электропитания; пользователи СЭД.

Для любой информационной системы, в том числе и для СЭД, основными угрозами считаются: угроза целостности информации; угроза доступности информации; угроза конфиденциальности информации.

Наряду с основным и самым предсказуемым источником угроз — внешними нарушителями (злоумышленниками), угрозу могут представлять и легальные пользователи СЭД — сотрудники организации, в частности, от наиболее привилегированных пользователей — администраторов системы. Они имеют неограниченные права доступа к информации и знают систему изнутри. Соответственно в результате внутренних атак вероятность нанесения колоссального ущерба организации крайне велика. При этом не так важны мотивы действий сотрудников — намеренные или непреднамеренные, в результате информация может оказаться утраченной или разглашенной, что повлечет за собой материальный и репутационный ущерб.

Соответственно, любые атаки на СЭД, а также на любые другие системы, основаны на описанном выше механизме. Элементы этого механизма могут видоизменяться для конкретных областей, в том числе и для СЭД. Все эти возможные изменения должны быть учтены.

Угрозы информационной безопасности СЭД можно разделить на несколько основных подгрупп: несанкционированный доступ; утечка информации; потеря данных. Для защиты информации в автоматизированных системах, в том числе СЭД, необходимо учитывать основные принципы: законность и

обоснованность защиты; системность; комплексность; непрерывность достаточность; гибкость; открытость алгоритмов и механизмов защиты; простота применения средств защиты.

Значительную часть угроз информационной безопасности составляют угрозы несанкционированного доступа (НСД). Эти угрозы ведут к утечкам конфиденциальной информации и утрате целостности этой информации. Для защиты информации в автоматизированных системах по требованию ФСТЭК и ФСБ должны использоваться встроенные или наложенные средства защиты информации от НСД [3].

В СЭД защита от НСД включает в себя аутентификацию, управление доступом.

В случае использования многофакторной аутентификации могут использоваться различные варианты комбинаций остальных методов аутентификации. Многофакторная аутентификация позволяет серьезно повысить защищенность системы от внешних злоумышленников, завладевших каким-либо из ключей доступа, поскольку для успешной аутентификации этого будет недостаточно.

Разграничение доступа — установление полномочий доступа субъектов к объектам информационной системы. Разграничение доступа позволяет строго определить полномочия субъекта списком ресурсов, которые доступны пользователю и права доступа к каждому ресурсу. В ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации» и в документах Гостехкомиссии РФ определены два вида (принципа) разграничения доступа: дискретное управление доступом; мандатное управление доступом.

Еще одним важным средством защиты информации является резервирование. Резервирование позволяет восстановить информацию, потерянную или искаженную в результате применения угрозы нарушения целостности, если основные контрмеры не помогают справиться с задачей. Кроме того, наличие резервной копии конфигурации или образа системы позволяет быстро восстановить полноценную работу ИС, доступность которой была нарушена. Во многих наиболее популярных СЭД реализована возможность работы с использованием протокола HTTPS. Это позволяет защитить данные за счет криптографического преобразования передаваемых данных. Отличие от HTTP заключается в том, что весь трафик передается в зашифрованном виде с использованием SSL и TLS. В работе HTTPS применяется SSL-сертификат, в котором содержатся уникальные ключи шифрования. Они позволяют подтвердить подлинность и используются для шифрования трафика.

Встроенные в СЭД средства защиты позволяют обеспечить высокий уровень безопасности, однако нельзя полностью полагаться только на них. Для обеспечения оптимальной защиты данных потребуется применять и другие меры, выходящие за границы встроенных решений.

Рассмотрим СЭД Directum RX на предмет встроенных средств безопасности. Среди встроенных средств, обеспечивающих безопасность в СЭД Directum RX, применяются криптографические методы и резервирование. В Directum RX реализована работа по протоколу HTTPS, это гарантирует, что данные при взаимодействии пользователей передаются в зашифрованном виде по защищенному каналу SSL/TLS. Такое взаимодействие обеспечивает конфиденциальность передаваемых электронных документов даже в случае перехвата их злоумышленником [4, 5].

Все данные в Directum RX хранятся централизованно, благодаря этому в системе возможно полноценное разграничение доступа. Права доступа могут быть заданы на каждый документ — в системе есть четыре типа прав доступа: «права доступа отсутствуют», «есть права на чтение», «есть права на чтение и запись» и «полные права доступа». Directum RX позволяет назначать права, как для каждого субъекта, так и для целых групп субъектов, что упрощает процесс администрирования.

В дополнение разграничения доступа можно добавить шифрование документов для дополнительного ограничения доступа к документам лиц, которым нельзя запрещать доступ к карточке документа, например администраторы системы. Шифрование в Directum RX возможно в следующих вариантах: на основе паролей и на основе сертификатов, либо их комбинированное использование.

Заключение. Такой подход имеет преимущество по сравнению с шифрованием на базе паролей, применяя шифрование на сертификате пользователям не требуется придумывать и запоминать множество паролей, которые должны быть достаточно сложными, и потерять доступ к документу, зашифрованному на сертификате сложнее.

Подлинность электронных документов обеспечивается применением электронной подписи. Для подписания документа сертификат открытого ключа каждого пользователя должен быть зарегистрирован в системе, секретный ключ хранится у пользователя, и он несет за него ответственность. В Directum RX возможно использование внешних носителей, например, rutoken и eToken. Работа пользователей в Directum RX протоколируется. Поэтому в случае возникновения инцидентов информационной безопасности, проанализировав сохраненные данные можно будет вычислить нарушителя либо определить причину независящую от человека. В истории фиксируются операции просмотра, изменения, создания, экспорта и импорта документов, назначения прав на доступ к ним и т.д. Протоколируется работа с записями справочников.

Можно сделать вывод, что СЭД Directum RX обладает весьма обширным и разнообразным набором встроенных средств защиты

СПИСОК ЛИТЕРАТУРЫ

1. Максимов М. В., Бобнев М. П., Кривицкий Б. Х. Защита от радиопомех. М. : Советское радио, 1976. 495 с.
2. Радзивский В. Г. Современная радиоэлектронная борьба. Вопросы методологии. М. : Радиотехника, 2006. 424 с.
3. Добыкин В. Д. Радиоэлектронная борьба. Силовое поражение радиоэлектронных систем. М. : Вузовская книга, 2007, 468 с.
4. Гапоненко Н. И., Горбань А. М., Горожанин Д. В. Формирование интенсивных электромагнитных импульсов, излучаемых при прямом возбуждении изолированной штыревой антенны короткоимпульсным сильноточным РЭП // Физика плазмы. 2000. Т. 26. № 4. С. 1-3.
5. Азаркевич Е. И. Генерация импульсного СВЧ излучения с помощью энергии химических взрывчатых веществ // Доклады Академии наук СССР. 1991. Т. 319. № 2. С. 352-355.

УДК 621.396.4

СУЩНОСТЬ, ЦЕЛИ И ПРИНЦИПЫ ОПТИМАЛЬНОГО АДАПТИВНОГО МОНИТОРИНГА БЕЗОПАСНОСТИ И КАЧЕСТВА КОНТЕНТА ЭЛЕКТРОННЫХ ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ, ДОСТУПНЫХ ПОЛЬЗОВАТЕЛЯМ ПО КАНАЛАМ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Крюкова Елена Сергеевна, Паращук Игорь Борисович
Военная академия связи им. Маршала Советского Союза С. М. Буденного,
Тихорецкий пр, 3, Санкт-Петербург, 194064, Россия
e-mails: e.kkrukovaa69@yandex.ru, shchuk@rambler.ru

Аннотация. В статье проведен анализ состава, особенностей и перспектив формирования контента электронных образовательных ресурсов, доступных пользователям по каналам телекоммуникационных сетей. Предпринята попытка сформулировать ключевые концептуальные основы оптимального адаптивного мониторинга контента, сформулирована сущность и введены квалиметрические понятия мониторинга, рассмотрены цели и задачи мониторинга объектов такого класса. Рассмотрен комплекс принципов оптимального адаптивного мониторинга контента электронных образовательных ресурсов, что создает предпосылки для синтеза алгоритмов оптимального и адаптивного наблюдения, оценивания и прогнозирования состояния (безопасности и качества) контента в целях снижения затрат ресурсов системы образования, повышения оперативности и достоверности принятия решений по созданию и управлению контентом электронных образовательных ресурсов в различных условиях обстановки.

Ключевые слова: оптимальный адаптивный мониторинг; контент; электронные образовательные ресурсы; телекоммуникационная сеть; показатель качества; оценивание и прогнозирование.

THE ESSENCE, GOALS AND PRINCIPLES OF OPTIMAL ADAPTIVE MONITORING OF THE SECURITY AND QUALITY OF THE CONTENT OF ELECTRONIC EDUCATIONAL RESOURCES AVAILABLE TO USERS THROUGH TELECOMMUNICATION NETWORKS

Kryukova Elena, Parashchuk Igor
Military Academy of Communications Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Ave., St. Petersburg, 194064, Russia
e-mails: e.kkrukovaa69@yandex.ru, shchuk@rambler.ru, andrsel@mail.ru

Abstract. The article analyzes the composition, features and prospects of the formation of the content of electronic educational resources available to users through telecommunication networks. An attempt is made to formulate the key conceptual foundations of optimal adaptive content monitoring, the essence is formulated and qualimetric concepts of monitoring are introduced, the goals and objectives of monitoring objects of this class are considered. A set of principles of optimal adaptive monitoring of the content of electronic educational resources is considered, which creates prerequisites for the synthesis of algorithms for optimal and adaptive monitoring, assessment and prediction of the state (safety and quality) of content in order to reduce the cost of resources of the education system, increase the efficiency and reliability of decision-making on the creation and management of content of electronic educational resources in various conditions of the situation.

Keywords: optimal adaptive monitoring; content; electronic educational resources; telecommunication network; quality indicator; evaluation and forecasting.

Введение. Анализ теоретических положений и результатов практического использования мониторинга в различных сферах деятельности, анализ современного состояния информационного обеспечения образования, современных требований и тенденций технической эволюции электронных образовательных ресурсов (ЭОР), доступных пользователям по каналам современных телекоммуникационных сетей (ТКС), а также широкое использование «де факто» рассматриваемого понятия в сфере информатики и телекоммуникаций, позволили сформулировать особую, новую систему взглядов на сущность мониторинга безопасности и качества контента ЭОР в целом.

При этом под такими ресурсами, доступными пользователям по каналам ТКС, понимается образовательный ресурс в электронно-цифровой форме, включающий в себя: структуру, предметное содержание и метаданные о них. Подразумевается, что ЭОР, доступные пользователям по каналам ТКС могут включать в себя данные, информацию и программное обеспечение, необходимые для его использования в процессе обучения [1, 2].

Главная цель, которая стоит перед ЭОР — повысить уровень качества, повысить эффективность образовательного процесса. В настоящие время ЭОР в сочетании с электронными средствами обучения представляют собой наглядный вид полученной информации, которая расширяет представление обучаемого об окружающем нас мире. Они усиливают мотивацию для продолжения самостоятельного изучения тем, а также позволяют осуществлять самоконтроль усвоения материала и приобретения компетенций.

Контент электронных образовательных ресурсов — смысловое (семантическое) и синтаксическое содержание, а также смысловое и информационное наполнение ЭОР [3].

Контент ЭОР бывает текстовым (учебники, книги, статьи, лонгриды и короткие посты в социальных сетях), графическим (картины, фотографии, иллюстрации, инфографики и любые другие изображения), видео (фильмы, сериалы, ролики на YouTube и т. д.), аудио (музыка, радиопередачи и подкасты) и мультимедийным (сочетает несколько вышеперечисленных, это презентации, обучающие платформы, компьютерные игры). Мультимедийный контент часто бывает интерактивным, т.е., построенным на взаимодействии с пользователем).

Базовыми подходами к созданию контента ЭОР принято считать: использование языков программирования; использование специальных и универсальных прикладных программных средств; использование цифровых инструментов и веб-сервисов; формирование контента ЭОР из информации, представленной на образовательных каналах, платформах, порталах и сайтах [1].

Мониторинг контента ЭОР — единый комплекс систематических целенаправленных мероприятий (организационных, технологических и технических), основанный на непрерывном либо периодическом (регулярном) наблюдении за состоянием контента (сбор, хранение, обработка и анализ информации о состоянии), качественном и количественном оценивании состояния и прогнозировании изменений состояния (безопасности и качества) контента ЭОР под влиянием конструктивных или деструктивных факторов.

Концепция оптимального адаптивного мониторинга (ОАМ) состояния (безопасности и качества) контента ЭОР — система взглядов, идей и принципов, определяющих общую методологию мониторинга объектов такого класса. Взяв за исходную точку сущность мониторинга, изложенную в определении, рассмотрим некоторые ключевые квалиметрические понятия, необходимые для изложения концептуальных основ ОАМ состояния (безопасности и качества) контента ЭОР, например: свойство контента, состояние контента ЭОР, безопасность и качество контента ЭОР, наблюдение, оценивание, прогнозирование, оптимальность мониторинга, адаптивность мониторинга и другие.

Примем за основу тот известный факт, что мониторинг сложных и многоплановых систем и объектов, например, таких, как контент ЭОР, должен включать ряд последовательных операций: 1) наблюдение (контроль) за состоянием контента ЭОР, состоянием его компонентов и за факторами, воздействующими на них; 2) текущее комплексное оценивание состояния (безопасности и качества) контента ЭОР и его компонентов; 3) прогнозирование возможных изменений состояния (параметров, показателей безопасности и качества) контента ЭОР и его компонентов.

Свойство контента ЭОР — это объективная особенность данного объекта исследований, зависящая от его строения и характеризующая отдельную его сторону [4].

Свойства контента ЭОР бывают внутренними и внешними. К свойствам контента ЭОР можно отнести полезность (информация, размещенная на ЭОР, должна нести пользу для обучаемого), соответствие запросу — пертинентность и релевантность (информация должна удовлетворять запрос пользователя), правдивость (информация не должна быть ложной или вводить пользователя в сомнения), разнообразие (информация должна быть представлена в разных форматах и освещать различные темы), вредоносность (уровень возможного негативного влияния на мировоззрение, психологию и здоровье обучаемого), актуальность (информация должна соответствовать времени) и грамотность (информация должна быть без орфографических и пунктуационных ошибок) [5].

Под состоянием контента ЭОР будем понимать множество параметров, численно характеризующих свойства этого объекта исследований в данный момент времени [4]. Иными словами, состояние контента ЭОР — вектор (вектор параметров) в параметрическом пространстве состояний, описывающих характеристики (свойства) данного объекта.

Безопасность контента ЭОР — свойство или совокупность свойств контента, обуславливающих защищенность содержания потоков информации, передаваемых из образовательной организации в Интернет и получаемых из глобальной сети в локальную сеть образовательной организации. Основывается на проверке информации, хранящейся в локальной сети образовательной организации, контроле нежелательности и вредоносности этой информации, контроле за содержанием электронной почты образовательной организации, а также контроле за просматриваемой сотрудниками информацией с целью предотвращения использования ЭОР в личных целях [6-8].

Качество контента ЭОР — свойство или совокупность свойств данного объекта исследований, обуславливающих его соответствие назначению — информационному обеспечению пользователей в интересах повышения эффективности образовательного процесса [4].

Наблюдение — комплексный целенаправленный процесс восприятия (сбора, хранения, обработки и анализа) информации о состоянии контента ЭОР и факторов, воздействующих на него [9].

Оценивание — процесс принятия решения о состоянии (безопасности и качестве) контента ЭОР, процедура получения качественных и количественных оценок состояния (оценочных значений показателей безопасности и качества) этого контента [9].

Прогнозирование — процесс разработки прогноза, исследования конкретных перспектив изменения состояния (безопасности и качества) контента ЭОР в различных ожидаемых условиях эксплуатации. Выработка вероятностного суждения о возможных изменениях состояния (параметров, показателей безопасности и качества) этого контента [9].

Адаптивность мониторинга — способность осуществлять целенаправленное приспособление (согласование) характеристик свойств поведения данного процесса к сложным условиям, имеющая целью оптимизацию параметров мониторинга контента ЭОР. Адаптация осуществляется в интересах получения оптимальной (необходимой и достаточной) информации о состоянии (безопасности и качестве) контента ЭОР, соответствующей, т.е., адекватной сложившейся ситуации.

Оптимальный мониторинг контента ЭОР — мониторинг, при котором траектория достижения цели данного процесса в пространстве ситуаций является самой предпочтительной в смысле принятого критерия.

Таким образом, опираясь на рассмотренные понятия, можно сформулировать концептуальную модель ОАМ контента ЭОР. Основополагающей целью ОАМ контента ЭОР является безопасное и качественное информационно-аналитическое обеспечение системы образования, адекватное целям функционирования и управления ею и учитывающее влияние внешних и внутренних, конструктивных и деструктивных факторов. Иными словами, цель ОАМ — обеспечение фактическим качественным материалом информационной базы системы образования (СО) в непрерывной динамике и с учетом влияющих факторов.

Для реализации указанной цели осуществляются процедуры ОАМ контента ЭОР, решающие следующие основные задачи:

–наблюдение — оптимизируемое по состоятельности, достоверности и точности, а также соответствующее (подстраивающееся к) условиям эксплуатации получение (выявление, регистрация и накопление) требуемой на данный момент информации о фактическом состоянии контента ЭОР;

–оценивание — оптимизируемое по состоятельности, достоверности и точности, а также соответствующее (подстраивающееся к) текущим требованиям СО получение оценок состояния (безопасности и качества) контента ЭОР;

–прогнозирование — оптимизируемое по состоятельности, достоверности и точности, а также соответствующее (подстраивающееся к) текущим требованиям СО получение прогностических оценок состояния (безопасности и качества) контента ЭОР.

Иными словами, выполняется ряд взаимосвязанных задач — на основании полученной в результате наблюдения информации решается задача принятия информационного решения о годности или негодности конкретного контента ЭОР для выполнения определенных функций образования в данный момент времени и в данных условиях. В случае, если принимается решение о негодности контента ЭОР, то возникает задача идентификации, аутентификации и локализации несоответствий, ошибок, неточностей, вредоносных факторов и иных коллизий в контенте ЭОР, обусловленных целенаправленными или случайными сбоями и нарушениями, а также алгоритмическими, программными, техническими отказами либо иными повреждениями на серверах СО и в каналах ТКС, по которым обучаемые получают доступ к этому контенту.

На основании результатов ОАМ контента ЭОР для СО осуществляется принятие решений по приостановке использования, регулировке, модернизации этого контента, замене его компонентов, реконфигурации контента ЭОР и т. п.

Рассмотрение задач ОАМ контента показывает, что его проведение необходимо для получения информации, используемой для управления процессами построения и эксплуатации ресурсов такого класса. Эта информация обеспечивает организацию обратной связи в управлении качеством и эффективностью построения и применения контента ЭОР. Отсюда следует, что отказаться в принципе от мониторинга нельзя, так как это будет означать утрату информации и, следовательно, потерю управления безопасностью и качеством ЭОР [9]. Однако процессом мониторинга можно и должно управлять, оптимизировать объем и номенклатуру наблюдаемых, оцениваемых и прогнозируемых параметров и (или) показателей безопасности и качества контента ЭОР с учетом условий эксплуатации.

Решение рассмотренных задач ОАМ контента ЭОР и принятие информационного решения о пригодности, безопасности и качестве этого контента может осуществляться различными способами. Содержание этих способов основывается на принципах оптимального адаптивного мониторинга.

Необходимым условием эффективного анализа и синтеза алгоритмов оптимального адаптивного мониторинга контента ЭОР является использование принципов системного подхода. Опираясь на основные принципы системного подхода, сформулируем базовые принципы и рекомендации, определяющие научную и практическую стороны реализации процесса оптимального адаптивного мониторинга контента ЭОР.

На наш взгляд, принципиальную основу ОАМ контента ЭОР должны составлять некоторые базовые принципы, которые общеприняты для построения и совершенствования сложных объектов исследования такого класса [10]:

1. Принцип единства (двойственности) ОАМ заключается в том, что мониторинг контента ЭОР должен рассматриваться и как процесс и как подпроцесс процесса более высокого уровня.

2. Принцип цели (целевой ориентации, целенаправленности) ОАМ контента ЭОР заключается в подчинении всех задач информационно-аналитической направленности, решаемых в рамках процедур наблюдения, оценивания и прогнозирования состояния (безопасности и качества) контента ЭОР и способов их решения достижению главной цели — повышению эффективности процесса мониторинга этого контента и, как следствие, повышению эффективности образовательного процесса.

3. Принцип сложности ОАМ указывает на необходимость мониторинга контента ЭОР как сложной совокупности различных его компонентов, находящихся в многообразных связях между собой, с обучаемыми и с элементами окружающей среды системы образования.

4. Принцип множественности моделей ОАМ заключается в том, что для полного описания процесса ОАМ контента ЭОР необходимо множество моделей мониторинга состояния (безопасности и качества) этого контента, каждая из которых описывает процедуры наблюдения, оценивания и прогнозирования его состояния (безопасности и качества) в каком-либо аспекте или (и) на каком-либо уровне представления.

5. Принцип преемственности информационно-аналитических методов мониторинга в рамках СО контента ЭОР для обеспечения взаимодействия с существующими средствами и методами контроля состояния (безопасности и качества) в интересах повышения эффективности образования с последующим эволюционным переходом к перспективным средствам и методам, призванным осуществлять мониторинг контента, входящего в состав единого глобального информационного пространства.

6. Принцип информационно-аналитического единства, требующий использования стандартных единых расчетно-аналитических подходов к реализации мониторинга контента ЭОР и взаимодействующих с ним иных информационных ресурсов, совместимости баз знаний методов мониторинга, баз данных результатов мониторинга и единых процедур агрегации информации в СО.

7. Принцип адаптивности мониторинга контента ЭОР, связанный с принципом целевой ориентации, призван обеспечивать приспособление (приведение в соответствие) характеристик процесса мониторинга к конкретной ситуации применения контента ЭОР и управления им. В основе реализации данного базового принципа могут лежать функциональные принципы обоснованности, тождественности и динамичности.

8. Принцип регулярности мониторинга контента ЭОР, заключающийся в проведении наблюдения, оценивания и прогнозирования показателей контента в соответствии с периодами, обусловленными целями, задачами и возможностями оценочной деятельности для конкретной образовательной деятельности.

9. Принцип постоянства мониторинга контента ЭОР (постоянный характер ОАМ), определяющий наблюдение, оценивание и прогнозирование его параметров и показателей, отражающих его состояние (безопасность и качество) и функционирование (качество использования), синхронно с процессом обучения и в соответствии с обусловленной периодичностью при исключении необоснованной фрагментарности, что должно обеспечивать максимально возможное приближение мониторинга к режиму непрерывности.

10. Принцип активности мониторинга контента ЭОР, заключающийся в инициации мониторинга со стороны субъекта контроля контента в соответствие с его (субъекта) планами и намерениями, определяемыми результатами анализа конкретных ситуаций (прошлых, настоящих, прогнозируемых).

11. Принцип комплексности (целостности, всесторонности, интегративности) мониторинга контента ЭОР, определяющий одновременное наблюдение, оценивание и прогнозирование отдельных взаимозависимых и взаимодействующих показателей безопасности и качества, отражающих основные свойства контента.

12. Принцип преемственности результатов (историзма) мониторинга контента ЭОР, заключающийся в обеспечении связи последующих результатов наблюдения, оценивания и прогнозирования с предыдущими для обеспечения сравнительного (во времени) анализа параметров и показателей, характеризующих свойства контента, для вскрытия закономерностей и выявления тенденций изменения состояния (безопасности и качества) контента ЭОР.

13. Принцип пригодности результатов ОАМ контента ЭОР для практического использования в интересах управления ресурсами образования.

Заключение. Таким образом, проведен анализ состава, особенностей и перспектив формирования (построения) контента ЭОР, доступных пользователям по каналам ТКС. Предпринята попытка сформулировать ключевые концептуальные основы ОАМ объекта такого класса — сформулирована сущность и введены квалиметрические понятия мониторинга контента ЭОР, рассмотрены цели и задачи ОАМ контента ЭОР.

Рассмотрен комплекс принципов оптимального адаптивного мониторинга контента ЭОР, что создает предпосылки для синтеза алгоритмов оптимального и адаптивного наблюдения, оценивания и прогнозирования состояния (безопасности и качества) контента в целях снижения затрат ресурсов СО, повышения оперативности и достоверности принятия решений по созданию и управлению контентом в различных условиях обстановки.

СПИСОК ЛИТЕРАТУРЫ

1. Панюкова С. В. Цифровые инструменты и сервисы в работе педагога. Учебно-метод. пособие. М, : Изд-во «Про-Пресс», 2020. 33 с.
2. Колыхматов В. И. Новые возможности и обучающие ресурсы цифровой образовательной среды: учеб-метод. пособие. СПб. : ГАОУ ДПО «ЛОИРО», 2020. 157 с.
3. Климович Н. Г. Контент: топовые техники SEO-продвижения. М. : Инфра-Инженерия. 2021. 330 с.
4. Петухов Г. Б. Основы теории эффективности целенаправленных процессов. Ч. 1. М. : МО СССР, 1989. 660 с.
5. Евстратова Е. Что такое контент — объяснение английского термина русскими словами // Что такое контент. 2020. [Электронный ресурс]. URL: https://elenaevstratova.ru/chto-takoe-kontent/ (дата обращения: 27.05.2023).
6. Ганжур А. П., Отакулов А. С., Дьяченко Н. В. Политика безопасности контента // Молодой исследователь Дона. № 6 (33), 2021. С. 41-44.
7. Котенко И. В., Саенко И. Б., Браницкий А.А., Паращук И.Б., Гайфулина Д.А. Интеллектуальная система аналитической обработки цифрового сетевого контента для защиты от нежелательной информации // Информатика и автоматизация (Труды СПИИРАН). Вып. 20(4), 2021. С. 755-792.
8. Десницкий В. А., Котенко И. В., Паращук И. Б. Методика оценки эффективности систем обработки сетевого контента для обнаружения вредоносной информации с учетом устранения неопределенности смыслового наполнения информационных объектов // XXII Международная конференция по мягким вычислениям и измерениям (SCM-2019) : сборник докладов. Санкт-Петербург, 23-25 мая 2019 г. СПб. : СПбГЭТУ «ЛЭТИ». 2019. С. 62-65.
9. Евланов Л. Г. Контроль динамических систем. М. : Наука, 1979. 432 с.
10. Паращук И. Б., Крюкова Е. С., Михайличенко Н. В. Особенности и принципы оптимального адаптивного мониторинга центров обработки данных и электронных библиотек // Перспективные направления развития отечественных информационных технологий: материалы VI межрегиональной научно-практической конференции. Севастополь, 22-26 сентября 2020 г. / науч. ред. Б. В. Соколов. Севастополь : СевГУ, Т. 2. 2020. С. 47-48.

УДК 004.056

СПОСОБ ПРОАКТИВНОГО УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ СЕТИ ПЕРЕДАЧИ ДАННЫХ С ПРОГНОЗОМ СТРАТЕГИИ ВТОРЖЕНИЯ НАРУШИТЕЛЯ

Липатников Валерий Алексеевич[1], Шевченко Александр Александрович[2], Мелехов Кирилл Витальевич[1]

[1] Военная академия связи имени Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

[2] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия

e–mails: lipatnikovanl@mail.ru, alex_pavel1991@mail.ru, kirill_melehov@bk.ru

Аннотация. В связи с быстрым развитием информационных технологий, в том числе сети Интернет, объединяющей разнородные сети, и переходом к информационному обществу, проблема обеспечения информационной безопасности и построения сети передачи данных стала одной из наиболее актуальных. Целью исследования является повышение вероятности защищенности сети передачи данных в течение заданного времени путем разработки способа проактивного управления безопасностью с прогнозом стратегии вторжения нарушителя за счет применения интеллектуальных технологий. Результат: предложена топология защищенной сети передачи данных и способ проактивного управления безопасностью с прогнозом стратегии вторжения нарушителя. Новизна: предлагаемые решения строятся на основе интеллектуальных технологий, позволяющим прогнозировать стратегии вторжения нарушителя. Практическая значимость: использование предложенного способа позволит повысить защищенность сети передачи данных.

Ключевые слова: информационная безопасность; сеть передачи данных; интеллектуальные технологии.

A WAY TO PROACTIVELY MANAGE DATA NETWORK SECURITY WITH PREDICTION OF AN INTRUDER'S INVASION STRATEGY

Lipatnikov Valery[1], Shevchenko Alexander[2], Melekhov Kirill[1]

[1] The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny,
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

[2] The Bonch-Bruevich Saint-Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia

e–mails: lipatnikovanl@mail.ru, alex_pavel1991@mail.ru, kirill_melehov@bk.ru

Absrtact. Due to the rapid development of information technology, including the Internet, uniting heterogeneous networks, and the transition to an information society, the problem of information security and data networking has become one of the most pressing. The aim of the study is to increase the probability of data network security for a given time by developing a way of proactive security management with prediction of intruder intrusion strategy through the use of

intelligent technologies. Result: A protected data network topology and a method of proactive security management with prediction of intruder intrusion strategy are proposed. Novelty: The proposed solutions are built on the basis of intelligent technologies that allow predicting the intruder's intrusion strategy. Practical Significance: The use of the proposed method will improve the security of the data transmission network.

Keywords: information security; data network; intelligent technology.

Введение. С эволюцией телекоммуникационных сетей и информационных технологий изменялись условия взаимодействия пользователя и вычислительной техники. Информация, циркулирующая в информационные системы, приобретала все большие объемы и влияние на разные сферы деятельности человека. При этом развивалась в соответствии с прогрессом информационных технологий и учетом возникающих угроз и новых видов воздействий на сети передачи данных (СПД).

Взаимодействие информационных технологий и деятельности человека породило уникальную среду — киберпространство. Его можно описать как виртуальную среду, которая не существует в какой-либо физической форме, но является комплексной средой или пространством, возникшим в результате возникновения Интернета, в сочетании с людьми, организациями и активностью на всех видах технологических устройств и сетей, к нему подсоединенных. Процесс организации и безопасности сети VoIP-телефонии специального назначения являет собой набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды, ресурсов организаций и пользователей. Кибербезопасность (КБ) подразумевает достижение и сохранение свойств безопасности у ресурсов организации или пользователей, направленных против соответствующих киберугроз. Четкое понимание связи термина КБ (*cybersecurity*) с сетевой безопасностью, прикладной безопасностью, Интернет-безопасностью и безопасностью критичных информационных инфраструктур дает стандарт *ISO/IEC* 27032:2012 (*Information technology — Security techniques–Guidelines for cybersecurity*).

КБ обеспечивается различными классами средств защиты информации, в том числе интеллектуальными. Одним из таких классов являются системы *SIEM (Security Information and Event Management)*. Основными задачами SIEM-систем являются процессы сбора больших массивов гетерогенных данных о событиях безопасности и обнаружения инцидентов и угроз безопасности в результате их обработки. Недостатком большинства средств защиты является реактивность используемых методов, с недостаточным вниманием к анализу динамики действий нарушителя при подготовке и реализации сценариев внешних, а также внутренних вторжений. За счет этого возникает противоречие между развивающимися средствами кибернетического вторжения и существующими способами защиты. В связи с этим задачи уточнения классификации при распознавании вторжений в интеллектуальных способах управления КБ информационной инфраструктуры, анализ и обработка рисков ИБ остается актуальной.

В [1] рассматривается подход к разработке и использованию систем ИБ, основанный на выделении интеллектуальной надстройки над традиционными способами защиты и построении единой унифицированной среды для создания и поддержки функционирования систем защиты. Представляются отдельные способы управления ИБ. Предложен способ управления безопасностью ИС на основе выделенного сервера с контейнерной виртуализацией. Не в полной мере рассмотрены вопросы распознавания вторжений и прогнозирования состояния защиты ИС, не рассматривались вопросы управления рисками ИБ при обеспечении КБ киберпространства.

В [2] рассматриваются вопросы модификации процесса генерации модели атак и методики его анализа для более адекватного мониторинга и выбора защитных мер. В данный работе основное внимание сконцентрировано на построении графов атак и не в полной мере рассмотрены вопросы прогнозирования и управления рисками информационной безопасности.

В [3] описан подход к анализу информационных рисков с применением нечеткого когнитивного подхода в сочетании с использованием искусственных нейронных сетей. Вопросы, рассмотренные в работе, ограничены анализом рисков ИБ, не затронуты обнаружение вторжений нарушителя и анализ его действий при осуществлении контейнерной виртуализацией.

В связи с быстрым развитием информационных технологий, в том числе сети Интернет, объединяющей разнородные сети, и переходом к информационному обществу, проблема обеспечения ИБ и построения СПД стала одной из наиболее актуальных. К средствам защиты в настоящее время предъявляются более жесткие требования.

Целью исследования является повышение вероятности защищенности СПД в течение заданного времени путем разработки способа проактивного управления безопасностью с прогнозом стратегии вторжения нарушителя за счет применения интеллектуальных технологий.

Задачей исследования является разработка способа проактивного управления безопасностью СПД с прогнозом стратегии вторжения нарушителя.

Решение. Защита периметра считается обязательным элементом системы обеспечения информационной безопасности организации и включает в себя шлюзы безопасности, средства межсетевого экранирования, организацию виртуальных частных сетей, системы обнаружения и предотвращения вторжений.

Реализация защиты остается одной из основных задач ИБ и основой надежного функционирования критичных для компании информационных систем. Но технологии не стоят на месте. Появляются новые концепции построения сетей, такие как «сети без границ» или «сети на основе намерений», являющиеся закономерным продолжением технологии SDN, а наряду с ними и новые виды вторжений злоумышленников.

Межсетевые экраны и граничные маршрутизаторы с верно настроенной конфигурацией являются первой линией обороны, предотвращающей несанкционированный доступ в СПД. На смену межсетевым экранам прежнего поколения (с фильтрацией пакетов), блокирующим только сетевые порты и IP и MAC-адреса, пришли новые системы с функциями обеспечения безопасности на уровне приложений, на котором сейчас осуществляется большинство атак.

Средства межсетевого экранирования обеспечивают не только защиту от атак, но и защищенное соединение между офисами, а также безопасный удаленный доступ сотрудников к информационным ресурсам. Их дополняют шлюзы безопасности, способные поддерживать большое число защищенных каналов связи.

Еще один класс продуктов — системы обнаружения/предотвращения вторжений (IDS/IPS). Они позволяют проводить глубокий анализ активности в сети на всех уровнях модели OSI, обновлять в реальном времени базы сигнатур атак и признаков вторжений, обеспечивать защиту от уязвимостей нулевого дня с помощью адаптивных технологий проверки.

Новые технологии и тенденции требуют иных подходов к организации защиты корпоративной сети. Учитывая стремительное распространение мобильных устройств, концепции BYOD, облачных вычислений и различных технологий для удаленной работы, все чаще приходится слышать об исчезновении периметра корпоративной сети, однако концепция его защиты не устарела, она лишь нуждается в адаптации к современным условиям. Немногие решатся отказаться от межсетевых экранов и шлюзов безопасности.

Необходимо предусмотреть возникновение новых рисков и внедрить дополнительные технические средства обороны. СПД является важным сегментом сети любого предприятия. Но вопрос ее безопасности не рассматривается на должном уровне. С развитием новых технологий, таких как нейросети, искусственный интеллект, программно-управляемые сети, ускорением скорости передачи данных и увеличением вычислительных мощностей появляются новые угрозы и, вместе с тем, новые методы защиты сетей. Вопрос защиты СПД средствами интеллектуальных технологий актуален. Проводятся научные исследования в областях обеспечения безопасной передачи информации, обеспечения качества при передаче голосовых и медиаданных, сжатия речи и видео, оценки качества [4, 5].

Однако, недостаточно освещенным остается вопрос определения эффективности использования технологий управления проактивной безопасностью СПД с возможностью прогноза стратегии вторжения нарушителя. Ведь среди факторов необходимости внедрения интеллектуальных средств защиты в сетях нового поколения можно выделить: многообразие возможных угроз безопасности (видов атак); высокая критичность последствий реализации угроз информационной безопасности; большая ответственность за выработку и реализацию контрмер по обеспечению информационной безопасности; ограниченность времени на принятие решений по защите информации (реальный масштаб времени или близкий к нему); большой масштаб объекта защиты информации; неполнота и противоречивость исходных данных; необходимость обнаружения «редких» атак; необходимость проактивной защиты информации (основанной на способности предвидеть намерения и поведения атакующего).

Примеры интеллектуальных сервисов защиты информации: сбора и предварительной обработки информации о состоянии инфраструктуры, угрозах безопасности, шаблонах атак, инцидентах и пр.; хранения информации о безопасности; аналитической обработки информации о безопасности (анализа защищенности, моделирования атак, принятия решений и т.д.); отображения информации (визуального анализа).

Сеть на основе цели строится на трех основных функциональных блоках: восприятие выраженного цели и намерения, автоматизация развертывания выраженного намерения по всей сетевой инфраструктуре и контроль за реализацией цели. Внедрена интеллектуальная система аналитической обработки цифрового сетевого контента для его защиты в условиях динамики угроз вторжений.

Получение аналитических выводов (корреляция событий и использование машинного обучения и искусственного интеллекта [ML/AI]) для проверки, изучения и прогнозирования работы сети. В дополнение к проверке текущего состояния сети и его соответствия выраженному намерению функции контроля выполняют более глубокий анализ поведения сети на основе намерения. Например, они могут предсказать нарушения в реализации выраженного намерения до внесения планируемых изменений, определить или спрогнозировать тенденции, выявить аномалии, предсказать и проверить производительность сети на системном уровне.

Использование замкнутого цикла для реализации мер по корректировке и оптимизации работы сети. Обнаруженные аномалии, нарушения и несоблюдение соглашения об уровне обслуживания (при выраженном намерении) могут быть программно исправлены в масштабе всей системы через обращение к функциональному блоку активации. Таким образом, в сети на основе намерения применяется механизм автоматизации для

исправления любого нарушения политики на основе намерения и для непрерывной оптимизации, гарантирующей реализацию выраженного намерения в любой момент времени. В зависимости от политики меры могут приниматься автоматически или сообщаться администратору в виде рекомендаций. В последнем случае решение об их исполнении принимает администратор.

Таким образом, в рамках поставленной задачи, целесообразно разработать новую модель информационной сети в условиях динамики угроз вторжения с использованием интеллектуальных технологий аналитики, прогнозирования и реагирования на инциденты. Для этого потребуется построить схему исследуемой сети (рис. 1).

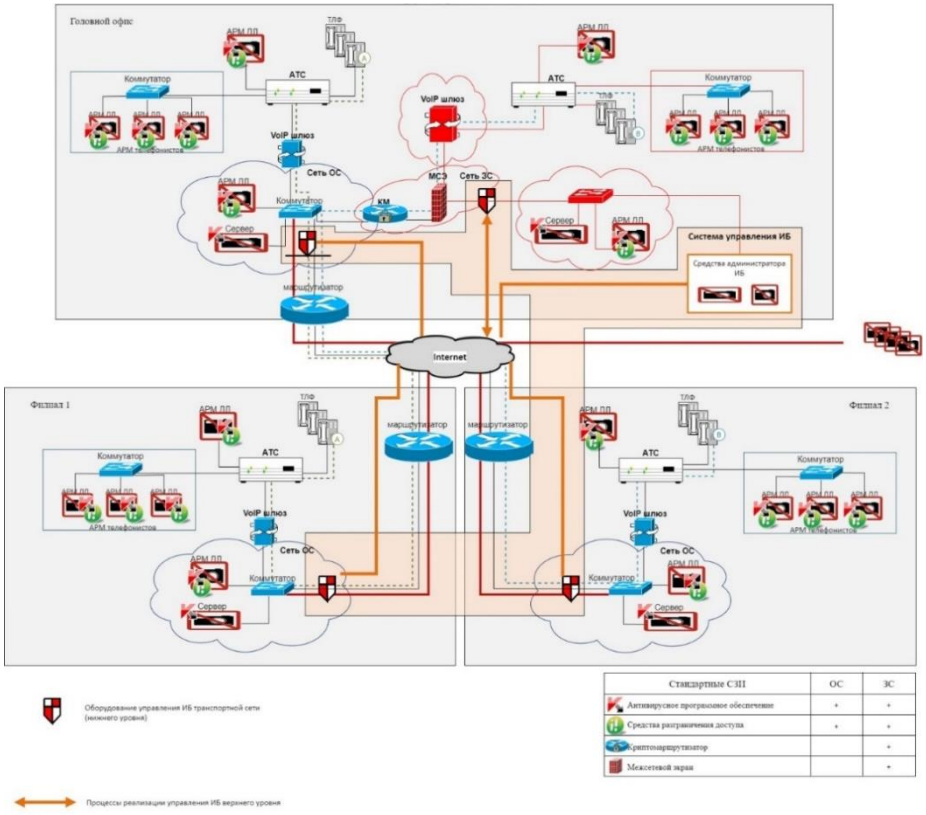


Рис. 1. Топология защищенной СПД

На схеме изображены три офиса предприятия — «Головной офис», «Филиал 1» и «Филиал 2». Каждый сегмент сети выходит в *WAN* через межсетевой экран, обеспечивающий защиту периметра от атак. Для обеспечения конфиденциальности и целостности данных передача производится посредством построения *VPN*-туннелей, которые конфигурируются на *VPN*-серверах. Чтобы обеспечить работу сети (маршрутизацию *ip*-пакетов), в инфраструктуру добавлены маршрутизаторы. А чтобы увеличить количество подключенных устройств и разбиение сети на сегменты подсети используются коммутаторы. Для обеспечения возможности интеллектуальной автоматизации, удобства управления, мониторинга и проактивной защиты от вторжения нарушителя необходимо внедрить сервер безопасности, который будет находиться в головном офисе и обеспечивать вышеперечисленные функции во всей сети.

В ходе рассуждений было выдвинуто предположение о необходимости моделирования процесса функционирования сети с целью качественной оценки параметров безопасности. Для разработки этого этапа необходимо сформировать и подготовить исходные данные. Согласно поставленной задаче обеспечения управления системами контроля и мониторинга безопасности предлагается алгоритм управления ИБ СПД (рис. 2). Алгоритм подразумевает описание полного цикла управления безопасностью СПД.

В рамках подпроцессов управления ИБ для СПД понятие объектов управления шире — это не только информационные активы, СПД, ИТ-услуги, но и риски ИБ, инциденты ИБ, непрерывность деятельности, изменения, совершенствования, сами меры обеспечения ИБ, обеспечивающие ресурсы, участвующую в реализации информационных процессов СПД [6]. Управляющим объектом является специальная система управления ИБ СПД организации СПД. СУИБ СПД должна обладать следующими чертами:

–ее построение и функционирование должно быть основано на постоянной оценке бизнес-рисков и рисков ИБ в частности, то есть на риск-ориентированном подходе;

–она должна быть предназначена для разработки, внедрения, эксплуатации, постоянного контроля, анализа, поддержания и улучшения ИБ СПД;

–она должна включать организационную структуру, политику, планирование действий, роли и обязанности, установившийся порядок, процедуры, процессы, меры обеспечения ИБ и ресурсное обеспечение для эффективного управления ИБ СПД.

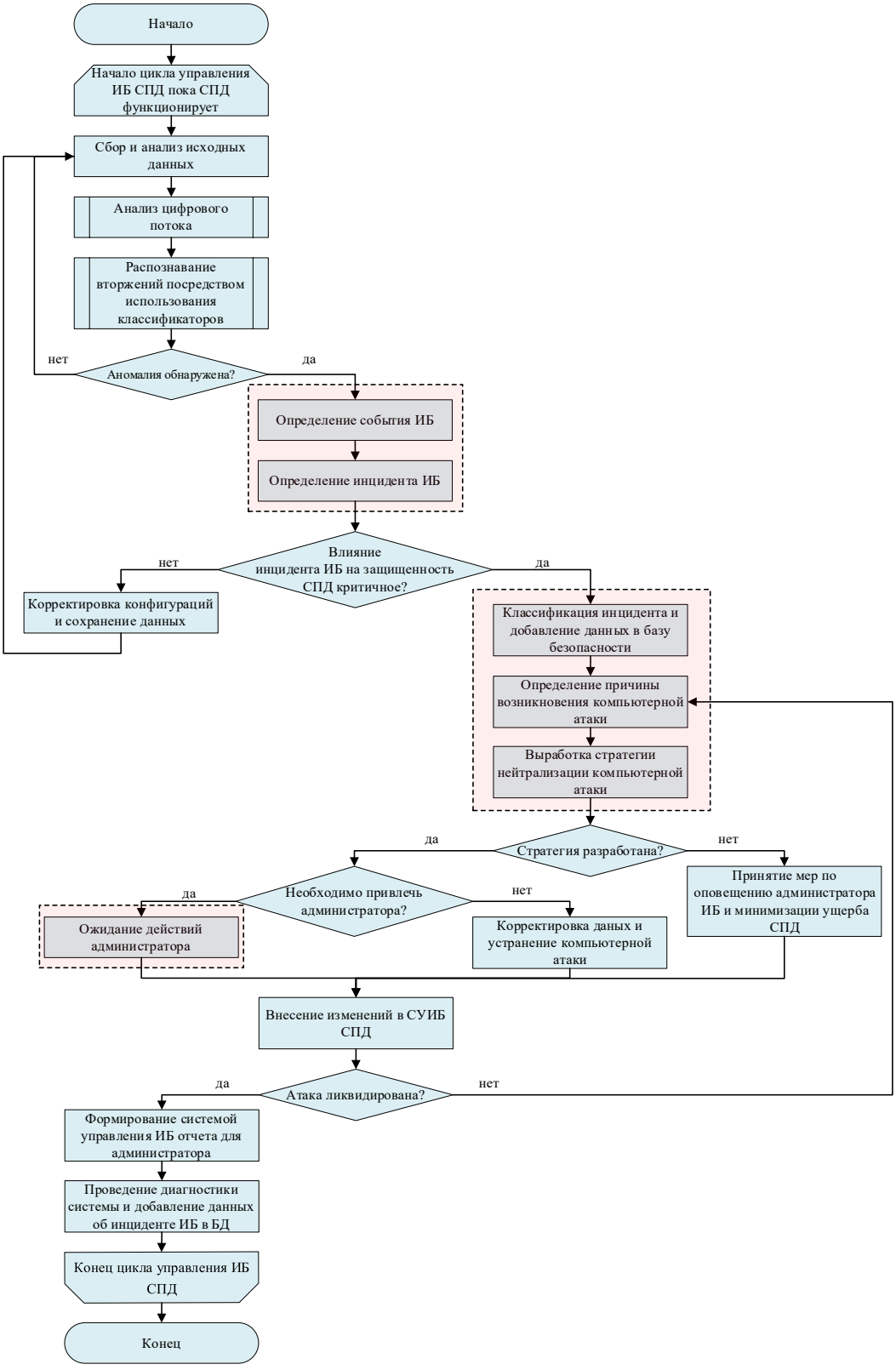


Рис. 2. Алгоритм управления ИБ СПД

Эффективность СУИБ СПД заключается в соотношении между достигнутым уровнем ИБ, полученным при управлении на основе СУИБ, и использованными ресурсами, обеспечившими его получение. Оценка эффективности СУИБ СПД должна осуществляться в рамках системного процесса получения и оценки объективных данных о текущем состоянии СУИБ, процессах и событиях, происходящих в ней, устанавливающего уровень их соответствия определенным организацией критериям. Разработанный алгоритм позволяет обеспечить требуемую эффективность.

Заключение. Таким образом, появляется возможность оценить действия администратора ИБ СПД при возникновении события безопасности и определить вероятность парирования компьютерной атаки согласно действиям администратора при возникновении событий нарушения ИБ, определить принципы функционирования механизма защиты благодаря обобщенному алгоритму управления безопасностью ИБ СПД и повысить качественную составляющую прогноза, анализа и управления рисками в СПД посредством использования интеллектуальных технологий, а именно когнитивной системы поддержки принятия решений, которая является основным элементом системы управления и представляет динамическую экспертную систему.

На основе предложенного способа формируются рекомендации администратору по парированию угрозы на основе информации о техническом состоянии объекта управления, компьютерной атаке, а также прогноза изменения условий.

Преимуществом предложенного способа является возможность идентификации непосредственной угрозы, а также выработка управленческих решений по уменьшению влияния уязвимости на безопасность.

Особенность способа заключается в классификации управленческих решений в зависимости от условий, что позволит снизить вычислительные затраты на формирование сигнала парирования угрозы. Численное моделирование работы с использованием результатов оценки набора правил поддержки принятия решений парирования многоэтапной атаки позволило подтвердить его работоспособность.

Разработанный способ предоставляет возможность исследовать вопросы по защищенности СПД, на которую проводится воздействие со стороны нарушителей. Практическая значимость способа определяется возможностью его использования при обеспечении защищенности СПД.

СПИСОК ЛИТЕРАТУРЫ

1. Липатников В. А., Шевченко А. А., Яцкин А. Д. Метод управления безопасностью информационно-вычислительных сетей на основе выделенного сервера с контейнерной виртуализацией // Информационные системы и технологии. 2017. № 4(102). С. 116-126.
2. Коршунов Г. И., Липатников В. А., Шевченко А. А., Малышев Б. Ю. Метод адаптивного управления защитой информационно-вычислительных сетей на основе анализа динамики действий нарушителя // Информационно-управляющие системы. 2018. № 4(95). С. 61-72.
3. Липатников В. А., Тихонов В. А., Шевченко А. А. Метод управления кибернетической безопасностью в системах критических инфраструктур, основывающийся на интеллектуальных сервисах защиты информации // Технологии построения когнитивных транспортных систем. Всероссийская научно-практическая конференция с международным участием, Санкт-Петербург, 28–29 мая 2019 г. : материалы конференции. СПб. : Институт проблем транспорта им. Н. С. Соломенко РАН, 2019. С. 207-214.
4. Федорченко Е. В. Новикова Е. С., Гайфулина Д. А., Котенко И. В. Построение профиля атакующего на основе анализа сетевого трафика в критических инфраструктурах // Системы управления, связи и безопасности. 2021. № 6. С. 76-89.
5. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 1. С. 70-76.
6. Шевченко А. А. Предложения по построению упреждающей системы управления информационной безопасностью информационной системы // Инновационная деятельность в Вооруженных Силах Российской Федерации : Труды всеармейской научно-практической конференции, Санкт-Петербург, 14–15 октября 2020 г. СПб. : ФГКВОУВО «Военная академия связи имени Маршала Советского Союза С. М. Буденного» МО РФ, 2020. С. 248-256.

УДК 621.396.67

ИССЛЕДОВАНИЕ БЛИЖНЕЙ ЗОНЫ ШИРОКОПОЛОСНОЙ БОРТОВОЙ АНТЕННЫ

Лянгузов Данила Андреевич,
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: danilalgz@ya.ru

Аннотация. В статье рассматривается задача разработки бортовых антенных устройств, диаграмма направленности которых незначительно искажается в диапазоне частот. Одним из факторов, влияющих на формирование излучения является затекание токов ближней зоны антенны на углы и кромки кузова. Полученные результаты позволяют сформулировать рекомендации по эффективному выбору места размещения бортовых антенн вблизи углов и кромок кузова.

Ключевые слова: широкополосные бортовые антенны; ближняя зона; диаграмма направленности.

INVESTIGATION OF THE NEAR ZONE OF A BROADBAND ON-BOARD ANTENNA

Lyanguzov Danila
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny,
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: danilalgz@ya.ru

Abstract. The article considers the problem of developing on-board antenna devices, the radiation pattern of which is slightly distorted in the frequency range. One of the factors influencing the formation of radiation is the leakage of currents of the near zone of the antenna on the corners and edges of the body. The results obtained allow us to formulate recommendations for the effective choice of the location of onboard antennas near the corners and edges of the body.

Keywords: broadband on-board antennas; near-field; radiation pattern.

Введение. Известно, что диаграмма направленности (ДН) широкополосных антенн, установленных на подвижных объектах (ПО) на практике имеет неидеальную форму. Это обусловлено затеканием вторичных токов ближней и промежуточной зон на углы и кромки корпуса. Причем различия в форме ДН обусловлены не только типом неравномерности (угол или кромка), но и расстоянием до него. Численно оценим объект и те области, которые будут влиять на форму ДН. Из [1] известно, что размер ближней зоны — $a_{бз}$ составляет (1):

$$a_{бз} \le \frac{D}{4} + \frac{D}{2}\sqrt[3]{\frac{D}{\lambda}}, \qquad (1)$$

где λ — длина волны, D — наибольший размер излучающей системы [2].

Размер промежуточной зоны — $a_{пр}$ составляет (2):

$$a_{бз} \le \frac{2D^2}{\lambda} \le a_{пр}, \qquad (2)$$

Введём понятия $a_{кр}$, $a_{уг}$ — расстояния от фазового центра антенны до кромок и углов соответственно. Разобьем рассмотрение промежуточной зоны на горизонтальную и вертикальную плоскости (рис. 1).

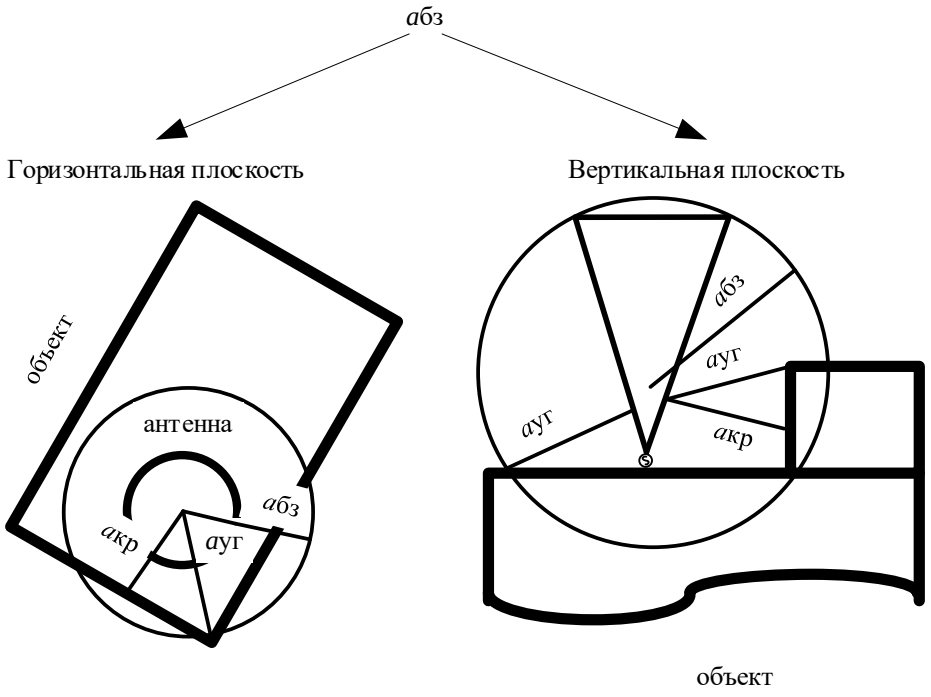


Рис. 1. Ближняя зона электродинамической системы антенна-корпус объекта

В зависимости от относительных размеров $a_{кр}$, $a_{уг}$ и $a_{БЗ}$ предположим, что степень искажения ДН корпусом объекта будет различной. Возможные случаи представлены на рис. 2. Варианты, при которых форма ДН будет искажаться выделены цветом.

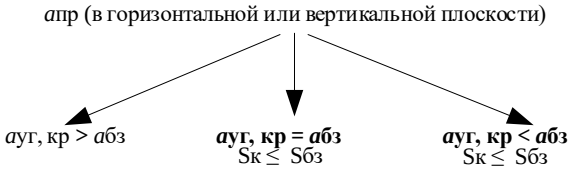


Рис. 2 Относительная зависимость $a_{кр}$, $a_{уг}$ и $a_{бз}$

Однако, если поверхность установки сложной формы частично находится внутри ближней зоны, то корректно говорить не о расстояниях до кромок и углов, а о площади двух фигур (во избежание необходимости учета множества параметров $a_{кр}$, $a_{уг}$). Одна из которых представляет собой ближнюю зону, а вторая — ту часть корпуса, которая входит в ближнюю зону антенны (рис. 3).

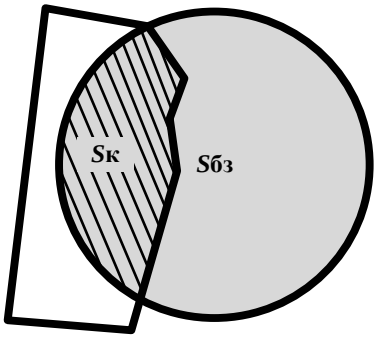


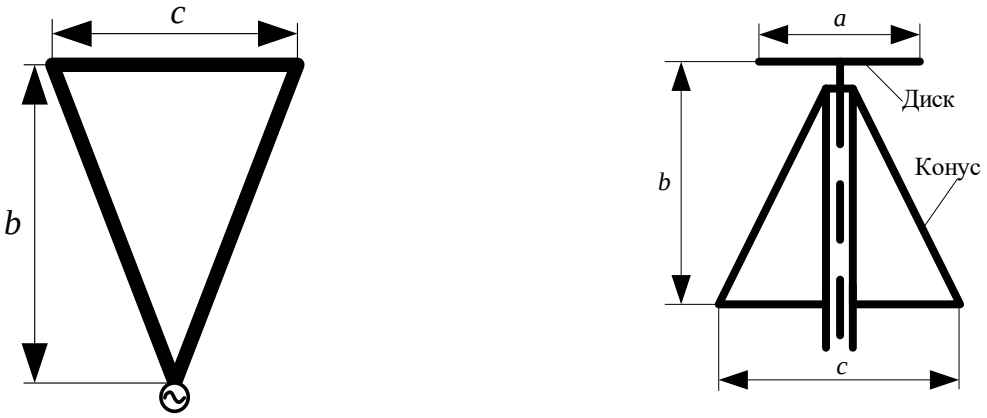
Рис. 3 К определению площадей ближней зоны и части корпуса объекта в ближней зоне

Проверим выдвинутую гипотезу для нескольких примеров. Исходными данными являются:

– рабочая длина волны: λ;

– тип и конструкционные параметры излучателя: конусный вибратор с нижней точкой питания.

Конус присоединяется к внешней оболочке кабеля, а корпус объекта к центральному проводнику (рис. 4 а). Характеристика направленности определена с помощью метода Стреттона-Чу. Распределение токов ближней зоны антенны рассчитано с использованием метода конечных элементов. Линия питания без потерь.



а б

Рис. 4 Диско-конусные антенны

Экспериментально подобранные размеры антенны следующие: $b/\lambda_{макс}$=0,25, $c/\lambda_{макс}$=0,275. Излучатель установлен сверху объекта установки в плоскости YoX, в точке P (X_{pit}, Z_{pit}). Линейные размеры объекта установки: длина L, ширина W, высота H. Геометрический центр верхней плоскости объекта находится в центре системы координат. Для линейных размеров объекта $L = W = 2a_{бз}(\lambda_{макс})$, $H = a_{бз}$ (в данном случае $a_{кр} = a_{бз}$, $a_{уг} > a_{бз}$, $S_к = S_{бз}$). На рис. 5-7 представлено:

– место установки антенны на корпусе подвижного объекта;

– форма диаграммы направленности антенны на корпусе подвижного объекта в рабочем диапазоне частот, но при фиксированном значении $\lambda_{макс}$, а также на идеально проводящей плоскости (ИПП).

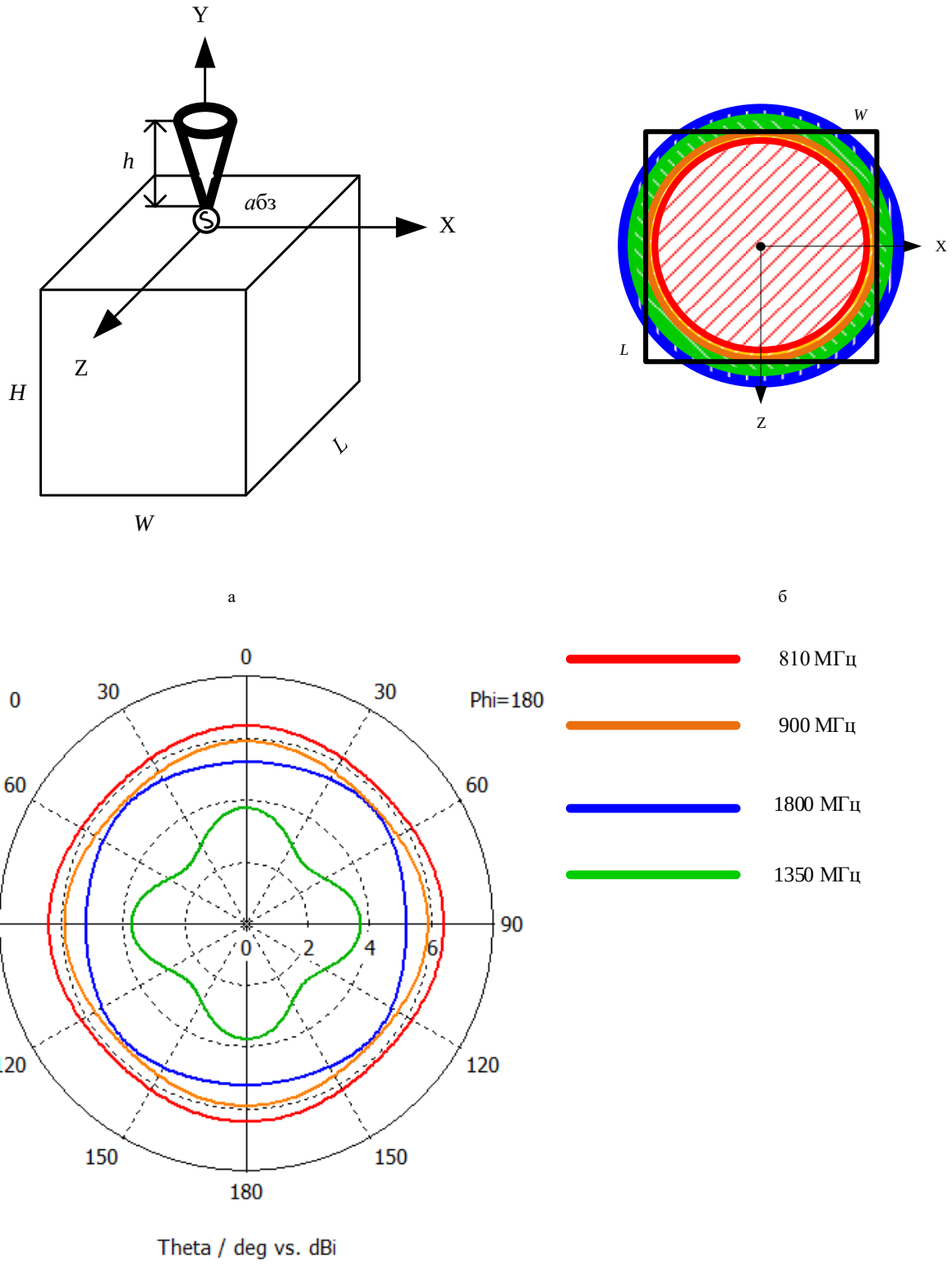
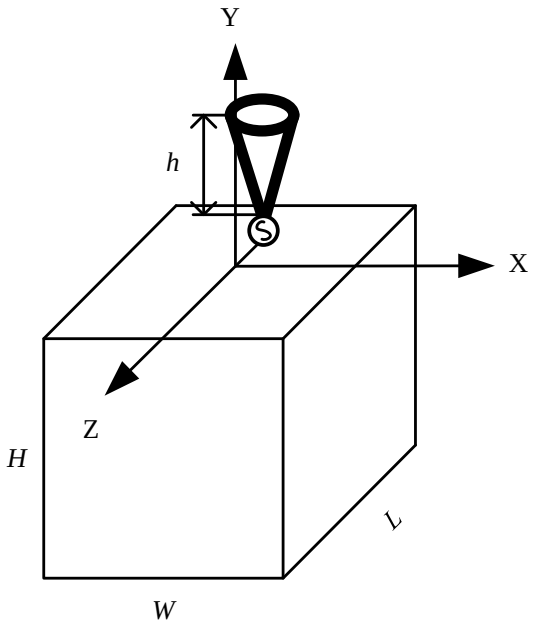
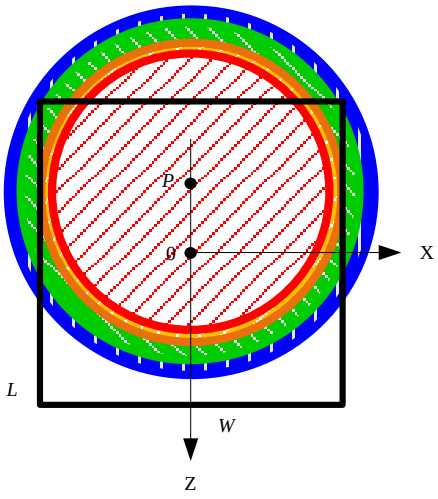


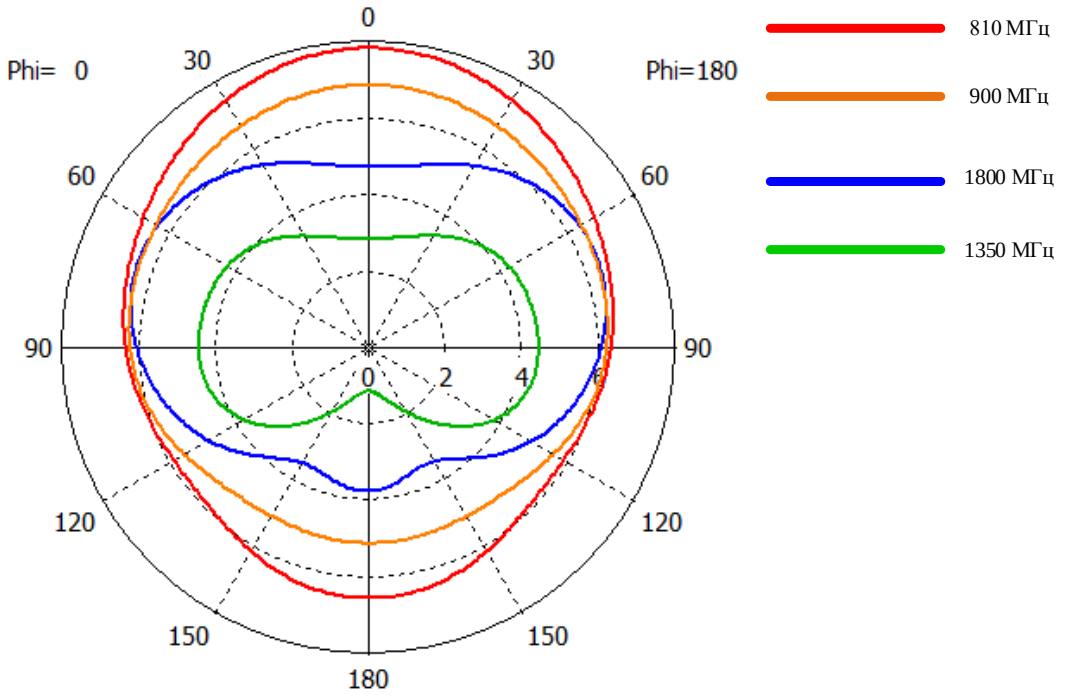
Рис. 5. Излучатель установлен в центре кузова. а — общий вид модели анализа, б — соотношение $S_{пр}$ и $S_к$, в — диаграмма направленности при различных значениях рабочей частоты



а

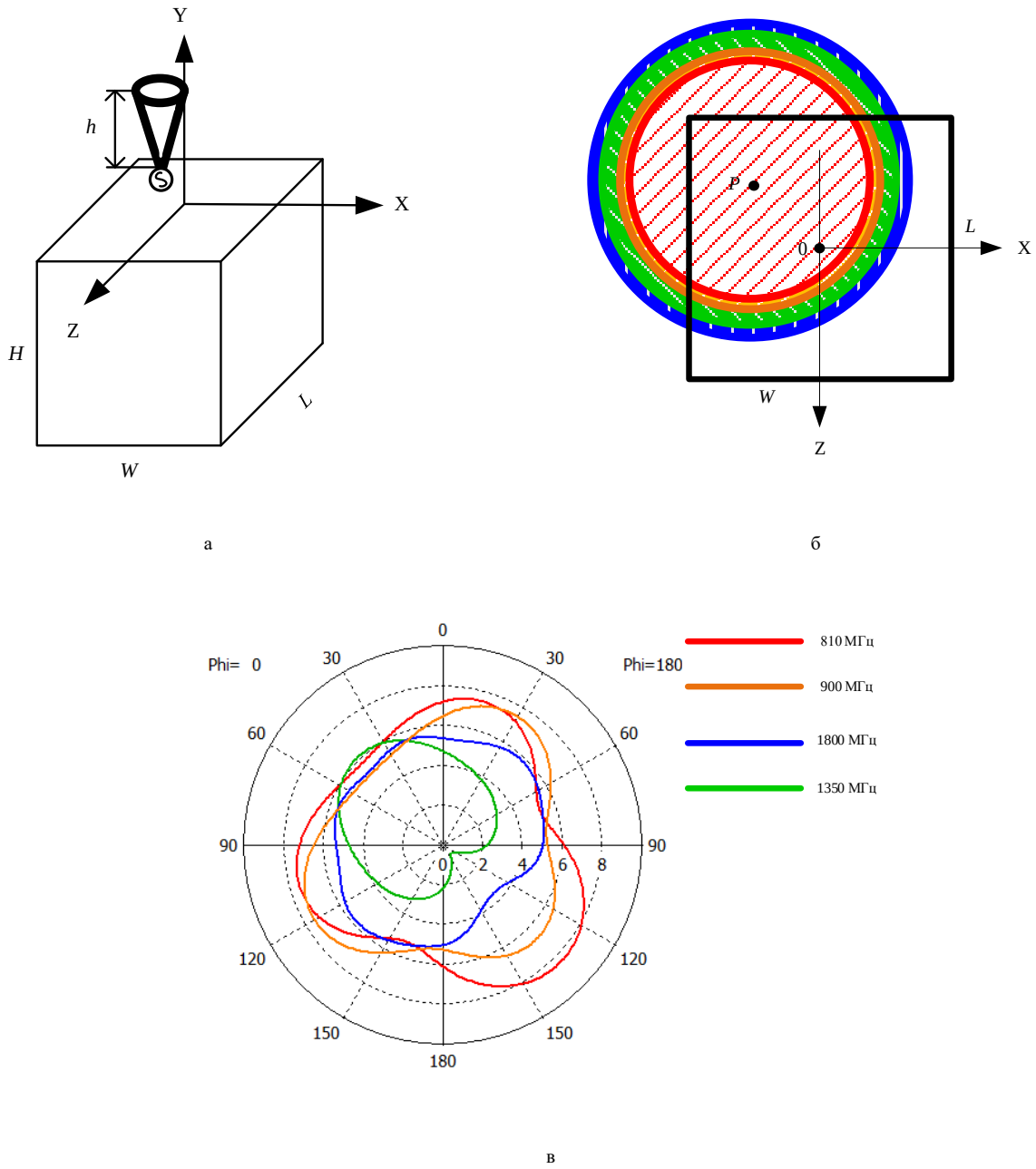


б



в

Рис. 6. Излучатель смещен к кромке кузова. а — общий вид модели анализа, б — соотношение $S_{пр}$ и $S_к$, в — диаграмма направленности при различных значениях рабочей частоты



а б

в

Рис. 7. Излучатель смещен в угол кузова а — общий вид модели анализа, б — соотношение $S_{пр}$ и $S_к$, в — диаграмма направленности при различных значениях λ

Видно, что вместо круговой форма диаграммы искривляется в сторону кромок или углов корпуса, находящихся в ближней зоне антенны. Выравнивания ДН можно добиться несколькими способами. Во-первых, можно изменить место установки антенны. Во-вторых — изменить конструкцию антенны: экранировать возбуждающий элемент или изменить поверхностное распределение токов ближней зоны широкополосной антенны таким образом, чтобы компенсировать затекание на углы и кромки с помощью емкостных вставок [3]. Внесение предыскажений в форму ДН возможно в случае использования активных фазированных антенных решёток (ФАР) с управляемой ДН [4].

В качества примера экранирования возбуждающего элемента примем дискоконусный вибратор, состоящий из конуса и диска, между которыми с помощью коаксиального кабеля прикладывается питающее напряжение. Конус присоединяется к внешней оболочке кабеля, а диск к центральному проводнику (рис. 4 б). Далее ограничимся рассмотрением промежуточной зоны, так как для подавляющего большинства подобных широкополосных антенн линейные размеры излучателя превосходят ближнюю зону антенны, и по существу токи ближней зоны являются поверхностными токами антенны.

Экспериментально подобранные размеры: $a/\lambda_{макс}$=0,175, $b/\lambda_{макс}$=0,25, $c/\lambda_{макс}$=0,275. Излучатель установлен сверху объекта установки в плоскости YoX, в точке P (X_{pit}, Z_{pit}).

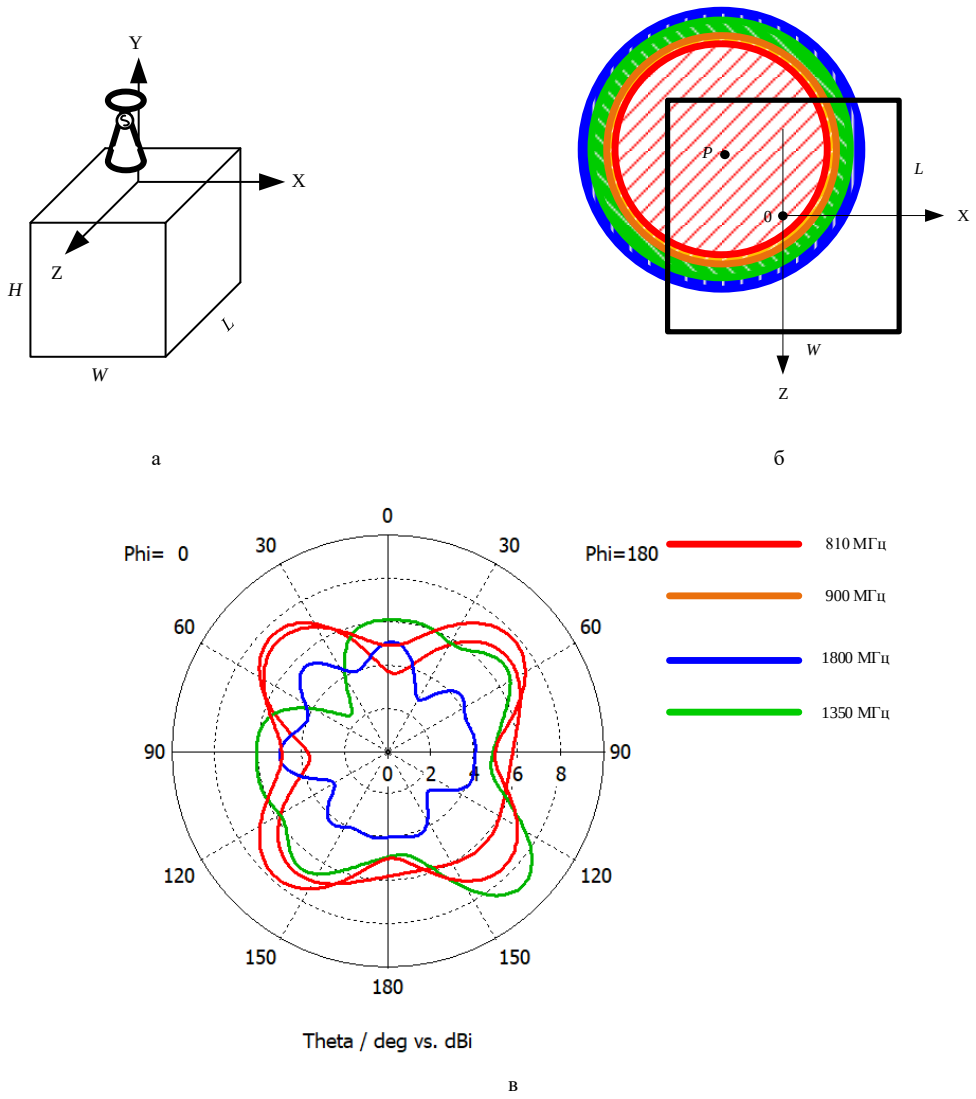


Рис. 8. Дискоконусная антенна в углу кузова а — общий вид модели анализа, б — соотношение $S_{пр}$ и $S_к$, в — диаграмма направленности при различных значениях λ

Видно, что форма диаграммы направленности меняется незначительно. Существенным недостатком данной конструкции являются большие геометрические размеры при использовании такого типа излучателя в качестве бортового (в диапазоне частот 25-2500 МГц) и высокая парусность. При необходимости определения ДН на меньших частотах целесообразно использовать принцип электродинамического моделирования [5].

Заключение. При размещение бортовой антенны вблизи неравномерностей корпуса ПО следует оценивать размер ближней зоны излучателя. Если размеры последней превышают расстояние от кромок и углов корпуса, необходимо учитывать искажение ДН при оценке предельной дальности радиосвязи. «Выравнивания» формы ДН можно добиться экранированием излучающего элемента, либо заблаговременным формированием «предыскаженной» ДН с использованием емкостных вставок или ФАР.

СПИСОК ЛИТЕРАТУРЫ

1. Марков Г. Т., Сазонов Д. М. Антенны : учебник. М.: Энергия, 1975. 528 с.
2. Бородулин Р. Ю. Конструкционный синтез электрически малых антенн : монография. СПб. : ВАС, 2020. 180 с.
3. Yijing He, Yue Li. Dual-polarized microstrip antennas with capacitive via fence for wide beamwidth and high isolation // IEEE Transactions on Antennas and Propagation. 2020. Vol. 67. № 7. Pp. 5095-5103.
4. Шанин А. М. Взаимное влияние элементов защищенных активных фазированных антенных решёток // Теория и техника радиосвязи. 2022. № 4. С. 73-79.
5. Шанин А. М. Модель передающего радиоцентра на основе принципа электродинамического подобия // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2023. № 5-6(179-180). С. 71-78.

УДК 621.391

ПРИМЕНЕНИЕ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ ДЛЯ МОНИТОРИНГА СОСТОЯНИЯ ТРУБОПРОВОДА НЕФТЕГАЗОВОЙ ОТРАСЛИ

Маслова Дарья Александровна
Нижегородский государственный инженерно-экономический университет
Октябрьская ул., 22а, Княгинино, 606340, Россия
e-mail: dasha.kirilova.96@bk.ru

Аннотация. В современных условиях нефтегазовым компаниям необходимо постоянно развиваться разрабатывая и применяя новые технологии. Одной из таких технологий являются беспроводные сенсорные сети, применение которых позволит повысить производительность и снизить производственные потери. В работе рассматриваются области применения беспроводных сетей в нефтегазовой отрасли. Основной проблемой применения беспроводных сенсорных сетей является энергопотребление. Предлагается применение пространственно-энергетической модели, учитывающей при подсчете затрачиваемой энергии ослабление сигнала.

Ключевые слова: нефтегазовая отрасль; энергопотребление; беспроводная сенсорная сеть; пространственно-энергетическая модель; ослабление сигнала.

APPLICATION OF A WIRELESS SENSOR NETWORK FOR MONITORING THE STATE OF A PIPELINE IN THE OIL AND GAS INDUSTRY

Maslova Daria
Nizhny Novgorod State of Engineering and Economic University
5 Oktyabrskaya St, Knyaginino, 606340, Russia
e-mail: dasha.kirilova.96@bk.ru

Abstract. In In modern conditions, oil and gas companies need to constantly develop by developing and applying new technologies. One of these technologies is wireless sensor networks, the use of which will increase productivity and reduce production losses. The paper discusses the areas of application of wireless networks in the oil and gas industry. The main problem of using wireless sensor networks is power consumption. It is proposed to use a space-energy model that takes into account signal attenuation when calculating the expended energy.

Keywords: oil and gas industry; energy consumption; wireless sensor network; spatial energy model; signal attenuation.

Введение. Эпоха Индустрии 4.0 позволила многим отраслям промышленности перейти к оцифровке, автоматизации и интеллектуализации производственной деятельности. Одной из ключевых технологий Индустрии 4.0, также называемой промышленной революцией, является технология Internet of Things (IoT) или интернет вещей. IoT за последние годы показывает высокий темп развития, позволяя соединять физические объекты и процессы с цифровым пространством. В отраслях промышленности существует отдельная категория, называемая Industrial Internet of Things (IIoT) — промышленный интернет вещей. Данная категория является более сложной системой, объединяющей в себе интеллектуальное производство и приложения, сочетающие в себе сразу несколько сквозных технологий. Одной из технологий IIoT являются беспроводные сенсорные сети, производящие сбор, обработку и мониторинг информации о физическом объекте, позволяя тем самым, принимать решении о рациональном распределении ресурсов предприятия.

Постоянное повышение спроса на топливо и продукты его переработки стимулирует нефтегазовые компании внедрять и использовать новые технологии. Отрасль нефтегазовой промышленности в настоящее время заинтересована во внедрении и использовании беспроводных сенсорных сетей с целью оптимизации процессов исследования местности, добычи ресурсов, их переработки, транспортировки и сбыта.

Основным средством транспортировки нефтегазового сырья являются трубопроводы, которые подвержены воздействию внешних факторов, таких как коррозия, воздействие окружающей среды, производственный брак и др. Кроме этого в трубопроводах нефтегазовой отрасли могут возникать места утечки, влекущие за собой потери производства и экологическую угрозу. Так, например, разлив нефти, нарушает многие естественные процессы природы, гибнут животные, уничтожается растительность, зоны поражения становятся непригодными для обитания живых существ. Утечка сырья в водоемах, образует нефтяную пленку, которая сокращает доступ к кислороду и меняет состав воды, загрязняет питьевую воду, всё это влечет за собой необратимые последствия. Помимо этого, многие утечки трудно обнаружить, не имея специализированного оборудования, например, утечки природного газа, не имеющего запаха. Поэтому крайне важным является мониторинг трубопроводов нефтегазовой отрасли на предмет утечек, повреждений и повышения давления.

Решение на основе беспроводных сенсорных сетей помогут решить данные проблемы, позволяя проводить мониторинг и прогнозирование нарушений [1]. Применение беспроводных датчиков позволяет отслеживать

состояние трубопровода в режиме реального времени, что дает возможность вовремя выявить те или иные отклонения.

В работе рассмотрены области применения беспроводных сетей в нефтегазовой отрасли, выделены отличительные особенности и недостатки их применения. Выявлено, что основной проблемой развертывания беспроводной сенсорной сети является низкая энергоёмкость автономного источника питания сенсорного устройства [2, 3]. Таким образом, снижение энергопотребления беспроводных сенсорных сетей является важной задачей.

Анализ существующих исследований показал, что при подсчете энергии, затрачиваемой сенсорным устройством на передачу пакета данных зачастую, не учитывается ослабление сигнала передачи, вызванное препятствиями на пути сигнала. Данный параметр напрямую влияет на точность прогнозируемых данных. В связи с этим, в работе предложена пространственно-энергетическая модель беспроводной сенсорной сети, позволяющая рассчитать энергопотребление сети с учётом ослабления сигнала.

На рис. 1 представлен график затрачиваемой мощности с учетом ослабления сигнала (P_c) и мощности без учета ослабления сигнала ($P_{\text{пер}}$) при разных значениях частоты потока сигнала.

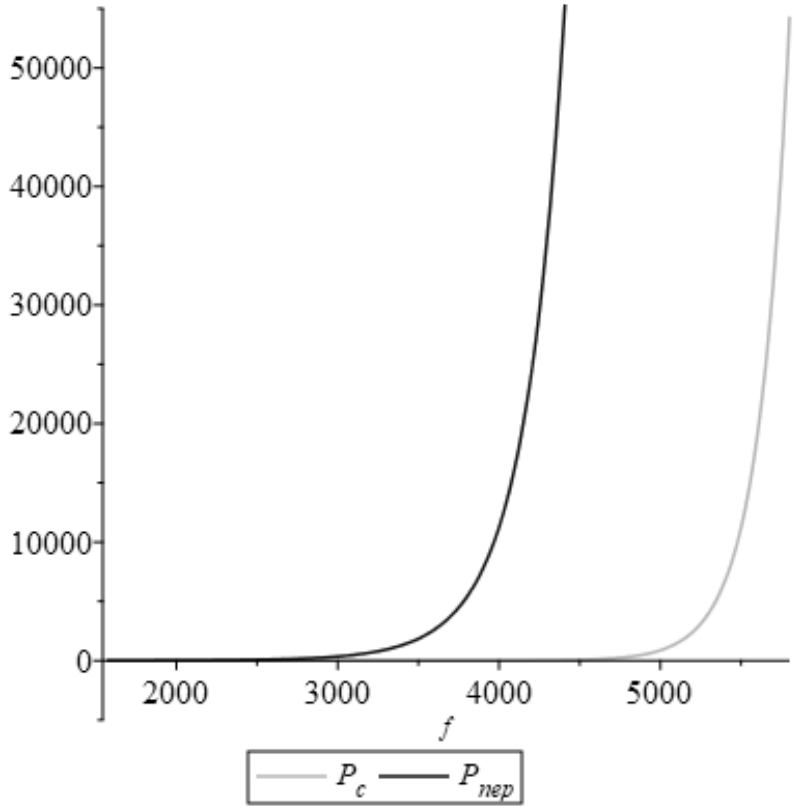


Рис. 1. Зависимость мощностей передающей антенны от частоты потока сигнала

Полученные данные подтверждают предположении о точности прогнозируемых данных. Таким образом, при проектировании и моделировании беспроводных сенсорных сетей для нефтегазовой отрасли, при подсчете параметров энергопотребления следует учитывать медианное ослабление сигнала.

Заключение. В работе отмечается, что в условиях большинства отраслей промышленности, в том числе и нефтегазовой, сложно создать идеальные условия для развертывания БСС. Застройки, особенности рельефа могут играть значительную роль при передаче сигнала. В связи с этим, при проектировании и моделировании беспроводных сенсорных сетей для отраслей промышленности, стоит учитывать ослабление сигнала. Это позволит увеличить точность прогнозируемых данных при планировании энергозатрат сети и помо-жет распределить нагрузку внутри сети.

СПИСОК ЛИТЕРАТУРЫ

1. Астахова Т. Н., Верзун Н. А., Колбанев М. О., Полянская Н. А., Шамин А. А. Вероятностно-энергетические характеристики взаимодействия умных вещей // Вестник НГИЭИ. 2019. №. 4 (95)
2. Research on the energy characteristics of routing in wireless sensor networks / T. Astakhova, D. Kirilova, A. Shamin, M. Kolbanev // CEUR Workshop Proceedings : 11, Saint Petersburg, 12–13 декабря 2019 года. Saint Pe-tersburg, 2020.
3. Астахова Т. Н., Зуева С. В., Кривоногов С. В., Романова А. А. Проектирование умного устройства, анализирующего выделение паров пропана для автомобилей, работающих на газомоторном топливе. 2021. Т. 9. № 9. С. 103-108.

УДК 621.396

АЛГОРИТМ РЕШЕНИЯ ДИФРАКЦИОННОЙ ЗАДАЧИ С ПРИМЕНЕНИЕМ МЕТОДА КОНЕЧНЫХ РАЗНОСТЕЙ ВО ВРЕМЕННОЙ ОБЛАСТИ

Мешалкин Валентин Андреевич, Коньков Денис Иванович,
Шанин Александр Михайлович, Тарасов Антон Александрович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий, пр., 3, Санкт-Петербург, 194064, Россия
e-mails: den.konkov.94@mail.ru, otesalex@yandex.ru, osmiy187@yandex.ru

Аннотация. Рассматривается алгоритм решения задачи дифракции с помощью метода конечных разностей во временной области.

Ключевые слова: численные методы; метод конечных разностей во временной области; дифракция; электромагнитное поле; поглощающие граничные условия.

ALGORITHM FOR SOLVING THE DIFFRACTION PROBLEM USING THE FINITE DIFFERENCE METHOD IN THE TIME DOMAIN

Meshalkin Valentin, Konkov Denis, Shanin Alexander, Tarasov Anton
Military Academy of Communications. Marshal of the Soviet Union S.M. Budyonny
Tikhoretsky, pr., 3, St. Petersburg, 194064, Russia
e-mails: den.konkov.94@mail.ru, otesalex@yandex.ru, osmiy187@yandex.ru

Absrtact. An algorithm for solving the diffraction problem using the finite difference method in the time domain is considered.

Keywords: numerical methods; time domain finite difference method; diffraction; electromagnetic field; absorbing boundary conditions.

Введение. С необходимостью решения задач дифракции встречаются при решении широкого круга задач электродинамики, например, проектировании и анализе антенных устройств, исследовании распространения радиоволн в неоднородных средах и т. д. В последние десятилетия, в связи с развитием вычислительной техники, широкое распространение получают численные методы решения подобных задач.

Метод конечных разностей во временной области (КРВО) один из перспективных численных методов. Данный метод широко применяется для анализа различных антенных устройств, при решении дифракционных задач на неоднородных структурах, при некоторой модификации его можно использовать для анализа сосредоточенных элементов и т.д. Метод КРВО в чистом виде предназначен для расчетов полей в ближней зоне, анализ которой является наиболее сложным.

В настоящее время разработан ряд приемов, позволяющих анализировать и дальнюю зону, что делает данный метод весьма универсальным, позволяющим решать практически любые задачи электродинамики.

Суть данного метода изложена в ряде работ зарубежных и российских авторов [1–10]. Поэтому подробное описание основных его положений не является целью данной статьи, ее цель - изложение алгоритма оценки дифракционной составляющей (ЭМП) и описание некоторых особенностей использования численного метода КРВО.

Основные шаги предлагаемого алгоритма сформулированы следующим образом:

1. Ввод исходных данных;
2. Выбор размеров расчетной области необходимой для обеспечения расчетов;
3. Задание объекта в счетном объеме;
4. Создание двух расчетных областей: одна с объектом исследования (область 1) и точно такая же без объекта (свободное пространство или область 2);
5. Расчет методом КРВО электромагнитных полей в областях 1 и 2;
6. Вычисление дифракционной составляющей поля;
7. Расчет характеристики рассеяния по дифракционной составляющей ЭМП.

Рассмотрим более подробно каждый шаг алгоритма.

1. Исходные данные состоят из трех групп:

–по первичному полю;

–по среде распространения;

–по исследуемому объекту.

Ввод исходных данных по первичному полю заключается во введении: длинны волны, амплитуды и поляризации. Причем, поляризация падающей волны задается путем присвоения первоначальных значений одной из составляющих поля электромагнитной волны E_x, E_y, E_z (H_x, H_y, H_z).

По среде распространения задаются: диэлектрическая проницаемость ε_1, удельная проводимость σ_1, магнитная проницаемость μ_1.

По исследуемому объекту задаются размеры частей, форма объекта (частей объекта), параметры материала объекта ε_2, μ_2, σ_2.

2. Размеры счетного объема определяются исходя из следующих условий:

1) размеров исследуемого объекта и расстояния необходимого для определения требующихся характеристик;

2) необходимой точности вычислений и максимального размера доступной оперативной памяти ЭВМ;

3) максимального времени расчета.

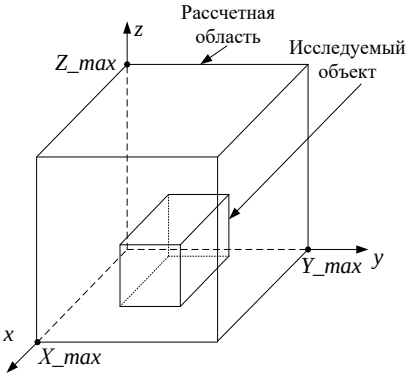


Рис. 1. Расположение исследуемого объекта в счетном объеме

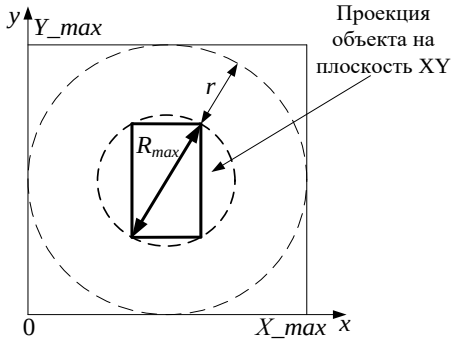


Рис. 2. Определение размера счетного объема

Поясним каждое из условий.

1) Размер счетного объема требуется задать таким, чтобы в него помещался исследуемый объект плюс расстояние необходимое для определения требуемых характеристик. Например, для нахождения характеристики направленности или в данном случае характеристики рассеяния объекта необходимо проводить расчет в дальней зоне [9–11]: $2\pi r \gg \lambda \quad \Rightarrow \quad r \gg \lambda/(2\pi)$, где r — расстояние необходимое для определения характеристики рассеяния.

Исходя из сказанного выше, размер счетного объема должен быть (рис. 1, 2): $L_{\max} \geq R_{\max} + 2r$, где $R_{\max}$ — максимальный линейный размер объекта; $L_{\max}$ - размер расчетной области по любой из координат (x, y, z).

В элементах КРВО размер расчетной области определяется следующим образом

$$NX = \frac{X_{\max}}{\Delta x}, \qquad NY = \frac{Y_{\max}}{\Delta y}, \qquad NZ = \frac{Z_{\max}}{\Delta z} \tag{1}$$

где Δx, Δy, Δz — линейные размеры ячейки КРВО.

2) Из (1) получаем размеры расчетной области в ячейках КРВО $NX \times NY \times NZ$. И здесь, при определении шага дискретизации приходится выбирать исходя из двух противоречивых условий — с одной стороны требуется обеспечить как можно меньшую погрешность вычислений, с другой стороны необходимо уложиться в доступную оперативную память ЭВМ.

Экспериментальные исследования зависимости погрешности расчетов метода КРВО от величины элемента разбиения пространства при кубической ячейке ($\Delta x = \Delta y = \Delta z$) показали, что чем меньше пространственный шаг, тем меньше погрешность вычислений. Эта закономерность наблюдается до тех пор, пока при очень мелкой сетке изменения составляющих ЭМП от одного элемента пространства до другого становится меньше разрядности электронной вычислительной машины (ЭВМ), тогда погрешность вычислений резко возрастает.

Если выбранный шаг дискретизации достаточно мелкий и размер расчетной области очень большой, то количество элементов станет таким, что оперативной памяти ЭВМ может не хватить для обработки имеющихся массивов информации. Это ограничение по доступной памяти ЭВМ является одним из ключевых в сдерживании широкого использования метода КРВО.

3) В настоящее время ЭВМ обладают достаточно большим объемом оперативной памяти, что позволяет производить расчеты областей достаточных для широкого спектра задач. При нехватке оперативной памяти это ограничение можно обойти различными программными методами, например, сохранять промежуточные результаты на жесткий диск. Но подобные ухищрения по увеличению счетного объема приводят к резкому увеличению времени, затрачиваемого на просчет одного временного шага, что тоже существенно ограничивает применение метода КРВО при обработке больших счетных объемов.

3. Разработка цифровых моделей объектов является отдельной сложной инженерной задачей, и в данной работе ее мы рассматривать не будем. Остановимся лишь на особенностях задания модели объекта в методе КРВО.

В счетном объеме объект задается путем присвоения ячейкам пространства, соответствующим форме исследуемого объекта, значений параметров материала объекта ε_2, μ_2, σ_2. Причем, обозначение параметров материала, из которого изготовлен объект ε_2, μ_2, σ_2 являются обобщенными, их индексы показывают лишь то, что они принадлежат объекту. На самом деле каждой *i*-й части объекта соответствуют свои ε_{2i}, μ_{2i}, σ_{2i}, которые характеризуют материал, из которого именно эта часть объекта изготовлена.

Преимуществом метода КРВО является удачное разбиение пространства. Из ячеек-параллелепипедов можно «собрать» объект практически любой формы. Если получается так, что размеры ячейки крупнее какой-либо детали объекта, то, если это не принципиально, данную деталь можно заменить целой ячейкой. Или если эта деталь является важной, то на этот случай можно использовать метод КРВО с переменными размерами расчетной сетки, и задать требующуюся деталь более точно [8].

4. Создаются две расчетных области одинакового размера $NX \times NY \times NZ$ с одинаковыми параметрами среды распространения ε_1, μ_1, σ_1. В одной из областей задается объект исследования по п. 3. Назовем область с объектом — область 1 (рис. 1), область без объекта — область 2. В каждой из областей задается падающая плоская волна с одинаковыми параметрами из п. 1.

5. В методе КРВО расчет ЭМП происходи пошагово по всему пространству с временным шагом Δt, который определяется из условия (условие Куранта–Фридрихса–Леви) [3-4]:

$$\Delta t \le \left(c \cdot \sqrt{\left(1/\Delta x^2 + 1/\Delta y^2 + 1/\Delta z^2\right)} \right)^{-1}$$

Причем, расчеты поля в определенной точке пространства (расчетной области) являются достоверными, если через нее прошло несколько полных длин волн. Экспериментальные исследования показывают, что для установки стационарного режима число полных волн пройденных через точку должно быть не меньше двух.

Каждая из составляющих ЭМ поля считается через четыре соседних, так происходит по всему счетному объему. Но на гранях расчетной области их есть только три, а на ребрах и вовсе две, поэтому правильно вычислить поле на границах без специальных действий не представляется возможным.

Такие специальные действия называются поглощающие или абсорбирующие граничные условия (ПГУ). Сравнение работы ПГУ различных типов проводилось в [3], там показано преимущество самых сложных в реализации ПГУ типа PML (Perfectly Matched Layer — идеально согласованный слой) перед остальными. Исходя из этого сравнения, в условиях данной задачи требуется использовать ПГУ типа PML, при использовании других неизбежно возникают отражения от границ расчетной области, что приводит к искажению результатов.

6. На каждом временном шаге производится вычитание полей, полученных в областях 1 и 2. В результате разности получаем дифракционную составляющую суммарного поля области 1.

7. В данной работе нас интересует получение характеристики рассеяния объекта. Имея значения, составляющих ЭМП ее можно вычислить следующим образом рис. 3 [11]:

$$F(\theta,\varphi) = \left|E(\theta,\varphi)\right| / \left|E_{\max}(\theta_0,\varphi_0)\right| \qquad (2)$$

где $F(\theta,\varphi)$ — трехмерная нормированная амплитудная характеристика рассеяния объекта; $E(\theta,\varphi)$ — амплитуда электрической напряженности ЭМП, в зависимости от угла наблюдения, взятая на определенном радиусе; $E_{\max}(\theta_0,\varphi_0)$ — максимальное значение амплитуды электрической напряженности ЭМП по модулю; θ – угол места; φ — азимут; θ_0, φ_0 — направление максимального излучения.

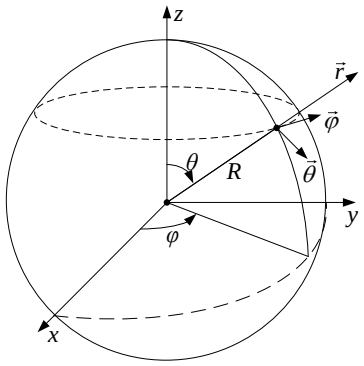


Рис. 3. Пояснение к определению характеристики рассеяния объекта

Заключение. Проверка данного алгоритма была проведена путем решения нескольких классических задач дифракции (дифракция на проводящем цилиндре бесконечной длинны, дифракция на проводящей сфере, дифракция на сфере из диэлектрика). Результаты, полученные численно, сравнивались с аналитическими решениями. Относительная погрешность вычислений не превышала 10% при шаге дискретизации пространства $\Delta x = \Delta y = \Delta z = \lambda / 20$, что позволяет сделать вывод о возможности использования данного алгоритма для решения задач дифракции на неоднородных телах сложной формы.

СПИСОК ЛИТЕРАТУРЫ

1. Taflove A. Computational Electrodynamics: the finite-difference time-domain method. Boston-London: Artech House, 1995.
2. Зеленин А.В. Вычисление электромагнитного поля в дальней зоне с использованием метода FDTD и интеграла Кирхгофа, «Технология ЭМС». СПб. : 2 кв. 2006.
3. Гринев А. Ю., Гиголо А. И. Математические основы и методы решения задач электродинамики. М., 2015. 216 с.
4. Липатников В. А., Парфиров В. А. Вероятностно-временные показатели процесса выявления сетей радиосвязи. Инновационные технологии и технические средства специального назначения // Труды XV научно-практической конференции : в 2-х т. Сер. »Библиотека журнала «Военмех. Вестник БГТУ»«. СПб., 2023. С. 172-175.
5. Шанин А. М. Взаимное влияние элементов защищенных активных фазированных антенных решёток // Теория и техника радиосвязи. 2022. № 4. С. 73-79.
6. Мешалкин В. А. Решение задач электродинамики с помощью вычислительного эксперимента // Прикладные информационные аспекты медицины. 2016. Т. 2. № 11. С. 80.
7. Шанин А. М. Модель передающего радиоцентра на основе принципа электродинамического подобия // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2023. № 5-6(179-180). С. 71-78.
8. Рыжов М. В., Токарев С. М., Беляцкий А. И. Соотношения между пространственными и временной решетками в методе конечных разностей во временной области. СПб. : сборник докладов 57 НТК НТОРЭС, 2002.
9. Пименов Ю. В., Вольман В. И., Муравцов А. Д. Техническая электродинамика / под ред. Ю. В. Пименова : учеб. пособие для вузов. М. : Радио и связь, 2002.
10. Петров Б. М. Электродинамика и распространение радиоволн : учебник для вузов. 2-е изд., испр. М.: Горячая линия Телеком, 2003.
11. Мешалкин В. А., Сосунов Б. В., Филиппов В. В. Поля и волны в задачах разведзащищенности и радиоэлектронной защиты систем связи. СПб. : ВАС, 1993.

УДК 004.738

ПОСТРОЕНИЕ ТАБЛИЦ МАРШРУТИЗАЦИИ ОДНОРАНГОВОЙ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ

Миклуш Виктория Александровна
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, Санкт-Петербург, 190121, Россия
e-mail: miklush-v@yandex.ru

Аннотация. Рассматривается актуальная задача актуализации маршрутных таблиц с учетом меняющейся топологии беспроводной сенсорной сети. Рассмотрены два метода построения таблиц маршрутизации — вероятностный и детерминированный. Вероятностный метод учитывает наличие коллизий при получении информации, необходимой для построения таблицы маршрутизации. Детерминированный метод реализует каскадную последовательную схему опроса узлов, начиная от центрального узла. Выведены математические выражения, позволяющие оценить время построения таблицы маршрутизации обоими методами.

Ключевые слова: беспроводная сенсорная сеть; меняющаяся топология; таблица маршрутизации; дерево маршрутов.

ROUTING TABLES CONSTRUCTING OF A PEER-TO-END WIRELESS SENSOR NETWORK

Miklush Vuktoria
Saint Petersburg State University of Aerospace Instrumentation
67 Bolshaya Morskaya St, St. Petersburg, 190121 Russia
email: miklush-v@yandex.ru

Abstract. The actual problem of updating routing tables is considered considering the changing topology of the wireless sensor network. Two methods for constructing routing tables are considered - probabilistic and deterministic. The probabilistic method considers the presence of collisions when obtaining the information necessary to build the routing table. The deterministic method implements a cascade sequential scheme for polling nodes, starting from the central node. Mathematical expressions are derived that allow estimating the time of building the routing table by both methods.

Keywords: wireless sensor network; changing topology; routing table; route tree.

Введение. Топология беспроводных сенсорных сетей (БСС) не является стационарной. Соответственно, со временем меняются и пути доставки данных от узла-источника (И-узла) к узлу-адресату (А-узлу). Поэтому необходимо периодически обновлять таблицу маршрутизации с целью поиска эффективных маршрутов [1].

В одноранговых БСС (Mesh сетях) применяется алгоритм маршрутизации AODV (Ad hoc On-demand Distance Vector), основанный на периодической оценке вектора расстояний по требованию узла, инициировавшего передачу данных [2].

Представим БСС в виде графа на рис. 1. На каждом узле БСС инициируется локальная таблица маршрутизации, в которую записывается адрес А-узла и адреса соседних узлов (находящихся на расстоянии одного хопа). Если И-узел при обращении к своей локальной таблице маршрутизации не обнаруживает среди соседей А-узел, то запускается процедура поиска эффективного маршрута к А-узлу.

Построение таблицы маршрутизации. Известный два метода построения маршрутных таблиц: вероятностный и детерминированный. Вероятностный метод подразумевает наличие коллизий при отправке узлами пакетов с информацией, необходимой для построения таблицы маршрутизации. Поэтому, если через узел 7 БСС, изображенной на рис. 1 раньше придет пакет от узла 8, то маршрут через узел 5 будет считаться резервным, а через узел 8 — кратчайшим. Детерминированный метод подразумевает отсутствие возникновения коллизий, поскольку для опроса каждого узла выделяется свое временное окно. В итоге все узлы будут опрошены и построено дерево всех возможных маршрутов узлов до любого узла назначения.

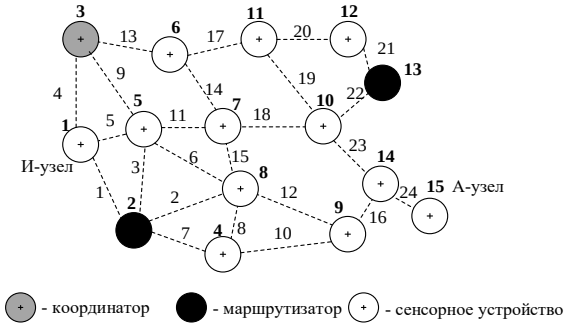


Рис. 1. К построению маршрутов от И-узла к А-узлу

Процесс построения таблицы маршрутизации начинается с широковещательной рассылки пакета инициализации от центрального узла, например, маршрутизатора или координатора.

При реализации вероятностного метода построения таблицы маршрутизации узлы, получившие пакет инициализации, записывают в свою локальную память уникальный номер беспроводной сенсорной сети, адрес координатора и адрес источника рассылки — родительского узла, от которого непосредственно получен пакет инициализации.

Узел, принявший пакет инициализации начинает формировать пакет подтверждения, в котором конечным адресатом указывается центральный узел, а промежуточным адресатом — родительский узел.

Любой узел, получающий пакет подтверждения, считывает из него адрес промежуточного узла и сравнивают его с собственным адресом. Если адреса не совпадают, то вместо считанного промежуточного адреса узел записывает адрес своего родительского узла и т.д., пока пакет подтверждения не достигнет центрального узла.

При получении пакетов подтверждений в центральном узле начинается процесс регистрации узлов и строится топология БСС типа «дерево», на базе которой строится таблица маршрутизации.

Для БСС, приведенной на рис. 1 топология, построенная от узла 2 (маршрутизатора БСС) приведена на рис. 2. Пунктирной линией выделены возможные узлы и каналы, которые подвергаются коллизиям.

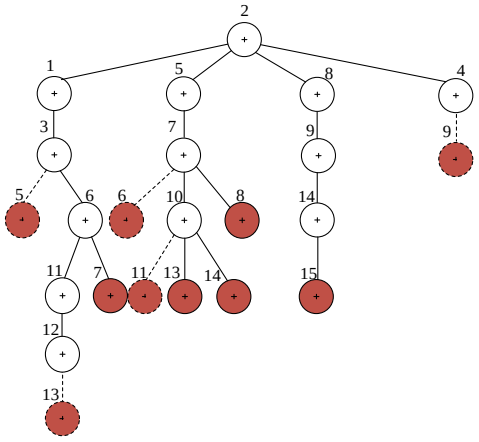


Рис. 2. Дерево маршрутов, построенных от маршрутизатора – узла 2

При передаче пакетов подтверждений возможны случаи возникновения коллизий — когда два и более пакета в один и тот же промежуток времени передаются на один узел. Для устранения коллизий пакетов применяется метод множественного доступа с контролем несущей CSMA (Carrier Sense Multiple Access) [3]. При возникновении условий для передачи данных, узел начинает прослушивать канал передачи с целью определения состояния канала — свободен или занят. Прослушивание продолжается в течение временного окна τ, с. Если канал свободен, то узел начинает передачу данных длиной L (размер пакета, бит) со скоростью канала V бит/с. После передачи данных узел еще определенное время θ, с занимает канал — это время выделяется для приема пакета принимающим узлом. Если канал занят, то узел ожидает случайное время $\sigma > L/V + \theta$ и делает повторную попытку прослушивания канала. Число попыток может быть ограничено. По их истечении пакет считается потерянным или отправляется по резервному пути [4, 5].

Таким образом, время построения таблицы маршрутизации вероятностным методом составит

$$t_{r.p} = \sum_{i=1}^{n} \frac{L}{V_i} + \sum_{i=1}^{n} \left(\tau + \frac{L}{V_i} + \theta \right) + \sum_{j=1}^{k} (\tau + \sigma), \tag{1}$$

где n – число хопов (ретрансляций) от центрального узла до самого удаленного узла БСС;

k — число повторных передач пакета подтверждения при возникновении коллизии.

Процесс построения таблицы маршрутизации детерминированным методом начинается с отправки центральным узлом (координатором или маршрутизатором) пакета инициализации всем узлам БСС. Узлы отвечают пакетом подтверждением, но не все сразу, а по каскадной схеме. Центральный узел сначала вносит запись в таблицу маршрутизации об узлах первого круга — узлах, находящихся на расстоянии одного хопа от центрального узла. При этом опрос узлов первого круга происходит последовательно. В свою очередь каждый узел первого круга рассылает пакет инициализации своим соседям — узлам, находящимся на расстоянии одного хопа от него и также последовательно принимая от них пакет подтверждения, заносит нужную информацию в свою локальную таблицу маршрутизации и передает пакет выше на центральный узел. Опрос узлов второго и последующих кругов происходит аналогично. Таблица маршрутизации считается построенной, когда опрошены все узлы БСС. Очевидно, что процесс построения таблицы маршрутизации занимает достаточное время, которое зависит от масштаба БСС и технических возможностей узлов БСС.

Если принять, что на рис. 3 функции построения таблицы маршрутизатора выполняет узел 2, то первым кругом являются узлы 1, 4, 5 и 8. Последовательно опрашивая первый круг, узел 2 получает информацию об их ближайших соседях — узлах 3, 7 и 9. Через опрос узлов второго круга определяются узлы третьего круга — 6, 10 и 14, опросив узлы третьего круга определяется четвертый круг — узлы 11 и 15, опросив узлы четвертого круга определяются узлы пятого круга — 12 и 13 и опросив узлы 12 и 14 центральный узел (узел 2), не получив ответа, заканчивает построение таблицы маршрутизации.

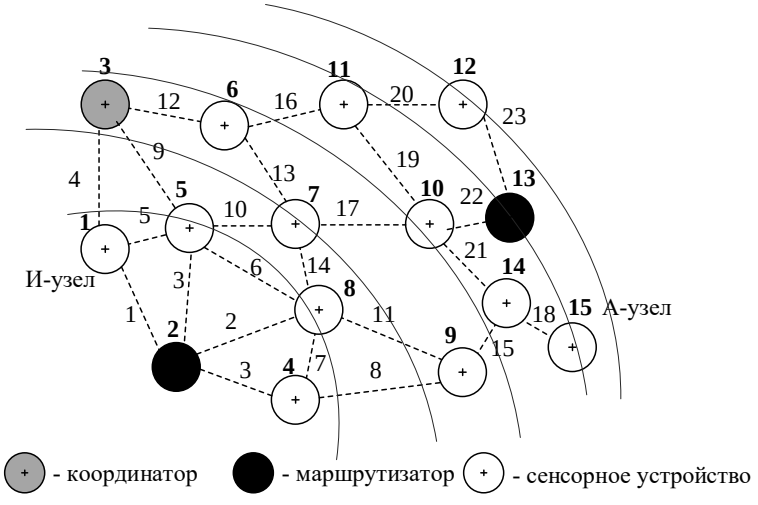


Рис. 3. К построению маршрутов детерминированным методом

На рис. 4 приведено дерево маршрутов, построенных от узла 2 детерминированным методом.

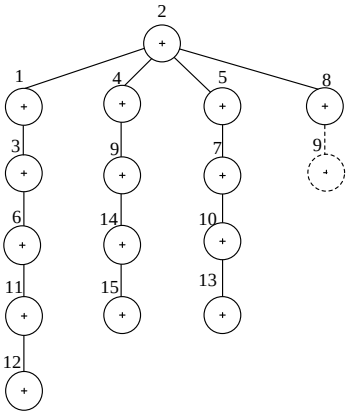


Рис. 4. Дерево маршрутов, построенных от маршрутизатора 2

Поскольку узлы опрашиваются последовательно центральным узлом, то коллизии возможны только при отправке пакетов подтверждения узлами БСС. Для разрешения коллизий предлагается использовать метод множественного доступа с разделением по времени TDMA (Time Division Multiple Access) [3]. Каждый узел посылает пакет только в свой временной слот.

Таким образом, время построения таблицы маршрутизации детерминированным методом составит

$$t_{r.d} = \sum_{i=1}^{h}\sum_{j=1}^{m}\frac{L}{V_j} + \sum_{j=1}^{m}\frac{L}{V_j}, \qquad (2)$$

где h — число каскадов (кругов) опроса центральным узлом;
m — число узлов в j-м круге.

СПИСОК ЛИТЕРАТУРЫ

1. Миклуш В. А., Татарникова Т. М. Имитационная модель одноранговой беспроводной сенсорной сети // T_Comm: Телекоммуникации и транспорт. 2023. Т. 17, № 3. С. 20-21.
2. Kraeva E., Miklush V., Palkin I., Tatarnikova T., Kunturov A. Information support in environmental monitoring systems // IOP Conference Series: Earth and Environmental Science. Сер. All-Russian Scientific-Technical Conference «Digital Technologies in Forest Sector». 2020. Vol. 507. Pp. 012-015.
3. Татарникова Т. М., Елизаров М. А. Процедура разрешения коллизий в RFID-системе // Известия высших учебных заведений. Приборостроение. 2017. Т. 60. № 2. С. 150-157.
4. Татарникова Т. М. Статистические методы исследования сетевого трафика // Информационно-управляющие системы. 2018. № 5(96). С. 35-43.
5. Татарникова Т. М. Миклуш В. А., Рудых С. В. Оценка показателей качества обслуживания беспроводных сенсорных сетей // Информация и Космос. 2022. № 4. С.2 1-27.

УДК 621.396.4

ФОРМИРОВАНИЕ ПОКАЗАТЕЛЕЙ ДЛЯ ТЕКУЩЕГО И ПРОАКТИВНОГО АНАЛИЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ТЕХНИЧЕСКОЙ НАДЕЖНОСТИ МОБИЛЬНЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Михайличенко Антон Валерьевич, Паращук Игорь Борисович, Селезнев Андрей Васильевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного,
Тихорецкий пр-т, д. 3, Санкт-Петербург, 194064, Россия
e-mails: toni09_91@mail.ru, shchuk@rambler.ru, andrsel@mail.ru

Аннотация. Рассматривается возможный подход к формулировке вероятностного комплексного показателя безопасности и технической надежности мобильных центров обработки данных на основе совместной условной вероятности выполнения требований к отклонениям его частных показателей надежности, характеризующих параметры безотказности, долговечности, ремонтопригодности и сохраняемости объекта такого класса. Проведен анализ потенциальных вариантов формулировки частных показателей и перспектив применения данного подхода для решения задач достоверного и оперативного оценивания и прогнозирования (проактивного контроля) безопасности и надежности современных мобильных центров обработки данных.

Ключевые слова: показатель технической надежности; проактивный анализ; мобильный центр обработки данных; требования; отклонения; условная вероятность; безотказность; ремонтопригодность.

FORMATION OF INDICATORS FOR THE CURRENT AND PROACTIVE ANALYSIS OF INFORMATION SECURITY AND TECHNICAL RELIABILITY OF MOBILE DATA CENTERS

Mikhailichenko Anton, Parashchuk Igor, Seleznev Andrey
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny,
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: toni09_91@mail.ru, shchuk@rambler.ru, andrsel@mail.ru

Abstract. A possible approach to the formulation of a probabilistic complex indicator of the technical reliability of mobile data centers based on the joint conditional probability of meeting the requirements for deviations of its particular reliability indicators characterizing the parameters of reliability, durability, maintainability and preservation of an object of this class is considered. The analysis of potential options for the formulation of particular indicators and the prospects of using this approach to solve the problems of reliable and operational assessment and forecasting (proactive control) of the reliability of modern mobile data centers is carried out.

Keywords: technical reliability indicator; proactive analysis; mobile data center; requirements; deviations; conditional probability; reliability; maintainability.

Введение. Анализ исследований в области контроля и управления современными мобильными центрами обработки данных (МЦОД) показывает, что сравнительная вероятностно-временная и многокритериальная оценка технической надежности таких сложных информационно-технических объектов непосредственно по частным показателям не только мало информативна, почти не применима в реальной практике, но и, зачастую, противоречива.

Между тем важность аспектов технической надежности МЦОД не вызывает сомнений, поскольку такие системы (центры) представляют собой согласованные по времени, задачам и развернутые на местности взаимосвязанные совокупности организационных и программно-аппаратных средств, предназначенных для создания высокопроизводительной и отказоустойчивой инфраструктуры, отвечающей за обработку и хранение информации. Небольшие затраты на транспортировку МЦОД и возможность их работы в любой местности являются важными достоинствами объектов такого класса. Мобильные центры обработки данных являются полноценными одномодульными аналогами классических центров обработки данных, но размещаются либо в специальном боксе на транспортной базе (автомобиль, судно, самолет), либо в специализированном транспортном контейнере (для перевозки железнодорожным, автомобильным или водным транспортом). Такие центры, как и их стационарные аналоги, оснащены комплексом информационной, телекоммуникационной и другой инженерной аппаратуры, подключены к каналам связи.

Помимо затрат на транспортировку, у МЦОД есть еще ряд достоинств:

Доступность вычислительных мощностей и ресурсов хранения данных для пользователей почти в любом месте их повседневной деятельности.

Модульная конструкция и комплексность технологического решения. Мобильный центр обработки данных изначально содержит в своем контейнере все необходимые компоненты: стойки с оборудованием, источники питания, системы охлаждения, кондиционирования, пожаротушения. В состав общего и системного программного обеспечения МЦОД также входят операционные системы, программные средства приема, обработки и отображения информации. Их тестируют и настраивают еще в процессе производства, поэтому доработки на месте минимальны.

Малые размеры — МЦОД не нужна развитая инженерная инфраструктура. Охлаждение и электроснабжение обеспечиваются за счет дополнительных микромодулей по периметру контейнера центра, поэтому для работы среднестатистического МЦОД достаточно горизонтальной площадки.

Невысокие энергозатраты (высокая энергоэффективность). За счет компактной установки внутри контейнера МЦОД всех вспомогательных систем, есть возможность экономить электроэнергию.

Низкая цена развертывания по сравнению с традиционными дата-центрами. Это возможно за счет того, что для развертывания МЦОД не нужны ни дополнительные материальные ресурсы организации, ни дополнительный штат специалистов. При этом срок службы такого МЦОД может составлять до 60 месяцев.

Время изготовления. На изготовление МЦОД в среднем требуется около 10 недель, это в разы быстрее строительства стандартного стационарного дата-центра.

Иными словами, мобильные центры обработки данных являются важным и эффективным инструментом в информационной инфраструктуре, а от их качества и технической надежности многое зависит в устойчивом, непрерывном и оперативном управлении.

Сложность сравнительной вероятностно-временной и многокритериальной оценки технической надежности таких сложных информационно-технических объектов связана с тем, что по одним показателям более надежным

может оказаться один МЦОД, а по другим — совсем другой мобильный дата-центр, с другим или даже с таким же набором элементов — средств и комплексов связи, хранения и обработки данных [1-3].

Этот объективный факт, затрудняющий оценку и связанный с многообразием и разноплановостью анализируемых и подлежащих текущему и проактивному контролю аспектов и показателей надежности технических (аппаратно-программных) систем, присутствует, несмотря на то, что существует целый ряд международных и национальных стандартов, определяющих не только методологические подходы к анализу надежности систем такого класса, но и примерный перечень параметров, по которым она могут быть оценена в целом, либо могут быть отдельно оценены такие аспекты технической надежности, как безотказность, долговечность, ремонтопригодность и сохраняемость [4, 5].

Помимо этого, приходится также учитывать субъективизм формулировки некоторых частных показателей технической надежности (ЧПТН), вносящий известную долю неопределенности в решение задач управления и вероятностно-временного оценивания безотказности, долговечности, ремонтопригодности и сохраняемости современных МЦОД [6, 7].

Выход из этой ситуации нам видится в формулировке и последующей текущей либо прогностической оценке вероятностного комплексного показателя технической надежности (КПТН) МЦОД, который бы функционально связывал все многообразие ЧПТН и требований к ним. Анализ различных методов формирования комплексных (обобщенных) показателей качества, надежности либо эффективности сложных систем показал, что наиболее полный учет особенностей решения задачи оценивания технической надежности МЦОД, а также естественное решение проблем нормализации и свертки систем показателей технической надежности (ПТН) достигается при применении метода вероятностной скаляризации [8, 9].

Сущность данного метода состоит в использовании в качестве КПТН совокупной (совместной) вероятности выполнения требований $p_{\text{вып птн}}(k)$, предъявляемых пользователем к технической надежности мобильного дата-центра на k-ом шаге его эксплуатации по безотказности, долговечности, ремонтопригодности и сохраняемости:

$$p_{\text{вып птн}}(k) = p(\Delta\vec{A}_{\text{птн}}(k) \le \Delta\vec{A}^{\text{тр}}_{\text{птн}}) \tag{1}$$

где $\Delta\vec{A}_{\text{птн}}(k)$ — вектор отклонений ПТН от требований на *k*-ом шаге эксплуатации МЦОД, а $\Delta\vec{A}^{\text{тр}}_{\text{птн}}$ — вектор требований к этим отклонениям.

Предпочтение, отданное данному методу, обусловлено учетом в нем случайного характера изменений основной массы ПТН МЦОД, а также практической возможностью автоматического решения основных проблем многокритериальной вероятностно-временной оценки качества, надежности и эффективности функционирования сложных технических систем (т.е., в нашем случае, возможностью нормализации компонент векторных ПТН МЦОД и их свертки) в рамках выбранного вероятностного подхода к анализу технической надежности [9].

Фундамент данного метода зиждется на пошаговом (поэтапном) расчете ЧПТН на любом *k*-ом шаге оценивания и их математически корректной «свертке» в КПТН МЦОД на этом же шаге. Математически метод может быть осуществлен на основе аппарата условных вероятностей, а также классических теорем функциональной и параметрической декомпозиции [9].

При этом вероятностный комплексный ПТН формируется из условных вероятностей выполнения требований к отклонениям ЧПТН МЦОД. Иными словами, для методики, учитывающей вероятностно-временную физическую сущность трансформации ПТН МЦОД на *k*-ом шаге его эксплуатации и, учитывая тот факт, что ПТН представляют собой отклонения параметров надежности от требуемых значений, КПТН $p_{\text{вып птн}}(k)$, опираясь на выражение (1), может быть аналитически записан как совместная условная вероятность выполнения требований к значениям отклонений показателей безотказности, долговечности, ремонтопригодности и сохраняемости МЦОД:

$$\begin{aligned} p_{\text{вып птн}}(k) = p_{\text{б}}(k)[(\Delta\vec{A}_{\text{б}}(k) \le \Delta A^{\text{тр}}_{\text{б}})/(\Delta\vec{A}_{\text{д}}(k) \le \Delta\vec{A}^{\text{тр}}_{\text{д}}) \bigcap (\Delta\vec{A}_{\text{р}}(k) \le \Delta\vec{A}^{\text{тр}}_{\text{р}}) \bigcap \\ \bigcap (\Delta\vec{A}_{\text{с}}(k) \le \Delta\vec{A}^{\text{тр}}_{\text{с}})] \times p_{\text{д}}(k)[(\Delta\vec{A}_{\text{д}}(k) \le \Delta\vec{A}^{\text{тр}}_{\text{д}}) / (\Delta\vec{A}_{\text{р}}(k) \le \Delta\vec{A}^{\text{тр}}_{\text{р}}) \bigcap \\ \bigcap (\Delta\vec{A}_{\text{с}}(k) \le \Delta\vec{A}^{\text{тр}}_{\text{с}})] \times p_{\text{р}}(k)[(\Delta\vec{A}_{\text{р}}(k) \le \Delta\vec{A}^{\text{тр}}_{\text{р}}) / \\ / (\Delta\vec{A}_{\text{с}}(k) \le \Delta\vec{A}^{\text{тр}}_{\text{с}})] \times p_{\text{с}}(k)[(\Delta\vec{A}_{\text{с}}(k) \le \Delta\vec{A}^{\text{тр}}_{\text{с}})], \end{aligned} \tag{2}$$

где $\Delta\vec{A}_{\text{б}}(k)$, $\Delta\vec{A}_{\text{р}}(k)$, $\Delta\vec{A}_{\text{д}}(k)$, $\Delta\vec{A}_{\text{с}}(k)$, $\Delta\vec{A}^{\text{тр}}_{\text{б}}$, $\Delta\vec{A}^{\text{тр}}_{\text{р}}$, $\Delta\vec{A}^{\text{тр}}_{\text{д}}$ и $\Delta\vec{A}^{\text{тр}}_{\text{с}}$ — вектора показателей безотказности, долговечности, ремонтопригодности и сохраняемости соответственно (в виде их отклонений от требований) на k-ом шаге эксплуатации МЦОД и вектора соответствующих требований; $p_{\text{б}}(k),\ p_{\text{р}}(k),\ p_{\text{д}}(k)$ — условные

вероятностей выполнения требований к отклонениям показателей безотказности, долговечности и ремонтопригодности на k-ом шаге эксплуатации МЦОД, определяемые с учетом (при условии) выполнения требований к отклонениям показателей сохраняемости; $p_{\text{с}}(k)$ — безусловная вероятность выполнения требований к отклонениям показателей сохраняемости на k-ом шаге эксплуатации МЦОД.

При этом вариант формулировки отдельного вероятностного частного ПТН, характеризующего, например, такой аспект (грань) надежности МЦОД, как безотказность, может быть представлен в виде условной вероятности выполнения требований на *k*-ом шаге эксплуатации МЦОД к отклонениям значений вероятности безотказной работы $\Delta p_{\text{бр}}(k)$, средней наработки до отказа $\Delta T_{\text{ср}}(k)$, средней наработки на отказ $\Delta T_{\text{о}}(k)$ и интенсивности потока отказов $\Delta\lambda_{\text{по}}(k)$, рассчитываемой при условии выполнения требований, например, к отклонениям одного из ключевых параметров безотказности — средней доли безотказной наработки $\Delta I(k)$:

$$
\begin{gathered}
p_{\text{б}}(k) = p(\Delta\vec{A}_{\text{б}}(k) \le \Delta\vec{A}_{\text{б}}^{\text{тр}}) = \\
p_{\text{б/сд}}(k)[(p_{\text{бр}}(\Delta p_{\text{бр}}(k) \le \Delta p_{\text{бр}}^{\text{тр}}) \cap p_{\text{ср}}(\Delta T_{\text{ср}}(k) \le \Delta T_{\text{ср}}^{\text{тр}}) \cap \\
p_{\text{о}}(\Delta T_{\text{о}}(k) \le \Delta T_{\text{о}}^{\text{тр}}) \cap p_{\text{ипо}}(\Delta\lambda_{\text{по}}(k) \le \Delta\lambda_{\text{по}}^{\text{тр}}) / (\Delta I(k) \le \Delta I^{\text{тр}})] \times \\
\times p_{\text{сдбн}}(k)[(\Delta I(k) \le \Delta I^{\text{тр}})],
\end{gathered}
\tag{3}
$$

где $p_{\text{б/сд}}(k)$ — совместная (по вероятности безотказной работы $p_{\text{бр}}(\Delta p_{\text{бр}}(k) \le \Delta p_{\text{бр}}^{\text{тр}})$ и вероятностям выполнения требований к отклонениям средней наработки до отказа $p_{\text{ср}}(\Delta T_{\text{ср}}(k) \le \Delta T_{\text{ср}}^{\text{тр}})$, средней наработки на отказ $p_{\text{о}}(\Delta T_{\text{о}}(k) \le \Delta T_{\text{о}}^{\text{тр}})$ и интенсивности потока отказов $p_{\text{ипо}}(\Delta\lambda_{\text{по}}(k) \le \Delta\lambda_{\text{по}}^{\text{тр}})$) условная вероятность выполнения требований к отклонениям показателей безотказности (без учета средней доли безотказной наработки) на *k*-ом шаге эксплуатации МЦОД, определяемая при условии выполнения требований к отклонениям значений средней доли безотказной наработки; $p_{\text{сдбн}}(k)[(\Delta I(k) \le \Delta I^{\text{тр}})]$ — безусловная вероятность выполнения требований к отклонениям средней доли безотказной наработки МЦОД.

Аналогичные показатели могут быть сформулированы и для информационной безопасности МЦОД.

Заключение. Таким образом, можно с большой долей уверенности утверждать, что, с учетом оговоренных ограничений на множество ПТН, формулировка вероятностного комплексного ПТН может быть осуществлена на основе условных вероятностей выполнения требований к отклонениям частных показателей надежности МЦОД, характеризующих его безотказность, долговечность, ремонтопригодность и сохраняемости. Предложен вариант формулировки ЧПТН, включающий условную вероятностную меру выполнения требований к отклонениям частных параметров безотказности.

Рассмотренный подход обладают универсальностью, а сочетание метода вероятностной скаляризации и математического аппарата условных вероятностей обуславливает перспективы в вопросах достоверного и оперативного проактивного анализа надежности современных мобильных центров такого класса.

СПИСОК ЛИТЕРАТУРЫ

1. Андреев А. В. Яковлев В. В., Короткая Т. Ю. Теоретические основы надежности технических систем : учебное пособие. СПб. : Изд. Полит. ун-та, 2018. 164 с.
2. Изергина А. Р. Обзор статистических методов оценки надежности // Математические модели современных экономических процессов, методы анализа и синтеза экономических механизмов. Актуальные проблемы и перспективы менеджмента организаций в России : сб. ст. XII Всерос. науч.-практ. конф. Самара : Изд-во СамНЦ РАН, 2018. С. 45-50.
3. Паращук И. Б., Михайличенко Н. В., Михайличенко А. В. Нейро-нечеткие сети и алгоритмы гранулярных вычислений в задачах интеллектуальной обработки данных для оценки надежности мобильных дата-центров // Применение искусственного интеллекта в информационно-телекоммуникационных системах. Сб. материалов научно-практической конференции. СПб. : ВАС, 2021. С. 110-115.
4. Межгосударственный стандарт ГОСТ 27.002-2015 Надежность в технике. Термины и определения. М. : Стандартинформ., 2016. 30 с.
5. Национальный стандарт РФ ГОСТ Р 51901.5-2005 (МЭК 60300-3-1:2003) Менеджмент риска. Руководство по применению методов анализа надежности. М. : Стандартинформ., 2005. 44 с.
6. Паращук И. Б., Михайличенко А. В., Крюкова Е. С. Анализ зашумленных и неоднородных данных о значениях параметров надежности дата-центров // Современные технологии: актуальные вопросы теории и практики : сборник статей Международной НПК. Пенза: МЦНС «Наука и Просвещение», 2021. С. 74-77.
7. Паращук И. Б., Башкирцев А. С., Михайличенко Н. В. Анализ уровней и видов неопределенности, влияющей на принятие решений по управлению информационными системами // Информация и космос. № 1, 2017. С. 112-120.
8. Надежность и эффективность в технике. Т. 3. Эффективность технических систем / под ред. В. Ф. Уткина и Ю. В. Крючкова. М. : Машиностроение, 1988. 328 с.
9. Терентьев В. М., Санин Ю. В. Анализ эффективности функционирования автоматизированных сетей многоканальной радиосвязи. СПб. : ВАС, 1992. 80 с.

УДК004.056.5

АНАЛИЗ И ОЦЕНКА БЕЗОПАСНОСТИ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА С ПОМОЩЬЮ DIRECTUM RX

Найданов Данил Евгеньевич, Яровой Николай Алексеевич, Ярош Артем Андреевич
Филиал Военного учебно-научного центра Военно-воздушных сил
«Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина
Городок 11 ул., 1, Челябинск, 454015, Россия
e-mails: s123.ert@yandex.ru, aros32495@gmail.com

Аннотация. В статье рассматривается определение следующих наборов базовых функций электронного ДКО создание документов в электронном виде. Решение о выборе той или иной СЭД должно быть основано на соответствии конкретной системы тем задачам, которые планируют с ее помощью решать. Наряду с основным и самым предсказуемым источником угроз — внешними нарушителями (злоумышленниками), угрозу могут представлять и легальные пользователи СЭД. Система защиты СЭД должна быть способна противостоять этим угрозам, защищая не только данные, хранящиеся внутри электронных документов, но и саму себя. Многофакторная аутентификация позволяет серьезно повысить защищенность системы от внешних злоумышленников. Но одним из важных средств защиты информации является резервирование. Все же для обеспечения оптимальной защиты данных потребуется применять и другие меры, выходящие за границы встроенных решений. В случае возникновения инцидентов информационной безопасности, проанализировав сохраненные данные можно будет вычислить нарушителя с помощью Directum RX. В дополнение разграничения доступа можно добавить шифрование документов для дополнительного ограничения доступа. Делаем вывод, что СЭД обладает весьма обширным и разнообразным набором встроенных средств защиты.

Ключевые слова: функции электронного ДКО; атаки на СЭД; защиты электронного документа.

ANALYSIS AND EVALUATION THE MODEL OF THE ELECTRONIC DOCUMENT MANAGEMENT SYSTEM USING DIRECTUM RX

Naydanov Danil, Yarovoy Nikolay, Yarosh Artem
Branch of the Military Educational and Scientific Center of the Air Force
Air Force Academy named after Professor N. E. Zhukovsky and Yu. A. Gagarin
1 Town 11 St., Chelyabinsk, 454015, Russia
e-mails: s123.ert@yandex.ru, aros32495@gmail.com,

Abstract. The article discusses the definition of the following sets of basic functions of electronic ATP — the creation of documents in electronic form. The decision to choose one or another EDMS should be based on the compliance of a particular system with the tasks that are planned to be solved with its help. Along with the main and most predictable source of threats — external intruders (intruders), legitimate users of the EDMS can also pose a threat. The EDMS security system must be able to withstand these threats, protecting not only the data stored inside electronic documents, but also itself. Multi-factor authentication allows you to seriously increase the security of the system from external intruders. But one of the important means of protecting information is redundancy. However, to ensure optimal data protection, other measures will need to be taken that go beyond the boundaries of embedded solutions. In the event of information security incidents, after analyzing the stored data, it will be possible to calculate the violator using Directum RX. In addition to access control, you can add document encryption to further restrict access. We conclude that the EDMS has a very extensive and diverse set of built-in protection tools.

Keywords: functions of electronic ATP; attacks on EDMS; protection of an electronic document.

Введение. Необходимая функциональность систем электронного документооборота (ДКО) формируется исходя из задач, стоящих перед автоматизацией ДКО организации.

Можно определить следующий набор базовых функций электронного ДКО: создание документов в электронном виде; создание карточки атрибутов для документа; формирование шаблонных документов, подстановкой в них переменных значений из атрибутной карточки документа; поиск атрибутной карточки документа; формирование электронного документа с использованием шаблонов на бланке организации; сохранение документов в необходимых форматах; формирование маршрутов документов и управление его перемещением; ведение журналов, классификаторов и справочников; регистрация и классификация документов; согласование документов; формирование о передвижении и исполнении документов.

Система электронного ДКО — это специальное приложение, которое обеспечивает участникам обмен электронными документами. Все системы электронного документооборота могут быть классифицированы по нескольким признакам.

Особенностью российского внутреннего электронного ДКО организации является его вертикальная направленность: электронный документ, прежде чем попасть к исполнителю, проходит ряд согласований и

утверждений у вышестоящего руководства. Помимо этого, в отечественном делопроизводстве присутствуют такие неотъемлемые части, как регистрационная система, подготовка отчетов, контроль исполнения.

Очевидно, что решение о выборе той или иной СЭД должно быть основано на соответствии конкретной системы тем задачам, которые планируют с ее помощью решать.

Чтобы окончательно определить, какое решение имеет смысл внедрить в работу организации необходимо руководствоваться следующими критериями: соответствие стандарту отрасли организации; соответствие целям и задачам организации; уровень технической поддержки СЭД со стороны поставщика как во время внедрения, так и в процессе эксплуатации; расширяемость СЭД в случае расширения деятельности организации; доступность документации по администрированию или изменению настроек СЭД; защита СЭД. Система должна обеспечивать защиту информации в соответствии с политикой безопасности организации; время, необходимое на восстановление СЭД после сбоев в работе; стоимость СЭД, включая стоимость покупки, лицензии, администрирования и технической поддержки [1, 2].

Современные СЭД являют собой автоматизированную информационную систему, предназначенную для обработки электронных документов, которая обеспечена комплексом средств защиты информации, программных и технических. СЭД можно разделить на четыре основные подсистемы: обработки электронных документов; обеспечения безопасности информации; электропитания; пользователи СЭД.

Наряду с основным и самым предсказуемым источником угроз — внешними нарушителями (злоумышленниками), угрозу могут представлять и легальные пользователи СЭД — сотрудники организации, в частности, от наиболее привилегированных пользователей — администраторов системы. Они имеют неограниченные права доступа к информации и знают систему изнутри. Соответственно в результате внутренних атак вероятность нанесения колоссального ущерба организации крайне велика. При этом не так важны мотивы действий сотрудников — намеренные или непреднамеренные, в результате информация может оказаться утраченной или разглашенной, что повлечет за собой материальный и репутационный ущерб.

Соответственно, любые атаки на СЭД, а также на любые другие системы, основаны на описанном выше механизме. Элементы этого механизма могут видоизменяться для конкретных областей, в том числе и для СЭД. Все эти возможные изменения должны быть учтены.

Угрозы информационной безопасности СЭД можно разделить на несколько основных подгрупп: несанкционированный доступ; утечка информации; потеря данных. Для защиты информации в автоматизированных системах, в том числе СЭД, необходимо учитывать основные принципы: законность и обоснованность защиты; системность; комплексность; непрерывность достаточность; гибкость; открытость алгоритмов и механизмов защиты; простота применения средств защиты.

Значительную часть угроз информационной безопасности составляют угрозы несанкционированного доступа (НСД). Эти угрозы ведут к утечкам конфиденциальной информации и утрате целостности этой информации. Для защиты информации в автоматизированных системах по требованию ФСТЭК и ФСБ должны использоваться встроенные или наложенные средства защиты информации от НСД.

В СЭД защита от НСД включает в себя аутентификацию, управление доступом.

В случае использования многофакторной аутентификации могут использоваться различные варианты комбинаций остальных методов аутентификации. Многофакторная аутентификация позволяет серьезно повысить защищенность системы от внешних злоумышленников, завладевших каким-либо из ключей доступа, поскольку для успешной аутентификации этого будет недостаточно.

Разграничение доступа — установление полномочий доступа субъектов к объектам информационной системы. Разграничение доступа позволяет строго определить полномочия субъекта списком ресурсов, которые доступны пользователю и права доступа к каждому ресурсу. В ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации» и в документах Гостехкомиссии РФ определены два вида (принципа) разграничения доступа: дискретное управление доступом; мандатное управление доступом [1, 3].

Еще одним важным средством защиты информации является резервирование. Резервирование позволяет восстановить информацию, потерянную или искаженную в результате применения угрозы нарушения целостности, если основные контрмеры не помогают справиться с задачей. Кроме того, наличие резервной копии конфигурации или образа системы позволяет быстро восстановить полноценную работу ИС, доступность которой была нарушена. Во многих наиболее популярных СЭД реализована возможность работы с использованием протокола HTTPS. Это позволяет защитить данные за счет криптографического преобразования передаваемых данных. Отличие от HTTP заключается в том, что весь трафик передается в зашифрованном виде с использованием SSL и TLS. В работе HTTPS применяется SSL-сертификат, в котором содержатся уникальные ключи шифрования. Они позволяют подтвердить подлинность и используются для шифрования трафика.

Встроенные в СЭД средства защиты позволяют обеспечить высокий уровень безопасности, однако нельзя полностью полагаться только на них. Для обеспечения оптимальной защиты данных потребуется применять и другие меры, выходящие за границы встроенных решений.

Рассмотрим СЭД Directum RX на предмет встроенных средств безопасности. Среди встроенных средств, обеспечивающих безопасность в СЭД Directum RX, применяются криптографические методы и резервирование. В Directum RX реализована работа по протоколу HTTPS, это гарантирует, что данные при взаимодействии пользователей передаются в зашифрованном виде по защищенному каналу SSL/TLS. Такое взаимодействие обеспечивает конфиденциальность передаваемых электронных документов даже в случае перехвата их злоумышленником.

Все данные в Directum RX хранятся централизованно, благодаря этому в системе возможно полноценное разграничение доступа. Права доступа могут быть заданы на каждый документ — в системе есть четыре типа прав доступа: «права доступа отсутствуют», «есть права на чтение», «есть права на чтение и запись» и «полные права доступа». Directum RX позволяет назначать права, как для каждого субъекта, так и для целых групп субъектов, что упрощает процесс администрирования [4, 5].

В дополнение разграничения доступа можно добавить шифрование документов для дополнительного ограничения доступа к документам лиц, которым нельзя запрещать доступ к карточке документа, например, администраторы системы. Шифрование в Directum RX возможно в следующих вариантах: на основе паролей и на основе сертификатов, либо их комбинированное использование.

Заключение. Такой подход имеет преимущество по сравнению с шифрованием на базе паролей, применяя шифрование на сертификате пользователям не требуется придумывать и запоминать множество паролей, которые должны быть достаточно сложными, и потерять доступ к документу, зашифрованному на сертификате сложнее.

Подлинность электронных документов обеспечивается применением электронной подписи. Для подписания документа сертификат открытого ключа каждого пользователя должен быть зарегистрирован в системе, секретный ключ хранится у пользователя, и он несет за него ответственность. В Directum RX возможно использование внешних носителей, например, rutoken и eToken. Работа пользователей в Directum RX протоколируется. Поэтому в случае возникновения инцидентов информационной безопасности, проанализировав сохраненные данные можно будет вычислить нарушителя либо определить причину независящую от человека. В истории фиксируются операции просмотра, изменения, создания, экспорта и импорта документов, назначения прав на доступ к ним и т.д. Протоколируется работа с записями справочников.

Можно сделать вывод, что СЭД Directum RX обладает весьма обширным и разнообразным набором встроенных средств защиты.

СПИСОК ЛИТЕРАТУРЫ

1. Максимов М. В., Бобнев М. П., Кривицкий Б. Х. Защита от радиопомех. М. : Советское радио, 1976. 495 с.
2. Радзивский В. Г. Современная радиоэлектронная борьба. Вопросы методологии. М. : Радиотехника, 2006. 424 с.
3. Добыкин В. Д. Радиоэлектронная борьба. Силовое поражение радиоэлектронных систем. М.: Вузовская книга, 2007. 468 с.
4. Гапоненко Н. И., Горбань А. М., Горожанин Д. В. Формирование интенсивных электромагнитных импульсов, излучаемых при прямом возбуждении изолированной штыревой антенны короткоимпульсным сильноточным РЭП // Физика плазмы. 2000. Т. 26. № 4. С. 1-3.
5. Азаркевич Е. И. Генерация импульсного СВЧ излучения с помощью энергии химических взрывчатых веществ // Доклады Академии наук СССР. 1991. Т. 319. № 2. С. 352-355.

УДК 004.771:004.056.53

ИССЛЕДОВАНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ СЕТИ С ЯЧЕИСТОЙ ТОПОЛОГИЕЙ

Подшибякин Александр Сергеевич[1], Пантюхин Олег Игоревич[2], Солодухин Борис Владимирович[2]
[1]Военно-космическая академия имени А. Ф. Можайского
Ждановская ул., 13, Санкт-Петербург, 197198, Россия
[2]Военная академия связи им. Маршала Советского Союза С. М. Буденного,
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: p_oleg99@mail.ru, alexrebell88@gmail.com, boris.soloduxin@yandex.ru

Аннотация. В статье рассматриваются вопросы обеспечения информационной безопасности (ИБ) в информационно-коммуникационной сети с ячеистой топологией (ИКСЯТ), использующую mesh-технологию по стандарту 802.11s. Произведен обзор стандарта 802.11s, позволяющего формировать беспроводные ячеистые сети на основе Wi-Fi устройств. Проанализированы возможные атаки на маршрутизацию кадров в ИКСЯТ. Разработан экспериментальный стенд с реализацией сети с ячеистой топологией на основе модулей Raspberry pi 4 с установленными мини Wi-Fi адаптерами на базе чипсета Ralink RT5370. Приведены наиболее опасные угрозы рассматриваемой сети стандарта 802.11s, результаты ее сканирования с помощью операционной системы (ОС) OpenWRT и схема возможного внедрения в сеть нарушителя безопасности информации.

Ключевые слова: беспроводные ячеистые сети; стандарт 802.11s; угрозы информационной безопасности.

INFORMATION SECURITY THREATS INVESTIGATION IN INFORMATION AND COMMUNICATION NETWORK WITH MESH TOPOLOGY

Podshibyakin Alexander[1], Pantyukhin Oleg[2], Solodukhin Boris
[1]Military Space academy named after A. F. Mozhaisky,
13 Zhdanovskaya St, St. Petersburg, 197198, Russia
[2]The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny,
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: p_oleg99@mail.ru, alexrebell88@gmail.com, boris.soloduxin@yandex.ru

Abstract. The article deals with the issues of ensuring information security (IS) in an information and communication network with a mesh topology (ICNMT), using mesh technology according to the 802.11s standard. A review of the 802.11s standard has been made, which allows the formation of wireless mesh networks based on Wi-Fi devices. Possible attacks on frame routing in ICNMT are analyzed. An experimental stand has been developed with the implementation of a network with a mesh topology based on Raspberry pi 4 modules with installed mini Wi-Fi adapters based on the Ralink RT5370 chipset. The most dangerous threats of the 802.11s standard network under consideration, the results of its scanning using the OpenWRT operating system (OS) and a scheme for the possible introduction of an information security violator into the network are given.

Keywords: wireless mesh networks; 802.11s standard; information security threats.

Введение. В настоящее время технология беспроводных сетей (БСП) получила широкую популярность вследствие относительной простоты их построения и дешевизны используемого оборудования. Тем не менее, БСП присущи ряд недостатков, связанных с наличием угроз безопасности (отказ в обслуживании, возможность прослушивания, внедрение поддельной точки доступа, искажение проходящей в сети информации и т.п.).

Сегодня одним из основных направлений развития технологии Wi-Fi является разработка и совершенствование ИКСЯТ, позволяющих не только повысить отказоустойчивость информационной системы, но и обеспечить лучшую мобильность, более низкую стоимость развертывания, простое расширение сети, а также устойчивую связь в труднодоступных регионах. Более того, такая сеть обладает такими возможностями как самоорганизованность и автоматическая настройка ее топологии.

ИКСЯТ представляет собой децентрализованную и полносвязную беспроводную ячеистую сеть, которая разработана в рамках стандарта IEEE 802.11s, где каждая точка доступа может осуществлять как беспроводное, так и проводное соединение с любой другой, в том числе с использованием интеграции различных существующих технологий. Однако появление подобных етей с ячеистой топологией, очевидно, вызовет порождение новых уязвимостей и угроз, а значит возможностей для различного рода атак со стороны нарушителей информационной безопасности. В связи с этим, ИКСЯТ становятся объектом исследований для решения задач по обеспечению достоверности и конфиденциальности передаваемой информации.

Таким образом, несмотря на ряд достоинств сетей с ячеистой топологией, анализ воздействия возможных угроз на их информационную безопасность представляет особый практический интерес.

Особенности построения и функционирования информационно- коммуникационной сети с ячеистой топологией. Одним из основных принципов построения ИКСЯТ является создание самоорганизации ее архитектуры, обеспечивающей такие возможности, как реализацию топологии сети «каждый с каждым», устойчивость сети при отказе отдельных компонентов, масштабируемость и контроль состояния сети, динамическую маршрутизацию трафика и т.д. При этом свойство самоорганизации ячеистых сетей заключается в том, что соединения между узлами устанавливаются автоматически, любой из которых может выполнять функции транзитной передачи пакетов (маршрутизации) для других участников сети. Кроме того, важными задачами, возлагаемые на сети с ячеистой топологией, являются оптимизация потоков данных и повышение пропускной способности каналов связи. Сеть с ячеистой топологией становится особенно необходимой при отсутствии проводной инфраструктуры в отдаленных и труднодоступных районах, что может быть использовано как для организации спасательных работ, так и для обеспечения управления в силовых структурах при выполнении специальных задач.

Кроме того, в архитектуру ИКСЯТ стандарта 802.11s включены станции (узлы), содержащие несколько радиоинтерфейсов, что позволяет одновременно использовать несколько частотных каналов для передачи информации. Общаясь с каждым из своих соседей, узел использует конкретный интерфейс (интерфейсы) с соответствующим ему каналом связи. При этом механизмы назначения каналов (и другие механизмы функционирования) влияют на производительность сети, которая к тому же зависит от особенностей трафика. Для такого случая целесообразно использовать один из наиболее известных алгоритмов назначения каналов в сетях стандарта 802.11s — алгоритм Hyacinth с централизованным способом назначения каналов [1, 2].

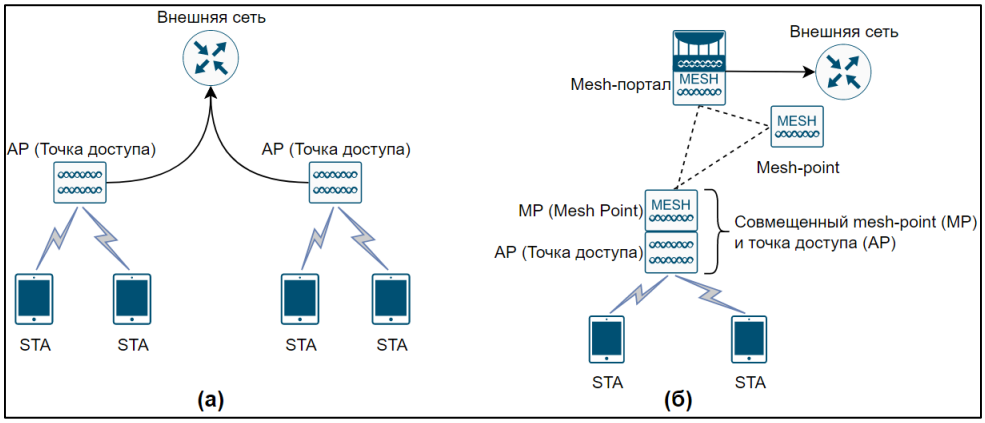


Рис. 1. Схемы функциональности сетей: общего стандарта 802.11 (а) и стандарта 802.11s (б)

Характерной особенностью типичной сети я ячеистой топологией (mesh-сети) является то, что каждый из ее узлов может одновременно работать как точка доступа, так и в качестве mesh-станции. Следует отметить, что некоторые устройства сети могут быть еще и шлюзами во внешнюю сеть, каждое из которых содержит в себе несколько радиоинтерфейсов, настроенных на определенный канал связи. При этом важной задачей назначения является определение с помощью какого интерфейса узел общается с каждым из своих соседей, а также канал передачи данных, используемый этими интерфейсами. Кроме того, предполагается, что каждый узел сети имеет соединение со всеми рабочими станциями, находящимися в области его устойчивого приема.

В существующих сетях общего стандарта 802.11 терминальные (абонентские, конечные) станции (STA) связаны с точками доступа (Access Point, AP) и могут взаимодействовать только с ними. Однако, при выходе этих точек доступа в другие сети (например, Ethernet), они не могут обмениваться информацией друг с другом (рис. 1а).

В mesh-технологиях, помимо терминальных станций и точек доступа, используются особые устройства — узлы mesh-сети (Mesh Point, MP), способные взаимодействовать друг с другом и поддерживать mesh-службы (рис. 1б).

Специфика функционирования mesh-технологии заключается в том, что некоторые из ее устройств могут совмещать несколько функций. Так, узлы mesh-сети, совмещенные с точками доступа, называются точками доступа mesh-сети (Mesh Access Point, MAP), а порталы mesh-сети (Mesh Point Portal, MPP), являясь одновременно и точками доступа, соединяют mesh-сеть с внешними по отношению к ней сетями.

Таким образом, mesh-сеть, с точки зрения других устройств и протоколов более высокого уровня, функционально является эквивалентом широковещательной Ethernet-сети, все узлы которой непосредственно соединены на канальном уровне. Отметим, что изменения в стандарте 802.11s практически не затрагивают физический уровень, а все нововведения относятся к MAC-подуровню канального уровня. Кроме того, в стандарте 802.11s рассматриваются вопросы маршрутизации пакетов в mesh-сети (сетевой и транспортный уровень модели OSI), что выходит за пределы возможностей основного стандарта 802.11. Структура пакетов MAC-уровня в mesh-сети (рис.2) аналогична стандартному формату пакетов сетей стандарта 802.11. Формат заголовка MAC-пакета в mesh-сети полностью соответствует MAC-заголовку пакета данных, определенному в стандарте 802.11 (за исключением поля HT Control (High Throughput Control)), предназначенного для поддержки оборудования стандарта 802.11n.

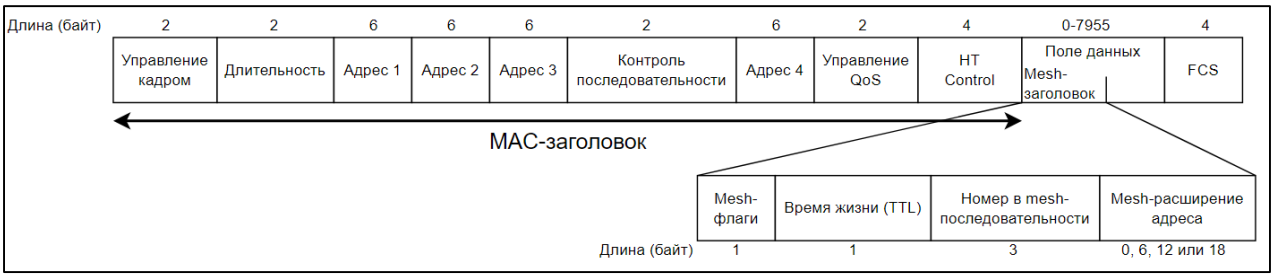


Рис. 2. Структура пакетов MAC–уровня mesh-сети

Первые три поля заголовка и поле контрольной суммы (FCS — Frame Check Sequence) присутствуют во всех пакетах MAC-уровня. Отличие MAC-пакетов стандарта 802.11s заключается в наличии mesh-заголовка в начале поля данных. Этот заголовок присутствует в пакетах данных, когда они передаются от одного mesh-узла к другому по установленному между ними соединению и присоединяется к одному из типов управляющих пакетов (Multihop Action). Кроме того, mesh-заголовок содержит четыре поля, а байт mesh-флагов регулирует его обработку. В настоящее время используются только первые два бита, которые просто определяют размер расширенного mesh-

адреса. Поле «время жизни пакета в mesh-сети» (MTL — Mesh Time To Live) содержит оставшееся максимальное число шагов между узлами, которое может совершить пакет в mesh-сети. В связи с этим ограничивается время жизни пакета при многошаговой пересылке, что помогает бороться с образованием циклических маршрутов. Номер пакета в последовательности (Mesh Sequence Number) пресекает появление дубликатов пакетов при широковещательной и многоадресной посылке.

Несмотря на то, что физический уровень стандарта 802.11 позволяет поддерживать 4 канала в технологии 802.11b и 12 каналов в технологии 802.11a, существующий канальный MAC-уровень его может использовать одновременно только один из этих каналов для всех станций сети. С целью повышения пропускной способности стандарта 802.11s необходимо осуществлять построение mesh-сети на основе станций, которые содержат несколько радиоинтерфейсов, что позволит им одновременно использовать больше частотных каналов для передачи информации. Даже при одном радиоинтерфейсе mesh-станции могут изменить используемый канал. Схема выбора/назначения каналов зависит от топологии сети и требований приложений. На рис. 3 показаны три примера распределения каналов с различными соединениями.

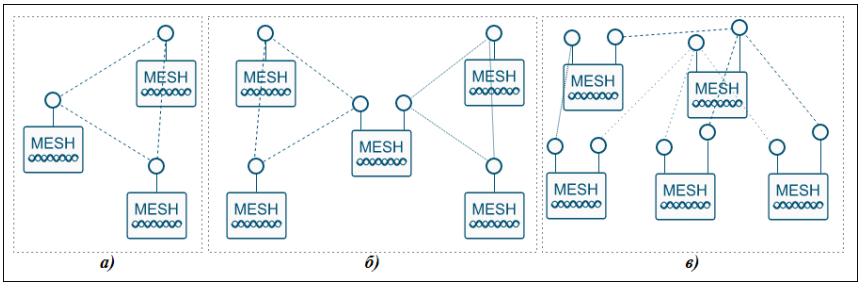


Рис. 3. Схема выбора/назначения радиоканалов с различными соединениями

Схема выбора/назначения радиоканалов (рис. 3а) соответствует простейшему случаю использования одного и того же канала всеми станциями. В схеме на рис.3б одна mesh-станция использует два радиоинтерфейса, а на рис. 3 в все mesh-станции используют два радиоинтерфейса. Таким же образом в примере (рис. 3б) используются 2 канала и mesh-станции разбиваются на 2 подмножества, не интерферирующие между собой. В примере на рис. 3 используются 3 канала, что еще больше снижает вероятность появления коллизий и повышает пропускную способность сети.

На основании вышеизложенного разработан экспериментальный стенд с реализацией ИКСЯТ для решения поставленной в статье задачи.

Реализация сети с ячеистой топологией на основе миктокопьютера под управлением операционной системы OpenWRT. Для реализации экспериментального стенда по организации беспроводной сети с ячеистой топологией в качестве основной аппаратно-программной платформы используются одноплатные миникомпьютеры Raspberry Pi 4 Model B с дополнительными Wi-Fi адаптерами на базе чипсета Ralink RT5370. Выбранное оборудование конфигурируется и управляется с помощью операционной системы (ОС) OpenWRT [3]. Данная ОС с открытым исходным кодом, основанная на ядре Linux, предназначена для сетевого оборудования, роль которого возложена на одноплатный компьютер. На рис. 4 представлена общая схема реализованной беспроводной mesh- сети.

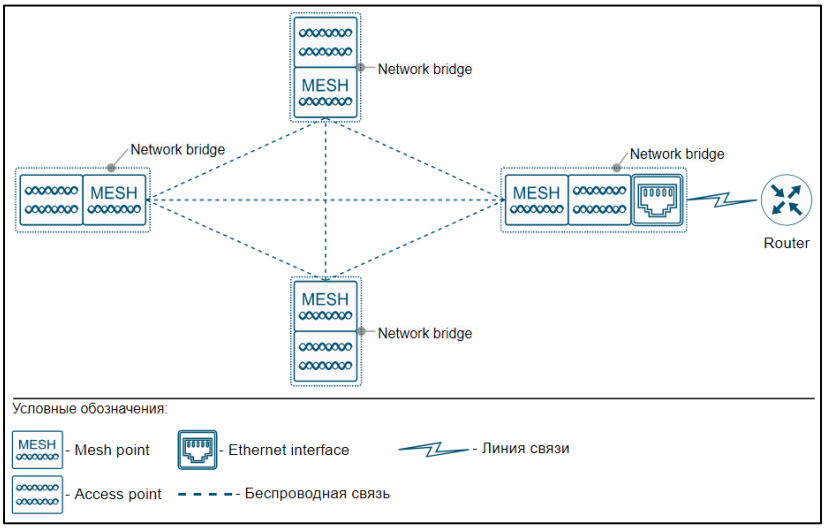


Рис. 4. Общая схема реализованной беспроводной сети с ячеистой топологией

Из рис. 4 следует, что каждый узел сети с ячеистой топологией, роль которого выполняет миникомпьютер, оснащен двумя Wi-Fi адаптерами. При этом различают следующие виды узлов такой сети: MP — узел сети, выполняющий функции маршрутизации и передачи пакетов по ячеистой топологии и AP — узел сети с функцией точки доступа, что позволяет различным беспроводным устройствам, поддерживающим стандарт 802.11, подключаться к ИКСЯТ.

Для корректной работы беспроводных интерфейсов узла MP и взаимодействия с подключенными клиентами к узлу AP реализован сетевой мост (network bridge), предназначенный для объединения сегментов сети этих узлов в единую сеть. При получении из сети кадра (пакета данных) сетевой мост проверяет в его заголовке MAC-адрес назначения и, если он принадлежит данной подсети, то передает кадр в назначенный для него сегмент. В случае, когда кадр не принадлежит данной подсети, то его передача не осуществляется. В подтверждение функционирования всех участвующих узлов в беспроводной ячеистой сети представляется список связанных между собой станций в ОС OpenWRT (рис. 5).

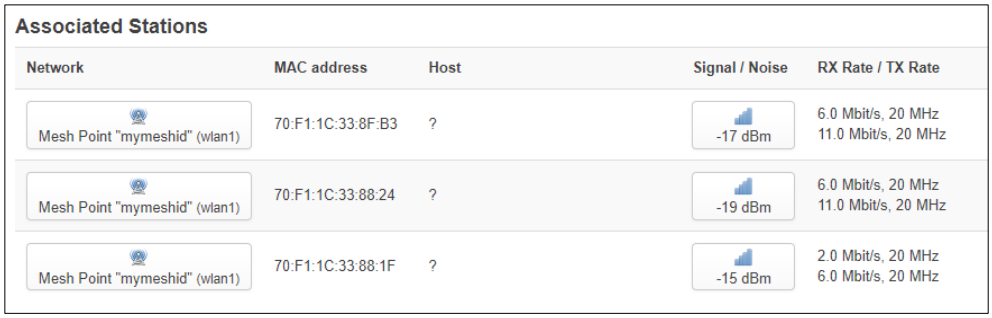


Рис. 5. Список связанных между собой станций в ОС OpenWRT

Кроме совместно работающих сетевых узлов MP и AP в экспериментальный стенд исследуемой ячеистой сети включен граничный узел mesh portal (MPP), выполняющий функцию шлюза для подключения беспроводной ячеистой сети к проводной или беспроводной внешней сети.

Разработанная таким образом структура беспроводной ячеистой сети может обеспечить следующую функциональность стенда:

–возможность подключаться к узлам AP пользователям с поддержкой стандарта 802.11 и обмениваться информацией как внутри сети, так и за ее пределами;

–осуществлять беспрепятственные подключения к беспроводной ячеистой сети устройствам взаимообмена при известном наименовании данной сети (mesh point) и каналов связи;

–проводить исследования по выявлению угроз информационной безопасности и разработки технологий предотвращения их в перспективных сетях с использованием ячеистой mesh-технологии.

Исходя из вышеизложенного, реализованная на стенде mesh-технология позволит провести необходимые исследования по выявлению угроз ИБ, характерных для беспроводных ячеистых сетей.

Реальные угрозы безопасности информации в информационно-коммуникационной сети с ячеистой топологией. В настоящее время одной из сложных проблем по защите информации (ЗИ) в сети является возрастающее количество все более изощренных атак нарушителей ИБ с использованием удаленного проникновения во внутреннюю инфраструктуру объектов беспроводной сети. Рассматриваемые mesh-технологии, как и классические беспроводные сети, используя радиоканалы для взаимообмена данными, уязвимы к прослушиванию и подмене сообщений по причине общей доступности среды передачи, а узлы, находящиеся в открытых местах расположения, могут быть легко использованы нарушителем. Действительно, с любого узла, находящегося в диапазоне источника сигнала, нарушитель, обладая информацией о частоте передачи и такими физическими параметрами как модуляция и алгоритм кодировки, может анонимно перехватить и дешифровать передаваемое сообщение. На рис. 6 представлена информация об активном сканировании беспроводных сетей с помощью ОС OpenWRT.

Рис. 6. Результаты сканирования БПС с помощью ОС OpenWRT

Как следует из рис. 6 нарушитель ИБ без каких-либо препятствий может получить о реализованной беспроводной ячеистой сети следующую информацию: символьное название беспроводной точки доступа SSID

(Service Set Identifier, в случае с ИКСЯТ — это наименование узла с функцией MP), канал передачи (Channel), режим (Mode) и шифрование (Encryption).

Кроме того, существует ряд объективных трудностей по выявлению угроз информационным ресурсам рассматриваемой mesh-сети вследствие ряда характерных ее особенностей.

Известно, что для обеспечения конфиденциальности передаваемых данных, как правило, применяется шифрование информации. Однако mesh-технологии в стандарте 802.11s не используют существующие стандарты беспроводного шифрования WEP, WPA, WPA2, что позволяет нарушителю ИБ не только скомпрометировать рассматриваемую сеть, но и стать ее частью как легитимный узел, на котором реализовывать функции MP и AP. В дальнейшем он может сконфигурировать свой узел как MPP, выполняющий роль граничного узла, что позволит перехватывать сетевой трафик, проходящий через его узел. На рис. 7 представлена схема с возможным внедрением нарушителя ИБ в рассматриваемую mesh-сеть.

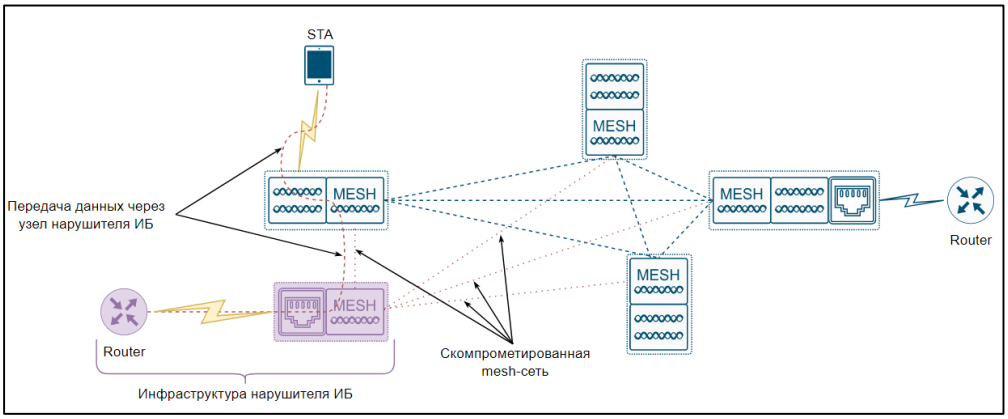


Рис. 7. Схема возможного внедрения нарушителя ИБ в mesh-сеть

Из рис. 8 очевидно, что при выборе режима mesh-point функциональность ячеистой сети в ОС OpentWRT не позволяет провести шифрование в беспроводной передаче данных, так как протокол 802.11s функционирует только с новым стандартом шифрования WPA3 [4].

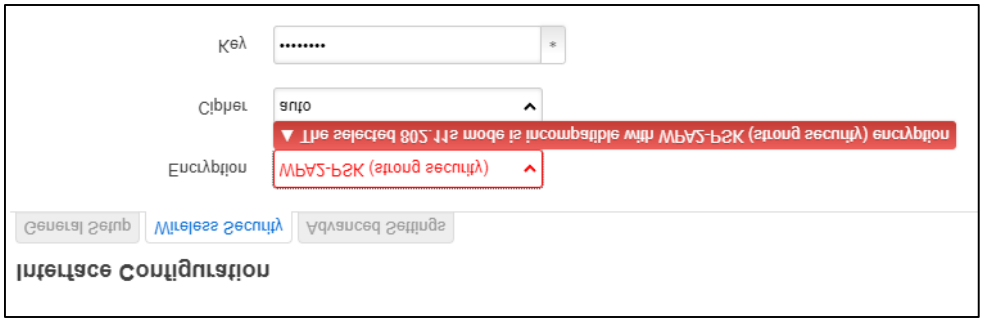


Рис. 8. Ограниченная функциональная возможность шифрования стандарта 802.11s в ОС OpentWRT

Необходимо заметить, что в разработанной на стенде mesh-сети используется радиомодуль Raspberry pi 4, который, в силу своих функциональных ограничений, также не поддерживает стандарт шифрования WPA3.

Еще одним источником угроз ИБ mesh-технологии является применение сложных алгоритмов маршрутизации при динамически изменяющейся топологии сети в случае появления некорректной информации от ее скомпрометированных узлов. Нарушение функциональности таких алгоритмов может привести к возникновению различного рода коллизий в ячеистой сети.

Таким образом, на основе вышеизложенного следует отметить, что реализованная mesh-сеть не является безопасной средой передачи данных между ее узлами. Поэтому, в силу сравнительно недавно появившейся и развивающейся такой технологии, необходимо более тщательное ее исследование по обнаружению уязвимостей и связанных с ними угроз безопасности информации в mesh-сетях с целью их предотвращения для обеспечения доступности, целостности и конфиденциальности передаваемого трафика.

Заключение. Возможность удаленного проникновения во внутреннюю инфраструктуру объектов беспроводной сети, использующей радиоканалы в качестве среды передачи данных, позволяет нарушителю ИБ анонимно и скрытно осуществлять атаки на информационные сети, что приводит к нанесению серьезного ущерба для различных организаций.

В настоящее время серьезное внимание уделяется развитию mesh-технологий, позволяющих разрабатывать беспроводные ячеистые сети, которые в рамках стандарта IEEE 802.11s осуществляют как беспроводное, так и проводное соединение с любой точки доступа. Детально описаны основные особенности построения и функционирования ИКСЯТ.

Для исследования безопасности таких сетей разработан экспериментальный стенд с реализацией ИКСЯТ на основе модулей Raspberry pi 4 с установленными мини Wi-Fi адаптерами на базе чипсета Ralink RT5370, что позволило определять специфику возможных угроз ИБ ячеистой сети, осуществлять беспрепятственные подключения к ней устройств взаимообмена при известном наименовании данной сети (mesh point) и каналов связи, а также получать информацию об активном сканировании беспроводных сетей с помощью ОС OpenWRT.

СПИСОК ЛИТЕРАТУРЫ

1. Raniwala A., Gopalan K., Chiueh T. Centralized channel assignment and routing algorithms for multi-channel wireless mesh networks // ACM Mobile Computing and Communications Review. 2004. Vol. 8, № 2. Pp. 50-65.
2. Легков К. Е., Донченко А. А. Беспроводные Mesh-сети специального назначения // Телекоммуникации и транспорт. 2009. № 3. С. 36-37.
3. OpenWrt Project: OpenWrt project operating system. URL: https://openwrt.org/ (дата обращения 17.06.2023).
4. Wi-Fi Alliance: New Wi-Fi security features available in 2018. URL: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements (дата обращения 17.06.2023).

УДК 004.056

ПОДХОД К РАСПРЕДЕЛЕНИЮ КРИПТОКЛЮЧЕЙ ДЛЯ КОНФЕРЕНЦСВЯЗИ

Рябов Геннадий Анатольевич[1], Пантюхин Олег Игоревич[1],
Солодухин Борис Владимирович[1], Вовк Александр Юрьевич[2]
[1] Военная академия связи им. Маршала Советского Союза С. М. Буденного,
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
[2] Военный инновационный технополис «Эра», Анапа, 194064, Россия
e-mails: p_oleg99@mail.ru,

Аннотация. В статье рассмотрен протокол аутентификации Kerberos, механизм взаимной аутентификации клиента и сервера перед установлением связи между ними.

Ключевые слова: Kerberos; аутентификация; сетевой протокол; атаки; стратегии безопасности.

APPROACH TO THE DISTRIBUTION OF CRYPTOCKEYS FOR CONFERENCE CALLS

Ryabov Gennady[1], Pantyukhin Oleg[1], Solodukhin Boris[1], Vovk Alexander[2]
[1] The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny,
3 Tikhoretsky Av., St. Petersburg, 194064, Russia
[2] Military innovation technopolis «Era», Anapa, 194064, Russia
e-mails: p_oleg99@mail.ru,

Abstract. The article discusses the Kerberos authentication protocol, a mechanism for mutual authentication of a client and a server before establishing a connection between them.

Keywords: Kerberos; authentication; network protocol; attacks; security strategies.

Введение. С развитием информационных технологий, возрастает возможность атак противника на компьютерные системы. В любой момент времени злоумышленник может воспользоваться уязвимостью в информационной системе для достижения своих целей [1], например, присоединиться к конференцсвязи, подменив собой кого-либо из участников. В условиях проведения СВО защита информационно-коммуникационных систем приобретает особую актуальность. Разумеется, при ее организации следует опираться на отечественные разработки, но в качестве образцов для них можно использовать зарубежные прототипы, хорошо зарекомендовавшие себя в вопросах проверки подлинности (аутентификации) участников обмена информацией.

Одним из таких инструментов является протокол *Kerberos* — сетевой протокол аутентификации, основанный на модифицированной модели Нидхема-Шрёдера (англ. *Roger Needham, Michael Shroeder*), который был разработан для клиент-серверных приложений, когда в сети выделяется один или несколько доверенных центров Т (*Trent*, от англ. *trust*), владеющих информацией о всех легальных участниках сети и их ключах. Трент также явно или неявно выступает одним из участников процессов формирования сеансовых ключей.

Протокол предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними. При этом учитывается, что начальный обмен информацией между клиентом и сервером происходит в незащищённой среде, а передаваемые пакеты могут быть перехвачены и модифицированы. Иными словами, *Kerberos* — это протокол распространения сессионных ключей, то есть распределенная система аутентификации

(проверки подлинности), которая позволяет процессу, запущенному от имени клиента, доказать свою личность серверу (и наоборот) без отправления по сети данных, которые могут позволить злоумышленнику впоследствии выдавать себя за пользователя [2].

1. Алгоритм работы протокола *Kerberos*

Для понимания сути протокола, который с точки зрения безопасности допустимо использовать для организации конференцсвязи, рассмотрим описание процесса получения сессионных ключей только двумя легальными абонентами сети с условными позывными Береза (клиент) и Дуб (сервер). Инициатором установления связи является Береза, которая должна доказать Дубу свою подлинность. Доверенный центр этой сети — Трент. И у Березы, и у Дуба есть собственные секретные ключи для общения с Трентом, которому известны ключи всех легальных абонентов.

Будем использовать следующие обозначения:

Б, Д — идентификаторы легальных абонентов Березы и Дуба соответственно;

ЕБ (…), ЕД (…) — результат шифрования некоторого блока данных с использованием ключей легальных абонентов сети (Березы и Дуба соответственно). Такое шифрование могут осуществить либо сами легальные абоненты, либо доверенный центр;

ЕК (…) — результат шифрования некоторого блока данных с использованием сессионного ключа, выданного Трентом;

t (*lifetime*) — период валидности сессионного ключа, задаваемый Трентом. Как правило, недолгий, чтобы противник не успел расшифровать ключ и не прибегнул затем к повторной атаке;

NБ, NД, NT — случайные числа, в необходимых случаях генерируемые Березой, Дубом и Трентом соответственно;

ТБ, ТД, ТТ — метки времени, выдаваемые при необходимости Березой, Дубом и Трентом по собственным часам;

К — секретный сеансовый ключ, получение которого участниками общения и является целью работы протокола.

Последовательность действий всех участников процесса в соответствии с протоколом:

1) Береза, запуская протокол, в открытом виде передает Тренту сообщение с идентификаторами абонентов, для которых необходимо получить К, а также свое условное число NБ.

С1 = Б, Д, NБ.

2) Трент, получив сообщение от Березы, генерирует ключ К для дальнейшего общения Березы и Дуба и передает обратно Березе сообщение из двух частей. Первая часть зашифрована секретным ключом Березы и содержит К, NБ, период валидности t и идентификатор Дуба.

Вторая часть неизвестна Березе — она зашифрована секретным ключом Дуба, и в ней содержится К, t и идентификатор Березы.

С2 = ЕБ (К, NБ, t, Д), ЕД (К, t, Б).

3) Береза расшифровывает первую часть принятого от Трента сообщения, получает ключ К и с его помощью создает пакет для отправки Дубу, в который входят идентификатор Березы, t и метка времени ТБ. После этого Береза отправляет Дубу сообщение из двух частей: первая часть — та, что пришла от Трента, а вторая — созданная Березой.

С3 = ЕД (К, t, Б), ЕК (Б, t, ТБ).

4) Дуб принимает сообщение. Расшифровав первую часть, он достает ключ К на текущий сеанс, а затем, используя его, расшифровывает вторую часть. Так он узнает, что Береза является Березой, поскольку в первой части С2 Трент сообщил ему, что с ним хочет связаться Береза, а во второй — сама Береза ему это подтвердила. Кроме того, Дуб знает, с какого момента (ТБ) отсчитывается время валидности текущего ключа. Чтобы подтвердить Березе, что он знает сеансовый ключ К, Дуб отправляет ей сообщение с первоначальной меткой времени Березы, зашифрованное ключом К.

С4 = ЕК (ТБ).

Береза при этом удостоверяется, что Дуб — это действительно Дуб. Здесь применимы следующие рассуждения: Дуб мог расшифровать сообщение от Березы с первоначальной меткой времени, только если он знал ключ К. А ключ К он мог узнать, только расшифровав ЕД из С3, то есть послание именно Дубу, зашифрованное секретным ключом конкретно этого легального абонента сети, который знают только Трент и Дуб. Следовательно, приславший сообщение Березе абонент — и есть Дуб.

Теперь Береза и Дуб готовы к обмену сообщениями с использованием сессионного ключа К.

Общая схема функционирования протокола *Kerberos* представлена на рис. 1.

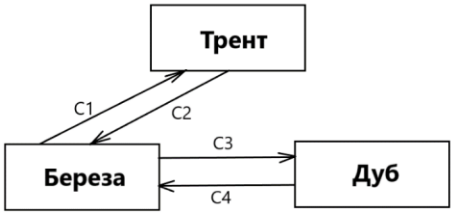


Рис. 1. Схема функционирования протокола Kerberos

2. Свойства безопасности протокола *Kerberos*

Криптографическая система может обеспечивать различные функции безопасности, для реализации которых применяются разнообразные криптографические протоколы. Обычно свойства протоколов, характеризующие их стойкость к различным атакам, формулируют как цели (*goals*) или требования к протоколам. Наиболее полное и современное толкование этих целей дается в документах международной организации *IETF*. Под свойствами (целями, требованиями) безопасности в документах *IETF* в настоящее время понимаются следующие 20 целей, сгруппированные в 10 групп и представленные в табл. 1 [3].

Таблица 1

Свойства безопасности протоколов

№ п/п	Код	Название
1	G1	Аутентификация субъекта
	G2	Аутентификация сообщения
	G3	Защита от повтора
2	G4	Неявная аутентификация получателя
	G5	Аутентификация источника
3	G6	Авторизация
4	G7	Аутентификация ключа
	G8	Подтверждение правильности ключа
	G9	Защищенность от чтения назад
	G10	Формирование новых ключей
	G11	Защищенная возможность договориться о параметрах безопасности
5	G12	Конфиденциальность
6	G13	Обеспечение анонимности при прослушивании
	G14	Обеспечение анонимности при работе с другими участниками
7	G15	Ограниченная защищенность от атак типа отказ в обслуживании
8	G16	Неизменность отправителя
9	G17	Подотчетность
	G18	Доказательство отправки
	G19	Доказательство получения
10	G20	Безопасное временное свойство

(G1) Аутентификация субъектов (*Peer Entity Authentication*) — проверка с подтверждением подлинности одной из сторон наличия полномочий (посредством представленных доказательств и/или документов) идентичности второй стороны, участвующей в выполнении протокола, а также того, что она действительно принимает участие в выполнении текущего сеанса протокола;

(G2) Аутентификация сообщения (*Message authentication*) — обеспечение аутентификации источника данных и целостности передаваемого сообщения;

(G3) Защита от повтора (*Replay Protection*) — гарантирование одним участником того, что аутентифицированное сообщение не является старым. В зависимости от контекста, это может иметь разный смысл:

–сообщение было сгенерировано в данном сеансе протокола;

–сообщение было сгенерировано в течение известного промежутка времени;

–сообщение не было принято ранее.

(G4) Неявная аутентификация получателя. Протокол должен гарантировать, что отправленное сообщение доступно для чтения только легальным получателям.

(G5) Аутентификация источника (*Source Authentication*) — законные группы участников способны аутентифицировать источник и содержание информации. Это относится к случаям, когда группы участников не доверяют друг другу.

(G6) Авторизация (третьей доверенной стороной). Гарантированность возможности авторизовать (в терминах протокола) одного участника на доступ к ресурсу другого с помощью третьей стороны, которой доверяют оба участника.

(G7) Аутентификация ключа (*Key Authentication*) — это свойство предполагает, что один из участников получает подтверждение того, что никакой другой участник, кроме заранее определенного второго участника, не может получить доступа ни к одному секретному ключу.

(G8) Подтверждение правильности ключа (*Key Confirmation, Key Proof of Possession*) — один из участников получает подтверждение того, что второй участник действительно обладает конкретным секретным ключом.

(G9) Защищенность от чтения назад / Совершенная секретность в будущем (*Perfect Forward Secrecy, PFS*) — протокол обладает этим свойством, если компрометация долговременных ключей не приводит к компрометации старых сеансовых ключей.

(G10) Формирование новых ключей. Гарантия возможности создать новые сессионные ключи для каждого сеанса протокола (динамическое распределение ключей).

(G11) Защищенная возможность договориться о параметрах безопасности.

(G12) Конфиденциальность (*Confidentiality, Secrecy*) — свойство, состоящее в том, что специфический набор данных не станет доступным или раскрытым для неавторизованных субъектов или процессов, а останется неизвестным противнику.

(G13) Защита идентификаторов от прослушивания. Гарантия, что злоумышленник (подслушивающий) не в состоянии связать обмен сообщениями участников с его реальной личностью.

(G14) Защита идентификаторов от других участников. Гарантия, что участник переписки не в состоянии связать обмен сообщениями субъекта с реальной личностью, но только с некоторым псевдонимом.

(G15) Ограниченная защита от атак отказа в обслуживании. Гарантия, что протокол следует определенным принципам, уменьшающих вероятность (усложняющих использование) отдельных классов атак отказа в обслуживании.

(G16) Неизменность отправителя. Обеспечение уверенности одного из участников, что источник сообщения остался таким же, как тот, который начал общение, хотя фактическая идентификация источника не важна для получателя.

(G17) Подотчетность. Предоставление гарантий в том, что действия системных субъектов могут быть однозначно прослежены теми субъектами, которые отвечают за все действия.

(G18) Доказательство происхождения. Гарантия невозможности отклонить доказательство того, что сообщение было отправлено субъектом.

(G19) Доказательство доставки. Гарантия неопровержимости доказательств факта получения сообщения.

(G20) Защищенное временное свойство. Гарантия возможности доказать, что факт нахождения системы в одном из состояний означает, что некогда в прошлом система хотя бы раз находилась в некотором другом состоянии. Например, что получение субъектом доступа к ресурсу означает, что некогда в прошлом субъект успешно оплатил данный доступ.

Протокол *Kerberos* удовлетворяет следующим требованиям: G1, G2, G3, G6, G7, G10 [4], чего, в принципе, достаточно для организации конференции в сети, где участники доверяют друг другу и не требуют дополнительных проверок и гарантий безопасности.

Заключение. В Kerberos могут быть реализованы несколько основных направлений (стратегий, политик) безопасности. Подробно возможные способы предотвращения и смягчения возможных атак представлены в опубликованном фирмой *Microsoft* руководстве [5].

Некоторые советы, которыми можно и должно пользоваться вне зависимости от избранной стратегии:

–запрет использования слабых паролей в учетных записях пользователей домена (применение опции сложного пароля в домене с помощью политики *Active Directory*);

–предварительная проверка подлинности учетных записей; в случае, если это невозможно, следует для таких записей создать псевдослучайные пароли с высоким уровнем сложности;

–исключение служб, которые работают в контексте учетной записи пользователя домена. В случае использования специальной учетной записи пользователя для запуска служб домена сгенерируйте надежный псевдослучайный пароль для этой учетной записи;

–проверка RAS: включить проверку RAS, чтобы избежать атак, таких как Silver Ticket. Чтобы включить эту проверку, установить значение ValidateKdcPacSignature (DWORD) в подразделе HKEY_LOCAL_MACHINE \SYSTEM \ CurrentControlSet \ Control \ Lsa \ Kerberos \ Parameters равным 1;

–периодическая смена паролей;

–отключение типов слабого шифрования *Kerberos*: должно быть разрешено только шифрование *Kerberos* с ключами *AES*. Кроме того, следует отслеживать запросы *Kerberos* с более низким уровнем шифрования, так как *RC4*, обычно используется инструментами атаки.

СПИСОК ЛИТЕРАТУРЫ

1. Фороузан Б. А. Криптография и безопасность сетей. М.: Изд-во БИНОМ. Лаборатория знаний, 2010. 784 с.
2. Kerberos: The Network Authentication Protocol : официальная Интернет-страница MIT Kerberos [Электронный ресурс]. URL: https://web.mit.edu/kerberos/ (дата обращения: 30.06.2023).
3. Experts in cybersecurity and cyber intelligence // Tarlogic [Электронный ресурс]. URL: https://www.tarlogic.com/en/blog/how-to-attack-kerbe.ros (дата обращения: 30.06.2023).
4. Рябов Г. А., Кривоногова Е. В., Карганов В. В., Вовк А. Ю. Протокол сетевой аутентификации Kerberos // Тенденции развития науки и образования, Ч. 8. № 96. Самара : Изд. Научный центр «LJournal», 2023. С. 82-87.
5. Download Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft, Version 1 and 2 from Official Microsoft Download Center [Электронный ресурс]. URL: https://www.microsoft.com/en-us/download/details.aspx?id=36036 (дата обращения: 30.06.2023).

УДК 621.391.

МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ СЕТИ ПЕРЕДАЧИ ДАННЫХ С ИСТОЧНИКОМ ПОМЕХИ НА ФИЗИЧЕСКОМ И КАНАЛЬНОМ УРОВНЕ

Сапунова Лидия Петровна[1], Кичко Яна Викторовна[1], Курашев Заур Валерьевич[2]
[1]Военная академия связи им. Маршала Советского Союза С. М. Буденного,
Тихорецкий пр-т, 3, Санкт-Петербург, 194064, Россия
[2]16 Центральный научно-исследовательский испытательный институт МО РФ
Комарова ул., 17, Мытищи, Московская обл., 141006, Россия
e-mails: lidiya.karmanec@mail.ru, kichkoyanka@mail.ru, frankilou@yandex.ru

Аннотация. Рассматриваются сети передачи данных с обратным каналом, функционирующие в условиях воздействия преднамеренных помех, структура которых может подбираться с позиции нарушения (ухудшения) работы самой системы. Обоснован выбор целевых функций, являющихся основными характеристиками сетей передачи данных. Предложено решение данных задач осуществлять на основе декомпозиции общей задачи синтеза на ряд взаимоувязанных подзадач формирования и обработки сигналов.

Ключевые слова: сети передачи данных; синтез; система с решающей обратной связью.

MODEL OF INTERACTION OF A DATA TRANSMISSION NETWORK WITH A SOURCE OF INTERFERENCE AT THE PHYSICAL AND CHANNEL LEVEL

Sapunova Lidiya[1], Kichko Yana[1], Kurashev Zaur[2]
[1]Military Academy of Communications Marshal of the Soviet Union S.M. Budyonny
Tikhoretsky Ave., 3, St. Petersburg, 194064, Russia
[2]16 Central Research and Testing Institute of the Ministry of Defense of the Russian Federation
17 Komarova str., Mytishchi, Moscow region, 141006, Russia
e-mails: lidiya.karmanec@mail.ru, kichkoyanka@mail.ru, frankilou@yandex.ru

Abstract. Data transmission networks with a reverse channel are considered, functioning under the influence of intentional interference, the structure of which can be selected from the position of disruption (deterioration) of the system itself. The choice of objective functions, which are the main characteristics of data transmission networks, is justified. The solution of these problems is proposed to be carried out on the basis of decomposition of the general synthesis problem into a number of interrelated subtasks of signal generation and processing.

Keywords: data transmission networks; synthesis; system with decisive feedback.

Введение. В данной работе осуществляется исследование методов анализа и оптимизации параметров и режима обработки сигналов в сети передачи данных (СПД), которые функционируют в условиях воздействия преднамеренных помех, структура которых может подбираться с позиции нарушения (ухудшения) работы сети [1-4].

Задачи анализа и синтеза систем повышения помехоустойчивости в условиях оптимизированных помех на физическом уровне направляются, с одной стороны на анализ и разработку алгоритмов формирования и приема сигналов, а с другой — на постановку оптимизированных помех. При этом установлено [5], что формируемые на физическом уровне сигналы должны быть рандомизированными (псевдослучайными), а решающее правило нерандомизированно.

Рассматривается модель источника помех с «сильной инерционностью» контура управления [6], в соответствии с которой невозможна постановка так называемой «помехи вслед сигналу», т.е. помехи, воздействующей на символ канального блока с использованием информации о ранее принятой части этого же символа. Вместе с тем источнику помех (ИП) известны все параметры, характеризующие СПД. Это условие обеспечивается на практике при построении помехозащищенных радиолиний за счет выполнения требований к длительности субэлемента псевдослучайного сигнала (в линиях с псевдослучайной перестройкой рабочей частоты темпа смены рабочих частот).

Для описания показателей, характеризующих воздействие помехи на процесс передачи данных, введем дополнительно обозначения: Es, Ev — соответственно энергия реализации сигнала и преднамеренной помехи на длительности сигнала, Eξ — спектральная плотность мощности шума; δv = Ev / Es, δξ = Eξ /2Es. На физическом уровне вероятность ошибки на 1 бит будем оценивать на основе интеграла вероятностей Гаусса Φ(·) выражением

$$p = p\left(\frac{\delta_v}{\beta} + \delta_\xi\right) \approx 1 - \Phi\left(\sqrt{\beta/\delta}\,\right), \quad (1)$$

где δ = δv + β δξ, являющимся асимптотически (при β → ∞) точным и дающим хорошее приближение уже при β ≥ 10 [7-9]. Разрабатываемая методика применима также для других зависимостей p, в том числе для рассмотренных в [10].

С учетом псевдослучайного перемежения символов в макроблоке суммарная помеха v(t) + ξ(t), действующая на канальный блок, задается распределением F(x) = Pr {δ ≤ x} случайной величины δ, порожденной реализацией (δ1, …, δn) на символах канального блока (a1, …, an), при этом ограничение на величину средней мощности преднамеренной помехи M[δv] описывается неравенством

$$\mathrm{M}[\delta_v] = \int_0^\infty x dF_v(x) \le \delta^- . \quad (2)$$

Множество распределений, удовлетворяющих неравенству (2), обозначается $\mathcal{F}(\delta^-)$.

Выполнение условия сильной инерционности позволяет редуцировать динамическую модель взаимодействия КПД с ИП в одношаговую (рис. 1).

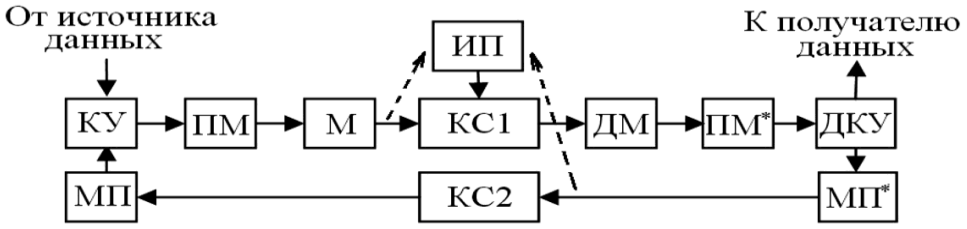


Рис. 1. Модель канала передач данных

На рис. 1 схематично показана модель канала передачи данных, описывающая взаимодействие объектов СПД с ИП на физическом и канальном уровнях.

Поступающие от источника данных информационные символы подаются в кодирующее устройство (КУ), которое формирует канальные блоки, представляющие собой кодовые слова. Сформированные в КУ канальные блоки поступают в перемежающий модуль (ПМ), где из определенного числа канальных блоков формируется макроблок из символов, перемешенных по псевдослучайному закону, известному как на передающем, так и принимающем концах СОД. Затем этот макроблок из символов подается в псевдослучайный модулятор (М), который преобразует каждый поступивший символ в псевдослучайный сигнал (ПСС) с подобранным соответствующим образом значением базы [11-12].

Полученные на передающем конце сигналы поступают в канал связи (КС1), в котором они смешиваются с генерируемой ИП помехой и совокупностью случайных помех (шумов). Поступающие из КС1 сигналы подаются на вход демодулятора (ДМ), который подает зарегистрированные данные в перемежающий модуль ПМ*, осуществляющий обратное перемежение (восстановление исходного порядка следования) символов макроблока и выдачу сформированных канальных блоков в декодирующее устройство (ДКУ).

Декодирующее устройство работает в режиме исправления [13]. В результате неисправленные ошибки либо переспрашиваются по обратному каналу связи (КС2) модулем переспроса (МП*), а затем повторяются на передаче модулем повторения (МП), либо декодируются неправильно и выдаются получателю с ошибкой.

В системах с РОС приемник по сигналу принимает окончательное решение на выдачу комбинации в приемник информации или на ее стирание и переспрос. В приемнике системы формируются сигналы подтверждения приема комбинации или переспроса, которые передаются по каналу обратной связи. Передатчик системы, в зависимости от принятого по каналу обратной связи сигнала передает новую комбинацию, полученную от датчика информации, или осуществляет повторение ранее переданной комбинации. Известно достаточно много

разновидностей систем с РОС. В зависимости от алгоритмов функционирования различают системы с РОС с ожиданием (РОС-ОЖ), с переспросом передаваемой комбинации, с накоплением правильно принятых комбинаций и системы с адресным переспросом.

Для любой системы с РОС являются определенные вероятностно-временные соотношения [14]. Так вероятность выдачи на выход системы комбинации с ошибкой $\mathcal{P}_{\text{ош}}$, соответствующая доле комбинаций с необнаруженными ошибками среди комбинаций, поступающих в приемник информации, будет равна

$$\mathcal{P}_{\text{ош}} = \frac{P_{\text{ош}}}{P_{\text{ош}} + P_{\text{пр}}} = \frac{P_{\text{ош}}}{1 - P_{\text{ст}}}, \tag{3}$$

где Рош — соответствует доле комбинаций с необнаруженными ошибками среди комбинаций, передаваемых по каналу связи и поступающих на вход системы, Рпр — вероятность правильного приема кодовой комбинации, Рст — вероятность стирания кодовой информации.

Скорость передачи данных на канальном уровне иерархии зависит от параметров кода, алгоритма функционирования с РОС, а также от значения вероятности стирания кодовых комбинаций.

Увеличение базы ПСС, с одной стороны, приводит к пропорциональному уменьшению скорости передачи информации на физическом уровне системы, а с другой, к уменьшению вероятности переспроса канального блока, что влечет повышение скорости на канальном уровне. Вопрос оптимизации базы ПСС совместно с параметрами и режимом декодирования кода изучался в [12,14], где показано, что в «типовых» случаях оптимальное значение базы может лежать в пределах $(3 \ldots 4)\delta$, где δ — отношение мощности помехи к мощности сигнала на входе приемника. При разработке аппаратуры помехозащиты для системы космической связи в 80-х годах при требованиях к коэффициенту помехозащищенности $\delta^* \approx 53$ дБ (максимально помехозащищенный режим) принимались значения базы $b = 63$дБ (25 бит/с в полосе 50 мГц), что достаточно для защиты от всех возможных в мире источников сигналов при их совместном использовании в качестве ИП.

При оценке выигрыша, обеспечиваемого рандомизацией базы ПСС, будем фиксировать параметры n, k кода и параметр r, характеризующий режим его декодирования. Принимая во внимание, что информационная скорость кода, равная k /n, одинакова для всех рассматриваемых случаев, анализ эффективности СПИ при текущих значениях базы β и величины δv будем проводить без учета коэффициента k /n по формуле

$$R(\delta, \beta) = \frac{1}{\beta} G(\delta/\beta), \tag{4}$$

где G (δ /β) — вероятность выдачи получателю поступившего из КС1 канального блока, которая оценивается выражением [4, 13]

$$G(\delta/\beta) = \sum_{j=0}^{r} \binom{n}{j} p^j (1-p)^{n-j} \tag{5}$$

При оценке показателей достоверности будем учитывать следующие моменты:

–необходимость приведения показателей к одинаковой длине информационного блока в передаваемой последовательности;

–зависимость показателя достоверности от параметров n, k, t кода и показателя r, определяющего режим декодирования;

–зависимость показателя достоверности от среднего числа повторений канальных блоков.

В предположении равенства вероятностей всех конфигураций ошибок веса более t справедлива оценка вероятности не обнаружения кодом ошибки в блоке на основе соотношения:

$$P_e(n,k,r) \approx \frac{2^k - 1}{\frac{2^n}{S_n(r)} - 1}, \text{ где } S_n(r) = \sum_{\mathrm{i}=0}^{\mathrm{r}} \mathrm{C}_{\mathrm{n}}^{\mathrm{i}} \text{ – объем шара радиуса r в } \mathrm{H}_2^n \tag{6}$$

При этом в любом случае обеспечивается выполнение условий:

1) $r \le t$ (условие допустимости режима декодирования);

2) $n - k \ge \log(\sum_{i=0}^{t} C_n^i)$ (граница Хэмминга — необходимое условие существования (n, k, t)кода).

Вероятность ошибки на бит $p_e(k)$, оценивается показателем $p_{\text{но}}$, для которого $p_e(k) = 1 - (1 - p_{\text{но}})^k \approx k p_{\text{но}}$, т. е. вероятностью:

$$p_{\text{но}} = 1 - \left(1 - p_e(k)\right)^{\frac{1}{k}} \approx \frac{p_e(k)}{k} \ . \tag{7}$$

Таким образом, на основе анализа требований к обмену информацией в сетях передачи данных, средств и комплексов связи, условий их функционирования сформулированы общие задачи синтеза структуры СПД с учетом параметров сигнала в каналах передач данных. Обоснован выбор целевых функций, являющихся основными

сетевыми характеристиками СПД. Решение данных задач базируется на декомпозиции общей задачи синтеза на ряд последовательных взаимоувязанных подзадач формирования различных параметров обработки сигналов в зависимости от структуры сети.

СПИСОК ЛИТЕРАТУРЫ

1. Чуднов А.М. Теоретико-игровые задачи синтеза алгоритмов формирования и приема сигналов // Проблемы передачи информации, 1991, № 3. С. 57-5.
2. Чуднов А. М. О минимаксных алгоритмах формирования и приема сигналов. Проблемы передачи информации. 1986. Т. 22, вып. 4. С. 49- 54.
3. Чуднов А.М. Помехозащищенность корреляционного приема псевдослучайных сигналов, модулированных по амплитуде и фазе // Радиотехника и электроника. 1987. Т. 31, № 1. С. 62-68.
4. Чуднов А. М., Кирик Д. И., Ермакова Е.М. Оптимизация параметров кода и режима обработки сигналов в условиях преднамеренных помех // Труды учебных заведений связи. 2019. Т. 5. № 4. С. 79. DOI:10.31854/1813-324X-2019-5-4-79-86.
5. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. СПб: Питер, 2011. 944 с.
6. Чуднов А. М. Математические основы моделирования, анализа и синтеза систем. СПб: ВАС, 2021.
7. Анфилатов В. С. Теоретические основы автоматизации управления войсками и связью. Ч. I. Системные основы автоматизации управления войсками и связью : Учеб. пособие. СПб. : ВАС, 2014. 312 с.
8. Аксенов Б. Е., Александров А.М. Повышение достоверности передачи информации в системах управления. Л: ЛПИ, 1981.
9. Беневоленский С. Б. Управление информационными потоками в распределенных вычислительных системах, объединенных каналами ограниченной пропускной способности: монография. М. : Издатель Мархотин П. Ю., 2009. 186 с.
10. Чуднов А. М., Сапунова Л. П. Об адаптивных алгоритмах ППРЧ в условиях случайных и преднамеренных помех // Региональная информатика и информационная безопасность. Сборник трудов. Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления. 2015. С. 73-78.
11. Чуднов А. М., Положинцев Б. И., Кичко Я. В. Анализ помехозащищенности обмена данными группы беспилотных летательных аппаратов в условиях оптимизированных помех // Радиотехника. 2022. Т. 86. № 12. С. 33–46. doi: 10.18127/j00338486-202212-03.
12. Чуднов А. М., Кичко Я. В., Сапунова Л. П. Оптимизация гарантированной скорости передачи информации псевдослучайными сигналами с рандомизированной базой в условиях преднамеренных помех // Радиотехника и электроника. 2023. Т. 68. № 3. С. 263-270.
13. Кларк Дж. Кодирование с исправлением ошибок в системах цифровой связи. М. : Радио и связь, 1987.
14. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М. : Мир, 1976.
15. Паращук И. Б. Основы передачи данных. Л. : ВАС, 2015.
16. Бертсекас Д., Шрив С. Стохастическое оптимальное управление: случай дискретного времени. М.: Наука, 1985.

УДК 621.396.4

РИСКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ПО КАНАЛАМ СОВРЕМЕННЫХ РЕГИОНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Саяркин Виталий Андреевич, Паращук Игорь Борисович
Военная академия связи им. Маршала Советского Союза С.М. Буденного,
Тихорецкий пр, 3, Санкт-Петербург, 194064, Россия
e-mails: vitaliysayarkin@gmail.com, shchuk@rambler.ru

Аннотация. В статье рассматриваются вопросы анализа и систематизации отличительных признаков и особенностей различных рисков информационной безопасности электронного документооборота по каналам и трактам современных региональных телекоммуникационных сетей, а также грани возможного ущерба, вызванных этими рисками. Анализ осуществлен в предположении, что риски условно сгруппированы по нарушаемым аспектам информационной безопасности электронного документооборота: риски нарушения конфиденциальности, нарушения целостности и нарушения доступности данных и (или) электронных документов, создаваемых, обрабатываемых и хранимых в рамках систем и сетей такого класса. Предполагается, что учет этих особенностей и классификационных признаков позволит повысить степень обоснованности принимаемых решений по разработке и технической реализации высококачественных подсистем информационной безопасности для систем автоматизированной обработки электронных документов.

Ключевые слова: информационная безопасность; риски; угрозы; электронный документооборот; региональная телекоммуникационная сеть; электронный документ; инцидент; событие информационной безопасности.

RISKS OF INFORMATION SECURITY OF ELECTRONIC DOCUMENT MANAGEMENT THROUGH THE CHANNELS OF MODERN REGIONAL TELECOMMUNICATION NETWORKS

Sayarkin Vitaly, Parashchuk Igor
Military Academy of Communications Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Ave., St. Petersburg, 194064, Russia
e-mails: vitaliysayarkin@gmail.com, shchuk@rambler.ru

Abstract. The article deals with the analysis and systematization of the distinctive features and features of various risks of information security of electronic document flow through the channels of modern regional telecommunication networks, as well as the facets of possible damage caused by these risks. The analysis is carried out under the assumption that the risks are conditionally grouped according to the violated aspects of information security of electronic document

management: the risks of violation of confidentiality, violation of integrity and violation of the availability of data and (or) electronic documents created, processed and stored within systems and networks of this class. It is assumed that taking into account these features and classification features will increase the degree of validity of decisions taken on the development and technical implementation of high-quality information security subsystems for automated electronic document processing systems.

Keywords: information security; risks; threats; electronic document management; regional telecommunication network; electronic document; incident; information security event.

Введение. Системы автоматизации документооборота, часто называемые также системами электронного документооборота, представляют собой совокупность территориально распределенных автоматизированных технических (аппаратно-программных и региональных телекоммуникационных) средств и комплексов для многопользовательского обмена электронными документами (ЭД).

Они призваны сопровождать все или почти все процедуры управления функционированием организации (министерства, учреждения, департамента) с иерархической структурой, имея целью обеспечение качественного и безопасного (защищенного) выполнения этой организацией своих задач [1-5].

Системы электронного документооборота используют каналы и тракты региональных телекоммуникационных сетей (РТКС). Региональным органам административного управления краевого, областного, городского и районного уровней всегда требуются разнообразные информационные услуги. Это и передача файлов данных достаточно большого объема, и передача факсимильной информации, и доступ районных центров к областным базам данных правовой и финансовой информации, электронная почта, а также электронный документооборот.

Это организационно-технические системы, предназначенными для создания, управления доступом и распространения электронной корреспонденции (электронных документов) в региональных сетях предприятий и организаций, а также обеспечения контроль над потоками документов в этих структурах [2, 3].

При этом, являясь одним из базовых элементов типовой IT-инфраструктуры региона или региональной организации практически любого масштаба, классическая система автоматизации документооборота (САДО) обеспечивает не только и не столько обмен ЭД с использованием своей информационно-телекоммуникационной транспортной составляющей — современных региональных телекоммуникационных сетей, но также предполагает и создание этих ЭД, управление доступом к ним пользователей, распространение этих ЭД по каналам и трактам РТКС между пользователями САДО, но главное — реализацию эффективного контроля над потоками ЭД в региональной организации (министерстве, учреждении, департаменте) с иерархической структурой, создавая, тем самым, предпосылки для обеспечения высокого качества предоставляемых информационных услуг [6].

С точки зрения контента, предоставляемого САДО своим пользователям по каналам и трактам РТКС, принято различать:

–ЭД в виде активных ЭД и архивов (различают протоколы и алгоритмы создания и управления актуальными и не актуальными ЭД, т.е., архивами);

–электронные материалы (данные), не попадающие под определение ЭД, протоколы (механизмы) реализации бизнес-процессов и обеспечения гарантии взаимосвязи между бизнес-процессами на основе потоков ЭД и протоколов (механизмов) коллективного сотрудничества — совместной, групповой работы над конкретными ЭД.

Не секрет, что весь этот контент, все эти ЭД и иные данные, создаваемые, хранимые и распространяемые в САДО по каналам и трактам РТКС, уязвимы, подвержены рискам модификации и уничтожения, нуждаются в дополнительных процедурах, обеспечивающих их информационную безопасность. Причем, особого внимания заслуживает контент САДО, распространяемый по открытым, не контролируемым каналам и трактам современных РТКС [7, 8].

В этой связи особую актуальность для понимания глубины проблемы, на наш взгляд, приобретают процедуры анализа и общей классификации возможных рисков (угроз) информационной безопасности ЭД и иных ресурсов, создаваемых, хранимых и распространяемых в рамках САДО по каналам и трактам современных РТКС [9].

При этом компонентами САДО, напрямую подверженными рискам информационной безопасности, являются не только и не столько данные (информация, ЭД) и их носители, но и процессы обработки этих данных в рамках систем такого класса, включая передачу ЭД по каналам и трактам современных региональных телекоммуникационных сетей.

С учетом того факта, что риски (угрозы) могут быть традиционно сгруппированы по нарушаемым аспектам информационной безопасности САДО, эти риски, как и для различных иных региональных телекоммуникационных систем, могут быть разделены на риски информационной безопасности с точки зрения нарушения конфиденциальности, нарушения целостности и нарушения доступности данных (ЭД), создаваемых, обрабатываемых и хранимых в рамках систем такого класса, а также передаваемых по каналам и трактам современных РТКС [10].

При этом считается, что наиболее серьезное значение имеют риски информационной безопасности САДО, связанные:

–с «утечкой» данных (ЭД) по техническим каналам взаимодействия между элементами САДО, а также по каналам и трактам транспортной (коммуникационной) базы таких систем — по каналам и трактам региональных телекоммуникационных сетей;

–с возможным несанкционированным доступом к данным (к ЭД), создаваемым, обрабатываемым и хранимым в рамках систем такого класса, а также передаваемым по каналам и трактам современных РТКС [9].

–С точки зрения анализа и общей классификации, под кризисными событиями информационной безопасности для САДО с точки зрения нарушения конфиденциальности, могут пониматься такие явные и неявные риски, как:

–риски нарушения конфиденциальности автоматизированного рабочего места (АРМ) САДО — угроза непосредственного физического доступа к АРМ, когда потенциальный нарушитель заранее обладает данными идентификации (например, логин и пароль) легитимного пользователя или системного администратора САДО;

–риски воровства или перехвата данных (ЭД);

–риск нарушения конфиденциальности сервера операционной системы, на которой работает САДО — угроза загрузки на сервер вредоносного программного обеспечения, включая программы-шпионы, облегчающие потенциальный взлом САДО;

–риски нарушения конфиденциальности сервера САДО — угроза получения несанкционированного доступа напрямую к САДО, в обход сервера операционной системы, т.е., минуя, обходя базовую систему информационной безопасности;

–риски нарушения конфиденциальности сервера базы данных САДО — угроза получения частичного или полного контроль над САДО и доступа к наиболее важным ЭД, хранимым в этой базе данных;

–риски для каналов взаимодействия между компонентами САДО — угроза перехвата пакетов между АРМ и базовыми серверами САДО;

–риски для каналов и трактов региональных телекоммуникационных сетей, действующих в интересах САДО — угроза преднамеренной подмены маршрутов доставки ЭД.

При этом, опираясь на современные стандарты в области защиты информации, принято различать инциденты и события информационной безопасности электронного документооборота.

Инцидент информационной безопасности электронного документооборота — любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность электронного документооборота.

Событие информационной безопасности электронного документооборота — идентифицированное возникновение состояния САДО или услуги электронного документооборота или РТКС, осуществляющей по своим каналам и трактам передачу ЭД в рамках электронного документооборота, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью.

Под кризисными событиями информационной безопасности с точки зрения нарушения целостности, могут пониматься риски, ориентированные на основной объект САДО — электронный документ:

–риски нарушения целостности ЭД, циркулирующих в САДО (с точки зрения злоумышленной модификации заранее определенных системой вида и качества этих ЭД, хранящихся в базе данных САДО);

–риски нарушения целостности, т.е., вида и качества резервных копий ЭД.

–Более того, некоторые работы, например [11, 12], среди рисков информационной безопасности для систем электронного документооборота рассматривают:

–риски целостности — уничтожение или искажение информации, которые могут быть как непреднамеренными, так и умышленными;

–риски конфиденциальности — любые нарушения конфиденциальности, при которых информация становится известной лицам, не имеющим к ней доступ (кража, перехват информации);

–риски доступности — комплекс потенциальных угроз, нарушающих возможность получить своевременный и беспрепятственный доступ к информации пользователям, имеющим к ней права доступа;

–риски работоспособности системы — угрозы, реализация которой приводит к сбою в работе системы;

–риски невозможности доказательства авторства — комплекс потенциальных угроз, выражающихся в том, что если в документообороте не используется электронная подпись, то невозможно доказать, что именно данный пользователь создал данный документ, при этом невозможно сделать документооборот юридически значимым.

И наконец, с точки зрения анализа и общей классификации, кризисными событиями и угрозами информационной безопасности с точки зрения нарушения доступности к коллекции ЭД, серверу операционной системы САДО, основному серверу САДО, серверу базы данных САДО, аппаратно-программным средствам САДО и каналам (каналам взаимодействия, а также каналам и трактам РТКС), выступать такие риски, как:

– риски нарушения доступности, связанные с халатным отношением при работе удаленного пользователя системы электронного докуменооборота;

– риски нарушения доступности, обусловленные непреднамеренными ошибками системных администраторов и иного персонала, обеспечивающих работу САДО.

Заключение. Таким образом, проведен анализ и рассмотрены отличительные особенности угроз и грани возможного ущерба, вызванных основными рисками информационной безопасности для электронного документооборота на базе современных региональных телекоммуникационных сетей.

Предполагается, что учет этих особенностей и классификационных признаков позволит повысить степень обоснованности принимаемых решений по разработке и технической реализации высококачественных подсистем информационной безопасности для систем автоматизированной обработки электронных документов, использующих каналы и тракты региональных телекоммуникационных сетей.

СПИСОК ЛИТЕРАТУРЫ

1. Национальный стандарт Российской Федерации ГОСТ Р ИСО 30300-2015 СИ-БИД. Информация и документация. Системы управления документами. Основные положения и словарь М. : Стандартинформ, 2015. 18 с.
2. Тищенко А.А., Казаков Ю.М., Терехов М.В. и др. Автоматизация документооборота: учебное пособие. М.: Издательство Флинта. 2018. 108 с.
3. Коржук В. М., Попов И. Ю., Воробьева А. А. Защищенный документооборот. Ч.1 : учеб.-метод. пособие. СПб. : Университет ИТМО, 2021. 67 с.
4. Паращук И. Б., Морозов И. В., Саяркин В. А. Подсистемы обеспечения безопасности электронного документооборота по каналам региональных телекоммуникационных сетей: требования и принципы построения // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2022)». Санкт-Петербург, 26-28 октября 2022 г. : Материалы конференции. СПб. : СПОИСУ, 2022. С. 114-116.
5. Селезнев А. В., Паращук И. Б., Саяркин В. А. Современный электронный документооборот в автоматизированных системах диспетчерского управления движением поездов: вопросы защиты информации // Материалы V-й международной научно-практической конференции «Инновационная железная дорога. Новейшие и перспективные системы обеспечения движения поездов. Проблемы и решения» : сборник статей // под общей редакцией Яшина М. Г. г. Санкт-Петербург, Петергоф: ВИ (ЖДВ и ВОСО), 2022. С. 405-413.
6. Стародубцев Ю. И., Бегаев А. Н., Давлятова М. А. Управление качеством информационных услуг / под общ. ред. Ю. И. Стародубцева. СПб. : Изд-во Политехн. Ун-та, 2017. 454 с.
7. Костарев С. В., Карганов В. В., Липатников В. А. Технологии защиты информации в условиях кибернетического противоборства: Научн. : монография / под общ. ред. В. А. Липатникова. СПб. : ВАС, 2020. 716 с.
8. Технологии и средства построения инфокоммуникационных систем специального назначения: Часть II: Учебник / Авраменко В. С. [и др.] ; под общ. ред. И. Б. Саенко. СПб. : ВАС, 2021. 416 с.
9. Ложников П. С., Жумажанова С. С. Об угрозах безопасности сведений ограниченного доступа в системах смешанного документооборота и правовом регулировании в области применения цифровых подписей с биометрической активацией // Доклады Томского государственного университета систем управления и радиоэлектроники. 2018. Т. 21, № 4. С. 35-43.
10. Десницкий В. А., Паращук И. Б. Анализ и обеспечение защищенности данных пользователей беспроводных сенсорных сетей: показатели доступности, целостности и конфиденциальности // Региональная информатика и информационная безопасность : сборник трудов. Вып. 7. СПб. : СПОИС, .2019. С. 34-38.
11. Анацкая А. Г. Защита электронного документооборота : учебное пособие. Омск : СибАДИ, 2019. 87 с.
12. Ушаков Н. О., Сибикина И. В., Космачева И. М. Информационная безопасность систем электронного докуменооборота // Техническая эксплуатация водного транспорта: проблемы и пути развития : материалы Третьей международной научно-технической конференции. 2021. С. 70-74.

УДК 621.396

УСЕЧЕНИЕ РАСЧЕТНОЙ ОБЛАСТИ ГРАНИЧНЫМИ УСЛОВИЯМИ В МЕТОДЕ КОНЕЧНЫХ РАЗНОСТЕЙ ВО ВРЕМЕННОЙ ОБЛАСТИ

Мешалкин Валентин Андреевич, Шанин Александр Михайлович, Коньков Денис Иванович, Ткачев Дмитрий Федорович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр. 3, Санкт-Петербург, 194064, Россия
e-mail: otesalex@yandex.ru, shanin.am@yandex.ru, den.konkov.94@mail.ru, dimas.portnoy@inbox.ru

Аннотация. Для ограничения расчетной области, при использовании метода КРВО, необходимы поглощающие граничные условия, которые моделируют уход электромагнитной волны на бесконечность. В статье рассматриваются основные методы создания поглощающих граничных условий такие как: «метод излучающей границы», метод Мура, метод Холланда и Вильямса, метод PML-слоев и метод на основе кратных поглощающих поверхностей. Рассматриваются их достоинства и недостатки.

Ключевые слова: поглощающие граничные условия; метод конечных разностей во временной области; расчетная область; электромагнитное поле; численные методы.

TRUNCATION OF THE COMPUTATIONAL DOMAIN BY BOUNDARY CONDITIONS IN THE FINITE DIFFERENCE METHOD IN THE TIME DOMAIN

Meshalkin Valentin, Shanin Alexander, Konkov Denis, Tkachev Dmitry
Military Academy of Communications Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Ave., St. Petersburg, 194064, Russia
e-mail: otesalex@mail.ru, shanin.am@yandex.ru, den.konkov.94@mail.ru, dimas.portnoy@inbox.ru

Abstract. To limit the computational domain, when using the KRVO method, absorbing boundary conditions are needed that simulate the departure of an electromagnetic wave to infinity. The article discusses the main methods of creating absorbing boundary conditions such as: «radiating boundary method», Moore's method, Holland and Williams method, PML-layers method and the method based on multiple absorbing surfaces. Their advantages and disadvantages are considered.

Keywords: absorbing boundary conditions; finite difference method in the time domain; computational domain; electromagnetic field; numerical methods.

Введение. Метод конечных разностей во временной области (КРВО) достаточно прост при формулировке, сеточной дискретизации и реализации, легко учитывает анизотропные и неоднородные материалы. Эффективность метода обусловлена отсутствием матричных уравнений и возможностью за один проход с помощью фурье-преобразования проанализировать характеристики в полосе частот. Одной из важнейших задач при реализации КРВО является создание граничных условий, причем таких что бы реализовывался принцип излучения на бесконечность [1, 2].

КРВО первоначально использует пространственную и временную дискретизацию вихревых уравнений Максвелла, представленных Kane S. Yee в 1966 году. При реализации этого метода возникает проблема рассеяния энергии электромагнитного поля (ЭМП) при дискретизации открытого пространства. Размер вычисляемой области ограничен оперативной памятью компьютера, следовательно, необходимы методы расчета ЭМП, позволяющие использовать ограниченные вычислительные ресурсы с наибольшей эффективностью. [3-5].

В источнике [2] авторы дают погрешность вычислений методом КРВО: менее 7% при шаге по пространству не более 1/10 длины волны и менее 2 % при шаге не более 1/20 длины волны. Как правило, 2 % - это достаточная точность. Но границы счетного объема могут все испортить, отразив всю электромагнитную энергию или ее часть обратно в счетный объем. На рис. 1 представлен пример отражения ЭМВ в расчетную область.

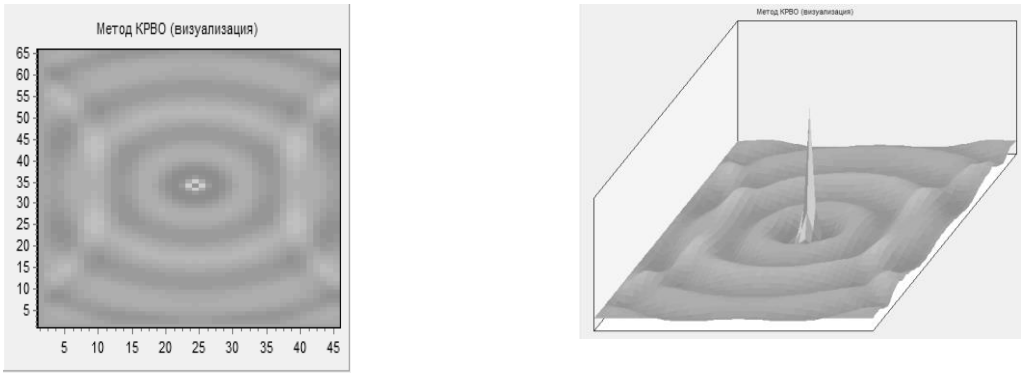


Рис.1. Пример отражения ЭМВ в расчетную область

Поэтому для ограничения объема сетки, при использовании метода КРВО необходимы поглощающие граничные условия, которые моделируют уход электромагнитной волны на бесконечность.

Постановка граничных условий является трудной и ресурсоемкой задачей. При этом граничные условия часто себя не оправдывают и вносят огромные ошибки в расчеты, вплоть до потери стабильности конечно-разностного алгоритма.

В настоящее время существует различные подходы при моделировании граничных условий, решающих эту нетривиальную задачу.

Одной из первых была техника «излучающей границы», которая в настоящее время не применяется. Другой метод реализовывал согласованные слои, которые окружали расчетную область поглощающей средой, чье сопротивление соответствовало сопротивлению свободного пространства. Третий метод появился после того, как Б. Энквист и А. Маэда односторонне аппроксимировали волновое выражение, которое изначально было реализовано для звуковых волн. После того как данный метод был применен для электромагнитного поля в 1981 году Г. Муром, было написано множество работ.

По условиям Мура считается, что волны приходят к границе счетного объема из некоторого центра, но центр рассеяния для каждой грани свой и удален в бесконечность. Волны затухают в пространстве по закону 1/R, где R-расстояние от центра рассеяния. Если расстояние от объекта до границы не менее половины длины объекта (это связано с частотой резонанса объекта), то результат получается хороший. Если расстояние меньше, то некоторые волны затухают уже не по закону 1/R, а, например, 1/R2, 1/R3. Тут возникает погрешность. Для узкополосных синусоидальных сигналов расстояние от объекта до границ должно быть не менее 1/4 длины волны. Другая погрешность возникает из-за невозможности выбрать точечный центр рассеяния для большого объекта. В итоге размер счетного объема приходится задавать очень большим. В литературе часто встречается, что расстояние до границ должно быть «не менее 1/6 длины волны», а также противоречащее этому требование «не менее 15 ячеек». И то, и другое в общем случае неверно, приемлемый результат получается при расстоянии не менее 1/3 длины волны, а для длинного тонкого объекта не менее 1/2 длины волны.

Следующим шагом были условия использующие оригинальную идею запаздывания времени на границах. Недостатком этих условий является то, что при большом количестве шагов счета появляется постоянная

составляющая, которая может экспоненциально расти, то есть данные условия неустойчивы. Этим условиям обычно достаточно 1/12-1/6 длины волны до границ. Реализация примерно в четыре раза сложнее, чем для условий Мура 1-го порядка.

Таким образом, описанные выше граничные условия малопригодны, если требуется хорошая точность вычислений, но вполне годятся для оценочных расчетов из-за малости требуемых ресурсов (памяти и времени).

В дальнейшем Р. Холланд и Дж. Вильямс предложили технику сочетающихся слоев, которые окружали расчетную область поглощающей средой, чье сопротивление соответствовало сопротивлению свободного пространства.

Следующим шагом было предложение Жан-Пьером Беренджером новой техники реализации граничных условий для решения электромагнитных задач [6].

Как и в работе Р. Холланда и Дж. Вильямса данная техника основана на использовании поглощающих слоев, но согласованная среда, используемая до этого, заменена новой согласованной средой, которая специально разработана для поглощения электромагнитных волн без отражения. В новой среде теоретический коэффициент отражения плоской волны, проходящей через границу вакуум-слой, равен нулю на любой частоте и при любом угле падения, в противоположность среде, разработанной до этого, которая реализует ноль только при нормальном угле падения волны. Итак, слой окружающий расчетную область, теоретически может поглотить без отражения любую волну, распространяющуюся по отношению к границе и, таким образом, может считаться идеально согласованным слоем. Новый слой был назван, как идеально согласованный слой (*perfectly matched layer – PML*), а сама техника – техникой *PML*. На рис. 3.5 показано распространение электромагнитной волны с применением граничных условий *PML*.

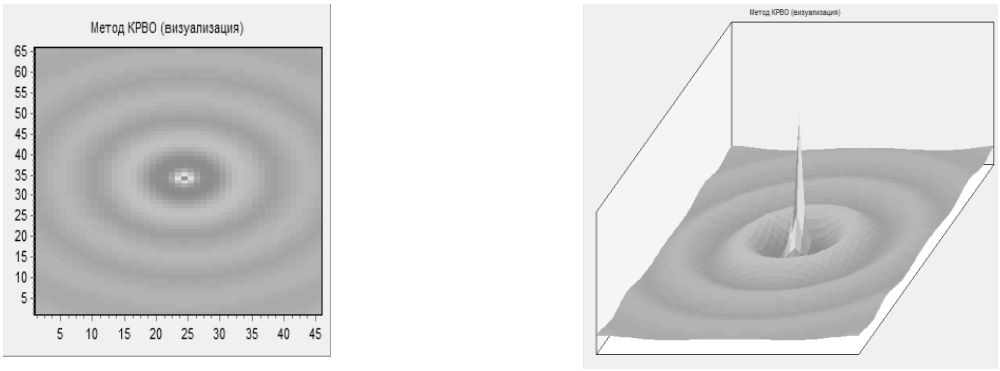


Рис.2. Применение граничных условий типа PML

Наиболее перспективным методом ограничения расчетной области в методе КРВО являются кратные поглощающие поверхности (КПП). КПП представляют из себя множество виртуально соединенных поверхностей (поверхностей Хигдона), используемых в формулировке результирующего и рассеиваемого поля в методе КРВО. Эти соединяющиеся поверхности сконструированы таким образом, что все падающие на них волны поглощаются (рис.3).

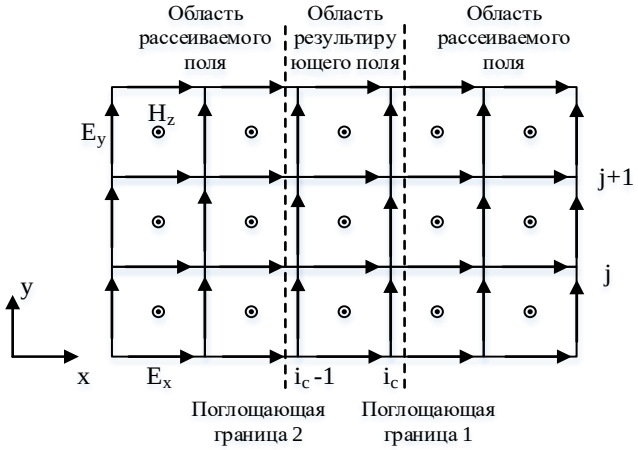


Рис. 3. Структура КПП на двухмерной сетке КРВО

В таком случае область результирующего поля будет находится между двумя поглощающими границами. При этом вторая граница является зеркальным отображением первой [7-9]. Следовательно, свойства второй границы противоположны первой. Это дает ряд преимуществ при их использовании. Первое преимущество заключается в том, что результирующая передача мала несмотря на направление падающих волн. Это очень важно для поддержания стабильности метода. Кроме того, для этой пары поглощающих границ нам необходимо оставить только две дополнительные переменные для аппроксимированных полей и три временных переменных для хранения старых значений компонент поля. Количество ячеек КРВО, необходимых для ПГУ, так же берется минимальным [10, 11].

Заключение. Рассмотрены преимущества и недостатки основных методов усечения расчетной области в методе КРВО. Наиболее перспективным методом ограничения расчетной области в методе КРВО являются кратные поглощающие поверхности [12, 13]. КПП показывают высокую точность, сопоставимую с *PML* методом, при этом КПП используют значительно меньший вычислительный ресурс. КПП показывают свою высокую эффективность в расчетных областях, расположенных в свободном пространстве.

СПИСОК ЛИТЕРАТУРЫ

1. Григорьев А. Д. Методы вычислительной электродинамики. М., 2012. 432 с.
2. Гринев А. Ю., Гиголо А. И. Математические основы и методы решения задач электродинамики. М., 2015. 216 с.
3. Липатников В. А., Парфиров В. А. Вероятностно-временные показатели процесса выявления сетей радиосвязи. Инновационные технологии и технические средства специального назначения // Труды XV научно-практической конференции : в 2-х т. Сер. »Библиотека журнала «Военмех. Вестник БГТУ»«, СПб, 2023. С. 172-175.
4. Липатников В. А., Парфиров В. А. Вероятностно-временные характеристики процесса измерения координат робототехнических комплексов военного назначения по излучаемым радиосигналам // Перспективные системы и задачи управления : материалы XVII Всероссийской научно-практической конференции и XIII молодёжной школы-семинара. Таганрог, 2022. С. 214-220.
5. Гладких Д. С., Парфиров В. А., Васильев Н. А. Математическая модель процесса обработки источников радиоизлучений комплексом радиоконтроля // Инновационные достижения и результаты научной деятельности операторов научных рот Вооруженных Сил Российской Федерации : сборник научных статей по материалам круглого стола. СПб. : Военная академия связи., 2022. С. 50-57.
6. Липатников В. А., Парфиров В. А Способ повышения защищенности радиосигналов на основе стохастической модуляции // Технологии. Инновации. Связь : Материалы научно-практической конференции. СПб., 2023. С. 175-180.
7. Шанин, А. М. Взаимное влияние элементов защищенных активных фазированных антенных решёток // Теория и техника радиосвязи. 2022. № 4. С. 73-79.
8. Шанин А. М. Модель передающего радиоцентра на основе принципа электродинамического подобия // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. – 2023. – № 5-6(179-180). – С. 71-78.
9. Мешалкин В.А., Чепелев К.В. Методика расчета внутренних характеристик активной фазированной антенной решетки с использованием современного программного обеспечения // Информационные системы и технологии. – 2020. – № 1(117). – С. 89-96.
10. Мешалкин В.А., Викторов В.А., Пилюгин А.А. Проблема электромагнитной совместимости -следствие научно-технического прогресса // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2019. № 12. С. 71-77.
11. Мешалкин В. А. Решение задач электродинамики с помощью вычислительного эксперимента // Прикладные информационные аспекты медицины. 2016. Т. 2. № 11. С. 80.
12. Лянгузов Д. А. Низкопрофильная антенна с изменяемой диаграммой направленности // Системы управления, связи и безопасности. 2022. № 2. С. 80-91.
13. Бородулин Р. Ю., Лянгузов Д. А. Модель низкопрофильной антенны для размещения на поверхности ограниченных размеров // Известия Тульского государственного университета. Технические науки. 2022. № 12. С. 193-199.

УДК 004.7

ТРУДНОСТИ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ФРАКТАЛЬНЫХ РАСПРЕДЕЛЕНИЙ НА ПРИМЕРЕ РАСПРЕДЕЛЕНИЯ ПАРЕТО

Янковский Никита Андреевич
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, Санкт-Петербург, 190121, Россия
e-mail: yannik98@yandex.ru

Аннотация. Обсуждаются трудности имитационного моделирования распределений с тяжелыми хвостами, которые связаны, во-первых, с дискретизацией представления непрерывной случайной величины, которая обусловлена шагом дискретизации в датчике базовой случайной величины, и, во-вторых, в медленной особенности сходимости эмпирических моментов к теоретическим. На примере распределения Парето продемонстрированы обе проблемы имитационного моделирования фрактальных распределений. Предложено применение подходящей аппроксимации зависимости вероятности отказа от длины очереди фрактальных систем массового обслуживания. Результаты эксперимента с выборками показывают, что правдоподобно выглядит гипотеза об асимптотически-степенном характере зависимости вероятности отказа от длины очереди фрактальных систем массового обслуживания и асимптотически-экспоненциальном у классических систем массового обслуживания.

Ключевые слова: распределение с тяжелыми хвостами; распределение Парето; имитационное моделирование; фрактальная система массового обслуживания; аппроксимация.

DIFFICULTIES OF SIMULATION MODELING OF FRACTAL DISTRIBUTIONS ON THE EXAMPLE OF THE PARETO DISTRIBUTION

Yankovskii Nikita
Saint Petersburg State University of Aerospace Instrumentation
67 Bolshaya Morskaya St, St. Petersburg, 190121 Russia
e-mail: yannik98@yandex.ru

Abstract. Difficulties in simulating heavy-tailed distributions are discussed, which are associated, firstly, with the discretization of the representation of a continuous random variable, which is due to the sampling step in the base random variable generator, and, secondly, in the slow convergence of empirical moments to theoretical ones. Using the Pareto distribution as an example, both problems of simulation modeling of fractal distributions are demonstrate. The use of a suitable approximation of the dependence of the probability of failure on the length of the queue of fractal queuing systems is proposed. The results of the experiment with samples show that the hypothesis of the asymptotically power-law nature of the dependence of the probability of failure on the queue length of fractal queuing systems and the asymptotically exponential character of classical queuing systems looks plausible.

Keywords: distribution with heavy tails; Pareto distribution; simulation modeling; fractal queuing system; approximation.

Введение. Отличительной особенностью нагрузки мультисервисных сетей является ее пачечный характер или еще говорят о пульсирующей структуре трафика. Пачки (скученности) появляются в разных масштабах времени. Пачечный трафик может быть описан статистически с использованием понятия самоподобия (масштабной инвариантности). Особенностью самоподобного трафика является устойчивость кластеризации. В то время как традиционные модели пакетного трафика являются кратковременно зависимыми (т.е. имеют экспоненциально затухающие корреляции). Данные реального пакетного трафика проявляют долговременную зависимость — то есть гиперболически затухающие корреляции [1, 2].

Пульсирующая структура трафика и ее описание. Наличие долговременной зависимости не приводит к сглаживанию пульсаций на больших масштабах времени простым сложением потоков. В этом основное отличие от пуассоновского потока, когда при моделировании делаем предположение о том, что на вход сетевого узла поступает пуассоновский поток, т.к. пульсации сглаживаются на больших масштабах времени.

Распределение медленно затухающей случайной величины X задается выражением (1), здесь параметр α характеризует хвост распределения, то есть пульсирующую структуру.

$$1-F(x)=P[X-x]\approx\frac{1}{x^{\alpha}}. \qquad (1)$$

при $x\to\infty$, $\alpha>0$.

Параметр $\alpha\in[0, 2]$ характеризует хвост распределения (пульсирующую структуру процесса).

Мерой пульсирующей структуры трафика является индекс Херста H

$$H=(3-\alpha)/2. \qquad (2)$$

Для визуализации фрактальных свойств процесса применяется структурное моделирование. Фрактальные свойства можно моделировать как пиковый процесс, с использованием продолжительности пиков [3, 4].

Временной пик представляет собой явление, при котором отдельным источником в течение продолжительного времени генерируется значительный по объему поток пакетов. Продолжительность пика, как правило задается распределением с тяжелыми хвостами, например, распределением Парето. Генераторы самоподобного сетевого трафика строятся как модель ON-OFF. Периоды ON и OFF независимы и чередуемы [5].

Многочисленные выборочные эксперименты с распределением Парето показывают плохую сходимость статистических оценок моментов распределения с тяжелыми хвостами к теоретическим значениям.

Так, например, по результатам генерация 100 млн. независимых значений паретовской случайной величины при K=1, α=1,1 вычислены статистические оценки для математического ожидания и среднеквадратичного отклонения. И получаемые оценки сильно отличаются от приведенных точных значений. Причиной больших ошибок здесь является дискретизация представления непрерывной случайной величины x, которая обусловлена шагом дискретизации в датчике базовой случайной величины.

Расчет показывает, что наибольшее значение шага дискретизации случайной величины, обеспечивающее «приемлемую» погрешность есть $\varepsilon\approx 2^{-147}$. Отсюда видно, что дискретность вещественных чисел, представимых в обычной 32-разрядной машинной арифметике, не позволяет обеспечить «приемлемую» погрешность реализации паретовской случайной величины при K=1, α=1.1.

Вторая проблема моделирования распределения Парето заключается в медленной особенности сходимости эмпирических моментов к теоретическим.

Используя правило 3σ рассчитаны длина выборки из распределения Парето с параметрами α = 1,1 и $K = 1$, гарантирующая отклонение оценки математического ожидания, не превосходящее 0.1 и время ее генерации приведены в таблице 1.

Таблица 1

Результаты моделирования

ε	$M(x)$	σ_x		T
10^{-4}	6.48	58.6	3.09×10^{6}	3 с
10^{-5}	7.34	151.1	2.05×10^{7}	20 с
10^{-6}	8.03	387.9	1.35×10^{8}	2 мин
10^{-7}	8.59	995.1	8.91×10^{8}	15 мин
10^{-8}	9.05	2552.5	5.86×10^{9}	1 ч 40 мин
10^{-12}	10.15	111278.7	1.11×10^{13}	129 дней
10^{-15}	10.55	1885871	3.20×10^{15}	100 лет
6.2×10^{-45}	11.00	1.74×10^{18}	2.74×10^{39}	10^{26} лет

Такая медленная сходимость оценок математического ожидания составляет после некорректной реализации моментов распределения вторую весьма труднопреодолимую проблему имитационного моделирования фрактальных распределений.

Таким образом, рассмотренные особенности реализации распределения Парето не позволяют гарантировать при имитационном моделировании фрактальных систем массового обслуживания (СМО) получение достоверных статистических оценок ряда традиционных показателей, таких как коэффициент загрузки ρ, средняя длина очереди L и вероятность отказа P.

Метод аппроксимации. Подход заключается в обосновании и применении подходящей аппроксимации зависимости P от L. Опыты с выборками показывают, что весьма правдоподобной выглядит гипотеза об асимптотически-степенном характере зависимости $P(L)$ у фрактальных СМО и асимптотически-экспоненциальном у классических СМО.

Уже при вероятности отказа порядка 0,01 погрешность лежит в пределах 1–3 %. Это позволяет по одному достаточно длинному прогону модели с бесконечным буфером оценить общее число отказов сразу для многих значений L и получить соответствующие оценки, сокращая тем самым затраты машинного времени на имитационное моделирование на два-три порядка.

Заключение. Погрешности реализации первого и второго моментов случайной величины с распределением Парето объясняются конечностью разрядной сетки компьютера и, соответственно, дискретным представлением вещественных чисел. Погрешность сходятся к нулю с ростом объема выборки, правда медленно в соответствии с асимптотическим степенным законом. Особенно это становится очевидным при приближении значения параметра α к единице.

Рассмотренные особенности реализации распределения Парето в общем случае не позволяют гарантировать при имитационном моделировании фрактальных систем массового обслуживания получение достоверных статистических оценок ряда традиционных показателей, таких как коэффициент загрузки, средняя длина очереди и вероятность отказа.

Метод аппроксимации для узлов сетей с фрактальным трафиком позволяет достаточной точностью оценивать основные характеристики, сокращая время имитационного моделирования на несколько порядков.

СПИСОК ЛИТЕРАТУРЫ

1. Шелухин О. И. Мультифракталы. Инфокоммуникационные приложения. М. : Горячая линия-Телеком, 2011. 576 с.
2. Кутузов О. И., Татарникова Т. М. Из практики применения метода Монте-Карло // Заводская лаборатория. Диагностика материалов. 2017. Т. 83. № 3. С. 65-70.
3. Татарникова Т. М. Анализ очередей и производительности узлов инфокоммуникационных сетей при обслуживании самоподобного трафика // Телекоммуникации. 2019. № 3. С. 6-11.
4. Татарникова Т. М., Вольский А. В. Оценка вероятностно-временных характеристик узлов с дифференциацией трафика // Информационно-управляющие системы. 2018. № 3 (94). С. 54-60. DOI: 10.15217/issn1684-8853.2018.3.54.
5. Kutuzov O. I., Tatarnikova T. M. Model of a self-similar traffic generator and evaluation of buffer storage for classical and fractal queuing system // Proc. 1st Moscow Workshop on Electronic and Networking Technologies (MWENT 2018). 2018. Pp. 1–3. DOI: 10.1109/MWENT.2018.8337306.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ И КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

УДК 004.8:336.1

ОЦЕНКА СОЦИАЛЬНО-ЭКОНОМИЧЕСКОГО СОСТОЯНИЯ РЕГИОНА ПРИ УПРАВЛЕНИИ РИСКАМИ

Булдакова Татьяна Ивановна, Джалолов Ахмад Шарофиддинович
Московский государственный технический университет им. Н. Э. Баумана
2-я Бауманская ул., 5, Москва, 105005, Россия
e-mails: buldakova@bmstu.ru, dzhalolov@mail.ru

Аннотация. В статье рассматривается задача оценки социально-экономического состояния региона на основе множества неструктурированных данных. Приведены особенности регионального управления и примеры постановок задач по управлению социально-экономическим развитием регионов. Отмечена необходимость обеспечения информационной безопасности путем постоянного отслеживания уровня информационных рисков и выработки соответствующих контрмер. Предложен подход для оценки рисков при бюджетном кредитовании регионов.

Ключевые слова: состояние региона; социально-экономические показатели; информационные процессы; информационная безопасность; информационные риски; риски бюджетного кредитования.

ASSESSMENT OF THE SOCIO-ECONOMIC STATE OF THE REGION FOR RISK MANAGEMENT

Buldakova Tatiana, Dzhalolov Ahmad
Bauman Moscow State Technical University
5 2nd Baumanskaya St., Moscow, 105005, Russia
e-mails: buldakova@bmstu.ru, dzhalolov@mail.ru

Abstract. The article considers the problem of assessing the socio-economic state of the region based on a set of unstructured data. The features of regional management and examples of tasks for managing the socio-economic development of regions are given. The need to ensure information security by constantly monitoring the level of information risks and developing appropriate countermeasures is noted. An approach for risk assessment in budget lending to regions is proposed.

Keywords: state of the region; socio-economic indicators; information processes; information security; information risks; risks of budget lending.

Введение. Оценка рисков является важной задачей при региональном управлении. При этом под рисками могут пониматься информационные риски, риски возникновения нежелательных процессов в регионе (экологических, экономических, кадровых и т.д.) или другие виды рисков. Управление рисками подразумевает оценку их уровня и выработку контрмер для снижения или исключения негативных факторов. Для повышения эффективности регионального управления и исключения возможных рисков важным является объективная оценка социально-экономического состояния региона. Подобная оценка требуется при решении многих задач по региональному управлению, например, при принятии решения о бюджетном кредитовании в зависимости от социально-экономической ситуации в регионе.

1. Особенности регионального управления. Задачи регионального управления, направленные на социально-экономическое развитие региона, можно представить как совокупность множеств ⟨ЦУР, МГР, АУР, КВР, ССР⟩, где ЦУР — множество целей управления регионами; МГР — множество методов генерации вариантов решения; АУР — множество альтернатив управленческих решений; КВР — множество критериев выбора (способов оценки эффективности вариантов решения); ССР — средства и способы реализации управленческих решений.

Сказанное обусловливает множество постановок задач по управлению социально-экономическим развитием регионов (рис. 1). Например, в зависимости от ЦУР различают задачи по развитию инфраструктуры, повышению инвестиционной привлекательности, повышению конкурентоспособности региона, снижению уровня дотационности, уменьшению безработицы и другие. Множество ССР включает различные подходы, которые

обеспечивают реализацию управленческих решений, например, управление финансами, совершенствование нормативно-законодательной базы, формирование кадрового потенциала. В основе множества этих задач лежит оценка социально-экономического состояния региона [1, 2].

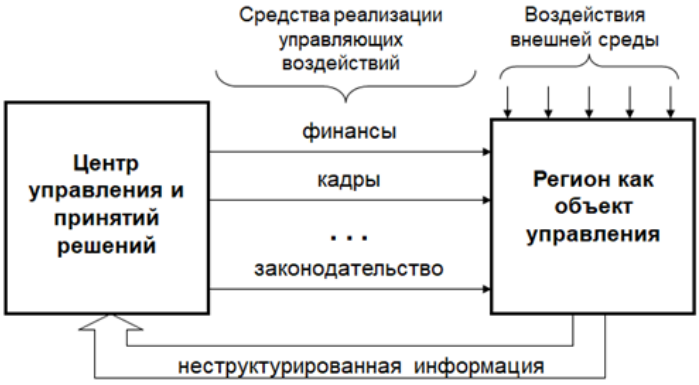


Рис. 1. Система регионального управления

Основной особенностью ситуационных центров органов регионального управления как систем обработки информации является разнородность анализируемой информации, а также средств и методов ее обработки. При этом функциональная архитектура центра определяется информационными процессами, связанными с принятием решений, а также с обеспечением информационной безопасности этих процессов [3]. Реализация информационных процессов требует интеграции и обработки разнотипной информации, а также защиты анализируемых данных. Это обусловлено тем, что показатели эффективности принимаемых решений при региональном управлении неразрывно связаны с достоверностью информации, поступающей из различных источников, которые должны быть объединены в единое информационное пространство. В свою очередь, это обусловливает повышенные требования к помехозащищённости информационных процессов для выработки обоснованных решений.

Информационные процессы для оценки социально-экономического состояния региона оказываются уязвимыми к внешним (несанкционированным) воздействиям на информацию, которые могут носить и целенаправленный характер. В результате даже незначительные, на первый взгляд, нарушения любого из информационных процессов могут привести к тяжёлым последствиям — потере конфиденциальности, целостности и/или доступности информации при региональном управлении. Сказанное обусловливает необходимость постоянного отслеживания уровня информационных рисков — потенциальной возможности искажения информации, а также выработки контрмер для их снижения, что составляет задачу управления рисками (рис. 2).

Рис. 2. Управление информационными рисками при региональном управлении

Таким образом, при региональном управлении необходимо решать проблему информационной безопасности, в том числе путем управления рисками ИБ [4].

2. Обеспечение безопасности информации в центрах регионального управления. Разработка системы информационной безопасности (ИБ) ситуационного центра регионального управления должна проводиться после тщательной проработки модели угроз и модели нарушителя, с учетом эффективной защиты от всех выявленных

угроз и потенциальных информационных рисков. При этом учитываются все технические и организационные требования, которые предъявляются к созданию таких систем, среди них [5, 6]: системный подход к организации защиты информации, что позволяет добиться оптимального сочетания всех средств (методологических, организационных, программно-аппаратных и др.); разделение и минимизация полномочий сотрудников по доступу к информации в системе и процессам обработки; обеспечение надежности защиты информации, мониторинг процесса работы системы защиты, контроль работоспособности и исправности всех механизмов защиты.

Внедрение указанных требований при проектировании и разработке подсистемы комплексной защиты информации в территориально распределенных системах регионального управления, несомненно, приведет к повышению качества принимаемых решений из-за того, что управленческий аппарат будет своевременно обеспечен информацией (о социально-экономическом состоянии регионов) с необходимой достоверностью.

Для управления рисками информационной безопасности требуется применять множество методов, используемых на различных этапах процесса оценки уровня рисков и удовлетворяющих соответствующим показателям эффективности: 1) наибольшая согласованность и адекватность оценок факторов риска; 2) максимальная адаптивность к качественным данным; 3) минимальная субъективность и неопределённость оценки риска; 4) учёт неодинаковой чувствительности риска к различным факторам [7].

Пример решения задачи управления информационными рисками при обеспечении ИБ региональных информационных процессов приведен в работе [8].

3. Оценка рисков при бюджетном кредитовании регионов. Важной задачей, связанной с развитием региона, является принятие решения о предоставлении ему бюджетного кредита, в том числе для улучшения ключевой инфраструктуры. Данное решение основывается на оценке социально-экономической ситуации в регионе, на основе которой требуется оценить риск R невозврата бюджетных средств, поскольку минимизация такого риска является главным условием предоставления региону бюджетного кредита.

Риск невозврата выделенных бюджетных средств можно оценить как $R = 1 - V_{\text{возвр}}/V_{\text{получ}}$. Здесь $V_{\text{возвр}} = P \cdot V_{\text{получ}}$ — объем денежных средств, который регион способен вернуть в бюджет; P — вероятность возврата полученных бюджетных средств; $V_{\text{получ}}$ — объем предоставленных бюджетных средств. В общем случае вероятность P неизвестна. Однако известно, что на риск невозврата выделенных бюджетных средств влияют следующие факторы: финансовые, непосредственно связанные с невозвратом бюджетных средств или их части со стороны региона; социально-политические, связанные с региональными процессами в этой сфере и обусловленные качеством жизни людей в регионе; экономические, связанные с развитием различных отраслей экономики в регионе.

В результате, чем лучше социально-экономическое состояние региона S_{reg}, тем выше вероятность возврата полученных бюджетных средств, поэтому $P = P(S_{reg})$. Следовательно, состояние региона S_{reg} можно рассматривать как косвенную оценку указанной вероятности. Таким образом, возможность бюджетного кредитования и объем денежных средств, который регион способен вернуть в бюджет, зависят от его социально-экономического состояния.

В общем случае процесс принятия решений по развитию регионов, основанный на оценке социально-экономического состояния, включает ряд этапов (рис. 3).

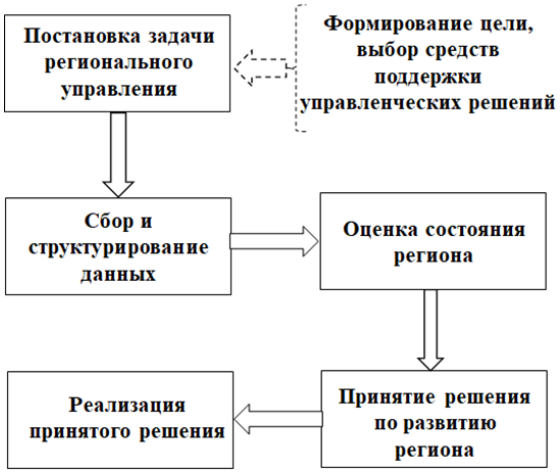


Рис. 3. Процесс принятия решений

Множество решений $D = (d_1, d_2, \ldots, d_m)$ о предоставлении регионам бюджетных (возвратных) кредитов формируется на основе анализа различных групп показателей социально-экономической ситуации $X =$

$(X_1,\ X_2,\ \dots,\ X_n)$, где n — количество групп показателей. Каждая группа включает l_i показателей, где $i = (1,\ 2,\ \dots,\ n)$, т.е. $X_1 = \left(x_1^1,\ x_2^1,\ \dots,\ x_{l_1}^1\right), \dots,\ X_n = \left(x_1^n,\ x_2^n,\ \dots,\ x_{l_n}^n\right)$.

В первую очередь учитывают группы показателей, которые определяют финансовое состояние (X_1), экономическую ситуацию (X_2), региональные процессы в социальной сфере (X_3). Эти три основные группы показателей оказывают наиболее значительное влияние на оценку состояния регионов.

Решение по j -му региону, $j = (1,\ 2,\ \dots,\ m)$, имеет вид:

$$d_j(X) = \begin{cases} 0, \text{ отказать в кредите,} \\ 1, \text{ предоставить кредит.} \end{cases}$$

Таким образом, в основе решения задачи о бюджетном кредитовании регионов лежит анализ показателей их социально-экономического развития, который необходимо провести для определения возможности возврата бюджетных средств. Для принятия решения требуется учесть множество разнородных показателей, среди которых уровень расчетной и фактической бюджетной обеспеченности, изменение структуры доходов и расходов региона, развитие производственной и добывающей сферы, уровень жизни населения, социальная обстановка, обеспеченность собственными ресурсами и многие другие. Все эти данные поступают из различных источников, имеют разное происхождение и степень влияния на принятие положительного или отрицательного решения.

Однозначной методики подобного оценивания нет, обычно решение принимается на основе мнения экспертов: в случае удовлетворительного состояния региона принимается положительное решение о выдаче бюджетного кредита, при неудовлетворительном состоянии — отрицательное решение. Фактически, оценка риска невозврата бюджетных кредитных средств является субъективной, поскольку экспертный подход характеризуется непрозрачностью и высокой степенью субъективности.

Для автоматизации процесса принятия решений по управлению социально-экономическим состоянием регионов, включая оценку рисков, создано специальное программное обеспечение. Оно реализовано как Web-сервис, который предоставляет зарегистрированному пользователю следующие возможности: выполнение анализа социально-экономического состояния региона; оценка развития региона по различным критериям (финансовым, экономическим, социальным); анализ рейтингов конкретного региона в зависимости от различных процессов; получение рекомендаций по улучшению рейтингов; анализ динамики изменения выбранного рейтинга; сравнение рейтингов разных регионов; оценка возможных рисков и возможности получения бюджетного кредита.

Программная система создана с использованием таких языков программирования, как HTML (HyperText Markup Language), CSS (Cascading Style Sheets), PHP (Hypertext Preprocessor / Personal Home Page Tools). Для повышения удобства пользователей применен набор инструментов Bootstrap Framework, а анализ каждого региона вынесен на домен третьего уровня.

Основное окно с адаптивным дизайном системы приведено на рис. 4.

Рис. 4. Адаптивный дизайн программной системы

Программный модуль СППР, реализующий оценку социально-экономического состояния регионов, повышает объективность оценки рисков в процессе принятия решений по бюджетному кредитованию [9].

Заключение. Эффективность регионального управления в значительной степени определяется принятыми управленческими решениями. Их качество зависит от достоверности анализируемых данных и помехозащищенности информационных процессов. С этой целью необходимо реализовать мероприятия по

обеспечению информационной безопасности путем постоянного отслеживания уровня информационных рисков и выработки соответствующих контрмер. Повысить объективность оценки рисков позволяет автоматизация процесса принятия решений по управлению социально-экономическим состоянием регионов.

СПИСОК ЛИТЕРАТУРЫ

1. Proletarsky A., Berezkin D., Popov A., Terekhov V., Skvortsova M. Decision Support System to Prevent Crisis Situations in the Socio-political Sphere // Cyber-Physical Systems: Industry 4.0 Challenges. Studies in Systems, Decision and Control, 2020. Vol. 260. Springer, Cham. DOI: 10.1007/978-3-030-32648-7_24.
2. Булдакова Т. И., Джалолов А. Ш. Управление развитием регионов на основе анализа рейтингов региональных процессов // Инжиниринг предприятий и управление знаниями (ИП&УЗ-2021) : сборник научных трудов XXIV Международной научной конференции. М. : РЭУ им. Г. В. Плеханова, 2022. С. 16-22.
3. Булдакова Т. И., Джалолов А. Ш. Анализ информационных процессов и выбор технологий обработки и защиты данных в ситуационных центрах // Научно-техническая информация. Серия 1. 2012. № 6. С. 16-22.
4. Булдакова Т. И., Джалолов А. Ш. Выбор технологий Data Mining для систем обнаружения вторжений в корпоративную сеть // Инженерный журнал: наука и инновации. 2013. № 11 (23). С. 36.
5. Маслобоев А. В. Модель и технология поддержки принятия решений в условиях сетецентрического управления региональной безопасностью // Надежность и качество сложных систем. 2019. № 2 (26). С. 43-59.
6. Мельников В. В. Безопасность информации в автоматизированных системах. М. : Финансы и статистика, 2003. 368 с.
7. Булдакова Т. И., Миков Д. А. Обеспечение согласованности и адекватности оценки факторов информационного риска // Вопросы кибербезопасности. 2017. № 3 (21). С. 8-15.
8. Булдакова Т. И., Джалолов А. Ш. Особенности разработки интеллектуальной системы защиты информации в ситуационном центре // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2014. № 4. С. 1-8.
9. Dzhalolov A. S., Buldakova T. I., Proletarsky A. Socio-Economic Decision Support Module by Unstructured Data // IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg, Moscow, Russia, 2020. Pp. 1931-1934. DOI: 10.1109/EIConRus49466.2020.9039086.

УДК 004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИЗНЕСА ПОД ОХРАНОЙ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Горина Елена Владимировна
Санкт–Петербургский государственный университет промышленных технологий и дизайна
Большая Морская, ул., 18, Санкт-Петербург, 191186, Россия
e-mail: 12345ele@mail.ru

Аннотация. В статье рассматриваются актуальные вопросы безопасности современного малого бизнеса, выявляются безопасные модули для управления бизнес-процессами, на основе сравнительного анализа конкурентных систем, а также преимущества реализации системы в виде основных инструментов обеспечения информационной безопасности.

Ключевые слова: система; информационная система; управление ресурсами; внедрение облачных технологий; управление; ИТ-сервис.

INFORMATION SECURITY OF BUSINESS UNDER PROTECTION OF INFORMATION TECHNOLOGY

Gorina Elena
Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya, st., St. Petersburg, 191186, Russia
e-mail: 12345ele@mail.ru

Abstract. The article discusses current issues of security for modern small businesses, identifies secure modules for managing business processes, based on a comparative analysis of competitive systems, as well as the advantages of implementing the system in the form of basic tools for providing information security.

Keywords: system; information system, resource management, integration of cloud technologies; management; IT-service.

Введение. Обеспечение информационной безопасности является одной из основных задач для современного бизнеса. Сегодня актуальность вопроса информационной безопасности в среде обмена данными значительно возросла в связи с развитием информационных технологий, зависимости бизнес-процессов от ИТ-сервисов.

Информационная безопасность бизнеса – это важный аспект деятельности любой компании, который связан с защитой конфиденциальной информации от несанкционированного доступа, использования и распространения. Сегодня с учетом развития информационных технологий и увеличения объемов данных, которыми оперируют компании, вопрос безопасности становится еще более актуальным.

Вместе с тем ужесточаются и требования, предъявляемые к системам обеспечения информационной безопасности (ИБ), что обусловлено обострением конкурентной борьбы, выходом компаний и предприятий на международные рынки, повышением уровня экономических преступлений, связанных с использованием ИТ.

Внедрение новых технологий, будь то интернет-банкинг или IP-телефония, приводит к возникновению новых угроз. Поэтому многие компании, чей бизнес зависит от использования информационных систем, вынуждены принимать меры к обеспечению безопасности корпоративных информационных систем, а главное — данных.

Одним из основных инструментов обеспечения информационной безопасности является ИТ-технологии. Они позволяют создать систему защиты, которая будет контролировать доступ к информации, шифровать данные и обнаруживать возможные угрозы [1]. Важно отметить, что безопасность данных – это не только технический аспект, но и организационный. Компания должна иметь четкие правила доступа к информации, контролировать действия своих сотрудников и обучать их основам информационной безопасности.

Одним из основных видов угроз является киберпреступность. Кибератаки могут привести к утечке конфиденциальной информации, блокировке работы компьютерных систем и серьезным финансовым потерям. Для предотвращения таких угроз необходимо использовать антивирусное программное обеспечение, защищать сеть компании от внешних атак и обучать сотрудников правилам безопасной работы в интернете.

Когда речь заходит о безопасности, первое, что приходит на ум, — обеспечение безопасности физической, и на этом не экономят [2]. С информационной безопасностью ситуация иная. О проблемах знают, но уделяют им значительно меньше внимания. Чаще всего обсуждаются защиты периметра, от вирусов, спама, сетевая безопасность, внешние угрозы, в частности, хакерские атаки. Активно дискутируется тема использования лицензионного ПО. Реже рассматриваются планы действий в условиях катастроф, обеспечения непрерывности бизнеса, вопросы, связанные с хранением и восстановлением данных. Далеко не всегда осуществляется оценка влияния на бизнес потери или утечки информации либо простоя информационной системы, а также степени категоризации информации и др.

Конфиденциальные документы должны храниться в закрытых помещениях, доступ к которым имеют только авторизованные лица. Компьютеры и сервера должны быть защищены паролями и находиться в помещениях с ограниченным доступом.

Одна из ключевых задач информационной безопасности — обеспечение непрерывности бизнеса, сохранности и неприкосновенности информации, как корпоративной, так и персональной.

Информационная безопасность подразумевает целый комплекс мероприятий по обеспечению сохранности информации и непрерывности бизнеса. Это единый процесс, не уступающий по своей значимости процессам производственным. В него должны быть вовлечены многие сотрудники, представители различных уровней управления, а не только специалисты по ИТ и ИБ.

Необходимым условием успеха является понимание того, что обеспечение информационной безопасности — процесс непрерывный, а применяемые меры должны носить комплексный и превентивный характер. Еще один важный момент — эффективная защита невозможна без комплекса организационных мер. Должны быть правильно определены цели, задачи, приоритеты и риски в области ИБ. С учетом перечисленных факторов формулируются требования к системе ИБ, разрабатываются политика и система управления ИБ.

С чего начать?

Прежде всего с определения того, «что и от чего» необходимо защищать, с анализа бизнес-процессов, информационных систем, информационных потоков, интерфейсов, операций пользователей, приложений, инфраструктуры сетей, операционных систем и баз данных.

Можно выделить несколько основных этапов построения системы информационной безопасности — обследование, разработка политики ИБ, проектирование, внедрение и поддержка в актуальном состоянии.

На первом этапе создается модель угроз, выстраивается система определений. Из всего множества угроз выделяются наиболее вероятные для данной организации. Модель информационно-технологических угроз для системы управления ИТ-деятельностью должна строиться с учетом международных, национальных стандартов, лучших мировых практик и подходов в области управления рисками ИТ, в соответствии с нормативной документацией организации в предметной области.

На втором этапе формируется политика управления ИТ-рисками, определяется место ИТ-рисков в системе управления рисками компании. Вопрос рисков ИТ должен рассматриваться как вопрос целедостижения основных шести параметров ИТ-услуги (функциональность, доступность, производительность, безопасность, непрерывность и стоимость) с учетом рисков системных и ИТ-проектов. На этой фазе важно определить зоны ответственности.

На следующем этапе разрабатываются методики управления ИТ-рисками.

Заключительный этап — внедрение управления рисками в систему управления ИТ. Реализуются организационные изменения, назначаются менеджеры управления соответствующими процессами. Разрабатываются и внедряются соответствующие внутренние стандарты и регламенты, конкретные технические решения.

В частности, можно внедрить систему сетевой безопасности, управления рабочими местами, мониторинга инфраструктурой, управления инцидентами, в том числе по ИБ, создать системы высокой готовности, модернизировать систему резервного копирования, повысить уровень технической поддержки.

Например, внедрение системы управления рабочими местами способствует выработке стандартов рабочих мест, что, с одной стороны, оптимизирует использование лицензий, с другой — улучшает контроль над использованием несанкционированного ПО. Кроме того, упрощается управление внешними накопителями, USB-портами, сокращаются затраты на эксплуатацию и т. д.

К системам защиты информации сегодня предъявляются все более высокие требования. Основными характеристиками эффективной системы информационной безопасности являются комплексность, интегрируемость, адекватность финансовым затратам, универсальность, управляемость, совместимость, превентивность, легитимность. Расширение функциональности информационных систем не должно приводить к снижению уровня их безопасности. Высокая эффективность систем ИБ достигается за счет использования качественных решений, которые функционируют как единый комплекс и имеют централизованное управление.

Политика безопасности информационных систем (ПБИС) – это набор правил и процедур, которые разрабатываются для обеспечения безопасности информации в организации. Цель ПБИС – защитить конфиденциальность, целостность и доступность информации, а также предотвратить утечки данных.

Основные принципы ПБИС:

1. Необходимость доступа – доступ к конфиденциальной информации должен быть предоставлен только тем сотрудникам, которые имеют необходимость в ее использовании.

2. Аутентификация – процесс проверки подлинности пользователя перед предоставлением ему доступа к информации.

3. Шифрование – процесс преобразования информации в нечитаемый вид для защиты от несанкционированного доступа.

4. Аудит – процесс мониторинга и анализа действий пользователей в информационной системе.

5. Физическая безопасность – защита физических объектов, содержащих конфиденциальную информацию, от несанкционированного доступа.

6. Обучение – обучение сотрудников правилам безопасной работы с информацией.

Важно отметить, что ПБИС должна быть разработана и реализована на всех уровнях организации, включая технические, организационные и правовые меры. Кроме того, ПБИС должна регулярно обновляться и адаптироваться к изменяющимся условиям и угрозам.

Компании могут использовать различные инструменты для обеспечения безопасности информации, включая антивирусное программное обеспечение, брандмауэры, системы контроля доступа и многое другое. Однако, самое важное – это осознание значимости безопасности информации среди сотрудников и руководства компании.

В целом, ПБИС является необходимой составляющей любой организации, которая хочет обеспечить надежную защиту своих данных и сохранить свою репутацию. Разработка и реализация ПБИС должны быть основаны на принципах безопасности информации и учитывать специфику деятельности компании.

Основанная на политике безопасности система информационной безопасности должна стать частью всей информационной системы компании, и ее функционирование не должно влиять на эксплуатационные параметры корпоративной ИТ-системы. В этих целях необходимо четко определить физические и логические границы системы информационной безопасности в соответствии с ИТ-политикой предприятия.

Проектирование и функционирование системы должны осуществляться на основе результатов анализа рисков. Управление ИТ-рисками — один из инструментов управления информационными технологиями в компании, а система управления ИБ — часть корпоративной системы управления.

Система должна обеспечивать адекватность и возврат инвестиций, снижать ущерб, минимизировать риски, быть достаточной, однородной, управляемой, масштабируемой, отказоустойчивой [3].

По оценкам специалистов, большое количество компаний в России нуждаются в дополнительных мерах защиты корпоративных ИТ-систем. Однако на решение проблем безопасности отводится незначительная часть бюджета.

Стоимость создания системы информационной безопасности зависит от многих факторов, прежде всего от бизнеса компании. Единого «тарифа» не существует. Сегодня, благодаря единому отраслевому стандарту ЦБ по информационной безопасности, наиболее обоснованной является стоимость решения по информационной безопасности для финансового сектора.

При определении бюджета на обеспечение ИБ необходимо исходить из того, что затраты на внедрение системы безопасности не должны превышать стоимости потери самой информации, убытков от простоя информационной системы. Но и предпринимаемые меры должны быть действительно эффективными.

Перед специалистами по ИТ и ИБ ставятся, как правило, две задачи: «чтобы все работало» и «чтобы это не стоило дорого». Они должны разрабатывать и реализовывать политику безопасности информационных систем, обеспечивать защиту данных от утечек и несанкционированного доступа, а также обучать сотрудников правилам безопасной работы с информацией. Их задачи также включают мониторинг и анализ действий пользователей в информационной системе, обеспечение физической безопасности объектов, содержащих конфиденциальную информацию, и выбор наиболее эффективных инструментов для обеспечения безопасности информации [4].

По мере расширения сферы использования и усложнения информационных систем проблема обеспечения ИБ обостряется. Безопасность уже невозможно обеспечить одним лишь набором технических средств и поддерживать только силами подразделения безопасности. Нерегулярная оценка информационных рисков, недостаточная информированность сотрудников о правилах работы с защищаемой информацией и соблюдении режима ИБ, отсутствие формализованной классификации информации по степени ее критичности и представлений о том, сколько стоят информационные активы, — все это может свести «на нет» усилия предприятия по обеспечению информационной безопасности [5].

Стремительное развитие рынка информационной безопасности свидетельствует о том, что современный бизнес понимает глобальность и важность задачи обеспечения информационной защиты. Важно отметить, что рынок информационной безопасности не ограничивается только компаниями, предоставляющими услуги по защите данных. Крупные игроки ИТ-рынка также активно вкладываются в развитие этой области.

Рынок информационной безопасности продолжает стремительно развиваться и привлекать все больше внимания со стороны компаний. Инвестирование в эту область становится необходимостью для тех, кто хочет обеспечить надежную защиту своих данных и сохранить репутацию своей компании.

Наконец, важно отметить, что информационная безопасность – это постоянный процесс. Компания должна постоянно обновлять свои системы защиты, следить за новыми угрозами и обучать своих сотрудников новым методам защиты. Только таким образом можно обеспечить надежную защиту конфиденциальной информации и сохранить репутацию компании.

В заключение можно сказать, что информационная безопасность бизнеса – это сложный и многогранный процесс, который требует постоянного внимания и усилий.

Информационная безопасность бизнеса — это комплекс мер и методов, направленных на защиту информации, которая является одним из наиболее ценных активов любой компании. Она включает в себя не только технические аспекты, но и организационные и человеческие, так как угрозы могут исходить как извне, так и изнутри организации.

Реализация эффективной системы информационной безопасности помогает предотвратить утечки конфиденциальной информации, уклонение от налогов, финансовые мошенничества и другие преступления, которые могут нанести серьезный ущерб бизнесу.

Инвестирование в ИТ-технологии и обучение сотрудников основам безопасности – это не только необходимость, но и инвестиция в будущее компании.

СПИСОК ЛИТЕРАТУРЫ

1. Еськов, А. В. Анализ действий злоумышленников при осуществлении компьютерных атак / А. В. Еськов, В. В. Селезнев // Информационные и телекоммуникационные технологии в противодействии экстремизму и терроризму: Материалы Всероссийской научно-практической конференции, Краснодар, 23 апреля 2021 года /Краснодар: ФГКОУ ВО «Краснодарский университет Министерства внутренних дел Российской Федерации», 2021. – С. 36-41.
2. Зегжда, П. Д. Информационная безопасность и киберустойчивость цифровой экономики и цифрового производства / П. Д. Зегжда, Д. П. Зегжда // Региональная информатика и информационная безопасность, Санкт-Петербург, 01–03 ноября 2017 года. – Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2017. – С. 406-407.
3. Синещук, Ю. И. Методика обоснования рационального состава средств защиты информации с учетом ресурсных ограничений / Ю. И. Синещук, Т. И. Давыдова // Автоматизация процессов управления. – 2021. – № 1(63). – С. 13-19.
4. Стандарт управления правами доступа к корпоративным файловым информационным ресурсам [Электронный ресурс] URL: https://habr.com/ru/post/281937/
5. Национальный стандарт РФ ГОСТ Р 50922-2006 «Защита информации Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст).

УДК 004.432.2

РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ СРЕДСТВАМИ ЯЗЫКА JAVA

Горина Елена Владимировна, Смирнов Артемий Михайлович
Санкт–Петербургский государственный университет промышленных технологий и дизайна
Большая Морская, ул., 18, Санкт-Петербург, 191186, Россия
e-mail: 12345ele@mail.ru

Аннотация. Данная статья является обзором современных технологий и инструментов языка программирования Java, которые могут быть применены при разработки информационной системы. В работе рассмотрены основные аспекты разработки, включая выбор среды разработки и использование соответствующих библиотек, фреймворков и других технологий. В целом, данное исследование представляет обзор актуальных технологий и инструментов, которые могут быть полезны как для начинающих, так и опытных разработчиков, занимающихся разработкой информационной системы на языке Java.

Ключевые слова: информационные системы; Java; Spring Security; PostgreSQL; разработка программного обеспечения.

DEVELOPMENT OF INFORMATION SYSTEM USING JAVA LANGUAGE

Gorina Elena, Smirnov Artemy
Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya, st., St. Petersburg, 191186, Russia
e-mail: 12345ele@mail.ru

Abstract. This article is a review of modern technologies and tools of the Java programming language that can be applied in the development of a document management information system. The paper considers the main aspects of development, including the choice of development environment and the use of appropriate libraries, frameworks and other technologies. In general, this study provides an overview of relevant technologies and tools that can be useful for both novice and experienced developers involved in the development of a document management information system in Java.

Keywords: information systems; Java; JCA; Spring Security; Spring Data; PostgreSQL; software development.

Введение. Информационные системы представляют собой программное обеспечение, которое используется для управления данными и связанными с ними процессами в организации. Эти системы обеспечивают эффективное управление данными, включая создание, хранение, обработку и передачу. Они позволяют пользователям создавать документы, контролировать их жизненный цикл, управлять правами доступа к документам и автоматизировать процессы, связанные с обработкой документов, такие как подписание, утверждение и уведомление. Информационные системы также могут предоставлять возможность для поиска, просмотра и печати документов, а также генерации отчетов и статистики. Такие системы могут использоваться во многих сферах деятельности, включая бизнес, правительственные учреждения, медицину, юриспруденцию и т.д. Они помогают организациям повышать эффективность работы, уменьшать время на обработку документов, снижать вероятность ошибок и обеспечивать безопасность документов.

Таким образом, информационные системы являются важным инструментом для управления в организации и помогают повысить эффективность бизнес-процессов. Они предоставляют централизованный подход к управлению документами, упрощают процессы обработки документов и повышают качество работы организации в целом.

Разработка информационных систем является актуальной и важной задачей для многих компаний и организаций. На сегодняшний день существует большое количество различных языков программирования и у каждого из них своя сфера применения. Одним из наиболее популярных языков программирования, используемых для создания ИС, является Java. В пятерку лучших языков вошли также: C#, Python, PHP.

Java — это объектно-ориентированный язык программирования, который широко используется для разработки веб-приложений и ИС. В настоящее время Java является одним из самых популярных языков программирования для создания информационных систем. Это связано с тем, что Java обладает множеством преимуществ, таких как кроссплатформенность, высокая производительность, безопасность и простота в использовании.

Разработка ИС средствами Java может быть выполнена с использованием различных инструментов и фреймворков, таких как Spring, Hibernate, Struts и другие. Эти инструменты обеспечивают удобную и эффективную разработку приложений, а также обеспечивают безопасность данных и защиту от утечек.

Одним из наиболее важных аспектов при разработке ИС является безопасность. Разработчик ИС должен обеспечить защиту данных от несанкционированного доступа и утечек. Для этого необходимо использовать специальные инструменты и технологии, такие как шифрование данных, механизмы аутентификации и авторизации, контроль доступа и многое другое.

Кроме того, разработчик ИС должен учитывать особенности конкретной организации и ее бизнес-процессов. Например, если ИС предназначена для банковской сферы, то требования к безопасности будут выше, чем для ИС в другой отрасли.

Разработка ИС средствами Java также может быть связана с использованием баз данных. Базы данных могут содержать конфиденциальную информацию, поэтому необходимо обеспечить их безопасность. Для этого можно использовать механизмы шифрования, контроль доступа и аудит.

Язык Java высокоуровневый объектно-ориентированный язык. Рассмотрим применение языка Java, для написания приложений. Java - это высокоуровневый объектно-ориентированный язык программирования, который был разработан компанией Sun Microsystems [1]. Язык Java относится к семейству языков программирования C, и его синтаксис похож на C++. Однако, в отличие от C++ и других языков, Java изначально был разработан как платформенно-независимый язык, что означает, что приложения, написанные на языке Java, могут быть запущены на любой платформе, поддерживающей виртуальную машину Java (JVM). Одной из ключевых особенностей языка Java является его объектно-ориентированная модель программирования. Это означает, что вся программа представляет собой набор объектов, которые взаимодействуют друг с другом. В языке Java также присутствует сборщик мусора, который автоматически освобождает память, занятую объектами, когда они больше не нужны. Java является одним из наиболее распространенных языков программирования и широко используется для разработки информационных систем. Одной из основных причин этого является тот факт, что Java обеспечивает высокую степень надежности и безопасности, а также гарантирует масштабируемость и портативность приложений.

Java обеспечивает надежность приложений благодаря своей структуре и типизации данных. Кроме того, Java предоставляет механизмы для обработки исключительных ситуаций, что повышает стабильность приложений и уменьшает вероятность возникновения ошибок. Безопасность в Java достигается благодаря многим механизмам, таким как система безопасности, контроль доступа и возможности проверки целостности кода. Язык Java известен своей надежностью и безопасностью, которые были важными критериями при его разработке. Безопасность достигается за счет механизма проверки типов, который позволяет избежать ошибок типизации и повышает надежность кода. Кроме того, Java имеет множество механизмов защиты от вредоносных программ, таких как защита от переполнения буфера и проверка безопасности кода перед его выполнением.

Java обеспечивает масштабируемость приложений, что является важным при разработке информационных систем, которые могут иметь большое количество пользователей и множество различных процессов. Благодаря механизмам многопоточности в Java, приложения могут быть оптимизированы для параллельной обработки больших объемов данных, что улучшает производительность и скорость работы приложений.

Сегодня язык Java является одним из самых популярных языков программирования в мире и используется множеством компаний и организаций. Он имеет огромную поддержку со стороны сообщества разработчиков, что делает его привлекательным выбором для создания различных программных продуктов. Уже длительное время разработчики не создают новые приложения с нуля, а используют готовые наборы инструментов для разработки – фреймворки.

Фреймворки для языка программирования Java. Фреймворки — это программные платформы, которые предоставляют готовые решения для различных задач, таких как управление объектами, управление транзакциями и обработка ошибок. Фреймворки в Java позволяют разработчикам избегать ошибок, связанных с низкоуровневым кодом, что снижает количество ошибок и упрощает тестирование приложений. Фреймворки имеют широкий спектр применения и могут использоваться для создания различных типов приложений, таких как веб-приложения, мобильные приложения и десктопные приложения. Они также позволяют создавать приложения с использованием различных архитектур, таких как MVC (Model-View-Controller) и MVP (Model-View-Presenter).

Одним из наиболее популярных фреймворков в Java является Spring Framework, который был разработан для упрощения разработки приложений на языке Java. Spring Framework предоставляет множество модулей, которые позволяют создавать приложения различных типов и облегчают работу с различными задачами, такими как управление объектами, управление транзакциями и безопасностью. Кроме того, Spring Framework поддерживает многопоточность, что позволяет создавать высокопроизводительные приложения. Таким образом, фреймворки в Java являются важным инструментом для разработки приложений на языке Java, который облегчает работу разработчиков и улучшает качество приложений. Они предоставляют готовые решения для ряда задач и позволяют разработчикам сосредоточиться на бизнес-логике приложений вместо того, чтобы тратить время на написание низкоуровневого кода.

Spring Framework - это фреймворк для разработки приложений на языке Java [2]. Фреймворк Spring был создан с целью облегчения разработки приложений на языке Java, предоставляя разработчикам готовые решения для ряда задач, таких как управление объектами, управление транзакциями и безопасностью. Spring Framework базируется на концепции инверсии управления (Inversion of Control, IoC), которая позволяет отделить бизнес-логику приложения от инфраструктурных задач. Это достигается путем создания контейнера, который управляет жизненным циклом объектов и связывает их между собой, что обеспечивает эффективное управление зависимостями и обеспечивает легкость тестирования. Spring Framework также предоставляет инструменты для решения других задач, таких как интеграция с базами данных, веб-разработка, обработка ошибок и логирование. Кроме того, Spring Framework поддерживает многопоточность, что позволяет создавать высокопроизводительные приложения.

В Spring Framework имеется множество модулей, которые могут использоваться в сочетании друг с другом для создания различных приложений. Некоторые из наиболее популярных модулей включают Spring Boot, Spring MVC, Spring Data, Spring Security. Spring Boot - это модуль, который позволяет создавать автономные приложения на основе Spring, которые не требуют многочисленных настроек. Spring MVC - это модуль, который предоставляет инструменты для разработки веб-приложений. Spring Data - это модуль, который облегчает работу с базами данных. Spring Security - это модуль, который обеспечивает безопасность веб-приложений.

Spring Framework является одним из наиболее популярных фреймворков для разработки приложений на языке Java, и он продолжает эволюционировать, чтобы удовлетворять потребности современных приложений. Он имеет широкое сообщество разработчиков и большое количество документации, что делает его привлекательным выбором для создания различных программных продуктов.

Spring Security - это фреймворк безопасности для приложений, написанных на языке Java, который предоставляет ряд инструментов и механизмов для защиты приложений от внешних угроз и атак. Фреймворк Spring Security основан на модели аутентификации и авторизации, которая позволяет управлять доступом к ресурсам приложения и контролировать действия пользователей внутри приложения. Spring Security предоставляет множество функций, таких как управление сессиями, шифрование паролей, поддержка различных методов аутентификации и авторизации, настройка прав доступа пользователей и т.д. В Spring Security реализовано множество механизмов безопасности, таких как фильтры безопасности, которые позволяют перехватывать запросы к приложению и анализировать их содержимое на предмет вредоносных действий. Также фреймворк предоставляет возможность

использовать SSL-шифрование и защищать данные в куках [3]. Spring Security также поддерживает различные методы аутентификации и авторизации, включая базовую аутентификацию, форму аутентификации, аутентификацию на основе токенов и т.д. [4] Фреймворк предоставляет множество конфигурационных параметров для настройки параметров безопасности и контроля доступа пользователей к ресурсам приложения.

Spring Security широко используется в различных приложениях, в том числе веб-приложениях, мобильных приложениях и API-интерфейсах. Он позволяет разработчикам обеспечить высокий уровень безопасности приложения и защитить его от внешних угроз и атак, что является важным фактором для обеспечения надежности и безопасности приложения.

Spring Data - это фреймворк для упрощения взаимодействия Java-приложений с различными источниками данных. Spring Data предоставляет набор абстракций и удобных API для работы с различными типами баз данных и хранилищ данных, включая SQL, NoSQL и т.д.

Фреймворк Spring Data позволяет разработчикам написать код, который работает с различными источниками данных, используя общие методы, которые автоматически переводятся в запросы к конкретным источникам данных. Это сокращает количество кода, необходимого для взаимодействия с различными источниками данных, и упрощает процесс разработки. Spring Data также предоставляет множество инструментов для работы с объектно-реляционной моделью данных, включая автоматическое создание запросов, генерацию метаданных и преобразование данных из одного формата в другой. Фреймворк облегчает работу с данными, сокращает время разработки и повышает качество кода. Spring Data поддерживает различные базы данных, такие как MySQL, PostgeSQL, MongoDB, Cassandra, Redis и др. Фреймворк также обеспечивает поддержку транзакций, что позволяет разработчикам безопасно работать с данными в различных источниках данных.

Spring Data является частью экосистемы Spring Framework и тесно интегрирован с другими компонентами фреймворка. Он обеспечивает удобный способ работы с данными в Java-приложениях, позволяет сократить время разработки и повысить качество кода, что делает его популярным инструментом для работы с данными в Java-приложениях.

Spring Boot — Spring Boot - это фреймворк, который упрощает создание и настройку самостоятельных приложений на основе Spring Framework. Он предоставляет ряд функций, таких как автоматическая конфигурация, управление зависимостями и встроенный веб-сервер, которые значительно упрощают процесс создания и развертывания приложений на основе Spring. Spring Boot использует принципы конвенции над конфигурацией, что позволяет разработчикам создавать приложения на основе Spring с минимальной необходимой конфигурацией. Фреймворк автоматически настраивает множество аспектов приложения, например, устанавливает настройки подключения к базе данных, настраивает веб-сервер и пр. [5].

Spring Boot также предоставляет множество встроенных инструментов для управления зависимостями и сборки приложений, что упрощает процесс создания и развертывания приложений. Фреймворк поддерживает множество сторонних библиотек и плагинов, что позволяет разработчикам использовать различные инструменты и технологии в своих приложениях. Spring Boot обладает мощным встроенным веб-сервером, который позволяет запускать приложения на основе Spring без необходимости установки и настройки отдельного веб-сервера. Это упрощает процесс развертывания приложений и делает их более переносимыми.

Spring Boot является одним из наиболее популярных фреймворков для создания и развертывания Java-приложений. Он упрощает процесс разработки, сборки и развертывания приложений, позволяет использовать различные технологии и инструменты, что делает его популярным инструментом для создания современных Java-приложений.

Заключение. Java является портативным языком программирования, что означает, что приложения могут быть запущены на различных платформах без необходимости изменения кода. Это особенно важно для информационных систем, которые могут использоваться на различных операционных системах и компьютерах. Таким образом, Java является идеальным языком программирования для разработки информационных систем благодаря своей надежности, безопасности, масштабируемости и портативности приложений. Java обеспечивает высокую производительность, стабильность и безопасность, что позволяет создавать эффективные и надежные приложения для управления.

Разработка ИС средствами Java является важной задачей, которая требует от разработчика знания и понимания особенностей языка программирования, инструментов и фреймворков. Кроме того, необходимо учитывать требования к безопасности и защите данных, а также особенности конкретной организации и ее бизнес-процессов.

СПИСОК ЛИТЕРАТУРЫ

1. Официальная документация Java. URL: https://www.java.com/en/ (дата обращения: 24.09.2023)
2. Официальная документация Spring. URL: https://spring.io/ (дата обращения: 03.10.2023)
3. Официальная документация PostgreSQL. URL: https://www.postgresql.org/ (дата обращения: 04.02.2023)
4. Spring Data JPA - Reference Documentation. URL: https://docs.spring.io/spring-data/jpa/docs/current/reference/html/ (дата обращения: 03.10.2023)
5. Флэнаган Д. JavaScript. Полное руководство. 7-е издание. – М.: Диалектика, 2021. 1080 с

УДК 004.91

ПРИМЕНЕНИЕ ИС ПРИ ВЕДЕНИИ БУХГАЛТЕРСКОГО УЧЕТА НА МАЛЫХ ПРЕДПРИЯТИЯХ

Горина Елена Владимировна, Тимофеева Елена Анатольевна
Санкт–Петербургский государственный университет промышленных технологий и дизайна
Большая Морская, ул., 18, Санкт-Петербург, 191186, Россия
e-mail: 12345ele@mail.ru

Аннотация. Эффективность работы малого предприятия складывается из различных показателей. Экономические показатели должны обрабатываться в условиях высокой конкуренции. Проведя аналитику программных продуктов, которые упрощают управленческий процесс, можно принять правильное направление по автоматизации бухгалтерского учета на предприятии.

Ключевые слова: малый бизнес; бухгалтерский учет; автоматизация; информационные технологии; программные продукты.

APPLICATION OF IS IN ACCOUNTING IN SMALL ENTERPRISES

Gorina Elena, Timofeeva Elena
Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya, st., St. Petersburg, 191186, Russia
e-mail: 12345ele@mail.ru

Abstract. The operational efficiency of a small business is formed by various factors. Economic indicators should be processed in a highly competitive climate. Once you've analyzed the software which facilitates the management process, it is possible to take the right direction in automating the accounting in your business.

Keywords: small business; accounting; automated; information technologies; software

Введение. Малый бизнес - одна из наиболее актуальных тем предпринимательства. Объясняется это, прежде всего, тем, что именно малый бизнес во многих областях деятельности может обеспечить реальные условия для подъема экономики и выхода России из экономического кризиса. Поэтому государственными органами финансируются различные экономические программы, принимаются законодательные акты, облегчающие ведения бизнеса проводиться исследования и внедряются новейшие технологии, позволяющие вести эффективную предпринимательскую деятельность.

Одним из показателей эффективности работы малого предприятия, является грамотное ведения бухгалтерского учета, что особенно важно в условиях финансового кризиса. В современном мире бухгалтерский учет является одним из самых важных аспектов любого бизнеса. Бухгалтерский учет позволяет компаниям следить за своей финансовой деятельностью, контролировать расходы и доходы, а также отслеживать эффективность своих инвестиций. Однако, с ростом технологий и увеличением объемов информации, которую необходимо обрабатывать, бухгалтерский учет становится все более сложным и требует новых подходов к его ведению. Конкурентные преимущества организации в настоящее время могут обеспечить только передовые технологии.

Поэтому в области финансового сопровождения все более актуальной становится автоматизация бухгалтерского учета [1]. Одним из таких подходов является применение информационных систем (ИС) при ведении бухгалтерского учета. ИС позволяют автоматизировать процессы сбора, обработки и хранения информации, что значительно уменьшает вероятность ошибок и упрощает работу бухгалтеров. Кроме того, ИС позволяют быстро получать доступ к нужной информации и анализировать ее, что помогает принимать более обоснованные решения. Применение ИС в бухгалтерском учете имеет множество преимуществ. Во-первых, это повышение точности и надежности учета. Автоматизация процессов позволяет исключить возможность человеческих ошибок и уменьшить вероятность мошенничества. Во-вторых, это ускорение процессов учета. Благодаря ИС бухгалтеры могут быстрее обрабатывать информацию и генерировать отчеты, что позволяет компаниям быстрее реагировать на изменения в своей деятельности. В-третьих, это снижение затрат на учет. Использование ИС позволяет сократить количество бумажной документации и снизить расходы на ее хранение.

Преимущества системы очевидны: исключается воздействие человеческого фактора, так как бухгалтерский учет полностью упорядочивается, повышается оперативность работы, уменьшаются риски потери информации. Бухгалтерская служба не только обеспечивает подготовку и хранение необходимой информации о финансовой деятельности организации, но и формирует бухгалтерскую и налоговую отчетность. Выполнить успешно данную функцию на сегодняшний день позволит лишь автоматизация бухгалтерского учета. Однако, применение ИС в бухгалтерском учете также имеет свои недостатки. Во-первых, это высокие затраты на внедрение и поддержку системы. Разработка и внедрение ИС требует больших финансовых затрат, а также квалифицированных специалистов для ее поддержки и обновления. Во-вторых, это угроза информационной безопасности. Использование ИС может быть связано с риском утечки конфиденциальной информации, поэтому необходимо принимать меры по ее защите.

Сегодня на рынке имеется обширный ряд программ по автоматизации бухгалтерского учета, такие программы как: 1С: Бухгалтерия, Aubi, Супер Менеджер, ИНФО - Бухгалтер, Парус-бухгалтерия, Инфин - Бухгалтерия, ABACUS, Турбо-бухгалтер. Каждая из которых отвечает всем последним требованиям учета и обладает рядом несомненных достоинств.

Автоматизация бухгалтерского учета на малых предприятиях становится все более популярной. Это связано с тем, что автоматизация позволяет сократить время на ведение бухгалтерского учета, уменьшить количество ошибок и повысить качество работы [2].

Одним из главных преимуществ автоматизации бухгалтерского учета является возможность быстрого получения информации о финансовом состоянии предприятия. Автоматизированные системы позволяют в режиме реального времени отслеживать движение денежных средств, контролировать задолженности и т.д.

Кроме того, автоматизация бухгалтерского учета позволяет сократить количество ошибок, связанных с ручным вводом данных. Автоматические системы не только уменьшают вероятность ошибок, но и позволяют быстро обнаружить и исправить их.

Важным преимуществом автоматизации является также возможность ускорения процесса закрытия периода. Автоматические системы позволяют быстро проводить расчеты и формировать отчетность, что позволяет сократить время на закрытие периода и уменьшить вероятность ошибок.

Кроме того, автоматизация бухгалтерского учета позволяет сократить затраты на содержание бухгалтерии. Автоматические системы позволяют снизить количество сотрудников, занятых ведением бухгалтерского учета, что позволяет сократить расходы на зарплату и налоги.

Наконец, автоматизация бухгалтерского учета позволяет повысить качество работы бухгалтерии. Автоматические системы позволяют быстро обрабатывать большие объемы информации, что позволяет бухгалтерам сосредоточиться на анализе данных и принятии правильных решений.

Найти оптимально подходящую бухгалтерскую программу очень сложная задача. При таком богатстве выбора задача главного бухгалтера сводится к выбору не более дорогой или дешевой программы, а именно к выбору подходящей. Как решить данную делему? Кому обратиться с таким вопрос, кто же может дать грамотную консультацию?

Однако, существует несколько критериев, которые помогут выбрать оптимальную программу для автоматизации бухгалтерского учета на малом предприятии [3].

Первым критерием является соответствие программы требованиям законодательства. Программа должна учитывать все изменения в законодательстве и иметь возможность формирования отчетности в соответствии с требованиями налоговой службы.

Вторым критерием является простота и удобство использования программы. Программа должна быть интуитивно понятной и иметь понятный интерфейс, чтобы ее могли использовать не только профессиональные бухгалтеры, но и люди без специального образования в этой области.

Третьим критерием является функциональность программы. Программа должна позволять вести учет всех операций, связанных с финансовой деятельностью предприятия, а также иметь возможность формирования отчетности и анализа финансовых показателей.

Четвертым критерием является цена программы. Программа должна быть доступной по цене и не создавать дополнительных затрат на ее установку и обслуживание.

Пятый критерий — это поддержка и обновление программы. Программа должна иметь регулярные обновления и техническую поддержку, чтобы быть всегда актуальной и работать без сбоев.

Выбор оптимальной программы для автоматизации бухгалтерского учета на малом предприятии может быть сложным, но при соблюдении вышеперечисленных критериев можно выбрать программу, которая наилучшим образом подходит для конкретных потребностей предприятия [4].

Наиболее популярные программы: «1С: Бухгалтерия», «Инфо-бухгалтер», «Парус-бухгалтерия», требуют детального рассмотрения.

«1С: Бухгалтерия»

Данная программа является универсальной бухгалтерской программой и предназначена для ведения синтетического и аналитического бухгалтерского учета по различным разделам.

Аналитический учет ведется по объектам аналитического учета (субконто) в натуральном и стоимостном выражениях. Программа предоставляет возможность ручного и автоматического ввода проводок. Все проводки заносятся в журнал операций. При просмотре проводок в журнале операций их можно ограничить произвольным временным интервалом, группировать и искать по различным параметрам проводок.

В программе существует режим формирования произвольных отчетов, позволяющий на некотором бухгалтерском языке описать форму и содержание отчета, включая в него остатки и обороты по счетам и по объектам аналитического учета. С помощью данного режима реализованы отчеты, предоставляемые в налоговые органы, кроме того, данный режим используется для создания внутренних отчетов для анализа финансовой деятельности организации в произвольной форме.

Существует несколько модификаций системы: базовая, профессиональная (для решения более сложных бухгалтерских задач, включающих элементы анализа хозяйственной деятельности предприятий), сетевая.

Система «1С: Предприятие» может быть адаптирована к любым особенностям учета на конкретном предприятии при помощи модуля «1С: Конфигуратор», позволяющего настраивать все основные элементы программной среды, генерировать и редактировать документы с любой структурой, изменять их экранные и печатные формы, формировать журналы для работы с документами с возможностью их произвольного распределения по журналам.

Система «Парус-бухгалтерия» предназначена для подготовки и учета документов финансово-хозяйственной деятельности предприятия, накопления информации о совершенных хозяйственных операциях на бухгалтерских счетах, получения внутренней и внешней отчетности. Система поставляется в различных комплектациях в зависимости от необходимости ведения учета операций в валюте, расширенного аналитического учета, учета торговых операций.

Основные возможности системы:

– учет основных средств, материалов и МБП;

– учет финансово-расчетных операций: подготовка платежных банковских и кассовых документов; учет операций по расчетному, валютному и прочим счетам; учет кассовых операций; учет всех видов взаимных расчетов;

– начисление заработной платы: расчет заработной платы по основной, совмещаемой и замещаемой должностям; расчет налогов и удержаний, оформление возврата сумм и перерасчет заработной платы; учет приказов по кадрам и оплате труда; формирование справок и налоговой отчетности; расчет выплат по больничным листам, отпускных, пособий на детей; печать расчетно-платежных ведомостей, расходных кассовых ордеров; перечисление зарплаты через банк; формирование сводов по заработной плате и журналов-ордеров;

– отчеты: книга учета хозяйственных операций; ведомости аналитического учета (журналы-ордеры); главная книга; оборотный баланс; баланс и все формы приложений к балансу; отчетные документы по расчету налогов; справки о наличии и движении денежных средств и материальных ценностей.

Введен новый механизм, позволяющий пользователю самостоятельно настраивать формы всех документов по реализации (накладные, счета, заказы и пр.), вводить несколько форм одного и того же документа, а также добавлять в систему документы, разработанные пользователем.

Предоставлена возможность вести учет хозяйственной деятельности в рублевом эквиваленте и различных валютах без ограничения количества валют. По каждой валюте ведется история курса по отношению к рублю для выполнения последующих перерасчетов и переоценок валютных активов и пассивов на любое число. Эта подсистема предназначена для финансовых служб предприятий, главных бухгалтеров, руководителей и позволяет:

– планировать предстоящие доходы и расходы, объединив их в финансовый план. План формируется на основе как разовых событий (ремонт помещения, приобретение мебели и т.п.), так и повторяющихся (уплата налогов, арендная плата и т.п.);

– контролировать платежи, оптимизировать финансовую деятельность, осуществлять анализ фактического исполнения планов;

– осуществлять расчет и анализ итоговых финансово-экономических показателей;

– проводить анализ реального финансового состояния предприятий по группам: структура имущества, собственные и заемные средства, оборотные средства и их источники, ликвидность, финансовая устойчивость, интенсивность использования ресурсов, рентабельность капитала и продаж;

– представлять результаты обработки информации в графическом виде (графики, диаграммы).

Еще одним из лидеров в этой области является программа для автоматизации малого и среднего бизнеса, для ведения бухучета в торговле - «Инфо – Бухгалтерский учет». Преимущество этого программного обеспечения в легкости установки, удобстве использования, в надежности системы и простоте освоения. Это чуть ли не единственная программа на огромном рынке бухгалтерских продуктов, работать на которой можно сразу, без прохождения этапа обучения. Бухгалтерский калькулятор, возможность внесения поправок «задним числом», интегрированная правовая система «Гарант», система генерации отчетов, полный комплект отчетных документов и многое другое - все, что необходимо бухгалтеру, программа обеспечивает надежную сохранность информации, адаптирована к различным режимам налогообложения, оснащена всеми разделами бухгалтерского и налогового учета.

К основным возможностям «Инфо - Бухгалтера» относятся автоматическое выполнение проводок, а также ручная корректировка, автоматическое заполнение всех ведомостей, главной книги, журналов - ордеров, ведение аналитического и синтетического учета, расчет амортизации и заработной платы и многое другое.

При проведении сравнительного анализа данных программ выясняется, что наиболее функциональным приложением является приложение «1С: Бухгалтерия». Следует также отметить и невысокую цену этой программы, что, несомненно, является положительны фактором для предприятий малого бизнеса. Но все это не говорит о том, что непременно нужно использовать на предприятии данную программу.

В Парус-бухгалтерия можно построить ту систему учета, которая нужна с учетом специфики предприятия. Можно самостоятельно «подогнать» любой документ или сделать новый, свободно создавать счета и субсчета, а в журналах операций - нужные подразделы. Однако и тут не обошлось без недостатков, основным из которых является высокая цена внедрения данного приложения. Можно сделать выводы. Для предприятий малого бизнеса наиболее приемлемыми приложениями являются «1С: Бухгалтерия» и «ИНФО-Бухгалтерский учет». Предпочтения между ними могут отдаваться уже исходя из целей и средств предприятий, на основе анализа положительных и отрицательных сторон. В свою очередь для предприятий со специфической формой построения бухгалтерского учета более удобным будет использование программы Парус-бухгалтерия, так как в нем можно построить ту систему учета, которая нужна с учетом специфики предприятия.

Польза от удобной и надежной бухгалтерской системы намного превосходит расходы на ее внедрение и сопровождение, а также дает юридические гарантии, ведь речь идет об учете материальных ценностей и денежных средств, сохранности персональных данных, минимизации возможных штрафов от контролирующих органов. Помимо этого, зарегистрированные пользователи получают квалифицированную техническую поддержку как удаленно, так и с выездом специалиста в офис клиентов.

Заключение. Применение ИС при ведении бухгалтерского учета имеет множество преимуществ, но также требует серьезного подхода к решению проблем информационной безопасности и высоких затрат на внедрение и поддержку системы. В целом, ИС являются важным инструментом для повышения эффективности бухгалтерского учета и помогают компаниям принимать более обоснованные решения. Важно понимать, что программа – это лишь инструмент в руках бухгалтера, а не решение всех проблем. Немаловажным фактором полноценного использования всего заложенного в систему потенциала является обучение сотрудников.

Таким образом, автоматизация бухгалтерского учета на малых предприятиях является важным шагом на пути к повышению эффективности работы и улучшению финансового состояния предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Шадиева, М. Ю. Некоторые особенности организации бухгалтерского и налогового учета субъектами малого бизнеса / М. Ю. Шадиева, Б. М. Мусаева // Естественно-гуманитарные исследования. –2021. - №34(2). – С. 332-336.
2. Приказ Минфина России от 02.07.2010 № 66н (ред. от 19.04.2019) «О формах бухгалтерской отчетности организаций» (Зарегистрировано в Минюсте России 02.08.2010 № 18023) (с изм. и доп., вступ. в силу с отчетности за 2020 год)
3. Беликова Т.Н. Бухгалтерский учет и отчетность от нуля до баланса: практ. курс / Т.Н. Беликова. – Санкт-Петербург: Питер, 2016. – 239 с.
4. Бухгалтерский учет: Учебник / Под ред. проф. В.Г. Гетьмана. – 2-е изд., перераб. и доп. – Москва: Инфра-М, 2017. – 601 с. 5. Лытнева Н.А. Бухгалтерский учет: Учебник / Н.А. Лытнева, Л.И. Малявкина, Т.В. Федорова. – 2-е изд., перераб. и доп. – Москва: Форум: Инфра-М, 2013. – 512 с

УДК 004.45

ИНТЕГРАЦИЯ ПРИНЦИПОВ БЕЗОПАСНОСТИ В ПРОЦЕСС РАЗРАБОТКИ ПО НА JAVA: ЛУЧШИЕ ПРАКТИКИ И РЕКОМЕНДАЦИИ

Дроздова Елена Николаевна, Смирнов Артемий Михайлович
Санкт–Петербургский государственный университет промышленных технологий и дизайна
Большая Морская, ул., 18, Санкт-Петербург, 191186, Россия
e-mails: endrozdova2@list.ru, amsmirnov.pub@gmail.com

Аннотация. В статье обсуждается важность и методы интеграции принципов безопасности в жизненный цикл разработки программного обеспечения на платформе Java. Основываясь на лучших практиках и рекомендациях в области кибербезопасности, статья представляет обзор ключевых аспектов, включая аутентификацию, авторизацию, шифрование данных и методы защиты. Описывая методы и концепции, направленные на обеспечение конфиденциальности информации и предотвращение уязвимостей, статья также предлагает руководство по интеграции данных принципов безопасности в процесс разработки, начиная с ранних стадий и до завершения проекта. Все эти меры нацелены на создание безопасного и надежного программного обеспечения, соответствующего современным стандартам безопасности и ожиданиям пользователей.

Ключевые слова: безопасность ПО; интеграция безопасности; разработка на java; рекомендации по безопасности; аутентификация; авторизация; шифрование данных; кибербезопасность; уязвимости приложений java; криптография; принципы безопасности разработки; конфиденциальность данных; защита информации; жизненный цикл ПО.

INTEGRATING SECURITY PRINCIPLES INTO THE JAVA SOFTWARE DEVELOPMENT PROCESS: BEST PRACTICES AND RECOMMENDATIONS

Drozdova Elena, Smirnov Artemy
Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya, st., St. Petersburg, 191186, Russia
e-mails: endrozdova2@list.ru, amsmirnov.pub@gmail.com

Abstract. This paper discusses the importance and methods of integrating security principles into the Java platform software development lifecycle. Based on cybersecurity best practices and best practices, the article provides an overview of key aspects including authentication, authorization, data encryption, and security techniques. While describing techniques and concepts aimed at ensuring information privacy and preventing vulnerabilities, the article also offers guidance on integrating these security principles into the development process, from the early stages through the completion of a project. All these measures are aimed at creating safe and reliable software that meets modern security standards and user expectations.

Keywords: software security; security integration; Java development; security recommendations; authentication; authorization; data encryption; cybersecurity; Java application vulnerabilities; cryptography; development security principles; data confidentiality; information protection; software life cycle.

Введение. Разработка программного обеспечения на языке Java сталкивается с многочисленными угрозами безопасности, требующими внимательного анализа и выявления. Идентификация рисков является первым шагом к эффективной интеграции принципов безопасности в разрабатываемое программное обеспечение [1].

1. Анализ угроз безопасности в разработке по на Java: обзор и идентификация потенциальных рисков

Рассмотрим классификацию уязвимостей Java-приложений.

Уязвимости, связанные с ошибками программирования. Рассмотрение ошибок в программировании, таких как недостаточная обработка исключений, некорректное использование API или слабая проверка ввода данных, является ключевым аспектом определения уязвимостей в Java-приложениях.

Угрозы, связанные с конфиденциальностью данных. Идентификация и анализ угроз, которые могут привести к компрометации конфиденциальности данных, включая утечку информации, недостаточную защиту хранимых данных или слабые механизмы шифрования.

Аутентификация и авторизация. Оценка уровня угроз, связанных с процессами аутентификации и авторизации в приложениях Java, включая возможные слабости в системах идентификации, утечки учетных данных или несанкционированный доступ [2].

Уязвимости системы управления безопасностью. Анализ угроз, касающихся слабостей в системах управления безопасностью, включая ошибки в настройках доступа, утечки конфиденциальных ключей или слабые механизмы аудита и мониторинга.

Далее рассмотрим методы идентификации и анализа угроз.

Статический анализ кода. Использование специализированных инструментов для обнаружения потенциальных уязвимостей в исходном коде Java-приложений путем проверки на соответствие передовым стандартам безопасности.

Динамическое тестирование приложений. Применение методов динамического тестирования для выявления уязвимостей в работающем приложении путем анализа его поведения в реальном времени.

Аудит безопасности. Проведение систематического аудита безопасности приложений с целью обнаружения потенциальных угроз и уязвимостей в рамках всего процесса разработки.

Анализ угроз безопасности в разработке программного обеспечения на Java является важным этапом для эффективной интеграции принципов безопасности. Идентификация потенциальных рисков позволяет разработчикам принимать целенаправленные меры по усилению защиты и предотвращению возможных угроз, обеспечивая более надежное и безопасное программное обеспечение [3].

Интеграция принципов безопасности в жизненный цикл программного обеспечения является критическим аспектом обеспечения безопасности приложений.

2. Принципы защиты и отладки в процессе разработки на Java: интеграция безопасности в жизненный цикл ПО

Рассмотрим принципы защиты в жизненном цикле ПО.

Принцип безопасности по умолчанию. Важность предоставления наиболее безопасной конфигурации по умолчанию для приложений Java, минимизируя поверхность атак и устанавливая настройки безопасности как первоочередные.

Принцип необходимости минимальных привилегий. Ограничение привилегий приложений на Java до минимально необходимого уровня для выполнения определенных задач с целью предотвращения распространения угроз.

Принцип защиты данных. Использование современных методов шифрования и защиты данных при работе с конфиденциальной информацией в приложениях Java.

Далее рассмотрим интеграцию безопасности в жизненный цикл ПО.

Анализ безопасности в фазе проектирования. Внедрение процесса анализа угроз безопасности на стадии проектирования приложения с целью выявления уязвимостей и разработки соответствующих мер безопасности.

Разработка с ориентацией на безопасность. Интеграция практик разработки, учитывающих аспекты безопасности, таких как проверка ввода данных, обработка ошибок и предотвращение утечек данных.

Тестирование и отладка безопасности. Использование инструментов для тестирования безопасности и отладки с целью выявления и исправления уязвимостей в приложениях Java на ранних стадиях разработки.

3. Концепции аутентификации и авторизации в приложениях Java: гарантирование доступа и контроль привилегий

В контексте разработки программного обеспечения на платформе Java, обеспечение аутентификации и авторизации является фундаментальным аспектом безопасности. Эффективное управление аутентификацией и авторизацией имеет критическое значение для предотвращения несанкционированного доступа к данным и ресурсам приложения [4].

Рассмотрим концепцию аутентификации в приложениях Java.

Идентификация пользователей. Процесс аутентификации включает в себя идентификацию пользователей с использованием уникальных учетных данных, таких как логины и пароли. Дополнительные методы аутентификации могут включать биометрическую аутентификацию и использование многофакторной аутентификации.

Управление сессиями. Сессионное управление в Java-приложениях позволяет создавать и управлять сеансами пользователей, а также обеспечивать их безопасность и конфиденциальность.

Далее рассмотрим концепцию авторизации и контроль привилегий.

Определение ролей и прав. Разработка ролей и прав доступа для пользователей позволяет определить, какие действия и ресурсы могут быть доступны каждой группе пользователей. Это обеспечивает детализированный контроль привилегий.

Политики авторизации. Определение политик авторизации, которые определяют, какие действия могут выполнять пользователи в зависимости от их роли и прав. Эти политики обеспечивают централизованный контроль над доступом.

Рассмотрим интеграцию и защиту ключевых компонентов.

Защита данных аутентификации. Сохранение учетных данных пользователей и паролей в безопасной форме, например, с использованием хэширования и соли, для предотвращения утечек информации.

Защита сессионных данных. Защита данных сессий пользователей от атак, таких как угон сессии и перехват данных, с использованием средств, таких как шифрование.

Аутентификация и авторизация играют важную роль в обеспечении безопасности приложений на платформе Java. Грамотное управление этими процессами позволяет гарантировать доступ и контроль привилегий, обеспечивая защиту данных и ресурсов.

4. Применение шифрования и криптографии в разработке ПО на Java: обеспечение конфиденциальности данных

В мире современных информационных технологий и передачи данных конфиденциальность информации играет ключевую роль. В рамках разработки программного обеспечения на платформе Java, применение шифрования и криптографии становятся неотъемлемой частью обеспечения конфиденциальности данных.

Рассмотрим основы криптографии.

Шифрование данных. Процесс шифрования позволяет преобразовывать исходные данные в нечитаемый формат, который может быть расшифрован только с использованием соответствующего ключа. В Java существует множество криптографических алгоритмов для шифрования данных.

Ключи шифрования. Ключи шифрования играют решающую роль в процессе шифрования и дешифрования данных. Их безопасное хранение и обмен является критически важным для предотвращения утечек информации.

Рассмотрим принципы защиты данных в приложениях Java.

Шифрование хранимых данных. Защита конфиденциальности данных, хранящихся в базах данных или файловых системах, путем их шифрования, чтобы предотвратить несанкционированный доступ.

Шифрование коммуникаций. Защита данных, передаваемых между клиентом и сервером, с использованием шифрования внутри приложений Java для предотвращения перехвата данных и атак на целостность.

Управление ключами. Реализация строгой политики управления ключами, включая их генерацию, хранение и обновление, с целью обеспечения безопасности шифрования.

Рассмотрим процессы аудита и мониторинга.

Аудит криптографии. Проведение аудита криптографических операций и ключевых компонентов для выявления аномалий и нарушений безопасности.

Мониторинг безопасности. Внедрение систем мониторинга безопасности для реагирования на потенциальные инциденты и угрозы в реальном времени.

Применение шифрования и криптографии в разработке ПО на платформе Java является критически важным аспектом обеспечения конфиденциальности данных. Грамотное использование криптографических методов и алгоритмов, а также строгое соблюдение практик безопасности, помогают предотвращать утечки информации и обеспечивать надежную защиту данных.

Заключение. В процессе разработки программного обеспечения на языке Java, интеграция принципов безопасности становится неотъемлемой частью обеспечения надежности и защиты данных. В данной статье рассмотрены основные аспекты, касающиеся лучших практик и рекомендаций по обеспечению безопасности в процессе разработки ПО на платформе Java.

В процессе анализа различных аспектов безопасности в разработке на Java были рассмотрены ключевые моменты, такие как аутентификация, авторизация, шифрование данных, обнаружение уязвимостей и принципы безопасности по умолчанию. Рассмотрены основные практики по интеграции этих принципов в жизненный цикл разработки программного обеспечения, начиная от стадии проектирования и до релиза продукта.

Основные рекомендации включают в себя строгое следование принципам безопасности на каждом этапе разработки, регулярное тестирование на уязвимости и внедрение методов безопасности, таких как шифрование данных и многофакторная аутентификация. Кроме того, внедрение обучения и постоянное обновление знаний команды по вопросам безопасности является ключевым фактором для поддержания безопасного процесса разработки [5].

Безопасность в разработке ПО на Java требует постоянного внимания и актуальных знаний по методам защиты. Предоставленные в статье рекомендации и лучшие практики призваны обеспечить не только надежность и безопасность создаваемого программного обеспечения, но и содействовать общей защите данных и приватности пользователей.

Итак, внедрение и последовательное следование рекомендациям по безопасности в разработке ПО на Java является необходимым условием для создания надежных, защищенных и доверительных приложений, соответствующих современным стандартам безопасности и требованиям пользователей.

СПИСОК ЛИТЕРАТУРЫ

1. Шилдт Г. Java 8. Полное руководство: Пер. с англ. – М.: ООО «И.Д. Вильямс», 2015. – 1376 с.
2. Смирнов А.М. Какие методы использует https, которые делают его более безопасным, чем http? // Вестник молодых ученых СПГУТД. № 1 (2022), с. 25-27
3. Смирнов А.М. Методы https, которые делают его более безопасным, чем http // Инновации молодежной науки тезисы докладов (2022), с. 77
4. Gaddis T. Starting Out With JavaTM. From Control Structures through Objects. – Haywood Community College: Pearson Education, Inc., 2016. – 1435 p.
5. Savitch W. Absolute Java. - Harlow: Pearson Education Ltd, 2016. – 1295 p.

УДК 004.43

ИСПОЛЬЗОВАНИЕ СРЕДСТВ MATLAB В СИСТЕМАХ РАСПОЗНАВАНИЯ

Кириллов Родион Олегович, Шефер Елена Александровна
Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
e-mails: kirillov3511@gmail.com, elenashefer2014@yandex.ru

Аннотация. В статье рассматриваются возможности Matlab, используемые в распознавании образов. Проблема распознавания образов в последнее время является наиболее актуальной и используется во многих сферах деятельности. Произведен анализ методов морфологии и сегментации изображений, который подтвержден примерами, выполненными в программной среде Matlab.

Ключевые слова: образ; бинарное изображение; морфология; сегментация; цифровая обработка изображений; системы распознавания.

USING MATLAB TOOLS IN RECOGNITION SYSTEMS

Kirillov Rodion, Shefer Elena
Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya, st., St. Petersburg, 191186, Russia
e-mails: kirillov3511@gmail.com, elenashefer2014@yandex.ru

Abstract. The article considers the capabilities of Matlab which used are used in image recognition. The problem of image recognition is the most important and is used in many fields of activity. The analysis of methods of morphology and segmentation of images, which is confirmed by examples performed in the Matlab software environment, executed.

Keywords: image; binary image; morphology; segmentation; digital image processing; recognition systems.

Введение. Во многих сферах деятельности человека, в том числе и в геоинформационных системах, решаются задачи распознавания образов, которые могут быть использованы в видеонаблюдении, мониторинге территорий, распознавании движущихся объектов, дорожных знаков, лиц и т.д. В задачах распознавания объектов применяют как традиционные методы обработки изображений, так и современные методы, например, сети глубокого обучения. В таких задачах рассматривается не сам объект, а его приближение, или образ, который можно представить определенным набором характеристик [1].

1. Классификация методов Matlab

В системе Matlab имеется определенный набор функций, используемых в распознавании областей и границ. Такие области также называют объектом или образом. Методы системы Matlab, используемые в распознавании образов, можно разделить на две группы: теории решений и структурного анализа. В первом случае используется описание количественных дескрипторов, основанное на векторе признаков, природа которого зависит от подхода к описанию объекта. Например, задача распознавания знаков. В основе методов второй группы лежит символьная информация [1]. В некоторых случаях характеристики объектов описывают с помощью структурных связей. Это видно при работе с мелкими деталями, например, в спутниковых снимках, где помимо относительных размеров и расположения данные признаки описывают свойства линий рельефа. В таких задачах принадлежность объекта к определенному классу определяется не только количественными параметрами, но и пространственными отношениями [2].

Ниже будут рассмотрены наиболее часто используемые методы морфологии и сегментации, которые подтверждены примерами, отработанными в системе Matlab путем компиляции программных кодов. В качестве исходных данных взяты определенного типа изображения, которым присущи такие характеристики, чтобы отразить картину работы каждого из рассмотренных методов [3].

2. Морфологические операции

В обработке изображений особое место занимают морфологические операции, основанные на идентификации и извлечении значимых дескрипторов из формы изображения. В основе этих методов лежит сегментация с автоматизированным подсчетом и проверкой. Морфологические операции могут быть применены к изображениям всех типов, но основное их использование заключается в обработке двоичных изображений. В данном случае двоичное (бинарное) изображение — это изображение, в котором каждый пиксель является одним из двух возможных дискретных значений, логические значения которых равны 1 или 0 [2]. В обработке изображения логическое значение 1 воспринимается, как изображение пикселей переднего плана, в то время как пиксели, имеющие логическое значение 0, являются фоновыми пикселями. Объект в двоичном изображении состоит из группы связанных между собой пикселей. Связи бывают четырехсвязные и восьмисвязные, в зависимости от расположения пикселей переднего плана.

Ключевыми морфологическими операциями являются дилатация (dilation) и эрозия (erosion). Все другие морфологические операции могут быть определены в терминах этих операторов [1, 2].

Механизм дилатации и эрозии схожи с пространственной фильтрацией [2]. Структурообразующий элемент перемещается по изображению так, что его центральный пиксель последовательно располагается поверх каждого пикселя переднего плана или пикселя фона. Затем новое значение каждого пикселя изображения зависит от значений пикселей в окрестности, определяемой структурообразующим элементом. При выполнении операции эрозии рассматриваются все те места в изображении, в которых структурообразующий элемент может быть размещен полностью поверх пикселей переднего плана изображения. Именно эти пиксели будут подвержены эрозии. В результате операции получим изображение, в котором значения пикселов, соответствующих положению центра структурообразующих элементов, равно 1. Таким образом, эрозия «истончает» границы. Дилатация выполняется аналогичным способом, а именно, рассматриваются те области изображения, в которых структурообразующий элемент может быть размещен так, чтобы полностью перекрывать пиксели фона. В результате выполнения операции эти пиксели останутся фоновыми и сформируют расширенное изображение (dilated image). Таким образом, дилатация приводит к расширению границ.

В пакете Image Processing Toolbox (IPT) имеются команды imdilate и imerode, позволяющие выполнять эти операции. Как правило, данные команды используют совместно с функцией strel, потому что, во-первых, все наиболее распространенные типы структурирующих элементов могут быть указаны непосредственно в качестве входных данных, во-вторых, в этом случае вычисление дилатации и эрозии выполняется наиболее эффективно. Эта эффективность основана на том, что дилатация за счет крупных структурирующих элементов часто может быть достигнута декомпозицией структурирующих элементов. На рис. 1 представлены результаты выполнения операций дилатации и эрозии.

В данном случае видно, что дилатация удаляет мелкие границы исходного изображение при сохранении наиболее существенных деталей, в то время, как эрозия наоборот расширяет структуру исходного изображения, делая акцент на темных участках, нежели при дилатации. При этом, функция strel позволяет использовать дилатацию и эрозию наиболее эффективно [3].

В Matlab имеется возможность определения границ объекта путем его свертки с подходящим структурообразующим элементом и последующим вычитанием результата из исходного изображения. Наиболее интересные данные можно получить при извлечении связанных компонент изображения, что приводит к новому изображению, в котором связанным группам пикселей (объектам) присваиваются последовательные целые значения. В задачах распознавания операция извлечения границ достаточно распространена и может быть выполнена с помощью функции bwlabel [2].

а б в

Рис. 1. Пример выполнения дилатации и эрозии с использованием функции strel:
а – исходное бинарное изображение; б – дилатация; в - эрозия

На рис. 2 представлено исходное изображение, у которого были определены границы объектов, а результатом является вычитания выявленных границ из исходного изображения [3].

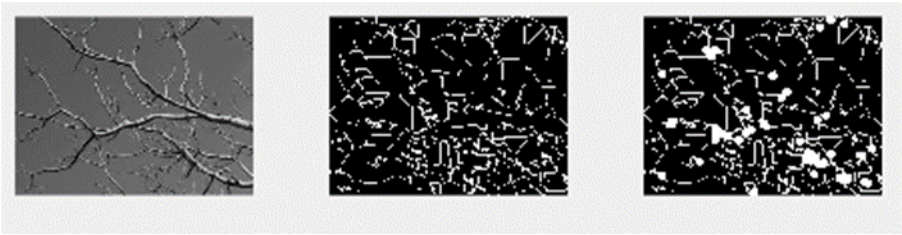
а б в

Рис. 2. Извлечение границ объектов
а – исходное бинарное изображение; б – определение границ объектов;
в – результат вычитания границ из исходного изображения

При выполнении морфологических операций в большинстве случаев требуется произвести корректировку границ с помощью операций размыкания (Opening) и замыкания (Closing). Размыкание — это морфологическая операция, заключающаяся в эрозии с последующей дилатацией тем же структурообразующим элементом. При размыкании в бинарном изображении происходит удаление мелких нежелательных объектов. Эрозия выбирает элемент определенного размера и гарантирует удаление любых объектов, внутри которых этот элемент отсутствует. Замыкание — это морфологическая операция, заключающаяся в дилатации с последующей эрозией с тем же структурообразующим элементом [1]. В результате операции Closing удаляются небольшие пробелы на переднем плане, а узкие участки между объектами соединяются.

Операции размыкания и замыкания используются для удаления с изображение шумовых элементов, что невозможно сделать, используя только низкоуровневые фильтры.

В проблеме распознавания часто встречается задача нахождения базовой формы объекта, приведенной к минимальному уровню. Для этого используют операцию скелетизации, которая показывает топологию объекта и числовые показатели, которые можно использовать для сравнения и категоризации [2]. Топология определяется количеством узлов (где встречаются ответвления) и количеством конечных точек, а метрическая информация представлена длинами ответвлений и углами между ними. Но эта операция может быть выполнена только с определенными изображениями, т.к., например, незначительные неровности границы могут привести к ложным ответвлениям в скелете, которые могут помешать процессам распознавания [3]. На рис. 3 представлен результат скелетизации полутонового изображения, а последующая дилатация показывает более четкий скелет.



а б в

Рис. 3. Демонстрация метода скелетизации: а – исходное изображение;
б – результат скелетизации; в – скелетизация с последующей дилатацией

В некоторых случаях для того, чтобы подчеркнуть детали, используется преобразование Top-hat, которое позволяет выделять и извлекать мелкие детали в изображении за счет комбинации эрозии и дилатации. Это можно использовать для отделения объекта от фона. Результатом преобразования является разность между исходным изображением и изображением после операции размыкания [3]. В полученном изображении детали распознаются независимо от изменения интенсивности отдельных участков. По этой причине этот метод целесообразно использовать в тех случаях, когда присутствуют области изменения освещения или затемнения. На рис. 4 представлены результаты преобразования Top-hat с бинарным и полутоновым изображением.

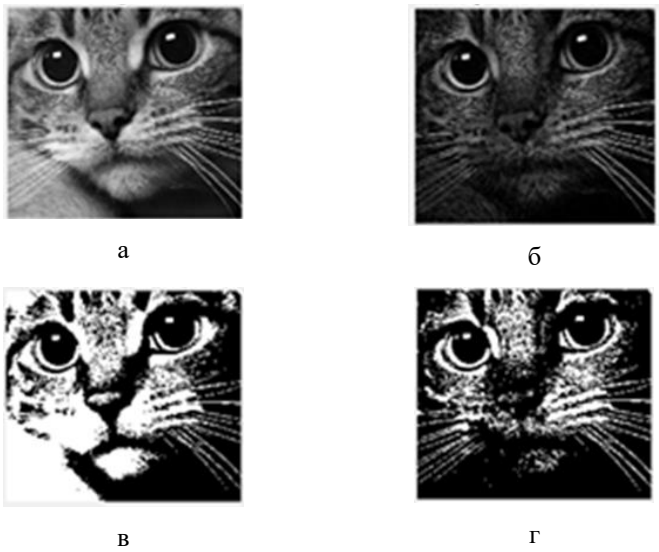


Рис. 4. Преобразование Top-hat: а – исходное полутоновое изображение; б – результат преобразования Top-hat; в – исходное бинарное изображение; г – результат преобразования Top-hat

3. Сегментация изображений

Если операции морфологии, рассмотренные выше, в большинстве своем, относятся к низкоуровневым методам обработки изображения, то сегментация является следующим шагом в процедурах распознавания образов [1]. Сегментация — это процесс, посредством которого изображение подразделяется на составляющие его области или объекты, а степень детализации зависит от решаемых задач. Сегментация является одной из самых сложных задач при проектировании систем компьютерного зрения и остается активной областью исследований в области обработки изображений и машинного зрения [4].

Основной целью сегментации является разделение изображения на взаимоисключающие помечаемые области. Сегментированные объекты часто называют передним планом, а остальную часть изображения — фоном. В методах сегментации определяются такие характеристики изображений, которые можно изменять: цвет, текстура, движение. В большинстве случаев в качестве информации перед сегментацией используют комбинацию этих свойств.

Для сегментации успешно применяются хорошо известные фильтры такие, как детекторы границ edge с оператором Лапласа, Превитта, Собеля, Робертса и др. Но в задачах распознавания образов часто используются и специальные методы, например, алгоритм разделения и слияния (Split and merge). Целью данного алгоритма является разбиение изображения на множество непересекающихся областей. Процедура выполняется в несколько шагов:

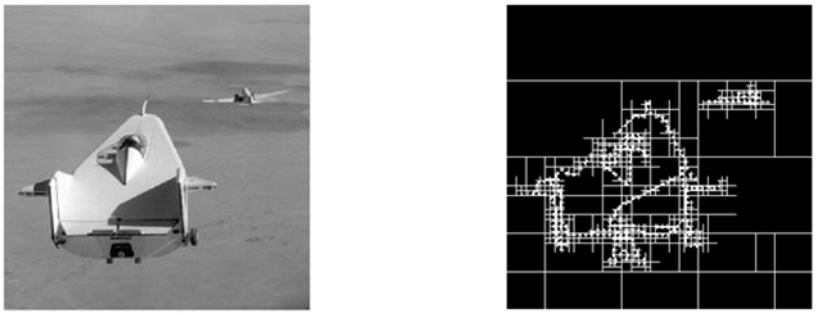
–выбирается определенная область на изображении;

–формулируется какой-либо критерий;

–выполняется оценка, удовлетворяет ли выбранная область данному условию; если да, то область помечается как подходящая, если нет, то область разделяется на сектора, которые далее рассматриваются по отдельности [3].

Этот процесс продолжается до тех пор, пока не прекратится дальнейшее разделение областей. Однако, если проводить только разделение, то окончательная сегментация будет содержать множество соседних областей, обладающих идентичными или сходными свойствами. Таким образом, после каждого разделения используется процесс слияния, который сравнивает соседние области и, при необходимости, объединяет их. Когда дальнейшее разделение или слияние не происходит, сегментация завершена.

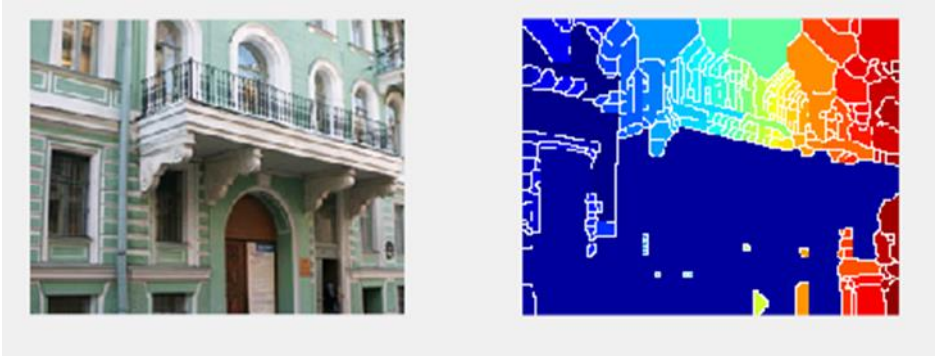
На рис. 5 приведено исходное изображение и результат его сегментации методом разделения и слияния.



а б

Рис. 5. Работа алгоритмасегментации Split and Merge:
а – исходное изображение; б – результат сегментации

Относительно новым алгоритмом сегментации является так называемый метод «водораздела» (Watershed), в основе которого лежит теория морфологии. В этом методе изображение рассматривается как топографическая карта градиента, в которой значение градиента соответствует высоте местности: высокое значение соответствует горным вершинам, а низкое значение соответствует долине. Вода всегда течет в сторону низкой местности, а низменное место — это котловина. В конечном итоге вся вода будет в разных бассейнах, а горы между бассейнами называют водоразделами [3]. В системе Matlab этот метод реализуется функцией wateshed. Изображение предварительно переводят в бинарное с пороговым значением, найденным функцией graythresh. На рис. 6 показан результат применения функции wateshed к цветному изображению.



а б

Рис. 6. Работа алгоритма Watershed:
а – исходное изображение; б – результат сегментации

Данный пример демонстрирует, что изображение преобразуется в некоторое подобие карты, где белые линии соответствуют границам между бассейнами или водоразделам.

Помимо описанных выше функций также существуют и другие, например, градиентные дифференциальные фильтры и оператор Лапласа. Однако, большинство таких фильтров не находят границы как таковые, а указывают на них, как наиболее вероятные, а некоторые факторы в дальнейшем решении задачи могут осложнить ситуацию. В отношении этих методов рассматриваются разные параметры фильтров. Также существует метод Кэнни, который наиболее эффективно справляется с обнаружения границ.

Данный метод работает согласно следующей последовательности действий:

– изображение сначала сглаживается с помощью гауссова фильтра;
– осуществляется поиск градиента. Границы отмечаются там, где градиент изображения приобретает максимальное значение;
– в качестве границ выступают точки локальных максимумов, все остальные подавляются;
– выделяются только сильные границы, все остальные подавляются.

Заключение. Все представленные методы, а их список далеко неполный, используются для определения свойств и характеристик изображения и могут применяться в разных комбинациях для решения разного типа задач. Выбор метода сегментации зависит от поставленной задачи, и даже для разных участков одного и того же метода могут применяться различные методы сегментации, а система Matlab предлагает разнообразие методов для реализации актуальных в настоящее время задач. Данные возможности при взаимодействии с другими технологиями создают множество функций, например, обучение нейронной сети с целью определения объектов или его идентификации по кадру, полученному с камеры [4].

СПИСОК ЛИТЕРАТУРЫ

1. Гонсалес Р., Вудс Р., Эддинс С.. Цифровая обработка изображений в среде MATLAB. - М.: Техносфера, 2005. 1072 с.
2. Solomon C., Breckon T. Fundamentals of digital image processing: a practical approach with examples in Matlab. - Oxford: Wiley Blackwell, 2011. 352 с.
3. Кириллов Р.О., Шефер Е.А. Применение Matlab в задачах распознавания образов // Вестник молодых ученых СПГУТД. № 4 (2023), с. 97-101.
4. Глубокое обучения с использованием AlexNet. URL: https://www.mathworks.com/help/deeplearning/ug/transfer-learning-using-alexnet (дата обращения: 20.03.2023).

УДК 004.85

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АВТОКОДИРОВЩИКОВ ПРИ ВЫЯВЛЕНИИ ЗАРАЖЕНИЯ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ КОМПЬЮТЕРНЫМИ ВИРУСАМИ

Леонова Амелия Александровна, Шошков Николай Олегович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия
e-mails: amelia.leonova@gmail.com, nikolay@shoshkov.com

Аннотация. Цель работы — сравнение эффективности нескольких автокодировщиков с числом слоев от 3 до 5 и различными функциями активациями (relu, sigmoid, tanh, linear, softplus, softsign) для выявления вредоносных данных трафика с помощью алгоритма классификации. Для анализа взят датасет с трафиком данных 9-ти устройств, в котором собраны данные с зараженных и незараженных ботнетами устройств. Анализируемый набор данных создан специалистами из университета имени Бен-Гуриона (Беэр-Шева, Израиль) и центра кибербезопасности iTrust при Сингапурском университете технологий и дизайна. Ожидаемая сетевая модель знаний, построенная алгоритмом, представлена в виде обученной нейронной сети, применяемой для обнаружения аномалий в нормализованных данных трафика устройств. Построенные модели оцениваются исходя из процента правильно классифицированных тестовых выборок. Представленный алгоритм может быть использован для анализа трафика устройств интернета вещей. По результатам расчета эффективности авторы рекомендуют использовать для классификации автокодировщик с тремя скрытыми слоями и функциями активации relu, sigmoid.

Ключевые слова: нейронная сеть; автокодировщик; нейронная сеть; точечная аномалия; интернет вещей; функция активации; кибербезопасность; сетевая модель знаний; анализ данных.

COMPARATIVE ANALYSIS OF AUTOENCODERS IN DETECTING INFECTION OF INTERNET OF THINGS DEVICES WITH COMPUTER VIRUSES

Leonova Amelia, Shoshkov Nikolay
St. Petersburg State Electrotechnical University «LETI» named after V. I. Ulyanov (Lenin)
5 Professor Popov st., St. Petersburg, 197022, Russia,
e-mails: amelia.leonova@gmail.com, nikolay@shoshkov.com

Abstract. The purpose of the work is to compare the effectiveness of several autoencoders with a number of layers from 3 to 5 and various activation functions (relu, sigmoid, tanh, linear, softplus, softsign) for identifying malicious traffic data using a classification algorithm. For analysis, a dataset was taken with the data traffic of 9 devices, which collected data from devices infected and not infected with botnets. The analyzed dataset was created by specialists from Ben-Gurion University (Beer Sheva, Israel) and the iTrust cybersecurity center at the Singapore University of Technology and Design. The dataset contains information about both devices infected and not infected with malware. The expected network knowledge model built by the algorithm is represented as a trained neural network, used to detect anomalies in normalized device traffic data. The constructed models are evaluated based on the percentage of correctly classified test samples. The presented algorithm can be used to analyze the traffic of Internet of Things devices. Based on the results of efficiency calculations, the authors recommend using an autoencoder with three hidden layers and activation functions relu and sigmoid for classification.

Keywords: neural network; autoencoder; point anomaly; Internet of things; activation function; cybersecurity; network knowledge model; data analysis.

Введение. Интернет вещей (Internet of Things, loT) — инфраструктура взаимосвязанных сущностей, систем и информационных ресурсов, а также служб, позволяющих обрабатывать информацию о физическом и виртуальном мире и реагировать на нее [6]. Интернет вещей в последнее время набирает популярность. Согласно исследованию Research and Markets, если рынок IoT в производстве в 2022 году оценивался в 209,4 млрд долларов, то прогноз на 2023 год — 252,2 млрд долларов, а на 2027 год — более 461 млрд долларов, что означает средний ежегодный рост более чем на 16%. Институт статистических исследований и экономики знаний НИУ ВШЭ назвал десять направлений, в которых в 2023 году будут востребованы технологии интернета вещей: интернет медицинских вещей, «туманные» вычисления и «облачный» интернет вещей, мобильный интернет вещей, искусственный

интеллект вещей, интернет вещей для «умного» города или дома, интернет робототехнических вещей, спутниковый интернет вещей, носимый интернет вещей, интеграция интернета вещей и периферийных устройств, интернет вещей на транспорте. Безопасность интернета вещей крайне важна, т. к. в него входят устройства, содержащие большое количество информации, примером могут быть веб-камеры. При взломе всю информацию получат злоумышленники.

В последние годы произошло несколько кибератак: 2016 — атака ботнета Mirai; 2018 — вредоносная программа VPNFilter; 2020 — взлом Tesla Model X; 2021 — взлом камеры Verkada.

Объектом исследования является взаимодействие устройств интернета вещей. Предметом исследования — оценка эффективности алгоритмов выявления с помощью автокодировщика аномалий зараженных устройств интернета вещей. Автокодировщик — специальная архитектура искусственной нейронной сети с одним и более скрытыми слоями без обратных связей [15]. При выявлении аномалий в трафике передаваемых данных можно определить заражение устройства вирусом. В работе для анализа данных используются автокодировщики [3], а также сравнивается их эффективность.

По мнению ряда исследователей [7-9], автокодировщики являются эффективным инструментом для выявления аномалий в трафике IoT.

Для анализа взят датасет с трафиком данных 9-ти устройств, в котором собраны данные с зараженных и незараженных ботнетами устройств. Анализируемый набор данных создан специалистами из университета имени Бен-Гуриона (Беэр-Шева, Израиль) и центра кибербезопасности iTrust при Сингапурском университете технологий и дизайна [14]. В датасете находится информации как о зараженных, так и не зараженных вредоносным ПО устройствах. Дата публикации набора данных: март, 2018.

В наборе представлены данные о трафике, собранные с 9 коммерческих IoT-устройств, достоверно зараженных Mirai и BASHLITE.

1) Danmini_Doorbell,
2) Ecobee_Thermostat,
3) Ennio_Doorbell,
4) Philips_B120N10_Baby_Monitor,
5) Provision_PT_737E_Security_Camera,
6) Provision_PT_838_Security_Camera,
7) Samsung_SNH_1011_N_Webcam,
8) SimpleHome_XCS7_1002_WHT_Security_Camera,
9) SimpleHome_XCS7_1003_WHT_Security_Camera.

Для каждого из 9 устройств предоставлены безопасные и вредоносные данные.

Набор данных может быть использован для обучения нейронной сети, специализированной для выявления вредоносных данных трафика с помощью методов обнаружения аномалий. Также данные можно использовать для многоклассовой классификации: 10 классов атак плюс 1 класс «безвредных», т. к. можно разделить на 10 атак, осуществляемых двумя ботнетами.

Описание целевой задачи анализа данных исходя из данных. Целевая задача — создание нескольких однотипных нейронных сетей с разными функциями активации и числом слоев для выявления вредоносных данных трафика с помощью методов обнаружения точечных аномалий. Сравнение эффективности созданных нейронных сетей.

Данные представлены в виде 89 реляционных таблиц. Для каждого из 9 устройств представлены безвредные данные в таблице bening.csv и вредоносные данные в таблицах mirai и gafgyt. В каждой таблице 115 атрибутов, представленных числами типа Real.

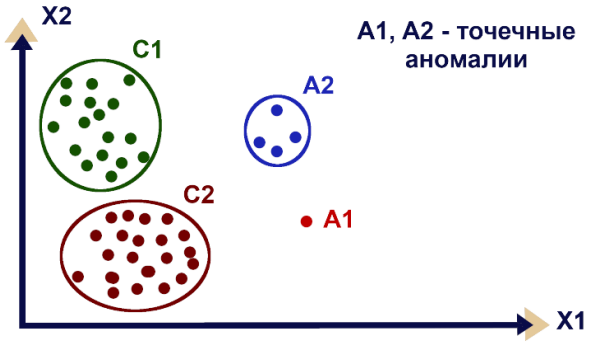


Рис. 1. Точечные аномалии

Датасеты каждого из 9 устройств представлены классом безвредных и классом вредоносных данных.

В наборе присутствуют безвредные данные в таблицах bening, вредоносные данные в таблицах mirai и gafgyt. Вредоносные данные представляют собой аномалии, выявление которых с помощью ML алгоритма является целью работы.

Вредоносные данные рассматриваются как точечные аномалии, т. е. отдельные экземпляры данных, представляющие собой аномалии по отношению к безвредным данным (см. рис. 1).

Исходные данные при таком подходе представляют собой класс безвредных данных. Создается несколько автокодировщиков. Скрытые слои всегда меньшей размерности, чем входной и выходной слои, что позволяет сети выделять наиболее общие признаки данных, и в соответствие с ними устанавливать значения весов.

Цель обучения автокодировщиков на безвредных данных — получение на выходном слое данных наиболее близких к данным на входном слое. Таким образом, после обучения на безвредных данных при вредоносных входных данных на выходном слое данные будут сильно искажены, что будет равносильно распознаванию аномалии.

Автокодировщики отличаются числом скрытых слоев и активирующими функциями (см. таблицу 1). По полученным результатам работы можно будет сравнить эффективность использования различного числа скрытых слоев и различных активирующих функций [1].

Для распределенного обучения должна быть выбрана стратегия параллельных данных, при которой одинаковая модель размещается на нескольких устройствах, данные разбиваются на несколько наборов, каждое устройство обучается на своем набор данных. Градиенты рассчитываются на нейронных сетях всех устройств [2, 3].

Таблица 1

Структура нейронной сети автокодировщиков

Автокодировщик, тип	Входной слой		Скрытый слой, номер						Входной слой	
			1		2		3			
	число узлов	функция активации	число узлов	функция активации	число узлов	функция активации	число узлов	функция активации	число узлов	функция активации
1	115	relu	86	sigmoid	-	-	-	-	115	sigmoid
2	115	relu	86	sigmoid	37	sigmoid	86	sigmoid	115	sigmoid
3	115	relu	86	tanh	37	tanh	86	tanh	115	tanh
4	115	relu	86	softpus	37	linear	86	softsign	115	linear

При синхронном параллелизме после мини-пакетного обучения устройств собираются все градиенты и берется среднее значение для обновления весов нейронных сетей на всех устройствах. Обновление моделей происходит только после обработки данных на всех устройствах, в результате чего происходит простой ресурсов. При асинхронном параллелизме после завершения мини-пакетного обучения, устройству не нужно ждать завершения шага обучения на других устройствах. Скорость обучения при асинхронном параллелизме больше, чем при синхронном, однако существует проблема сбоя градиента. После завершения шага обучения устройства может оказаться, что параметры модели на других устройствах уже были обновлены и рассчитанный градиент «устарел», из-за чего происходит снижение производительности обучения. В работе реализуется асинхронный параллелизм.

Входные данные автокодировщиков должны быть нормализованы для скорейшего обучения сети. При поступлении обучающей выборки на входной слой автокодировщика после расчета выходных значений входного слоя сети применяется функция активации. От скорости изменения функции активации зависит скорость изменения функции весов, следовательно, при правильной нормализации входных значений ускоряется обучение нейронной сети. В работе для независимости обработки выборки от всего набора данных предполагается использование масштабирование MinMaxScaler библиотеки Scikit-Learn.

Ожидаемая сетевая (семантическая) модель знаний представлена в виде обученной нейронной сети, применяемой для обнаружения аномалий в нормализованных данных трафика устройств.

Построенные модели оцениваются исходя из процента правильно классифицированных тестовых выборок. Также возможна оценка времени обучения моделей.

Данные удобнее всего размещать в «облачном» хранилище (например, YandexCloud), куда входят наборы данных с 9 устройств. Для каждого устройства представлен набор безвредных данных и несколько наборов вредоносных данных. Выходной поток данных представляет собой нормализованные для дальнейшего анализа данные.

При распределенном обучении нормализованный датасет безвредных данных одного из устройств разделяется на несколько частей, в соответствие с числом рабочих узлов. В результате обработки выходного потока системой анализа данных в потоке обобщения передаются агрегированные данные, содержащие классификацию обработанных данных на вредоносные и безвредные.

Система анализа данных представлена в виде распределенной нейронной сети, отображающей информацию об обнаружении аномалий на исследуемом устройстве.

Для анализа данных предполагается использовать Yandex DataSphere — сервис, который упрощает использование среды разработки JupyterLab на вычислительных мощностях YandexCloud.

Алгоритм реализован на языке Python с помощью открытой программной библиотеки TensorFlow, разработанной для решения задач построения и тренировки нейронной сети, а также библиотеки Keras, разработанной для глубокого обучения, работающая поверх TensorFlow.

Все данные в датасете хранятся в формате csv. Файлы csv загружены непосредственно в хранилище YandexCloud. Для импортирования данных для их дальнейшего анализа используется библиотека numpy.

Для анализа данных использовалась библиотека TensorFlow, Keras. TensorFlow — открытая программная библиотека для машинного обучения, разработанная компанией Google для решения задач построения и тренировки нейронной сети [10-12].

Процесс анализа состоит из следующих этапов:

1) нормализация данных с помощью MinMaxScaler;
2) построения модели автокодировщика;
3) обучение автокодировщика на безвредных данных;
4) классификация данных на вредоносные и безвредные входные данные.

Последовательный алгоритм проверяется на 4 типах автокодировщиках, представленных ранее. Было создано 4 типа автокодировщиков, различных по числу слоев и функций активаций. Слои делятся на энкодер и декодер. При создании любого слоя в качестве параметров вводятся чило узлов слоя и функция активации (например, «relu», «sigmoid», «tanh»).

При параллельном алгоритме на каждом из узлов обучается автокодировщик, затем после каждой эпохи обучения происходит сложение весовых коэффициентов.

Датасет содержит информацию о вредоносном и безвредном трафике, собранном с 9 типов устройств. Например, фрагменты данных с 4-го устройства.

До начала использования данных для обучения (частично с учителем) нейронных сетей данные проходят масштабирование.

На рис. 2 представлен фрагмент масштабированных безвредных данных.

```
print(scaler.fit_transform(X_train))
```

```
[[0.00000000e+00 0.00000000e+00 0.00000000e+00 ... 0.00000000e+00
  7.45566352e-01 5.89404063e-01]
 [0.00000000e+00 0.00000000e+00 0.00000000e+00 ... 0.00000000e+00
  7.45566352e-01 5.89404063e-01]
 [0.00000000e+00 2.02484806e-01 0.00000000e+00 ... 3.15345721e-02
  7.45566352e-01 5.89404063e-01]
 ...
 [5.98978614e-03 1.20657549e-02 1.24104110e-04 ... 1.51040200e-04
  7.45569273e-01 5.94262761e-01]
 [5.18272713e-03 1.47195865e-02 4.76793515e-05 ... 1.57004913e-04
  7.45557832e-01 5.75744037e-01]
 [2.64565855e-06 4.31034400e-03 1.02950331e-07 ... 1.58557587e-04
  7.45580746e-01 6.12213708e-01]]
```

Рис. 2. Масштабированные безвредные данные

Фрагменты кода и значение параметров для описания всех четырех типов автокодировщиков представлены на рис. 3–6.

```
class Autoencoder(Model):
    def __init__(self):
        super(Autoencoder, self).__init__()
        self.encoder = Sequential([
            layers.Dense(115, activation="relu"),
            layers.Dense(86, activation="sigmoid")
        ])
        self.decoder = Sequential([
            layers.Dense(115, activation="sigmoid")
        ])

    def call(self, x):
        encoded = self.encoder(x)
        decoded = self.decoder(encoded)
        return decoded
```

Рис. 3. Тип 1 автокодировщика

```
class Autoencoder(Model):
    def __init__(self):
        super(Autoencoder, self).__init__()
        self.encoder = Sequential([
            layers.Dense(115, activation="relu"),
            layers.Dense(86, activation="sigmoid"),
            layers.Dense(37, activation="sigmoid")
        ])
        self.decoder = Sequential([
            layers.Dense(115, activation="sigmoid"),
            layers.Dense(115, activation="sigmoid")
        ])

    def call(self, x):
        encoded = self.encoder(x)
        decoded = self.decoder(encoded)
        return decoded
```

Рис. 4. Тип 2 автокодировщика

```
class Autoencoder(Model):
    def __init__(self):
        super(Autoencoder, self).__init__()
        self.encoder = Sequential([
            layers.Dense(115, activation="relu"),
            layers.Dense(86, activation="tanh"),
            layers.Dense(37, activation="tanh")
        ])
        self.decoder = Sequential([
            layers.Dense(115, activation="tanh"),
            layers.Dense(115, activation="tanh")
        ])

    def call(self, x):
        encoded = self.encoder(x)
        decoded = self.decoder(encoded)
        return decoded
```

Рис. 5. Тип 3 автокодировщика

В функции EarlyStopping, предназначенной для ранней остановки алгоритма обучения при переобучении модели, устанавливается пороговое min_delta значение для количественного определения потери в какую-то эпоху как улучшение или нет, устанавливается количество эпох до остановки алгоритма, как только потеря начинает увеличиваться, аргумент mode зависит от того, в каком направлении контролируется ваше количество (оно должно уменьшаться или увеличиваться). Также устанавливается оптимизатор, функция потерь (см. рис. 6).

```
def compile_and_train(ae, x):
    ae.compile(optimizer=adam_v2.Adam(learning_rate=0.01), loss='mse')
    monitor = EarlyStopping(
        monitor='val_loss',
        min_delta=1e-9,
        patience=5,
        verbose=1,
        mode='auto'
    )
    ae.fit(
        x=x,
        y=x,
        epochs=800,
        validation_split=0.3,
        shuffle=True,
        callbacks=[monitor]
    )
```

Рис. 6. Настройка алгоритма обучения автокодировщика

Результаты оценки эффективности работы автокодировщиков представлены в таблице 2. Наивысшую скорость работы продемонстрировал автокодировщик первого типа с входным слоем relu, одним скрытым слоем sigmoid и выходным слоем также sigmoid. Самую низкую скорость построения продемонстрировал автокодировщик второго типа с входным слоем relu, тремя скрытыми слоями sigmoid и выходным слоем также sigmoid. Автокодировщики первого и второго типа являются самыми популярными.

Таблица 2

Сравнительный анализ автокодировщиков по времени построения моделей в зависимости от объема данных

Тип автокодировщика	Структура автокодировщика				Время построения моделей в зависимости от объема данных		
	Параметры функции активации				число вызовов функций	период времени, с	скорость построения, число вызовов в секунду
	кол-во скрытых слоев	входной слой	скрытый слой (-и)	выходной слой			
1	1	relu	sigmoid	sigmoid	8 538 597	25,43	335 769
2	3	relu	sigmoid (все 3)	sigmoid	7 442 788	33,88	219 681
3	3	relu	tanh (все 3)	tanh	5 442 928	15,90	342 323
4	3	relu	1-ый -'softplus', 2-ой — 'linear', 3-ий — 'sofsign'	linear	6 855 920	22,23	308 408

В таблице 3 указана информация о проценте верно выявленных аномалий для 1-го и 2-го автокодировщика в датасетах, как самых широко используемых на практике. Данные из таблицы 3 свидетельствует о правильность работы математической модели для ботнетов mirai и gafgyt. Автокодировщик типа 1 с одним скрытым слоем выявил аномалии для все 5 датасетов, зараженных mirai, и для 3 из 5 датасетов, зараженных gafgyt. Автокодировщик типа 2 с тремя скрытыми слоями выявил аномалии для всех датасетов обоих вирусов, но значение параметра «скорость построения вызовов» у него (219 681) на 53 % ниже, чем у автокодировщика типа 1 (335 769). Уровень ошибок с выявлением ложных аномалий в безвредных данных примерно одинаковый для автокодировщиков обоих типов и равен 2,32 % для автокодировщика первого типа, и 2,38 % для второго.

Таблица 3

Сравнительный анализ автокодировщиков по проценту выявленных аномалий

Тип данных (безвредные, датасет с mirai, датасет с gafgyt)	Количество датасетов	Автокодировщик с одним скрытым слоем (тип 1)		Автокодировщик с тремя скрытыми слоями (тип 2)	
		Выявлены аномалии, %	Ошибка, %	Выявлены аномалии, %	Ошибка, %
Безвредные данные	1	2,32	2,32	2,38	2,38
mirai	5	100	0	100	0
gafgyt	5	66	34	100	0

Заключение. В рамках работы был реализован с помощью автокодировщиков алгоритм классификации датасета с трафиком данных девяти устройств интернета вещей. Предложен способ оценки эффективности автокодировщиков, по параметру «скорость построения вызовов в секунду». Выполнена оценка эффективности четырех типов автокодировщиков с числом слоев от 3 до 5 и различными функциями активации (relu, sigmoid, tanh, linear, softplus, softsign). В результате сравнения эффективности работы автокодировщиков (см. таблица 1) было измерено время работы различных автокодировщиков, отличающихся функциями активации узлов и числом слоев, а также определен процент верно выявленных аномалий. Скорость построения вызовов в секунду выше всего у автокодировщика с тремя скрытыми слоями и функциями активации tanh, relu, близкий результат к максимальному показал автокодировщик с одним скрытым слоем и функциями активации relu и sigmoid. Сравнительный анализ по проценту выявленных аномалий автокодировщиков (см. таблицу 2) с наиболее часто используемой на практике функцией активации sigmoid показал, что автокодировщик с тремя скрытыми слоями эффективнее, чем с одним скрытым слоем, но проигрывает в быстродействии на 53 %.

СПИСОК ЛИТЕРАТУРЫ

1. Klopries H. Flexible Activation Bag: Learning Activation Functions in Autoencoder Networks // IEEE International Conference on Industrial Technology (ICIT), 04-06 April 2023.
2. Autoencoders UFLDL Tutorial : учеб. UFLDL [Электронный ресурс]. URL: http://ufldl.stanford.edu/tutorial/unsupervised/Autoencoders/ (дата обращения 01.06.2023).
3. Автокодировщик // Статья по теме автокодировщик в Википедии [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D0%BA%D0%BE%D0%B4%D0%B8%D1%80%D0%BE%D0%B2%D1%89%D0%B8%D0%BA (дата обращения 10.06.2023).
4. What is IoT? // Что такое интернет вещей [Электронный ресурс]. URL: https://www.oracle.com/internet-of-things/what-is-iot/ (дата обращения 05.06.2023).
5. Классификация данных при помощи нейронных сетей [Электронный ресурс]. URL: https://loginom.ru/blog/neural-classification?ysclid=lmpuoxae3623273972 (дата обращения 10.06.2023).
6. Верещагина Е. А., Капецкий И. О., Ярмонов А. С. Проблемы безопасности Интернета вещей : учеб. пособие. М.: Мир науки, 2021.
7. Гурина А. О., Гузев О. Ю., Елисеев В. Л. Обнаружение аномальных событий на хосте с использованием автокодировщика / International Journal of Open Information Technologies. 2020. Vol. 8. № 8. ISSN: 2307-8162.
8. Daboubi, Walid. Anomaly detection with autoencoder neural network applied on detecting malicious [Электронный ресурс]. URL: https://medium.com/@walid.daboubi/anomaly-detection-with-autoencoder-neural-network-applied-on-detecting-malicious-urls-7536abcb403f (дата обращения 28.06.2023).
9. Gurina A., Eliseev V. Anomaly-Based Method for Detecting Multiple Classes of Network Attacks // Information. 2019. Т. 10 (3):84.
10. Руководство TensorFlow // Руководство на официальном сайте TensorFlow [Электронный ресурс]. URL: https://www.tensorflow.org/guide?hl=ru (дата обращения 20.06.2023).
11. TensorFlow license // Текст лицензии TensorFlow [Электронный ресурс]. URL: https://github.com/tensorflow/tensorflow/blob/master/LICENSE (дата обращения 22.06.2023).
12. Keras license // Текст лицензии Keras [Электронный ресурс]. URL: https://github.com/keras-team/keras/blob/master/LICENSE (дата обращения 22.06.2023).
13. Developer Guides // Руководство разработчика Keras [Электронный ресурс]. URL: https://keras.io/guides/ (дата обращения: 22.06.2023).
14. N-BaIoT Dataset to Detect IoT Botnet Attacks // Анализируемый в работе датасет [Электронный ресурс]. URL: https://www.kaggle.com/datasets/mkashifn/nbaiot-dataset (дата обращения 22.06.2023).
15. Роман Д. Искусственный интеллект. ДМК Пресс, 2019. 280 с.

УДК 004.056

ОСОБЕННОСТИ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ЗНАЧИМОМ ОБЪЕКТЕ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ И МЕРЫ ПО ЕГО ЗАЩИТЕ

Локнов Алексей Игоревич, Симакова Екатерина Андреевна
Санкт-Петербургский университет МВД России
Лётчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
emails: info_for_aleksey@mail.ru, ekaterina.simakova.2001@yandex.ru

Аннотация. Критическая информационная инфраструктура обеспечивает надежную работу ключевых систем, экономики и национальной безопасности, предотвращает информационные угрозы и сохраняет стабильность в обществе. Нарушение в работе объектов критической информационной инфраструктуры может привести к серьезным последствиям, как для экономики, так и общества в целом. Основное внимание в статье уделяется разработке и реализации мер по защите информации, принимаемых с учетом особенностей значимого объекта критической информационной инфраструктуры.

Ключевые слова: значимый объект критической информационной инфраструктуры; меры обеспечения безопасности; уязвимость; угроза; защита информации.

ENSURING INFORMATION SECURITY AT THE OBJECT OF CRITICAL INFORMATION INFRASTRUCTURE

Loknov Alexey, Simakova Ekaterina
Saint Petersburg University of the Ministry of internal Affairs of the Russian Federation
1, Pilyutov'spilot St., St. Petersburg, 198206, Russia
emails: info_for_aleksey@mail.ru, ekaterina.simakova2018@mail.ru

Abstract. Critical information infrastructure ensures the reliable operation of key systems, the economy and national security, prevents information threats and maintains stability in society. Disruption of critical information infrastructure facilities can lead to serious consequences for both the economy and society as a whole. The main focus of the article is on the development and implementation of information protection measures taken taking into account the characteristics of a significant object of critical information infrastructure.

Keywords: significant object of critical information infrastructure; security measures; vulnerability; threat; information protection.

Введение. В современном информационном обществе критическая информационная инфраструктура играет важную роль в обеспечении функционирования различных сфер жизнедеятельности. Вмешательство в работу критической информационной инфраструктуры может привести к серьезным последствиям, таким как: нарушение работы крупных предприятий, утечка конфиденциальной информации в организации, причинение крупного материального ущерба. В связи с этим обеспечение информационной безопасности объектов критической информационной инфраструктуры становится одной из приоритетных задач государства.

Объекты критической информационной инфраструктуры (КИИ) — это информационные системы, сети и ресурсы, которые обеспечивают работу критически важных секторов экономики. Эти объекты могут включать системы управления энергетическими сетями, транспортные системы, финансовые платформы, системы связи и государственные информационные системы. Постановление Правительства РФ от 8 февраля 2018 года № 127 (ред. от 20.12.2022) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» определяет правила категорирования объектов КИИ. То есть, каждому объекту присваивается одна из категорий значимости, а руководитель субъекта КИИ должен создать комиссию по категорированию; выделить объекты; провести категорирование в соответствии с утвержденным порядком и с соблюдением определенных сроков.

Значимым объектом критической информационной инфраструктуры считается объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры. В соответствии с Приказом ФСТЭК России от 6 декабря 2017 года № 227 (ред. от 01.09.2023) «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» у ФСТЭК России есть собственный реестр значимых объектов КИИ, в который заносятся сведения по всем значимым объектам, по которым субъектами КИИ подаются сведения во ФСТЭК России. На Рис. 3 представлена схема внесения объекта критической информационной инфраструктуры в реестр значимых объектов критической информационной инфраструктуры.

Реализация угроз на значимых объектах критической информационной инфраструктуры (КИИ) может иметь серьезные последствия для безопасности информации и функционирования систем. Сбои в работе значимых объектов критической инфраструктуры могут привести к значительным экономическим потерям, включая ущерб

для экономики государства, потери производительности и дополнительным высоким затратам на восстановление. На значимых объектах КИИ можно столкнуться с такими угрозами:

1.Хакерские атаки, или покушение на систему безопасности. Включают в себя DDoS-атаки, взломы информационных систем, внедрение вредоносного программного обеспечения и другие атаки на сети и системы значимых объектов КИИ.

2.Атаки на физическом уровне. Реализация атак на физическую инфраструктуру, а именно, на каналы передачи данных, например, между энергетическими объектами, телекоммуникационными центрами и дата-центрами, которые могут привести к серьезным нарушениям функционирования объектов. Отказ в работе или недоступность ключевых систем и сервисов объектов КИИ может создать проблемы для обеспечения нормального функционирования критической инфраструктуры.

3.Утечка конфиденциальных данных. Нарушения информационной безопасности при передаче, обработке, хранении конфиденциальных данных могут привести к их утечке или краже, что влечет за собой финансовые и репутационные потери. Чаще всего к утечкам данных приводят ошибки персонала или неправильные действия могут привести к угрозам безопасности информации.

Рис. 3. Порядок внесения объекта критической информационной инфраструктуры в реестр значимых объектов критической информационной инфраструктуры

Для успешного обеспечения безопасности на объектах КИИ необходимо проводить анализ угроз и рисков, разрабатывать и реализовывать соответствующие меры безопасности, а также проводить регулярный мониторинг и обновление систем для минимизации уязвимостей и рисков.

Уязвимости объектов критической информационной инфраструктуры могут возникать из-за недостатков в проектировании, реализации и эксплуатации информационных систем. Основные уязвимости включают отсутствие достаточного контроля доступа к системам, неэффективное управление учетными записями, недостаточную защиту сетевых связей, отсутствие мониторинга и обнаружения вторжений [1], а также отсутствие регулярного обновления программного обеспечения.

Для реализации мер по информационной безопасности на значимом объекте критической информационной инфраструктуры нужно подготовить план для разработки концепции безопасности информации на значимом объекте критической информационной инфраструктуры. Этот план должен охватывать основные этапы проектирования систем защиты. Концепция информационной безопасности на значимом объекте критической информационной инфраструктуры может включать следующие шаги:

1.Анализ существующих угроз и рисков информационной безопасности:

– Идентификация основных угроз и рисков для информационной безопасности значимого объекта критической информационной инфраструктуры.

– Анализ существующих организационных и технических мер безопасности.

– Оценка уровня уязвимости и поиск возможных уязвимых систем.

2.Определение требований к информационной безопасности:

– Формулирование основных принципов и целей безопасности значимого объекта критической информационной инфраструктуры.

– Установление соответствия необходимым стандартам по информационной безопасности значимого объекта КИИ.

3.Разработка концепции безопасности:

– Определение структуры и организации системы безопасности значимого объекта критической информационной инфраструктуры.

– Выделение основных компонентов, включая их организационные и технические аспекты безопасности.

– Формирование стратегии обеспечения безопасности на основе анализа рисков и требований по безопасности.

4.Организационные меры безопасности:

– Разработка плана управления информационной безопасностью значимого объекта критической информационной инфраструктуры.

– Установление процедур и политик безопасности.

– Определение ролей и обязанностей сотрудников по обеспечению безопасности.

5.Технические меры безопасности:

– Разработка архитектуры системы защиты информационной безопасности значимого объекта критической информационной инфраструктуры.

– Выбор и внедрение средств технической защиты (системы шифрования, антивирусы и иные).

– Разработка систем мониторинга и анализа событий.

6.Тестирование и аудит:

– Проведение тестирования системы безопасности.

– Анализ результатов тестирования и внесение изменений в систему защиты.

– Проведение аудита системы безопасности для проверки соответствия стандартам и требованиям нормативно-правовых актов.

7.Обучение персонала:

– Проведение обучающих мероприятий для сотрудников по вопросам безопасности информации.

– Разработка методических рекомендаций для повышения осведомленности о правилах безопасности.

8.Внедрение и мониторинг:

– Последовательное внедрение разработанных мер безопасности.

– Внедрение системы мониторинга и анализа безопасности для оперативного реагирования на инциденты.

– Подведение итогов разработки концепции безопасности информации на объекте КИИ.

– Оценка эффективности внедренных мер и достижение поставленных целей.

Для обеспечения комплексной информационной безопасности необходимо выполнения мер по защите информационной безопасности. А после внедрения данных мер необходим постоянный мониторинг и усовершенствование систем безопасности, так как со временем появляются новые угрозы, выявляются каналы утечки информации и уязвимости в системах.

Меры по обеспечению информационной безопасности объектов КИИ включают:

1.Анализ информации. Первым шагом в обеспечении безопасности объектов КИИ является анализ обрабатываемой информации на значимом объекте КИИ, её классификация по уровню конфиденциальности [2]. Это позволит определить, какие данные требуют наибольшей защиты. Важным шагом в обеспечении безопасности значимых объектов КИИ является проведение комплексной оценки рисков и угроз. Это включает идентификацию потенциальных уязвимостей и угроз, анализ возможных последствий инцидентов безопасности, а также определение вероятности их возникновения. Результаты оценки рисков помогут разработать эффективные стратегии и меры по обеспечению безопасности.

2.Физическую безопасность. Обеспечение физической безопасности значимых объектов КИИ играет важную роль в предотвращении несанкционированного доступа к системам и ресурсам. Данная мера должна включать установку: систем видеонаблюдения, контроля доступа, защиты помещений с серверами и сетевым оборудованием, а также обучение персонала вопросам физической безопасности значимых объектов КИИ.

3.Защиту сетевой инфраструктуры. Сетевая инфраструктура значимых объектов КИИ является ключевым элементом, который требует надежной защиты. Важно соблюдать меры по обеспечению безопасности сети, такие как использование межсетевых экранов (firewalls), систем обнаружения вторжений (intrusion detection systems), систем предотвращения вторжений (intrusion prevention systems) и виртуальных частных сетей (Virtual Private Networks, VPN).

4.Управление уязвимостями. Эффективное управление уязвимостями является неотъемлемой частью обеспечения информационной безопасности значимых объектов КИИ. Данная мера включает регулярное сканирование и анализ уязвимостей, а также исправление выявленных проблем [3]. Рекомендуется использовать автоматизированные инструменты для обнаружения и управления уязвимостями, а также следить за обновлениями списков уязвимостей. Также необходимо регулярно обновлять и проверять сетевое оборудование и программное обеспечение, чтобы устранить известные уязвимости.

5.Обучение и повышение осведомленности персонала является важным аспектом обеспечения информационной безопасности значимого объекта КИИ. Персонал должен быть обучен базовым принципам безопасности информации, распознаванию фишинговых атак, использованию безопасных паролей и защите

конфиденциальных данных [4]. Лекции, инструктажи, повышения квалификации по повышению знаний и навыков в информационной безопасности персонала помогут снизить риск внутренних угроз и ошибок.

Одновременно с принятием мер безопасности необходимо готовиться к реагированию на такую атаку, если применяемые мер защиты не предотвратят атаку. Если на всех предприятиях, входящих в реестр критической информационной инфраструктуры не будет компетентных специалистов, то необходимо создавать центры компетенции, которые будут непосредственно подключаться к противодействию атакам на данных объектах [5].

Также регулярный аудит и мониторинг системы безопасности значимых объектов КИИ необходимы для обнаружения и реагирования на потенциальные инциденты безопасности. Это включает мониторинг сетевого трафика, журналов событий и системных ресурсов [6]. Результаты мониторинга должны быть анализированы и своевременно реагировать на любые аномальные или подозрительные активности.

Заключение. Управление доступом, шифрование, мониторинг и обнаружение инцидентов, а также обучение персонала представляют собой интегрированный подход, направленный на обеспечение всесторонней безопасности информации на значимых объектах КИИ. В ходе анализа особенностей реализации угроз было выявлено, что современные атаки на значимые объекты критической информационной инфраструктуры характеризуются сложностью и многообразием способов и методов их совершения, а также негативными последствия от этих атак для государства и общества в целом. Обеспечение безопасности на значимых объектах КИИ — это сложная, но важная задача, требующая постоянного контроля, регулярного внедрения современных технологий и координации усилий всех государственных органов.

СПИСОК ЛИТЕРАТУРЫ

1. Вавичкин А. Н. «К вопросу категорирования объектов критической информационной инфраструктуры». // Безопасность информационных технологий, [S.l.], т. 26, № 2, с. 44–57, 2019. [Электронный ресурс] URL: https://www.elibrary.ru/item.asp?id=38568103 (дата обращения: 07.06.2023).
2. Гатчин, Ю. А. «Информационная безопасность критической информационной инфраструктуры: теоретико-методологические аспекты» / Ю. А. Гатчин, В. В. Сухостат // Инновационные, информационные и коммуникационные технологии: сборник трудов XVII Международной научно-практической конференции, Сочи, 01–10 октября 2020 года / под.ред. С.У. Увайсов. – Москва: Ассоциация выпускников и сотрудников ВВИА имени профессора Н.Е.Жуковского содействия сохранению исторического и научного наследия ВВИА имени профессора Н.Е. Жуковского, 2020. – С. 213-217.
3. Сиротский А.А., Резниченко С.А. «Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов». Безопасность информационных технологий, [S.l.], т. 28, № 3, с. 103–117, 2021. [Электронный ресурс] URL: https://www.elibrary.ru/item.asp?id=46709372 (дата обращения: 13.06.2023).
5. Чернова, Е.В. «Информационная безопасность человека: учебное пособие для вузов» / Е.В.Чернова. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2023. — 243 с. // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518441 (дата обращения: 18.06.2023).
6. Организационно-правовые основы технической защиты конфиденциальной информации: Учебное пособие / Ю. И. Синещук, В. Н. Родин, 5 Д. Н. Саратов, А. И. Локнов. – Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2023. – 80 с. – ISBN 978-5-91837-677-5. – EDN ORYQEQ. С. 43.
7. Бегишев, И.Р. «Безопасность критической информационной инфраструктуры Российской Федерации» // Безопасность бизнеса. 2019. № 1. С. 27–32.

УДК 004.94

РЕШЕНИЕ ЗАДАЧ УПРАВЛЕНИЯ ПРОЕКТАМИ С ПОМОЩЬЮ МЕТОДА ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

Пуха Геннадий Пантелеевич
Санкт-Петербургский государственный университет сервиса и экономики
канала Грибоедова наб., 30-32, лит. А, Санкт-Петербург, 191023, Россия
e-mails: pgp2003@list.ru

Аннотация. В статье на примере одного из возможных вариантов процесса развертывания полевого узла связи рассматривается применение метода имитационного моделирования для решения задачи по оценки своевременности данного процесса.

Ключевые слова: принятие решения; сетевое планирование; случайные продолжительности работ; нормальный закон; ограничения; имитационная модель; своевременность реализации проекта.

SOLUTION OF PROJECT MANAGEMENT PROBLEMS USING SIMULATION MODELING METHOD

Puha Gennady
Saint Petersburg State University of Service and Economics
30-32 Griboyedov Canal emb., letter A, St. Petersburg, 191023, Russia
e-mails: pgp2003@list.ru

Abstract. In the article, using the example of one of the possible options for the deployment of a field communication center, the application of the simulation method to solve the problem of assessing the timeliness of this process is considered.

Keywords: decision making; network planning; random durations of work; normal law; constraints; simulation model; timeliness of project implementation.

Введение. К настоящему времени сложились четыре основные школы разработки управленческих решений, которые различаются своими концептуальными подходами к решению этой проблемы, и сделавшие существенный вклад в развитие теории и практики управления. К таковым, как правило, относят школы [1]:

- научного управления;
- административного управления;
- человеческих отношений и науки о поведении;
- науки управления, или количественных методов.

Данные школы возникли и развивались в конце XIX начале XX века. Приемы и методы, предложенные каждой из школ, во многом пересекаются и используются в практике современных предприятий и по сей день.

Так, например, основной идеей создателей школы «научное управление» было то, что, используя наблюдения, замеры, логику и анализ, можно усовершенствовать многие операции ручного труда, добиваясь более эффективного их выполнения. Первой фазой методологии научного управления был анализ содержания работы и определение ее основных компонентов. Затем требовалось изменить рабочие операции, устранив лишние, непродуктивные движения, и, используя стандартные процедуры и оборудование, повысить эффективность работы. Таким образом, предметная область применения методов данной школы, в общем случае, сводится к исследованию совокупности связанных между собой организационно-технических операций (или целых процессов), необходимых для достижения конечного результата — выполнения некого *проекта*. При этом, как правило, в интересах получения наиболее рационального варианта его реализации порядком выполнения соответствующих работ целесообразно *управлять*.

В теоретическом плане решение подобных задач связано, зачастую, с использования аппарата, так называемого сетевого планирования (СП) (или в современной трактовке — *управления проектами*), который основан на использовании математического аппарата теории графов и системного подхода для отображения и алгоритмизации комплексов взаимосвязанных работ, действий или мероприятий для своевременного и планомерного достижения четко поставленной цели [1].

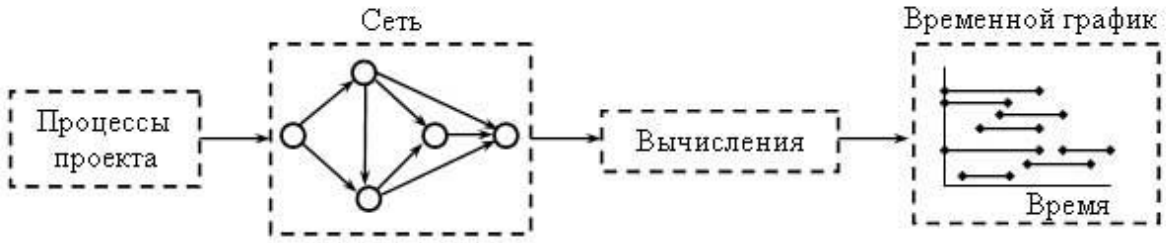


Рис. 1. Основные этапы выполнения проектирования

Для отображения и алгоритмизации тех или иных действий или ситуаций в данном аппарате используются экономико-математические модели, которые принято называть сетевыми моделями, простейшие из них — *сетевые графики*. (рис. 1).

На первом этапе определяются отдельные процессы, составляющие проект, их отношения предшествования (т. е. какой процесс должен предшествовать другому) и их длительность. Далее проект представляется в виде сети, показывающей отношения предшествования среди процессов, составляющих проект. На третьем этапе на основе построенной сети выполняются вычисления, в результате которых составляется рациональный временной график реализации проекта. При этом, если временные параметры продолжительности выполнения отдельных работ комплекса являются детерминированными, то продолжительность так называемого «критического пути», состоящего из работ с детерминированными временными оценками просто определяется как их сумма (1):

$$T_{кр} = \sum_{i,j \in L_{кк}} t(i, j) \tag{1}$$

где работы (i, j) составляют данный критический путь $L_{кр}$.

В случае же вероятностных параметров продолжительности работ, каждая из них рассматривается как непрерывная случайная величина, заполняющая интервал, ограниченный пределами, априорно задаваемыми ответственными исполнителями в виде минимальной (оптимистической) оценки продолжительности t_{min} или a и

максимальной (пессимистической) t_{max} или b. Одновременно ответственные исполнители дают и наиболее вероятную оценку продолжительности работ $t_{н.в.}$ или m (рис. 2).

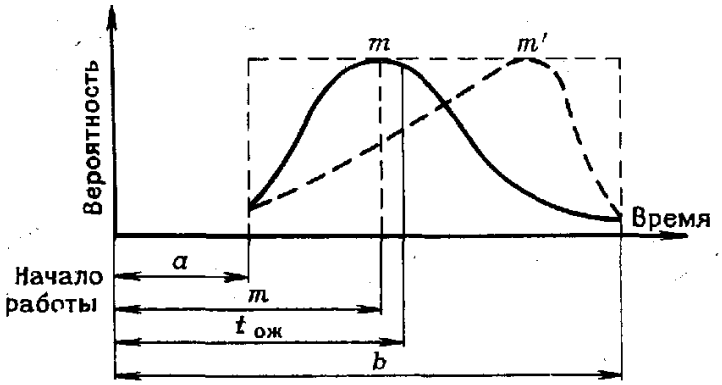


Рис. 2. Кривая распределения вероятности времени выполнения работ

Для расчета же параметров всей сети с вероятностными оценками продолжительностей работ наиболее широко применяется метод усреднения, суть которого состоит в том, что вероятностные оценки «превращают» в детерминированные и, вводя добавочную характеристику — меру неопределенности оценки — ее дисперсию $\sigma^2(t)$, производят расчет параметров сетевого графика.

Тогда вероятностная оценка ожидаемой продолжительности работы или ее математическое ожидание могут быть рассчитаны по формуле (2):

$$t_{ож} = \frac{a + 4m + b}{6} \tag{2}$$

Неопределенность $t_{ож}$ или ее дисперсия характеризуется размахом кривой распределения от a до b и вычисляется по формулам (3):

$$\sigma^2(t) = \frac{(b-a)^2}{36} \tag{3}$$

Далее на основании центральной предельной теоремы теории вероятностей принято считать, что распределение сроков наступления событий сетевого графика, в том числе завершающего со значением срока $T_{ож}$ и его дисперсией $\sigma^2(T)$, подчинено нормальному закону [3]. Поэтому, например, продолжительность критического пути и его дисперсия могут быть рассчитаны следующим образом (4):

$$T_{ож} = M\left[T_{кр}\right] = \sum_{\{i,j\} \in L_{кр}} t_{ож}(i,j)$$
$$\sigma^2(T) = \sum_{\{i,j\} \in L_{кр}} \sigma^2\left[t(i,j)\right] \tag{4}$$

В сетях со случайными продолжительностями работ всегда рассчитывается вероятность P того, что продолжительность всего комплекса работ не превысит заданного (директивного) срока $T_д$ (5)

$$P\left(T_{ож} \le T_Д\right) = \Phi\left[\frac{T_Д - T_{ож}}{\sigma(T)}\right] \tag{5}$$

где значение функции $\Phi\left[\frac{T_Д - T_{ож}}{\sigma(T)}\right]$ берется из таблиц или графиков нормального распределения.

Очевидно, что наличие предположения о нормальном распределении значений отдельных операций существенно снижает адекватность сетевых моделей и накладывает определенные ограничения на область применения метода. Снять указанные ограничения аналитических моделей аппарата СП на законы распределения случайных величин исходных данных, по нашему мнению, позволяет метод имитационного моделирования (ИМ), так как соответствующие технологии его реализации имеют возможность задавать любые их варианты.

В качестве примера решения задачи, связанной с оценкой своевременности реализации предполагаемого комплекса работ (проекта) с использованием технологии ИМ можно привести несложную сетевую модель процесса развертывания полевого узла связи (ПУС), заданную в частности в виде ориентированного (рис. 3) и табличного (табл. 1) графов.

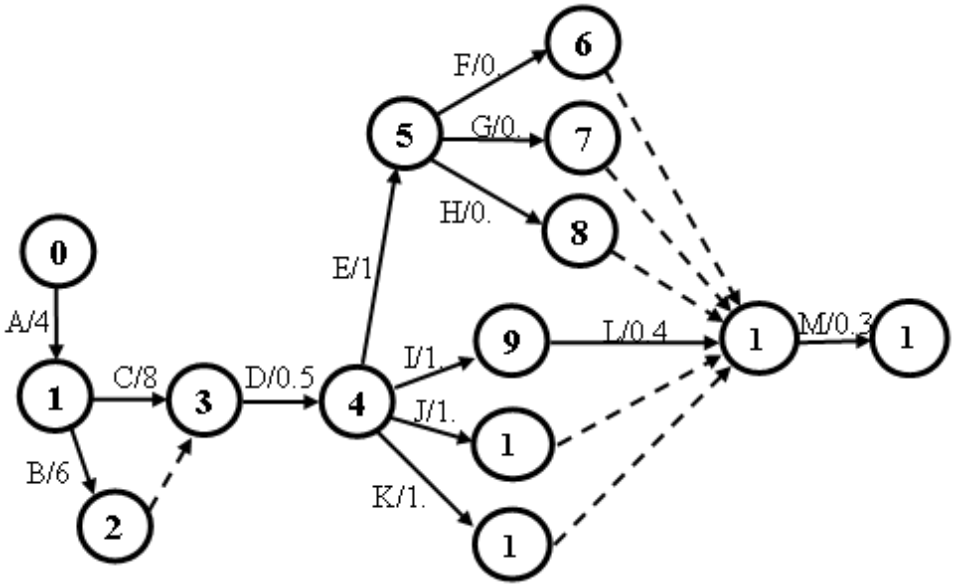


Рис. 3. Взаимосвязь процессов развертывания ПУС

Таблица 1

Описание сетевой модели процесса развертывание полевого узла связи

№ работы	События (узлы)	Содержание работы	$T_{мин.}$, мин.	T наиболее вероятное, мин.	$T_{макс.}$, мин.	Последующая работа
A.	0—1	Формирование походных колонн	180	240	300	B, C
B.	1—2	Перемещение колонны 1 в район развертывания ПУС	300	360	420	D
C.	1—3	Перемещение колонны 2 в район развертывания ПУС	360	480	600	D
D.	3—4	Формирование элементов ПУС	20	40	60	E, I, J, K
E.	4—5	Выдвижение элементов ПДРЦ на боевую позицию	40	60	120	F, G, H
F.	5—6	Развертывание аппаратных ПДРЦ	20	30	50	M
G.	5—7	Развертывание АФУ ПДРЦ	30	45	60	M
H.	5—8	Развертывание РРЛ привязки ПДРЦ-ПРЦ	25	35	45	M
I.	4—9	Развертывание аппаратных ПУ-ПУС и ЦКО	40	70	90	M
J.	4—10	Развертывание аппаратных ПРЦ	60	90	130	M
K.	4—11	Развертывание АФУ ПРЦ	45	60	90	M
L.	9—12	Привязка ПУС к ОСС	30	45	60	L
M.	12—3	Открытие радиовахт	20	30	45	-

Номера узлов сети возрастают в направлении выполнения проектов. Фиктивный процесс (2-3) введен для того, чтобы «развести» параллельные (конкурирующие) процессы C и B, а фиктивные работы 6-12, 7-12, 8-12, 10-12, 11-12 указывают на несвязность параллельных процессов F, G, H, I, J и K.

Решение задачи. Вариант блок-схемы алгоритма имитационной модели, соответствующий данному сетевому графику, для ее реализации, например, специализированной среде GPSS Studio [3], представлена на рис. 4.

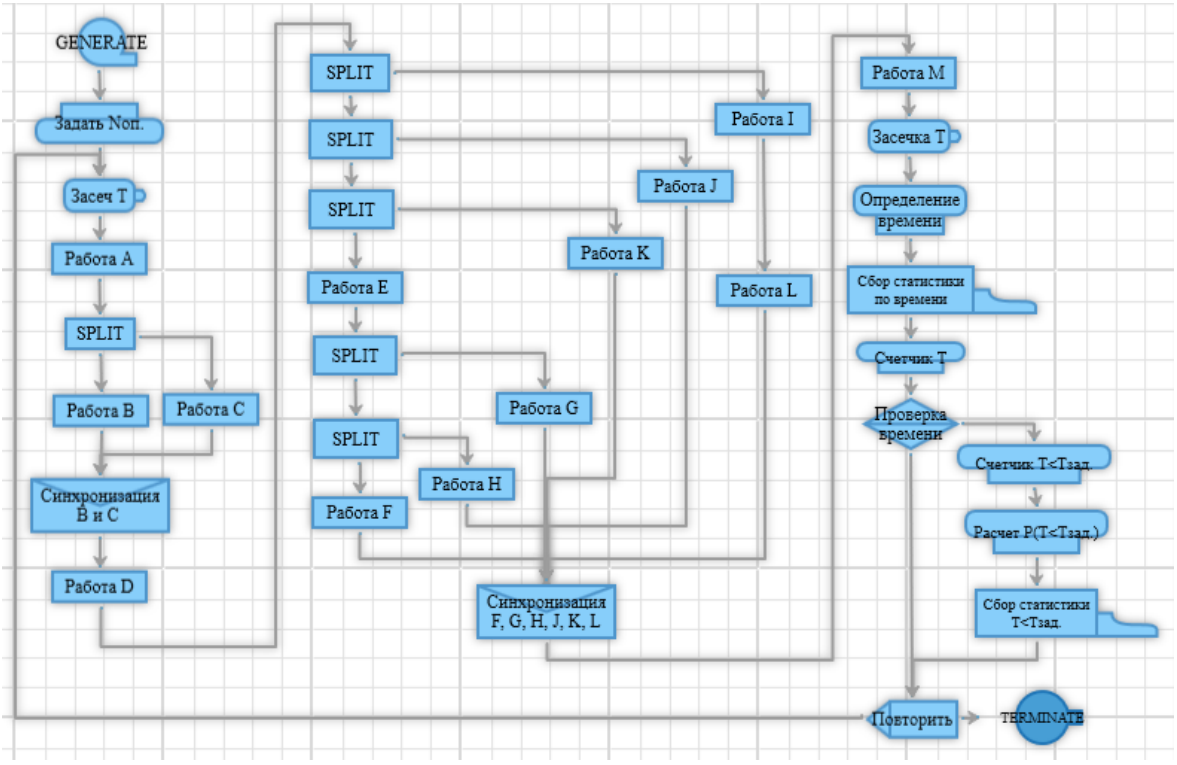


Рис. 4. Блок-схема алгоритма ИМ процесса развертывания ПУС (вариант)

Как уже отмечалось выше, при решении подобных задач в качестве ограничивающих *факторов*, как правило, выступают: **время**, отведенное на выполнение проекта, и имеемые людские *ресурсы,* а в качестве исследуемых параметров (показателей эффективности) — такие вероятностно-временные характеристики (ВВХ) как: *среднее время* выполнения проекта, его дисперсия и *своевременность* решения задачи как вероятность реализации проекта в установленные сроки [4, 5].

Поэтому для проведения серии экспериментов в интересах оптимизации СГ есть смысл, в первую очередь, обратить внимание на наиболее трудоемкие операции, в частности; B и C, задав для них диапазон наиболее вероятных значений с определенным шагом, имея при этом ввиду — перераспределение объема работ между исполнителями проекта, и закладывая соответствующие риски в максимальные их значения (например, рис. 5).

Рис. 5. Значения заданного времени и продолжительности операций, выбранные в качестве факторов модели

Значительное число экспериментов, которое потребуется при этом провести, несомненно, является заметным препятствием практического применения метода ИМ. Однако развитие современных технологий его реализации помогают автоматизировать данную процедуру [3].

Так, например, используя возможности среды GPSS Studio по проведению серии экспериментов и ее средств анализа, можно получить следующие результаты зависимости временных характеристик процесса развертывания ПУС, графическая интерпретация одного из которых представлена на рис. 7.

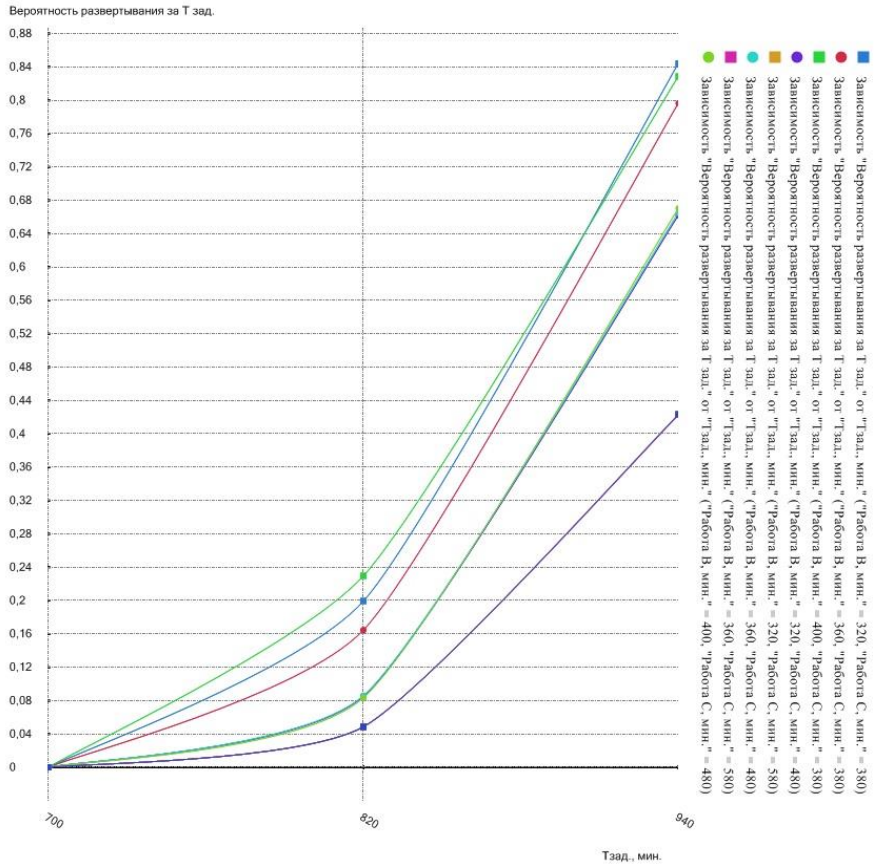


Рис. 7. Зависимость своевременного развертывания ПУС от заданного срока при различных соотношениях продолжительности работ В и С

Уменьшение вероятности своевременного решения задачи по развертыванию ПУС при ужесточении требований (заданных сроков) очевидна. Однако данные результаты позволяют определить, все-таки, и соответствующие пределы таких требований для конкретных ситуаций и организационно-технических возможностей этой системы. В данном случае, реально на это мероприятие следует отводить не менее 15 часов, когда в результате оптимизационных мероприятий можно будет ставить задачу о получении гарантированного (например, с вероятностью 0.9) результата своевременного развертывании ПУС.

В частности, таковыми мероприятиями могут стать изменения маршрутов или скоростей движения колон, обеспечивающие продолжительность работы В в пределах 320-400 минут, а работы С — не более 380 мин.

Наилучший же результат достигается при соотношении продолжительностей этих работ 320/380.

Очевидно, что перераспределяя между исполнителями параллельных работ (как это и положено при сетевом планировании) их объемы, выравнивая при этом соотношения их временных интервалов, и выполняя аналогичные серии экспериментов можно: во-первых, существенно сократить критический путь выполнения поставленной задачи; во-вторых, найти условия при которых она будет выполнена своевременно; и, в-третьих, определить какие из операций (процедур) оказывают наибольшее влияние на конечный результат и, поэтому требуют особого внимания с точки зрения риска их невыполнения при управлении «проектом».

Заключение. Таким образом применение технологии имитационного моделирования в сочетании с методами сетевого планирования позволяет успешно решать задачи, связанные с поддержкой принятия решений по управлению организационно-техническими проектами.

СПИСОК ЛИТЕРАТУРЫ

1. Пуха Г. П. Моделирование систем : учеб. пособие. СПб. : СПбГЭУ, 2020. 279 с.
2. Вентцель Е. С. Исследование операций: задачи, принципы, методология. М. : Наука, 1988. С. 206.
3. Девятков В. В., Девятков Т. В., Федотов М. В. Имитационные исследования в среде моделирования GPSSSTUDIO : учеб. пособие / под общ. ред. В. В. Девяткова. М. : Вузовский учебник : ИНФРА-М, 2018. 283 с.
4. Пуха Г. П. К вопросу об использовании системы поддержки принятия решений в работе пунктов управления связью флотов // Морская радиоэлектроника. № 2 (72), июнь. 2020. С. 10-13.
5. Котомин М. А., Пуха Г. П. Применение имитационного моделирования для поддержки принятия решения на организацию технического обслуживания производственных объектов // Актуальные проблемы защиты и безопасности : Труды XXV Всероссийской научно-практической конференции. СПб., 2022. С. 268-278.

УДК 004.056.5

ОЦЕНКА РИСКОВ ДЛЯ БЕЗОПАСНОСТИ И БАЗОВАЯ ЗАЩИТА ДАННЫХ ПРИ ПЕРЕДАЧЕ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Тетюев Евгений Викторович[1, 2]
[1]Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
[2]Санкт-Петербургский государственный экономический университет
Грибоедова канала наб., 30-32, лит. А, Санкт-Петербург, 191023, Россия
e-mail: tetiuev.ev@mail.ru

Аннотация. Рассматриваются общие принципы передачи данных в телекоммуникационных сетях и связанные с этим риски для их безопасности. Приведены доводы в пользу того, что, несмотря на свою надежность и наличие современных протоколов взаимодействия, современные сети не могут гарантировать защиту передаваемой информации от завладения третьими лицами. Сделаны выводы о необходимости защиты критических данных при передаче по сети с помощью организации частных сетей и каналов связи, использования шифрования и технологии обфускации трафика.

Ключевые слова: телекоммуникационные сети; компьютерные сети; безопасность данных; шифрование.

SECURITY RISK ASSESSMENT AND BASIC DATA PROTECTION DURING TRANSMISSION IN TELECOMMUNICATION NETWORKS

Tetiuev Evgenii[1, 2]
[1]Saint Petersburg National Research University of Information Technologies, Mechanics and Optics
49 Kronverkskiy Av, St. Petersburg, 197101, Russia
[2]Saint Petersburg State University of Economics
30-32 Griboyedov Canal Emb, letter A, St. Petersburg, 191023, Russia
e-mail: tetiuev.ev@mail.ru

Abstract. The general principles of data transmission in telecommunication networks and the associated risks to their security are considered. Arguments are given in favor of the fact that, despite its reliability and the availability of modern protocols, the networks cannot guarantee the protection of transmitted information from third parties. Conclusions are drawn about the need to protect critical data during transmission over the network by organizing private networks and communication channels, using encryption and traffic obfuscation technology.

Keywords: telecommunication networks; computer networks; data security; encryption.

Введение. Информационно-экономическая безопасность предприятий [1-3] во многом определяется надежностью [4, 5] и информационной безопасностью инфокоммуникационных систем. Современные телекоммуникационные сети имеют сложную структуру, представленную широким спектром физических каналов передачи данных, узлов коммутации, множеством протоколов и схем взаимодействия между отдельными узлами и сегментами сети. Чтобы понять возможные риски при передаче данных необходимо оценить безопасность каналов и среды передачи данных между узлами сети.

Традиционно телекоммуникационные сети рассматривают, как совокупность сетей, способных передавать информацию. К ним относятся компьютерные сети, сети телефонной, сотовой, спутниковой и радиосвязи, телевизионные сети. Теоретически в структуру можно включить и специфические решения вроде PLC (связь через ЛЭП), но они недоступны для работы обычных пользователей. Каждая из упомянутых технологий имеет как преимущества, так и недостатки, и применяется в зависимости от масштаба охватываемого региона, сложностей в организации канала связи, количества устройств в сети. В процессе обмена данными всегда существуют риски, связанные с их потерей или искажением. Большинство подобных проблем доставки уже решены с помощью использования протоколов с контролем доставки, функций хэширования и самокорректирующихся кодов. Поэтому сегодня самым большим риском для безопасности при передаче данных является их утечка, то есть получение третьими лицами.

По аналогии с законом Амдала для вычислительных систем, уровень безопасности канала передачи данных будет определяться самым уязвимым его звеном, будь то узел или среда передачи.

В рамках данной статьи основной упор делается именно на исследование сети, поэтому локальные вопросы информационной безопасности для конечных устройств, между которыми идет передача данных, не рассматриваются. Таким образом, мы будем рассматривать утечку данных либо на узлах сети, либо через передающую среду. Чаще всего считывание данных может быть организовано с помощью снифферов — специального оборудования или ПО, способного считывать и анализировать трафик на узлах сети, либо имеющего доступ к среде передачи данных, проводной и особенно беспроводной.

Передающие узлы сети различаются по уровням охвата: от узловых станций провайдеров глобальной сети до локальных коммутаторов или АТС уровня жилого дома и предприятия. По очевидным причинам сложнее всего получить доступ к спутникам связи и оборудованию магистральных провайдеров. Высокий уровень охвата сети подразумевает большой объем потенциальных данных для обработки и поиска, серьезные меры безопасности и жесткий контроль со стороны надзорных органов, поэтому технически считывание данных проще организовать в локальных масштабах: на уровне локальных коммутационных устройств, оборудования интернет-провайдера, предприятия или, в идеальном случае, на конечном оборудовании пользователя. Очевидно, что самой уязвимой в этом случае является аналоговая телефонная сеть, поскольку она не обладает механизмами защиты передаваемых данных. При наличии доступа к коммутационному устройству злоумышленник получает практически прямой доступ к передаваемым данным в пределах узла. Несмотря на это, аналоговая телефонная связь остается популярной и сегодня, преимущественно за счет своей простоты. Проблему ее безопасности можно решить переходом в цифровой формат, в частности использованием технологии VoIP. Тем более, развертывание IP-сети можно организовать прямо на инфраструктуре телефонных сетей с использованием DSL технологий, и большинство современных АТС поддерживают такую возможность. Минусы технологии в том, что она не отличается высокой скоростью связи, и в начале развертывания ADSL в России наблюдались проблемы совместного использования канала со службами пожарной и вневедомственной охраны, хотя они и остались в прошлом.

Покушаться на сохранность данных могут не только заинтересованные неизвестные, но и сам провайдер услуги. Например, если речь идет о сети Интернет, провайдеры могут использовать технологии вроде DPI для отслеживания содержимого передаваемых пакетов с целью фильтрации трафика, сбора статистики, либо в интересах государственных служб. Здесь, опять же, стоит понять уровень, на котором осуществляется мониторинг. В стандартах связи магистральных провайдеров упор делается на скорость передачи данных и низкое время отклика, поэтому у магистральных устройств нет времени на глубокий анализ передаваемого трафика. Если речь идет о третьих лицах, физический доступ к передающему оборудованию совсем не обязателен. Удаленное администрирование, карантинные ограничения и банальная халатность привели к тому, что множество действующих сетей имеют незащищенные точки входа. Например, в исследовании 2021 года специалист обнаружил уязвимые точки входа и проник в корпоративную сеть РЖД [6]. Помимо непосредственной утечки важных данных вроде доступа к камерам или корпоративным сервисам, использование подобных лазеек могло привести к более серьезным последствиям, например, в случае установки специализированного или вредоносного ПО на сервера и устройства компании. Пример наглядно показывает, что даже в сети крупной компании могут иметь критические уязвимости.

Среда играет огромную роль в безопасности передачи данных. Проводные компьютерные сети традиционно строились с использованием коаксиального кабеля, витой пары и оптоволокна, и ничто из них не гарантирует безопасность передачи данных. Медные и алюминиевые кабели, особенно низкого качества, ожидаемо дают наводки. Даже будучи экранированным, коаксиальный кабель остается самым простым вариантом для врезки и сниффинга. Несмотря на угасающую популярность, некоторые провайдеры до сих пор используют компьютерные сети и цифровое телевидение на базе коаксиального кабеля, в виду простоты его прокладки. Витая пара создавалась с задумкой, в том числе на уменьшение влияния сигналов в проводах друг на друга и на окружающую среду. Тем не менее, их сигналы можно считать достаточно чувствительным оборудованием. Даже оптоволоконный кабель при определенных условиях может испускать часть светового потока наружу, позволяя считывать данные, минимально влияя на качество исходного сигнала [7]. И, конечно же, ни один из упомянутых способов организации сети не защищает от банальной врезки в кабель с установкой устройства-повторителя. Подобные риски нивелируются только при использовании специализированных кабелей с защитой и системой обнаружения воздействия, но маловероятно, что рядовой провайдер услуги будет расходовать дополнительные ресурсы на физическую защиту линии, если это не требуется.

Также важную роль играет топология сети. В плане безопасности наиболее уязвимой из топологий является шина, поскольку в ней отсутствует коммутация каналов, и конечные получатели технически имеют доступ к информации для соседних абонентов из-за распараллеливания канала. Такой подход характерен при использовании архитектуры PON сетей на базе оптоволоконного соединения при обустройстве т.н. канала «последней мили». К счастью, современные стандарты вроде GPON и SPON подразумевают шифрование, но сама концепция дает абонентам доступ к данным других участников сети, пусть и зашифрованным. При наличии соответствующей аппаратуры, эти данные можно сохранить и впоследствии расшифровать.

В радиосвязи ситуация с доступом к передающей среде еще проще: использование точек доступа и широковещательных технологий является массовым, особенно в сфере сотовой и спутниковой связи. Для связи между собой базовые станции сотовой сети используют либо оптоволоконные кабели, либо радиорелейную связь со стационарными антеннами, способными обеспечивать направленный мощный сигнал, для считывания которого требуется находиться в узком конусе его распространения. Однако в зоне охвата конечных пользователей несущий сигнал доступен всем участникам сети, и говорить о какой-либо защите именно передающей среды не приходится.

Основная причина такого подхода в том, что обеспечить узконаправленный сигнал к каждому отдельному устройству при большом количестве абонентов в сети либо технически невозможно, либо экономически нецелесообразно. Бывают и исключения, например, проект Starlink использует в своих терминалах и спутниках активные фазированные антенные решетки (АФАР), что сужает зону распространения сигнала до узкого конуса, затрудняя возможность его считывания. Однако такие решения отличаются большой стоимостью и требуют наличия субсидирования [8].

Считывание информации доступно не только напрямую с несущего сигнала, но и по косвенным признакам. Ярким примером является эксперимент, где исследователи смогли считать звуковую информацию в звукоизолированном помещении, анализируя колебания света, испускаемые обыкновенной лампочкой, которые считывала чувствительная аппаратура [9]. Таким образом, требуется не только обеспечить изоляцию канала передачи данных, но и минимизировать сторонние эффекты, возникающие при использовании устройств и передающей среды, особенно наводки и микровибрации.

Описанные выше примеры показывают, что организовать полноценную защиту передающей среды и каналов связи практически невозможно, надеяться на защищенность сетей и оборудования — наивно, следовательно, необходимо защищать сами передаваемые данные еще до попадания их в сеть, то есть на конечном оборудовании клиента. Защита данных осуществляется несколькими путями. Самый очевидный из них — криптография и шифрование. Если речь идет о компьютерных сетях, в том числе Интернет, то шифровать можно как отдельные блоки важных данных, так и канал связи, например, организованный посредством VPN. Исторически технология использовалась для организации корпоративных сетей, но в последние годы к ней значительно вырос интерес широкой публики. Здесь стоит напомнить, что VPN по определению является не защитой, а лишь способом организации сети внутри сети, и защищенным каналом становится только тогда, когда на всех устройствах этой сети включено шифрование.

Использование популярных сервисов, предоставляющих шифрованный VPN также вызывает вопросы, поскольку это означает генерацию или передачу ключей владельцам сервиса и использование их серверов, давая возможность расшифровывать и анализировать данные. Поэтому лучшее решение — собственноручное создание защищенного соединения. При этом предпочтение стоит отдать ассиметричному шифрованию, поскольку оно не требует передачи ключа для расшифровки. Динамическая смена ключей также положительно влияет на безопасность передачи данных, а симметричное шифрование подходит разве что для локального хранения данных или при работе в сети в комбинированной схеме. В любом случае следует помнить, что абсолютных методов шифрования не существует, и все они сводятся только к увеличению времени на расшифровку сообщения до неприемлемого. Теоретически, большинство современных криптографических систем, основанных на факторизации чисел, в будущем станут уязвимы для мощных квантовых компьютеров, но на данном этапе их развития это не является приоритетной угрозой. К счастью, уже сейчас разрабатываются шифраторы нового поколения, способные не только обеспечить надежную передачу данных, но и выявить возможное считывание канала и противодействовать ему [10]. Ожидаемо, внедрение подобных систем обещает быть трудозатратным и дорогостоящим, вряд ли они будут доступны широкой аудитории в обозримом будущем.

Есть ли разница между шифрованием отдельных блоков данных и использованием защищенного канала? С математической точки зрения разницы нет, при условии, что используются одни и те же алгоритмы шифрования. Однако, с точки зрения обработки и анализа данных, разница огромна.

Большая доля зашифрованных данных в трафике однозначно будет привлекать внимание алгоритмов и заинтересованных лиц. Поэтому наиболее разумным решением будет шифрование только части трафика через использование проксирования, где некритичные данные идут по стандартному маршруту, а критичные — через защищенный канал. К тому же, VPN соединение подразумевает подключение к одному или нескольким серверам, и частое к ним обращение также может привлечь лишнее внимание. Поэтому следующий этап защиты — обфускация зашифрованного трафика, то есть маскировка его под обыкновенный, не представляющий интереса для наблюдателя. Это обширная тема, представленная множеством технологий, большинство из которых основаны на протоколах Shadowsocks и V2Ray и их многочисленными клонами. Использование различных их сочетаний позволяет замаскировать данные под обычный трафик, например, стандартное общение с веб-сервером через HTTPS.

Одним из лидеров по разработке средств противодействия подобным решениям является Китай, но и энтузиасты не стоят на месте, разрабатывая новые методы защиты данных и обфускации трафика [11].

Заключение. Анализ основных методов и средств передачи информации с использованием телекоммуникационных сетей показывает, что физические каналы связи не могут обеспечить абсолютную защиту. Обеспечение безопасной передачи данных — комплексная задача, которую требуется решать на всех уровнях сетевой модели, не стоит слепо доверять ее поставщику услуг связи. Оптимальным решением будет повышение собственной информационной грамотности и использование соответствующих средств защиты, лучшим из которых является адекватное шифрование самих данных с использованием проверенных алгоритмов, чья

надежность доказана исследованиями и подтверждена временем, и без использования сторонних сервисов. Альтернативой является создание между устройствами защищенного соединения также с использованием шифрования. В этом случае, даже при наличии в канале передачи данных скомпрометированных узлов или передающей среды, информация будет малополезной для третьих лиц.

СПИСОК ЛИТЕРАТУРЫ

1. Верзун Н. А., Колбанев М. О., Омельян А. В. Сетевая архитектура цифровой экономики. СПб. : СПбГЭУ, 2018. 156 с.
2. Колбанёв М. О., Верзун Н. А., Нестеренко Е. С. Применение и влияние цифровых технологий в экономической деятельности // Информационные системы и технологии в экономической деятельности : сборник статей. СПб. : СПбГЭУ, 2020. С. 27-32.
3. Верзун Н. А., Колбанев М. О., Шамин А. А. Архитектура цифровой экономики // Региональная информатика и информационная безопасность : сборник трудов межрегиональной конференции и Санкт-Петербургской международной конференции. СПб., 2018. Выпуск 6. С. 110-114.
4. Bogatyrev V. A., Derkach A. N., Bogatyrev S. V. Timeliness of the reserved maintenance by duplicated computers of heterogeneous delay-critical stream // CEUR Workshop Proceedings. ISTMC 2019 — Selected Papers of the 4th All-Russian Scientific and Practical Conference with International Participation «Information Systems and Technologies in Modeling and Control». 2019. С. 26-36.
5. Богатырев В. А. Отказоустойчивость и сохранение эффективности функционирования многомагистральных распределенных вычислительных систем // Информационные технологии. 1999. № 9. С. 44-48.
6. Самый беззащитный — уже не Сапсан. Всё оказалось куда хуже… [Электронный ресурс] // Хабр : [сайт]. URL: https://habr.com/ru/articles/536750/ (дата обращения: 29.09.2023).
7. Iqbal M. Z., Fathallah H. and Belhadj N. Optical fiber tapping: Methods and precautions // 8th International Conference on High-capacity Optical Networks and Emerging Technologies. 2011. Pp. 164-168.
8. Урличич Ю. Старые и новые идеи в спутниковой связи // Первая миля. 2021. № 3(95). С. 14-21.
9. Nassi B., Pirutin Y., Shamir A., Elovici Y., Zadov B. Lamphone: Real-Time Passive Sound Recovery from Light Bulb Vibrations // IACR Cryptol. ePrint Arch. 2020.
10. Карцан И. Н., Аверьянов В. С. Гибридный квантово-классический подход для защиты наземных линий связи // Южно-Сибирский научный вестник. 2019. № 4-1(28). С. 264-269.
11. Qingbing J., Zhihong R., Man C., Jie L., Zhili Z. Security Analysis of Shadowsocks(R) Protocol [Электронный ресурс] // Sec. and Commun. Netw. 2022 (2022). // URL: https://doi.org/10.1155/2022/4862571 (дата обращения: 23.08.2023).

УДК 742.012

ПЛАНОВАЯ ЭКОНОМИКА ПОЛНОГО ЦИКЛА — ГАРАНТ ПЕРСПЕКТИВНОГО РАЗВИТИЯ

Ярошевич Людмила Ивановна
Санкт-Петербургский государственный институт кино и телевидения
Правды ул., 13, Санкт-Петербург, 191119, Россия
e-mail: Ludmila-arttech@rambler.ru

Аннотация. Структура системных устройств как проводник информации. Разные смыслы прилагательных плановая и рыночная в системе экономика.

Ключевые слова: прямая и обратная информационная связь; терминология экономики; план; рынок.

PLLANNED FULL — CYCLE ECONOMY-THE GUARANTOR OF LONG-TERM DEVELOPMENT

Yaroshevich Ludmila
St. Petersburg State institute of film and television
13 Pravda str., St. Petersburg, 191119, Russia
e-mail: Ludmila-arttech@rambler.ru

Abstract. The structure of system devices as a conductor of information. Different meanings of the adjectives plan and market economy in the system.

Keywords: feedback; terminology of economy; plan, market.

Введение. Мир стремительно движется вперед, порой не оставляя человеку ни времени ни сил разобраться с пристрастием, в том, что происходит, например, в Экономике.

Парадокс сегодняшнего дня заключается в том, что музыканты, преодолевая трудности в работе с партитурой, упорно оттачивают мастерство, в то время как экономисты, к счастью не все, не справляясь с планом, решают его уничтожить. На самом деле, разрушители Административно-хозяйственной экономической системы не предоставили аргументированных доказательств, основанных на научных знаниях, о правомерности своих действий. По логике вещей, сначала идет управление и связь – командная структура, а потом то, чем управляют, рынок. В народе говорят: «Хвост не может идти впереди лошади».

План (партитура, композиция, сценарий) это — запись алгоритма, точной последовательности действий от цели к результату. Фазовая диаграмма сложного формообразования идет именно по плану. В основе произведений искусства, литературы, музыки, архитектуры,… лежит план.

Системная плановая экономика являет собой последовательную, многоуровневую, логически осмысленную сложную конструкцию представления данных, объединенных устремлением к общей цели — перспективному

развитию. И эта правильная междисциплинарная концепция подтверждается во всех уровнях формообразования. С точки зрения Кибернетики, системные устройства, такие как план, партитура, композиция,… имеют целевое предназначение управлять экономикой, здравоохранением, обучением, полетами,… и действуют подобно механизму передачи информации внутри процесса (проводники). Внутренняя плановая структура сохраняет, поддерживает и передает единое содержание большого объема, направленное на осуществление общей цели. Недаром, синоним единства — монолит. Что доказывает, что система это — неразъемное соединение, описывающее логически обоснованный рабочий процесс, где каждая фаза обеспечивает основание для развития следующей фазы и т.д. вплоть до достижения результата.

Циклы процессов конструирования: цели, развития, достижения стадии готовой формы системных величин аналогичны при формировании механических, графических, вербальных, звуковых устройств. Системное устройство, порядок (по рядам) имеет естественное происхождение. Ориентируясь в окружающей среде, человек считывает пространственные уровни, описывая события, происходящие ближе, дальше,… На самом примитивном уровне он мысленно фиксирует точки в пространстве и на плоскости. Так он поступает, отыскивая ряд и место в кинотеатре, определяя шахматную позицию на шахматной доске. В более сложных случаях профессиональной необходимости он определяет точки координат, методом ортогонального проектирования или находит объекты в море, воздухе и на суше методом эхо. Подобно тому, как камень, брошенный в воду, является «эпицентром», создающим круги волнового поля, так и человек, приемник/передатчик информации создает зрительное поле в процессе получения и обратной связи.

Список, как форма представления данных, является более простой копией фазовой диаграммы Экономика и также демонстрирует порядковую последовательность отраслей, символизирующих перспективу развития системы в пространстве и времени.

Рассмотрим примерный список отраслей современной экономики за последние 20 лет, взятый из интернета [1].

На первый взгляд, удивляет позиция № 25, а, именно, почему Управление находится в конце списка?

По логике вещей, любой план должен начинаться с обозначения курса следования (куда мы идем?), далее предполагается целевое управление сформированным списком приоритетных задач, связанных воедино обоснованным соподчинением параметров. Однако, № 3 Сельское хозяйство, а обслуживание сельского хозяйства идет под № 7, и заготовки под № 12, и т. д. О каком, логически выверенном соподчинении параметров может идти речь? Заметим также, что лидирующие позиции в списке заняты базовыми отраслями промышленностью и сельским хозяйством, как в Плановой экономике, а не рынком.

1. Промышленность
2. Сельское хозяйство
3. Лесное хозяйство
4. Строительство
5. Сферы материального производства
6. Обслуживание сельского хозяйства
7. Транспорт
8. Связь
9. Торговля и общественное питание
10. материально-техническое снабжение и сбыт
11. Заготовки
12. Информационно-вычислительное обслуживание
13. Операции с недвижимым имуществом
14. Общая коммерческая деятельность по обеспечению функционирования рынка
15. Геология и разведка недр, геодезическая и гидрометеорологическая служба
16. Жилищное хозяйство
17. Коммунальное хозяйство
18. Не производственные виды бытового обслуживания населения
19. Здравоохранение, физическая культура социальное обеспечение
20. Народное образование
21. Культура и искусство
22. Наука и научное обслуживание
23. Финансы, кредит, страхование пенсионное обеспечение
24. Управление
25. Общественные объединения

Отсутствует функциональная зависимость между параметрами.

Попробуем мысленно перенести каждую позицию экономических отраслей от 1-26, на уровни зрительного поля, согласно направлению взгляда, получим перспективу развития Экономики. Само понятие перспектива означает смотреть сквозь, проникать взором, наблюдая из центра зрительного поля. Каков современный план, такова и перспектива, недостатки присутствуют. Тогда как, в функцию Плановой экономики входит организация

структуры изображения, т.е. наведение правильного порядка, обеспечивающего как можно более точный прием, передачу, хранение и прочтение информации, с целью исключить ошибки и искажения.

План, это, как траектория полета из пункта А в пункт В, где все стадии полета обязательны к выполнению. Если рынок выходит из экономической системы, он становится самостоятельным, самоопределяется и работает по своим законам. При этом, нет плана нет обязательств внутри рабочего цикла, уходят из поля зрения цель,…, результат, многоуровневая перспектива развития. Пример, морковка остается целой только до попадания в суп, в супе она — ингредиент, и уже не имеет самостоятельности, результатом является суп.

В советские времена рынок не был выведен из системы Экономика и не имел самостоятельного значения. Суть в том, план это — устройство непрерывного процесса, неделимое целое. Если «вытаскивать» из него отдельные составляющие, то рушится все. Внутри системы нельзя менять местами последовательно соединенные составляющие части.

Так система образования, условно говоря, состоит из дошкольного, начального, среднего и высшего этапов, изменить последовательность нельзя, они связаны единым содержанием.

Нет смысла менять название биосистемы, даже если какие-либо проблемы в ней возникают. Если «вырвать» кусок из биосистемы, или поменять местами составляющие части, то она погибнет. «Титульное» название сложной информационной системы нельзя переименовывать в простое. Кроме того, при наличии проблем в биосистеме она не перестает быть биосистемой.

Представим себе цикл пошива пальто: выбор модели, ткани, кроя, рабочий процесс, пошив воротника, рукавов, соединение частей. Пошив рукавов выведем из системы, в результате цель не будет достигнута, пальто нет, а рукавами не согреешься. Управление и связь нарушаются.

Теперь о рынке: Если говорить о, возможно, бесконечной актуальности рынка, то необходимо понимать, что название «Рыночная экономика» возникло в подсистеме и обслуживает интересы только рынка.

В народе говорят: «Рачительный хозяин не все покупает и не все продает», да и рынок занимает всего одну зависимую позицию в системе Экономика.

Плановая экономическая система моделирует процесс развития страны, осуществляет переход от одного качественного состояния к другому, более высокому, стабильному.

Моделирование процесса разрушения запускается движением системы вспять, т. е. в обратном порядке. Поэтому, замена названия Плановая экономика на Рыночную экономику не говорит ни о чем хорошем. Системные величины, такие как экономика, литература, музыка, архитектура, образование, … имеют плановую структуру и являются произведениями человеческой мысли.

План это — конструктивное устройство для проведения информации, а рынок — это место или, может быть — метод осуществления товарно-денежного оборота**,** способ быстрого получения денег. Главный смысл Плановой экономики — перспективное развитие, а не сиюминутная прибыль. Можно ли считать эти две величины взаимозаменяемыми? Думается, что конструкцию следует сравнивать и менять на конструкцию, а метод на метод.

Заключение:

1. Единое информационное поле, общие законы аудиовизуального восприятия и обратной связи предполагают формирование общей теории представления данных для точных и гуманитарных наук. Важность такого шага подтверждается проблемами с планом в Экономике. Сначала идет управление и связь — командная структура, а потом то, чем управляют, а не наоборот. Уникальный человеческий мозг создает рынок и управляет им в системе Экономика, и никак иначе.
2. Сложная система Экономика не может опираться только на рынок. Экономика — процесс хозяйственной деятельности, а рынок- место, процесс торговли, в крайне случае, может трактоваться как метод, способ деятельности. Соотношение величин план и рынок — целое и часть сложной системы Экономика.
3. Одна фаза «Рынок» из всей фазовой диаграммы «Экономика» не выстраивает должной перспективы в сравнении с полной системой. Пространство и время являются обязательными компонентами абсолютно всех изображений.
4. Государственная экономика России это — сложная целевая система, которая, категорически, не может быть выстроена по простой схеме «Рынок». Иерархия способов представления данных по объему и важности информации обычно оформляется от простого к сложному или от сложного к простому: рисунок, схема, расписание, график, содержание, оглавление, таблица, система,…

Синонимы к слову простой — упрощенный, наивный, незначительный, незнатный…

5. Рынок пусть будет, но пусть он ничего не возглавляет. Не нужно, чтобы руководители страны ходили с протянутой рукой и просили у олигархов денег на содержание государства. Командная структура предписана Кибернетикой.

СПИСОК ЛИТЕРАТУРЫ

1. Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка М. : Издательство «АЗЪ», 1995.
2. РосИнфоСтат : сайт. Отрасли современной экономики в России [1].

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ НА ТРАНСПОРТЕ

УДК 66.013.51

ПРИМЕНЕНИЕ БЕРЕЖЛИВОГО ПОДХОДА В ПРОЦЕССАХ СУДОСТРОИТЕЛЬНОЙ ОТРАСЛИ

Антонова Алёна Евгеньевна[1], Соколов Сергей Сергеевич[2]
[1] Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
[2] Российский университет транспорта
Октябрьский пер., 7, Москва, 127018, Россия
e-mails: vasalen2@rambler.ru, sokolovss@gumrf.ru

Аннотация. В статье рассматривается возможность внедрения бережливого производства в судостроительной промышленности, позволяющее оптимизировать процессы, сократить потери и улучшить коммуникации между участниками производства. Определён ряд мероприятий для внедрения бережливого судостроения, выделены проблемы и перспективы, а также аспекты полезности бережливого судостроения.

Ключевые слова: бережливое производство; судостроительная отрасль; оптимизация производственных процессов; конкурентоспособность; контроль качества; оценка эффективности; аспекты полезности судостроения.

APPLICATION OF THE LEAN APPROACH TO THE SHIPBUILDING INDUSTRY

Antonova Alena[1], Sokolov Sergey[2]
[1] Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya st., St. Petersburg, 198035, Russia
[2] Russian University of Transport
7 Oktyabrsky Av., Moscow, 127018, Russia
e-mails: vasalen2@rambler.ru, sokolovss@gumrf.ru

Abstract. The article discusses the possibility of using lean manufacturing in the shipbuilding industry, which allows to reduce processes, reduce and increase the interaction between production factors. A number of activities to attract lean shipbuilding have been identified, problems and prospects, as well as aspects of the usefulness of lean shipbuilding, have been identified.

Keywords: Lean; shipbuilding industry; optimization of production processes; competitiveness; quality control; efficiency mark; aspects of the usefulness of shipbuilding.

Введение. Бережливое судостроение становится все более актуальным в современном мире судостроения. Оно позволяет повысить качество и конкурентоспособность продукции, сократить затраты на производство и увеличить производительность. Бережливое судостроение включает в себя оптимизацию процессов, сокращение потерь и улучшение коммуникации между участниками производства.

Внедрение бережливого судостроения может стать ключевым фактором для успешного развития судостроительных компаний в условиях жесткой конкуренции на мировом рынке. В судостроительной отрасли бережливое производство является одним из самых сложных процессов, так как при строительстве судов задействовано большое количество персонала, различных видов техники, оборудования и другие виды ресурсов [1]. Внедрение метода бережливого производства в судостроении позволяет экономить до 30% материальных и трудовых затрат. При этом, по оценкам экспертов, сэкономленные средства, как правило, направляются на повышение качества судов, увеличение их конкурентоспособности.

Бережливое производство — это концепция управления производственным процессом, которая нацелена на устранение потерь и повышение эффективности производства. В судостроительной промышленности бережливое производство может быть использовано для повышения качества продукции, сокращения времени производства, снижения затрат на материалы и энергию, а также увеличения производительности труда [2].

Бережливое судостроение включает в себя несколько основных принципов (рис.1), которые помогают снизить затраты, улучшить качество продукции и повысить эффективность производственных процессов.

Рис.1 Основные принципы бережливого производства

Одним из ключевых принципов бережливого производства является устранение потерь. Потери могут возникать на различных этапах производственного процесса, таких как ожидание, транспортировка, хранение и обработка материалов. Чтобы устранить потери, необходимо оптимизировать процессы и улучшить координацию между различными отделами. Также бережливое производство предполагает использование принципов канбан (система управления запасами) и кайдзен (постоянное улучшение процессов). Канбан позволяет оптимизировать процесс производства и сократить время ожидания материалов, а кайдзен — повысить качество продукции и уменьшить количество брака. Кроме того, бережливое производство включает в себя использование современных технологий и оборудования, таких как автоматизация и роботизация, которые позволяют увеличить производительность и снизить затраты на производство, а также обучение сотрудников с целью развития навыков и знаний, чтобы они могли эффективно работать в рамках бережливого подхода.

В целом, бережливое производство является эффективным инструментом для улучшения производственных процессов в судостроительной промышленности и повышения конкурентоспособности продукции [3]. Бережливое судостроение помогает компаниям снизить затраты, увеличить производительность и улучшить качество продукции. Оно также способствует созданию культуры инноваций и постоянного улучшения, что является важным фактором для успеха в современном бизнесе.

Основная идея бережливого судостроения заключается в том, чтобы максимально использовать ресурсы и минимизировать потери в производственном процессе. Для этого используются различные методы и инструменты, такие как автоматизация процессов, оптимизация производственных линий, улучшение коммуникации между сотрудниками и т. д.

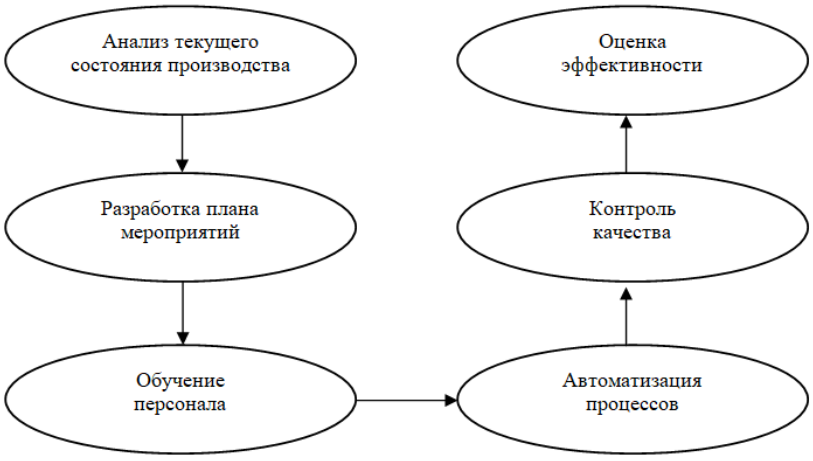


Рис. 2 Мероприятия для внедрения бережливого производства

Примерами бережливого судостроения могут служить:

Использование системы управления производством для определения оптимальной загрузки производственных линий и предотвращения простоев.

Внедрение системы контроля качества для выявления и устранения дефектов на ранних стадиях производственного процесса.

Использование технологии автоматизированного проектирования для оптимизации конструкции судна и сокращения времени на проектирование.

Обучение сотрудников методам бережливого производства для повышения их производительности и снижения издержек.

Бережливое судостроение является эффективным инструментом для повышения конкурентоспособности судостроительных компаний на мировом рынке и улучшения качества продукции.

Для внедрения бережливого производства в судостроении необходимо провести ряд мероприятий, представленных на рис. 2.

В судостроении, как и в любой другой отрасли, существуют свои проблемы при внедрении бережливого производства [4]:

– Сложность производства: судостроение является сложной отраслью, которая требует высокой квалификации и опыта от специалистов. Это может затруднить внедрение бережливых методов, так как они требуют более гибкого подхода к работе.

– Ограниченность ресурсов: судостроение связано с использованием большого количества различных материалов и оборудования, что может ограничивать возможности для внедрения бережливых методов.

– Высокая стоимость: бережливые методы требуют значительных инвестиций в оборудование и обучение персонала, что может быть дорогостоящим для судостроительных компаний.

– Отсутствие культуры: некоторые судостроительные компании могут не иметь культуры бережливости, что затрудняет внедрение бережливых методов и достижение результатов.

После внедрения бережливого судостроения у судостроительных компаний появляются следующие перспективы:

– снижение затрат на производство (бережливое судостроение помогает снизить потери и оптимизировать процессы, что приводит к уменьшению затрат на производство);

– повышение качества продукции (благодаря оптимизации производственных процессов качество продукции повышается, что позволяет увеличить удовлетворенность клиентов и повысить конкурентоспособность компании);

– увеличение производительности (благодаря сокращению времени и усилий, затрачиваемых на производство, увеличивается производительность, что позволяет быстрее и эффективнее выполнять заказы);

– улучшение взаимодействия между подразделениями (бережливое судостроение способствует улучшению взаимодействия между различными подразделениями компании, что повышает эффективность работы и улучшает качество продукции);

– возможность постоянного совершенствования (компании, внедряющие бережливое судостроение, могут постоянно совершенствовать свою продукцию и процессы, что позволяет им оставаться конкурентоспособными на рынке и развиваться).

К минусам внедрения бережливого судостроения можно отнести следующие:

– высокие затраты на внедрение и обучение персонала новым методам работы;

– сложность процессов производства, требующих специальных знаний и опыта;

– необходимость постоянного улучшения и адаптации к изменяющимся условиям рынка;

– возможные изменения в структуре и процессах организации, что может вызвать сопротивление со стороны персонала.

Заключение. Бережливое судостроение необходимо для всех судостроительных компаний, которые хотят повысить свою конкурентоспособность на рынке, улучшить качество своей продукции и снизить затраты на производство. Бережливое судостроение является актуальной темой для судостроительной отрасли. Бережливые принципы позволяют компаниям сокращать издержки, повышать качество продукции, увеличивать производительность и конкурировать на мировом рынке. Бережливость в судостроении позволяет снизить затраты на материалы, сократить время на производство, повысить качество продукции и удовлетворить потребности клиентов.

Бережливое судостроение может быть полезно во многих аспектах судостроения, в том числе [5]:

– Оптимизация производственных процессов: бережливое судостроение позволяет сократить время и затраты на производство, улучшить качество продукции и повысить производительность.

– Устранение потерь: бережливое судостроение устраняет потери времени, энергии и материалов, что позволяет снизить затраты и повысить эффективность работы.

– Определение ценности продукта: бережливое судостроение определяет ценность продукта, что помогает компаниям сосредоточиться на том, что действительно важно для клиентов.

– Улучшение коммуникации: бережливое судостроение улучшает коммуникацию между сотрудниками, что помогает им лучше понимать друг друга и работать более эффективно.

– Постоянный анализ: бережливое судостроение требует постоянного анализа процессов, чтобы находить новые возможности для улучшения.

Успешное внедрение бережливого судостроения зависит от нескольких факторов, включая готовность руководства и персонала к изменениям, наличие необходимых ресурсов и поддержку со стороны высшего руководства. Кроме того, успешное внедрение требует постоянного мониторинга и анализа процессов, а также обучения и мотивации персонала.

СПИСОК ЛИТЕРАТУРЫ

1. Beifert A., Gerlitz L., Prause G. Industry 4.0 — For Sustainable Development of Lean Manufacturing Companies in the Shipbuilding Sector // Reliability and Statistics in Transportation and Communication. RelStat, 2017 / I. Kabashkin, [ets al], 2018. Lecture Notes in Networks and Systems, Vol. 36. Springer, Cham. https://doi.org/10.1007/978-3-319-74454-4_54.
2. ГОСТ Р 57522–2017. Бережливое производство. Руководство по интегрированной системе менеджмента качества и бережливого производства. М. : Изд-во «Стандартинформ», 2017. 16 с.
3. Синго С. Изучение производственной системы Тойоты с точки зрения организации производства / пер. с англ. М. : Институт комплексных стратегических исследований, 2006. 312 с.
4. О'Лири Д. ERP системы. Современное планирование и управление ресурсами предприятия. Выбор, внедрение и эксплуатация / пер. с англ. Водянова Ю. И. М. : Вершина, 2004. 372 с.
5. Hebbar S. Value Stream Mapping: A Continuous Improvement tool for Reduction in Total Lead Time, 2014. С. 931-934.

УДК 004.056

ИННОВАЦИОННЫЕ ПОДХОДЫ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ ПРОТИВ СЕМАНТИЧЕСКИХ АТАК

Богданова Полина Вадимовна, Прокопенко Даниил Николаевич
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: Emofor40@yandex.ru, prokopenko.danilka121@gmail.com

Аннотация. Рассмотрены основные виды семантических атак. Представлены системы на основе машинного обучения, которые направлены на устранение семантических атак.

Ключевые слова: машинное обучение; искусственный интеллект; семантические атаки.

SEMANTIC ATTACKS AND POSSIBLE WAYS TO PROTECT AGAINST THEM

Bogdanova Polina, Prokopenko Daniil
Admiral Makarov State University of Maritime and Inland Shipping
Dvinskaya st., 5/7, Saint-Petersburg, 198035, Russia
e-mails: Emofor40@yandex.ru, prokopenko.danilka121@gmail.com

Abstract. The main types of semantic attacks are considered. Machine learning-based systems are presented, which are aimed at eliminating semantic attacks.

Keywords: machine learning; artificial intelligence; semantic attacks.

Введение. В настоящей эпохе цифровой информации существуют различные методы осуществления семантических атак с целью искажения обучающих данных. Семантические атаки становятся все более распространенными и угрожают надежности и конфиденциальности данных. Они представляют серьезные риски для информационной безопасности, так как могут привести к утечке чувствительной информации, нарушению целостности данных и даже потере контроля над системами. Разработка эффективных мер по защите информации от семантических атак становится неотъемлемой частью современных технологий безопасности. В данной статье рассматривается актуальная проблема защиты информации от семантических атак, а также сделан обзор подходов к их предотвращению или устранению.

Состязательные атаки. Существует 3 класса атак [1]: WhiteBox (обеспечивает полный доступ к архитектуре и параметрам модели, а также к программе обучения и гиперпараметрам обучения), BlackBox (имеет ограниченный доступ к модели) и GrayBox (позволяет получать информацию о типе алгоритма и его гиперпараметрах).

Нейросети также обладают гиперпараметрами, которые называют параметрами модели. Они задаются перед началом обучения и не изменяются в процессе обучения. Параметры обучения — это внутренние параметры модели, которые оптимизируются в процессе обучения.

При анализе WhiteBox, где есть полный доступ модели, анализатор может изучать архитектуру сети, параметры модели и обучающие данные. Это позволяет провести более детальный анализ и исследовать все возможные выходные данные нейронной сети при различных входных данных. Однако, при масштабировании сети, количество данных и параметров может стать слишком большим, что затрудняет проведение полного анализа до больших классификаторов.

Атаки белого ящика используют информацию о градиенте. В сценарии белого ящика есть несколько атакующих стратегий, каждая из которых представляет собой различные компромиссы между вычислительными затратами на их создание и успешностью. Все эти методы максимизируют изменение функции потери модели,

сохраняя при этом небольшое возмущение входного изображения. Чем выше размерность пространства входного изображения, тем легче создавать состязательные примеры.

В случае BlackBox, где доступ к модели ограничен, анализатору может быть доступна только входная и выходная информация сети. Это ограничение делает проведение анализа сложнее, поскольку анализатору неизвестны параметры и архитектура модели. Кроме того, масштабирование сети в BlackBox может привести к еще большей сложности анализа, поскольку анализатору может быть недостаточно информации для полного понимания работы сети. Атаки черного ящика могут быть запущены с использованием методов оптимизации без градиента, например: генетические алгоритмы, случайные поиски и стратегии эволюции. Так как для атак черного ящика градиенты не доступны, то построение замещающей (теневой) модели, которая будет белым ящиком, позволяет совершить атаку. Используя любой из алгоритмов белого ящика, генерируются состязательные примеры для альтернативной модели, которые могут быть перенесены и станут состязательными примерами для целевой модели.

Атака GrayBox [2] находится между атаками WhiteBox и BlackBox. При анализе GreyBox, где доступ к модели ограничен, анализатор имеет ограниченную информацию о внутренней структуре и параметрах модели. В таком случае анализатор может использовать только входные и выходные данные модели для проведения анализа. Это ограничение может затруднить детальное исследование модели и выявление ее уязвимостей.

Атаки GrayBox [3] используют информацию о модели и ее выходных данных. В сценарии GrayBox, анализатор может иметь некоторое представление о внутренних механизмах модели, но не полную информацию. Он может использовать эту информацию, чтобы создавать состязательные примеры, которые максимизируют изменение функции потери модели, сохраняя небольшое возмущение входных данных. Однако, из-за ограниченной информации о модели, создание состязательных примеров может быть более сложным и требовать больше вычислительных ресурсов. Атака GrayBox может быть эффективнее, чем атака BlackBox, но менее мощно, чем атака WhiteBox.

В обоих случаях, как в WhiteBox, так и в GreyBox, анализаторы стремятся выявить уязвимости и слабые места модели, чтобы улучшить ее безопасность. Однако, выбор между различными сценариями зависит от доступности информации и целей атакующей стороны.

Высокоточные нейронные сети уязвимы для состязательных примеров. Они обычно получаются путем незначительного изменения входных данных, которые правильно классифицированы сетью, так что сеть неправильно классифицирует возмущенные входные данные. Было показано, что различные виды возмущений успешно генерируют состязательные примеры. Наиболее распространенной атакой в этом случае является FGSM (Fast Gradient Sign Method).

Атака FGSM (метод быстрого градиентного знака) — является атакой, основанной на особенностях обучения моделей. Вместо корректировки веса сети на основе градиентов обратного распространения, FGSM корректирует входные данные, добавляя определенный вектор шума, умноженный на є (допустимая величина возмущения), что максимизирует потери сети. Таким образом FGSM обманывает модель нейронной сети, заставляя ее делать неверные прогнозы, наложением шума, который препятствует корректной работе модели.

Атака DeepFool представляет собой метод, который используется для генерации состязательных примеров для нейронных сетей. Она является нецелевой атакой белого ящика, что означает полный доступ к архитектуре и параметрам модели, а также к обучающим данным.

Целью атаки DeepFool является создание состязательных примеров с минимальным возмущением относительно исходного входного изображения. Чтобы достичь этого, атаки DeepFool выполняют поиск кратчайшего расстояния от исходного изображения до ближайшей границы решения (гиперплоскости) и проецируют исходное изображение ортогонально на эту границу решения.

Для выполнения атаки DeepFool, злоумышленник сначала аппроксимирует границу решения сети с использованием метода итеративной линейной аппроксимации. Затем вычисляется ортогональный вектор от исходного изображения до этой линеаризованной границы решения.

Атака DeepFool может быть применена и в случае бинарной классификации, и в случае мультиклассификации [5]. Для бинарной классификации атака DeepFool вычисляет оптимальное возмущение между двумя границами решения (гиперплоскостями) классов. Для мультиклассификации атака DeepFool выбирает границу решения с наименьшим отступом от исходного изображения и проецирует его на эту границу.

Существует также обновленная версия атаки DeepFool, называемая Adversarial Perturbation. Она использует метод DeepFool для генерации минимального возмущения для каждого изображения, а затем находит универсальное возмущение, которое удовлетворяет двум ограничениям. Это позволяет использовать одно универсальное возмущение для атаки множества изображений. Более подробно с атакой Adversarial Perturbation можно ознакомиться в источнике [6].

Атака Карлина и Вагнера (C & W) [5] представляет собой метод атаки на модели машинного обучения, который направлен на поиск минимального возмущения входных данных, достаточного для изменения результатов классификации модели. В отличие от некоторых других методов атаки, C & W не требует доступа к внутренним параметрам модели и может быть применен к моделям, которые доступны только через интерфейс предсказания.

Применение C & W к моделям машинного обучения может быть полезным для оценки их устойчивости к возмущениям и повышения их защищенности. Однако, как и с любыми методами атаки, необходимо быть осмотрительным при использовании C & W, так как он может привести к нежелательным последствиям, таким как неправильная классификация данных или нарушение конфиденциальности.

Порождающая состязательная сеть (Generative Adversarial Network). Генеративные состязательные сети (GAN) [7] представляют собой недавнюю разработку в области машинного обучения и представляют собой мощный класс нейронных сетей, который используется при обучении без контроля. Они являются порождающими моделями в том смысле, что они создают новые данные, которые напоминают исходные обучающие данные. Новые данные создаются на основе изучения закономерностей в исходных данных. Данный алгоритм машинного обучения использует две состязательно обучаемые нейронные сети: генератор и дискриминатор.

Генератор создает новые данные путем сопоставления вектора случайного шума с реалистичным выходным сигналом, таким как изображение. Затем дискриминатор обучается различать сгенерированные и реальные данные.

Генератор и дискриминатор обучаются вместе в процессе, называемом состязательным обучением. Во время этого процесса генератор пытается создать данные, которые могут обмануть дискриминатор, в то время как дискриминатор пытается точно определить, являются ли данные реальными или поддельными. Затем выходные данные генератора уточняются на основе обратной связи от дискриминатора, и процесс продолжается до тех пор, пока генератор не сможет выдавать данные, неотличимые от реальных.

Атаки GAN в основном происходят в процессе обучения FL (федеративное обучение) моделям распознавания классификации изображений. Процесс атаки выполняется злоумышленником локально и не уничтожает саму модель, поэтому, с точки зрения жертвы, существование такой атаки невозможно обнаружить, следовательно, конфиденциальность жертвы часто просачивается при неизвестных обстоятельствах. Возможные атаки GAN включают добавление шума к обучающим данным, внесение изменений в изображения или злонамеренное исправление этикеток классов. Цель таких атак — обмануть модель классификации и изменить ее выводы.

Состязательные патчи. Как говорилось выше, состязательные примеры создаются путем добавления небольших возмущений к исходному входному образцу. Состязательные патчи отличаются от состязательных примеров тем, что они добавляют шум только в определенные области изображения, а не ко всему изображению. Авторы в [8] продемонстрировали состязательные патч-атаки на системы распознавания лиц с использованием генеративных состязательных сетей. Они использовали метод атаки GAN. Метод атаки предполагает использование модели черного ящика и применение его как к цифровому, так и к физическому миру, поэтому злоумышленнику не требуется знание параметров и структуры модели глубокого изучения, используемой системой распознавания лиц, для проведения атаки. Этот метод заставляет систему распознавания лиц ошибочно идентифицировать злоумышленника как кого-то другого, тем самым создавая значительную угрозу. Авторы пользуются фактором ношения очков, как аксессуара для того, чтобы скрыть враждебное возмущение в очках. При атаке с выдачей себя за другого человека очки и патчи маскируют человека, не искажая черты лица.

Инверсия модели. Информация о достоверности, возвращаемая многими классификаторами машинного обучения, позволяет проводить новые атаки с использованием инверсии модели (рис. 1), которые могут привести к неожиданным проблемам с конфиденциальностью [9].

Целью атаки является: восстановить или исследовать исходные данные, используемые для обучения модели, исходя из выданных ей предсказаний и соответствующих уровней достоверности. Например, зная, что объект был правильно классифицирован с высокой достоверностью, атакующий может попытаться определить особенности данного объекта, которые привели к такому предсказанию. Это может привести к утечке конфиденциальной информации или нарушить приватность пользователей.

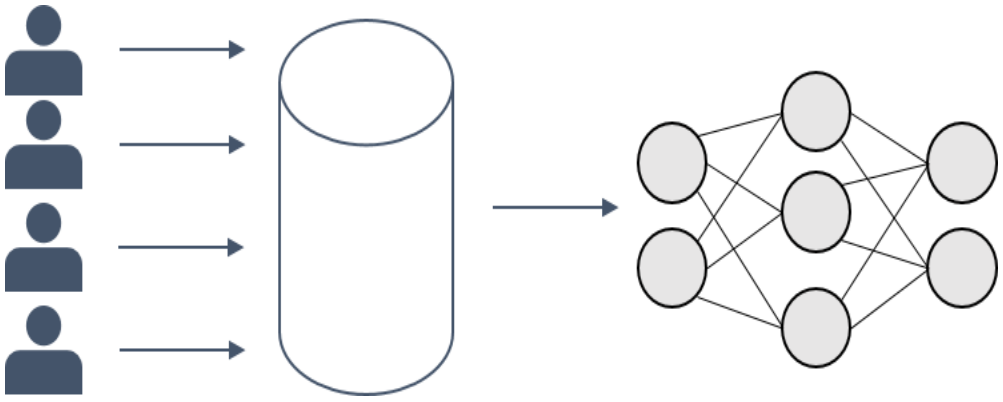


Рис. 1. Идея модельной инверсионной атаки

Способы защиты от состязательных атак. AI2 (Adversarial Input Interpretation) — это метод защиты нейронных сетей от враждебных атак. Алгоритм AI2 использует сверточную сеть MMSTV (Makoto Mori Slow Scan TV) и внедряет слой возмущения перед входным слоем в процессе обучения. Этот слой применяет FGSM атаку, чтобы «обучить» модель быть устойчивой к подобным атакам. Таким образом, благодаря этому методу MMSTV становится значительно устойчивее к FGSM атаке.

Для обеспечения доказуемой устойчивости AI2 к FGSM атаке используется классическая структура абстрактной интерпретации. Это позволяет получить надежные, вычислимые и точные конечные приближения потенциально бесконечных наборов поведения нейронных сетей. Абстрактная область состоит из логических формул, описывающих определенные формы, такие как зонотопы и ограниченные формы многогранников.

Ключевой идеей AI2 является переформулирование проблемы анализа нейронных сетей в рамках классической абстрактной интерпретации. Для этого определены абстрактные преобразователи, которые фиксируют поведение обычных слоев нейронной сети, и представлен ограниченный домен (powerset), который обеспечивает компромисс между точностью и масштабируемостью.

Экспериментальные результаты показали, что AI2 может эффективно обрабатывать нейронные сети, которые недоступны существующим методам защиты. Помимо этого, AI2 разрабатывается и дополняется абстрактными преобразователями для поддержки большего количества функций нейронных сетей. Также создается библиотека для моделирования распространенных возмущений, таких как вращение, сглаживание и эрозия. Эти расширения позволят лучше применять AI2 в области информационной безопасности. Метод защиты AI2 от враждебных факторов представлен в исследовании [4].

Метод состязательного обучения, представленный в [6] основан на базе данных MNIST (Modified National Institute of Standards and Technology) и CIFAR-10 (Canadian Institute For Advanced Research). Сетевая архитектура состоит из двух сверточных слоев ReLU (сверточные слои нейронной сети с выправленными активациями линейных единиц), один из которых содержит 32 фильтра размером 3 на 3, а за ним 64 фильтра размером также 3 на 3. Затем слой с максимальным объединением 2 на 2 и отсевом со скоростью 0,25 применяется перед полностью подключенным слоем ReLU с 1024 единицами. Последний уровень — это еще один полностью связанный уровень с 11 блоками и функцией активации softmax для классификации в 10 обычных классов плюс состязательный класс. Используется набор инструментов для обеспечения состязательной надежности для создания состязательных примеров для обучения и тестирования. Из-за ограниченных вычислительных ресурсов авторы используют только атаки BIM (Basic Iteractive Method) и C & W (самые сильные атаки) и гауссов шум для генерации дополнительных изображений для обучения. С помощью этого метода удалось повысить точность классификаторов на тестовых изображениях MNIST и CIFAR-10 и точность классификатора при атаках FGSM, C & W, BIM и DeepFool.

Способы защиты генеративно-состязательных сетей. Существует метод против GAN-атак [10]. Защитная идея заключается в следующем: во-первых, частично маскируются изображения в исходном наборе обучающих данных defender, чтобы злоумышленник не мог использовать поддельные данные, сгенерированные локально после атаки GAN, для идентификации исходного внешнего вида реального изображения невооруженным глазом для достижения цели защиты конфиденциальности. Также в [10] обучающие изображения смешиваются с CutMix, что улучшает способность модели к обобщению и гарантирует, что точность модели, обученной с использованием замаскированных изображений, не пострадает слишком сильно.

Способы защиты от состязательных патчей. Одним из способов защиты от состязательных патчей заключается в использовании супервизора, контролирующего систему распознавания лиц. Этот подход является наиболее эффективным, так как супервизору не нужно распознавать всё изображение, а лишь небольшую область, которую занимают патчи на лице. Основная система распознавания лиц обрабатывает изображение и предоставляет свои результаты, затем супервизор анализирует эти результаты и ищет признаки, которые могут указывать на наличие адверсариальных патчей (небольшие модификации или добавления к изображению, которые могут быть незаметны для человеческого восприятия, но способны вводить в заблуждение алгоритмы компьютерного зрения или нейронные сети) на лице [11]. Если супервизор обнаруживает подозрительные признаки, он может отметить область, где могут быть патчи, и запросить уточнение или дополнительную информацию от системы распознавания лиц.

Система может повторно обработать указанные области или запросить более точные данные от пользователя, чтобы убедиться в правильности идентификации.

Этот подход обеспечивает более высокую защиту от состязательных патчей, поскольку супервизор способен выявлять подозрительные изменения, которые могли быть внесены в изображение [12].

Способы защиты от инверсии модели. Один из способов защиты от атак инверсии модели — это использование деревьев принятия решений. Подобно тому, как порядок объектов в дереве решений влияет на его точность, он также может влиять на уязвимость дерева к атакам инверсии. В частности, уровень, на котором возникает уязвимая функция, может повлиять на точность атаки. Если этот уровень находится на более низком уровне, то точность атаки может быть выше. Проверка этой гипотезы представлена в [13, 14].

Все атаки на модели распознавания лиц основаны на градиентном спуске. Одной из возможных мер защиты является снижение качества или точности информации о градиенте, извлекаемой из модели [14]. Это может быть достигнуто за счет снижения точности, с которой сообщаются показатели достоверности. При этом, при вычислении градиента, можно добавить шум или искажение, которые затруднят атакующему получение точной информации о градиенте и, следовательно, инверсии модели.

Заключение. Подводя итоги, отметим необходимость постоянного совершенствования систем безопасности и применения инновационных методов для борьбы с семантическими атаками. Только таким образом можно повысить уровень защиты информационных систем и минимизировать потенциальные угрозы для безопасности данных [15, 16]. Дальнейшие исследования в этой области могут привести к разработке более эффективных методов защиты и обеспечения безопасности в сфере информационных технологий. Было обнаружено, что искусственный интеллект является перспективным инструментом в области информационной безопасности, способным обнаруживать киберугрозы, вредоносные действия и предсказывать потенциальные атаки [11, 17, 18].

Системы искусственного интеллекта, основанные на машинном и глубинном обучении, а также нейронных сетях, имитируют работу биологических нейронных сетей в мозге человека [17]. Они обучаются распознавать вредоносные программы и реагировать на них, а также анализировать данные о киберугрозах для прогнозирования их влияния.

Использование искусственного интеллекта в области информационной безопасности открывает новые возможности для защиты от семантических атак. Он позволяет обнаруживать даже незначительные проявления вредоносных программ или атак вымогателей до их проникновения в систему. Кроме того, анализ данных о киберугрозах позволяет предсказывать потенциальные атаки и принимать соответствующие меры предосторожности.

СПИСОК ЛИТЕРАТУРЫ

1. Bhambri S., Muku S. A Survey of Black-Box Adversarial Attacks on Computer Vision Models, 2020 [Электронный ресурс]. URL: https://arxiv.org/pdf/1912.01667.pdf (дата обращения: 10.07.2023).
2. Намиот Д. Е. Схемы атак на модели машинного обучения // International Journal of Open Information Technologies ISSN, 2023. [Электронный ресурс]. URL: file:///C:/Users/l/Downloads/shemy-atak-na-modeli-mashinnogo-obucheniya.pdf (дата обращения: 10.07.2023).
3. Lin Z., Li K., Yang Y., Sun F., Wu L., Shi P., Ci S., Zuo Y. DRESIA: Deep Reinforcement Learning-Enabled Gray Box Approach for Large-Scale Dynamic Cyber-Twin System Simulation // IEEE Open Journal of the Computer Society, 2021. [Электронный ресурс]. URL: https://ieeexplore.ieee.org/document/9488228/authors#authors (дата обращения: 10.07.2023).
4. Gehr T., Mirman M., Drachsler-Cohen D., Tsankov P., Chaudhuri S., Vechev M. AI2: Safety and Robustness Certification of Neural Networks with Abstract Interpretation // IEEE Symposium on Security and Privacy (SP), 2018. [Электронный ресурс]. URL: https://ieeexplore.ieee.org/document/8418593 (дата обращения: 10.07.2023).
5. Lin J., Dang L., Rahouti M., Xiong K. ML Attack Models: Adversarial Attacks and Data Poisoning Attacks, 2021. [Электронный ресурс]. URL: https://arxiv.org/ftp/arxiv/papers/2112/2112.02797.pdf (дата обращения: 10.07.2023).
6. Lin J., Laurent L. Njilla, Xiong K. Secure machine learning against adversarial samples at test time, 2022. [Электронный ресурс]. URL: https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-021-00125-2 (дата обращения: 10.07.2023).
7. Andrei-Grigore M., Zinca D., Dobrota V. Development of a Machine-Learning Intrusion Detection System and Testing Its Performance Using a Generative Adversarial Network, 2023. [Электронный ресурс]. URL: https://www.researchgate.net/publication/367403291_Development_of_a_Machine-Learning_Intrusion_Detection_System_and_Testing_of_Its_Performance_Using_a_Generative_Adversarial_Network (дата обращения: 10.07.2023).
8. Ren-Hung Hwang, Jia-You Lin, Sun-Ying Hsieh, Hsuan-Yu Lin, Chia-Liang Lin. Adversarial Patch Attacks on Deep-Learning-Based Face Recognition Systems Using Generative Adversarial Networks, 2023. [Электронный ресурс]. URL: https://www.mdpi.com/1424-8220/23/2/853 (дата обращения: 10.07.2023).
9. Boenisch F. Attacks against Machine Learning Privacy (Part 1): Model Inversion Attacks with the IBM-ART Framework, 2020. [Электронный ресурс]. URL: https://franziska-boenisch.de/posts/2020/12/model-inversion/ (дата обращения: 10.07.2023).
10. Xiaoyu Ma, Lize Gu. Research and Application of Generative-Adversarial-Network Attacks Defense Method Based on Federated Learning, 2023. [Электронный ресурс]. URL: https://www.mdpi.com/2079-9292/12/4/975 (дата обращения: 10.07.2023).
11. Sokolov S., Zhilenkov A., Chernyi S., Nyrkov A., Glebov N. Hybrid neural networks in cyber physical system interface control systems // Bulletin of Electrical Engineering and Informatics, Vol. 9. №. 3. 2020. Pp. 1268-1275. https://doi.org/10.11591/eei.v9i3.1293.
12. Ныркова А. П., Соколов С. С., Алимов О. М., Черный С. Г., Доровской В. А. Оптимальная идентификация объектов в задачах распознавания необитаемыми подводными аппаратами // Проблемы информационной безопасности. Компьютерные системы. № 2 (42). 2020. С. 58–64.
13. Fredrikson M., Jha S., Ristenpart T. Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures [Электронный ресурс]. URL: https://rist.tech.cornell.edu/papers/mi-ccs.pdf (дата обращения: 10.07.2023).
14. Полтавцева М. А., Лаврова Д. С. Высокопроизводительные системы обнаружения вторжений. СПб. : Политех-пресс, 2020. 186 с.
15. Ныркова А. П., Рудакова С. А. Методика аудита объектов информатизации по требованиям информационной безопасности // Журнал университета водных коммуникаций. № 3, 2012. С. 146–149.
16. Sokolov S. S., Glebov N. B., Antonova E. N., Nyrkov A. P. The Safety Assessment of Critical Infrastructure Control System // Proceedings of the IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies», IT and QM and IS, 5 November 2018, 2018. Pp. 154-157. https://doi.org/10.1109/ITMQIS.2018.8524948.
17. Tsymay Y. V., Nyrkov A. P., Kardakova M. V. Neurointerface Modeling For Controlling Dynamic Systems // Intellectual Technologies on Transport. 2022. № 4. Pp. 85-93. https://doi.org/10.24412/2413-2527-2022-331-52-60.
18. Sobolev A.S., Chernyi S. G., Krivoguz D. O., Nyrkov A. P., Zinchenko E. G. Convolution Neural Network for Identification of Underwater Objects // Proceedings of the Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus 2022 9755621. 2022. Pp. 455-458. https://doi.org/10.1109/ElConRus54750.2022.9755621.

УДК 681.5

ПРОБЛЕМНО-ОРИЕНТИРОВАННОЕ МОДЕЛИРОВАНИЕ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ УПРАВЛЕНИЯ

Голоскоков Константин Петрович, Астапкович Алексей Александрович, Коротков Виталий Валерьевич
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: goloskokovkp@gumrf.ru, kafkoib@gumrf.ru, korotkovvv@gumrf.ru

Аннотация. В статье раскрывается содержание основных принципов проблемно-ориентированного моделирования в исследовании интегрированной автоматизированной системы управления запасами и транспортно-технологическими процессами. При этом рассматриваются методологические аспекты создания автоматизированных систем моделирования: концептуальная математическая модель анализа и нормирования технико-экономических показателей, функционирования систем материально технического обеспечения: моделирования системы (поставка — транспорт).

Ключевые слова: математическая модель; автоматизированная система; транспортно-технологический процесс; проблемно-ориентированный подход; поставки; сырье.

PROBLEM-ORIENTED MODELING IN AUTOMATED CONTROL SYSTEM

Goloskokov Konstantin, Astapkovich Alexey, Korotkrv Vitaly
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya st., Saint-Petersburg, 198035, Russia
e-mails: goloskokovkp@gumrf.ru, kafkoib@gumrf.ru, korotkovvv@gumrf.ru

Abstract. The article reveals the content of the main principles of problem-oriented modeling in the study of an integrated automated system for managing inventory and transport and technological processes. At the same time, methodological aspects of creating automated modeling systems are considered: a conceptual mathematical model for the analysis and standardization of technical and economic indicators, the functioning of logistics systems: system modeling (supply — transport).

Keywords: mathematical model; automated system; transport and technological process; problem-oriented approach; supplies; raw materials.

Введение. Решение задач взаимодействия и взаимосвязей, оптимизации ресурсопотоков, повышение эффективности принятия управленческих решений с целью оптимизации могут решаться достаточно хорошо на основе моделирования в рамках АСУ транспортно-технологическим процессом, АСУ материально техническим снабжением, АСУ запасами и других АСУ.

Однако, решение этих задач не такое уж простое дело. Так, если разработан план развития промышленности и хозяйства, детализированный до отраслевой номенклатуры ресурсов, решены вопросы структурно-технологической оптимизации, рассчитаны отраслевые схемы размещения производства, возникает проблема полной взаимной увязки отраслевых схем. [1-3] При решении этой проблемы следует различать два основных случая. Первый, когда существенными являются затраты на перевозки ресурсов и готовой продукции. Второй, когда на первый план выдвигается не транспортный фактор, а наличие необходимых ресурсов в том или ином регионе. Следовательно, межрегиональное моделирование материальных потоков тесно связано с размещением и объемами различных видов ресурсов. [4-7]

Необходимо иметь четкую картину сверхнормативных запасов, информировать возможных потребителей о том, какие ресурсы, где и в каких объемах могут быть реализованы. [8-10] Обменные операции следует расценивать как регулятор изменения потребности в ресурсах из-за корректировок в номенклатуре и объемах выпускаемой продукции, необходимо повысить их оперативность. Повышение запасов обусловлено несвоевременными, неритмичными поставками, многоступенчатое распределение запасов (по централизованным поставкам) и т. п. осложняет работу предприятий и вызывает излишний расход ресурсов. В номенклатуре планирования запасов следует выделять позиции, относящиеся к малотранспортабельным ресурсам (трудовые ресурсы, строительные мощности, некоторые виды сырья, многотоннажные и негабаритные грузы и т. д.). [11-14] Избыток малотранспортабельных видов ресурсов в *n*-м регионе обозначим вектором *Rn.*

При создании эффективных АСУ необходимо подробно исследовать первичный объект — непосредственно систему материально-технического снабжения. Их исследование показывает, что они, как правило, обладают достаточно сложной эшелонированной структурой с взаимозависимыми звеньями и разнообразными функциями. Изучение таких систем с помощью аналитических методов затруднительно, поэтому возрастает актуальность разработки эффективных имитационных моделей для анализа и нормирования технико-экономических показателей функционирования системы материально-технического обеспечения.

Решением данной проблемы является создание прикладного математического обеспечения автоматизированной системы моделирования, предназначенной для автоматизации процессов анализа и функционирования на основе применения средств имитационного моделирования и принятия решений, а также вычислительной техники.

Анализ возможных подходов [9, 10] к построению АСУ показывает, что это можно сделать на хорошем качественном уровне, если наиболее полно удовлетворить разнообразные требования к АСУ, в том числе:

– адекватно отражать специфику процессов функционирования конкретных материально-технического обеспечения;

– обладать широкими функциональными возможностями по моделированию процессов материально-технического обеспечения с различными уровнями их детализации;

– обеспечивать поэтапное наращивание функциональных возможностей АСУ за счет включения в ее состав новых моделей;

– способствовать снижению трудоемкости и стоимости, а также повышению качества вырабатываемых решений;

– предъявлять невысокие требования к математической и программистской квалификации пользователей.

В связи с этим при создании АСУ наиболее целесообразно использовать модельно-ориентированный подход, который основывается на принципах системного анализа, стандартизации, классификации, упорядочения, модульности. Использование принципов развития и совместимости обеспечивает возможность расширения функциональных характеристик АСУ с минимальной трудоемкостью. Суть данного подхода заключается в следующем.

На основе детального анализа специфики проблемной области моделирования АСУ осуществляется классификация и упорядочение понятий, объектов, процессов, функций и структур материально-технического обеспечения. Кроме того, систематизируются, обобщаются и разбиваются на классы уже существующие и вновь разработанные задачи анализа и нормирования технических показателей процессов материально-технического обеспечения, а также модели функционирования материально-технического обеспечения, обеспечивающие решение этих задач.

Формализация осуществляется на основе множества проблемных переменных, принимающих классифицируемые или числовые значения, т. е. (1)

$$K = <\{P\},\ \{\Pi\}, \varphi_э^к>, \tag{1}$$

где *{P}* — множество проблемных переменных концептуальных элементов, описывающих понятия, объекты, процессы и отношения проблемной области моделирования; *{П}*—множество значений, принимаемых проблемными переменными *P;* $\varphi_э^к$ — отображение переменных *P* на их значения *П* (2):

$$\varphi_э^к : P \longrightarrow \Pi. \tag{2}$$

Сущность задачи состоит в выработке (корректировке) оценочных или нормативных значений показателей содержания запасов и снабжения ресурсами исследуемой системы материально технического обеспечения и определяется в виде (3)

$$3 = <\{U\},\ \{V\},\ \{E\},\ \{R\},\ \{\Phi\},\ \{J\},\ \{\varphi\}>, \tag{3}$$

где *{U}* — множество управляемых переменных, которые можно варьировать для поиска решения задачи; *{V}* — множество наблюдаемых переменных, значения которых не изменяются в условиях данной задачи; *{E}* — множество критериев оценки решения задачи; *{R}* -множество переменных описания результатов решения задачи; *{Ф}*—множество нормообразующих факторов задачи; *{J}*—множество типов отображений между компонентами задачи; $\{\varphi\}$ — множество отображений *j*-го типа между компонентами задачи *(j =1,J)*, являющихся, в частности, следующими:

$$\varphi_1 : U \times V \times E \to R,\ \varphi_2 : U \times V \to E\ \varphi_3 : U \times V \times E \times R \to \Phi. \tag{4}$$

Множества *{U}, {V}* и *{R}* могут включать в зависимости от конкретной решаемой задачи различные сочетания показателей функционирования материально технического обеспечения, формируемые, например, из следующего набора характеристик: *{B}; Ь=1* — это стоимость содержания запасов; *Ь=2* — ожидаемый средний объем дефицита; *Ь=3* — ожидаемый средний объем сверхнормативных запасов; *Ь=4* — издержки доставки поставок; *Ь=5* — задолженность по поставкам ресурсов; Ь = 6 — норма страхового запаса; *Ь=7* — норма максимального запаса; *Ь=8* — норма заказа (пороговый уровень запаса для заявки на пополнение); *Ь=9* — норма снабжения материалами и др.

Критериями *{E}* при этом могут быть следующие показатели: стоимость содержания запасов в материально техническом обеспечении при *e=1;* приведенная обеспеченность ресурсами потребителей, при *e=2*- надежность снабжения потребителей, при e=3 и др.

Решение задач, определяемое отображением $\{\varphi\}$, осуществляется на моделях функционирования системы материально технического обеспечения. Эти модели представляют собой концептуальное описание состава, структуры, функций и процессов функционирования в виде (5)

$$m = \langle S, \{P\}, \{W\}, \{\mathrm{L}\}, \{\mathrm{H}\}, \{\mathrm{J}\}, \{\Phi\}, \mathrm{Q}, \mathrm{G}, \{\varphi\}\rangle \tag{5}$$

где *S* — структура (одноэшелонная или многоэшелонная) система материально технического обеспечения; *{P}* — множество подразделений, складов, баз; {W}—множество запасов ресурсов (страховых, текущих и др.); *{L}* — множество обеспечиваемых систем внешних потребителей ресурсами; *{H}* — множество номенклатур (марок) ресурсов; *{J}* — множество типов функций хранения, наполнения, расходования, выполняемых системой материально технического обеспечения; *{Ф;}* — множество функций *i*-го типа, выполняемых системой; *Q* — процесс функционирования системы; *G* — стратегия управления запасами в системе материально технического обеспечения; {**φ**} — множество нормообразующих факторов модели.

Концептуальная модель $M_к$ отображением $F^{км}$ преобразуется в математическую модель $M_м$. Модель $M_м$ задает структуру, состав и взаимосвязи типовых модельных компонентов, реализованных в составе автоматизированной системы моделирования задач *{3}* и моделей *{M},* в виде (6):

$$M = \langle \{\Delta\}, \{T\}, Z, \{X\}, \{Y\}, \{\mathrm{J}\}, \{\varphi\}\rangle \tag{6}$$

где {Δ} — множество модельных компонентов, поддерживающих задачи *{3}* и модели *{M}; {T}* — множество моментов времени, которые характеризуют процессы, описываемые модельными компонентами; *Z* — пространство состояния модельных компонентов; *{X}, {Y}* — множества входных и выходных переменных модельных компонентов соответственно; *{J}* — множество типов отображений между компонентами модели; *{φ}* — множество отображений *j*-го типа между компонентами модели *M,* в частности, имеющими вид (7):

$$\varphi_1 : \{\mathrm{T}\}\times\{\mathrm{Z}\}\times\{\mathrm{Y}\} \to \{\square\} \quad \varphi_2 : \{\mathrm{T}\}\times\{X\}\times\{\mathrm{Y}\} \to Z \quad , \varphi_3 : \{\mathrm{T}\}\times\{X\}\times Z \to \{Y\}. \tag{7}$$

Анализ существующих моделей и задач управления запасами, используемых в практике анализа и нормирования процессов, позволяет сделать вывод о необходимости построения АСУ на основе единой математической схемы.

Очевидно, что общее число ограничений на потребляемые ресурсы не превышает произведения рассматриваемого числа ресурсов на количество регионов. Общее число неизвестных — это произведение числа всех размещаемых предприятий на число регионов. Известно, что при планировании выпуска и потребления материальных ресурсов достигается баланс в регионально не увязанной системе отраслевого планирования. И тем не менее распределение ресурсов по регионам (базам) может оказаться настолько нерациональным, что не окажется ни одного набора величин h_{kn}, удовлетворяющего условиям выше сформированной задачи.

Заключение. Таким образом использование проблемно ориентированного подхода при создании АСУ позволяет снизить трудоемкость ее разработки и реализации, обеспечить возможность с единых методологических позиций унифицировать не только алгоритмы решения задач, но и применить стандартные методы обработки результатов решения задач.

Качественное исследование системы материально технического обеспечения основывается на создании проблемно-ориентированных автоматизированных систем. Для их разработки наиболее целесообразно использовать модельно ориентированный подход, позволяющий снизить трудоемкость разработки и реализации ее концептуальной, математической и алгоритмической моделей. Построение концептуальной модели в виде сети фреймов обеспечивает применение стандартных средств общения с пользователем системы и снижает требования к их квалификации.

При создании математической модели наиболее целесообразно выбрать представление процессов материально технического обеспечения в виде систем с типовой математической схемой.

СПИСОК ЛИТЕРАТУРЫ

1. Голоскоков К. П. Прогнозирование и оценка технического состояния сложных систем // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. 2008. № 1 (53). С. 164-168.
2. Малюк В. И., Голоскоков К. П. Методика оценки рационального распределения ограниченных инвестиций в развитие производственной системы региона // Вестник ИНЖЭКОНа. Серия: Экономика. 2009. № 1 (28). С. 51-60.
3. Брусакова И. А., Власов М. П., Голоскоков К. П Информационные технологии в научных исследованиях высшей школы : монография. Санкт-Петербург, 2012.
4. Голоскоков К. П Автоматизированная система испытаний в структуре системы управления качеством // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2008. № 6 (69). С. 116-120.
5. Голоскоков К. П. Прогнозирование и оценка технического состояния сложных систем // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. 2008. № 1 (53). С. 164-168.

6. Голоскоков К. П., Нестеренко Н. К., Чиркова М. Ю. Повышение эффективности деятельности производственного предприятия // Аудит и финансовый анализ. 2014. № 1. С. 331-335.
7. Брусакова И. А., Голоскоков К. П. Математическая модель функциональной надежности автоматизированных систем управления // Вестник ИНЖЭКОНа. Серия: Технические науки. 2010. № 8. С. 48-51.
8. Голоскоков К. П., Железняк М. В Прогнозирование с применением теории распознавания образов // Вестник ИНЖЭКОНа. Серия: Технические науки. 2011. № 8. С. 114-118.
9. Goloskokov K., Korotkov V., Marley V., Knysh T. Assessment of technical means quality indicators for smart transport systems // Journal of Physics: Conference Seriesthis link is disabled, 2021. 2096(1), 012184.
10. Goloskokov, K., Korotkov, V., Marley, V., Knysh, T. Improving reliability of smart transport systems // Journal of Physics: Conference Seriesthis link is disabled, 2021, 2096(1), 012183
11. Goloskokov K., Korotkov V., Marley V., Knysh T. Modeling of intelligent transport systems maintenance processes // Journal of Physics: Conference Seriesthis link is disabled, 2021. 2061(1), 012126.
12. Goloskokov K., Korotkov V., Nyrkov A., Knysh T. Error correction algorithms in on-board intelligent transport data transmission systems//Journal of Physics: Conference Seriesthis link is disabled, 2021, 2061(1), 012097.
13. Goloskokov K., Korotkov V., Gaskarov V., Knysh T. Methods of formalized quality assessment of intelligent transport systems // Journal of Physics: Conference Seriesthis link is disabled, 2021. 2061(1), 012125.
14. Shipunov I. S., Nyrkov A. P., Ryabenkov M. U., Morozova E. V., Goloskokov K. P. Investigation of Computer Incidents as an Important Component in the Security of Maritime Transportation // Proceedings of the IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2021, 2021. 9396501. С. 657–660.

УДК 681.5

ОПТИМИЗАЦИЯ РЕСУРСОПОТОКОВ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ УПРАВЛЕНИЯ

Голоскоков Константин Петрович, Астапкович Алексей Александрович, Коротков Виталий Валерьевич
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург,198035, Россия
e-mails: goloskokovkp@gumrf.ru, kaf_koib@gumrf.ru, korotkovvv@gumrf.ru

Аннотация. В статье решена задача взаимодействия и взаимосвязей, оптимизации ресурсопотоков, повышение эффективности принятия управленческих решений. Показано, что моделирование потоков ресурсов предусматривает корректировку путем итеративного перераспределения межрегиональных и внутри региональных поставок по поставщикам и потребителям.

Ключевые слова: математическая модель; автоматизированная система; транспортно-технологический процесс; модельно-ориентированный подход; объект; эффективность.

OPTIMIZATION OF RESOURCE FLOWS IN AUTOMATED CONTROL SYSTEM

Goloskokov Konstantin, Astapkovich Alexey, Korotkov Vitaly
Admiral S.O. Makarov state university of marine and river fleet
5/7 Dvinskaya st., St. Petersburg,198035, Russia
e-mails: goloskokovkp@gumrf.ru, kaf_koib@gumrf.ru, korotkovvv@gumrf.ru

Abstract. The article solves the problem of interaction and interconnections, optimization of resource flows, increasing the efficiency of managerial decision-making. it is shown that modeling of resource flows provides for adjustment by iterative redistribution of interregional and intra-regional rates by suppliers and consumers

Keywords: mathematical model; automated system; transport and technological process; model-oriented approach; object; efficiency.

Введение. Совмещение номенклатурных позиций в одну поставку ведет к экономии издержек формирования запасов за счет уменьшения числа заказов. Для создания эффективных АСУ необходимо подробно исследовать первичный объект - непосредственно систему материально- технического обеспечения [1-4]. Создание прикладного математического и программного обеспечения является перспективным направлением решения этой проблемы и развития его как системы автоматизированного моделирования [5-7]. В связи с этим при создании таких АСУ наиболее целесообразно использовать модельно-ориентированный подход, который основывается на принципах системного анализа, стандартизации, классификации и модульности [8-10]. Таким образом, показано, что использование проблемно-ориентированного подхода к созданию автоматизированной системы моделирования позволяет снизить трудоемкость ее разработки и реализации [11], обеспечить возможность унифицировать алгоритмы решения задачи [12, 13], но и применить стандартные методы обработки результатов экспериментов [11, 14, 15].

При создании, автоматизированной системы наиболее целесообразно использовать представление объекта исследования в виде линейных систем [16, 17].

Агрегат, выбранный в качестве моделирующего объекта, имеет динамический характер, наглядно представляет структурные и временные особенности, описывает обмен сигналами с внешней средой и учитывает воздействие случайных факторов. Выделенные и стандартизованные объекты и процессы системы материально технического обеспечения, заданные в виде типовых математических компонент, представляют собой простейшие линейные системы,

которые при построении моделей процессов материально технического обеспечения вместе могут образовывать новые, более сложные линейные системы [4].

С помощью типовых математических компонент задаются такие типовые элементы системы материально технического обеспечения, как запас, спрос, пополнение запасов, заказ на пополнение и др. Кроме того, типовые математические компоненты обеспечивают построение блоков анализа и оптимизацию параметров моделей, расчет критериев оптимизации и ограничений, а также организацию итеративного поиска оптимальных значений параметров при решении задач [18-20].

Для построения из типовых математических компонент моделей реальных систем материально технического обеспечения и постановки на них задач анализа и нормирования технико-экономических показателей разрабатывается комплекс конструктивных параметров. С помощью конструктивных параметров выполняется настройка типовых математических компонент на конкретную математическую модель. Настройка может заключаться, например, в выборе стратегий пополнения запасов ресурсов, планировании отгрузки ресурсов, управлении запасами ресурсов, а также в выборе критериев оптимизации и ограничений, определении набора исследуемых и нормируемых технико-экономических показателей процессов материально технического обеспечения. Помимо этого, с помощью конструктивных параметров определяются связи между отдельными типовыми математическими компонентами. Учет связей между типовыми математическими компонентами, направлений передачи сигналов и видов сигналов проводится с помощью предикатов, задающих оси выдачи и приема входных (или управляющих) сигналов.

Проанализируем, следующим образом, систему ограничений. Пусть g — некоторый вектор оценок «транспортабельности» ресурсов, и оценки эти тем выше, чем больше затраты на перемещение ресурсов из одного региона в другой (из одной базы на другую). Запишем значения критерия W в виде (1)

$$W = g\sum_{n}(R^{n} - \sum_{k} P^{k} h_{kn}), \tag{1}$$

Отсюда вытекает, что минимум потерь за счет межрегиональных поставок материальных ресурсов достигается при (2)

$$R^{n} < \sum_{k} P^{k} h_{kn}), \tag{2}$$

Если имеется несовместимость ограничений, она легко выявляется решением задачи с критерием. Несовместимость означает, что при спланированном распределении ресурсов по совокупности регионов рассчитанный ранее хозяйственный план не может быть реализован. В этом случае необходимо осуществить очередную итерацию межрегионального перераспределения ресурсов с учетом некоторого возрастания затрат. При использовании итеративных методов решения задачи несовместимость ограничений выразится в том, что оценки некоторых ресурсов в одних регионах будут возрастать до бесконечности, а в других - принимать нулевые значения. Исходя из этого, можно организовать итеративный процесс перераспределения материальных ресурсов, изменяя величины R^n и минимизируя хозяйственные потери от межрегиональных поставок ресурсов. Проведение ряда итераций приведет к совместимости ограничений задачи, что гарантируется сбалансированностью регионально не увязанной системы оптимальных отраслевых планов производства. Повторяя решение задачи для различных векторов оценок g, можно получить несколько вариантов R^n, а, следовательно, разные направления перераспределения и поставок ресурсов.

Издержки при поставках по маршруту ss' для v-го ресурса примут следующий вид (3, 4):

$$f_{ss}(q_{ss}) = \mu_{ss}\delta_{ss} + (C_{ss} + E\, l_v \Theta_{ss}) q_{ss} \tag{3}$$

где μ_{ss}— издержки организации поставки;

$$\delta_{ss} = \begin{cases} 1, при & q_{ss} > 0 \\ 0, при & q_{ss} = 0 \end{cases} \tag{4}$$

где C_{ss}—удельные издержки реализации поставки по маршруту ss'; l_v — цена единицы v-го ресурса, Θ_{ss} — время реализации поставки; q_{ss}— величина транспортируемой партии ресурса.

На основе детального анализа специфики проблемной области моделирования АСУ осуществляется классификация и упорядочение понятий, объектов, процессов, функций и структур материально-технического обеспечения. Кроме того, систематизируются, обобщаются и разбиваются на классы уже существующие и вновь разработанные задачи анализа и нормирования технических показателей процессов материально-технического обеспечения, а также модели функционирования материально-технического обеспечения, обеспечивающие решение этих задач.

Заключение. Таким образом, использование проблемно ориентированного подхода при создании АСУ позволяет снизить трудоемкость ее разработки и реализации, обеспечить возможность с единых методологических позиций унифицировать не только алгоритмы решения задач, но и применить стандартные методы обработки результатов решения задач.

Анализ существующих моделей и задач управления запасами, используемых в практике анализа и нормирования процессов, позволяет сделать вывод о необходимости построения АСУ на основе единой математической схемы.

Очевидно, что общее число ограничений на потребляемые ресурсы не превышает произведения рассматриваемого числа ресурсов на количество регионов. Общее число неизвестных - это произведение числа всех размещаемых предприятий на число регионов. Известно, что при планировании выпуска и потребления материальных ресурсов достигается баланс в регионально не увязанной системе отраслевого планирования. И тем не менее распределение ресурсов по регионам (базам) может оказаться настолько нерациональным, что не окажется ни одного набора величин h_{kn}, удовлетворяющего условиям выше сформированной задачи.

Качественное исследование системы материально технического обеспечения основывается на создании проблемно-ориентированных автоматизированных систем [21-24]. Для их разработки наиболее целесообразно использовать модельно ориентированный подход, позволяющий снизить трудоемкость разработки и реализации ее концептуальной, математической и алгоритмической моделей [25, 26]. Построение концептуальной модели в виде сети фреймов обеспечивает применение стандартных средств общения с пользователем системы и снижает требования к их квалификации.

При создании математической модели наиболее целесообразно выбрать представление процессов материально технического обеспечения в виде систем с типовой математической схемой.

СПИСОК ЛИТЕРАТУРЫ

1. Голоскоков К. П., Нестеренко Н. К., Чиркова М. Ю. Повышение эффективности деятельности производственного предприятия // Аудит и финансовый анализ. 2014. № 1. С. 331-335.
2. Малюк В. И., Голоскоков К. П. Методика оценки рационального распределения ограниченных инвестиций в развитие производственной системы региона // Вестник ИНЖЭКОНа. 2009. № 1 (28). С. 51-60. (Экономика).
3. Ныркова А. П., Дмитриева Т. В., Соколов С. С. Методы повышения эффективности работы портов в рамках международных транспортных коридоров // Речной транспорт (XXI век). 2009. № 6 (42). С. 75–77.
4. Голоскоков К. П. Прогнозирование и оценка технического состояния сложных систем // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. 2008. № 1 (53). С. 164-168.
5. Люльченко А. Н., Ныркова А. П., Швед В. Г. Модель системы обеспечения информационной безопасности на транспорте // Вестник государственного университета морского и речного флота имени адмирала С. О. Макарова, 2015. № 5 (33). С. 184-193.
6. Ныркова А. П., Дмитриева Т. В. Математическая модель резервирующей системы и оптимизация ее работы // Журнал университета водных коммуникаций. 2011. № 2. С. 98–101.
7. Брусакова И. А., Голоскоков К. П. Математическая модель функциональной надежности автоматизированных систем управления // Вестник ИНЖЭКОНа. 2010. № 8. С. 48-51. (Технические науки).
8. Ныркова А. П., Каторин Ю. Ф., Соколов С. С., Ежгуров В. Н. Основные принципы построения защищенных информационных систем автоматизированного управления транспортно-логистическим комплексом // Проблемы информационной безопасности. Компьютерные системы. 2013. № 2. С. 54–58.
9. Федоровская Н. К., Федоровский К. Ю. Оценка эффективности систем охлаждения судовых энергетических установок с учетом экологического фактора // Вестник государственного университета морского и речного флота им. адмирала С. О. Макарова. 2021. Т. 13. № 4. С. 559-568.
10. Ныркова А. П., Соколов С. С., Башмаков А. В. Методика проектирования безопасных информационных систем на транспорте // Проблемы информационной безопасности. Компьютерные системы. 2010. № 3. С. 58–61.
11. Брусакова И. А., Власов М. П., Голоскоков К. П. Информационные технологии в научных исследованиях высшей школы. СПб, 2012. 160 с.
12. Галин А. В., Кузнецов А. Л., Валькова С. С., Сампиев А. М. Расчет вместимости склада навалочных грузов морского порта с помощью имитационного моделирования // Вестник АГТУ. Астрахань, 2022. № 3. С. 82-89. (Морская техника и технология).
13. Ныркова А. П., Караваев В. И., Багаева Н. Г., Караваева Е. Д., Соколов С. С. Алгоритмы автоматизированного управления технологическими процессами мультимодальных перевозок // Журнал университета водных коммуникаций. 2010. № 4. С. 43–53.
14. Галин А. В., Кузнецов А. Л., Валькова С. С., Сампиев А. М. Технологическая трансформация универсальных причалов в малые контейнерные терминалы //Транспортное дело России. Москва, 2022. № 2 (159). С. 243-249.
15. Галин А. В., Слицан А. Е., Виноградова Э. В. Особенности определения количества погруженного груза на судах типа река-море // Транспортное дело России. Москва, 2022. № 3 (160). С. 124-126.
16. Ныркова А. П., Соколов С. С., Шнуренко А. А. Автоматизированное управление транспортными системами: монография // СПб.: ГУМРФ имени адмирала С. О. Макарова, 2013. 325 с.
17. Ныркова А. П. Автоматизированная система подготовки исходных данных для пакета программ ЛП АСУ // Применение средств вычислительной техники в задачах контроля и управления : сб. науч. тр. Л.: ЛИВТ, 1990. С. 103–106.
18. Mathematical Models for Solving Problems of Reliability Maritime System / A. Nyrkov, K. Goloskokov, E. Koroleva, S. Sokolov [et al] // Lecture Notes in Electrical Engineering. 442, 2018. Pp. 387-394. https://doi.org/10.1007/978-981-10-4762-6_37.
19. Ныркова А. А., Ныркова А. П. Автоматизация информационного обеспечения деятельности исследовательской проблемной лаборатории // Управление транспортными системами : сб. науч. тр. СПб.: СПГУВК, 1997. С. 98–99.
20. Галин А. В., Слицан А. Е. Развитие сборных отправок грузов в ситуации роста стоимости контейнерных перевозок // Транспортное дело России. 2022. № 3 (160). С. 117-119.
21. Goloskokov K., Korotkov V., Marley V., Knysh T. Assessment of technical means quality indicators for smart transport systems // Journal of Physics: Conference Seriesthis link is disabled, 2021. 2096(1), 012184.
22. Нечеткие модели и системы управления / Кудинов Ю. И. [и др]. М. : Ленанд, 2017. 328 с.
23. Ныркова А. П., Ныркова А. А., Соколов С. С., Шнуренко А. А. Обеспечение безопасности объектов информатизации транспортной отрасли / под ред. А. П. Ныркова. СПб.: Изд-во Политехн. ун-та, 2015. 544 с.
24. Голоскоков К. П Автоматизированная система испытаний в структуре системы управления качеством // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2008. № 6 (69). С. 116-120.
25. Sokolov S., Zhilenkov A., Chernyi S., Nyrkov A., Mamunts D. Dynamics Models of Synchronized Piecewise Linear Discrete Chaotic Systems of High Order // Symmetry, 2019. № 11(2). 236. https://doi.org/10.3390/sym11020236.
26. Голоскоков К. П., Железняк М. В Прогнозирование с применением теории распознавания образов // Вестник ИНЖЭКОНа. 2011. № 8. С. 114-118. (Технические науки).

УДК 004.942

РАСЧЕТ ПАРАМЕТРОВ ДВИЖЕНИЯ БЕЗЭКИПАЖНОГО СУДНА В ПРОГРАММНОЙ СРЕДЕ MAPLE 12

Данилин Герман Владиславович, Соколов Сергей Сергеевич
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: t.101@mail.ru, sokolovss@gumrf.ru

Аннотация. Математическая модель движения судна призвана дать возможность вычислить значения 3-х пространственных координат центра масс судна, а также 3-х углов, описывающих положение судна в пространстве: угла крена, дифферента и курсового угла. Данная работа посвящена реализации в программной среде Maple 12 математической модели движения судна, предложенной А.М. Басиным, с целью расчета таких параметров движения судна, как координаты его центра масс, курсовой угол и угол дрейфа, угловая и линейная скорость.

Ключевые слова: безэкипажное судно; математическая модель; модель Басина; Maple; расчет координат.

CALCULATION OF THE PARAMETERS OF THE MOVEMENT OF AN UNMANNED VESSEL IN THE MAPLE 12 SOFTWARE ENVIRONMENT

Danilin German, Sokolov Sergey
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya str., St. Petersburg, 198035, Russia
e-mails: t.101@mail.ru, sokolovss@gumrf.ru

Abstract. The mathematical model of the vessel's motion is designed to make it possible to calculate the values of 3 spatial coordinates of the center of mass of the vessel, as well as 3 angles describing the position of the vessel in space: the angle of roll, trim and heading angle. This work is devoted to the implementation in the Maple 12 software environment of a mathematical model of ship movement proposed by A.M. Basin, in order to calculate such parameters of ship movement as the coordinates of its center of mass, heading angle and drift angle, angular and linear velocity.

Keywords: unmanned vessel; mathematical model; Basin model; Maple; coordinate calculation.

Введение. Математическая модель движения судна [1-3] призвана дать возможность вычислить значения 3-х пространственных координат центра масс судна, а также 3-х углов, описывающих положение судна в пространстве: угла крена, дифферента и курсового угла.

$$\left.\begin{aligned}
&\frac{dx_0}{dt} = v\cos(q-\beta);\\
&\frac{dy_0}{dt} = v\sin(q-\beta);\\
&\frac{dq}{dt} = w;\\
&\frac{dv}{dt} = -vw\sin\beta\cos\beta\left(\frac{1}{1+k_{11}} - \frac{1}{1+k_{22}}\right) - \frac{(\sum_i F_{yi})\sin\beta}{(1+k_{22})\,pV} + \frac{(\sum_i F_{xi})\cos\beta}{(1+k_{11})\,pV};\\
&\frac{d\beta}{dt} = w\left(\frac{(\sin\beta)^2}{1+k_{11}} + \frac{(\cos\beta)^2}{1+k_{22}}\right) - \frac{(\sum_i F_{xi})\sin\beta}{(1+k_{11})\,pVv} - \frac{(\sum_i F_{yi})\cos\beta}{(1+k_{22})\,pVv};\\
&\frac{dw}{dt} = \frac{\sum_i M_i}{(1+k_{66})I_z};\\
&\sum_i F_{xi}(t,C,v(t),w(t),\beta(t),x_0(t),y_0(t),q(t),U(t),L(t),E(t)) = X_в + X_р + T_E + X_{внеш};\\
&\sum_i F_{yi}(t,C,v(t),w(t),\beta(t),x_0(t),y_0(t),q(t),U(t),L(t),E(t)) = Y_в + Y_р + T_{ПУ} + Y_{внеш};\\
&\sum_i M_i(t,C,v(t),w(t),\beta(t),x_0(t),y_0(t),q(t),U(t),L(t),E(t)) = M_в + M_р + M_{ПУ} + M_{внеш};
\end{aligned}\right\} \quad (1)$$

Из-за того, что часто изменение осадки, угла крена и угла дифферента невелико, авторы моделей переходят к рассмотрению плоскопараллельного движения судна.

Большинство авторов предпочитает использовать для описания модели характеристики, являющиеся производными координат и курсового угла: линейную скорость v, угловую скорость w и угол дрейфа β. Тем самым авторы используют две системы координат одновременно: подвижную, и неподвижную.

При таком подходе любая математическая модель движения судна сокращенно описывается при помощи набора основных формул (1), а отличает модели друг от друга то, как их авторы вычисляют силы и коэффициенты, задействованные в основных формулах.

Реализация модели Басина в Maple. В рамках данной работы проводился вычислительный эксперимент по расчету координат центра масс судна, а также его курсового угла, угла дрейфа, угловой и линейной скорости при помощи модели, описывающей движение судна, предложенной А.М. Басиным.

Поскольку все искомые величины являются результатами вычислений дифференциальных уравнений, в первую очередь было необходимо вычислить промежуточные величины. В результате произведенных вычислений стало возможным вычислить значения дифференциальных уравнений, определяющих искомые величины. Демонстрация вычислений представлена на рис. 1 и 2.

$$Y[\text{в}] := -C[\text{уг}]\cdot\frac{p\cdot v^2\cdot A[Lsigma]}{2};\#\text{поперечное вязкостное сопротивление на корпусе судна}$$

$$-9.395$$

if $Ul \le 4$ **then** $G := -1.3\,Ul + 7.8 + 0.01792\left(\frac{L}{B}\right)^2 - 0.1275\left(\frac{L}{B}\right) + 6.113$ **elif** $Ul > 4$ **then** $G := -1.3\,Ul + 7.8 + 0.02333\left(\frac{L}{B}\right)^2 - 0.045\left(\frac{L}{B}\right) + 1.187$ **end if**;

 # Значение коэффициента G определяется в зависимости от полученного на предыдущем шаге значения Ul

$$-22.71$$

$$m[1] := \left(\left(-0.1317\left(\frac{d}{L}\right)^2 + 0.05358\left(\frac{d}{L}\right) + 0.000181\right)G + \left(-2.361\left(\frac{d}{L}\right)^2 + 0.8653\left(\frac{d}{L}\right) - 0.000161\right)\right)K[bm];\ \#\ \text{Коэффициент одной из составляющих позиционного момента}$$

$$-0.01326$$

$$m[2] := \left(-\frac{\ln(1.023\,\sigma)}{11.6 - 9.29}\right)K[bm];\#\ \text{Коэффициент одной из составляющих позиционного момента}$$

$$0.003259$$

$$C[Wm] := \left(0.739 + \frac{8.7\,d}{L}\right)\left(1.611\sigma^2 - 2.873\,\sigma + 1.33\right)K[Wm];\ \#\ \text{Коэффициент демпфирующего момента}$$

$$0.9726$$

$$wr := \frac{w\cdot L}{v};\#\text{относительная (безразмерная) угловая скорость судна}$$

$$0.$$

$$C[mz] := evalf(m[1]\cdot\sin(2\cdot Bet) + m[2]\cdot\sin(Bet) - C[Wm]wr);\ \#\ \text{Безразмерный момент сопротивления на корпусе}$$

$$-0.01559$$

$$M[\text{в}] := C[mz]\cdot\frac{p\cdot v^2\cdot A[Lsigma]}{2};\#\text{момент сил вязкостного сопротивления на корпусе судна}$$

$$-9.160$$

$$sum(F[x\,i], i = 1..N) := X[\text{в}] + X[\text{р}] + T[E] + X[\text{внеш}];\#\text{сумма сил, направленных вдоль оси x, кН}$$

$$-200.3$$

$$sum(F[y\,i], i = 1..N) := Y[\text{в}] + Y[\text{р}] + TПУ + Y[\text{внеш}];\#\text{сумма сил, направленных вдоль оси y, кН}$$

$$56.00$$

$$sum(M[i], i = 1..N) := M[\text{в}] + M[\text{р}] + МПУ + M[\text{внеш}];\#\text{сумма моментов сил, вращающих судно (в общем виде), кН*м}$$

$$-5.679\,10^5$$

Рис. 1. Вычисление сумм сил, действующих на корпус судна

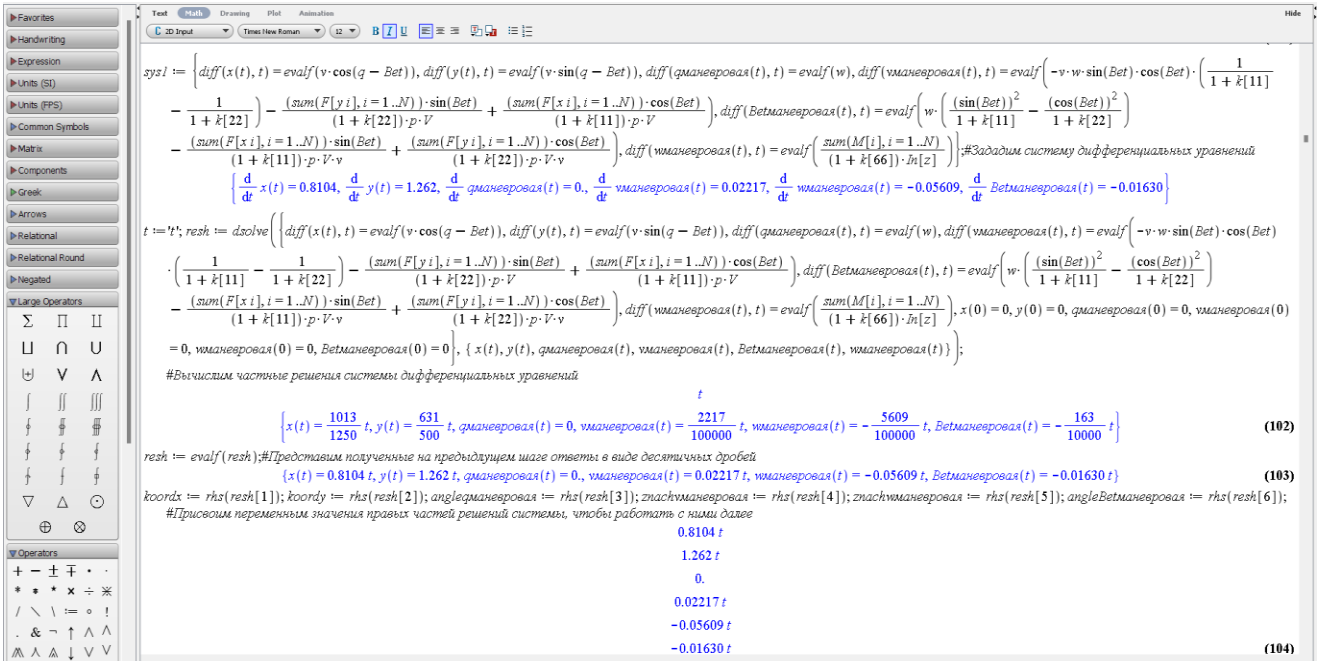


Рис. 2. Вычисление координат центра масс судна и его курсового угла

На следующем шаге изначальный алгоритм вычисления был записан в цикл, осуществляющий 60 итераций. Результаты вычислений, полученные на каждой итерации, вносились в соответствующие массивы.

Заключение. В результате произведенных вычислений были сформированы массивы данных, на основании которых были построены графики, наглядно отображающие изменение рассчитываемых величин. В дальнейшем планируется проведение работ по доработке модели А.М. Басина, в частности, по вычислению возможных координат габаритной точки судна, наиболее удаленной от его центра масс.

СПИСОК ЛИТЕРАТУРЫ

1. Юдин Ю. И., Сотников И. И. Математические модели плоскопараллельного движения судна. Классификация и критический анализ // Вестник МГТУ. Труды Мурманского государственного технического университета. 2006. Т. 9. № 2. С. 200-208. EDN ICJVHH.
2. Буцанец А. А. Разработка предложений по типовой структуре системы дистанционного управления беспилотным техническим флотом // Транспортное дело России. 2019. № 4. С. 100-103. EDN YWDGXB.
3. Данилин Г. В., Соколов С. С. Исследование математических моделей движения судна и технологий безэкипажного судовождения // Сборник научных статей национальной научно-практической конференции профессорско-преподавательского состава ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова», Санкт-Петербург, 19–21сентября 2022 г. Т. 1. СПб. : Федеральное государственное бюджетное образовательное учреждение высшего образования Государственный университет морского и речного флота им. адмирала С. О. Макарова, 2022. С. 72-78. EDN JNGEEK.

УДК 004.942

ПОИСК КООРДИНАТ ГАБАРИТНОЙ ТОЧКИ, НАИБОЛЕЕ УДАЛЕННОЙ ОТ ЦЕНТРА МАСС, КАК ОДНОГО ИЗ КЛЮЧЕВЫХ ПАРАМЕТРОВ РАСЧЕТА ТРАЕКТОРИИ ДВИЖЕНИЯ АВТОНОМНОГО СУДНА

Данилин Герман Владиславович, Соколов Сергей Сергеевич
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: t.101@mail.ru, sokolovss@gumrf.ru

Аннотация. Большинство, существующих на сегодня, математических моделей движения судна позволяют вычислить координаты только центра масс судна, чего может быть недостаточно для расчета параметров движения судна в узкостях. Это, в свою очередь, накладывает ограничения на создание универсальной математической модели движения судна. В данной работе рассматривается система формул для проведения расчета координат габаритной точки судна, наиболее удаленной от центра его масс, которая сможет быть использована при разработке математической модели движения судна, пригодной для проведения судна в узкостях, а также проводится расчет, на основании которого строятся графики, наглядно отображающие коридоры изменения рассчитываемых значений.

Ключевые слова: безэкипажное судно; математическая модель; модель Басина; Maple; расчет координат.

SEARCH FOR THE COORDINATES OF THE DIMENSIONAL POINT FURTHEST FROM THE CENTER OF MASS AS ONE OF THE KEY PARAMETERS FOR CALCULATING THE TRAJECTORY OF AN AUTONOMOUS VESSEL

Danilin German, Sokolov Sergey
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya str., St. Petersburg, 198035, Russia
e-mails: t.101@mail.ru, sokolovss@gumrf.ru

Abstract. Most of the mathematical models of ship movement that exist today allow us to calculate the coordinates of only the center of mass of the ship, which may not be enough to calculate the parameters of ship movement in narrow spaces. This, in turn, imposes restrictions on the creation of a universal mathematical model of ship movement. In this paper, we consider a system of formulas for calculating the coordinates of the overall point of the vessel, the most distant from the center of its mass, which can be used in the development of a mathematical model of the vessel's movement, suitable for carrying out the vessel in narrowness, and also a calculation is carried out, on the basis of which graphs are constructed, visually displaying the corridors of changes in the calculated values.

Keywords: unmanned vessel; mathematical model; Basin model; Maple; coordinate calculation.

Введение. В значительной части известных математических моделей движения судна [1-3] осуществляется расчёт значений координат центра масс судна и его курсового угла. Но судно не является материальной точкой, и этот факт требует учёта при прохождении судна в условиях ограниченного пространства, например в канале или проливе, а также при расхождении с другими судами. Поэтому в рамках данной работы реализованная в программной среде «Maple 12» математическая модель движения судна А.М. Басина была дополнена формулами (1), позволяющими определить координаты габаритной точки судна, наиболее удаленные от центра его масс.

$$\left.\begin{aligned} x_л &= x - (L_{\max}\cos\beta + B_{\max}\sin\beta); \\ x_п &= x + (L_{\max}\cos\beta + B_{\max}\sin\beta); \\ y_л &= y - (L_{\max}\sin\beta + B_{\max}\cos\beta); \\ y_п &= y + (L_{\max}\sin\beta + B_{\max}\cos\beta); \end{aligned}\right\} \quad (1)$$

Реализация дополнений модели Басина в Maple. В рамках работы по реализации модели А.М. Басина в Maple проводился вычислительный эксперимент по расчету координат центра масс судна, а также его курсового угла, угла дрейфа, угловой и линейной скорости при помощи модели. На следующем шаге изначальный алгоритм вычисления был записан в цикл, осуществляющий 60 итераций. Результаты вычислений, полученные на каждой итерации, вносились в соответствующие массивы. В рамках данной работы были сформированы 4 новых массива, в которые вносились данные с учетом дополнений, вносимых формулами (1). Демонстрация примера на рис. 1.

```
139.0
for i from 0 to 59 do Gl1[i] := G[i] - (L·sin(Bet) + B·cos(Bet)) end do;#Вычислим возможные координаты габаритных точек судна слева от оси Y
-19.23
-17.96
-17.96
-17.96
-17.96
-17.96
-17.96
-17.96
-17.96
-17.96
-17.96
-17.96
-17.96
-17.96
```

Рис. 1. Вычисление координат габаритных точек судна

В результате были получены 4 массива с координатами местоположения габаритных точек судна в дополнение к массивам координат его центра масс. По данным, хранимым в массивах, построены наглядные графики, представленные на рис. 2 и 3.

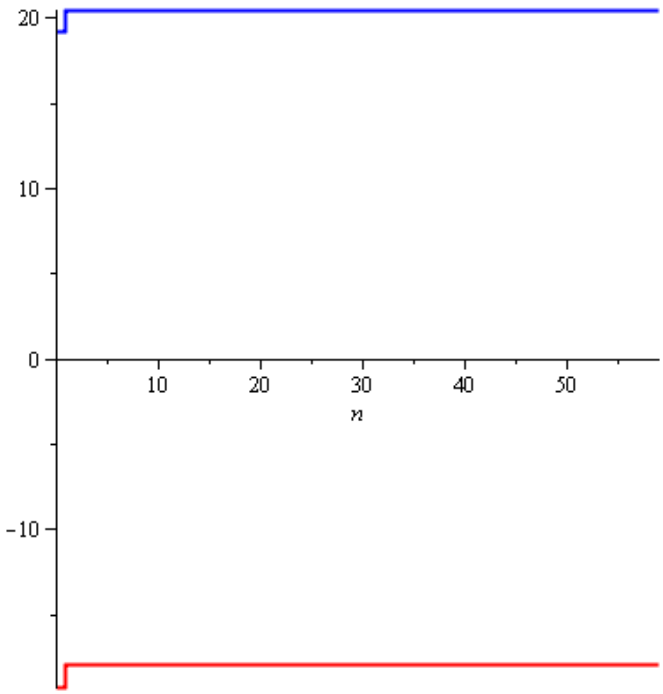


Рис. 2. Построение коридора значений координат Y габаритных точек судна

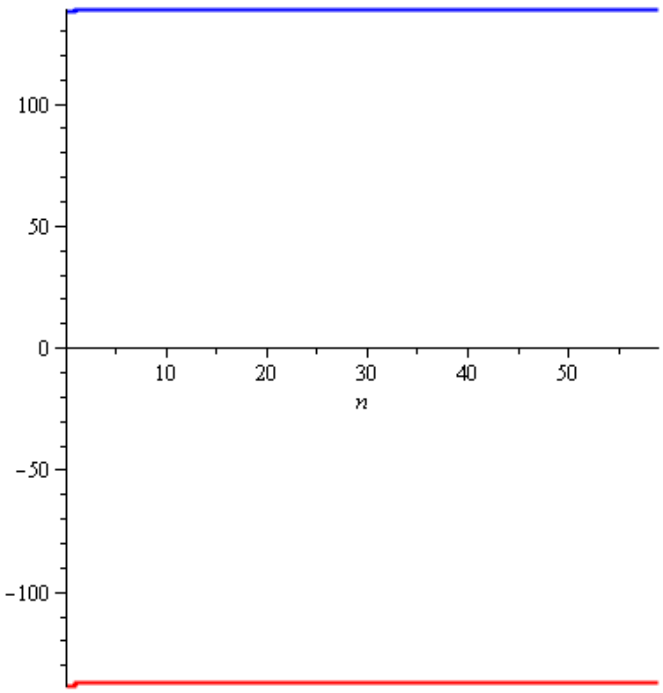


Рис. 3. Построение коридора значений координат X габаритных точек судна

Заключение. В результате произведенных вычислений были сформированы массивы данных, на основании которых были построены графики, наглядно отображающие коридоры изменения координат выступающих за центр масс габаритных точек судна. Дополнительных исследований требует вопрос возможности повышения точности модели А. М. Басина.

СПИСОК ЛИТЕРАТУРЫ

1. Юдин Ю. И., Сотников И. И. Математические модели плоскопараллельного движения судна. Классификация и критический анализ // Вестник МГТУ. Труды Мурманского государственного технического университета. 2006. Т. 9. № 2. С. 200-208. EDN ICJVHH.
2. Буцанец А. А. Разработка предложений по типовой структуре системы дистанционного управления беспилотным техническим флотом // Транспортное дело России. 2019. № 4. С. 100-103. EDN YWDGXB.
3. Данилин Г. В., Соколов С. С. Исследование математических моделей движения судна и технологий безэкипажного судовождения // Сборник научных статей национальной научно-практической конференции профессорско-преподавательского состава ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова», Санкт-Петербург, 19–21 сентября 2022 г. Т. 1. СПб. : Федеральное государственное бюджетное образовательное учреждение высшего образования Государственный университет морского и речного флота им. адмирала С. О. Макарова, 2022. С. 72-78. EDN JNGEEK.

УДК 681.5, 004.9

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПОИСКА АВАРИЙНЫХ РАЗЛИВОВ НЕФТИ И НЕФТЕПРОДУКТОВ ГРУППОЙ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Егорова Кристина Вадимовна, Соколов Сергей Сергеевич
Государственный университет морского и речного флота им. адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: natashov1397@mail.ru, sokolovss@gumrf.ru

Аннотация. Обеспечение информационной безопасности в контексте модели поиска аварийных разливов нефти и нефтепродуктов группой беспилотных летательных аппаратов подразумевает собой разработку и интеграцию мер безопасности для обеспечения конфиденциальности и целостности информации. Это включает в себя: шифрование, контроль доступа, аутентификацию, мониторинг, обучение персонала и сотрудничество с экспертами по безопасности и так далее.

Ключевые слова: беспилотные летательные аппараты; автоматизированная система поиска; информационная безопасность.

ENSURING INFORMATION SECURITY OF AN AUTOMATED SYSTEM FOR OIL AND PETROLEUM SPILL RESPONSE BY A GROUP OF UNMANNED AERIAL VEHICLES

Egorova Kristina, Sokolov Sergey
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya str, St. Petersburg, Russia, 198035
e-mails: natashov1397@mail.ru, sokolovss@gumrf.ru

Abstract. Ensuring information security in the context of a model for oil and petroleum spill response by a group of unmanned aerial vehicles (UAVs) involves the development and integration of security measures to ensure confidentiality and integrity of information. This includes encryption, access control, authentication, monitoring, personnel training, collaboration with security experts, and so on.

Keywords: unmanned aerial vehicles; automated search system; information security.

Введение. Защита информации является критическим аспектом в работе модели поиска аварийных разливов нефти и нефтепродуктов группой беспилотных летательных аппаратов (БПЛА). В свете все возрастающих киберугроз и уязвимостей систем, необходимо разработать и внедрить эффективные меры безопасности, чтобы обеспечить конфиденциальность, целостность и доступность информации [1].

Одним из ключевых моментов в защите информации является шифрование. Шифрование позволяет защитить данные путем преобразования их в зашифрованный формат, который доступен только авторизованным пользователям или системам. Это может быть достигнуто с помощью симметричного или асимметричного шифрования, где важен выбор подходящего алгоритма и использование надежных ключей.

Другим важным аспектом является контроль доступа к информации. Необходимо разработать строгие политики доступа и определить роли пользователей, чтобы гарантировать, что только авторизованные лица имеют доступ к конфиденциальной информации. Использование многоуровневой аутентификации, такой как пароли, биометрические данные или двухфакторная аутентификация, может значительно повысить уровень безопасности [2].

Мониторинг информационной системы играет также важную роль в обеспечении безопасности. Необходимо регулярно контролировать доступ и использование информации, чтобы выявить любые подозрительные действия, нарушения или аномалии. Это может быть достигнуто с помощью системы журналирования, мониторинга сетевого трафика и использования системы обнаружения вторжений (IDS) или системы предотвращения вторжений (IPS).

Обучение персонала также является неотъемлемой частью обеспечения безопасности информации. Регулярные тренинги и обучение персонала по основам безопасности помогут повысить их осведомленность о современных угрозах и методах атак. Это также позволит персоналу быстро реагировать на инциденты безопасности и применять соответствующие меры защиты.

Сотрудничество с экспертами по безопасности также является важной составляющей защиты информации. Регулярное общение с экспертами позволит получить ценные рекомендации и советы по улучшению безопасности модели и системы. Это также поможет быть в курсе последних тенденций и событий в области информационной безопасности.

Регулярное обновление и патчинг системы необходимо для применения последних исправлений безопасности и патчей. Неисправленные уязвимости могут стать точкой входа для злоумышленников, поэтому важно следить за обновлениями от производителей и применять их своевременно. Также существует возможность периодического анализа рисков и уровня уязвимостей системы для максимальной эффективности защиты информации.

Непрерывное улучшение безопасности является ключевым аспектом. Необходимо проводить анализы и аудиты безопасности, чтобы выявить потенциальные слабые места и улучшить их. Постепенное обновление мер безопасности в соответствии с новыми угрозами и требованиями позволит поддерживать лояльность пользователей и минимизировать риски.

Наконец, физическая безопасность также имеет значение. Защита серверов, баз данных и другого оборудования от несанкционированного физического доступа является важным аспектом обеспечения безопасности информации. Отдельные серверные комнаты, системы контроля доступа и видеонаблюдение могут быть реализованы для защиты физической инфраструктуры.

В целом, разработка плана мер безопасности и его последовательное внедрение и поддержание поможет обеспечить безопасность модели поиска разливов нефти и конфиденциальность информации. Постоянное обновление знаний и сотрудничество с экспертами являются важными для адаптации к изменяющейся угрозовой ситуации и защите от эволюции вида атак.

Кроме описанных выше мер безопасности, существуют и другие важные аспекты, которые необходимо учесть при защите информации в модели поиска разливов нефти.

Один из таких аспектов — это резервное копирование данных. Регулярное создание резервных копий данных является неотъемлемой частью стратегии безопасности [3]. Это позволяет восстановить информацию в случае потери, повреждения или угона данных. Рекомендуется использовать разные типы хранилищ для резервных копий, такие как локальное хранилище, облачное хранилище или внешние носители.

Также важно обеспечить физическую безопасность рабочих мест и инфраструктуры. Это может включать установку камер наблюдения, средств физической защиты (например, замки и тревожные системы), ограничение доступа к помещениям, где размещена инфраструктура модели, и многое другое.

Регулярное тестирование на проникновение (пентестинг) также может быть полезным для оценки уровня безопасности системы и выявления возможных уязвимостей. Пентестинг может быть проведен внешними экспертами по безопасности или внутренними специалистами, которые протестируют систему на наличие уязвимостей и предоставят рекомендации по их устранению.

Соответствие нормативным требованиям также является важным аспектом. Некоторые отраслевые стандарты, такие как стандарты безопасности информации ISO 27001 или GDPR (Общее регламентирование по защите данных), могут определить требования и рекомендации по инфраструктуре и защите данных. Соблюдение этих требований может помочь обеспечить соответствие и защиту информации.

Необходимо также соблюдать принципы минимизации данных и принципы доступа по необходимости. Это означает, что только необходимая информация должна быть хранена и обрабатываться, а пользователи должны иметь доступ только к информации, которая необходима для выполнения своей работы.

С учетом развития технологий и интеграции с другими системами, также следует учесть проверку безопасности сторонних компонентов и интеграций. Некорректно сконфигурированные или уязвимые компоненты могут стать точкой входа для злоумышленников.

Наконец, важно иметь план реагирования на инциденты. Проактивность в отношении обнаружения, анализа и реагирования на возможные инциденты безопасности может существенно снизить их влияние. План реагирования на инциденты должен включать процессы обработки инцидентов, команду реагирования, процедуры уведомления и восстановления после инцидента.

Соблюдение всех этих мер безопасности позволит обеспечить надежность и сохранность информации в модели поиска аварийных разливов нефти и нефтепродуктов группой БПЛА, уменьшить риски и повысить доверие пользователей к системе [4, 5].

Заключение. Безопасность данных в модели поиска аварийных разливов нефти и нефтепродуктов группой БПЛА — это важный аспект, который должен быть тщательно рассмотрен и реализован. Защита информации включает в себя различные аспекты, включая шифрование данных, контроль доступа, обеспечение физической безопасности, создание резервных копий данных, тестирование на проникновение и соблюдение нормативных требований.

Правильная реализация мер безопасности позволяет снизить риски утечки и несанкционированного доступа к информации, обеспечивает конфиденциальность, целостность и доступность данных. Кроме того, создание плана реагирования на инциденты помогает быстро и эффективно реагировать на возможные угрозы и минимизировать их последствия.

Защита данных требует постоянного мониторинга и обновления, чтобы учитывать новые уязвимости и сценарии атак. Ответственность за безопасность лежит на всей команде, включая разработчиков, сетевых администраторов и пользователей.

Все эти меры безопасности необходимо рассматривать в контексте специфических потребностей и требований вашей организации. Соблюдение всех рекомендаций по безопасности позволит защитить информацию в модели поиска аварийных разливов нефти и нефтепродуктов и дать уверенность в ее надежности и сохранности.

СПИСОК ЛИТЕРАТУРЫ

1. Ныркова А. П., Вайгандт Н. Ю. Контроль целостности данных при мониторинге транспортных средств // Журнал университета водных коммуникаций. № 1, 2013. С. 54-61.
2. Ныркова А. П., Рудакова С. А. Методика аудита объектов информатизации по требованиям информационной безопасности // Журнал университета водных коммуникаций. № 3, 2012. С. 146-149.
3. Черняков А. В., Ныркова А. П. Алгоритмы резервного копирования // Материалы работы III научно–исследовательской конференции студентов и аспирантов факультета информационных технологий. «IT: ВЧЕРА, СЕГОДНЯ, ЗАВТРА — 2014», 19 декабря 2014 г. СПб. : ГУМРФ имени адмирала С. О. Макарова, 2015. С. 129–133.
4. Егорова К. В. Имитационная модель управления полетом группы беспилотных летательных аппаратов на основе алгоритма пчелиной колонии // Вестник Воронежского государственного технического университета, 2023. Т. 1. № 2. С. 68-71.
5. Егорова К. В., Соколов С. С., Гаскаров В. Д. Автоматизированная идентификация разливов нефти при помощи группы беспилотных летательных аппаратов // Сборник научных статей национальной научно-практической конференции профессорско-преподавательского состава ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова». Санкт-Петербург, 2022. С. 96-102.

УДК 004.032

О ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ МОДЕЛЕЙ ОБРАБОТКИ ИНФОРМАЦИИ НА ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Зубанова Анастасия Александровна, Когтев Алексей Валерьевич
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: nasty213@mail.ru, xx.ww.zz@ya.ru

Аннотация. Проводится анализ возможности и целесообразности использования моделей обработки информации на объектах критической информационной инфраструктуры в соответствии с требованиями законодательства.

Ключевые слова: критическая информационная инфраструктура; категория значимости; модели обработки данных; сервер; требования информационной безопасности.

ON THE POSSIBILITY OF USING INFORMATION PROCESSING MODELS ON OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE

Zubanova Anastasia, Kogtev Alexey
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya st., Saint-Petersburg, 198035, Russia
e-mails: nasty213@mail.ru, xx.ww.zz@ya.ru

Abstract. An analysis is being made of the possibility and feasibility of using information processing models at critical information infrastructure facilities in accordance with legal requirements.

Keywords: critical information infrastructure; significance category; data processing models; server; information security requirements.

Введение. В настоящее время объекты критической информационной инфраструктуры (далее — ОКИИ) имеют высокую значимость для государства. ОКИИ — это объекты, выполняющие технологические процессы, однако, помимо таких объектов в состав также входят информационные системы, осуществляющие сбор информации о технических средствах, программном обеспечении, технических проверках сканерами систем, а также событиях информационной безопасности, которые на них происходят, информационно-телекоммуникационные сети [1, 2]. Помимо ОКИИ существуют также субъекты критической информационной инфраструктуры, которые представляют собой государственные органы или учреждения, юридические лица или индивидуальные предприниматели, на правах полной собственности или аренды, владеющие ОКИИ, которые в свою очередь функционируют в сферах науки, здравоохранения, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка [2-5]. Также субъектами критической информационной инфраструктуры могут быть государственные органы или учреждения, обеспечивающие функционирование ОКИИ.

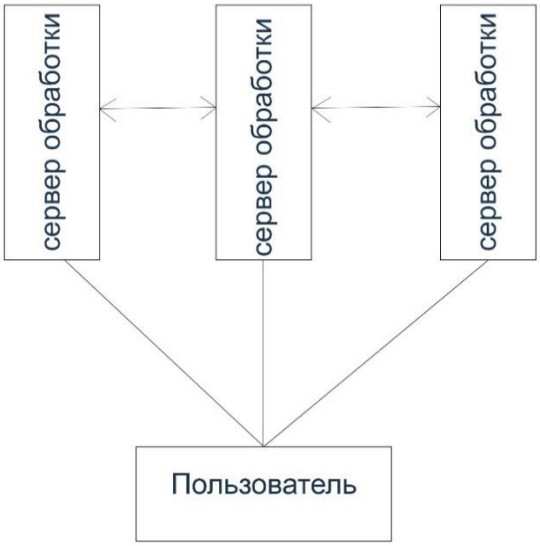


Рис. 4. Модель распределенной системы обработки информации

Начиная с 2013 года на государственном уровне было принято решение о формировании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы, в последствии в 2017 году был принят федеральный закон 187 «О безопасности КИИ Российской Федерации» [1], в соответствии с которым и должна производиться обработка данных на ОКИИ. Но вернемся к непосредственной обработке информации.

На данный момент существуют несколько моделей обработки информации. Рассмотрим их подробнее.

На рис. 1 представлена схема модели распределенной обработки информации. Обработка информации в рамках такой модели производится на распределенных в локальной сети системах [3, 4]. Такое распределение осуществляется с помощью специального инструментария, в виде программного обеспечения [5, 6]. Процесс обработки делится на самостоятельные блоки. Взаимодействие между компонентами системы обработки информации осуществляется одним из двух вариантов: удаленный вызов процедур или электронная почта. Удаленный вызов процедур характеризуется прозрачностью, высокой скоростью отклика, но в то же время является достаточно дорогостоящим, поскольку все сервера, участвующие в обработке, должны быть доступны на протяжении всего времени обработки информации и передачи ее между компонентами системы.

Далее рассмотрим модель обработки информации в рамках одного сервера/персонального рабочего места. В рамках данной модели обработка происходит, как отмечено выше, в рамках одного сервера. Такая модель в современном обществе малоприменима, поскольку в нынешней ситуации преобладает многопользовательская обработка, при которой данные доступны с нескольких рабочих мест. Также данная модель не является надежной, поскольку при нарушении работоспособности сервера/персонального рабочего места, на котором происходит обработка, высока вероятность утраты обрабатываемой информации, что является неприемлемым.

Модель клиент/сервер заключается в том, что хранение, администрирование и предоставление конечной информации пользователям организуется на сервере (рис.2). Использование данных непосредственно пользователем происходит на клиенте. Модель централизованной обработки информации отличается от модели клиент/сервер что при централизованной обработке информации предоставление конечной информации распределяется через порты/каналы ввода-вывода, а при использовании модели клиент/сервер распределение происходит через сетевые средства. Достоинствами модели клиент/сервер в первую очередь является возможность установки гибких рабочих мест, в частности гибкость заключается в разнообразии используемых платформ, операционных систем и т. д.

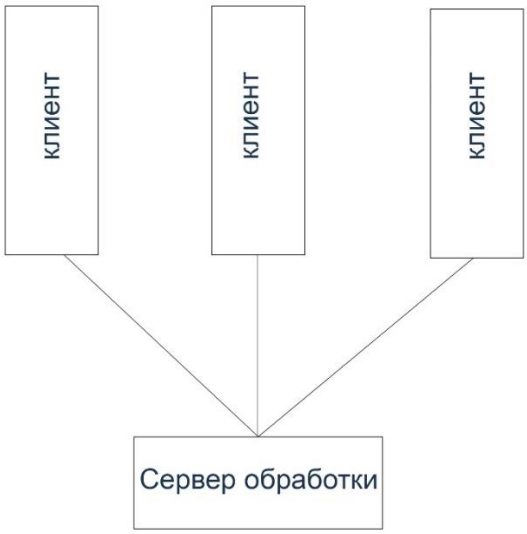


Рис. 5. Модель обработки информации клиент/сервер

Рассмотрев вышеописанные модели, проанализируем возможность и эффективность их использования в рамках ОКИИ, например, 3 категории значимости, используем эту категорию, поскольку она требует минимальных соблюдений требований.

Итак, в соответствии с 239 приказом ФСТЭК на ОКИИ 3 категории необходимо соблюдение некоторых мер, в частности [7]:

- Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему (УДП.6);
- Разделение полномочий (ролей) пользователей (УДП.4);
- Реализация защищенного удаленного доступа (УДП.13);
- Реализация антивирусной защиты (АВЗ.1);
- Резервное копирование информации (ОДТ.4);

– Обеспечение возможности восстановления информации (ОДТ.5).

При модели распределенной обработки информации, используется несколько серверов, блоков, для каждого из которых необходимо обеспечить соответствие мерам, описанным выше. Соответственно, стоимость содержания такой модели будет велика, и будет снижаться скорость передачи информации между блоками, из-за установки межсетевых экранов, с каждой стороны.

Если же речь идет про модель однопользовательской системы, то затраты на инструментарий необходимый для соответствия мерам гораздо ниже, чем при использовании первой модели, но необходимо предусмотреть варианты передачи информации между системами, а также затраты на количество лицензий в соответствии с количеством пользователей, для которых придется установить такую систему.

Что касается моделей клиент/сервер и модель централизованной обработки информации, то обеспечение соответствию мерам обеспечивается еще более меньшими затратами, даже по сравнению с предыдущей моделью, поскольку соблюдение мер ОДТ.5 и ОДТ.4 осуществляется для одного сервера, а не для всех экземпляров систем, как в модели однопользовательской системы.

Заключение. Итак, проанализировав все описанные выше модели для возможности использования на ОКИИ со стороны затрат на соблюдение мер, можно сделать вывод, что наиболее целесообразно использование модели клиент/сервер.

СПИСОК ЛИТЕРАТУРЫ

1. О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон РФ от 26.07.2017 г. № 187-ФЗ: принят Гос. Думой 12 июля 2017 г.: одобр. Советом Федерации 19 июля — 26 июля 2017 г.
2. Sokolov S. S. The Safety Assessment of Critical Infrastructure Control System / S. S. Sokolov, N. B. Glebov, E. N. Antonova, A. P. Nyrkov // IEEE International Conference Quality Management, Transport and Information Security, Information Technologies, IT and QM and IS, 5 November 2018 : proceedings of the Conference, 2018. Pp. 154-157. DOI.org/10.1109/ITMQIS.2018.8524948.
3. Ныркова А. П. Обеспечение безопасности объектов информатизации транспортной отрасли / под ред. А. П. Ныркова. ; А. П. Ныркова, А. А. Ныркова, С. С. Соколова, А. А. Шнуренко. СПб. : Изд-во Политехн. ун-та, 2015. 544 с. ISBN 978–5–7422–4841–5.
4. Информационные сети и телекоммуникационные каналы. Модель распределённой обработки информации // Bourabai Research [Электронный ресурс]. URL: http://bourabai.ru/telecom/nets17.htm (дата обращения: 29.06.2023).
5. Наташова К. В. К вопросу о категорировании объектов критической информационной инфраструктуры морских портов / К. В. Наташова, С. С. Соколов, О. Н. Губернаторов, А. П. Ныркова, А. В. Кириков // Безопасность информационных технологий. Т. 27. № 2. 2020. С. 35–46. http://dx.doi.org/10.26583/bit.2020.2.03
6. Ныркова А. П. Использование автоматизированной системы управления предприятием при территориально распределённом характере предприятия / А. П. Ныркова, К. С. Воеводский, К. О. Князева // Юбилейная XV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2016)». Санкт-Петербург, 26-28 октября 2016 : материалы конференции. СПб.: СПОИСУ, 2016. С. 528-529.
7. Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации: приказ ФСТЭК России от 25 декабря 2017 г. № 239: зарегистрировано в Министерстве юстиции РФ 26 марта 2018 г., рег. № 50524.

УДК 681.3.06

АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДОВ ПРОГНОЗИРОВАНИЯ И ТЕХНИЧЕСКИХ СРЕДСТВ АСУ. ПЕРСПЕКТИВЫ И ВОЗМОЖНОСТИ РАЗВИТИЯ АСУ

Капустин Артем Сергеевич
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mail: kapustin-7@mail.ru

Аннотация. Данная научная статья представляет собой комплексный анализ существующих методов прогнозирования и технических средств автоматизированных систем управления (АСУ). Рассматриваются различные методологии, включая статистические модели, искусственные нейронные сети и методы машинного обучения, а также их применение в АСУ для прогнозирования производственных и технических показателей. В заключение статьи представлены рекомендации по дальнейшему развитию и улучшению прогнозных методов с учетом особенностей АСУ.

Ключевые слова: gрогнозирование; технические средства; автоматизированные системы управления; статистические модели; искусственные нейронные сети; машинное обучение; производственные показатели; технические параметры.

ANALYSIS OF EXISTING FORECASTING METHODS AND TECHNICAL TOOLS IN AUTOMATED CONTROL SYSTEMS. PROSPECTS AND OPPORTUNITIES FOR THE DEVELOPMENT OF UTOMATED CONTROL SYSTEMS

Kapustin Artem
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mail: kapustin-7@mail.ru

Abstract. This scientific article provides a comprehensive analysis of existing forecasting methods and technical tools in automated control systems (ACS). Various methodologies, including statistical models, artificial neural networks, and machine learning methods, are examined, along with their application in ACS for forecasting production and technical indicators. The conclusion of the article includes recommendations for further development and improvement of forecasting methods, taking into account the specificities of ACS.

Keywords: forecasting; technical tools; automated control systems; statistical models; artificial neural networks; machine learning; production indicators; technical parameters.

Введение. Автоматизированные системы управления (АСУ) являются важной составной частью современных промышленных и технических процессов. Они позволяют повысить эффективность работы, снизить операционные издержки и обеспечить стабильность производственных процессов. Прогресс в области информационных технологий и развитие методов прогнозирования позволяют создавать более точные и надежные прогнозы, что играет ключевую роль в обеспечении безотказной работы АСУ.

Тема данной статьи — анализ существующих методов прогнозирования и технических средств в АСУ. Важность этой темы обусловлена необходимостью предсказания будущих технических и производственных показателей, что позволяет оперативно принимать решения и эффективно управлять производством. Далее будут рассмотрены методы прогнозирования и технические средства АСУ.

1. Статистические модели прогнозирования

Статистические методы прогнозирования являются одними из наиболее распространенных и хорошо изученных. Они основаны на анализе статистических данных, а именно временных рядов, и позволяют выявить закономерности и тренды в исторических данных, что обеспечивает возможность предсказания будущих значений. Классические статистические модели включают методы экстраполяции, регрессионный анализ, метод ARIMA (авторегрессия с интегрированным скользящим средним) и др. Однако статистические методы имеют свои ограничения, такие как невозможность учесть сложные нелинейные зависимости, что делает их менее эффективными в некоторых сценариях прогнозирования [1].

2. Искусственные нейронные сети

Искусственные нейронные сети (ИНС) — это математические модели, которые пытаются воспроизвести работу человеческого мозга. Они состоят из множества взаимосвязанных искусственных нейронов, которые способны обрабатывать информацию и «обучаться» на основе исторических данных. ИНС способны выявлять сложные зависимости и нелинейные взаимосвязи в данных, что делает их мощным инструментом для прогнозирования. В зависимости от архитектуры, искусственные нейронные сети могут использоваться для прогнозирования временных рядов, классификации, регрессии и др. [2]. Однако для эффективной работы ИНС требуется большой объем данных и правильная настройка гиперпараметров [3].

3. Методы машинного обучения

Машинное обучение представляет собой подраздел искусственного интеллекта, который позволяет системам учиться на основе опыта и данных. В области прогнозирования машинное обучение может быть использовано для создания различных моделей, таких как линейная регрессия, метод опорных векторов, случайные леса, градиентный бустинг и др. Эти методы позволяют достичь высокой точности прогнозирования, особенно когда имеется большой объем данных. Важным преимуществом методов машинного обучения является их способность автоматически выявлять и использовать наиболее значимые признаки для прогнозирования [4, 5].

4. Интеграция методов прогнозирования в АСУ

Эффективное применение прогнозных методов требует их интеграции в автоматизированные системы управления. Интеграция предполагает разработку соответствующих программных интерфейсов, а также адаптацию моделей к специфике конкретной АСУ. Для управления сложными техническими системами необходимо комбинировать различные методы прогнозирования и учитывать другие факторы, которые могут повлиять на производственные процессы [6].

5. Оценка качества прогнозов и управление рисками

Качество прогнозов играет важную роль в принятии решений и планировании в АСУ [7]. Оценка качества прогнозов включает использование различных метрик, таких как среднеквадратическая ошибка, коэффициент детерминации и другие. Управление рисками, связанными с неточностью прогнозов, требует применения соответствующих методов и стратегий [8]. Важно проводить регулярный мониторинг и анализ качества прогнозов, чтобы оперативно вносить корректировки в управленческие решения и минимизировать возможные негативные последствия неточных прогнозов [9].

6. Применение в различных областях АСУ

Методы прогнозирования и технические средства нашли применение в различных областях автоматизированных систем управления. Например, в промышленности прогнозирование позволяет планировать производственные процессы, оптимизировать запасы сырья и материалов, а также прогнозировать спрос на продукцию. В энергетических системах прогнозирование потребления энергии позволяет эффективно управлять

производством электроэнергии и распределением нагрузки. В финансовой сфере прогнозирование играет ключевую роль в управлении рисками, определении инвестиционных стратегий и принятии финансовых решений.

7. Преимущества и ограничения

Каждый метод прогнозирования имеет свои преимущества и ограничения. Статистические модели позволяют выявлять тренды и сезонность, но могут быть менее эффективными при наличии нелинейных зависимостей. Искусственные нейронные сети способны обрабатывать сложные данные, но требуют большого объема данных для обучения и настройки параметров. Методы машинного обучения отличаются высокой точностью, но могут быть менее интерпретируемыми и требовательными к вычислительным ресурсам [10].

8. Будущее развитие и перспективы

С развитием технологий и методов анализа данных, прогнозирование в АСУ будет продолжать улучшаться и находить новые области применения. Одной из перспективных областей является использование искусственного интеллекта и глубокого обучения для создания более точных и адаптивных прогнозных моделей. Применение алгоритмов адаптивного прогнозирования позволит автоматически корректировать модели на основе актуальных данных и событий, что повысит их эффективность и устойчивость к изменениям в окружающей среде [11].

Перспективы и возможности технических средств автоматизированных систем управления (АСУ) открывают перед нами широкий горизонт для улучшения эффективности и надежности различных процессов и систем. В последние десятилетия прогресс в области технологий привел к значительному развитию АСУ, и в будущем ожидается еще больший прорыв в этой области.

Одной из ключевых перспектив технических средств АСУ является интеграция с передовыми технологиями, такими как Интернет вещей (IoT) и искусственный интеллект (ИИ). Интернет вещей позволяет подключать сенсоры и устройства к сети, собирать данные и передавать их в реальном времени [12, 13]. Это предоставляет операторам и системам управления ценную информацию о состоянии оборудования, среде и производственных процессах, что помогает быстро реагировать на изменения и предотвращать возможные сбои.

Искусственный интеллект также играет ключевую роль в развитии технических средств АСУ. Алгоритмы машинного обучения и нейронные сети способны анализировать огромные объемы данных и выявлять сложные взаимосвязи, что делает прогнозирование надежности более точным и эффективным. Это также позволяет создавать автоматизированные системы управления, которые способны адаптироваться к изменяющимся условиям и оптимизировать работу процессов [10].

Другой важной перспективой технических средств АСУ является улучшение систем мониторинга и диагностики. Современные технологии позволяют создавать более точные и надежные системы мониторинга, которые способны оперативно обнаруживать проблемы и предупреждать о возможных отказах. Это помогает предотвращать серьезные аварии и минимизировать простои оборудования, что в свою очередь повышает эффективность работы и снижает затраты на обслуживание [14].

Перспективы технических средств АСУ также связаны с их применением в различных отраслях. Например, в промышленности технические средства АСУ могут использоваться для автоматизации производственных линий и оптимизации производственных процессов. В энергетической отрасли они позволяют управлять энергоэффективностью и оптимизировать расход электроэнергии. В транспортной отрасли они могут обеспечить автоматизацию управления транспортными потоками и обеспечить безопасность движения [4, 15].

В целом, перспективы и возможности технических средств АСУ огромны и постоянно расширяются с развитием технологий. Применение передовых технологий, таких как IoT и ИИ, улучшение систем мониторинга и диагностики, а также разнообразное применение в различных отраслях делают технические средства АСУ мощным инструментом для оптимизации работы систем и процессов, обеспечивая более эффективное и безопасное функционирование различных отраслей промышленности и общественной инфраструктуры.

Заключение. Анализ существующих методов прогнозирования и технических средств в автоматизированных системах управления является важным шагом в разработке эффективных прогнозных систем. Статистические модели, искусственные нейронные сети и методы машинного обучения предоставляют разнообразные инструменты для предсказания будущих значений. Интеграция этих методов и оценка качества прогнозов являются ключевыми факторами в принятии обоснованных решений и управлении рисками в автоматизированных системах управления [7-9, 16].

СПИСОК ЛИТЕРАТУРЫ

1. Dynamics Models of Synchronized Piecewise Linear Discrete Chaotic Systems of High Order / Sokolov S. [ets al] // Symmetry. 2019. № 11(2). 236 p.
2. Sobolev A. S., Chernyi S. G., Krivoguz D. O., Nyrkov A. P., Zinchenko E. G. Convolution Neural Network for Identification of Underwater Objects // Proceedings of the Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus 2022 9755621. 2022. Pp. 455-458.
3. Медведев Д. С. Интеграция технических средств АСУ с технологией Интернета вещей // Мир автоматики и управления. 2022. Т. 56. № 6. С. 42-49.
4. Ныркov А. П., Соколов С. С., Шнуренко А. А. Автоматизированное управление транспортными системами: монография. СПб. : ГУМРФ имени адмирала С. О. Макарова, 2013. 32 с.
5. Zhilenkov A. A., Sokolov S. G., Chernyi A. P. Nyrkov and others]. Intelligent autonomous navigation system for UAV in randomly changing environmental conditions // Journal of Intelligent and Fuzzy Systems. 2020. Vol. 38. № 5. Pp. 6619-6625.
6. Глушко О. В. Адаптивные алгоритмы прогнозирования надежности технических средств АСУ // Техническая кибернетика. 2023. Т. 34. № 3. С. 87.
7. Анализ информационных рисков / Н. М. Вихров [и др.] // Морской вестник. 2015. № 3 (55). С. 81–85.

8. Veselkov V., Vikhrov N., Nyrkov A., Chernyi S., Titov I. Development of Methods to Identify Risks to Build up the Automated Diagnosis Systems // Proceedings of the IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg, 2017. Pp. 598–601.
9. Ныркова А. П., Ныркова А. А. Модели, алгоритмы и программное обеспечение минимизации рисков мультимодальных перевозок // Вестник государственного университета морского и речного флота имени адмирала С. О. Макарова. 2013. № 1 (20). С. 67–73.
10. Иванов А. Б. Алгоритмическое обеспечение прогнозирования надежности технических средств АСУ морского порта // Вестник технического университета. 2018. Т. 21. № 3. С. 345-352.
11. Goloskokov K., Korotkov V., Nyrkov A., Knysh T. Error correction algorithms in on-board intelligent transport data transmission systems // Journal of Physics: Conference Series 2061(2021). 2021. 012097.
12. Zhilenkov A. A., Nyrkov, S. Chernyi, S. Sokolov Simulation of in-sensor processes in the sensor — Object system type when scanning the elements of underwater communication lines with a probe beam // International Review on Modelling and Simulations. 2017. 10(15). Pp. 363-370.
13. Zhilenkov A. A., Tsvetkov Y. N., Chistov V. B., Nyrkov A. P., Sokolov S. S. Simulink-aided Design and Implementation of Sensorless BLDC Motor Digital Control System // IOP Conf. Series: Materials Science and Engineering 221. 2017. № 012004.
14. Сидоров П. Н. Интеграция технических средств АСУ с системами мониторинга и диагностики // Автоматика и автоматизация. 2020. Т. 45. № 1. С. 76-82.
15. Ковалев А. М. Использование искусственного интеллекта в алгоритмическом обеспечении прогнозирования надежности технических средств // Интеллектуальные системы и технологии. 2021. Т. 10. № 4. С. 24-31.
16. Models and algorithms for estimation and minimization of the risks associated with dredging / Mamunts D. G. [ets al] // Transport and Telecommunication. 2017. Vol. 18. № 2. С. 139–145.

УДК 004.896

ТЕНДЕНЦИИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДИАГНОСТИКЕ ТЕХНИЧЕСКИХ СИСТЕМ

Котов Александр Дмитриевич
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mail: policookie@yandex.ru

Аннотация. В данной статье кратко описаны методы и технологии, на основе которых строится искусственный интеллект, а также описаны основные тенденции применения искусственного интеллекта в диагностике технических систем.

Ключевые слова: искусственный интеллект; техническая диагностика; нейронные сети; машинное обучение.

TRENDS IN THE USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGY IN THE DIAGNOSIS OF TECHNICAL SYSTEMS

Kotov Aleksandr
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mail: policookie@yandex.ru

Abstract. This article briefly describes the methods and technologies on the basis of which artificial intelligence is built, as well as describes the main trends in the use of artificial intelligence in the diagnosis of technical systems.

Keywords: artificial Intelligence; technical diagnostics; neural networks; machine learning.

Введение. На сегодняшний день искусственный интеллект (Artificial Intelligence, AI) является одной из наиболее привлекательных, перспективных и активно развивающихся технологий, охватывающей практически все сферы жизни общества. Одной из таких областей применения является диагностика различных технических систем. Техническая диагностика включает в себя обработку и анализ огромного объема информации, полученной из множества источников, что хорошо ложится на концепцию применения искусственного интеллекта и открывает для диагностики новые возможности и перспективы.

Искусственный интеллект — это область компьютерных наук, которая занимается созданием интеллектуальных машин, способных выполнять задачи, которые обычно требуют человеческого интеллекта, такие как распознавание речи, принятие решений, обработка естественного языка и т.д. ИИ может быть использован для автоматизации процессов, улучшения производительности и повышения эффективности. Искусственный интеллект построен на основе различных принципов и технологий, включающих машинное обучение, нейронные сети, генетические алгоритмы, обработку естественного языка и другие [1].

Искусственный интеллект может быть реализован с использованием различных методов и техник, включая: символьный подход, основанный на символьной обработке информации и использовании формальных правил для решения задач, подход включает в себя логическое программирование и экспертные системы; статистический подход, основанный на анализе статистических данных и построении моделей, способных обобщать и делать вывод на основе

данных; подход глубокого обучения, использующий искусственные нейронные сети с большим количеством слоев для извлечение сложных иерархических признаков из данных и позволяющий моделям обучаться на большом объеме данных, и достигать высокой точности в различных задачах [2].

Одним из основных методов, на котором строится искусственный интеллект, является машинное обучение — технология, которая изучает и разрабатывает алгоритмы и модели, которые позволяют компьютерам обучаться и делать прогнозы или принимать решения на основе большого объема данных без явного программирования. Концепция машинного обучения основана на идее, что компьютерные системы могут обучаться на основе данных и опыта с целью улучшения производительности в выполнении задач. Для решения задач машинное обучение использует различные методы и алгоритмы, такие как линейная регрессия, деревья решений, метод опорных векторов, нейронные сети, глубокое обучение и т.д. Эти методы позволяют моделям обрабатывать данные, находить закономерности и делать предсказания или принимать решения на основе этих данных.

Другой важной технологией, используемой в формировании искусственного интеллекта, являются нейронные сети. Нейронные сети — математические модели, состоящие из соединенных между собой и взаимодействующих искусственных нейронов, которые имитируют работу человеческого мозга и используются для решения сложных задач обработки и передачи информации [3]. Основные компоненты нейронной сети: нейроны — базовые блоки нейронной сети, имитирующие работу нейронов в мозге и принимают на вход сигналы, обрабатывают и передают входной сигнал другим нейронам, каждый нейрон имеет свои веса, функцию активации и выход; веса — параметры, определяющие силу связей между нейронами, вес нейрона характеризует степень влияния входного сигнала на выходной сигнал; функция активации — функция, определяющая выходной сигнал нейрона на основе его входных данных и весов, тем самым добавляя нелинейность в нейронную сеть, что позволяет моделировать сложные зависимости в данных; слои — нейроны организованы в слои, в типичной нейронной сети есть входной слой, принимающий входные данные, скрытые слои, выполняющие обработку и выходной слой, предсказывающий результаты или принимающий решения на основе обработанных данных. Существует несколько типов нейронных сетей: персептрон, рекуррентные, сверточные и глубокие — каждый из которых имеет свои особенности и применяется для решения определенных задач.

Еще одним методом, используемым в искусственном интеллекте, являются генетические алгоритмы — эволюционный метод оптимизации, основанный на принципах естественного отбора и генетики, и используемый в задачах с поиском наилучшего решения в большом пространстве возможных вариантов. Основными компонентами генетического алгоритма: популяция — генетический алгоритм работает с популяцией индивидуальных решений, называемых хромосомами или генотипами. Каждая хромосома представляет собой потенциальное решение задачи и представляется в виде набора генов или параметров; функция приспособленности — функция, оценивающая качество каждой хромосомы в популяции; операторы генетической манипуляции — используются для создания новых потомков на основе родительских хромосом, операторы включают скрещивание и селекцию; эволюция — генетический алгоритм эмулирует процесс естественной эволюции, где популяция проходит через несколько поколений, на каждой итерации алгоритма проходит оценка приспособленности, генетическая манипуляция и формирование нового поколения. Через несколько поколений популяция сходится к наилучшему решению.

Обработка естественного языка (Natural Language Processing, NLP) — еще одна важная технология, используемая в искусственном интеллекте, которая занимается взаимодействием между компьютером и естественным языком, используемым людьми, включающая в себя различные методы и техники для понимания, интерпретации и генерации текста на естественном языке. Основная цель NLP — эффективная работа с текстом и выполнение задач, требующих понимания и генерации естественного языка, например, синтаксический, семантический анализ, распознавание именованных сущностей, классификация текста, машинный перевод и т. д.

Принципы работы искусственного интеллекта включает следующие этапы:

1. Предварительный анализ и сбор данных;
2. Обучение модели на основе предоставленных данных, в случае машинного обучения — определение архитектуры модели, выбор функции потерь и оптимизатора, а также обучение модели на тренировочных данных;
3. Оценка и настройка модели на тестовых данных для определения ее точности и производительности;
4. Развертывание и использование на реальных данных для конкретных задач.

Потенциал использования искусственного интеллекта не ограничен. Одной из областей применения его возможностей — техническая диагностика. Техническая диагностика — процесс изучения и анализа технического состояния систем, оборудования или устройств с целью обнаружения неисправностей, проблем или возможных отказов. Техническая диагностика играет важную роль в обслуживании и эксплуатации систем, позволяя обнаружить неисправности на ранних стадиях, предотвратив негативные последствия и отказы в обслуживании. В зависимости от особенностей системы и оборудования в технической диагностике используются различные этапы и методы, например, физические измерения, анализ данных, визуальное обследование, испытания и т.д. Сфера применения технической диагностики обширна и включает в себя промышленную отрасль, медицину, энергетику, транспортную отрасль и другие.

Внедрение искусственного интеллекта в техническую диагностику дает возможность автоматизировать процессы анализа данных, увеличить точность обнаружения неисправностей и предоставления рекомендаций по их исправлению, оптимизировать процесс диагностики. Искусственный интеллект может быть использован в технической диагностике следующим образом [4]:

– Анализ данных и обнаружение аномалий — важная задача в эксплуатации и обслуживании технических средств. Применение искусственного интеллекта для решения задач такого типа позволяет автоматизировать и увеличить точность обработки большого объема исторических данных и скрытых паттернов, что дает возможность с большей эффективностью выявлять отклонения и нехарактерное поведение систем, которые могут быть признаками дефектов и сбоев в работе системы. Весь процесс состоит из следующих этапов: автоматическая подготовка данных, включающая в себя удаление лишней информации, нормализацию и заполнение пропущенных значений; обработка данных и выявление аномального поведения с применением статистических методов, машинного обучения, глубокого обучения; предоставление рекомендаций по устранению выявленных проблем. В качестве примера можно привести компанию General Electric (GE), которая применяет искусственный интеллект в своей системе мониторинга и диагностики «Predix Asset Performance Management» (APM) для диагностики аномалий и предотвращения отказов в различных промышленных системах, таких как энергетические установки, нефтегазовые платформы и железнодорожные сети. Система APM собирает данные о температуре, давлении, вибрациях и прочих параметров с датчиков, и иных источников, а затем искусственным интеллектом, обученным на исторических данных и моделях работы оборудования, изучает эти данные, определяет нормальное поведение и обнаруживает аномалии. При обнаружении отклонении система генерирует предупреждение и рекомендацию для персонала технической поддержки.

– Прогнозирование отказов, позволяет предсказывать неисправности и сбои в различных технических системах. Идея метода заключается в создании модели, основанной на обработке доступных данных о состоянии системы и применения различных алгоритмов машинного обучения. Процесс прогнозирования состоит из сбора данных о производительности, нормальном и аномальном состояниях системы, обработки этих данных, обучении модели прогнозированию отказов с использованием различных методов машинного обучения (регрессионный анализ, нейронные сети) и в итоге эксплуатации в режиме реального времени. Так авиакомпания Delta Air Lines использует алгоритмы прогнозирования отказов, собирая и обрабатывая информацию с большого количества датчиков, для определения возможных неисправностей в своем авиатехническом оборудовании, что способствует повышению уровня безопасности и снижению экономических затрат.

– Экспертные системы на базе искусственного интеллекта представляют собой компьютерные программы, основанные на статистическом анализе и интеллектуальных алгоритмах, которые используют знания и опыт эксперта конкретной предметной области для принятия решений или предоставления рекомендаций. Экспертная система состоит из созданной экспертом базы знаний, содержащей данные о предмете и предметной области, а также механизма вывода, представляющего собой набор правил и алгоритмов, определяющих поведение работы системы, и использующего данные из этой базы для принятия или поиска решений. Процесс работы состоит из следующих процедур: запрос информации от пользователя с целью определения контекста и характеристик проблемы, анализ полученных и экспертных данных, результат и рекомендации пользователю, сгенерированные с учетом правил и алгоритмов механизма вывода, обратная связь и обучение. Примером применения может послужить экспертная система SISHIP EcoMain компании Siemens, позволяющая определить ранние признаки отказов в судовых двигателях, выдавая рекомендации по предотвращению повреждений и оптимизации технического обслуживания [5].

– Интеллектуальные сенсоры, на искусственном интеллекте — устройства, способные собирать данные из различных источников основанные, анализировать их с помощью алгоритмов машинного обучения и предоставлять информацию о работоспособности системы. Главная идея таких сенсоров — анализ полученных данных и предсказание отказов и неисправностей в реальном времени. В качестве примера можно привести автомобили компании Tesla, оснащенные множеством сенсоров, данные с которых анализируются искусственным интеллектом для выявления потенциальных проблем с системой автопилотирования.

– Робототехника и автономные системы, использующие искусственный интеллект способны распознавать, обрабатывать и интерпретировать данные для поиска и чинить неисправности и неполадки в технических системах. За счет применение технологии искусственного интеллекта процесс диагностики автономными системами требует меньшего временного ресурса, а также становится более точным и эффективным. Таким системы и роботы могут самостоятельно подстраиваться под изменяющиеся условия и обучаться на прошлом опыте. Примером могут послужить роботы и автономные системы компании Asea Brown Boveri, умеющие проводить самостоятельную проверку оборудования, обрабатывать данные с датчиков, предсказывать возможные аварийные ситуации и предоставлять рекомендации по улучшению эффективности работы технических систем.

– Планирование в диагностике — применение искусственного интеллекта позволяет на базе исторических данных, паттернов отказов и иных аспектов прогнозировать затраты ресурсов на уход и ремонт технических средств, тем самым оптимизируя процесс обслуживания и обеспечивая экономическую выгоду в планировании

бюджета. Одной из компаний, использующих искусственный интеллект в прогнозировании затрат на обслуживание и ремонт, является компания Rolls-Royce, которые на базе большого объема данных и алгоритмов машинного обучения, создали цифровые копии своих двигателей, позволяющие отслеживать не только внутренние показатели работы, такие как температура, давление, но и внешние факторы и условия эксплуатации, чтоб позволяет им предсказывать оптимальное время и объем работ по уходу и ремонту двигателей.

Заключение. Применение искусственного интеллекта выводит техническую диагностику на новый этап развития, что позволяет существенно сократить ресурсы на обслуживание, увеличить объем обрабатываемых данных, повысить точность результатов диагностических тестов. В России применение искусственного интеллекта в технической диагностике считается очень перспективным направлением и находится на развивающемся этапе. Так искусственный интеллект постепенно внедряется в автомобильную промышленность, энергетику, промышленное оборудования и т.д. Несмотря на уже имеющий прогресс, существует ряд проблем эксплуатации ИИ таких как: отсутствие исторических данных хорошего качества, высокая сложность интеграции искусственного интеллекта в существующие системы, а также потенциальные проблемы с безопасностью и конфиденциальностью данных [6]. Однако преимущества его использования вызывают большой интерес и внимание со стороны российских компаний и организаций. Кроме того, государственная поддержка и инвестиции также оказывают положительное влияние на развитие и внедрение искусственного интеллекта в различные отрасли, в том числе и использовании искусственного интеллекта в технической диагностике.

СПИСОК ЛИТЕРАТУРЫ

1. Искусственный интеллект это что, объяснение, как работает, практическое применение [Электронный ресурс]. URL: https://oksait.ru/obrazovanie/iskusstvennyy-intellekt (дата обращения: 23.07.2023).
2. Что такое искусственный интеллект [Электронный ресурс]. URL: https://garpix.com/blog/chto-takoe-iskusstvennyj-intellekt (дата обращения: 21.07.2023).
3. Tsymay Y. V., Nyrkov A. P., Kardakova M. V. Neurointerface Modeling For Controlling Dynamic Systems // Intellectual Technologies on Transport. 2022. № 4. Pp. 85-93.
4. Примеры применения технологий Искусственного интеллекта [Электронный ресурс]. URL: https://digital.gov.ru/uploaded/files/primeryi-primeneniya-tehnologij-iskusstvennogo-intellekta.pdf?utm_referrer=https%3a%2f%2fyandex.ru%2f#:~:text=Примеры.%20Глубокое%20понимание%20и%20перевод,вычисления%2C%20распознавание%20лиц%2C%20машинный%20перевод (дата обращения: 24.07.2023).
5. Искусственный интеллект: от метафоры к техническим решениям [Электронный ресурс]. URL: https://controlengrussia.com/innovatsii/iskusstvenny-j-intellekt/iskusstvennyj-intellekt/ (дата обращения: 22.07.2023).
6. Искусственный интеллект в России и мире: эволюция, тенденции, будущее [Электронный ресурс]. URL: https://habr.com/ru/companies/inferit/articles/739514/ (дата обращения: 21.07.2023).

УДК 004.01

МОДУЛЬНЫЙ КОМПЛЕКС АВТОМАТИЗИРОВАННОЙ ВЫДАЧИ ПАРОЛЕЙ ЛОКАЛЬНОГО АДМИНИСТРАТОРА ОС WINDOWS «СКРЕПЫШ-ПАРОЛИ»

Скобелев Алексей Вячеславович, Голоскоков Константин Петрович
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: skobelevav@gumrf.ru, goloskokovkp@gumrf.ru

Аннотация. В статье представлен программный комплекс «Скрепыш-Пароли», разработанный для автоматизации процесса выдачи паролей локального администратора операционной системы Windows. Комплекс основан на использовании Telegram для обмена информацией между администратором и конечным пользователем. Рассматриваются особенности разработки этого программного комплекса, а также проводится сравнение с альтернативным решением Windows LAPS (Local Administrator Password Solution).

Ключевые слова: информационная безопасность; пароль; локальный администратор; операционная система Windows; автоматизация; Telegram; Windows LAPS.

MODULAR COMPLEX FOR AUTOMATED ISSUANCE OF PASSWORDS OF LOCAL ADMINISTRATOR OF WINDOWS OS «SKREPYSH-PAROLI»

Skobelev Alexey, Goloskokov Konstantin
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya str., St. Petersburg, 198035, Russia
e-mails: skobelevav@gumrf.ru, goloskokovkp@gumrf.ru

Abstract. The paper presents a program complex «Screpysh-Paroli», which is designed to automate the process of issuing local administrator passwords for the Windows operating system. The program complex is based on the use of Telegram to exchange information between the administrator and the end user. The article discusses the peculiarities of the development of this program complex and compares it with the alternative solution Windows LAPS (Local Administrator Password Solution).

Keywords: information security; password; local administrator; Windows operating system; automation; Telegram; Windows LAPS.

Введение. С обширным развитием информационных технологий и компьютерной техники важность обеспечения безопасности информации в организациях становится все более значимой. Попадание пароля локального администратора операционной системы Windows в руки нарушителя, как и его нестойкость к взлому, является первостепенной задачей в обеспечении информационной безопасности локальной системы. Такой пароль дает полный доступ к компьютерной системе, и его утечка или несанкционированное использование может представлять серьезную угрозу для информационной безопасности организации.

Методика. В ходе разработки программного комплекса «Скрепыш-Пароли», был использован язык программирования Python и библиотека Telegram API для создания Telegram-бота. Процесс разработки включал следующие этапы:

1. Изучение проблемы управления доступом к паролю локального администратора в организациях и анализ существующих решений.
2. Проектирование архитектуры программного комплекса «Скрепыш-Пароли», включая определение функциональных требований и механизмов безопасности.
3. Реализация функционала программного комплекса, включая автоматизацию процесса выдачи паролей и механизмы аутентификации.
4. Тестирование и отладка программного комплекса для обеспечения надежной работы и безопасности.
5. Сравнение с альтернативным решением Windows LAPS [1] для выявления преимуществ и ограничений.

Результаты. При разработке программного комплекса «Скрепыш-Пароли» были достигнуты следующие результаты:

– Реализована автоматизация процесса выдачи паролей локального администратора операционной системы Windows с использованием Telegram для обмена информацией между администратором и конечным пользователем.

– Обеспечено безопасное хранение паролей локального администратора, что предотвращает утечку или несанкционированный доступ.

– Разработан механизм аутентификации и авторизации пользователей [2], что предоставляет контроль доступа к выдаче паролей локального администратора.

– Предоставлен механизм централизованного контроля доступа, позволяющий определить список авторизованных пользователей, имеющих право получать пароли локального администратора.

Для соблюдения конфиденциальности и безопасности, ниже приведена часть кода программы, демонстрирующая основной функционал:

```python
# ... (другие функции)

# Функция для получения пароля из файла
def get_local_admin_password(pcname):
    path = «/mnt/passes/»
    with codecs.open(path + pcname + '.pass', encoding='cp866') as f:
        l = f.read().strip()
        return l[l.find(':')+2:]
# ... (другие функции)
def main():
    # Инициализация Telegram бота
    updater = Updater(token=config.token)
    dispatcher = updater.dispatcher
    # Добавление обработчиков команд
    dispatcher.add_handler(CommandHandler('help', help))
    dispatcher.add_handler(CommandHandler('getpass', getpass))
    dispatcher.add_handler(CommandHandler('start', start))
    # Запуск бота
    updater.start_polling()

if __name__ == «__main__»:
    main()
```

Анализ. Проведенный анализ результатов показал, что программный комплекс «Скрепыш-Пароли» эффективно автоматизирует процесс выдачи паролей локального администратора и значительно улучшает безопасность этого процесса [3]. Однако, следует учитывать некоторые ограничения:

– Возможное влияние внешних факторов, таких как неполадки в сети или сбои в Telegram, на доступность сервиса.

– Необходимость соблюдения рекомендаций по безопасности при использовании мессенджера Telegram для передачи паролей.

Сравнение сервисов

Для сравнения программного комплекса «Скрепыш-Пароли» было выбрано альтернативное решение Windows LAPS (Local Administrator Password Solution). Результаты сравнения приведены в таблице 1.

Таблица 1

Сравнение характеристик двух комплексов генерации паролей

Характеристика	Скрепыш-Пароли	Windows LAPS
Автоматизация выдачи паролей	Да	Да
Безопасное хранение паролей	Да	Да
Механизм аутентификации и авторизации	Да	Да
Централизованный контроль доступа	Да	Да
Интеграция с существующей инфраструктурой	Да	Да
Гибкость настройки	Да	Ограниченная
Легкость внедрения	Да	Требует дополнительных настроек и ресурсов
Стоимость реализации	Доступный	Значительные затраты на лицензии

Из таблицы видно, что оба решения обладают схожими преимуществами, такими как автоматизация процесса и безопасное хранение паролей.

Однако, «Скрепыш-Пароли» обладает гибкостью настройки и более доступной стоимостью, что делает его более привлекательным выбором для многих организаций.

Выводы. Программный комплекс «Скрепыш-Пароли» представляет собой полезное и безопасное решение для обслуживания парка компьютерной техники и управления доступом к паролю локального администратора ОС Windows. Он позволяет упростить процесс выдачи паролей и обеспечивает высокий уровень безопасности.

В сравнении с альтернативным решением Windows LAPS, «Скрепыш-Пароли» обладает более гибкой настройкой и доступной стоимостью, что делает его привлекательным выбором для многих организаций [4].

При этом, необходимо учитывать возможные недостатки, связанные с использованием мессенджера Telegram для передачи паролей, и принимать соответствующие меры для обеспечения безопасности данного процесса [5].

Заключение. Программный комплекс «Скрепыш-Пароли» представляет собой инновационное решение для автоматизации процесса выдачи паролей локального администратора ОС Windows. Разработанный комплекс обладает значительными преимуществами в сравнении с альтернативным решением Windows LAPS, такими как гибкая настройка и доступная стоимость. Однако, необходимо принимать во внимание ограничения, связанные с использованием мессенджера Telegram, и обеспечивать соответствующий уровень безопасности для предотвращения возможных угроз.

СПИСОК ЛИТЕРАТУРЫ

1. Что такое Windows LAPS? [Электронный ресурс]. URL: https://learn.microsoft.com/ru-ru/windows-server/identity/laps/laps-overview (дата обращения: 12.05.2023).
2. Ерисова А. Д., Нырков А. Д., Каторин Ю. Ф. О безопасности применения цифровых сертификатов как средства аутентификации в информационных системах на транспорте // Материалы межвузовской научно-практической конференции «Современные тенденции и перспективы развития водного транспорта России», 1 октября 2020 г. Ч. 3. СПб. : Изд-во ГУМРФ им. адм. С. О. Макарова, 2020. С. 70–71.
3. Голоскоков К. П Автоматизированная система испытаний в структуре системы управления качеством // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2008. № 6 (69). С. 116-120.
4. Малюк В. И., Голоскоков К. П. Методика оценки рационального распределения ограниченных инвестиций в развитие производственной системы региона // Вестник ИНЖЭКОНа, 2009. № 1 (28). С. 51-60. (Экономика).
5. Голоскоков К. П. Прогнозирование и оценка технического состояния сложных систем // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. 2008. № 1 (53). С. 164-168.

УДК 004.021

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ АВТОМОБИЛЕЙ

Хасанов Дмитрий Салимович
СПИИРАН ─ СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: dkhasanovsuai@yandex.ru

Аннотация. С развитием коммуникационных технологий становится очевидной необходимость обеспечения безопасности связи. В настоящее время существует вполне реальный риск того, что современные автомобили подвергнутся кибератакам, направленным на автомобильные коммуникации. Проблема состоит из динамики развития автомобилей и датчиков окружающей среды, которые уязвимы для атак подслушивания, глушения и подмены. Коммуникационный уровень включает в себя как бортовые, так и коммуникации с внешними блоками, которые подвержены влиянию подслушивания, подмены. На вершине иерархии находится уровень управления, позволяющий реализовать автономные функции автомобиля, включая автоматизацию скорости движения, торможение и рулевого управления. Атаки, направленные на сенсорный и коммуникационный уровни, могут распространяться вверх и влиять на функциональность, а также могут нарушить безопасность управления. В данной работе представлен обзор современного состояния атак и угроз, относящихся к коммуникационному уровню.

Ключевые слова: киберфизические системы; транспорт; безопасность; кибератаки.

AUTOMOTIVE CYBERSECURITY ISSUES

Khasanov Dmitry
SPIIRAN ─ SPb FRC RAS
39 14th Line V. I., St. Petersburg, 199178, Russia
e-mail: dkhasanovsuai@yandex.ru

Abstract. With the advancement of communication technology, the need for secure communications is becoming apparent. There is now a very real risk that modern automobiles will be subject to cyberattacks targeting in-vehicle communications. The problem consists of the dynamics of automobiles and environmental sensors that are vulnerable to eavesdropping, jamming and spoofing attacks. The communication layer includes both on-board and communications with external units that are vulnerable to eavesdropping, spoofing. At the top of the hierarchy is the control layer, which enables autonomous vehicle functions including automating vehicle speed, braking, and steering. Attacks targeting the sensor and communication layers can propagate upwards and affect functionality and can compromise control security. This paper presents an overview of the current state of the art of attacks and threats related to the communication layer.

Keywords: cyber-physical systems; transportation; security; cyber-attacks.

Современные автомобили уже нельзя воспринимать как просто механические системы, общая архитектура которых насчитывает более 100 млн. строк кода, что больше, чем у современной операционной системы. Автомобили становятся все более подключенными и похожими на компьютеры: они могут синхронизироваться с мобильными телефонами, предоставлять пассажирам последние погодные и навигационные данные, передавать информацию о безопасности другим автомобилям и окружающей инфраструктуре [1]. Несмотря на очевидные преимущества для пассажиров и безопасности на дорогах, компьютеризация и подключение к сети автомобилей открывают новые возможности для хакеров по взлому автомобилей и подвергают опасности жизни пассажиров и пешеходов. Многие широко разрекламированные взломы автомобилей были успешными благодаря тому, что хакеры смогли использовать автомобильные коммуникации [2]. Уязвимости в автомобильных коммуникациях приводят к четырем проблемам кибербезопасности транспортных средств:

1. Ограниченные возможности подключения. Хотя возможности внешнего подключения автомобилей растут, большинство из них пока не имеют возможности обновления программного обеспечения по воздуху, что позволило бы им всегда быть защищенными от новейших кибератак. Даже когда облачные-обновления станут более стандартными, автомобили также будут подвержены риску сбоев в работе из-за неполного обновления.

2. Ограниченная вычислительная производительность. Вычислительная производительность автомобиля, как правило, ограничена по сравнению с вычислительной производительностью компьютера. Это ограничение объясняется тем, что транспортные средства имеют более длительный срок службы и подвержены более высоким температурам и вибрациям, чем обычные ПК или ноутбуки. Вследствие недостатка вычислительных возможностей автомобили более подвержены взлому, чем компьютеры. Ограниченные вычислительные возможности автомобилей также приводят к тому, что некоторые решения по кибербезопасности транспортных средств будут иметь слишком высокие накладные расходы [3].

3. Непредсказуемые сценарии атак и угроз. В автомобильную архитектуру можно проникнуть через множество различных точек входа, включая автомобильные базы данных, технологии удаленной связи и

автомобильные детали. Постоянно разрабатываются новые атаки, поэтому автопроизводителям трудно предугадать, где хакеры нанесут следующий удар [4].

Критический риск для жизни водителей и пассажиров: Даже если всего несколько датчиков будут дезинформированы или будет отправлено лишь небольшое количество нелегитимных сообщений, в автомобиле могут возникнуть неисправности, которые поставят под угрозу жизнь водителей, пассажиров и пешеходов.

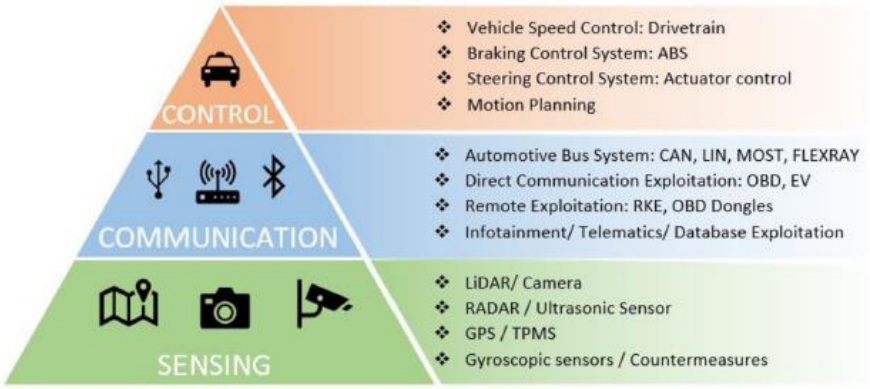


Рис.1. Структура AutoVSCC

Угрозы, направленные на автомобильные коммуникации, можно понять с помощью трехслойной структуры Autonomous Vehicular Sensing Communi-cation Control (AutoVSCC), представленной на рис. 1. В самом низу иерархии находится сенсорный уровень, который уязвим для спуфинга и атак на подслушивание датчиков автомобиля, таких как инерциальные или радарные датчики. Выше сенсорного уровня находится коммуникационный уровень, который охватывает как межтранспортные, так и внутритранспортные коммуникации и уязвим для атак подслушивания и манипулирования сообщениями между транспортными средствами и придорожной инфраструктурой. Коммуникационный уровень также подвержен угрозам, распространяющимся вверх от сенсорного уровня, состоящего из автомобильных датчиков. Угрозы для сенсорного и коммуникационного уровней могут повлиять на самый верхний уровень - уровень управления, который описывает автоматизированные методы управления автомобилем, такие как контроль скорости и рулевого управления [5].

Коммуникационный уровень состоит из автомобильных коммуникаций, которые могут быть как внутренними, так и внешними по отношению к автомобилю. Внутренние автомобильные коммуникации могут осуществляться в рамках бортовой сети. Бортовая сеть основана на взаимодействии множества электронных блоков управления (ЭБУ), входящих в состав электронных подсистем автомобиля.

Внешние автомобильные коммуникации возникают при непосредственном подключении автомобилей к USB-накопителям и средствам технического обслуживания, удаленном подключении к системам дистанционного без ключевого доступа, а также в процессе коммуникаций, обеспечивающих передачу сообщений между автомобилями и инфраструктурой.

Рис. 2. Типы обучения

Программные решения в области кибербезопасности с использованием машинного обучения Достижения в области машинного обучения (ML) и глубокого обучения (DL) привели к изменению парадигмы разработки программного обеспечения. В программных решениях, основанных на ML и DL, наиболее важными компонентами являются не алгоритм/модель, а наличие данных, которые могут быть использованы для обучения модели выполнению полезных функций [6]. К счастью, ежедневно генерируются и хранятся сотни терабайт оперативных и диагностических данных из обширной географической зоны, которые могут стать отличным ресурсом для разработки решений кибербезопасности нового поколения для автомобильных платформ. При этом решения, основанные на классических статистических моделях и логике, основанной на правилах, не смогут в полной мере использовать данные в таких масштабах.

Как показано на рис. 2, ниже приведен обзор типов обучения и их применимости в кибербезопасности автомобилей:

– Supervised ML: Простейшим решением для обнаружения аномалий является использование существующей автомобильной базы данных с лабельным набором данных (например, набором чистых и аномальных CAN-сообщений) для обучения классификационной модели ML. Эти же модели могут быть переобучены на различных автомобильных платформах с использованием нового набора данных.

– Unsupervised ML: Супервизорное обучение зависит от наборов данных, помеченных человеком, которые могут быть недоступны, а их создание часто требует больших затрат. Используя неконтролируемое обучение, мы можем создавать кластеры из различных потоков данных в автомобиле (например, телеметрических данных от ЭБУ), которые затем могут быть проанализированы для обнаружения аномального поведения. Алгоритмы кластеризации типа k-means могут быть достаточными для потоков данных с небольшим количеством признаков. Для отражения нелинейных связей в потоках данных с сотнями признаков требуются глубокие генеративные модели, такие как автоэнкодеры (АЭ) и вариативные автоэнкодеры (ВАЭ).

– Обучение с подкреплением: По сравнению с супервизорным и не супервизорным обучением алгоритмы обучения с подкреплением (RL) менее развиты. Однако некоторые из наиболее заметных достижений в области машинного обучения были связаны именно с обучением с подкреплением. RL предоставляет возможность разработки автономных решений по кибербезопасности, которые могут принимать на вход метацели, определяемые человеком (например, сокращение случаев ручного управления человеком-водителем в самодвижущемся автомобиле), и принимать решения для достижения этой цели. Решение на основе RL взаимодействует с окружающей средой, изучает ее и принимает решения, используя полученные знания [7].

Ключевыми задачами при разработке решений по кибербезопасности на основе ML являются определение

а) типа задачи (например, классификация, регрессия),

б) типа обучения (например, контролируемое, неконтролируемое),

в) архитектуры модели (например, деревья, плотные, рекуррентные и т. д.)

Тип используемой ML-модели зависит в первую очередь от типа потока данных и наиболее значимых для решения задачи характеристик. Например, если эти характеристики представляют собой дискретные CAN-сообщения, то достаточно использовать нейронную сеть с плотной связью. В случае временных рядов данных (например, телеметрических данных, таких как скорость и обороты двигателя) необходимы модели, которые могут делать временные шаги во входном слое, такие как рекуррентные нейронные сети или одномерные нейронные сети. Отметим, что решение кибербезопасности на основе ML/DL не обязательно должно ограничиваться использованием одной архитектуры или одной модели. Мы можем использовать несколько архитектур в рамках одной модели и несколько моделей для разработки решения [8].

Обнаружение и изоляция аномалий (обнаружение вторжений) при обмене информацией между различными подсистемами или компонентами автомобильной системы является критически важной задачей (например, телеметрическая информация, передаваемая между ЭБУ и ADAS). Аномалии в потоке данных могут быть обнаружены путем:

а) обучения на основе правил путем оценки каждого измерения, полученного из предыдущих знаний;

б) перекрестной проверки параметров (например, скорости, GPS) в потоках данных от нескольких датчиков;

в) мониторинга потока данных в течение временного скользящего окна для обнаружения подозрительных тенденций.

Масштаб и разнообразие данных часто делают нецелесообразным написание вручную правил для обнаружения аномальных сигналов в каждом экземпляре потока данных. Одним из непосредственных применений контролируемого ML является замена алгоритмов обнаружения вторжений, основанных на правилах, написанных людьми-экспертами. Это позволит использовать возможности ML и глубокого обучения для поиска закономерностей в больших наборах данных.

СПИСОК ЛИТЕРАТУРЫ

1. Курчин В. О., Карев В. Ф. Безопасность транспортных средств, ее роль в решении проблем обеспечения безопасности дорожного движения // Автомобильный транспорт Дальнего Востока. 2018. № 1. С. 185-190. EDN YZIVDV.
2. Титова Н. К. Понятие и содержание терминов «транспортная безопасность» и «угроза транспортной безопасности»: теоретический аспект // Транспортное право. 2012. № 3. С. 30-33. EDN PCSZJF.

3. Blinov P. D., Klekovkina M. V., Kotelnikov E. V., Pestov O. A. Research of lexical approach and machine learning methods for sentiment analysis // Компьютерная лингвистика и интеллектуальные технологии : по материалам ежегодной Международной конференции «Диалог» : в 2 т., Бекасово, 29 мая – 02 июня 2013 г. Vol. 2, Вып. 12(19). Бекасово : Российский государственный гуманитарный университет, 2013. Pp. 51-61. EDN HWKYXO.
4. Галимов Р. Г. Основы алгоритмов машинного обучения - обучение с учителем // Аллея науки. 2017. Т. 1. № 14. С. 810-817. EDN ZTBUCH.
5. Хасанов Д. С., Свистунова А. С. Технология сбора данных в логистике // Системный анализ в проектировании и управлении : сборник научных трудов XXV Международной научной и учебно-практической конференции : в 3 ч. Санкт-Петербург, 13–14 октября 2021 г. Ч. 3. СПб. : Политех-Пресс, 2021. С. 275-279. DOI 10.18720/SPBPU/2/id21-377. EDN RRNLCN.
6. Свистунова А. С., Хасанов Д. С. Возможности автоматических транспортеров-погрузчиков и их использование при создании имитационной модели развития контейнерного терминала // Морские интеллектуальные технологии. 2020. № 4-1(50). С. 169-174. DOI 10.37220/MIT.2020.50.4.023.
7. Concept and Models of Information Application for Actions in Systems / A. Geyda [et al.] // Conference of Open Innovations Association, FRUCT. 2022. № 31. Pp. 407-415.
8. Svistunova A. S., Khasanov D. S. Improving the efficiency of traffic management in a metropolis based on computer simulation // Computing, Telecommunications and Control. 2021. Vol. 14. № 3. Pp. 33-42. DOI 10.18721/JCSTCS.14303. EDN OEBQIQ.

УДК 004.05 : 004.5

О СТРУКТУРЕ МОДУЛЕЙ КОММУНИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ «АИС ИТ КЛИНИКА»

Шипунов Илья Сергеевич, Ныркov Анатолий Павлович,
Ротнов Дмитрий Александрович, Шипунова Диана Алексеевна
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: shipunovis@gumrf.ru, kaf.koib@gmail.com, erikfrish@gmail.com, shipunovada@gumrf.ru

Аннотация. Приведены основные этапы разработки коммуникационных модулей «АИС ИТ клиника» ГУМРФ имени адмирала С. О. Макарова. Структура модулей позволяет наладить эффективную коммуникацию между акторами АИС.

Ключевые слова: АИС; телеграмм боты; почтовые боты; генерация отчетов; геолокация информационная безопасность.

ABOUT THE STRUCTURE OF COMMUNICATION MODULES FOR USERS OF «AIS IT CLINIC»

Shipunov Ilya, Nyrkov Anatoliy, Rotnov Dmitry, Shipunova Diana
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg,198035, Russia
e-mails: shipunovis@gumrf.ru, kaf.koib@gmail.com, erikfrish@gmail.com, shipunovada@gumrf.ru

Abstract. The main stages of the development of communication modules «AIS IT Clinic» GUMRF named after Admiral S.O. Makarov. The structure of the modules allows you to establish effective communication between AIS actors.

Keywords: AIS; telegram bots; mail bots; report generation; geolocation; information security.

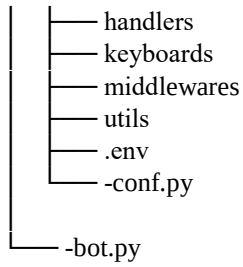
Введение. Для реализации проекта АИС «ИТ-Клиника» в защищенном исполнении необходимо было тщательно выбрать определенные технологии, языки программирования и расширения [1-6]. Это обусловлено тем, что разработка велась в модульном стиле, а, следовательно, каждый модуль имел свои специфические требования, которые определяли выбор соответствующих инструментов.

Важным аспектом разработки было обеспечение эффективного сотрудничества всех участников команды разработчиков. Для этого был создан специальный сервер на основе GitLab Community Edition. Он служил централизованной платформой для управления кодом, предоставляя доступ к нему только участникам команды разработчиков.

Первым этапом разработки АИС «ИТ-Клиника» стал модуль «Бот». Он был выбран как стартовый в связи с его объемностью и относительной независимостью от остальных частей системы.

После завершения разработки итоговая структура модуля «Бот» представляет собой следующую иерархию каталогов и файлов:

```
tg_bot
├── .Venv
├── core
│   ├── filters
```



Каждый из указанных каталогов и файлов имеет свое предназначение в структуре модуля:

– Корневая папка «tg_bot» содержит основные файлы и каталоги для работы бота;

– «.Venv» — виртуальное окружение Python, в котором установлены все необходимые для работы бота библиотеки и зависимости, в том числе основная библиотека aiogram.

– В каталоге «core» хранятся основные скрипты для работы бота:

– «filters» — каталог, включающий в себя фильтры для обработки входящих сообщений;

– «handlers» — каталог с обработчиками сообщений, которые определяют поведение бота в ответ на различные команды и запросы от пользователей;

– «keyboards» — каталог с набором клавиатур, используемых ботом для упрощения взаимодействия пользователя с ботом;

– «middlewares» применяется для обработки и преобразования сообщений до и после обработки обработчиками;

– «utils» — каталог с вспомогательными инструментами и функциями, используемыми в процессе работы бота;

– «.env» — файл с переменными окружения, в котором хранятся различные конфигурационные данные, такие как токены API, пути к базам данных и т. д.;

– «conf.py» — файл конфигурации для бота, содержащий настройки и параметры, используемые в работе бота, загружает в бота данные из файла с переменными окружения;

– «bot.py» — главный исполняемый файл, запускающий работу бота и подключающий к нему различные пакеты из каталога «core».

Файл «bot.py» служит центральным местом управления ботом. Он инициирует запуск и связывает все другие модули и функции вместе. Важным элементом этого файла является функция «start_bot()», которая отвечает за начало работы бота.

В самом начале функции настраивается логирование, чтобы отслеживать все, что происходит с ботом во время его работы. Затем функции «on_startup» и «on_shutdown» регистрируются как функции, которые должны быть вызваны при запуске и остановке бота соответственно.

Далее регистрируются промежуточные обработчики («middleware»), которые выполняются до или после обработки сообщения.

Затем регистрируются обработчики сообщений («handlers»), которые реагируют на различные входящие сообщения и команды от пользователей. Например, обработчик «message_handlers.start_handler» реагирует на команды «start», «run», «старт».

Особое внимание стоит уделить обработчикам «got_true_contact» и «got_fake_contact». Они будут вызываться при получении ботом контактной информации пользователя. Обработчик «got_true_contact» запустится, если информация будет соответствовать определенному критерию (проверяется с помощью фильтра «IsTrueContact()»), в противном случае будет вызван обработчик «got_fake_contact».

После регистрации всех обработчиков функция запускает поллинг — постоянный опрос Telegram на предмет новых сообщений. Когда бот заканчивает свою работу, его сессия закрывается.

Теперь о создании аудита и триггерной функции. Для мониторинга изменения статуса задач и своевременного оповещения пользователей была создана отдельная таблица «Tasks_audit» в базе данных. Эта таблица отслеживает любые изменения в таблице «Tasks». Бот постоянно проверяет эту таблицу на наличие новых записей для уведомления пользователей.

Для автоматического заполнения аудита была создана триггерная функция на языке PL/pgSQL. Эта функция активируется SQL-сервером при любых изменениях в таблице «Tasks».

Модуль «Почта» разрабатывался с использованием чистого PHP для отправки автоматических уведомлений пользователям при появлении новой записи в аудите задач. Почтовый сервер iRedMail использовался как надежный и проверенный инструмент для отправки электронной почты.

В рамках работы модуля «Почта» были разработаны различные функции для поддержки разнообразных задач, связанных с обработкой и отправкой электронной почты.

Взаимодействие с почтовым сервером осуществлялось через стандартные функции PHP для работы с SMTP. Соединение с сервером осуществляется с помощью функции «fsockopen()», которая устанавливает открытое интернет-соединение с сервером iRedMail.

Модуль «Почта» генерирует содержимое письма на основе события, произошедшего в системе, например, появления новой записи в аудите задач, который был описан выше. Для этого создается функция, которая принимает параметры, такие как адресат, тема письма и тело письма. Модуль «Почта» также следит за статусом отправленных сообщений. Если сообщение не было успешно доставлено, то модуль «Почта» пытается повторить отправку и ведет лог этих событий. В целом, модуль «Почта» обеспечивает надежную и автоматизированную отправку уведомлений пользователям о событиях, происходящих в системе, обеспечивая своевременное информирование и улучшая взаимодействие пользователей с системой, особенно тех пользователей, кто по тем или иным причинам не предпочитает уведомления через Telegram.

Для определения местоположения пользователя был создан модуль «Геолокация». Для реализации этой функции не требовались сторонние инструменты, так как встроенные возможности языка JavaScript позволяют запрашивать доступ к текущей геопозиции пользователя. При авторизации исполнителя в системе и попытке выполнения любого действия, открывается окно с запросом на предоставление доступа к геопозиции. После получения доступа широта и долгота пользователя отправляются на сервер для дальнейшей обработки с помощью AJAX.

В центре работы модуля находится функция geoscript_get_location(). Эта функция активирует встроенный в браузер функционал по работе с геопозицией. Этот код делает запрос к API геолокации браузера и в случае успешного получения данных формирует запрос к серверу с координатами пользователя. В случае неудачи пользователю выводится сообщение о необходимости предоставления доступа к геопозиции. Этот подход позволяет использовать возможности JavaScript для определения местоположения пользователя и соответствующего обмена данными с сервером.

В архитектуре проекта используется модель MVC (Model-View-Controller), что означает, что код, связанный с геопозицией, размещен в нескольких файлах, а именно в некотором контроллере и некоторой модели, даже может повторяться в нескольких похожих файлах для разных типов пользователей. В контроллере выполняется проверка на наличие переданных широты и долготы в POST-запросе, после чего эти данные передаются в модель для заполнения соответствующих полей в таблице «Students» базы данных. Модель, в свою очередь, получает эти данные и с помощью метода is_nearby() класса University проверяет, находится ли исполнитель в пределах здания ИВТ на Двинской.

Код контроллера отвечает за получение данных о геопозиции от клиента и передачу их модели для сохранения. Модель выполняет сохранение данных о геопозиции и статусе студента «рядом/не рядом» с университетом в базу данных.

Класс University содержит методы для расчета дистанции и проверки, находится ли исполнитель в заданной геолокации. Этот класс представляет собой реализацию функциональности по расчету дистанции между точками и определению, находится ли заданная точка в пределах определенного радиуса от центральной точки (в данном случае, это здание ИВТ на Двинской). Параметры университета на Двинской задаются в родительском контролере, на базе которого создаются остальные контролеры:

Для создания модуля «Генерация отчетов» было принято решение использовать библиотеку PHPWord, поскольку она предоставляет инструменты для генерации документов на основе шаблонов. Это позволяет быстро масштабировать функциональность модуля при необходимости добавления нового типа отчетов. В начальной стадии было создано два шаблона отчетов: отчет по группам, отсортированным по убыванию прогресса групп, и отчет по студентам, отсортированным по убыванию их персонального прогресса.

В качестве инструмента для установки библиотеки был выбран менеджер зависимостей Composer, являющийся широко используемым и удобным решением для языка PHP.

На стороне клиента, при нажатии на соответствующую кнопку, отправляется AJAX-запрос на сервер для формирования отчета указанного формата. Сервер, получив запрос, через контроллер обращается к модели для запуска модуля генерации отчетов («reports_generator.php»), где и происходит основная работа по созданию отчета. После формирования отчет отправляется клиенту в виде ответа на запрос и на клиентской стороне принимается как blob-объект, после чего начинается загрузка файла с расширением .docx. В файле «reports_generator.php» описывается класс «reports_generator», в котором определены методы для генерации отчетов различных типов.

Метод «make_students_report()» предназначен для генерации отчета по студентам. В этом методе формируется SQL-запрос, который выбирает данные о студентах и их прогрессе по практикам. Запрос составлен таким образом, чтобы каждый студент представлялся в отдельной строке.

После выполнения запроса результаты сохраняются в массив «$query_result». Далее с использованием библиотеки PHPWord и метода «cloneRowAndSetValues()» создается новый отчет, основанный на этих данных. В отчет также добавляется текущая дата и время, после чего он сохраняется в соответствующем файле с расширением .docx.

Метод «make_groups_report()» предназначен для генерации отчета, собирающего информацию о студентах по группам. Первый SQL-запрос извлекает данные о каждом студенте, включая его прогресс в выполнении практик. Эти данные затем сохраняются в массиве «$query_result». Второй SQL-запрос выделяет все группы из базы данных, результат этого запроса хранится в массиве «$groups_query_result».

Затем выполняется процесс преобразования исходных данных для подготовки к наполнению шаблона отчета. Все группы и соответствующие им студенты и их данные обрабатываются и сохраняются в массиве «$filling_data», который затем используется для заполнения шаблона отчета. Массив «$filling_data» содержит данные по каждой группе и студентам внутри нее. Если для группы нет данных о студентах, вставляется пустая строка.

Затем создается объект «TemplateProcessor» с шаблоном отчета, который будет заполняться данными из массива «$filling_data». Данные вставляются в документ во вложенном цикле для каждой группы и каждого студента в группе. Также в документ добавляется текущая дата и время, а затем отчет сохраняется в файле с расширением .docx.

Важным моментом является то, что метод «cloneRow» используется для создания множественных строк в документе на основе шаблона строки, и каждая строка затем заполняется данными о студентах.

Метод «make_groups_report()» возвращает отчет, организованный по группам, что может быть полезно для анализа общего прогресса группы в целом или для выявления студентов, которые отстают или превосходят в выполнении практик.

Функция «make_report(report_name)» находится на стороне клиента и служит для отправки AJAX-запроса к серверу с запросом на генерацию и последующее скачивание отчета. Вначале функция «make_report(report_name)» создает объект данных «data», содержащий одно свойство: имя отчета («report_name»). Затем эти данные кодируются в формат, который подходит для передачи в теле POST-запроса. Далее создается новый объект «XMLHttpRequest» и с его помощью на текущий URL («document.location.pathname») отправляется POST-запрос.

Установка «request.responseType» в ««blob»« указывает, что ответ сервера должен быть в формате Blob (Binary Large OBject), который подходит для передачи бинарных данных, таких как файлы. Событие «onreadystatechange» используется для обработки ответа сервера. Если запрос успешно выполнен (то есть «readyState» равен 4 и «status» равен 200), то создается новый Blob из ответа сервера.

Затем создается временная ссылка («dummy») на Blob-объект, которая затем симулирует клик мыши, заставляя браузер скачать файл. Файл сохраняется на компьютере пользователя под именем, указанным в параметре «dummy.download». Таким образом, этот код позволяет клиенту запросить отчет с сервера и скачать его в формате .docx.

Заключение. В статье этапы и ход разработки коммуникационных модулей «АИС ИТ Клиника».

Модуль «Бот» был создан с использованием языка программирования Python 3.11 и асинхронной библиотеки aiogram 3.0. Библиотека aiogram основывается на aiohttp и обеспечивает возможность написания эффективных и производительных ботов для Telegram. Модуль «Почта» был реализован на языке PHP. Для отправки сообщений от собственного доменного имени использовался сервер iRedMail.

Это решение позволило обеспечить уверенную и надежную работу функционала почты. Модуль «Геолокация» был разработан на языке JavaScript. Этот скрипт обеспечивает доступ к текущему местоположению пользователя с помощью встроенного функционала браузеров. Обработка запроса с позицией пользователя на стороне сервера осуществлялась с использованием PHP. Модуль «Генерация отчетов» был создан с использованием языка PHP, менеджера пакетов Composer и библиотеки phpword версии 1.0.

Важно отметить, что в каждом модуле присутствует код на языке SQL, так как он обеспечивает взаимодействие с базой данных системы, что необходимо для чтения и записи данных.

СПИСОК ЛИТЕРАТУРЫ

1. Sokolov S. S., Glebov N. B., Antonova E. N., Nyrkov A. P. The Safety Assessment of Critical Infrastructure Control System // Proceedings of the IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies», IT and QM and IS. 2018. 5 November. Pp. 154-157.
2. Нырков А. П., Каторин Ю. Ф., Нырков А. А. Обеспечение безопасной передачи информации по открытым каналам на транспорте // Сборник тезисов докладов национальной ежегодной научно-практической конференции профессорско-преподавательского состава ГУМРФ имени адмирала С. О. Макарова. СПб. : Изд-во ГУМРФ им. адм. С. О. Макарова, 2016. С. 47–49.
3. Zhilenkov A, Chernyi S., Sokolov S., Nyrkov A. Algorithmic approach of destabilizing factors of improving the technical systems efficiency // Vibroengineering Procedia. 2017. Pp. 261-265.
4. Гаскаров В. Д., Голоскоков К. П., Нырков А. П. Использование средств интеллектуальной поддержки при разработке защищенных систем обработки информации // Сборник тезисов докладов национальной ежегодной научно-практической конференции профессорско-преподавательского состава ГУМРФ имени адмирала С. О. Макарова. СПб. : Изд-во ГУМРФ им. адм. С. О. Макарова, 2016. С. 14–15.
5. Нырков А. П., Соколов С. С., Башмаков А. В. Методика проектирования безопасных информационных систем на транспорте // Проблемы информационной безопасности. Компьютерные системы. № 3, 2010. С. 58-61.
6. Соколов С. С., Нырков А. П., Ковальногова Н. М., Мамунц Д. Г., Пастушок Е. М. Методы обеспечения информационной защищенности данных электронной информационно-образовательной среды университета // Региональная информатика и информационная безопасность. СПб. : СПОИСУ, 2017. Вып. 4. С. 309–312.

УДК 004.05 : 004.5

РЕАЛИЗАЦИЯ МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЯ «АИС ИТ КЛИНИКА»

Шипунов Илья Сергеевич, Ныркov Анатолий Павлович, Шипунова Диана Алексеевна
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: shipunovis@gumrf.ru, kaf.koib@gmail.com, shipunovada@gumrf.ru

Аннотация. Рассматриваются механизмы обеспечения информационной безопасности веб-приложения «АИС ИТ клиника». Безопасность работы компонентов приложения обеспечивается параметризованные SQL запросами, проверенными и безопасными библиотеки и API, применением технологий шифрования SSL/TLS и HTTPS, резервным копированием и контролем доступа к базе данных.

Ключевые слова: SSL/TLS; DDoS; SQL injection; Content Security Policy; xss; GitLab.

ON THE IMPLEMENTATION OF MECHANISMS TO ENSURE INFORMATION SECURITY OF COMMUNICATION MODULES BETWEEN USERS OF «AIS-IT-CLINIC»

Shipunov Ilya, Nyrkov Anatoliy, Shipunova Diana
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: shipunovis@gumrf.ru, kaf.koib@gmail.com, shipunovada@gumrf.ru

Abstract. The mechanisms for ensuring information security of the web application «AIS IT Clinic» are considered. The security of the application components is ensured by parameterized SQL queries, proven and secure libraries and APIs, the use of SSL/TLS and HTTPS encryption technologies, backup and database access control.

Keywords: SSL/TL; DDoS; SQL injection; Content Security Policy; xss; GitLab.

Введение. Обеспечение безопасности на уровне веб-приложения включает в себя создание безопасного кода, включая валидацию ввода, использование параметризованных запросов для предотвращения SQL-инъекций, и применение безопасных API и библиотек [1]. Важной составляющей является также система аутентификации и авторизации для контроля доступа к функциям веб-приложения, которая может использовать сессии, токены, двухфакторную аутентификацию и контроль доступа на основе ролей [2, 3].

Защита баз данных направлена на обеспечение безопасности хранящихся в ней данных [4]. Использование шифрования [5], резервного копирования [6] и контроля доступа помогает обеспечить целостность и конфиденциальность данных [7]. Предотвращение SQL-инъекций с помощью параметризованных запросов и валидации ввода, а также мониторинг и аудит для выявления подозрительной активности также являются важными составляющими защиты баз данных [8].

Безопасность на уровне пользовательского интерфейса обеспечивается применением различных мер на стороне пользователя. Использование HTTPS для безопасной передачи данных, токенов CSRF для защиты от межсайтовой подделки запросов и Content Security Policy (CSP) для защиты от межсайтового скриптинга важны для обеспечения безопасности взаимодействия пользователя с приложением.

Модули «Бот» и «Почта» играют важную роль в АИС ИТ-клиника, обеспечивая своевременное информирование. Однако, такие модули также могут стать объектами для атаки. Угрозы и уязвимости для этих модулей могут включать в себя перехват данных, попытка атаки вредоносным программным обеспечением, атаки с целью отказа в обслуживании и прочее.

Для обеспечения безопасности модулей «Бот» и «Почта» применяются различные методы. Во-первых, эти модули запускаются как изолированные серверы в отдельных докерконтейнерах. Это обеспечивает изоляцию модулей друг от друга и повышает устойчивость основной системы, поскольку атаки на почту и бот не влияют на работу основного приложения.

Во-вторых, для обеспечения целостности данных используется таблица аудита «Tasks_audit» в базе данных. Это позволяет отслеживать все изменения в таблице «Tasks» и в случае необходимости восстановить данные. Утеря данных из таблицы «Tasks» становится менее вероятной. На данный момент реализован аудит только для задач, но в будущем можно на шаблоне уже созданного аудита и триггерной функции с небольшой корректировкой кода создать похожий функционал для остальных таблиц [9].

Также важно упомянуть о соблюдении законодательства о защите персональных данных. При работе с ботом пользователь дополнительно даёт согласие на обработку своих персональных данных в соответствии с 152-ФЗ, что обеспечивает законность обработки информации и защищает интересы пользователей (рис. 1).

Обеспечение безопасности модулей «Бот» и «Почта» включает в себя использование изоляции модулей от основной системы, наличие аудита данных, а также соблюдение законодательства о защите персональных данных.

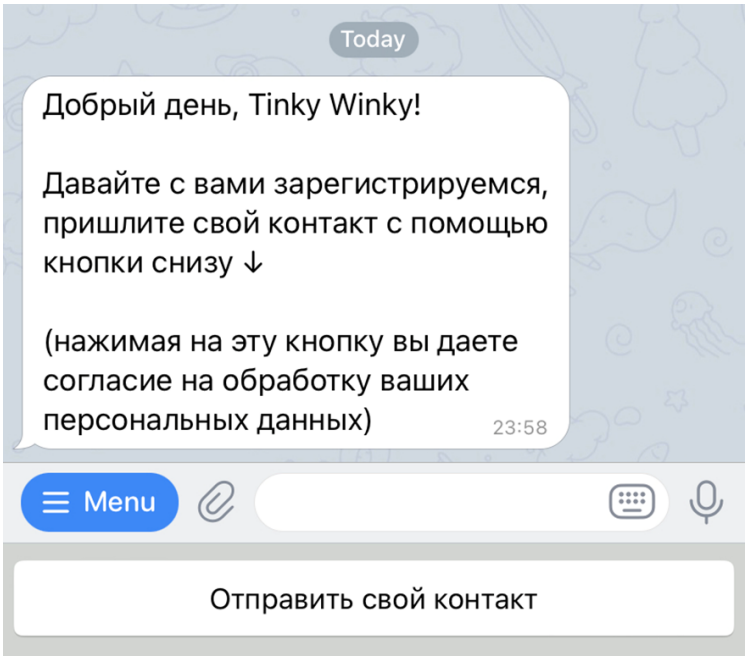


Рис. 1 Согласие на обработку ПДн.

Модуль «Геолокация» в АИС ИТ-клиника определяет местонахождение пользователя, т.е. находится ли пользователь в пределах университета. Такой модуль может быть подвержен угрозам и уязвимостям, связанным с приватностью и конфиденциальностью. Угрозы могут включать несанкционированный доступ к геолокационным данным пользователя, фальсификацию геолокационных данных, а также отказ в обслуживании.

Для обеспечения безопасности модуля «Геолокация» используются несколько методов.

Во-первых, обеспечивается безопасность на транспортном уровне с помощью технологии SSL/TLS. Это гарантирует, что все передаваемые между клиентом и сервером данные зашифрованы и не могут быть перехвачены или прочитаны третьей стороной. Для использования SSL/TLS у веб-сайта должен быть установлен доверенный SSL-сертификат, который подтверждает его подлинность и обеспечивает безопасное соединение.

Во-вторых, для обеспечения приватности пользователя, в базе данных не хранятся конкретные геолокационные данные, такие как широта и долгота. Вместо этого, в базе данных хранится лишь булево значение, указывающее, находится ли пользователь в пределах университета. Это исключает возможность утечки геолокационных данных и гарантирует конфиденциальность информации о местоположении пользователя.

В целом, безопасность модуля «Геолокация» обеспечивается за счет использования технологии SSL/TLS для защиты данных на транспортном уровне, а также путем ограничения хранения геолокационных данных на уровне базы данных.

Модуль «Генерация отчетов» представляет собой критически важный компонент системы, так как обрабатывает и агрегирует большое количество данных. Вместе с тем он подвержен целому ряду угроз и уязвимостей. К ним относятся: угроза SQL-инъекции, угроза несанкционированного доступа к данным, угроза модификации данных в отчете и угроза вставки злонамеренного кода.

Существуют различные меры безопасности, которые можно применить для обеспечения защиты модуля «Генерация отчетов».

Во-первых, для предотвращения SQL-инъекций используются параметризованные запросы. Это означает, что значения, вводимые пользователем, передаются в запрос отдельно от самого SQL-кода, что обеспечивает безопасность от инъекций.

Во-вторых, безопасность на уровне транспорта гарантируется благодаря использованию SSL/TLS. Эта технология обеспечивает шифрование данных, передаваемых между клиентом и сервером, и предотвращает их перехват третьими лицами.

Кроме того, для обеспечения безопасности на уровне приложения используется протокол HTTPS. Он обеспечивает защиту данных при передаче между клиентом и сервером за счет шифрования.

В долгосрочной перспективе для обеспечения целостности данных в отчетах планируется использование электронной подписи. Сервисы CryptoPro и VipNet рассматриваются как возможные варианты для реализации этой функции. Они оба сертифицированы ФСБ, но CryptoPro не предоставляет бесплатных лицензий, лишь пробную версию на 90 дней. VipNet предлагает бесплатную персональную лицензию, которая вполне подойдет для администратора.

Таким образом, обеспечение безопасности модуля «Генерация отчетов» включает в себя несколько слоев: защиту от SQL-инъекций, безопасность на транспортном уровне и уровне приложения, а также планируется использование электронной подписи для обеспечения целостности данных.

Заключение. В процессе разработки и внедрения АИС «ИТ-Клиника» были использованы передовые методы и технологии обеспечения информационной безопасности. Например, в разработке применялись параметризованные SQL запросы для предотвращения SQL-инъекций, использовались проверенные и безопасные библиотеки и API. Для обеспечения безопасности передачи данных применялись технологии шифрования SSL/TLS и HTTPS. Для обеспечения конфиденциальности пользовательских данных применялись шифрование, резервное копирование и контроль доступа на уровне базы данных. На уровне пользовательского интерфейса использовались механизмы защиты от межсайтовой подделки запросов (CSRF) и межсайтового скриптинга (XSS) с использованием Content Security Policy (CSP).

СПИСОК ЛИТЕРАТУРЫ

1. Михеева О. И., Гатчин Ю. А., Савков С. В., Хамматова Р. М., Ныркov А. П. Методы поиска аномальных активностей веб-приложений // Научно-технический вестник информационных технологий, механики и оптики. СПб., 2020. Т. 20. № 2. С. 233–242.
2. Ерисова А. Д., Ныркov А. П. Возможности цифровых сертификатов при аутентификации // Информационные управляющие системы и технологии (ИУСТ–Одесса–2020). Материалы IX международной научно-практической конференции. О., 2020. С. 87–91.
3. Ерисова А. Д., Ныркov А. П. О применении цифровых сертификатов как средства аутентификации в транспортно-логистических компаниях // Материалы конференции «XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Ч. 1. Санкт-Петербург, 28-30 октября 2020 г. СПб. : СПОИСУ, 2020. С. 343–345.
4. Nyrkov A. P., Glebov N. B., Novoselov R. O., Alimov O. M., Chernyi S. G. Databases Problems for Maritime Transport Industry on Platform Highload // Proceedings of the IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies», IT and QM and IS 5 November 2018, 2018. Pp. 132-135.
5. Ныркov А. П., Романова Ю. Н., Янюшкин К. А. К вопросу о применении отечественных алгоритмов шифрования // Сб. тр. «Региональная информатика и информационная безопасность». Вып. 2 СПб. : СПОИСУ, 2016. С. 117–120.
6. Ныркov А. П., Черняков А. В. Алгоритмы резервного копирования для обеспечения защиты данных // IX Санкт–Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР–2015). СПб .: СПОИСУ, 2015. С. 127-128.
7. Ныркov А. П., Вайгандт Н. Ю. Контроль целостности данных при мониторинге транспортных средств // Журнал университета водных коммуникаций. 2013. № 1. С. 54-61.
8. Mikheeva O. I., Gatchin Yu. A., Savkov S. V., Khammatova R. M., Nyrkov A. P. Search methods for abnormal activities of web applications // Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 2020. 2020. Vol. 20. № 2. Pp. 233–242.
9. Ныркov А. П., Рудакова С. А. Методика аудита объектов информатизации по требованиям информационной безопасности // Журнал университета водных коммуникаций. 2012. № 3. С. 146-149.

УДК 005.5:005.92

СИСТЕМА ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ АВТОМАТИЧЕСКОГО ПОДБОРА ИСПОЛНИТЕЛЯ НА ПРИМЕРЕ «АИС ИТ КЛИНИКА»

Шипунов Илья Сергеевич, Ныркov Анатолий Павлович, Шипунова Диана Алексеевна
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: shipunovis@gumrf.ru, kaf.koib@gmail.com, shipunovada@gumrf.ru

Аннотация. Рассматриваются современные подходы к созданию АИС с автоматическим подбором исполнителя. Подобные системы могут быть применены в рамках безэкипажного судоходства, с целью оказания своевременной и квалифицированной технической поддержки прибывающим безэкипажным судам. Построение подобной системы рассматривается на примере разработки «АИС ИТ-Клиника», так как разнообразие входящих задач требует подбора исполнителя с разными компетенциями.

Ключевые слова: АИС; безэкипажное судоходство; автоматический подбор исполнителей.

TECHNICAL SUPPORT SYSTEM FOR AUTOMATIC SELECTION OF AN EXECUTOR ON THE EXAMPLE OF «AIS IT CLINIC»

Shipunov Ilya, Nyrkov Anatoliy, Shipunova Diana
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 7198035, Russia
e-mails: shipunovis@gumrf.ru, kaf.koib@gmail.com, shipunovada@gumrf.ru

Abstract. Modern approaches to creation of AIS with automatic selection of the contractor are considered. Such systems can be applied within the framework of crewless shipping in order to provide timely and qualified technical support to arriving crewless vessels. Construction of such system is considered on the example of «AIS IT-Clinic» development, as the variety of incoming tasks requires selection of an executor with different competencies.

Keywords: AIS; crewless shipping; automatic selection of executors.

Введение. Беспилотные технологии в настоящее время развиваются с невероятной скоростью, и многие страны уже начали использовать их в различных областях [1-5]. В России также существует национальный проект «Беспилотники», который направлен на развитие и внедрение беспилотных технологий в различные сферы жизни. Одной из проблем при безэкипажном судоходстве является сложность оказания квалифицированной технической поддержки электронных компонентов безэкипажных судов удаленно. Имеющиеся в текущем порту специалисты могут не обладать нужными компетенциями. Однако, если расширить радиус поиска, то нужный специалист скорее всего найдется. А если сообщить о его необходимости заранее, а подбор вести в автоматическом режиме, то ремонт может начаться гораздо быстрее.

Далее рассмотрим подходы к созданию АИС с автоматическим подбором исполнителя. Подобные системы могут быть применены в рамках безэкипажного судоходства с целью оказания своевременной и квалифицированной технической поддержки прибывающим безэкипажным судам. Построение подобной системы рассмотрим на примере разработки «АИС ИТ Клиника», так как разнообразие входящих задач требует подбора исполнителя с разными компетенциями.

В 2017 году в Российской Федерации была утверждена программа «Цифровая экономика Российской Федерации» (далее — Программа). Программой определены цели, задачи, направления и сроки реализации основных мер государственной политики по созданию необходимых условий для развития в России цифровой экономики, в которой данные в цифровом виде являются ключевым фактором производства во всех сферах социально-экономической деятельности, что является необходимым условием повышения конкурентоспособности страны, качества жизни граждан, обеспечения экономического роста и национального суверенитета [6].

Для управления программой определены пять базовых направлений развития цифровой экономики в России на период до 2024 года. К базовым направлениям отнесены: нормативное регулирование, кадры и образование, формирование исследовательских компетенций и технических заделов, информационная инфраструктура и информационная безопасность.

Важным аспектом реализации данной программы являются специалисты в сфере IT, которых готовят современные вузы. Развитие подходов к подготовке IT кадров сегодня задает тональность развитию и остальных направлений подготовки. Важной частью обучения на сегодняшний день является получение практических навыков [7-10]. Одной из новых форм в данной сфере образования является прохождение практики на базе IT клиники, созданной университетом.

Клиническая практика — это форма получения практических навыков без отрыва от учебного процесса для решения задач, поставленных клиентом (сотрудником университета, преподавателем).

В ходе работы клиники в первый месяц стало очевидно, что для эффективного управления данным подразделением необходимо создать Автоматизированную информационную систему — АИС «ИТ клиника». Это обусловлено огромным количеством участников клиники при управляющем составе из двух человек — делопроизводителя и руководителя.

Перед началом разработки были описаны основные типы пользователей системы (Рис. 1).

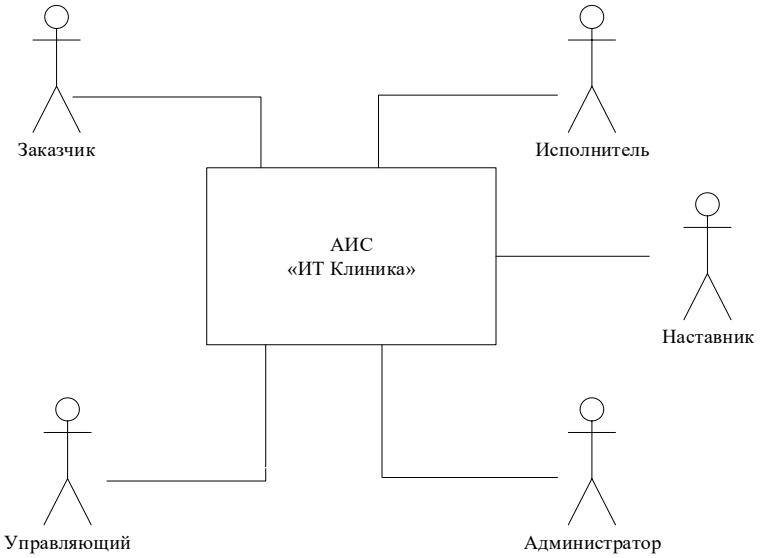


Рис. 2. Основные типы пользователей.

Администратор — выполняет функции по настройке системы, занимается исправлением и доработкой системы, тестированием и введением в эксплуатацию новых модулей, проводит инструктаж новых пользователей системы. В обязанности администратора входит обслуживание сервера, на котором развернута система.

Управляющий выполняет функции обработки задачи, проводит оценку необходимых для выполнения данной задачи параметров исполнителя, определяет наставника для задачи, обрабатывает отчеты, выданные системой. В случае необходимости Управляющий связывается с заказчиком для уточнения информации по задаче, вносит в систему новых Исполнителей и новых Наставников, выполняет ряд организационных задач по контролю активности Исполнителей и их верификации.

Заказчик выполняет функции по первичной постановке задачи, загружает в систему техническое задание на работу, устанавливает сроки выполнения задачи.

Исполнитель — обучающийся, зарегистрировавшийся в системе ИТ клиники и прошедший верификацию, выполняет задачи, поставленные системой, получая новые навыки, делает пометки о ходе выполнения задачи.

Наставник — преподаватель, руководитель практики, обладающий знаниями и навыками для помощи Исполнителю в решении поставленной задачи. Задача наставника — добавить к рабочему процессу обучающую составляющую. Также на наставника, при необходимости, может быть возложена задача первичного контроля качества исполнения задачи Исполнителем и подтверждение получения Исполнителем в ходе работы над задачей навыков, знаний и умений, указанных Управляющим.

В соответствии с типами пользователей система должна включать в себя модули, представленные на рис. 2.

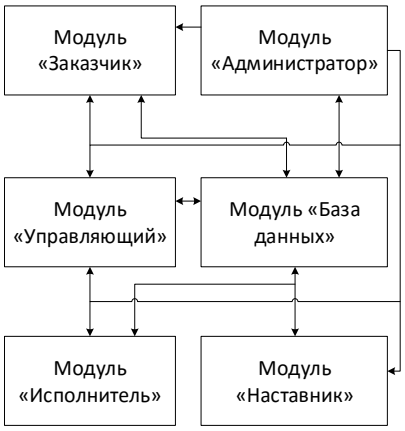


Рис. 3. Модули АИС

Модуль «Заказчик» содержит в себе необходимый инструментарий для работы Заказчика с системой. Основные инструменты представлены на рис. 3.

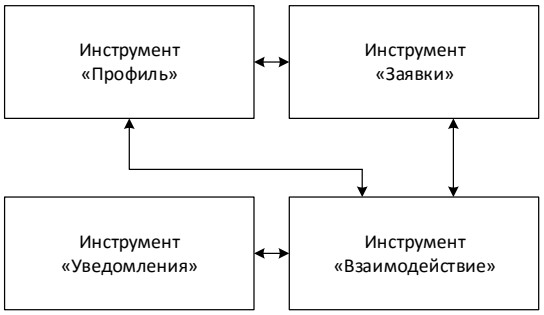


Рис. 4. Модуль заказчик

Инструмент «Профиль» позволяет Заказчику единожды указать свои данные, которые будут связаны со всеми его заявками и помогут связаться с ним в случае необходимости.

Инструмент «Заявки» предназначен для отображения информации по состоянию всех заявок от данного пользователя. Стоит отметить, что некоторые заявки на ИТ клинику могут быть переадресованы Управлением информатизации. В этом случае, при правильном заполнении профиля, данные заявки также будут доступны здесь. Также в этом инструменте реализован механизм подтверждения приема результатов работы с помощью цифровой рукописной подписи.

Инструмент «Уведомления» предназначен для настройки уведомлений Заказчика о ходе выполнения заявки в формате push-уведомлений. Также может быть настроена интеграция с корпоративной почтой, ВКонтакте, Telegram.

Инструмент «Взаимодействие» напрямую недоступен Заказчику и призван выступать неким коннектором между всеми инструментами модуля и модулем «База данных».

Модуль «Исполнитель» содержит в себе необходимый инструментарий для работы Исполнителя с системой. Основные инструменты представлены на рис. 4.

Рис. 5. Модуль Исполнитель

Инструмент «Профиль» в модуле «Исполнитель» позволяет обучающемуся, зарегистрировавшись единожды заполнить свои данные с указанием принадлежности к своей студенческой группе. Это позволит автоматизированной системе на основе алгоритма подбора включать его в список претендентов на выполнение задач, соответствующих освоению необходимых навыков и умений на основе учебных программ, осваиваемых обучающимся в данный период обучения. Также инструмент позволит указать навыки и умения, которые не входят в рабочие программы, уже освоенные обучающимся самостоятельно. Это позволит расширить спектр задач, до которых может быть допущен Исполнитель. Данный инструмент автоматически будет дополнять уже имеющийся перечень навыков у Исполнителя на основе данных об успеваемости (результатах промежуточной аттестации) и выполненных задач в рамках работы в ИТ клинике.

Инструмент «Текущая задача» позволит взаимодействовать с текущей задачей, вести учет рабочего времени, делать записи о ходе работы. В инструменте предусмотрена возможность связи с наставником по задаче через инструмент «Чат». По окончании выполнения задачи для подтверждения Инструмент «Текущая задача» запросит Исполнителя поставить свою цифровую рукописную подпись.

Инструмент «Журнал» служит для отображения всех задач Исполнителя. Данный инструмент позволит быстро и эффективно составить дневник практики обучающегося, соответствующий всем требованиям образовательной организации, даст возможность провести с наставником различные процессы, посвященные рефлексии и работе над ошибками. История выполнения тех или иных задач позволит пополнять базу знаний.

Инструмент «Достижения» является элементом геймификации процесса работы Исполнителя. Здесь в соответствии с рабочими программами практик автоматически будут установлены наборы целевых показателей — количество часов, индикаторы и компетенции. Это эффективный механизм, не только позволяющий правильно распределять задачи между Исполнителями, но и реализующий элементы стимулирования Исполнителя достичь нужных показателей.

Инструмент «Чат» в общем случае служит для обмена информацией между Наставниками и Исполнителями, а также для связи с другими Исполнителями. Данный элемент позволяет получить доступ ко всем ранее открытым чатам. Также инструмент позволяет выделить чат по конкретной задаче и обеспечить взаимодействие с ним инструменту «Текущая задача».

Инструмент «База знаний» содержит в себе информацию справочного характера: методические рекомендации, инструкции и опыт выполнения всех задач. Данный инструмент позволит получить не только помощь в выполнении Исполнителем поставленной задачи, но и в получении знаний, исходя из опыта других Исполнителей.

Инструмент «Распределение» предназначен для механизма подбора Исполнителя для задачи. Данный механизм позволит Исполнителю самостоятельно принять решение: браться за задачу или нет. В данный

инструмент задача «без Исполнителя» будет передана автоматически системой, на основании удовлетворения параметров профиля Исполнителя всем требованиям, установленным к задаче Управляющим. Также инструмент с определенным периодом проверяет геопозицию Исполнителя для того, чтобы система знала, находится ли Исполнитель на какой-либо площадке вуза или нет.

Инструмент «Взаимодействие» аналогичен по назначению инструменту, описанному в модуле «Заказчик».

Модуль «Наставник» содержит в себе необходимый инструментарий для работы Наставника с системой. Основные инструменты представлены на рис. 5.

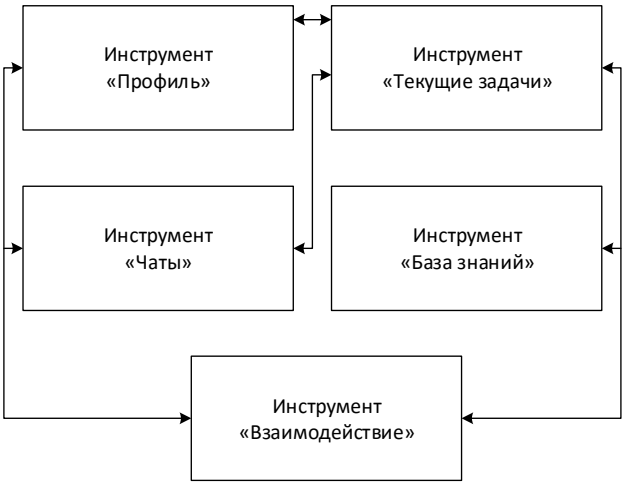


Рис. 6. Модуль Наставник

Все инструменты данного модуля по функциональности и назначению соответствуют одноименным инструментам, описанным выше с той лишь разницей, что ориентированы на Наставника.

Модуль «Управляющий» содержит в себе необходимый инструментарий для работы Управляющего с системой. Основные инструменты представлены на рис. 6.

Инструменты «Заказчики», «Исполнители» и «Наставники» предназначены для работы с информацией о соответствующих участниках системы.

Инструмент «Заявки» служит для определения параметров подбора Исполнителя заявки. Только в случае грамотного описания параметров уровня знаний Исполнителя, а также навыков и умений, приобретаемых Исполнителем в ходе решения заявки, система в автоматизированном режиме подберет кандидатов и предложит им выполнение данной задачи. Также немаловажным аспектом является определение срочности выполнения. Этот параметр необходим для определения базового уровня Исполнителя. Алгоритм подбора исполнителя будет описан ниже.

Рис. 7. Модуль Управляющий.

Инструмент «Отчеты и документы» предназначен для автоматической сборки различных отчетов и документов, шаблоны которых будут загружены в систему. Для удобства дальнейшей обработки предусмотрен

вывод в формате *.docx. Одним из важных отчетов является отчет об активности Исполнителей. Именно он поможет Управляющему обратить внимание на простой некоторых Исполнителей и невыполнение ими плановых показателей. Это поможет своевременно принять меры организационного характера. На основании данного отчета могут быть сформированы списки самых активных Исполнителей для их поощрения.

Инструмент «Планировщик» поможет Управляющему работать в соответствии с планом работы ИТ клиники. План формируется в начале года. Управляющий может добавлять в план текущие дела.

Инструмент «Взаимодействие» аналогичен по назначению инструменту, описанному в модуле «Заказчик».

Модуль «База данных» содержит в себе набор утилит для управления базой данных системы, а также инструмент «Взаимодействие».

Модуль «Администратор» позволяет администратору получить доступ ко всем инструментам с возможностью подмены своей роли на другую. Возможные роли: Р0 — Администратор; Р1 — Управляющий; Р2 — Заказчик; Р3 — Наставник; Р4 — Исполнитель.

В таблице 1 представлены обозначения инструментов системы.

Таблица 1

Кодировка инструментов

Инструмент	Обозначение
Взаимодействие	И0
Профиль	И1
Текущая задача	И2
Журнал	И3
Достижения	И4
Чат	И5
База знаний	И6
Распределение	И7
Заявки	И8
Уведомления	И9
Заказчик	И10
Исполнитель	И11
Наставники	И12
Отчеты и документы	И13
Планировщик	И14

Доступность инструментов в зависимости от подменной роли определяется в таблице 2.

Таблица 2

Доступность инструментов в подменных ролях

	Р1	Р2	Р3	Р4
И0	+	+	+	+
И1			+	+
И2			+	+
И3				+
И4				+
И5			+	+
И6			+	+
И7				+
И8	+	+		
И9		+		
И10	+			
И11	+			
И12	+			
И13	+			
И14	+			

Алгоритм подбора исполнителя базируется на стратегии прямого отбора. В качестве определяющих признаков будут использоваться параметры, установленные в заявке Управляющим, а также отметка о том, на какой площадке находится Исполнитель (эти данные предоставляет инструмент «Распределение» модуля «Исполнитель»).

Стратегия алгоритма, следующая.

Шаг 1. Отсеять всех Исполнителей, не находящихся на требуемой площадке вуза.

Шаг 2. Отсеять всех Исполнителей со статусом «Занят»

Шаг 3. Отсеять всех Исполнителей, профиль которых не соответствует минимальным требованиям задачи. В случае если заявка срочная, исключить всех без «открытых» компетенции, на которые опирается данная задача.

Шаг 4. Выбрать тех Исполнителей, которым необходимо получить либо отработать знания, умения и навыки, предоставляемые в ходе выполнения данной задачи. В случае отсутствия таковых пропустить данный шаг.

Шаг 5. Разослать приглашения на выполнение данной заявки всем подходящим Исполнителям.

Шаг 6. После отклика Исполнителя удалить задачу из инструмента «Распределение», поместить ее в инструмент «Текущая задача» для откликнувшегося Исполнителя.

Такой алгоритм решения задачи позволяет получить оптимальное решение. Для того, чтобы удостовериться в этом, был сгенерирован набор Исполнителей и Задач с разной сложностью и срочностью. Затем алгоритму предлагалось выбрать для каждой из них Исполнителя. В качестве откликнувшегося выбирался случайный Исполнитель из итогового списка. Каждую итерацию подбора у случайного набора Исполнителей (до 50 %) устанавливался параметр «Занят» и «Не на площадке». В результате Алгоритм подобрал Исполнителей в 100 % случаев.

Заключение. По итогам проектирования было сформировано первичное техническое задание и стартовал сбор команды разработчиков. Отбор проходил среди студентов старших курсов IT направлений. По итогу набралось несколько команд, между которыми и был распределен фронт работы. В качестве среды коммуникаций была выбрана и развернута среда Mattermost. Выбор стоял между Mattermost и Slack, но определяющую роль сыграла стоимость. В качестве методологии производства был выбран KANBAN. На текущий момент создана база данных, а также набор утилит, обеспечивающих выдачу данных в требуемом формате для нужд инструментов «Чат», «База знаний», «Журнал», «Задача», «Профиль», «Достижения».

Клиническая практика — это важный элемент обучения новых кадров, полностью соответствующий программе «Цифровая экономика Российской Федерации». Это значит, что данный подход к подготовке кадров будет только набирать обороты, а разработки различных информационных систем только подстегнут этот процесс. Стоит отметить, что наряду с IT клиникой в Государственном университете морского и речного флота имени адмирала С.О. Макарова уже инициирована Юридическая клиника, а также запущены в разработку на ранней стадии Экономическая клиника (центр финансовой грамотности), строительная клиника и лингвистическая клиника. Автоматизированная система, о которой идет речь в данной статье, может быть применена и в этих подразделениях, а работы по доработке имеющихся в разработке новых необходимых инструментов может взять на себя IT клиника.

СПИСОК ЛИТЕРАТУРЫ

1. Butsanets, A., Ol'Khovik E. Development of Technical Means for Mooring the Unmanned Vessels, 2019.
2. Shipunov I. S., Nyrkov A. P., Ryabenkov M. U., Nyrkov A. A., Katorin Y. F. The Concept of a Partially Unmanned Sea Convoy // Proceedings of the IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus 2021 9396302. 2021. Pp. 661-664.
3. Shipunov I. S., Nyrkov A. P., Kardakova M. V., Katorin Y. F., Vychuzhanin V. V. Information System for Monitoring and Analyzing the Technical Condition of Autonomous Vehicles // Proceedings of the IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2020. Pp. 497-500.
4. Zhilenkov A. A., Sokolov S. S., Chernyi S. G., Nyrkov A. P. Intelligent autonomous navigation system for UAV in randomly changing environmental conditions // Journal of Intelligent and Fuzzy Systems. 2020. Vol. 38. № 5. Pp. 6619- 6625.
5. Shipunov I. S., Voevodskiy K. S., Nyrkov A. P., Katorin Y. F., Gatchin Y. A. About the Problems of Ensuring Information Security on Unmanned Ships // Proceedings of the IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2019. Pp. 339-343.
6. Цифровая экономика РФ [Электронный ресурс]. URL: https://digital.gov.ru/ru/activity/directions/858/?utm_referrer=https%3a%2f%2fwww.google.com%2f/ (Дата обращения: 07.08.2023).
7. Кардакова М. В., Ныркoв А. П., Цымай Ю. В. Концепция игрового тренажера по информационной безопасности на речном транспорте // Речной транспорт (XXI век). 2022. № 3 (103). 2022. С. 45–49.
8. Kardakova M. V. Nyrkov A. P., Tsymay Y. V. Water Transport Information Security Trainer Concept (final part) // XIII International Conference on Transport Infrastructure: Territory Development and Sustainability (TITDS-XIII 2022). Volume 68. Transportation Research Procedia 68. 2023. Pp. 372–382.
9. Shipunov I., Nyrkov A., Korotkov V., Alimov O., Knysh T. Principles of using modern IT trends in maritime shipping //иE3S Web Conf., 203 (2020) 05005 Published online: 2020-11-05.
10. Ныркoв А. П., Алексеев С. А., Стахно Р. Е. Структурно-функциональная модель обучающегося в системе тренажерной подготовки по судовождению // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. 2018. Т. 10. № 6. С. 1288-1298.

УДК 004.855.5

ПРИМЕНЕНИЕ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ В СЕТЯХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Юмашева Елена Сергеевна, Ныркoв Анатолий Павлович
Государственный университет морского и речного флота им. адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: kaf.koib@gmail.com, elena_umasheva@mail.ru

Аннотация. В статье исследуется возможность использования алгоритмов машинного обучения для обнаружения аномального поведения и вторжений в сетях, связанных с критической информационной инфраструктурой.

Ключевые слова: машинное обучение; автоматизированные системы; управление технологическими процессами; информационная безопасность; критическая информационная инфраструктура.

MACHINE LEARNING ALGORITHMS APPLICATION TO DETECT ABNORMAL BEHAVIOR IN CRITICAL INFORMATION INFRASTRUCTURE NETWORKS

Yumasheva Elena, Nyrkov Anatoliy
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St., St. Petersburg, 198035, Russia
e-mails: kaf.koib@gmail.com, elena_umasheva@mail.ru

Abstract. The article explores the possibility of using machine learning algorithms to detect anomalous behavior and intrusions in networks associated with critical information infrastructure.

Keywords: machine learning; automated systems; process control; information security; critical information infrastructure.

Введение. С появлением четвертой промышленной революции все производства перешли к внедрению информационных технологий в промышленность и автоматизации большинства бизнес-процессов, что в свою очередь открыло новые возможности: увеличение оборотов, выход на международный рынок, сокращение рабочих мест в особо опасных и токсичных условиях труда и многие другие преимущества. Однако Индустрия 4.0 привела и к росту кибератак на автоматизированные системы, входящие в состав критической информационной инфраструктуры (КИИ). Такие системы вызывают наибольший интерес у хакеров из-за возможности вымогать крупные суммы денег, влиять на ключевые сферы жизнедеятельности государства и общества (финансовый сектор, промышленность, транспорт, связь и т. д.). Несмотря на то, что разработано значительное количество систем обнаружения вторжения, предприятия по-прежнему сталкиваются с успешно проведенными атаками, которые традиционные системы IDS не могут выявить.

Данная статья направлена на выявление наиболее актуальных уязвимостей для автоматизированных систем управления технологическими процессами (АСУ ТП), а также на проведение анализа современных методов обнаружения вторжения, основанных на алгоритмах машинного обучения (МО).

Как было рассмотрено ранее, чем выше становится технологическая составляющая предприятия, тем больше оно подвержено атакам как внешним, так и внутренним. На рис. 1 представлен график, где отображена доля атак на промышленные предприятия от общего числа атак на организации.

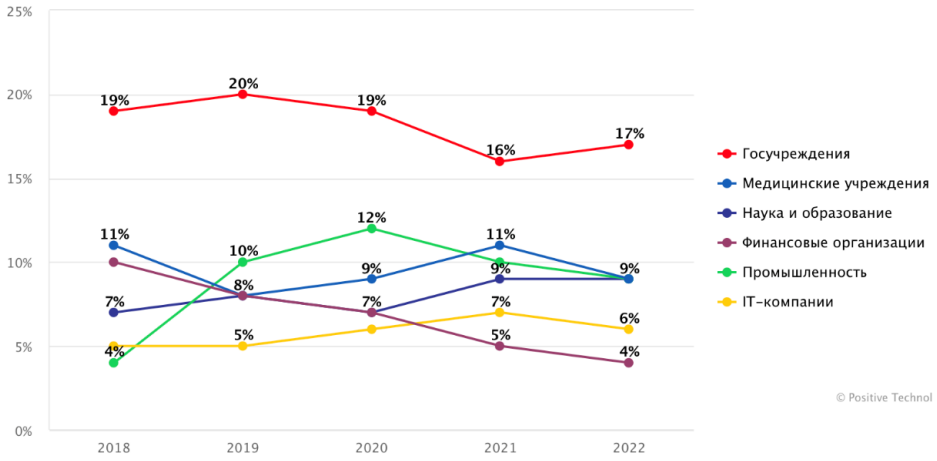


Рис. 1. Доля атак на промышленные организации (от общего числа атак на организации) [1]

Всего за 2022 год по данным Positive Technologies было официально зафиксировано на 7% (223) успешных инцидентов больше, чем в 2021. Среди общего количества атак 97% являлись целевыми. Например, одной из крупных атак в прошлом (2011 год) стала кибератака на иранский ядерный объект. Вредоносное программное обеспечение (далее — ПО) распространилось на все программируемые логические контроллеры (ПЛК), что привело к уничтожению существенного количества центрифуг [2, 3]. Если говорить о более свежих инцидентах, то стоит вспомнить о кибератаке на трубопроводы Colonial [4], обеспечивающие почти половину потребления топлива вдоль восточного побережья США. Компании пришлось приостановить свою деятельность на несколько дней, что естественно привело к росту цен на топливо, его нехватке и распространению панических настроений в обществе. Таким образом, можно наглядно увидеть к чему приводят «дыры» в безопасности автоматизированных систем управления технологическими процессами в рамках критической информационной инфраструктуры.

АСУ ТП — это совокупность аппаратно-программных средств, осуществляющих контроль и управление производственными и технологическими процессами [5]. Говоря иначе, это программируемые системы, используемые для мониторинга и регулирования производственных процессов. Построение АСУ ТП, в упрощенной схеме, состоит из 3-х уровней:

– верхний (SCADA, HMI);
– средний (ПЛК, регуляторы, программируемые реле, счетчики);
– нижний (датчики, сенсоры, исполнительные механизмы).

ПЛК программируются с использованием релейной логики. ПЛК имеет настраиваемую операционную систему, блоки функционального кода и данных, что, в свою очередь, служит отличной возможностью для проникновения в систему [6].

HMI (human-machine interface) — это устройства, требующие взаимодействия с человеком, для обеспечения безотказной работы системы, ее оптимизации и адаптации. Довольно часто на таких устройствах установлены облегченные популярные операционные системы (Windows, Unix), что служит приманкой для злоумышленников.

На нижнем уровне располагаются датчики и сенсоры, которые отвечают за передачу необработанных данных. Однако одной из главных проблем безопасности тут является то, что они не способны обеспечить аутентификацию или целостность передаваемых данных. Но ПЛК выстраивают свою логику управления процессами на основе данных, полученных от датчиков. Таким образом, на этом этапе взаимодействия мы также видим уязвимость (в случае подмены данных с датчиков, злоумышленник может существенно повлиять на изменение логики взаимодействия остальных процессов системы).

Также не стоит забывать про удаленные терминалы (Remote Terminal Units — RTU), которые зачастую располагаются в удаленных местах для мониторинга полевых устройств. ПЛК и RTU имеют довольно слабый уровень защищенности и могут быть подвержены таким атакам как искажение протокольных сообщений, обход аутентификации и манипуляции с данными. Как пример, можно привести инцидент, произошедший с компанией Industroyer в 2017 году.

Распространенные типы атак на АСУ ТП

Атаки на АСУ ТП могут быть как целенаправленные, так и нецеленаправленными. Первый тип атак готовится планомерно, т.е. проводится разведка с помощью инструментов Open Source Intelligence (OSINT), планирование действий (некоторые векторы внедрения в инфраструктуру могут соответствовать матрице MITRE ATT&CK) и подготовка при необходимости к физическому проникновению на объект. Например, одним из рабочих векторов атаки на такие объекты является «подавление функции управления». Так как целевые атаки не проводятся в один этап, то по определенным признакам система может отследить готовящуюся атаку и уведомить специалистов ИБ.

Нецелевые атаки обычно выполняются спонтанно и не имеют цели взломать тот или иной объект. Например, сканирование ботами сети привело к взлому учетной записи пользователя на веб ресурсе или уволенный сотрудник обнаружил, что специалисты IT не забрали у него доступ к корпоративной сети.

Автоматизированные системы обычно разрабатываются так чтобы их информационная безопасность зависела от своей среды. Уязвимые места в работе промышленных протоколов закрываются выделенной сетью, контролируемой оператором. Однако не всегда такая реализация возможна. Снижение уровня безопасности в сетях АСУ ТП происходит преимущественно из-за 3-х тенденций:

1. Конвергенция сетей. Сети перестают быть изолированными, взаимодействуют с компонентами автоматизации и, следовательно, область атак увеличивается. Например, если в АСУ ТП появляется облачная платформа, с возможностью управления различными компонентами через смартфон.
2. Устаревшие best practices. Устройства и приложения в среде АСУ ТП предназначены для длительного срока эксплуатации при обычном (рядовом) использовании, а не для устойчивости к сетевым атакам. Несмотря на передовые исследования, выпуск обновлений ПО, во многих средах по-прежнему остаются старые бэкдоры или происходит удаленное администрирование с помощью небезопасных протоколов (FTP, VNC, TeamViewer и др.).
3. Безопасность не является приоритетом в бизнес-процессах. Эта проблема касается абсолютно любого бизнес-процесса, так как в приоритет всегда ставится работоспособность того или иного приложения, из-за чего часто процессы запущены с повышенными привилегиями «все разрешено». Например, инженерные станции, на которых используется ПО для перепрограммирования ПЛК, плохо работают в многопользовательском режиме и должны быть доступны контрагентам в случае проведения плановых работ. Здесь обычные брандмауэры не будут эффективны, и для обнаружения вторжения потребуется понимание трафика на уровне протоколов.

На сегодняшний день исследователи в области ИБ фокусируются на конкретных типах атак АСУ ТП. Например, в работе [7] методы МО базируются на поиске атак в стеке протоколов АСУ ТП. Работа [8] основана на обнаружении ввода ложного набора данных, повторов и атаках с нулевой динамикой [9]. В работе [7] рассмотрены методы обнаружения, оценки и контроля атак в рамках 2х типов атак: отказ в обслуживании (DoS), атаки с подменой данных. В некоторых работах функционирование алгоритмов МО строится для более широкого спектра задач (обнаружение аномалий и программно-аппаратных сбоев) [10]. В таблице 1 приведено сравнение наиболее эффективных и популярных методов для конкретного пула атак.

Таблица 1

Алгоритмы машинного обучения

Алгоритмы МО	DoS	Ввод ложных данных	Разведка	Spoofing
k-Nearest neighbour [17]	+	+	+	+
Decision trees [18]	+	+	+	+
Bayes [19]	+	+	+	+
Artificial neural networks [20]	+	+	+	
Isolation forest [21]	+	+		
Deep belief network [22]	+	+	+	
Boosting [23]	+	+	+	

Машинное обучение — это прежде всего наука, изучающая алгоритмы, автоматически обучаемые на основе опыта.

Все решения записываются как алгебраические функции, которые отображают объекты в предсказания (цели). У функции нет единственно верного решения (например, каждый из переводчиков переводит текст по-разному, но оба таких перевода будут верными). Функция обучается на основе довольно большого количества верных/неверных примеров. Функция, отображающая модель в предсказания, называется моделью, а набор примеров — это датасет (обучающая выборка), которая состоит из объектов и ответов.

Алгоритмы (задачи) МО используются для изучения паттернов на основе входных данных для построения модели, которая в последствии может быть использована для распространения изученных паттернов.

Одним из популярных видов задач, является задача обучения с учителем (supervised learning). Такие алгоритмы используются при взаимодействии с простыми данными и признаками.

Ниже приведено 5 видов задач обучения с учителем [11]:

1. Регрессия. $Y = R$ или $Y = R^M$. Позволяет предсказать значение. Например, регрессия используется для предсказания роста атак
2. Бинарная классификация. $Y = \{0,1\}$. Позволяет предсказать категорию событий (конкретные угрозы в ИБ).
3. Многоклассовая классификация. $Y = \{1,\ldots,K\}$
4. Многоклассовая классификация с пересекающимися классами. $Y = \{0,1\}^K$.
5. Ранжирование. Y — конечное упорядоченное множество.

Алгоритмы машинного обучения с учителем позволяют выявлять загрузку вредоносного кода, фишинг, C2 инструменты и т д., но в таких моделях, как и в эвристических IDS мы должны дать на вход датасет, в котором четко размечены легитимные и вредоносные данные.

Но что, если невозможно четко разграничить весь объем данных и различные малвари выпускаются ежедневно в существенном объеме. В таком случае можно воспользоваться задачами обучения без учителя (unsupervised machine learning). В таких задачах известны только данные, а ответы либо неизвестны, либо не существуют. Одним из примеров таких задач может быть кластеризация. Задача разделения объектов на группы, обладающими определенными паттернами, например, можно искать структуру и зависимости в неразмеченных данных и делать выводы уже на их основе.

Следовательно, обучение с учителем позволит выявлять новые, но уже известные типы угроз, а обучение без учителя уделяет большее внимание утечкам данных, аномальному доступу, повышению привилегий и т д. Исходя из вышесказанного, МО позволяет сделать правильный вывод, опираясь на качественно сгенерированный датасет. Чем более разнообразнее обучающая выборка, тем точнее будет результат. Для генерации качественного датасета потребуется не только обработать довольно большой объем данных состоящий из сетевого трафика, URL, поведения пользователей, поведения вредоносов и т д., но и расставить метрики, чтобы система понимала разницу между шумом и полезными данными.

Современные алгоритмы МО, используемые в ИБ

Большинство подходов сочетают в себе больше 2 алгоритмов в целях повышения производительности.

Алгоритмы глубокого обучения представляют собой комбинацию алгоритмов с учителем и без. Глубокое обучение использует несколько уровней обработки для изучения получаемых данных с несколькими уровнями абстракции. Такие алгоритмы при правильном подборе датасета могут обеспечивать более точные результаты, чем традиционные алгоритмы МО. Широкое распространение в этом подвиде получили такие алгоритмы как: глубокие нейросети (Deep Neural Network) [12], свёрточная нейросеть (Convolutional neural network) [13], рекуррентная нейронная сеть (Recurrent Nerural Network) [14] и др.

Ансамблевое алгоритмы (EL) базируется на основе одного алгоритма МО, но обучение происходит несколько раз (каждый раз используется другая настройка параметров). Далее результаты объединяются для формирования единой модели. Следовательно, если предположить, что у каждого предсказания есть ошибка, то объединение двух и более

предсказаний может существенно ее уменьшить и снизить показатели ложного срабатывания. Примерами таких алгоритмов являются: Метод случайного леса (Random forest) [15]; Бэггинг (bootstrap aggregation) [16] и др.

В таблице 1 подобраны алгоритмы, использующие различные подходы к обучению и наглядно отображающие, как именно они справляются с атаками.

Показатели эффективности алгоритмов машинного обучения рассчитываются на основе 4 метрик:

– истинно положительный (кол-во верно обнаруженных экземпляров атак);
– истинно отрицательный (кол-во ложно обнаруженных экземпляров даных);
– ложно положительный (кол-во ложных срабатываний на экземпляры атаки);
– ложно отрицательный (кол-во ложных срабатываний на экземпляры данных).

Также немаловажными в алгоритмах МО являются такие метрики как:

1. Accuracy — доля верных предсказаний, т. е. с ее помощью можно определить долю верно обнаруженных атак и обычных экземпляров данных, но такая метрика не позволит найти долю неверно обнаруженных экземпляров.

2. Precision (предварительная точность) — представляет собой число объектов верно классифицированных как положительные, т.е. такая метрика позволит измерить долю успешных атак, но данный подход имеет низкую точность, а следовательно, и высокое число ложно положительных срабатываний.

3. Recall (полная) — рассчитывается как отношение числа положительных выборок, корректно классифицированных как положительные, к общему количеству положительных объектов. Такую метрику часто называют показателем чувствительности или мерой полноты.

4. Kappa (коэффициент Коэна) — используется для измерения надежности результатов обнаружения. Метрика полезна при оценке качества модели.

Заключение. Подводя итоги, можно выделить три критические проблемы, поставленные перед исследователями в области МО, в рамках ИБ АСУ ТП:

1. Ограниченные сценарии атак для оценки модели.

2. Ограниченный набор входных данных, а также трудоемкость генерации и проставление метрик в таком датасете.

3. Эффективность методов МО напрямую зависит от правильности и точности датасета.

Сочетание этих проблем привело к одной из наибольших трудностей, а именно, оценки реалистичности атак. Эффективность современных подходов не может быть точно оценена из-за ограничений в реальных атаках и датасетах. Также не существует стандартного набора показателей эффективности, благодаря которым было бы возможно измерить эти подходы. Из-за таких, казалось бы, незначительных проблем данному виду систем тяжело применить МО к своим предприятиям. Таким образом, становится очевидной необходимость в решении этих проблем не только в рамках разработки более эффективного детектора атак, но и для повышения надежности систем построенных с использованием МО.

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные киберугрозы для промышленных организаций: итоги 2022 года // Positive technologies, 2023 [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/industrial-cybersecurity-threatscape-2022/ (дата обращения: 04.07.2023).
2. Langner R. Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, 2011. Vol. 9. Issue 3. Pp. 49–51.
3. LeCun Y., Bengio Y., Hinton G. Deep learning. Nature, 2015. 521(7553). Pp. 436–444.
4. Case D. U. Analysis of the cyber attack on the ukrainian power grid. Washington DC: Electricity Information Sharing and Analysis Center (E-ISAC), 2016. 388 p.
5. Ныркov А. П., Соколов С. С., Шнуренко А. А. Автоматизированное управление транспортными системами : монография. СПб.: ГУМРФ им. адмирала С. О. Макарова, 2013. 325 с.
6. Зубанова А. А., Шипунов И. С., Ныркov А. П. О возможностях применения программируемых логических контроллеров для целей мониторинга состояния судового оборудования // XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября 2020 г. Ч. 1. : материалы конференции. СПб. : СПОИСУ, 2020. С. 345–348.
7. Maynard P., McLaughlin K., Sezer, S. Decomposition and sequential-and analysis of known cyber-attacks on critical infrastructure control systems // Journal of Cybersecurity, 2020. Vol. 6. Issue 1, DOI:10.1093/cybsec/tyaa020.
8. Cui L., Qu Y., Gao L., Xie G., Yu S. Detecting false data attacks using machine learning techniques in smart grid: A survey // Journal of Network and Computer Applications, 2020. 170(2):102808. DOI:10.1016/j.jnca.2020.102808.
9. Zero-dynamics Attack, Variations and Countermeasures // Cornell University, 2021. [Электронный ресурс]. URL: https://arxiv.org/abs/2101.00556 (дата обращения: 02.07.2023).
10. Diez-Olivan A., Del Ser J., Galar D., Sierra B. Data fusion and machine learning for industrial prognosis: Trends and perspectives towards industry 4.0 // Information Fusion 50, 2019. Pp. 92–111. DOI:10.1016/j.inffus.2018.10.005.
11. Федотов С., Синицин Ф. Учебник по машинному обучению // Академия Яндекса [Электронный ресурс]. URL: https://academy.yandex.ru/handbook/ml/article/mashinnoye-obucheniye (дата обращения: 07.07.2023).
12. Deconvolutional Neural Network // Nordavind [Электронный ресурс]. URL: https://habr.com/ru/companies/nordavind/articles/253859/ (дата обращения: 14.07.2023).
13. Sobolev A. S., Chernyi S. G., Nyrkov A. P., Krivoguz D. O., Zinchenko E. G. Convolution Neural Network for Identification of Underwater Objects // Proceedings of the 2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus, 2022. Pp. 455-458. https://doi.org/10.1109/ElConRus54750.2022.9755621.
14. Рекуррентные нейронные сети (KTT) с Keras // Xabr, 2020. [Электронный ресурс]. URL: https://habr.com/ru/articles/487808 (дата обращения: 10.07.2023).
15. Random forest // Анализ малых данных, 2016. [Электронный ресурс]. URL: https://alexanderdyakonov.wordpress.com/2016/11/14/случайный-лес-random-forest (дата обращения: 11.07.2023).
16. Бэггинг // Machinelearning [Электронный ресурс]. URL: http://www.machinelearning.ru/wiki/index.php?title=Бэггинг (дата обращения: 14.07.2023).

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ ОБЪЕКТАМИ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

УДК 629.12, 65.011, 681.518

МОДЕЛЬ ЦИФРОВОВИЗАЦИИ КОНФИДЕНЦИАЛЬНОСТИ, ДОСТУПНОСТИ, ЦЕЛОСТНОСТИ ДАННЫХ И ЕЕ РЕАЛИЗАЦИЯ В ПРОГРАММНОМ КОМПЛЕКСЕ «КАСОР»

Алексеев Анатолий Владимирович
Санкт-Петербургский государственный морской технический университет
Лоцманская, ул., 3, Санкт-Петербург, 194064, Россия
e-mail: iapbgks@bk.ru

Аннотация. На основе анализа теории и практики оценки информационной безопасности разнородных объектов морской техники и инфраструктуры (ОМТИ) сформулирован квалиметрический подход и разработана модель квалиметрического представления базовых критериев информационной безопасности ОМТИ – конфиденциальности, доступности целостности их данных (КДЦ). Представлен вариант реализации и на базе программного комплекса (ПК) «КАСОР» приведены примеры количественной оценки, контроля КДЦ и информационной безопасности в целом (КДЦ-ИБ) систем комплексной защиты информации (СКЗИ). Разработанный ПК «КДЦ-ИБ СКЗИ» предназначен для цифровой оценки и контроля основных свойств СКЗИ и их оптимизации в процессе проектирования, эксплуатации СКЗИ, а также подготовки/переподготовки специалистов в области информационной безопасности.

Ключевые слова: информационная безопасность; конфиденциальность; доступность; целостность данных; модель; валидный контроль; программный комплекс «КАСОР».

THE MODEL OF DIGITAL ASSESSMENT OF CONFIDENTIALITY, AVAILABILITY, INTEGRITY OF DATA AND ITS IMPLEMENTATION IN THE SOFTWARE PACKAGE «KASOR»

Alekseev Anatoly
Saint Petersburg State Maritime Technical University
3 Lotsmanskaya str., St. Petersburg, 194064, Russia
e-mail: iapbgks@bk.ru

Abstract. Based on the analysis of the theory and practice of assessing the information security of heterogeneous objects of marine equipment and infrastructure (OMTI), a qualimetric approach is formulated and a model of qualimetric representation of the basic criteria for information security of OMTI – confidentiality, availability, integrity of their data (CDC) is developed. A variant of implementation is presented and on the basis of the software package (PC) «KASOR», examples of quantitative assessment, control of CDC and information security in general (CDC-IB) of integrated information protection systems (SCSI) are given. The developed PC «KDC-IB SKZI» is designed for digital assessment and control of the basic properties of the SKZI and their optimization in the process of designing, operating the SKZI, as well as training / retraining of specialists in the field of information security.

Keywords: information security; confidentiality; accessibility; data integrity; model; valid control; software package «KASOR».

Научная проблема. Развитие направления исследований и отрасли информационной безопасности (ИБ), как показывает анализ [1-25], можно охарактеризовать сегодня следующими особенностями:

–бурное развитие в конце XX века информационных технологий побудило специалистов отрасли в ускоренном темпе исследовать комплекс вопросов информационной безопасности, однако,

–в условиях интенсивного развития и спектра программно-аппаратных средств защиты информации (СЗИ) вопросы модельного представления их функционирования, а, тем более, формирования теории ИБ (моделирования анализа, синтеза, оптимизации средств и систем ИБ) в целом носил отстающий характер;

–одновременное становление рыночных отношений и ограничение возможностей национальных регуляторов привело к необоснованно широкой номенклатуре даже сертифицированных СЗИ, число которых сегодня превышает 4,5 тысячи при числе типовых решаемых ИБ-задач порядка 20;

–в этих условиях системные вопросы анализа, количественной оценки и контроля уровня решения задач ИБ современных сложных организационно-технических СКЗИ продолжают оставаться «в тени», что, естественно, не позволяет предметно, на цифровом уровне решать задачи обоснования и оптимизации структур и функционала СКЗИ, эффективно решать задачи вариантного проектирования и развития СКЗИ.

Задачи развития. В этой связи одной из приоритетных задач развития средств и систем обеспечения ИБ, а, тем более, информационного противодействия (ИПД) в обеспечение информационного превосходства в информационной сфере следует назвать решение проблемы форсированного развития теории ИБ, ИПД и в целом – теории информационного противоборства (ТИП), теории практики развития систем информационного противоборства (СИП) [20-25], включая решение следующих, по нашему мнению, первоочередных научно-технических задач [1-21]:

1. систематизации, уточнения и минимизации терминологического аппарата ТИП (энциклопедического словаря, глоссария, тезауруса, ИБ-википедии и т.п.);
2. актуализации данных по классификации и типизации СЗИ и СИП с формированием базы данных по лучшим практикам их создания, эксплуатации и эффективности использования;
3. формирования системы критериев анализа, синтеза и оптимизации СИП и СЗИ с соответствующей системой цифровых показателей и шкалами измерения/оценивания, метриками ИБ, ИПД, СИП;
4. разработки теории практики исследовательского проектирования СИП и СЗИ с систематизацией и классификацией методов и технологий их реализации;
5. создания и актуализации типовых баз данных и знаний СИП и СЗИ, включая квалиметрические (КБДЗ), применительно к решению наиболее значимых практических задач;
6. формирования системы квалиметрического ранжирования сертифицированных СЗИ и их систем, прежде всего, по системным характеристикам, включая показатели конкурентной способности (КС), информационно-технологического превосходства (ИТП) и их перспективности развития (ПР);
7. формирования системы квалиметрии моделей и полимодельных комплексов, включая их верификацию и оценку валидности, сертификацию, аттестацию и соответствующее лицензирование.

Решение комплекса представленных задач при соответствующей регулирующей роли ФСТЭК, по нашему мнению, обеспечит качественно новый этап развития бурно развивающейся отрасли ИБ [22-25].

Предлагаемый вариант. На основе анализа теории и практики оценки ИБ разнородных ОМТИ сформулирован квалиметрический подход (концепция), ключевыми принципами которого следует считать:

1. Принцип цифровизации проектного качества и эффективности эксплуатации для всего жизненного цикла ОМТИ как основного системного показателя СИП, подлежащего первоочередному сравнительному мониторингу, анализу, контролю и оптимизации при решении любой из решаемых задач и их комплекса.
2. Принцип полимодельного представления СИП, позволяющий минимизировать погрешности моделирования и неопределенности задания исходных данных Заказчиком.
3. Принцип вариантного обоснования/оптимизации решений, обеспечивающий комплексную/оптимальную реализацию задач СКЗИ в составе АСЗИ.

Для реализации декларируемых принципов и обеспечения ИБ информационных ресурсов (ИР) АСЗИ типовой состав задач ИБ может быть представлен в виде комплекса взаимосвязанных задач и соответствующих функциональных технических подсистем СКЗИ (в приоритетном порядке, рис. 1) [17]:

1.ПМУБ – мониторинга и управления безопасностью (в отличии от похожих в ряде работ [3-9, 13, 16]);
2.ПРД – разграничения доступа (с учетом аналогичных в ряде работ);
3.ПКЗИ – криптографической защиты информации;
4.ПЗВ – защиты от вторжений;
5.ПАЗ – анализа защищенности;
6.ПКЦ – контроля целостности;
7.ПЗВК – защиты от вредоносных кодов, а также подсистем обеспечения
8.КОТМ – комплекса организационно-технических мероприятий;
9.СМИБ – системного менеджмента (управления) качеством информационной безопасности.

Представленные на рис. 1 названные функциональные подсистемы СКЗИ в составе АСЗИ дополнены «самым слабым звеном» (элементом) СКЗИ, отражающим

10.Н-ЧФ – наряду с позитивным - негативное проявление субъективных свойств операторов, часто именуемых пресловутым «Человеческим фактором» и, естественно, негативно влияющим на качество СКЗИ,

и разработана модель квалиметрического представления базовых критериев информационной безопасности ОМТИ – конфиденциальности, доступности целостности их данных (КДЦ).

Для полноты структурно-информационной модели СКЗИ наряду с ресурсной подсистемой учета

11.СВм – стоимости владения, приведенной к месяцу для удобства сопоставления и интерпретации получаемых результатов, структура СКЗИ дополнена элементом, учитывающим все другие критерии и показатели качества, условно объединенные в элементе СКЗИ,

12.Др. – другие критерии и показатели проектного качества и эффективности эксплуатации.

Математическая модель оценки КДЦ-ИБ. Применительно к представленной типовой структурной модели СКЗИ АСЗИ и с учетом ранее разработанного в [22] Обобщенного метода оценки и анализа комплексного показателя качества (КПК) отдельного объекта исследовательского проектирования (ОИП) и их системы (ПСПК – полимодельного системного показателя качества) математическая модель оценки качества этого ОИП по критерию агрегированного показателя качества (АПК) представляется в частном виде

$$\boldsymbol{Q_k = C^{А}_{k,6}\{w_m, C^{Г}_{m,12}[w_g, C^{Г}_{g,12}(w_n, q_n)]\}}, \quad (1)$$

$$\boldsymbol{Q = C^{Г}_{P}\{w_p, C^{Г}_{p,R}[w_r, C^{Г}_{r,11}(w_k, Q_k)]\}}, \quad (2)$$

где: $\boldsymbol{k \in [1; K]}$ – порядковый номер ОИП из их произвольного общего числа $\boldsymbol{K}$ в составе системы ОИП, характеризующейся соответственными системными показателями качества (СПК), а при «усреднении» по ряду системных моделей – полимодельным системным показателем качества (ПСПК);

$\boldsymbol{n \in [1; N]}$ – порядковый номер частных показателей качества (ЧПК) $\boldsymbol{q_n}$ с общим их числом $\boldsymbol{N = 12}$ и индексом критериальной значимости (ИКЗ, весовым коэффициентом) $\boldsymbol{w_n}$ для каждого $\boldsymbol{g}$ – ого (с общим их числом $\boldsymbol{g \in [1; G]}$, в нашем частном случае $\boldsymbol{G = 12}$) группового качества (ГПК) $\boldsymbol{C^{Г}_{g,12}(\dots)}$ и общего числа ЧПК для ОИП $\boldsymbol{N_о = N \times G}$;

$\boldsymbol{m \in [1; M]}$ – порядковый номер показателей качества при использовании каждой модели (МПК) при их общем числе в нашем частном случае $\boldsymbol{M = 6}$ и индексе критериальной значимости МПК $\boldsymbol{w_g}$;

$\boldsymbol{C^{Г}_{g,12}(w_n, q_n)}$ – обобщенный оператор свертки ЧПК $\boldsymbol{q_n}$ с общим их числом $\boldsymbol{N = 12}$ и индексом критериальной значимости $\boldsymbol{w_n}$ в $\boldsymbol{g}$ - ый ГПК $\boldsymbol{C^{Г}_{g,12}(\dots)}$, характеризующий свойства ОИП по алгоритму типа $\boldsymbol{t_N = Г}$ из целого ряда возможных альтернатив первого уровня свертки показателей качества, включая: А - аддитивный (линейный) алгоритм, впервые предложенный А.Н. Крыловым; М - мультипликативный алгоритм Д.Ф. Нэша; Г - гармонический алгоритм (комбинация алгоритмов типа А и М);

$\boldsymbol{C^{Г}_{m,12}[w_g, C^{Г}_{g,12}(\dots, \dots)]}$ – аналогично обобщенный оператор свертки ГПК с общим их числом $\boldsymbol{G = 12}$ и ИКЗ $\boldsymbol{w_g}$ в $\boldsymbol{m}$ - ый МПК $\boldsymbol{C^{Г}_{m,12}[w_g, \dots]}$ по алгоритму типа $\boldsymbol{t_M = Г}$;

$\boldsymbol{C^{А}_{k,6}\{w_m, C^{Г}_{m,12}[w_g, \dots]\}}$ – аналогично обобщенный оператор свертки МПК с общим их числом $\boldsymbol{M = 6}$ и ИКЗ $\boldsymbol{w_m}$ масштабируется в $\boldsymbol{k}$ - ый АПК по алгоритму типа $\boldsymbol{t_M}$ = А, либо М, либо Г (по выбору Заказчика) для ОИП с номером $\boldsymbol{k}$;

$\boldsymbol{C^{Г}_{r,11}(w_k, Q_k)}$ – аналогично обобщенный оператор свертки $\boldsymbol{k}$ - ого АПК для каждого ОИП и ИКЗ $\boldsymbol{w_k}$ в альтернативном множестве (ТОР-ряде) со значением $\boldsymbol{K}$=11 в нашем частном случае (как показано ниже, 10 альтернативных вариантов ОИП и исследовательский (оптимизируемый) вариант) масштабируется в $\boldsymbol{r}$ - ый модельный системный показатель качества (МСПК) $\boldsymbol{C^{Г}_{p,R}[w_r, \dots]}$ по алгоритму типа $\boldsymbol{t_M = Г}$ (по согласованию с Заказчиком) для системы ОИП и по модели с номером $\boldsymbol{p}$;

$\boldsymbol{C^{Г}_{P}\{w_p, C^{Г}_{p,R}[w_r, \dots]\}}$ – аналогично обобщенный оператор свертки $\boldsymbol{p}$ - ого МСПК для системы ОИП и ИКЗ $\boldsymbol{w_p}$ при числе моделей системного уровня (уровня мета-данных) $\boldsymbol{P}$ масштабируется в полимодельный системный показатель качества (ПСПК) $\boldsymbol{C^{Г}_{P}\{w_p, \dots\}}$по алгоритму типа $\boldsymbol{t_P = Г}$.

В условиях представленной модели оценки качества ОИП рассмотрим конфиденциальность, доступность и целостность информационного ресурса в АСЗИ как выделенные информационные свойства СКЗИ (элемента АСЗИ), в формировании которых участвуют соответствующие подсистемы с их ГПК, в виде модели

$$\text{К}_k = \boldsymbol{C^{Г}_{k,12}[w_b, C^{Г}_{b,12}(w_n, q_n)]}, \quad \sum_{b=1}^{B=12} \boldsymbol{w_b = 1}, \quad (3)$$

$$\text{Д}_k = \boldsymbol{C^{Г}_{k,12}[w_c, C^{Г}_{c,12}(w_n, q_n)]}, \quad \sum_{c=1}^{C=12} \boldsymbol{w_c = 1}, \quad (4)$$

$$\text{Ц}_k = \boldsymbol{C^{Г}_{k,12}[w_d, C^{Г}_{d,12}(w_n, q_n)]}, \quad \sum_{d=1}^{D=12} \boldsymbol{w_d = 1}. \quad (5)$$

Представленные модели цифровизации (количественной оценки) типовых показателей и требований к информационной безопасности АСЗИ как отдельного $\boldsymbol{k}$-ого ОИП $\boldsymbol{S_k}$ (3), (4), (5) можно интерпретировать как результат агрегирования качества элементов СКЗИ (с соответствующими порядковыми номерами $\boldsymbol{b}$, $\boldsymbol{c}$ и $\boldsymbol{d}$ при соответствующих ИКЗ $\boldsymbol{w_b}$, $\boldsymbol{w_c}$ и $\boldsymbol{w_d}$), обеспечивающих решение задач обеспечения К, Д, Ц.

Как показано ниже, для этого достаточно полученные при оценке проектного качества или эффективности эксплуатации СКЗИ свернуть с соответствующими значениями матрицы ИКЗ, что, например, реализовано в РПК «КАСОР-23.5» [17], как показано ниже на представленном рис. 1.

В свою очередь, для оценки уровня обеспечения информационной безопасности в АСЗИ будет необходимо и достаточно выполнить агрегирование показателей К, Д, Ц в виде

$$\boldsymbol{S_k} = [(\boldsymbol{w_{k,1}} \times \text{К}_k + \boldsymbol{w_{k,2}} \times \text{Д}_k + \boldsymbol{w_{k,3}} \times \text{Ц}_k) \times \text{К}_k^{\boldsymbol{w_{k,1}}} \times \text{Д}_k^{\boldsymbol{w_{k,2}}} \times \text{Ц}_k^{\boldsymbol{w_{k,3}}}]^{0,5}, \quad \sum_{k,s=1}^{S=3} \boldsymbol{w_{k,s}} = 1. \quad (6)$$

В заключение следует отметить с учетом результатов моделирования [25], что погрешность агрегирования показателей качества и оценки уровня ИБ, ПК и Э по критерию коэффициента вариации (отношение среднеквадратичного значения к математическому ожиданию) составит

$$\boldsymbol{K_{var}} = \boldsymbol{K}_{\text{ЧПК}} \Big/ \sqrt{\boldsymbol{N} \times \boldsymbol{G}} \quad , \tag{7}$$

что, как показывают результаты компьютерного моделирования, весьма незначительно и составляет даже при $\boldsymbol{K}_{\text{ЧПК}} = 10\%$ порядка (1…2)%.

Реализация модели цифровизации К, Д, Ц и S. В рамках представленной модели ниже приводится вариант реализации процедуры количественной оценки с возможностью последующего мониторинга, анализа, синтеза и оптимизации свойств и характеристик СКЗИ на базе Роботизированного проектного комплекса (РПК) «КАСОР-23.5» [17], главная экранная форма которого в режиме цифрового паспорта приведена на рис. 1.

Приведенный пример количественной оценки представлен для условия «СКЗИ-1», т.е. использования в составе СКЗИ средств, приведенных в нижней части рис.1 и имеющих в составе своих подсистем рейтинговый в TOP-10 уровень R=1. При этом, уровни ИБ составили по К=76%, Д=82%, Ц=86%.

Для иллюстрации влияния качества СЗИ на результаты моделирования приведен рис. 2, на котором представлены аналогичные оценки для условия «СКЗИ-2» и составившие: К=67%, Д=61%, Ц=80%.

Наконец, на рис. 3 для условия «СКЗИ-Ф» (фактического набора СЗИ в составе СКЗИ для, например, варианта проведения аудита ИБ [11, 25] в организации ПКБ «Лоцман», состав СЗИ приведен в нижней части рис. 1) аналогичные оценки составили: К=65%, Д=74%, Ц=82%.

Анализ результатов цифрового моделирования. Анализ представленных на рис. 1 и рис. 3 результатов, позволяет утверждать:

1. Представленная модель и результаты ее реализации в РПК «КАСОР-23.5» позволяют перейти от традиционной качественной (однобитовой) оценки соответствия СЗИ и СКЗИ в целом – к требованиям К, Д, Ц к количественной многокритериальной и полимодельной (цифровой, многобитовой) оценке уровня ИБ, включая оценку по критериям проектного качества (ПК) СКЗИ в целом по критерию АПК $\boldsymbol{Q}$ и эффективности ее эксплуатации (Э) $\boldsymbol{W}$ (как меры реализации проектного качества), а также производных от ПК, Э – оценке конкурентной способности и перспективности развития (КС, ПР).

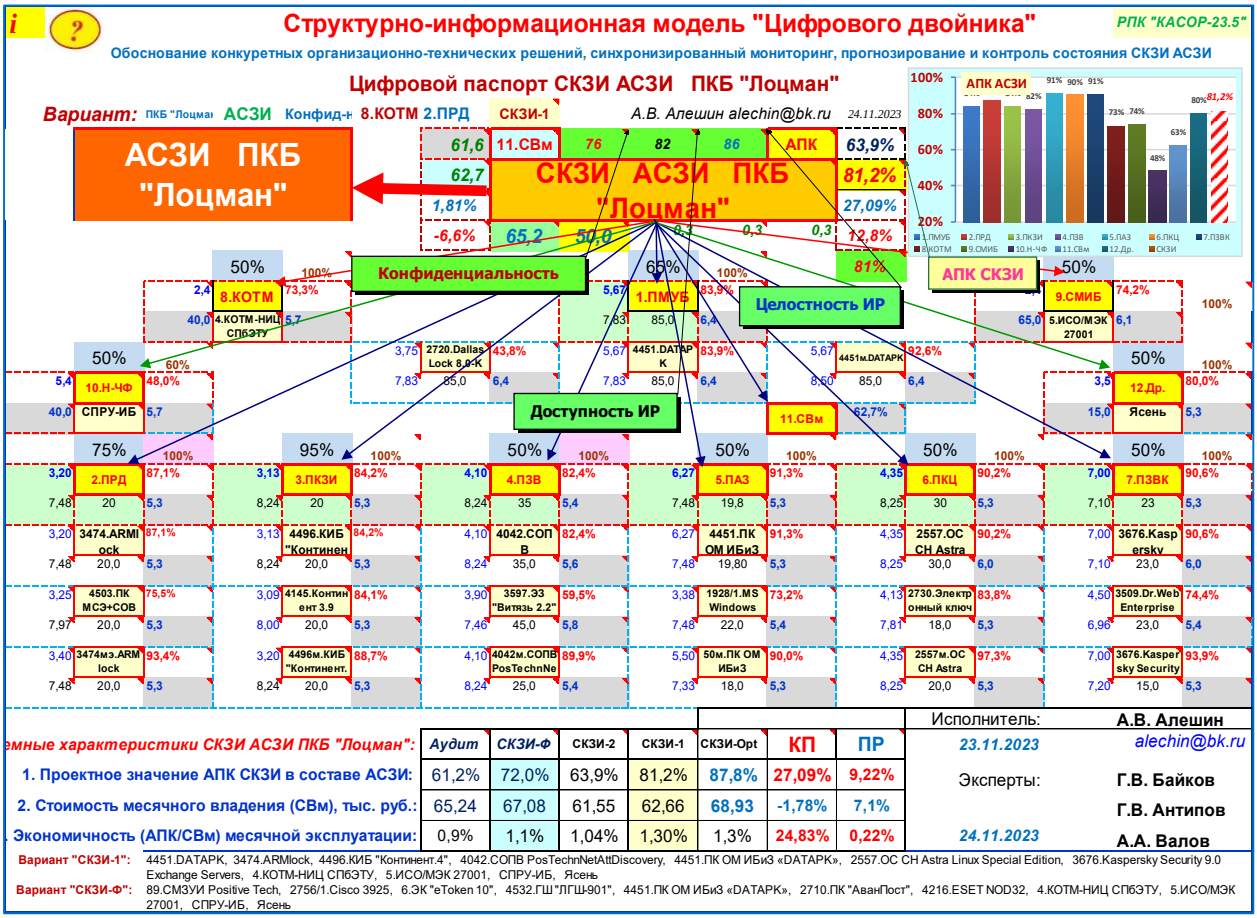


Рис. 1 – Главная экранная форма РПК «КАСОР-23.5» в режиме «СКЗИ-1»

Приведенный пример количественной оценки представлен для условия «СКЗИ-1», т.е. использования в составе СКЗИ средств, приведенных в нижней части рис. 1 и имеющих в составе своих подсистем рейтинговый в ТОР-10 уровень R=1. При этом, уровни ИБ составили по К=76%, Д=82%, Ц=86%.

Для иллюстрации влияния качества СЗИ на результаты моделирования приведен рис. 2, на котором представлены аналогичные оценки для условия «СКЗИ-2» и составившие: К=67%, Д=61%, Ц=80%.

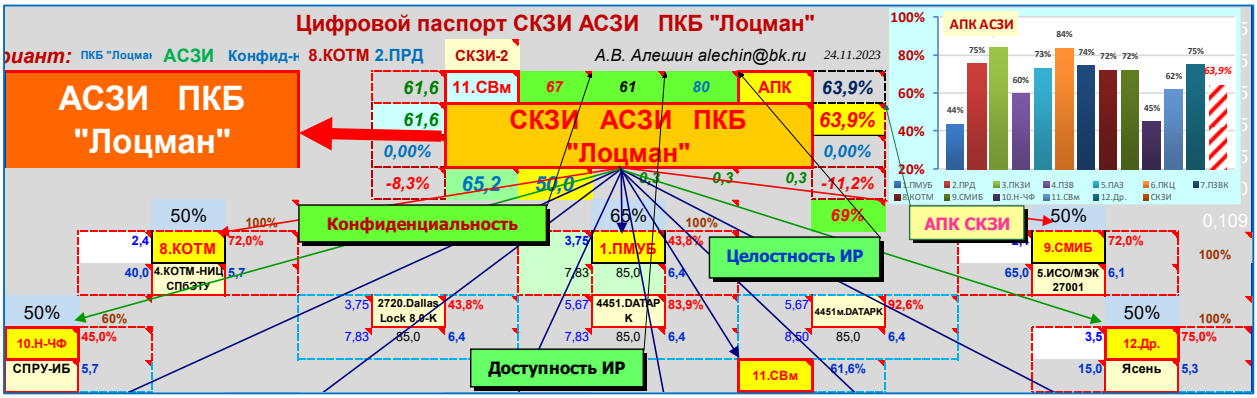


Рис. 2 – Фрагмент главной экранной формы РПК «КАСОР-23.5» в режиме «СКЗИ-2»

Наконец, на рис. 3 для условия «СКЗИ-Ф» (фактического набора СЗИ в составе СКЗИ для, например, варианта проведения аудита ИБ в организации ПКБ «Лоцман», состав СЗИ приведен в нижней части рис. 1) аналогичные оценки составили: К=65%, Д=74%, Ц=82%.

Анализ результатов цифрового моделирования. Анализ представленных на рис. 1 рис. 3 результатов, позволяет утверждать:

1. Представленная модель и результаты ее реализации в РПК «КАСОР-23.5» позволяют перейти от традиционной качественной (однобитовой) оценки соответствия СЗИ и СКЗИ в целом к требованиям К, Д, Ц, к количественной многокритериальной и полимодельной (цифровой, многобитовой) оценке уровня ИБ, включая оценку по критериям проектного качества (ПК) СКЗИ в целом по критерию АПК ***Q*** и эффективности ее эксплуатации (Э) ***W*** (как меры реализации проектного качества), а также к производным от ПК - к оценке конкурентной способности и перспективности развития (КС, ПР).

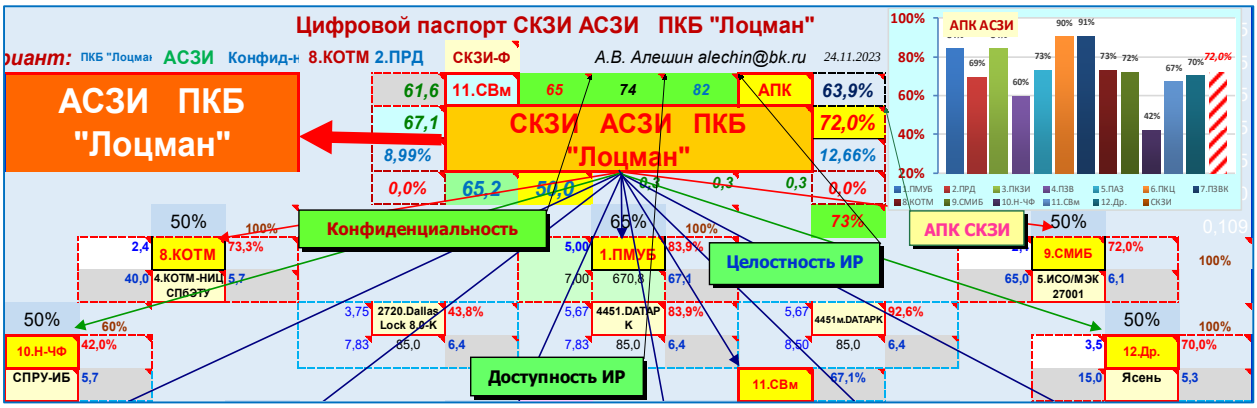


Рис. 3. Фрагмент главной экранной формы РПК «КАСОР-23.5» в режиме «СКЗИ-Ф»

2. Представленный математический аппарат (1) – (7) и средства его реализации типа РПК «КАСОР-23.5» по квалиметрическому и многовариантному оцениванию ПК и Э, К, Д, Ц и КС, ПР использования СЗИ при погрешностях оценивания порядка (1…2)% позволяют перейти к цифровому мониторингу, анализу, синтезу и оптимизации СКЗИ в составе АСЗИ объектов информатизации и исследовательского проектирования, в том числе в классе ОМТИ, на качественно новом (цифровом, полимодельном, роботизированном) уровне.

3. Представленные ключевые элементы технологии цифрововизации проектного качества и эффективности эксплуатации СКЗИ, включая оценки конфиденциальности, доступности, целостности информационных ресурсов и ИБ в целом, в настоящее время активно используются для формирования, актуализации и аналитического использования квалиметрических баз данных и знаний (КБДЗ) в составе одного из ключевых элементов технологии и средств реализации так называемых цифровых двойников СКЗИ АСЗИ разнородных объектов информатизации, включая ОМТИ.

Заключение. Количественная (цифровая) оценка и контроль основных свойств и системных характеристик средств и систем защиты информации в условиях резкого возрастания в современных условиях сложности и многофункциональности объектов информатизации, а их анализ, синтез и оптимизации, как ключевые элементы теории информационной безопасности и информационного противоборства в целом, являются в настоящее время давно назревшими и исключительно актуальными для обеспечения процессов концептуального, системного, исследовательского и технического проектирования, эффективной эксплуатации и прогрессивного развития СКЗИ в составе разнородных АСЗИ, а также для подготовки/переподготовки специалистов в области информационной безопасности и обеспечения информационного превосходства в области информационного превосходства и безопасности в целом.

В этих условиях системные вопросы анализа, количественной оценки и контроля уровня решения задач ИБ современных сложных организационно-технических СКЗИ, в том числе по требованиям конфиденциальности, доступности, целостности информационных ресурсов, ИБ, ИПД и ИП в целом продолжают оставаться «в тени» прикладной теории информации и информационной безопасности. Это, естественно, не позволяет предметно, на цифровом уровне решать задачи обоснования и оптимизации структур и функционала СКЗИ, эффективно решать задачи вариантного проектирования и развития СКЗИ.

На основе анализа теории и практики оценки ИБ разнородных ОМТИ сформулирован квалиметрический подход и разработана модель квалиметрического представления базовых критериев информационной безопасности ОМТИ – конфиденциальности, доступности целостности их данных. Представленный вариант реализации концепции, модели и ключевых элементов технологии квалиметрии ИП, как комплекса ИБ и ИПД, на базе РПК «КАСОР-23.5», а также приведенные примеры количественной оценки, контроля КДЦ и информационной безопасности в целом (КДЦ-ИБ) СКЗИ в составе АСЗИ подтвердили возможность и перспективность разработанного ПК «КДЦ-ИБ СКЗИ» при решении задач цифровой оценки и контроля основных свойств СКЗИ и их оптимизации в процессе проектирования, эксплуатации СКЗИ, а также подготовки/переподготовки специалистов в области ИБ, ИПД и информационного противоборства в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Заводцев И.В., Бирюков Р.Е., Зерщиков М.А. Методика выбора стратегий защиты для систем управления инцидентами информационной безопасности на основе теории игр \ В сб.: Математические методы и информационно-технические средства. Материалы XI Всероссийской научно-практической конференции, 2015, с. 101-104.
2. Архангельская А.В., Когос К.Г. Теория алгоритмов в задачах информационной безопасности\ Конспект лекций / Москва, 2022.
3. Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. Теория информационной безопасности и методология защиты информации (2-е издание, исправленное и дополненное) - Санкт-Петербург, 2018.
4. Азамов О.В. Информационная безопасность / О. В. Азамов, К. Ю. Будылин, Е. Г. Бунев, С. А. Сакун, Д. Н. Шакин (Электронный ресурс) - http://www.naukaxxi.ru/materials/41/.
5. Введение в информационную безопасность / А.А. Малюк, В.С. Горбатов, В.И. Королев и др.; под ред. В.С. Горбатова. - М.: Горячая линия - Телеком, 2013. - 288 с.
6. Гатчин Ю.А. Основы информационной безопасности: учебное пособие/ Ю.А. Гатчин, Е.В. Климова. - СПб.: СПбГУ ИТМО, 2009. – 84 с.
7. Гатчин Ю.А., Сухостат В.В. Теория информационной безопасности и методология защиты информации / Ю.А. Гатчин, В.В. Сухостат - СПб., СПбГУ ИТМО, 2010. - 98 с.
8. Гатчин Ю.А. Система оценки информационно-психологической устойчивости IT-специалиста / Ю.А. Гатчин, В.В. Сухостат // Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT'13». Научное издание в 4-х томах. - Москва: Физматлит, 2013. - Т. 2. - С. 273-282. - 430 с.
9. Теория и практика обеспечения информационной безопасности / Сборник научных трудов по материалам всероссийской научно-теоретической конференции, 2021, 363 с.
10. Международная информационная безопасность: теория и практика: учебное пособие для вузов в 3 т. / Под общ. ред. А.В. Крутских. М.: Аспект Пресс, 2019. Т. 1. С. 18—88.
11. Смирнов Г.Е. Актуальные вопросы развития теории и практики аудита информационной безопасности / Школа Науки. 2021. № 10 (47). С. 4-6.
12. Тутубалин П.И. Основные задачи прикладной теории информационной безопасности АСУ / Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2007. № 39. С. 63-72.
13. Баркалов С.А., Моисеев С.И. Модель оценки безопасности информационных систем, основанная на теории латентных переменных / В сборнике: XIII Всероссийское совещание по проблемам управления ВСПУ-2019. Сборник трудов XIII Всероссийского совещания по проблемам управления ВСПУ-2019. Институт проблем управления им. В.А. Трапезникова РАН. 2019. С. 2507-2511.
14. Бухаров Е.О., Соколовский С.П., Калач А.В., Зыбин Д.Г. Поддержка принятия управленческих решений в сфере информационной безопасности в терминах теории игр - Вестник Воронежского института ФСИН России. 2018. № 2. С. 46-54.
15. Информационная безопасность: современная теория и практика: сборник научных трудов студентов, аспирантов и преподавателей по материалам III Межвузовской научно-практической конференции / отв. ред. З.В. Семенова. − Электрон. дан. – Омск : СибАДИ, 2020. – URL: http://bek.sibadi.org/cgi- bin/irbis64r_plus/cgiirbis_64_ft.exe. – Режим доступа: для авторизованных пользователей.
16. Разумников С.В., Курманбай А.К. Разработка интегральной модели оценки информационной безопасности информационных систем / В сборнике: Информационные технологии в экономике и управлении. материалы II Всероссийской научно-практической конференции (с международным участием). Под редакцией Т.А. Исмаилова. 2016. С. 42-45.
17. Свидетельство о государственной регистрации программ для ЭВМ (Реестр программ Федеральной службы по интеллектуальной собственности) № 2023616388, 27.03.2023 (поступление: 13.03.2023).
18. Бондаренко Д.Л., Жбанов И.Л. Анализ существующих подходов к трактовке понятия «живучесть» информационно-управляющей подсистемы асу специального назначения / Актуальные вопросы технических наук, 2017, с. 100-104.
19. Информационные технологии в судостроении: существующие системы, сферы и возможности их использования [Электронный ресурс] URL: https://uchimsya.com/a/qC363Pr9 (дата обращения 24.05.2023).

20. Алексеев А.В., Кириллов Н.П. Информационная устойчивость морских радиоэлектронных систем в условиях широкомасштабной информационной войны / Наука и техника: Вопросы истории и теории - Тезисы 18 конф. СПб отд-я Нац. комитета по истории и философии науки и техники. Вып. 13 - СПб: СПФИИЕТ РАН, 1997, с.13-14.
21. Алексеев А.В., Кириллов Н.П. Информационная устойчивость систем морской разведки в условиях широкомасштабной информационной борьбы / Сборник «Разведка и радиоэлектронная борьба». - Тез. докл. МВНС - СПб.: В/ч 48252, 1999, с. 65-67.
22. Алексеев А.В. Информационная живучесть судна: понятие, проблемы, технологии / Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 7 / СПОИСУ. – СПб., 2019, с. 345 – 348.
23. Алексеев А.В., Кузнецов В.В., Согонов С.А., Мусатенко Р.И., Тычинин И.Ю., Балицкая К.В. Система критериев оценки информационной живучести судна / Информационная безопасность регионов России (ИБРР-2019). – СПб., 2019, с. 329-330.
24. Бобрович В.Ю., Алексеев А.В., Антипов В.В., Смольников А.В. Информационная живучесть корабля: угрозы, модель, системные требования, пути реализации / Информационная безопасность регионов России (ИБРР-2021). – СПб., 2021, с. 265-267.
25. Алексеев А.В. Модель и программный комплекс цифровой трансформации кибербезопасности / Вопросы обеспечения безопасности в киберпространстве: материалы Всероссийской НТК – Махачкала: ДГТУ, 2022 г. - 387 с. с. 251-255.

УДК 57.08

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ СУДОВОЖДЕНИЯ ЗА СЧЕТ ПРИМЕНЕНИЯ ИНСТРУМЕНТАЛЬНОГО КОМПЛЕКСА ВЫПОЛНЕННОГО В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ ПО ОБНАРУЖЕНИЮ ДЕПРЕССИВНОГО СОСТОЯНИЯ У СПЕЦИАЛИСТОВ МОРСКОГО И РЕЧНОГО ФЛОТА

Артемов Станислав Игоревич[1], Алексеев Сергей Алексеевич[2], Рябков Яков Игоревич[3]
[1]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
[2] Государственный университет морского и речного флота имени адмирала С. О. Макарова,
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
[3]Военно-космическая академия имени А.Ф. Можайского
Ждановская ул., 13, Санкт-Петербург, 197198, Россия
e-mails: pushokcheck@yandex.ru, ksgati@yandex.ru, yakovrt@mail.ru

Аннотация. Рассмотрена задача повышения безопасности судовождения за счет применения автоматизированного инструментального комплекса, выполненного в защищенном исполнении по оценке и обнаружению депрессивного состояния у специалистов морского и речного флота. В статье представлен метод и алгоритм анализа многоканальной электроэнцефалограммы и выявления связи динамики параметров распределения амплитуд с наличием депрессивного состояния у испытуемых. В основу метода положена информационная символьно-динамическая модель формирования многоканальной электроэнцефалограммы, которая позволяет за счет использования соответствующего структурно-лингвистического метода модификации нелинейных сигналов представлять их оператору в защищенном исполнении и удобной, читаемой форме. Полученные результаты позволяют делать выводы о качестве влияния наличия депрессивного состояния у испытуемого на параметры динамики распределения амплитуд в многоканальном сигнале электроэнцефалограммы.

Ключевые слова: обработка сигналов; восприятия; психофизиологические реакции мозга; обработка электроэнцефалограмм; интерфейс мозг-компьютер; нелинейный анализ сигналов; энтропия.

IMPROVING THE SAFETY OF NAVIGATION THROUGH THE USE OF A TOOL COMPLEX MADE IN A PROTECTED VERSION TO DETECT A DEPRESSIVE STATE IN SPECIALISTS OF THE MARINE AND RIVER FLEET

Artemov Stanislav [1], Alekseev Sergey [2], Ryabkov Yakov [3]
[1]St. Petersburg State Electrotechnical University «LETI» named after V.I. Ulyanov (Lenin)
5 Professor Popov St, St. Petersburg, 197376, Russia
[2] Admiral Makarov State University of Maritime and Inland Shipping,
Dvinskaya St, 5/7, St. Petersburg, 198035, Russia
[3]Military Space Academy named after A.F. Mozhaisky
Zhdanovskaya St, 13, St. Petersburg, 197198, Russia
e-mails: pushokcheck@yandex.ru, ksgati@yandex.ru, yakovrt@mail.ru

Absrtact. The task of improving the safety of navigation through the use of an automated tool complex made in a protected design for the assessment and detection of a depressive state in specialists of the marine and river fleet is considered. The article presents a method and algorithm for analyzing a multichannel electroencephalogram and identifying the relationship between the dynamics of the amplitude distribution parameters and the presence of a depressive state in the subjects. The method is based on an informational symbolic-dynamic model of the formation of a multichannel electroencephalogram, which allows, through the use of an appropriate structural-linguistic method of modification of nonlinear signals, to present them to the operator in a secure version and a convenient, readable form. The results obtained allow us to draw conclusions about the quality of the influence of the presence of a depressive state in the subject on the parameters of the dynamics of the distribution of amplitudes in the multichannel signal of the electroencephalogram.

Keywords: signal processing; perception; psychophysiological reactions of the brain; processing of electroencephalograms; brain-computer interface; nonlinear signal analysis; entropy.

Введение. В современном народном хозяйстве важную роль играет бесперебойное функционирование транспортной инфраструктуры. Поэтому для обеспечения безопасности эксплуатации транспортных средств и техники морского и речного флота используются существенные человеческие и материальные ресурсы. Разрабатываются нормативные акты и методы предрейсового медицинского контроля и осмотра физического состояния лиц, привлеченных к управлению техникой морского и речного флота. Важным требованием для допуска является соблюдение режима труда и отдыха. При этом в методических рекомендациях не представлены методы, позволяющие осуществлять объективный контроль последствий нарушения режима труда и отдыха, таких как утомление и депрессивные состояния. Известно, что традиционные линейные методы анализа ЭЭГ недостаточно эффективны при обнаружении депрессивных состояний [1 - 4].

Различными областями мозга постоянно излучается сигнал, известный как «спонтанная активность». Спонтанная активность и аддитивность сигнала, регистрируемого отведениями электроэнцефалографа, являются причиной того, что соотношение сигнал-шум при обнаружении вызванного потенциала имеет очень низкие значения. Поэтому для обнаружения волны вызванного потенциала, соответствующей предъявляемому стимулу, обычно используется накопление синхронных относительно предъявления стимула временных интервалов сигнала электроэнцефалограммы (ЭЭГ).

По данным таких известных исследователей, как П. Линдсей (1974), Саид Саней (1990) и многих других, при предъявлении стимула сигнал от рецепторов проходит последовательную обработку в различных областях мозга. Поэтому в различные моменты времени относительно предъявления стимула импульсы электрической активности формируются различными областями мозга, что проявляется в виде «спонтанной активности». Сигнал вызванного потенциала, синхронизированного с предъявлением стимула, фиксируется прибором снятия ЭЭГ как суперпозиция с сигналами «спонтанной активности». Этим объясняется низкие значения отношения сигнал-шум при обнаружении волны вызванного потенциала. В настоящем исследовании предлагается использование информационной символьно-динамической модели для обработки электрофизиологических сигналов мозга без подавления «спонтанной активности» накоплением.

Целью исследования, представленного в статье метода контроля и обнаружения последствий нарушения режима труда и отдыха в виде утомления и депрессивного состояния лиц, привлеченных к управлению средствами морского и речного флота. Для достижения цели были поставлены и решены следующие задачи:

– разработана модель контроля маркеров утомляемости и депрессивного состояния через оценку сигнала электроэнцефалограммы (ЭЭГ), как проекции сигналов пространственно-временной обработки поступающего потока сенсорной нейронной активности на точки установления электродов съёма гальванических потенциалов для обоснования выбора метода выделения паттернов ЭЭГ (паттерн является качественной характеристикой ЭЭГ, отражающей функциональное состояние головного мозга);

1) разработана методика обнаружения маркеров утомляемости и депрессивного состояния, базирующуюся на оценке изменений элементного состава множества паттернов, выделяемых в сигнале ЭЭГ;

2) разработан алгоритм автоматизации и интеллектуализации процесса обнаружения маркеров утомляемости и депрессивного состояния в сигнале ЭЭГ, позволяющий автоматизировать выделение множества специфических паттернов, представленных амплитудно-временными структурами сигнала;

3) выполнена экспериментальная проверка разработанных инструментов обработки и анализа сигналов ЭЭГ для выделения маркеров депрессивного состояния специалистов морского и речного флота.

В «спонтанной активности» содержатся сообщения, которыми обмениваются области мозга в процессе переработки информации. Поэтому при анализе электрофизиологических сигналов мозга возможно использование «спонтанной активности» для поиска маркеров депрессивных состояний, что обеспечивается использованием информационной символьно-динамической модели.

Информационная символьно-динамическая модель электрофизиологических сигналов мозга включает следующие отличия от известных моделей обработки ЭЭГ, а именно:

1) в процессе последовательной переработки сигналов рецепторов различными областями мозга формируется пространственно-временное распределение экстремумов значений напряжения в отведениях электроэнцефалографа;

2) последовательности различаются между собой амплитудными и фазовыми отношениями входящих в состав экстремумов и могут характеризовать текущий процесс переработки мозгом информации;

3) фазоамплитудные последовательности, вызываемые процессом восприятия текущего стимула, преобладают над другими последовательностями, если сформирована доминанта внимания (А. А. Ухтомский, 1978);

4) информационная модель деятельности мозга определяется как качественный и количественный состав множества фазоамплитудных последовательностей, входящих в состав электрофизиологических сигналов мозга (1):

$$Z_k(X) = \sum_{i=1}^{N} W_{ik} z_i \quad (1)$$

где z_k - текущий паттерн (символ), выделенный из сигнала ЭЭГ в точках отведения ЭЭГ;

z_i - составляющая паттерна, сформированная i-м функционально обособленным нейронным ансамблем в точке отведения;

W_{ik} - весовой коэффициент (информационная значимость) i-й составляющей паттерна k-й точки отведения;

X – вектор отсчетов сигнала ЭЭГ x_j

Задача исследования может быть представлена следующей записью (2):

$$q(v, \Delta\tau, \gamma) \xrightarrow{М} Q(t_i) \xrightarrow{Э} S(t_i), \quad (2)$$

где $q(v, \Delta\tau, \gamma)$ – визуальный стимул с параметрами: пространственное распределение v , интервал времени предъявления $\Delta\tau$ и смысловое содержание ; $Q(t_1)$ – ЭФР мозга на восприятие стимула и $S(t_i)$ – сигнал ЭЭГ на момент предъявления визуального стимула t_i. Требуется найти такую функцию F, чтобы на основе отображения P возможно было обнаруживать момент времени t_i,- маркер, в который происходит восприятие стимула (3).

$$S(t_i) \xrightarrow{F} P(t_i) \quad (3)$$

На основе поставленной задачи (2) и (3) сформулирована концепция исследования, представленная на рис. 1 в виде структурной схемы экспериментального макета прибора управления «Интерфейс мозг-компьютер», отражающего сущность целевой обработки и анализа ЭЭГ.

В статье представлен метод обнаружения моментов восприятия человеком визуальных стимулов, базирующийся на оценке изменений элементного состава множества паттернов, выделяемых путём построения амплитудно-временных конструкций, выделяемых в сигнале ЭЭГ. Теория и практика препроцессинга сигналов ЭЭГ и последующего анализа с применением информационного подхода получили название структурно-лингвистического анализа сигналов (СЛАС).

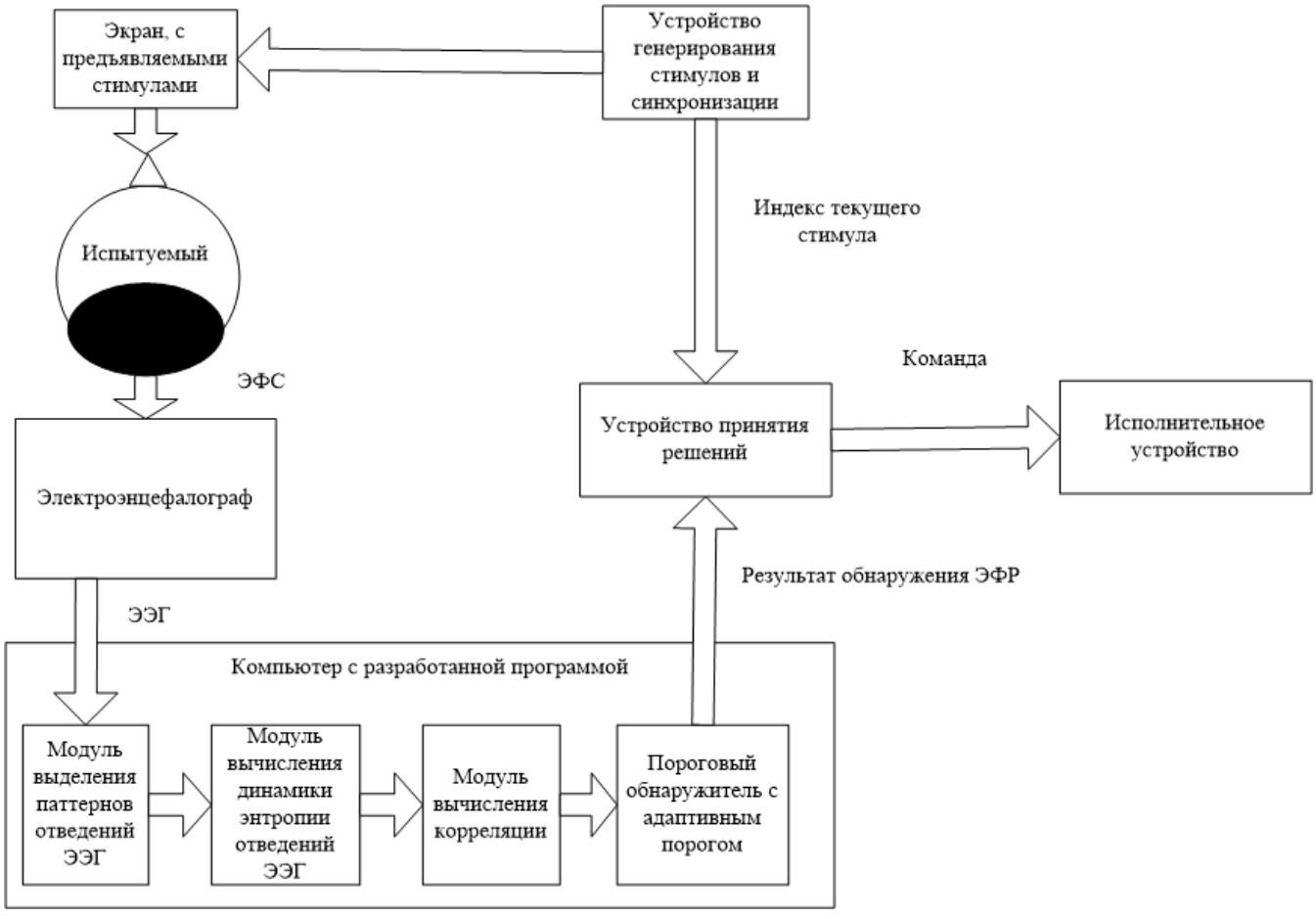


Рис. 1. Структурная схема экспериментального макета прибора управления «Интерфейс мозг-компьютер», где ЭФС – электрофизиологические стимулы; ЭФР – электрофизиологические реакции

В основе СЛАС положено выделение из сигнала повторяющихся конструкций с идентичными амплитудно-временными отношениями последовательностей максимальных и минимальный значений функции сигнала на протяжении фрагмента анализа выделенного ЭЭГ – паттернов (Рис. 2).

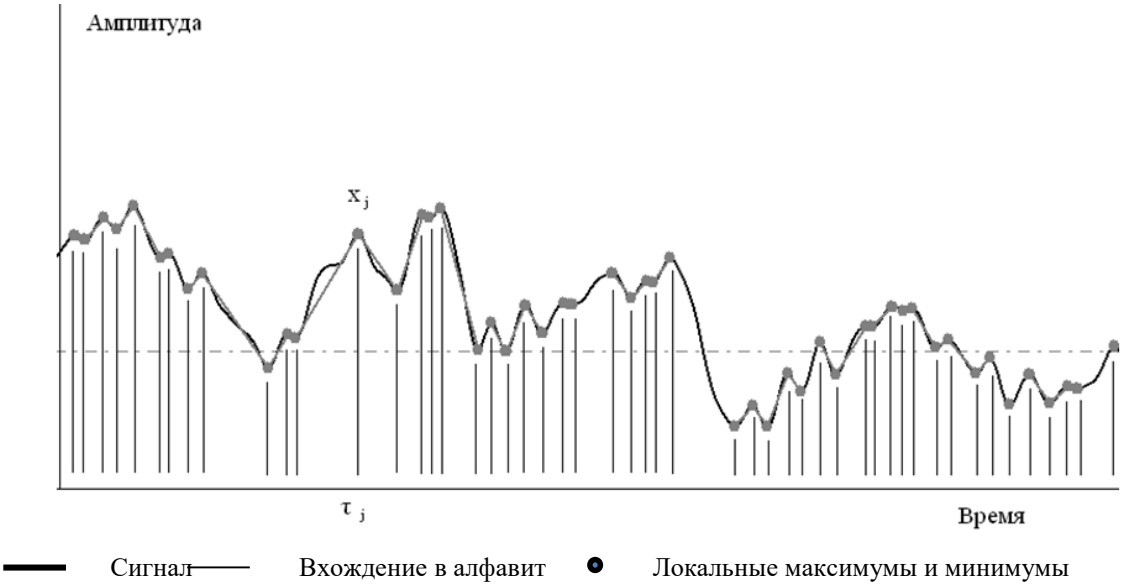


Рис. 2. Пример представления оцифрованного сигнала в виде конструкций амплитудно-временных отношений последовательностей его экстремумов

Суть метода основывается на информационной символьно-динамической модели, как модификации метода структурно-лингвистического анализа сигналов (СЛАС). В соответствии с данным методом производится поиск в сигнале фазоамплитудных последовательностей – символов и формирование для анализируемого сигнала множества символов – алфавита. Принцип преобразования сигнала ЭЭГ в последовательность особых точек носит нелинейный характер и включает автосегментацию, что делает его устойчивым к шумам и изменению масштабов пространства, времени и амплитуды сигнала.

Текущее распределение амплитуд по отведениям ЭЭГ представлено на рис. 3.

Рис. 3. Пример пространственной структуры символа

Для выполнения экспериментальной проверки разработана программа высокопроизводительного структурно-лингвистического анализа сигналов ЭЭГ. Выполнена экспериментальная проверка полученного инструментального комплекса с использованием сигналов ЭЭГ из открытого источника. Полученные значения количество символов и энтропии Шеннона для алфавитов ЭЭГ испытуемых, находящихся в состоянии депрессии и испытуемых в нормальном состоянии представлены на рис. 4.

При использовании таких вычисляемых параметров сигнала, как количество символов (размер алфавита) и энтропия Шеннона достигнута чувствительность обнаружения депрессивных состояний, превышающая 0,95.

Выводы. Разработана модель многоканального сигнала электроэнцефалограммы, отличающаяся от известных тем, что в ней распределения электрической активности по поверхности головы испытуемого представляются как информационные символы. Анализом временной последовательности (динамики) таких символов достигается возможность классификации интенсивности деятельности головного мозга испытуемого. Разработана методика обнаружения маркеров депрессивного состояния, базирующаяся на оценке изменений элементного состава множества паттернов, выделяемых в сигнале ЭЭГ.

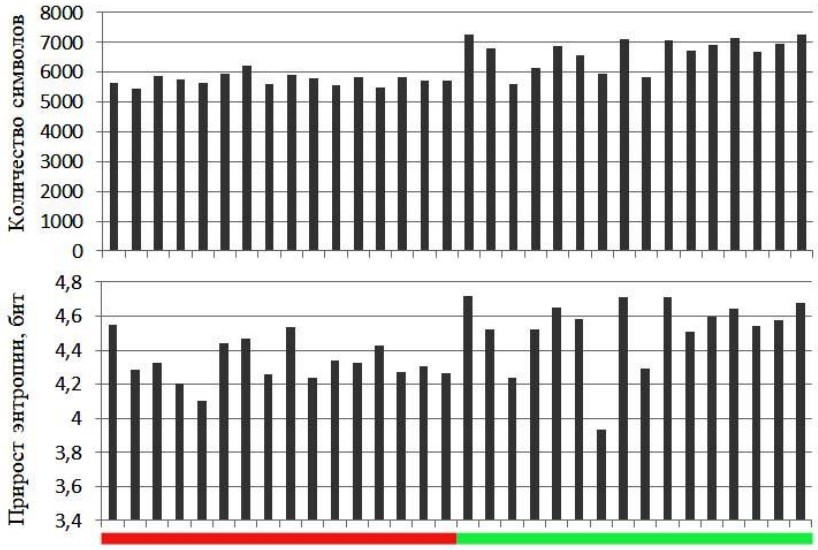


Рис. 4. Результат определения параметра количество символов и энтропии двух групп испытуемых, находящихся в состоянии депрессии (красный) и испытуемых в нормальном состоянии (зеленый)

Разработан алгоритм автоматизации и интеллектуализации процесса обнаружения маркеров утомляемости и депрессивного состояния в сигнале ЭЭГ, позволяющий автоматизировать выделение множества специфических паттернов, представленных амплитудно-временными структурами сигнала, и отличающийся от традиционных тем, что позволяет выполнять анализ сигналов в соответствии с информационной символьно-динамической моделью.

Выполнена экспериментальная проверка разработанных инструментов обработки и анализа сигналов ЭЭГ для выделения маркеров депрессивного состояния.

Показано, что предложенный метод может быть использован для обнаружения маркеров депрессивных состояний у сотрудников морского и речного флота. Чувствительность метода составляет не менее 95%.

СПИСОК ЛИТЕРАТУРЫ

1. Артемов С. И., Алексеев С. А., Рябков Я. И. Анализ модели электроэнцефалограммы специалистов морского и речного флота как суперпозиции излучений множества источников // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. СПб. : СПОИСУ, 2022. 626 с.
2. Артемов С. И. Инвариантное кодирование сигналов электроэнцефалограммы для исследования ее информационных характеристик // Прикладные проблемы безопасности технических и биотехнических систем. СПб., 2019. С. 37-41.
3. Артемов С. И. Информационная модель электрофизиологических сигналов мозга [электронный ресурс] // Universum: Химия и биология. 2015. № 12 (19). URL: http//7universum.com/ru/nature/archieve/item/2809 (дата обращения: 21.06.2023).
4. Артемов С. И. Многоканальная обработка данных электроэнцефалограммы на основе структурно-лингвистического анализа сигналов // Актуальные проблемы естественных и математических наук в России и за рубежом. Н., 2015. № 2. С. 100-103.

УДК 681.3.06

АКТУАЛИЗАЦИЯ БАЗЫ ДАННЫХ И ЗНАНИЙ ИТ КЛАССА «EAM» ПРИМЕНИТЕЛЬНО К АО «ЦЕНТР СУДОРЕМОНТА «ЗВЕЗДОЧКА»

Бондаренко Андрей Игоревич, Головизнина Ольга Игоревна, Алексеев Анатолий Владимирович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 194064, Россия
e-mails: bear555.ru@gmail.com, golovizninaolga92@yandex.ru, 25st1@bk.ru

Аннотация. В статье рассматриваются, анализируются и ранжируются по критериям проектного качества и эффективности эксплуатации информационные технологии и реализующие их программные средства и программные комплексы (EAM–системы) автоматизации процессов учета, технического обслуживания и ремонта основных фондов, в том числе с учетом факторов информационной живучести, применительно к условиям АО «Центра судоремонта «ЗВЕЗДОЧКА». Квалиметрическое ранжирование технологий EAM – систем позволило обоснованно рекомендовать к внедрению в морских проектно-конструкторских бюро, на судостроительных и судоремонтных предприятиях программное средство «NERPA» при конкурентном превосходстве в 4,5% и перспективности развития 95,7%.

Ключевые слова: EAM; ОА центр судоремонта «ЗВЕЗДОЧКА»; информационные технологии; жизненный цикл, ранжирование.

UPDATING OF DB AND RANKING OF IT CLASS «EAM» IN ZHTS OMT TYPE JSC SHIP REPAIR CENTER «ZVEZDOCHKA»

Bondarenko Andrey, Goloviznina Olga, Alekseev Anatoly
St. Petersburg State Marine Technical University,
3 Lotsmanskaya St, St. Petersburg, 194064, Russia
e-mails: bear555.ru@gmail.com, 25st1@bk.ru

Absrtact. The report examines and analyzes the information survivability of technologies and software systems of the EAM class that provide automation of accounting processes, maintenance and repair of fixed assets of the enterprise in relation to the conditions of JSC «Ship Repair Center «ZVEZDOCHKA». Qualimetric ranking of technologies and EAM systems, including taking into account the protection from operator errors caused by the functional and algorithmic complexity of use, allowed us to reasonably recommend the NERPA software tool for implementation in marine design bureaus, shipbuilding and ship repair enterprises with a competitive advantage of 4.5 % and a development prospect of 95.7 %.

Key words: EAM; JSC ship repair center «ZVEZDOCHKA»; information technology; life cycle; ranking.

Введение. Развитие глобальных транспортных систем становится приоритетным видом деятельности в бизнесе и политике ведущих стран мира. Так, в РФ к числу таких систем отнесен водный транспорт, развитие которого обуславливает судостроение в качестве базовой отрасли при внедрении в нее наукоемких инновационных технологий и современной организации производства. Создана судостроительная корпорация, объединяющая ведущие судостроительные предприятия и проектные организации как центрального, так и регионального назначения.

Развитие судостроения и его конкурентоспособность связаны с целым рядом факторов, снижающих себестоимость продукции. К их числу необходимо отнести такие, как сокращение затрат на проектирование и постройку судов, углубленную специализацию предприятий, уменьшение доли затрат рабочей силы за счет повышения производительности труда при одновременном обеспечении требуемого качества изделий.

Снижение затрат, связанных с проектированием и постройкой судов, невозможно без комплексного использования информационных технологий (ИТ) различных классов, но, безусловно, в информационно защищенном исполнении (ЗИ) [1].

Среди факторов ЗИ, как известно, обязательно следует учитывать защиту используемых программных средств (ПС) и их комплексов (ПК) от возможных (случайных), а также преднамеренных (в случае инсайдеров) ошибок операторов в разных вариантах. И чем выше функциональная сложность ПС и ПК, тем большее значение имеет фактор деструктивного воздействия, неустойчивости функционирования и ограниченной информационной живучести наряду с другими, а, следовательно, требует внимания и контроля при выборе и внедрении соответствующих ПС и ПК в производство.

Несколько классов ИТ и реализующих их программных средств (ПС) интегрированы в ИТ АСУП (автоматизированная система управления предприятием), предназначенную для решения задач планирования и управления различными видами деятельности предприятия [2], включая задачи и технологии:

- управления цепочками поставок (SCM);
- планирования ресурсов предприятия (ERP);
- планирования производства (MRP, MRP II).

Одной из таких ИТ в классе АСУП является система EAM (Enterprise Asset Management System) - логическое развитие компьютерных систем управления ремонтами, существующих уже более 20 лет.

К середине 90-х годов системы CMMS (Computerized Maintenance Management System) в составе EAM были постепенно расширены функциональностью по управлению закупками (МТР), складскими запасами, людскими ресурсами, документооборотом и рядом других возможностей, что позволило вывести данные системы на качественно новый уровень с точки зрения бизнес-преимуществ для компании.

EAM-система предназначена для автоматизации бизнес-процессов учета, технического обслуживания и ремонта основных фондов, обеспечивая комплексную и согласованную деятельность организации, целью которой является идеальное управление физическими активами и режимами их работы, рисками и расходами в процессе жизненного цикла для достижения и выполнения стратегических планов организации.

EAM дает возможность уменьшения простоя оборудования, сокращения затрат на техобслуживание, ремонты и материально-техническое снабжение [3].

Методология EAM дает возможность за счет применения ИТ, не прибегая к закупкам нового оборудования, увеличить производственную мощность предприятия, согласованно управляя такими процессами как:

- ТОиР - техническое обслуживание и ремонт;
- МТС - материально-техническое снабжение;
- ТОиР - управление складскими запасами (запчасти для);
- прикладное управление финансами, персоналом и документами.

EAM-системы появились из CMMS-систем (систем управления ремонтами). Сейчас модули EAM являются составляющими крупных пакетов управленческого программного обеспечения, таких как ERP-систем (IFS

Applications, Oracle E-Business Suite, Галактика ERP и др.). Каждому EAM-объекту любого уровня присваивается карточка-паспорт, которая учитывает десятки административных, технических и экономических параметров оборудования. Каждая такая карточка-паспорт оборудования может иметь связь с корпоративной СУБД для передачи данных.

Фактически, задачей EAM-системы является оказание поддержки руководства предприятия в поиске оптимального соотношения между затратами на изменение и ремонт производственных фондов с потерями, которые могут возникнуть вследствие внеплановой остановки производства. В то же время EAM-системы призваны решать основные задачи:

1. Управления финансами.
2. Управления материально-техническим обеспечением (materials management) - подходящие модули обычно объединяются с системами управления закупками, дают возможность автоматически регистрировать поступление комплектующих и деталей на склад, контролируют заказы на доставку.
3. Управления кадрами (HRMS).
4. Управления активами (asset management) - полное описание активов, предупредительный ремонт, руководство запросами на обслуживание, составление расписания и смет на работы.

Функциями EAM-системы являются:

1.Формирование целостной базы оборудования и нормативно-справочной информации по его обслуживанию.
2. Составление плана мероприятий по техническому обслуживанию и ремонтам оборудования (ТОРО).
3. Организация заявочной компании.
4. Наблюдение за процессами обслуживания и ремонта оборудования.
5. Контроль реальных затрат в разрезе объектов и мероприятий.
6. Фиксация главных технологических подходов в работе оборудования (выходы из строя, простои).
7. Прорабатывание требующихся мероприятий по обслуживанию на базе данных АСУТП.
8. Обеспечение передачи необходимой информации в ERP.
9. Проведение оценки информации по ТОРО и организация корпоративной отчетности.

EAM-системы являются одной из составляющих комплексных корпоративных информационных систем и дают возможность:

- сократить производственные расходы и стоимость владения главными производственными фондами;
- увеличить их окупаемость;
- повысить результативность планирования ремонтов;
- гарантировать действенность и безопасность производства.

Все более расширяющийся круг компаний и организаций в российской нефтегазовой отрасли, проявляющих интерес к развитию систем управления ТОРО на базе современных ИТ, объясняется тем, что доля операционных затрат на ТОРО в общей структуре себестоимости добычи может достигать 25-30 %. Поэтому даже относительно небольшое в процентном отношении снижение затрат может существенно улучшить общие показатели эффективности предприятия.

Обычный, практически типовой, набор задач ТОРО включает:

- оперативный производственный учет наличия оборудования в сегментах как эксплуатации, так и ремонта или временного хранения;
- сбор, обработку и хранение сведений о техническом состоянии оборудования, получаемых как средствами инструментальной диагностики, так и в результате визуальных наблюдений за работой оборудования;
- регистрацию всех событий, связанных с нарушениями или отклонениями от нормальных режимов работы оборудования, планирование и организацию ремонтно-восстановительных мероприятий по устранению нарушений, отказов или аварий;
- планирование мероприятий, направленных на предупреждение отказов в работе оборудования (планово-предупредительные ТОРО);
- оперативное управление процессами ТОРО, выполняемыми как внешними сервисными организациями, так и собственными ремонтными подразделениями;
- годовое планирование ТОРО и оценку потребности в ресурсах, необходимых для ремонтно-эксплуатационных нужд.

К числу положительных сторон EAM в составе АСУП относятся:

1.Сокращение трудоемкости процессов управления главными фондами.

2.Увеличение показателя готовности оборудования, повышение срока его работы.

3. Обеспечение совместного планирования ремонтов оборудования и уменьшение времени их проведения.

4.Увеличение продуктивности работы ремонтного персонала.

5.Сокращение объема складских запасов ТМЦ и оптимизация расходов на выполнение заявочной компании.

6.Способность оценить расходы и эффективность деятельности подразделений по обеспечению работоспособности оборудования.

7. Методология управления, с помощью которой можно повысить производственную мощность предприятия используя только ИТ, без приобретения нового оборудования.

В настоящее время система EAM — это полностью интегрированное программное решение, созданное для контроля за каждодневной эксплуатационной деятельностью капиталоемкого предприятия и сопровождения жизненного цикла его основных активов и фондов. Использование EAM-систем позволяет сократить время простаивания, уменьшаются затраты на техобслуживание оборудования, и эксплуатация базовых средств становится наиболее эффективной [4].

В результате квалиметрического исследования ИТ класса EAM по методологии применительно к условиям управления ремонтами и техническим обслуживанием инфраструктурных объектов типа «АО центр судоремонта «ЗВЕЗДОЧКА» была актуализирована ранее сформированная база данных и знаний (БДЗ) на интервале актуализации 1.09.2022-15.05.2023 с использованием технологии и робототехнического проектного комплекса (РПК) «АСОР-22.4» с учетом специфики объекта информатизации и сложившейся геополитической ситуации.

При этом, рассматривались EAM – системы, распространенные как на российском рынке, так и на зарубежном в контексте импортозамещения наиболее совершенных ПС и их ПК. Также при актуализации БДЗ учитывалась информация российской прессы, печатные материалы фирм–разработчиков и отзывы пользователей. Критериями выбора ПС и ПК из общего числа программного обеспечения (далее ПО) класса EAM – систем стали: функциональные возможности и свойства, эксплуатационные показатели, интегрируемость с ПС и ПК в составе АСУ и другими ИТ, ресурсные показатели и обеспеченность, эргономические показатели, популярность, отзывы, массовость на рынке, полнота информации о ПО.

Однако, наиболее значимым с индексом критериальной значимости 0,15 при общем числе критериев 12 был определен обобщенный показатель качества информационной защищенности контента ПС по данным сертификации (ОУС). Именно это позволило с учетом функциональной и алгоритмической сложности альтернативных вариантов ПС, ПК и соответствующей важности фактора информационной живучести и устойчивости, учесть одно из важнейших требований к современным ИТ и реализующим их ПС по обеспечению конфиденциальности данных (учитывает факторы качества защиты корпоративной, государственной и т.п. тайны), доступности (факторы разграничения доступа, надежности и информационной живучести, устойчивости функционирования, киберзащищенности), целостности (факторы возможности модификации данных), что в целом определяет интегральный уровень информационной защищенности (информационной безопасности (ИБ) и ЗИ ПС).

Сравнительный анализ был выполнен применительно к судостроительным, судоремонтным предприятиям и проектно-конструкторским бюро (при управлении ЖЦ ОМТ типа «АО центр судоремонта «ЗВЕЗДОЧКА») с целью решения следующих основных задач:

- оптимизации управления складскими процессами;
- сокращения издержек;
- переход к дистанционному управлению.

В ходе ранжирования конкурентными вариантами ИТ класса EAM (ТОП – 5) было принято целесообразным по методологии ранжирования считать:

1.«NERPA» [5]. У данного ПС агрегированный (сводный) показатель качества по методике квалиметрического SWOT-анализа (QSWOT) $Q = 6{,}32$; коэффициент конкурентного преимущества – $КП = 1{,}045$; коэффициент перспективности развития – $ПР = 0{,}957$;

2.«Галактика». $Q = 6{,}05$; $КП = 1{,}000$;$ПР = 1{,}000$;

3.«IBM Maximo». Q=6,19; КП=1,023; ПР=0,978;

4.«CalemEAM». Q=6,40; КП=1,57; ПР=0,946;

5.«InforEAM». Q=5,69; КП=0,940; ПР=1,064.

Заключение. В результате актуализации БДЗ ПС в классе EAM и актуализации соответствующего ряда ТОП-5 лидирующее средство «NERPA» при конкурентном превосходстве в 4,5 % и перспективности развития 95,7 % может быть обоснованно рекомендовано к внедрению в морских проектно-конструкторских бюро, на судостроительных и судоремонтных предприятиях типа «АО центр судоремонта «ЗВЕЗДОЧКА», что позволит повысить эффективность управления в целом жизненным циклом продукции и услуг.

СПИСОК ЛИТЕРАТУРЫ

1. Информационные технологии в судостроении: существующие системы, сферы и возможности их использования [Электронный ресурс] URL: https://uchimsya.com/a/qC363Pr9 (дата обращения: 24.05.2023).
2. Алексеев А. В. Информационные технологии в жизненном цикле морской техники: курс лекций. СПб.: СПбГМТУ, 2023.
3. Информационные системы управления основными фондами (EAM-системы) [Электронный ресурс]. URL: http://www.systematic.ru/informatsionnye_sistemy.html (дата обращения 25.05.2023).
4. Анализ рынка EAM-систем. [Электронный ресурс]. URL: http://www.galaktika.ru/eam/analiz-rynka-eam-sistem.html (дата обращения: 25.05.2023).
5. NERPA EAM — система управления основными фондами и активами предприятия [Электронный ресурс]. URL: https://www.novosoft.ru/nerpa/eam (дата обращения: 29.03.2023).

УДК 681.518, 65.011.56

АНАЛИЗ ВАРИАНТОВ ЧИСЛОВОГО МОДЕЛИРОВАНИЯ И ИССЛЕДОВАТЕЛЬСКОГО ПРОЕКТИРОВАНИЯ СИСТЕМ АВТОМАТИЗАЦИИ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОГО МОНИТОРИНГА СТРОИТЕЛЬСТВА СУДОСТРОИТЕЛЬНОГО ЗАКАЗА В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Миклуш Сергей Владимирович
АО «Адмиралтейские верфи»
Фонтанки р. наб., 203, Санкт-Петербург, 190121, Россия
e-mail: miklush.sv@ashipyards.com

Аннотация: Представлены результаты анализа вариантов прогнозирования проектных решений строительства судового заказа при аппроксимации модели успешной реализации заказа степенной функцией и показана целесообразность использования при планировании модели реального опережающего развития «20/10» при индексе степенной зависимости 0,639 в обеспечение 20% планируемого значения агрегированного показателя качества на момент времени 10% от заданного срока выполнения проекта. Предпочтение отдано принципам форсированного развития «50/20» при индексе 0,431 и принципу Парэто «80/20» при индексе 0,139. Рекомендовано использовать полученные результаты при использование модифицированного программного комплекса «Прогноз-2023.М» в защищенном исполнении, реализующего задачу мониторинга, прогнозирования и контроля результативности проектов на дату окончания проекта в отличие от программных комплексов планирования типа «MS Project», «1С: Предприятие». Показана возможность на качественно новом уровне решать задачу системной и объективной оценки вариантов управленческих решений.

Ключевые слова: прогнозирование; системные показатели; агрегирование показателей; степенной алгоритм; принцип Парэто; принцип реального опережающего развития.

ANALYSIS OF VARIANTS OF NUMERICAL MODELING AND RESEARCH DESIGN OF AUTOMATION SYSTEMS FOR ORGANIZATIONAL AND TECHNICAL MONITORING OF CONSTRUCTION AND SHIPBUILDING ORDERS IN PROTECTED EXECUTION

Miklush Sergey
JSC «Admiralty Shipyards»
203 Fontanka River Emb, St. Petersburg, 190121, Russia
e-mail: miklush.sv@ashipyards.com

Abstract. The results of the analysis of options for predicting design solutions for the construction of a ship order are presented when approximating the model of successful implementation of the order by a power function and the expediency of using the real advanced development model «20/10» when planning with a power dependence index of 0.639 to ensure 20% of the planned value of the aggregate quality indicator at the time point is shown 10% of the specified project completion time. Preference was given to the principles of forced development «50/20» with an index of 0.431 and the principle of Pareto «80/20» with an index of 0.139. It is recommended to use the obtained results when using the modified software package «Prognoz-2023.M» in a protected version, which implements the task of monitoring, forecasting and controlling the effectiveness of projects at the end of the project, in contrast to the planning software systems such as «MS Project», «1C: Enterprise» . The possibility of solving the problem of systematic and objective assessment of options for management decisions is shown at a qualitatively new level.

Keywords: prediction; system indicators; aggregation of indicators; power algorithm; Pareto principle; the principle of real advanced development.

Введение. В современном судостроении все большее значение приобретает создание цифровых двойников предприятий, включающие в себя процедуры цифровизации всех производственных процессов с целью оптимизации технологии, уменьшения издержек и повешения качества выпускаемой продукции [1]. Мониторинг и моделирование являются основными направлениями, обеспечивающими наиболее полную и достоверную картину продвижения строительства судового заказа, позволяющие определить «бутылочные горлышки» в технологических процессах и подготовить варианты для принятия управленческого решения в соответствии с развитием ситуации на данный момент времени и прогнозированием влияния на конечный результат в целом.

В современных программных комплексах планирования производства, типа «MS Project», «1С: Предприятие», отсутствует функция оценки продвижения проекта, с последующим прогнозированием влияния на достижение конечного результата с элементами поддержки принятия управленческих решений.

Основной задачей построения систем мониторинга производственных процессов в судостроении является обеспечение своевременной и достоверной информации о влияние степени продвижения всех производственных процессов на конечный результат строительства судового заказа в целом, базирующейся на современных методах числового анализа, моделирования и прогнозирования.

Решение. Технологические процессы в судостроительном производстве имеют сложносоставную структуру и множество переплетающихся взаимосвязей, что делает мониторинг и моделирование процесса строительства судового заказа достаточно сложной и трудоемкой задачей без средств автоматизации и интеллектуальной поддержки принятия решений.

Принимая во внимание сложность и многообразие процессов, основной методологией при проведении моделирования таких систем целесообразно считать квалиметрический анализ с формированием агрегированного (системного) показателя качества (АПК), включающего в себя частные и групповые показатели качества, охватывающие весь процесс строительства судового заказа [2].

В настоящее время известно множество алгоритмов агрегирования частных показателей качества в сводный [3], включая методы:

- равномерной оптимальности АПК по ЧПК;
- справедливого компромисса по ЧПК;
- среднестепенной функции оптимальности;
- гармонической оптимальности;
- пессимистической оценки ЧПК и гарантированного результата АПК;
- максимальной (гипотетической) эффективности;
- последовательных уступок по АПК;
- идеальной точки по АПК;
- минимизации сумм нормированных отклонений АПК;
- эвристических решений;
- комбинированного решения многовекторных задач;
- анализа и синтеза при информационном дефиците профессора Н.В. Хованова;
- анализа иерархий Томаса Саати;
- множество полимодельных методов (отношений критериев; модельных предпочтений и квалиметрической ранговой оптимизации; анализа, синтеза и оптимизации решений; ранговой партнерской сертификации качества).

Из всех приведенных методов, только полимодельный метод анализа сложных систем и процессов позволяет существенно уменьшить методологические погрешности многокритериального оценивания, и является наиболее подходящим для формирования представления о продвижении строительства судового заказа.

Для прогнозирования конечной результативности производственного процесса строительства и оценки текущего значения степени продвижения строительства рассмотрены следующие варианты числового моделирования:

- линейная модель, подразумевает равномерное развитие процессов во времени. Подходит для простых и отработанных технологических процессов, не предусматривает возможные недостатки и сложности в реализации;
- модель по принципу Парето, определяет, что за первые 20% времени, отведенного для производственного процесса, выполняется 80% от запланированного объёма работ и достигаемого результата;
- модель форсированного развития, определяет, что первые 20% времени, отведенного для производственного процесса, выполняется 50% от запланированного объёма работ и достигаемого результата;
- модель реального опережающего развития, первые 10% времени, отведенного для производственного процесса, выполняется 20% от запланированного объёма работ и достигаемого результата.
- Расчет требуемого уровня результативности процесса $R_Т$ на текущий момент времени $Д_т$ осуществляется с использованием модели вида

$$R_Т = 100 \times (\frac{Д_Т - Д_Н}{Д_О - Д_Н})^n \quad (1)$$

где: $Д_Н$ – дата начала процесса, $Д_О$ – дата окончания процесса, n – индекс степенной зависимости, выбираемый в соответствии с данными таблицы 1 для различных видов модели результативности.

Таблица 1

Значения индексов модели результативности

Модель результативности	**Значение индекса n**
Линейная «20/20»	1,000
Опережающего развития «20/10»	0,639
Форсированного развития «50/20»	0,431
По Парето «80/20»	0,139

Результат вычисления $R_Д$ представляется на главной экранной форме интерфейса мониторинга и оценки результативности строительства судового заказа программного комплекса «Прогноз-2023.М», приведенном на рис. 1, а график зависимости при различных значениях n – на рис. 2.

Руководитель строительства заказа, исходя из опыта и учета специфики проекта имеет возможность выбирать в соответствии с каким типом модели прогнозировать результативность продвижения производственного процесса.

Этапы	Решаемые задачи	ИКЗ (важность), %	Руководитель, исполнители	Начало	Окончание	Текущий результат	Прогноз по задаче
	Критерий (ГПК). Ожидаемая результативность, %:			01.03.20	30.08.23	97,6	97,9
	Проект решения	*Цель достигается*			*Действовать по плану*		
	Отставание, резерв(дней)/Рекомендуемое текущее значение:				-31	*99,94*	п
	1. УП-1 Сборка, сварка и конструкция секций основного	4,0%		30.06.20	30.03.21	100,0	100,0
	2. УП-2 Сборка, сварка и конструкция секций на верхней	3,0%		30.03.21	30.12.21	100,0	100,0
	3. УП-4 Закладка судна	2,0%		01.03.20	30.06.20	100,0	100,0
	4. УП-5 Установка и сварка секций на стапеле	2,0%		01.02.21	10.10.21	100,0	100,0
	5. УП-6 Установка и сварка туннеля носового	1,0%		01.03.21	30.04.21	100,0	100,0
	6. УП-8 Изготовление, установка и сварка корпусных	2,0%		01.09.21	10.10.21	100,0	100,0
	7. УП-9 Качество сварных швов корпуса по результатам	4,0%		10.10.20	10.10.21	100,0	100,0
	8.. УП-10 Конструкция помещений группы «А» корпуса и	10,0%		01.06.22	30.12.22	100,0	100,0
	9. УП-11 Конструкция помещений группы «Б» корпуса и	14,0%		01.01.23	30.08.23	90,0	92,0
	10. УП-12 Установка и испытания на непроницаемость	1,0%		01.02.21	30.03.21	100,0	100,0
	11. УП-13 Непроницаемость монтажных швов НО корпуса	3,0%		01.02.21	10.10.21	100,0	100,0
	12. УП-14 Непроницаемость кингстонных ящиков, канала	2,0%		01.04.21	30.06.21	100,0	100,0
ГПК по этапам ЖЦ на стадии постройки	13. УП-15 Непроницаемость помещений группы «А»,	7,0%		01.07.21	30.11.21	100,0	100,0
	14. УП-16 Непроницаемость монтажных швов НО до	3,0%		01.09.20	30.03.21	100,0	100,0
	15. УП-17 Непроницаемость помещений группы «А», не	5,0%		01.09.21	30.12.21	100,0	100,0

Тип модели:
Л - линейная
П - закон Парето, "80/20".
Ф - модели форсированного развития "50/20";
Р - модели реального орежающего развития "20/10";
Др - другие модели.

Рис. 1. Фрагменты главной экранной формы ПК «Прогноз-2023.М»

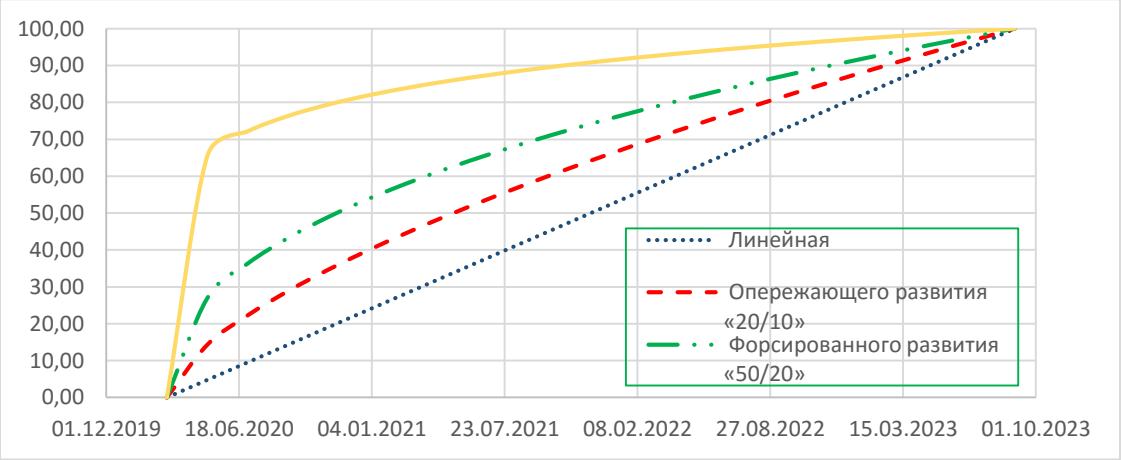


Рис. 2. Влияние выбора модели на результативность процесса

Анализ графиков показывает возможность эффективного использования ПК «Прогноз-2023.М» в защищенном исполнении для реализации задачи мониторинга (непрерывного наблюдения), прогнозирования и контроля результативности группы проектов на дату их окончания.

В отличие, например, от ПК типа «MS Project», «1С: Предприятие» в ПК «Прогноз-2023.М» на качественно новом уровне решается задача системного (по значениям АПК и ГПК) прогнозирования с более адекватной (объективной оценкой) вариантов управленческих решений в целом.

При этом повышается значимость получаемых оценок (системных показателей), что повышает требования к защищенности данных. Реализуются повышенные требования по информационной безопасности, прежде всего, усилением разграничения доступа с назначением грифа не ниже «ДСП», а также соответствующей двухфакторной аутентификацией, сегментированием данных, используемых в системе, повышением достоверности вводимых данных, например, за счет технологий радиочастотной идентификации [4] и т.п.

Заключение. В сравнении результатов прогнозирования, полученных при использовании указанных вариантов числового моделирования продвижения проектных процессов строительства судостроительного заказа, наиболее предпочтительным, следует считать модель форсированного развития «20/10», в виду необходимости выполнения большего количества работ на начальном этапе и организации технологических процессов с целью формирования реального задела и исключения возможных задержек. Это позволит нейтрализовать дефицит времени, возникающий из-за непредвиденных обстоятельств типа замечаний заказчика, конструкторских доработок

проекта, технологических пауз в виду «накладывающихся» производственных процессов. Это обеспечит соблюдение «сроковой дисциплины выполнения работ на качественно новом уровне, решение системной задачи оценки успешности выполнения поставленных задач, выработку и оптимизацию вариантов поддержки принятия управленческих решений.

Для отдельных технологических процессов, особенно, на заключительных этапах строительства заказа, когда технологические процессы тесно «переплетаются» и форсировать работы приходится на «всех направлениях», целесообразно использовать модель по принципу Парето, что позволит сконцентрировать технологические и трудовые ресурсы на выполнение особенно важных производственных процессов в обеспечение выполняя строительства судового заказа в утверждённые сроки.

СПИСОК ЛИТЕРАТУРЫ

1. Прохоров А., Лысачев М. Цифровой двойник. Анализ, тренды, мировой опыт. Изд. первое, испр. и доп. М.: АльянсПринт, 2020. 401 с.
2. Миклуш С. В., Александров В. Л., Алексеев А. В. Концепция развития судостроительного предприятия на основе интеграции производственных процессов по системному критерию качества // Имитационное комплексное моделирование морской техники и морских транспортных систем (ИКМ МТМТС – 2023). СПб., 2023. С. 148-154.
3. Алексеев А. В. Концептуальные аспекты развития критических объектов морской техники и морской инфраструктуры. СПб.: Морские интеллектуальные технологии. 2015. Т. 1. № 2 (28). С. 48-58.

УДК 519.687.1

АЛГОРИТМ ОПТИМИЗАЦИИ МЕСТОПОЛОЖЕНИЯ ЦЕНТРА УПРАВЛЕНИЯ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ СИСТЕМОЙ ВИДЕОНАБЛЮДЕНИЯ В ВЫСОТНОМ ЗДАНИИ МОРСКОЙ ИНФРАСТРУКТУРЫ

Плотников Павел Владимирович[1], Алексеев Сергей Алексеевич[2]
[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича
Большевиков пр., 22, корп.1, литера А, Ж, Санкт-Петербург, 193232, Россия
[2] Государственный университет морского и речного флота имени адмирала С. О. Макарова,
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: pavplot@gmail.com, ksgati@yandex.ru

Аннотация. В статье рассматривается задача оптимизации местоположения центра управления в защищенном исполнении на примере системы видеонаблюдения в 3D пространстве. Приведен алгоритм расчета оптимального местоположения центра управления системой видеонаблюдения на плоскости и в 3D пространстве в реальном времени. Процесс поиска решения заключается в простом подсчете значений выражений при конкретных значениях параметра и может быть автоматически проведен вычислительными устройствами за малое время, при этом полученные решения являются численными и точными.

Ключевые слова: задача размещения Ролса; задача оптимизации; тропическая оптимизация; прямоугольная метрика; идемпотентное полуполе; полное решение.

AN ALGORITHM FOR OPTIMIZING THE LOCATION OF THE CONTROL CENTER IN A PROTECTED VERSION BY A VIDEO SURVEILLANCE SYSTEM IN A HIGH-RISE BUILDING OF THE MARINE INFRASTRUCTURE

Plotnikov Pavel [1], Alekseev Sergey[2]
[1]St. Petersburg State University of Telecommunications named after Prof. M.A.Bonch-Bruevich
22 Bolshevikov Av, 22, bld 1, lit. A, Zh, St. Petersburg, 193232, Russia
[2] Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: pavplot@gmail.com, ksgati@yandex.ru

Absrtact. The article deals with the problem of optimizing the location of the control center in a secure design using the example of a video surveillance system in 3D space. The algorithm for calculating the optimal location of the control center of the video surveillance system on the plane and in 3D space in real time is given. The process of finding a solution consists in a simple calculation of the values of expressions for specific parameter values and can be automatically carried out by computing devices in a short time, while the solutions obtained are numerical and accurate.

Keywords: Rolls placement problem; optimization problem; tropical optimization; rectangular metric; idempotent half-field complete solution.

Введение. На практике большое значение имеет решение задач выбора мест размещения объектов, пространственно-распределенных информационных, социальных, экономических и иных систем. В качестве примеров можно привести такие задачи, как выбор мест размещения маршрутизаторов сети передачи данных, центров обработки информации в распределенных вычислительных сетях, перегрузочных узлов на транспортной

сети, обоснование распределения на некоторой территории элементов производственного комплекса, расчет оптимального размещения в городе магазинов шаговой доступности и др.

Задачи размещения объектов в пространстве образуют широкий класс задач оптимизации. Задачи размещения можно разделить по способу задания ограничений и по выбору критерия оптимальности. Основная **цель** при решении таких задач состоит в определении оптимального места расположения нового объекта с учетом местоположения уже имеющихся.

При описании задачи размещения следует рассматривать два множества: объекты, которые уже расположены в точках или на маршрутах в области исследования, и объекты, для которых оптимальное место расположения следует найти. Также нужно задать параметры пространства, в котором объекты находятся, и выбрать метрику, в которой необходимо оценивать и оптимизировать расстояние или время.

Традиционно рассматривают два типа задач размещения: минисуммные (минимизируется сумма расстояний) и минимаксные (минимизируется максимальное расстояние) задачи размещения.

Для описания и решения минимаксных задач размещения с прямоугольной и чебышевской метрикой достаточно полезным оказывается применение методов тропической оптимизации. При этом задача сводится к минимизации рациональной функции в терминах тропической математики.

Тропическая (идемпотентная) математика представляет собой область прикладной математики, связанную с изучением полуколец с идемпотентным сложением.

За последние десятилетия эта область превратилась в один из наиболее быстро развивающихся разделов математики, роль которого как теоретической дисциплины и эффективного инструмента решения практических задач в экономике, технике, управлении и других областях постоянно растет.

Решение задач пространственного (3D) размещения объектов зависят от метрики, в которой вычисляется расстояние между объектами. В данной статье рассматривается решение задач пространственного размещения объектов в прямоугольной метрике с использованием методов тропической (идемпотентной) математики.

Основная часть. В статье рассматривается минимаксная задача (Ролса) размещения на плоскости и в 3D пространстве с прямоугольной метрикой, которая может быть представлена в терминах идемпотентной алгебры. Подход к решению основывается на преобразовании задач размещения к экстремальным задачам. В ходе исследования были получены аналитические зависимости, предлагающие на основе известных данных о размещении обслуживаемых объектов (видеокамер) найти оптимальные зоны размещения обслуживающих их объектов (маршрутизаторов, серверов, и др.). При этом требуется разместить новый обслуживающий объект так, чтобы минимизировать расстояние от этого объекта до самого удаленного из обслуживаемых объектов.

Полученные результаты позволяют сделать вывод, что решением задачи может быть не только одна точка, где размещение будет оптимальным, а зона или поле оптимального размещения. Это весьма важно с прикладных позиций, т.к. позволяет учесть возможные ограничения задачи.

Важным преимуществом предлагаемого алгоритма является простота итоговых формульных зависимостей, позволяющая легко использовать его при создании и развитии информационных и иных систем искусственного интеллекта.

Решение задачи оптимального размещения центрального сервера управления сетью локальных видеокамер в высотном здании может быть полезным при проектировании и решении задачи повышения эффективности функционирования этой сети в целом. В статье последовательно представлены алгоритмы решения двух задач оптимизации на плоскости и в пространстве [1-3].

Сначала сформулируем в общем виде задачу оптимизации на плоскости.

Пусть необходимо собирать, обрабатывать и хранить информацию, поступающую с n видеокамер локальной сети. Координаты этих видеокамер задаются векторами $v_i = (v_{1i}, v_{2i})^T \in R^2$, где $i = 1, \dots, n$. Задача размещения состоит в том, чтобы найти оптимальное местоположение центрального сервера (центра управления), которое задано неизвестным вектором $x = (x_1, x_2)^T$. При этом, необходимо минимизировать расстояние от этого сервера до самой дальней видеокамеры. Основная задача (критерий) состоит в снижении величины затухания сигнала, которое прямо пропорционально расстоянию, например: длине кабеля, что соответственно оправдывает минимаксную постановку задачи.

Прокладка оптоволоконных и проводных сетей осуществляется вдоль или внутри каналов других сетей. Поэтому для описания и решения задач оптимального размещения может быть использована прямоугольная метрика.

Вычисление расстояний между объектами является важным этапом решения любой задачи пространственной оптимизации. Часто способ измерения расстояний обусловлен рассматриваемой моделью, но в некоторых случаях, четких критериев для однозначного определения метрики выделить не удается. В представленной задаче в качестве метрики выбрана прямоугольная (L_1 – метрика) метрика в силу того, что она проста в описании и позволяет учитывать не прямолинейный монтаж сети видеокамер.

Прямоугольной метрикой в R^n пространстве предлагается называть величину, характеризующую расстояние между двумя точками $A(x_1, x_2, \dots, x_n)$ и $B(y_1, y_2, \dots, y_n)$ и вычисляемую по следующей формуле:

$$\rho(A,B) = \sum_{i=1}^{n} |x_i - y_i|.$$

Для решения задачи 1-центра существует три подхода:

1.геометрический подход с нахождением оптимального положения управляющего объекта методами построений;

2.итерационный метод моделирования решения задачи размещения с использованием компьютерных мощностей;

3.получение решения в явном виде методами идемпотентной алгебры.

Первый подход требует больших вычислительных мощностей, если количество точек в исходном наборе велико, и размерность пространства решений больше двух.

Второй подход основан на последовательном переборе по определенному правилу точек пространства и получения одноточечного множества решений, что на практике не всегда оказывается удобным для использования. При этом, стоит отметить, что незначительное изменение исходного множества точек потребует полного пересчета всей задачи в случае сбоя или ошибочного ввода данных.

Третий подход имеет важные преимущества, а именно:

1.полученное решение оказывается некоторой областью в пространстве R^n, что позволяет пользователю выбирать ту точку, которая ему кажется наиболее подходящей для решения поставленных практических задач с сохранением значения целевой функции расстояния;

2.вычислительные формулы задаются в явном виде, сами расчетные формулы содержат только операции сложения и умножения, перерасчет в случае ошибочного ввода данных или изменения исходного множества может быть произведен с использованием значительно меньших затрат.

Задача оптимального размещения для сети локальных видеокамер состоит в поиске минимума функции

$\varphi(\mathrm{x}) = \max\limits_{1\le i\le n}(\rho(v_i,x) + w_i) = \max\limits_{1\le i\le n}(|v_{1i} - x_1| + |v_{2i} - x_2| + w_i) = \varphi(x_1,x_2)$, которая определяет максимальное по всем $\boldsymbol{i}$ расстояние в прямоугольной метрике от центра управления системой (сервера) $\boldsymbol{x}$ до видеокамер $\boldsymbol{v_i}$ - с учетом дополнительного слагаемого $\boldsymbol{w_i}$. Числа $\boldsymbol{w_i}$ отражают дополнительные затраты, связанные с высотностью зданий и дополнительных затрат на пространственное планирование системы внутри сервера локального управления.

Оптимальное решение задачи размещения точечного объекта на плоскости сводится к нахождению минимума $\varphi(\mathrm{x})$, то есть

$$\phi = \max_{x\in R^2} \varphi(x). \quad (1)$$

Решение задачи в численном виде, может быть сформулировано следующим образом:

Минимум в задаче (1) равен

$$\phi = max(a+d, b+c)/2$$

и достигается тогда и только тогда, когда

$$\boldsymbol{x} = \begin{pmatrix} (2t-1)\phi + \dfrac{(1-t)(a+c)}{2} - t(b+d)/2 \\ \dfrac{(1-t)(a-c)}{2} - t(d-b)/2 \end{pmatrix}, t \in [0,1],$$

где

$$a = \max_{1\le i\le n}(w_i + v_{1i} + v_{2i}), \qquad b = \max_{1\le i\le n}(w_i - v_{1i} + v_{2i}),$$

$$c = \max_{1\le i\le n}(w_i + v_{1i} - v_{2i}), \qquad d = \max_{1\le i\le n}(w_i - v_{1i} - v_{2i}).$$

Предложенное решение численное, т.е. для любого набора данных v_i найдется оптимальное решение задачи размещения, при этом полученный результат примечателен тем, что найденная область задается не точкой, что могло бы быть в реальной задаче недопустимым в силу логистических ограничений, а отрезком прямой линии, что дает большую свободу в выборе оптимального положения искомого объекта.

Графическое представление полученного результата частного случая представлена на рис. 1. Точками обозначено исходное рассматриваемое множество v_i, отрезком прямой линии – оптимальное решение задачи размещения. Вертикальные отрезки вокруг v_i – характеристики w_i. Отрезком жирной линии обозначено оптимальное решение поставленной задачи размещения.

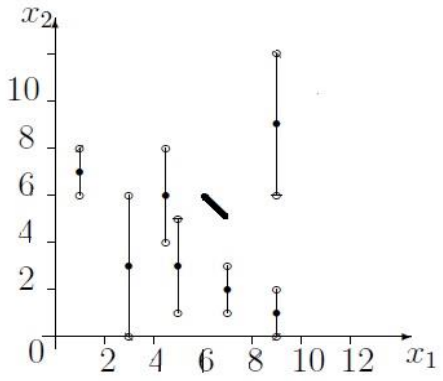


Рис. 1. Представление полученного результата частного случая

Выбор оптимального положения для размещаемой видеокамеры сопряжен с введением дополнительных ограничений. Ввести в задачу (1) дополнительные условия на область размещения можно следующим образом

(1.1)Прямоугольная область

$$\{f \le x_1 \le g,\ p \le x_2 \le q\}\ldots \qquad (1.1)$$

(1.2)Различные типовые прямые

(1.2.1) Горизонтальная и вертикальная прямые

$$\{\mathrm{f} \le \mathrm{x}_1 \le \mathrm{g},\ \mathrm{x}_2 = \mathrm{q}\} \text{ и } \{\mathrm{x}_1 = \mathrm{p}, \mathrm{f} \le \mathrm{x}_2 \le \mathrm{g}\}. \qquad (1.2.1)$$

(1.2.2) Произвольный отрезок прямой

$$\{\mathrm{f} \le \mathrm{x}_1 \le \mathrm{g},\ \mathrm{x}_2 = \mathrm{kx}_1 + \mathrm{q}\} \qquad (1.2.2)$$

Решение задачи (1) с дополнительными условиями (1.1) и (1.2) в численном виде:

Введем обозначения

$$a = \max_{1\le i\le n}(w_i + v_{1i} + v_{2i}), \qquad b = \max_{1\le i\le n}(w_i - v_{1i} + v_{2i}),$$
$$c = \max_{1\le i\le n}(w_i + v_{1i} - v_{2i}), \qquad d = \max_{1\le i\le n}(w_i - v_{1i} - v_{2i}),$$

а также

$$k = \max\left(\frac{a+c}{2}, a - q, c + p\right), \quad l = \max\left(\frac{b+d}{2}, b - q, d + p\right).$$

Выбор оптимального положения для размещаемой видеокамеры сопряжен с введением дополнительных ограничений. Ввести в задачу (1) дополнительные условия на область размещения можно следующим образом

(1.3)Прямоугольная область

$$\{\mathrm{f} \le \mathrm{x}_1 \le \mathrm{g},\ \mathrm{p} \le \mathrm{x}_2 \le \mathrm{q}\}\ldots \qquad (1.3)$$

(1.4)Различные типовые прямые

(1.4.1) Горизонтальная и вертикальная прямые

$$\{\mathrm{f} \le \mathrm{x}_1 \le \mathrm{g},\ \mathrm{x}_2 = \mathrm{q}\} \text{ и } \{\mathrm{x}_1 = \mathrm{p}, \mathrm{f} \le \mathrm{x}_2 \le \mathrm{g}\}. \qquad (1.4.1)$$

(1.4.2) Произвольный отрезок прямой

$$\{\mathrm{f} \le \mathrm{x}_1 \le \mathrm{g},\ \mathrm{x}_2 = \mathrm{kx}_1 + \mathrm{q}\} \qquad (1.4.2)$$

Решение задачи (1) с дополнительными условиями (1.1) и (1.2) в численном виде:

Введем обозначения

$$a = \max_{1\le i\le n}(w_i + v_{1i} + v_{2i}), \qquad b = \max_{1\le i\le n}(w_i - v_{1i} + v_{2i}),$$
$$c = \max_{1\le i\le n}(w_i + v_{1i} - v_{2i}), \qquad d = \max_{1\le i\le n}(w_i - v_{1i} - v_{2i}),$$

а также

$$k = \max\left(\frac{a+c}{2}, a - q, c + p\right), \quad l = \max\left(\frac{b+d}{2}, b - q, d + p\right).$$

Минимум в задаче (1.1) равен

$$\phi = \max((k + l)/2, k - g, l + f, (a + d)/2, (b + c)/2),$$

и справедливы следующие утверждения:

1) если $\phi = (k + l)/2$ при $k = (a + c)/2$ и $l = b - q$ или $k = a - q$, то $x_1 = \max\left(\frac{a+c}{4}, \frac{a-q}{2}\right) - \max\left(\frac{b-q}{2}, \frac{l}{2}\right)$, $x_2 = q$;

2) если $\phi = (k + l)/2$ при $k = (a + c)/2$ и $l = d + p$ или $k = c + p$, то

$$x_1 = \max\left(\frac{a + c}{4}, \frac{c + p}{2}\right) - \max\left(\frac{d + p}{2}, \frac{l}{2}\right), \quad x_2 = p;$$

3) если $\phi = k - g$, то $x_1 = g$, $x_2 = \max\left(-\max\left(\frac{-a+c}{2}, -q\right), p\right)$;

4) если $\phi = l + f$, то $x_1 = f,\ x_2 = \max\left(-\max\left(\frac{-b+d}{2}, -q\right), p\right)$;

5) если $\phi = (a + d)/2$, то

$$x_1 = (1 - t)\max\left(\frac{-a - d}{2} + k, f\right) - t\max\left(\frac{-a - d}{2} + l, -g\right),$$

$$x_2 = \frac{a - d}{2} - x_1;$$

6) если $\phi = (b + c)/2$, то

$$x_1 = (1 - t)\max\left(\frac{-b - c}{2} + k, f\right) - t\max\left(\frac{-b - c}{2} + l, -g\right),$$

$$x_2 = \frac{b - c}{2} + x_1,$$

где t – вещественное число, удовлетворяющее условию $0 \le t \le 1$.

Процесс поиска решения задачи (1) с ограничениями заключается в простом подсчете значений выражений при конкретных значениях параметра и может быть автоматически проведен вычислительными устройствами за малое время, при этом полученные решения являются численными и точными. Визуализация численного примера приведена на рис. 2.

Решение задач (1.2.1) и (1.2.2) в численном виде для наиболее общей задачи с ограничениями на отрезке. [2].

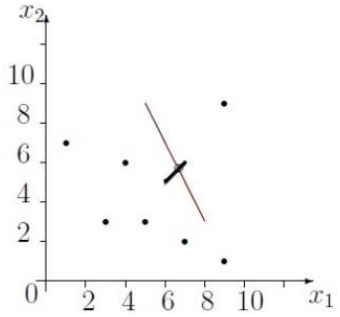


Рис.2. Численный пример

Введем обозначения

$$a = \max_{1\le i\le n}(w_i + v_{1i} + v_{2i}), \qquad b = \max_{1\le i\le n}(w_i - v_{1i} + v_{2i}),$$
$$c = \max_{1\le i\le n}(w_i + v_{1i} - v_{2i}), \qquad d = \max_{1\le i\le n}(w_i - v_{1i} - v_{2i}).$$

Тогда справедливы следующие утверждения:

1) если $k < -1$ или $k > 1$, то минимум в задаче (1.2.1) равен $\phi = \max\left(\frac{a+b}{2}, \frac{a(k+1)+c(k-1)}{2k}, \frac{b(k+1)+d(k-1)}{2k}, \frac{c+d}{2},\right.$

$$a + \min\big((k - 1)f, (k - 1)g\big), \qquad b - \max\big((k - 1)f, (k - 1)g\big),$$
$$c - max\big((k + 1)f, (k + 1)g\big), \qquad d + min((k + 1)f, (k + 1)g))$$

и достигается тогда и только тогда, когда

$$x_1 = (1 - t)\max\left(\min\left(\frac{\phi - a}{k - 1}, \frac{b - \phi}{k - 1}\right), \min\left(\frac{c - \phi}{k + 1}, \frac{\phi - d}{k + 1}\right), f\right) -$$
$$- t\max(\min(\frac{a - \phi}{k - 1}, \frac{\phi - b}{k - 1}), \min(\frac{\phi - c}{k + 1}, \frac{d - \phi}{k + 1}), -g),$$
$$x_2 = kx_1 + q;$$

2) если $-1 \le k \le 1$, то минимум равен

$$\phi = \max\left(\frac{a + b}{2}, \frac{a(k + 1) - d(k - 1)}{2}, \frac{b(k + 1) - c(k - 1)}{2}, \frac{c + d}{2},\right.$$
$$a + (k-1)g, \qquad b - (k - 1)f, \qquad c - (k + 1)g, \qquad d + (k + 1)f)$$

и достигается тогда и только тогда, когда

$$x_1 = (1 - t)\max\left(\frac{\phi - a}{k - 1}, \frac{c - \phi}{k + 1}, f\right) - t\max\left(\frac{\phi - b}{k - 1}, \frac{d - \phi}{k + 1}, -g\right),$$
$$x_2 = kx_1 + q;$$

Визуализация численного примера приведена на рис. 3.

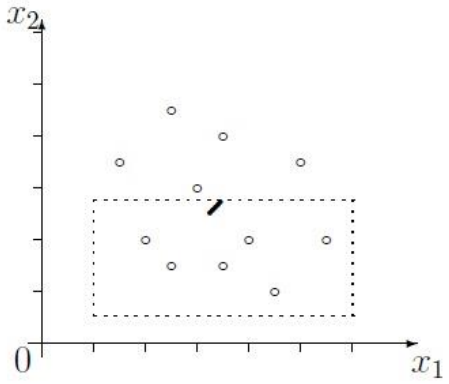


Рис. 3. Визуализация численного примера

Постановка задачи размещения центра управления системой видеонаблюдения в трехмерном пространстве. Поставленную задачу оптимального размещения на плоскости можно расширить на случай трехмерного пространства. Одним из примеров задачи, рассматриваемого типа является задача оптимального размещения управляющего сервера системой видеонаблюдения в высотном здании или центра управления разветвленной локальной сети управления, развернутой в офисном здании.

Пусть необходимо осуществлять управление системой из n видеокамер. Координаты этих видеокамер задаются векторами $\boldsymbol{vi} = (\boldsymbol{v1i}, \boldsymbol{v2i}, \boldsymbol{v3i})\boldsymbol{T} \in \boldsymbol{R3}$, где $\boldsymbol{i} = \boldsymbol{1}, \ldots, \boldsymbol{n}$. Задача размещения состоит в том, чтобы найти оптимальное положение центра управления, заданного вектором $x = (\boldsymbol{x1}, \boldsymbol{x2}, \boldsymbol{x3})\boldsymbol{T}$, чтобы он имел минимальное расстояние до самой удаленной видеокамеры. Целевая функция расстояния вычисляется по формуле:

$$\varphi(x) = \max_{1 \le i \le n}(\rho(v_i, x) + w_i) = \max_{1 \le i \le n}(|v_{1i} - x_1| + |v_{2i} - x_2| + |v_{2i} - x_2| + w_i) = \varphi(x_1, x_2, x_3).$$

В трехмерном случае коэффициенты $\boldsymbol{w_i}$ могут отражать дополнительные затраты, связанные с приоритетным статусом видеокамеры в рассматриваемой сети.

Задача оптимизации в трехмерном пространстве примет следующий вид

$$\mu = \max_{x \in R^3} \varphi(x). \quad (2)$$

Численное решение сформулированной задачи оптимизации может быть представлено в виде явных формул, сложность вычислений которых достаточно низкая. [2]

Введем обозначения

$$a = \max_{1 \le i \le n}(w_i + v_{1i} + v_{2i} + v_{3i}), \qquad b = \max_{1 \le i \le n}(w_i + v_{1i} + v_{2i} - v_{3i}),$$
$$c = \max_{1 \le i \le n}(w_i + v_{1i} - v_{2i} + v_{3i}), \qquad d = \max_{1 \le i \le n}(w_i + v_{1i} - v_{2i} - v_{3i}).$$
$$e = \max_{1 \le i \le n}(w_i - v_{1i} + v_{2i} + v_{3i}), \qquad f = \max_{1 \le i \le n}(w_i - v_{1i} + v_{2i} - v_{3i}),$$
$$g = \max_{1 \le i \le n}(w_i - v_{1i} - v_{2i} + v_{3i}), \qquad b = \max_{1 \le i \le n}(w_i - v_{1i} - v_{2i} - v_{3i}).$$

Введем дополнительные параметры

$a_1 = max(a + d,\ b + c)/2,\quad b_1 = max(a + f,\ b + e)/2,$
$c_1 = max(e + h,\ f + g)/2,\quad d_1 = max(c + h,\ d + g)/2,$
$e_1 = (a + b)/2,\quad f_1 = (c + d)/2,\quad g_1 = (e + f)/2,$
$h_1 = (g + h)/2,\quad k_1 = max(a + h,\ b + g,\ c + f,\ d + g)/2,$
$a_2 = max(b_1 + f_1,\ d_1 + e_1)/2,\quad b_2 = max(b_1 + h_1,\ d_1 + g_1)/2,$
$c_2 = max((e_1 + f_1)/2,\ a_1),\qquad d_2 = max((g_1 + h_1)/2,\ c_1),$
$e_2 = max(b_1 + d_1,\ f_1 + g_1,\ e_1 + h_1,\ 2k_1)/2,$

Тогда минимум в задаче (2) равен

$$\mu = \max\left(\frac{a_2 + b_2}{2}, \frac{2a_2 + d_2}{3}, \frac{2b_2 + c_2}{3}, \frac{c_2 + d_2}{2}, e_2\right),$$

и справедливы следующие утверждения:

1)если $\mu = (a_2 + b_2)/2$, то $x_1 = -b_2$,

$$x_2 = \begin{cases} \dfrac{(3b_1 - f_1)}{4} - \dfrac{b_2}{2}, & \text{если } a_2 = \dfrac{(b_1 + f_1)}{2}, \\ \dfrac{(-3d_1 + e_1)}{4} + \dfrac{b_2}{2}, & \text{если } a_2 = \dfrac{(d_1 + e_1)}{2}, \end{cases}$$

$$x_3 = (1-\alpha)max(-\mu+\alpha-x_1-x_2,\ -\mu+c-x_1+x_2,\ -\mu+e+x_1-x_2,\ -\mu+g+x_1+x_2) - \alpha max(-\mu+b-x_1-x_2,\ -\mu+d-x_1+x_2,\ -\mu+f+x_1-x_2,\ -\mu+h+x_1+x_2);$$

2)если $\mu = (2a_2 + d_2)/3$, то $x_1 = (2a_2 - 2d_2)/3$,

$$x_2 = \begin{cases} \dfrac{(2b_1 - f_1 - d_2)}{3}, & \text{если } a_2 = \dfrac{(b_1+f_1)}{2}, \\ \dfrac{(-2d_1 + e_1 + d_2)}{3}, & \text{если } a_2 = \dfrac{(d_1+e_1)}{2}, \end{cases}$$

$$x_3 = (1-\alpha)max(-\mu+\alpha-x_1-x_2,\ -\mu+c-x_1+x_2,\ -\mu+e+x_1-x_2,\ -\mu+g+x_1+x_2) - \alpha max(-\mu+b-x_1-x_2,\ -\mu+d-x_1+x_2,\ -\mu+f+x_1-x_2,\ -\mu+h+x_1+x_2);$$

3)если $\mu = (2b_2 + c_2)/3$, то $x1 = (2b_2 + c_2)/3$,

$$x_2 = \begin{cases} \dfrac{(2b_1 - h_1 - c_2)}{3}, & \text{если } b_2 = b_1^{1/2} * h_1^{1/2}, \\ \dfrac{(-2d_1 + e_1 + d_2)}{3}, & \text{если } b_2 = \dfrac{(d_1+g_1)}{2}, \end{cases}$$

$$x_3 = (1-\alpha)max(-\mu+\alpha-x_1-x_2,\ -\mu+c-x_1+x_2,\ -\mu+e+x_1-x_2,\ -\mu+g+x_1+x_2) - \alpha max(-\mu+b-x_1-x_2,\ -\mu+d-x_1+x_2,\ -\mu+f+x_1-x_2,\ -\mu+h+x_1+x_2);$$

4)если $\mu = (c_2 + d_2)/2$, то $x_1 = (c_2 - d_2)/2$,

$$x_2 = \begin{cases} (e_1 - f_1)/2, & \text{если } c_2 = (e_1+f_1)/2, \\ (g_1 - h_1)/2, & \text{если } d_2 = (g_1+h_1)/2 \\ (1-\alpha)\max\left(\dfrac{(-a_1-c_1)}{2} + b_1,\ -a_1+e_1,\ -c_1+g_1\right) - & \\ -\alpha\max(\dfrac{(-a_1-c_1)}{2} + d_1, - & \\ -a_1+f_1,\ -c_1+h_1), & \text{если } c_2 = a_1,\ d_2 = c_1 \end{cases}$$

$$x_3 = (1-\beta)max(-\mu+\alpha-x_1-x_2,\ -\mu+c-x_1+x_2,\ -\mu+e+x_1-x_2,\ -\mu+g+x_1+x_2) - \beta max(-\mu+b-x_1-x_2,\ -\mu+d-x_1+x_2,\ -\mu+f+x_1-x_2,\ -\mu+h+x_1+x_2);$$

5)если $\mu = e_2$, то $x_1 = (1 - \alpha)\ \max(2a_2 - 2e_2,\ c_2 - e_2) - \alpha\ \max(2b_2 - 2e_2,\ d_2 - e_2)$,

$$x_2 = \begin{cases} (b_1 - d_1)/2, & \text{если } e_2 = (b_1+d_1)/2, \\ \dfrac{(-f_1+g_1)}{2} + x_1, & \text{если } e_2 = (f_1+g_1)/2, \\ \dfrac{(e_1-h_1)}{2} - x_1, & \text{если } e_2 = (e_1+h_1)/2, \end{cases}$$

$$x_3 = (1-\beta)max(-\mu+\alpha-x_1-x_2,\ -\mu+c-x_1+x_2,\ -\mu+e+x_1-x_2,\ -\mu+g+x_1+x_2) - \beta max(-\mu+b-x_1-x_2,\ -\mu+d-x_1+x_2,\ -\mu+f+x_1-x_2,\ -\mu+h+x_1+x_2);$$

6)если $\mu = e_2 = k_1$, то $x_1 = (1 - \alpha)\ \max(2a_2 - 2k_1,\ c_2 - k_1) - \alpha\ \max(2b_2 - 2k_1,\ d_2 - k_1)$,

$x_2 = (1 - \beta)\ max(b_1 - k_1,\ -k_1 + e_1 - x_1,\ -k_1 + g_1 + x_1) - \beta\ max(k_1 + d_1,\ -k_1 + h_1 + x_1)$,

$$x_3 = \begin{cases} \dfrac{(a-h)}{2} - x_1 - x_2, & \text{если } k_1 = (a+h)/2, \\ \dfrac{(c-f)}{2} - x_1 + x_2, & \text{если } k_1 = (c+f)/2, \\ \dfrac{(-d+e)}{2} + x_1 - x_2, & \text{если } k_1 = (d+e)/2, \\ \dfrac{(-b+g)}{2} + x_1 + x_2, & \text{если } k_1 = (b+g)/2, \end{cases}$$

где $\boldsymbol{\alpha}, \boldsymbol{\beta}$ вещественные числа, удовлетворяющие условиям $0 \le \boldsymbol{\alpha} \le 1$, $0 \le \boldsymbol{\beta} \le 1$.

Вывод: для решения описанных выше задач получены полные аналитические решения в явном виде, их использование при решении минимаксных задач размещения позволяет понизить алгоритмическую сложность вычислений, в сравнении с известными итерационными подходами. Предложенный в статье| алгоритм нахождения оптимальной области размещения видеокамер как на плоскости, так и в трехмерном пространстве с прямоугольной метрикой на основе геометрического подхода, имеет низкую алгоритмическую сложность.

Заключение. В статье рассмотрена минимаксная задача размещения точечного объекта в двух и трехмерном пространстве с прямоугольной метрикой. Такая задача встречается на практике, например, при размещении центра управления системой камер видеонаблюдения в здании. Разработанный и представленный в статье алгоритм можно применить в области проектирования и создания аппаратных средств автоматизации решения задач автоматической оптимизации построения сложных информационных систем и их сетей.

СПИСОК ЛИТЕРАТУРЫ

1. Плотников П. В. Решение минимаксных задач размещения на плоскости с прямоугольной метрикой на основе методов идемпотентной алгебры: автореферат диссертации. СПб., 2018.
2. Плотников П. В., Кривулин Н. К. Прямое решение минимаксной задачи размещения в прямоугольной области на плоскости с прямоугольной метрикой // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. СПб., 2018. Т. 14. № 2. С. 116-130.
3. Плотников П. В., Кривулин Н. К. Решение минимаксной задачи размещения в трехмерном пространстве с прямоугольной метрикой // Компьютерные инструменты в образовании. СПб., 2018. № 1. С. 31-50.

УДК 629.561

ОСОБЕННОСТИ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ В БЕЗОПАСНОМ ИСПОЛНЕНИИ НАУЧНО-ПРОИЗВОДСТВЕННЫХ ОБЪЕДИНЕНИЙ МОРСКОЙ ИНФРАСТРУКТУРЫ, КАК СОЦИАЛЬНЩЙ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЙ СИСТЕМЫ

Рябков Яков Игоревич[1], Алексеев Сергей Алексеевич[2], Артемов Станислав Игоревич[3]

[1]Военно-космическая академия имени А.Ф. Можайского
Ждановская ул., 13, Санкт-Петербург,197198, Россия
[2]Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
3Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: yakovrt@mail.ru, ksgati@yandex.ru, pushokcheck@yandex.ru

Аннотация. В современной России динамично развиваются научно производственные объединения (НПО). Появление таких организаций вызвано развитием наукоемких отраслей производства страны в целом. Статья посвящена рассмотрению возможностей повышения эффективности функционирования НПО в России. Целью данной статьи является выявление отраслевых структурных и производственных особенностей НПО морской инфраструктуры в России и их роли в развитии потенциала страны. Данные мероприятия в совокупности позволят сформировать комплексное представление о сущности и особенностях НПО в России, что позволит в дальнейшем совершенствовать эффективную организацию и управление предприятиями наукоемких отраслей в безопасном исполнении.

Ключевые слова: автоматизация управления; организационное управление; научно-производственное объединение; социальная организационно-техническая система.

FEATURES OF AUTOMATION OF MANAGEMENT IN THE SAFE EXECUTION OF SCIENTIFIC AND INDUSTRIAL ASSOCIATIONS OF MARINE INFRASTRUCTURE AS A SOCIAL ORGANIZATIONAL AND TECHNICAL SYSTEM

Ryabkov Yakov[1], Alekseev Sergey[2], Artemov Stanislav[3]

[1]Military Space Academy named after A.F. Mozhaisky
13 Zhdanovskaya St, St. Petersburg, 197198, Russia
[2] Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
[3]St. Petersburg State Electrotechnical University «LETI» named after V.I. Ulyanov (Lenin)
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: yakovrt@mail.ru, ksgati@yandex.ru, pushokcheck@yandex.ru

Absrtact. Scientific and industrial associations (NGOs) are dynamically developing in modern Russia. The emergence of such organizations is caused by the development of knowledge-intensive industries of the country as a whole. The article is devoted to the consideration of the possibilities of improving the efficiency of the functioning of NGOs in Russia. The purpose of this article is to identify the sectoral structural and production features of marine infrastructure NGOs in Russia and their role in the development of the country's potential. These events together will form a comprehensive understanding of the nature and features of NGOs in Russia, which will further improve the effective organization and management of knowledge-intensive industries in safe execution.

Keywords: automation of management; organizational management; scientific and production association; social organizational and technical system.

Введение. Достижение высокого уровня конкурентоспособности выпускаемых изделий возможно, если при его производстве используется высокий процент интеллектуальных ресурсов. Большая роль в этом направлении принадлежит НПО, выпускающим высокотехнологичную продукцию. Главным отличием от производственных предприятий состоит в том, что НПО представляют собой совокупность не только средств производства,

работников и служащих, но и коллектива ученых, имеющих высокий уровень образования в производственной области. Порядок планирования деятельности НПО морской инфраструктуры сохраняет обособленность подразделений внутри НПО с одной стороны, по промышленности, с другой — по направлениям отраслей науки. К научным продуктам можно отнести знания и информацию в виде монографий, отчетов, рекомендаций, чертежей, проектов, опытных образцов, которые обладают новизной.

В руководство НПО морской инфраструктуры в России, как правило, входят: начальник, первый заместитель начальника НПО и заместители начальника НПО по специальным направлениям. НПО состоит из отделов, специальных центров, отделений и групп. Все рабочие места руководства НПО, руководителей подразделений и рабочих смен оснащены средствами вычислительной техники различной конфигурации, которые функционируют при поддержке определенного программного и информационного обеспечения.

Исходя из сказанного, вариант примерной основной структуры НПО морской инфраструктуры в России может быть представлен в следующем обобщенном виде, как на рис. 1.

Все изложенное выше позволяет сделать вывод о том, что НПО морской инфраструктуры является, во-первых, социальной системой, в состав которой входят как сотрудники руководства НПО, отделов, отделений и групп, так и персонал учреждений, организаций и объектов, которые совместно с сотрудниками НПО обеспечивают функции сбора оперативной информации, состоянии функциональных и территориальных подсистем и оперативной координации действий органов повседневного управления. Во-вторых, НПО совместно с учреждениями, организациями и объектами управления является организационной системой, т.е. системой иерархической с горизонтальными и вертикальными связями между ее компонентами. В-третьих, НПО, сотрудники которого сами работают на АРМ и управляют научными и производственными подразделениями, которые также оснащены рядом цифровой техникой, является технической системой, так как его персонал на всех уровнях управления использует средства вычислительной техники с соответствующим программным и информационным обеспечением.

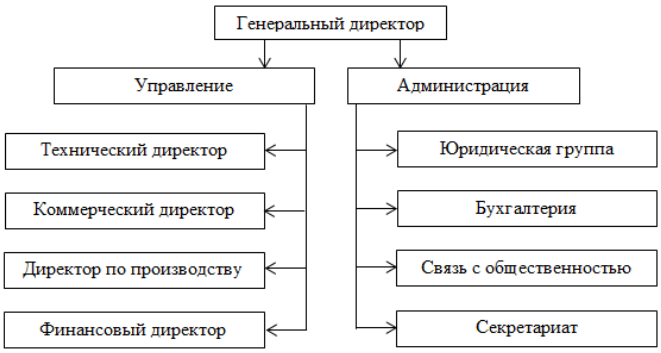


Рис. 1. Примерная структура НПО России

Таким образом, НПО морской инфраструктуры является социальной организационно-технической системой (СОТС), относящейся к классу сложных, иерархических, самоорганизующихся и самоадаптирующихся человеко-машинных систем (ЧМС), в которых персонал управленцев работает, в том числе, на АРМ. Вывод: для исследования законов функционирования СОТС НПО морской инфраструктуры можно использовать уже известные, рабочие законы, применяемые при исследовании ЧМС.

Проведенный анализ структуры и функций НПО морской инфраструктуры, как СОТС показывает, что процесс управления таким сложным иерархическим объектом может осуществляться эффективно в случае, если все компоненты такой СОТС будут объединены в региональную вычислительную сеть (ВС). Такая сеть является сетью передачи данных, в узлах которой располагаются ЭВМ и персонал, их использующий.

Фактически НПО, с точки зрения автоматизации управления, может быть представлен в виде совокупности локальных вычислительных сетей (ЛВС) ЛВС – это сеть передачи данных, связывающая ряд рабочих станций (рабочих мест операторов, оборудованных средствами для выполнения функций управления) в одной локальной зоне. Такие сети обеспечивают высокие скорости (до 100 000 Мб/с) передачи данных непосредственно в ЭВМ, подключенные к сети. Машины-шлюзы (межсетевые интерфейсы, служащие для соединения двух и более ЛВС, которые объединяют пользователей этих сетей) соединяют ЛВС между собой или подключают их к сетям большей протяженности. Каждая ПЭВМ в ЛВС имеет сетевой адаптер, который соединяет ее со средой передачи. Для решения научных и производственных задач ЛВС НПО с совокупностью подчиненных подразделений и подведомственных организаций для достижения определенных целей путем осуществления совместной деятельности на основе взаимных интересов может быть объединена в корпоративную сеть (КС).

Основными звеньями любой структуры обмена информацией и управления являются системные специалисты

– операторы, рабочими местами которых являются рабочие станции или АРМ, входящие в состав. Кроме операторского состава компонентами КС являются:

– коммутационные узлы (КУ) – все сетевые устройства для соединения и объединения сети (повторитель, концентратор, коммутатор, маршрутизатор и др.),

– рабочие узлы (рабочие станции), оснащенные ПЭВМ, принтерами, сканерами, серверами и др.,

– каналы передачи данных, т.е. среда передачи информации (оптоволоконные, коаксиальные, радиоканалы и др.).

Следовательно, НПО морской инфраструктуры, как СОТС представляет собой разновидность ЧМС вида «группа операторов – корпоративная сеть» (ГОКС).

В данной статье КС рассматривается на канальном уровне, т.е. не рассматриваются: программное и информационное обеспечение, установленное на коммутационных и рабочих узлах; особенности аппаратуры; способы обработки и передачи информации в узлах; сетевые протоколы и другие аспекты КС. Рассматриваются надёжностные и временные характеристики деятельности операторов на рабочих станциях при обработке и передаче информации, циркулирующей в НПО. При этом КС целесообразно изучать в виде графа, вершины которого соответствуют узлам КС, а дуги – каналам передачи информации.

При этом надежностными характеристиками вершин и дуг являются вероятности безошибочной обработки (передачи) информации, а временными – средние времена обработки (передачи) информации. Основной задачей КС, моделирующей информационные технологии, реализуемые в рамках НПО, как СОТС, является передача информации между различными приложениями (базы данных, электронная почта и т.д.), используемыми сетевыми специалистами НПО. КС позволяет взаимодействовать приложениям, обеспечивая доступ к ним удаленных пользователей. В состав КС входят магистральные сети, связывающие отдельные компоненты КС.

Сетевые специалисты-операторы КС используют три основных метода передачи данных путем: коммутации каналов связи; коммутации сообщений, передаваемых по каналам связи; коммутации пакетов, которые подразделяются на коммутацию кадров и коммутацию ячеек.

К любой КС предъявляются три основных требования: масштабируемость, производительность и управляемость. В настоящее время не существует отлаженной универсальной методики реализации мероприятий по синтезу, созданию и внедрению КС. Это связано с тем, что практически не существует двух абсолютно одинаковых организаций, представляющих собой СОТС. Каждая НПО характеризуется уникальным стилем руководства, иерархией, правилами ведения дел, принятия решений. Любая КС в принципе должна отражать структуру организации, в том числе и НПО, основой которого является персонал, работающий на своих цифровых производственных системах и АРМ. Каждый сетевой специалист-оператор должен осуществлять управление магистралью, которое включает: конфигурирование магистрали, поддержку ее работоспособности, передачу и прием сообщений.

Автоматизация процессов управления СОТС. Под термином «автоматизация процессов управления» принято понимать комплекс мероприятий, направленных на внедрение средств вычислительной техники (СВТ) и современных информационных технологий (ИТ) в работу органов управления НПО, как СОТС с целью создания условий повышения эффективности деятельности лица, принимающего решение (ЛПР) при управлении объектами СОТС. Достижение целей автоматизации управления связано с необходимостью выполнения следующих процедур:

1.Технико-экономический анализ и оценка целесообразности автоматизации управления. При этом необходимо правильно выбрать критерий оценки эффективности функционирования СОТС и устойчивости ее свойств.

2.Моделирование процесса управления НПО, как объекта автоматизации. При этом необходимо разработать спецификацию СОТС путем ее декомпозиции с необходимой степенью детализации, описания отдельных компонент и их взаимосвязей, разработка информационно-логической модели системы, выявления с помощью полученной модели первоочередных звеньев автоматизации, выработки требований к системе управления.

3.Разработка структуры НПО, определение требований к видам обеспечения, исходя из требований к системе в целом, согласование требований по видам обеспечения.

4.Техническая реализация, т.е. синтез системы управления НПО, выбор ИТ в соответствии с требованиями к видам обеспечения и к системе управления в целом, выбор структуры системы и средств автоматизации.

Исходя из сказанного, можно выделить предмет автоматизации управления СОТС, который определяет закономерности и принципы автоматизации процессов управления, методологию автоматизации процессов управления, методы моделирования процессов управления в целях автоматизации и обоснования требований к системе управления, методики выбора программных, информационных и технических средств.

Показано, что основными принципами автоматизации являются:

1)принцип системного подхода к автоматизации управления, предусматривающий рассмотрение всех аспектов автоматизации, как единого целого, а также необходимую степень автоматизации всех основных элементов процесса управления;

2)принцип новизны задач автоматизации управления, предусматривающий перестройку методов и средств управления в соответствии с новыми возможностями СВТ, в традиционно сложившихся к настоящему времени методах и средствах автоматизации определенных классов СОТС;

3)принцип непрерывного развития системы (гибкость структуры управления), предусматривающий возможность ее развития в соответствии с изменением методов организационно-технического управления, использованием новых образцов СВТ и оргтехники при минимальных затратах времени и средств на перестройку;

4)принцип целесообразности, предполагающий получение экономического, социального или иного эффекта от автоматизации.

Автоматизация управления НПО должна выполнять две основные функции:

1.Познавательную, которая состоит в раскрытии сущности закономерностей и принципов, а именно: технологии автоматизации процессов управления, подлежащих автоматизации; оценки эффективности автоматизации управления; автоматизации моделирования процессов управления; организации работ по созданию, развитию и применению средств и систем автоматизации управления.

2.Прогнозирующую, состоящую в определении тенденций развития методов, технических, программных и информационных средств и систем автоматизации управления; последствий принимаемых управленческих решений и выполнении на этой основе анализа, оценки эффективности и оптимизации систем управления.

Основным методом теории автоматизации управления является математическое моделирование, реализуемое на основе разработки моделирующих алгоритмов и программ решения задач трех основных классов с использованием ЭВМ:

– расчетных, реализуемых на основе расчетных моделей, когда результатом решения является число,

– информационных, реализуемых на основе информационных моделей, когда результатом решения является смысловой текст, график, рисунок и т.д.,

– модельных, реализуемых на основе моделей знаний о предметных областях и потоках на множестве решений, когда результатом решения является либо числа (расчетные модели), либо смысловой текст, график, рисунок (информационные модели).

Использование моделирования (расчетного, статистического, имитационного) для области управления НПО проявляется в двух аспектах. Во-первых, для анализа и синтеза собственно средств и систем автоматизации управления. Во-вторых, для реализации основных функций управления ЛПР и персоналом органов управления СОТС.

В ряде работ рассматривается структура теории автоматизации управления. Применительно к СОТС структура такой теории представлена на рис. 2. Из рисунка видно, что в структуру теории автоматизации управления входит ряд важных самостоятельных дисциплин, непосредственно связанных с изучением вопросов автоматизации процессов управления, а именно: методология исследовательского синтеза информационно-управляющей системы (ИУС), методология разработки трех основных видов обеспечения функционирования ИУС, средства и методы искусственного интеллекта.

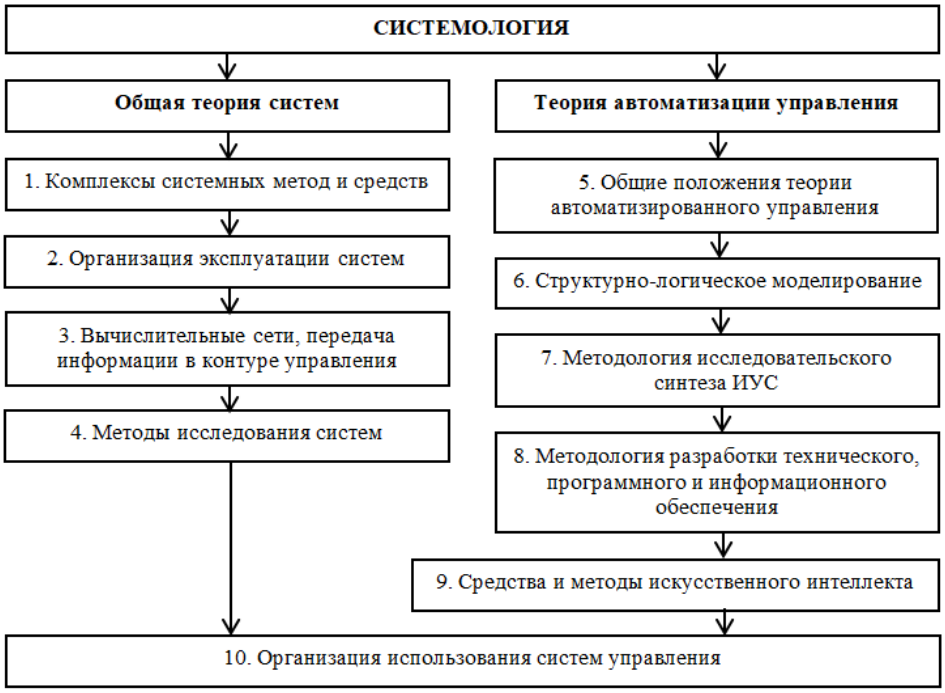


Рис. 2. Обобщенная структура теории автоматизации управления

Особенно важным вопросом при решении задач автоматизации процессов управления является задача оценки эффективности автоматизации управления. При этом эффективность выступает, как самая полная, всесторонняя и общая характеристика системы, которая качественно и количественно определяет ее способность, имея определенную совокупность свойств оцениваемой системы, выполнять свою основную функцию – функцию управления.

Оценка эффективности требует наличия критерия и показателя эффективности. Показатель эффективности – системная мера, количественно характеризующая степень выполнения системой цели функционирования, поставленной задачи и функции управления, или количественная оценка свойства, выбранного в качестве характеристики эффективности системы. Критерий эффективности – это правило или способ принятия какого-либо управленческого решения, осуществления того или иного управляющего воздействия на основе анализа выработанного показателя эффективности.

Одной из самых важных задач при оценке эффективности автоматизации управления НПО является выбор или формулировка показателя эффективности. Во-первых, этот показатель (интегральный) должен описать степень проявления автоматизированной системой своего главного, интегрального свойства, определяющего цель ее функционирования. Во-вторых, такой показатель должен складываться из ряда показателей, характеризующих частные, второстепенные свойства НПО, которые в разной степени и часто противоречиво влияют на интегральный показатель эффективности. В-третьих, интегральный показатель должен учитывать многоцелевой характер функционирования НПО. В-четвертых, реально существующая иерархичность НПО, многоуровневость целей ее функционирования могут приводить к крайнему усложнению формулировки или выбора показателя эффективности автоматизированной системы, осуществляющей управление СОТС.

Объективные трудности, связанные с выбором или формулировкой интегрального показателя эффективности НПО морской инфраструктуры, привели к тому, что на практике используют не один интегральный показатель, а ряд частных показателей, которые в совокупности с достаточной полнотой и точностью характеризуют эффективность автоматизации управления НПО. В ряде случаев целесообразно множество частных показателей декомпозировать в иерархически связанные уровни. На рис. 3 показаны взаимосвязь целей и показателей эффективности автоматизации управления НПО.

Практика показывает, что, как правило, получить точные значения частных и общих показателей эффективности выбранной степени автоматизации управления такой сложной системы, как НПО нереально. Это можно сделать только в том случае, если в модели процесса функционирования НПО будет корректно учтено влияние автоматизации управления на качество творческого процесса выработки управленческих решений органом управления во главе с ЛПР и их практическую реализацию. Невозможность моделирования творческих процессов делает уровень показателей, характеризующих процессы принятия решений и контроля их исполнения, не столько научно-модельным, сколько вербально-описательным, т.е. только качественным.

Рис. 3. Взаимосвязь целей и показателей эффективности автоматизации управления СОТС

Показатели организационно-технической эффективности автоматизации управления в совокупности должны характеризовать все стороны обеспечения средствами автоматизации эффективной работы органа управления НПО во главе с ЛПР по выработке управленческих решений. В состав частных организационно-технических показателей обычно включают характеристики надежности и быстродействия комплекса технических и программных средств, а также показатели того, насколько они удовлетворяют требованиям точности, достоверности, наглядности и полноты обеспечения средствами и системами автоматизации процессов работы органа управления НПО во главе с ЛПР.

Из сказанного выше может быть сделан вывод о том, что наиболее важным в конкретном решении задачи выбора степени автоматизации управления функционированием НПО, является уяснение непосредственных целей, задач и функций управления НПО и ее компонентами. При этом должны четко формулироваться требования по автоматизации процессов управления, определяющей повышение эффективности работы органов управления и ЛПР при управлении. Не менее важной задачей при выборе систем, средств и методов автоматизации управления, обеспечивающих построение математических моделей и собственно моделирование процессов функционирования НПО, является адекватное использование математического аппарата, формализующего названный процесс управления. Одним из основных математических методов, используемых при управлении сложными, большими, иерархическими объектами, к которым в полной мере относится и НПО, является метод сетевого планирования, позволяющий организовать в пространстве и времени взаимодействие компонент названного объекта для достижения единой цели управления.

СПИСОК ЛИТЕРАТУРЫ

1. Рябков Я.И., Алексеев С. А., Артемов С. И. Повышение эффективности управления маломерными судами в сложной обстановке. // Региональная информатика. Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. СПб. : СПОИСУ, 2022. 626 с.
2. Алексеев С. А. Автоматизация процессов управления социальными организационно-техническими системами // Научное обозрение. 2009. № 4 .С.72-77.
3. Алексеев С. А. Оценка характеристик процесса функционирования системы «оператор (группа операторов) – корпоративная сеть» МЧС // Проблемы управления рисками в техносфере. 2008. №2. С. 50-56.
4. Алексеев С. А. Концепция создания единого информационного пространства социальной организационно-технической системы // Сборник трудов. Первого СПб. конгресса «Проф. образование, наука, инновации в XXI веке». СПб., 2007.

УДК 004.056

ОЦЕНКА УРОВНЯ ЗРЕЛОСТИ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА СУДОСТРОИТЕЛЬНОМ ПРЕДПРИЯТИИ АО «ВОСТОЧНАЯ ВЕРФЬ»

Тарасов Валентин Сергеевич, Кудинова Екатерина Андреевна
Владивостокский государственный университет «ВВГУ»
Гоголя ул., 41, Владивосток, 690014, Россия
e-mails: katyku221133@gmail.com, Vals.tarasov@gmail.com

Аннотация. В статье рассматривается новый подход к оценке уровня зрелости системы обеспечения информационной безопасности на предприятии морской отрасли на примере предприятия АО «Восточная Верфь». Оценка зрелости проведена по разработанной автором системе метрик и, по результатам оценки, даны рекомендации по модернизации системы обеспечения информационной безопасности, персональные данные.

Ключевые слова: СОИБ; информационная безопасность; уровни зрелости; модель зрелости; критическая информационная инфраструктура; информационные системы персональных данных.

ASSESSMENT OF THE LEVEL OF MATURITY OF THE INFORMATION SECURITY SYSTEM AT THE SHIPBUILDING ENTERPRISE JSC «VOSTOCHNAYA VERF»

Tarasov Valentin, Kudinova Ekaterina
Vladivostok State University «VSU»
41 Gogol St, Vladivostok, 690014, Russia
e-mails: katyku221133@gmail.com, Vals.tarasov@gmail.com

Absrtact. The article discusses a new approach to assessing the level of maturity of the information security system at a marine industry enterprise using the example of Vostochnaya Verf JSC. The maturity assessment was carried out according to the system of metrics developed by the author and, based on the results of the assessment, recommendations were given for modernizing the information security system, personal information.

Keywords: IS Maintenance System; information security; maturity levels; maturity model; critical information infrastructure; personal data information systems.

Введение. Организации, деятельность которых во многом зависит от использования современных информационных технологий, для достижения целей бизнеса должны поддерживать на необходимом уровне

систему обеспечения информационной безопасности (СОИБ). СОИБ представляет собой совокупность аппаратно-программных, технических и организационных защитных мер, функционирующих под управлением системы менеджмента информационной безопасности (ИБ) и процессов осознания ИБ, инициирующих и поддерживающих деятельность по менеджменту ИБ [1, 2].

Желание иметь СОИБ, адекватную целям ИБ организации по обеспечению доступности, целостности и конфиденциальности информационных активов, приводит к стремлению совершенствовать СОИБ. Совершенствование СОИБ возможно при условии знания состояний характеристик и параметров, процессов менеджмента, осознания ИБ и понимания степени их соответствия требуемым результатам [3]. Понять эти аспекты СОИБ можно только по результатам оценки ИБ организации, полученной с помощью модели оценки ИБ на основании свидетельств оценки, критериев оценки и с учетом контекста оценки [4, 5].

В настоящий момент к продуктам ИБ относится большой спектр самых различных решений, включая систему сбора корреляции событий, аналитические системы, системы контроля за утечками и т.д. Обеспечение ИБ предприятия возможно только при системном и комплексном подходе к защите и подразумевает непрерывный контроль в реальном времени всех важных событий и состояний, влияющих на безопасность данных. Как результат, современные СОИБ приобрели функцию контроля, а именно функцию контроля и управления определенной части производственных и информационных процессов.

Модель зрелости используется как инструмент измерения состояния процесса на основе набора метрик, которые представляют собой определенные характеристики. Оценка этих метрик по оговоренной шкале позволяет понять состояние процессов организации, которая и будет характеризовать уровень зрелости. После получения оценки зрелости можно выработать необходимые мероприятия для повышения зрелости процессов и организации в целом [5, 6].

Подход к оценке процессов информационной безопасности базируется не только на требованиях к составу и модели зрелости процессов информационных технологий, но и на требованиях к другим службам и сервисам предприятия. В российской практике не сложилась целостная система использования моделей зрелости; в зарубежной – применение моделей зрелости как инструмента управления широко развито, в том числе и для управления процессами безопасности. В [6] приведен сравнительный анализ наиболее распространенных и часто используемых моделей зрелости, а именно:

- Open Information Security Management Maturity Model (O-SIM3);
- Process Capability Model (PCM);
- Enterprise Information Management Maturity Model (EIM MM);
- Community Cyber Security Maturity Model (CCSMM);
- Program Review for Information Security Management Assistance (PRISMA);
- COBIT 5 for Information Security.

Анализ показывает, что ни одна из рассмотренных моделей в полной мере не отражает всех современных требований по организации ИБ для организаций различного размера и сферы деятельности. Поэтому для оценки ИБ предприятия была разработана собственная модель зрелости с подходящими для нее метриками, используя рассмотренные модели в качестве образца.

Уровень зрелости любого процесса чаще всего определяют, как показатель процесса, характеризующий его способность соответствовать текущим и будущим целям стратегии предприятия. В литературных источниках применяются различные модели зрелости для задач ИБ [7]. В соответствии с принятой в настоящем исследовании методологии вводятся следующие уровни зрелости для ИБ:

3.Начальный. Процесс обеспечения ИБ выполняется на нерегулярной основе.

4.Осуществленный. Процесс обеспечения ИБ выполняется на регулярной основе и поддерживается на уровне планирования.

5.Управляемый. Процесс обеспечения ИБ выполняется, планируется, и имеется достаточный объем организационных ресурсов для поддержки и управления.

6.Предсказуемый. Процесс обеспечения ИБ выполняется, планируется, управляется и контролируется.

7.Адаптивный. Процесс обеспечения ИБ выполняется, планируется, управляется, измеряется при помощи количественных показателей (метрик) и постоянно совершенствуется.

Уровень зрелости определялся на основании наличия и полноты традиционных атрибутов процессов:

- управление процессом;
- состояние объектов, которыми управляет процесс.

Только на основании атрибутов оценить уровень зрелости процесса обеспечения ИБ невозможно, поэтому различные модели зрелости предлагают оценивать широкий диапазон доменов информационной безопасности, из которых состоят атрибуты, от инфраструктуры, данных и сетей до людей, приложений, процессов управления и реагирования, требований по соблюдения правовых норм и управления контрактными обязательствами.

Для оценки обеспечения ИБ предприятия были выбраны домены ИБ с учетом специфики деятельности предприятия, наиболее известной международной практики и общепринятых стандартов: ISO27000, COBIT5 for Information Security, SANS, NIST [8, 9]:

– информационное управление безопасностью;
– обучение и образование в области ИБ;
– соответствие требованиям регуляторов;
– информационно-техническое обеспечение ИБ.

Таким образом, выделенные домены группируются в соответствии с традиционными атрибутами зрелости процесса обеспечения ИБ, образуя иерархичную структуру, которая является ядром модели зрелости. Данная иерархическая структура представлена на рис. 1.

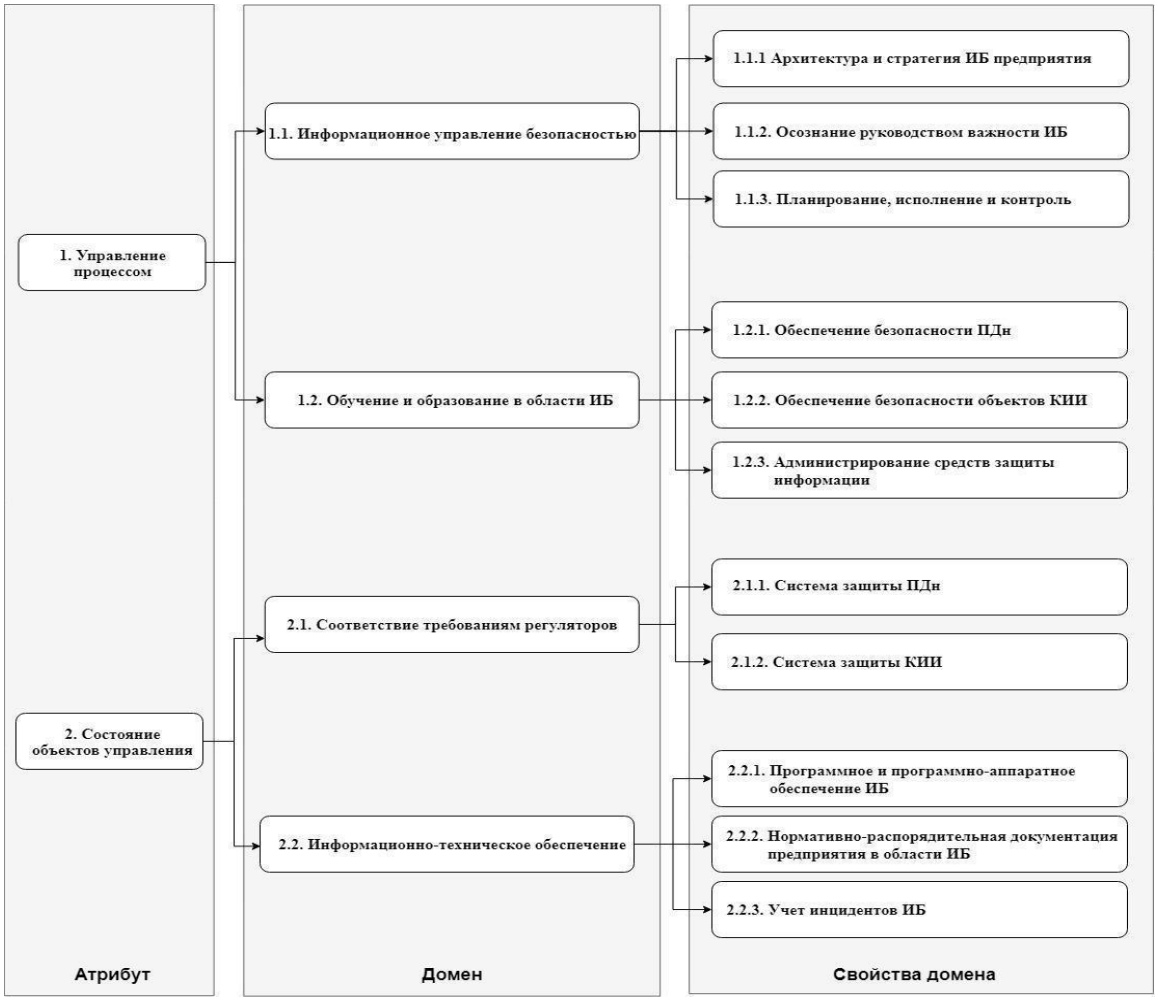


Рис. 1. Иерархия атрибутов, доменов и их свойств

Оценивание уровня зрелости процесса обеспечения ИБ начинается с доменов ИБ на основании их свойств. Оценка производится по следующим доменам:

– информационное управление безопасностью и культура;
– обучение и образование в области ИБ;
– соответствие требованиям регуляторов;
– информационно-техническое обеспечение ИБ.

При этом есть 4 уровня зрелости, по которым, в соответствии с доменами, проводится оценка.

1.Начальный.
2.Осуществленный.
3.Управляемый.
4.Предсказуемый.

Определение зрелости информационной безопасности организации строится на рассмотрении документации предприятия в области ИБ, интервьюирования персонала предприятия и анализа каждого из 4 доменов. Интересен такой подход тем, что таким образом описывается не только сам процесс, но и вовлекаемые в него работники.

В основу методологии оценивания уровня зрелости, в соответствии с предложенной моделью, легла методология PRISMA (NISTIR-7358) [8]. Процесс оценки начинается с индивидуальной оценки каждого из приведенного домена ИБ по разработанным критериям. Эти критерии и являются метриками модели. Для критерия

производится оценка на каждом из уровней зрелости. Оценка выполнения критерия, т.е. оценка метрики, может быть следующая: «Полностью соответствует» (ПС), «Частично соответствует» (ЧС), «Не соответствует» (НС). Оценивание начинается с самого нижнего уровня, если для рассматриваемого домена ИБ имеют оценку «Не соответствует», то весь уровень получает такую же оценку по указанному критерию. Если для одного из критериев оценка «Полностью соответствует», но оценка других критериев (одного или более) «Частично соответствует»/»Не соответствует», тогда общая оценка критерия для уровня будет «Частично соответствует».

Такое оценивание проводится для всех доменов ИБ по всем уровням зрелости. Результаты оценки приведены в сводной таблице с использованием цветовой маркировки, которую предполагает методологий PRISMA: «зеленый» для «Полностью соответствует», «желтый» для «Частично соответствует», «красный» для «Не соответствует». На основе данной таблицы был проведён анализ предприятия АО «Восточная верфь». Результаты оценки приведены в таблице 1.

Таблица 1

Результаты оценки доменов ИБ в соответствии с моделью зрелости

Домен ИБ	Уровень зрелости			
	1	2	3	4
Информационное управление безопасностью и культура	ЧС	ЧС	НС	НС
архитектура и стратегия ИБ	ЧС	ЧС	НС	НС
осознание руководством важности ИБ	ПС	ЧС	НС	НС
планирование, исполнение и контроль	ЧС	НС	НС	НС
Обучение и образование в области ИБ	ЧС	ЧС	ЧС	НС
администрирование средств защиты информации	ПС	ПС	ЧС	НС
обеспечение безопасности персональных данных (ПДн)	НС	НС	НС	НС
обеспечение безопасности критической информационной инфраструктуры (КИИ)	ПС	ЧС	ЧС	НС
Соответствие требованиям регуляторов	ПС	ЧС	ЧС	НС
система защиты ПДн	ПС	ЧС	НС	НС
система защиты КИИ	ПС	ПС	ПС	НС
Информационно-техническое обеспечение ИБ	ПС	ЧС	ЧС	НС
программно-аппаратное обеспечение ИБ	ПС	ЧС	ЧС	НС
ИБ нормативно-распорядительная документация	ПС	ЧС	НС	НС
Учет инцидентов ИБ	ПС	ЧС	НС	НС

Для понимания, как именно следует действовать, в случае развития и повышения уровня зрелости, вводится подсчет индекса зрелости атрибутов ИБ. Для расчёта данного индекса необходимо принять общий уровень зрелости за 100% и разделить на количество уровней. В зависимости от уровня, на котором находится атрибут, он получает от 0 % до 20%. Общий индекс рассчитывается как среднее арифметическое полученных результатов по каждому атрибуту.

По результатам оценки был определён индекс зрелости СОИБ АО «Восточная верфь» - 20%. Результаты оценки зрелости процесса представлен в виде лепестковой диаграммы на рис. 2.

В ходе анализа процесса обеспечения ИБ предприятия был выявлен ряд проблемных сторон, характеризующих определенный домен ИБ и препятствующих цифровой трансформации предприятия на основе внедрения в управление системы уровня Enterprise Resource Planning (ERP).

Общий индекс зрелости системы обеспечения информационная безопасность предприятия равен 20%, что в основном соответствует первому уровню («Начальный») согласно разработанной модели зрелости. Таким образом, индекс зрелости процесса обеспечения ИБ предприятия не соответствует заявленным требованиям по цифровой трансформации предприятия.

Рис. 2. Оценка индекса зрелости доменов процесса обеспечения ИБ предприятия

Для приведения информационной безопасности предприятия в состояние готовности к цифровой трансформации на основе системы класса ERP, необходимо достичь по крайней мере третьего уровня зрелости и выполнить мероприятия по приведению в соответствие уровней зрелости, атрибутов управления и состояния безопасности.

С учетом оценки уровня зрелости процесса обеспечения ИБ предприятия, полученную в результате исследования, а также учитывая сложность технический решений, необходимых для реализации перехода на следующий уровень зрелости, предлагается модернизацию службы обеспечения ИБ выполнить в три этапа. На первом этапе будут созданы условия для внедрения системы мониторинга событий ИБ, предлагаемой для внедрения на втором этапе.

На первом этапе для гарантированного и надежного функционирования информационных систем с учетом требований ИБ необходимо:

1.Провести организационно-технические мероприятия:

– определить цели, задачи и стратегию развития процесса обеспечения ИБ;

– доработать нормативно-распорядительную базу предприятия в части обеспечения ИБ;

– доработать нормативно-распорядительную базу предприятия в части соответствия требованиям ФЗ-152 «О персональных данных».

2. Провести инженерно-технические мероприятия:

– выстроить систему защиты периметра организации, состоящую из средств межсетевое экранирование, развертывания систем обнаружения и предотвращения вторжений;

– выстроить систему защиты от вредоносного кода и спама, состоящую из средств антивирусной защита рабочих станций и серверов, средств защиты от спама, контентной фильтрации трафика;

– выстроить систему обеспечения конфиденциальности информации при хранении передаче, состоящую из средств шифрования каналов связи, средств шифрования носителей информации;

– выстроить систему защиты информации от несанкционированного доступа.

На втором этапе предлагается внедрение специализированной системы, осуществляющей управление и мониторинг событий ИБ, их автоматизированную обработку и выявление инцидентов.

После реализации второго этапа модернизации служба обеспечения ИБ готова к переходу на третий этап модернизации и последующим испытаниям. В процессе испытаний выполняются тестовые задания и контролируются полученные результаты, которые и являются индикатором работоспособности спроектированной комплексной системы защиты информации.

Заключение. По результатам проделанной работы была предложена новая модель метрик для оценки уровня зрелости и было проведено исследование уровня зрелости СОИБ судостроительного предприятия АО «Восточная Верфь» по разработанной метрике. По результатам оценки были выявлены сильные и слабые стороны системы обеспечения ИБ. На основе сделанных выводов были предложены мероприятия по модернизации системы для подготовки предприятия к цифровой трансформации с последующим внедрением ERP-системы.

СПИСОК ЛИТЕРАТУРЫ

1. Трунова А. В. Обеспечение информационной безопасности предприятия // Современные инновации. 2018. №4 (26). С. 33-35.
2. Корчак В. Ю., Ефимова Н. С., Калачанов В. В., Давыдов Д. А. Развитие средств информационной безопасности для роста конкурентоустойчивости предприятия // Компетентность= Competency.M., 2017. № 8 (149). С. 6–12.
3. Макаренко С. В. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. №1. С. 1-29.
4. Шубин А. Н. Оценка свойств информационных систем в стандартах по информационной безопасности // Известия ТулГУ. Технические науки. 2013. №3. С. 336-344.
5. Самохвалов Ю. Я., Браиловский Н. Н. Оценка информационной безопасности организации по критерию уверенности // Защита информации. 2019. Том 21. № 1. С. 13-24.
6. Милославская Н., Сагиров Р. Обзор моделей зрелости процессов управления информационной безопасностью // Безопасность информационных технологий. МИФИ (НИЯУ МИФИ). М., 2015. Том 22. № 2. С. 76-84.
7. Дмитриева М. А. Применение анализа зрелости информационной безопасности в системе оценки зрелости бизнес-процессов предприятия в целом // Информационная безопасность регионов. С., 2015. №3 (20). С. 20-24.
8. Bower P., Kissel R. L. Program Review for Information Security Management Assistance (PRISMA) [Электронный ресурс] // NIST Interagency/Internal Report (NISTIR). №7358. URL: https://www.nist.gov/publications/program-review-information-security-management-assistance-prisma. (дата обращения: 27.06.2023).
9. Нарыжный К. Cobit 5: модель оценки процессов [Электронный ресурс] // Статьи консультантов Cleverics. URL: https://cleverics.ru/subject-field/articles/554-cobit5-pam. (дата обращения: 21.07.2023).

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СОЦИОКОМПЬЮТИНГЕ

УДК 004.932

ЦВЕТОВЫЕ ХАРАКТЕРИСТИКИ АВАТАРОВ: ПОДХОД К ОЦЕНКЕ ВЫРАЖЕННОСТИ ПСИХОЛОГИЧЕСКИХ ОСОБЕННОСТЕЙ ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНЫХ СЕТЕЙ

Бушмелев Федор Витальевич[1], Тулупьева Татьяна Валентиновна[1, 2]
[1] СПИИРАН ─ СПб ФИЦ РАН
В. О. 14 линия, 39, Санкт-Петербург, 199178, Россия
[2] Северо-Западный институт управления Российской академии народного хозяйства
и государственной службы при Президенте РФ,
В. О. Средний проспект, 57/43, Санкт-Петербург, 199178, Россия
e-mails: fvb@dscs.pro, tvt@dscs.pro

Аннотация. Исследование посвящено формированию подхода, что на основании набора цветовых характеристик изображений профиля социальной сети — аватаров — позволяет автоматизировано строить предсказания о выраженности личностных характеристик пользователя, в частности на основе адаптированной версии теста 5PFQ. На Gradient Boosting Tree была обучена предсказательная модель и определено количество ближайших к прохождению аватаров, необходимых для достижения точных оценок. Результаты исследования являются новыми в области компьютерного зрения и машинного обучения и составляют основу для личностно ориентированных предсказательных моделей, которые могут использоваться в рамках задач по профориентированию или оценке защищенности пользователей от социоинженерных атак.

Ключевые слова: анализ изображений; компьютерное зрение; извлечение признаков; личностные особенности, информационная безопасность; социальные сети; машинное обучение.

COLOR CHARACTERISTICS OF AVATARS: AN APPROACH TO ASSESSING THE EXPRESSION OF PSYCHOLOGICAL CHARACTERISTICS OF SOCIAL MEDIA USERS

Bushmelev Fedor[1], Tulupyeva Tatiana[1,2]
[1] SPIIRAN ─ SPb FRC RAS
39 V.I. 14th Line, St. Petersburg, 199178, Russia
[2] The North-West Institute of Management of the Russian Presidential Academy
of National Economy and Public Administration
57/43 V.I. Middle Av, St. Petersburg, 199178, Russia
e-mails: fvb@dscs.pro, tvt@dscs.pro

Abstract. The research focuses on the formation of an approach that, based on a set of color characteristics of social network profile images - avatars - enables automated predictions about the expression of a user's personality characteristics, based on an adapted version of the 5PFQ test. A predictive model was trained on the Gradient Boosting Tree and the number of nearest-to-follow avatars needed to achieve accurate scores was determined. The results of the study are novel in the field of computer vision and machine learning and form the basis for person-centered predictive models that can be used as part of career guidance tasks or to assess users' defensiveness against social engineering attacks.

Keywords: image processing; computer vision; feature extraction; personality traits; information security; social media; machine learning.

Введение. Динамичное развитие информационных технологий в последние годы [1] и активная работа по цифровизации общества сегодня [2] в значительной степени изменили способы общения, взаимодействия, а также обмена, обработки и распространения информации. Растущая популярность социальных сетей привела к значительному росту числа их активной аудитории и увеличению среднесуточного количества времени, проводимого на этих платформах [3]. Большей популярностью у пользователей в мире среди социальных медиа пользуются такие площадки, как Facebook* (запрещенный на территории РФ компании Meta), YouTube, Instagram* и

TikTok, а у русскоязычной аудитории в свою очередь ВКонтакте, Telegram, TikTok и Одноклассники [4, 5], где ВКонтакте имеет наибольший охват аудитории (86%). Высокий уровень активности на подобных площадках становится причиной появления больших объемов информации, в особенности «цифровых следов», которые сегодня находят применение во многих областях, например, при личностном анализе; при исследовании рынка и потребительского поведения; для персонализации и таргетирования рекламы; для анализа общественного мнения; для информационной безопасности и выявления мошенничества; для здравоохранения и эпидемиологии; в психологии и социальных науках. В рамках данной работы наибольший акцент делается на построении представления о личностных особенностях пользователя, которое подразумевает анализ источников, идентификацию личностных характеристик и их выраженностей на основе цифрового контента, включая текст, аудио-, видео- и изображения, которые пользователи публикуют на своих страницах в социальных сетях. Зачастую подобный контент может содержать в себе множество скрытых характеристик личности. Так, например, изображение профиля пользователя – аватар – можно назвать основной цифровой проекцией пользователя в метавселенную отдельно взятой социальной сети или иной информационной системы. В связи с чем существует гипотеза о том, что в аватаре, как в устойчивом элементе профиля в социальной сети могут содержаться множество ключевых признаков, позволяющих строить представления об особенностях личности пользователя. В рамках данной работы предлагается подход к оценке выраженности психологических особенностей пользователей социальных сетей за счет автоматизации анализа цветовых характеристик изображений-аватаров их профилей.

Для проведения исследования был подготовлен набор данных, состоящий из пар «фотография – набор черт личности», где в качестве фотографии выступали аватары, а в качестве методики оценки выраженности личностных черт пятифакторный опросник личности (5PFQ) [6] — а именно адаптация для стран СНГ популярного психологического тестирования «Большая пятерка». Данное тестирование позволяет представить личность человека в виде разбиения по 5 факторам, оценив степень выраженности каждого из них:

- Экстраверсия / Интроверсия;
- Привязанность/ Обособленность;
- Самоконтроль / Импульсивность;
- Эмоциональная неустойчивость / устойчивость;
- Экспрессивность / Практичность.

Каждый фактор может принимать значения от 15 до 75.

Всего было опрошено 1415 пользователей ВКонтакте, и собрано 12035 аватаров. Изображения отбирались с разницей в датах публикации и прохождения тестирования не больше года. На Рис. 1 показана плотность распределения пользователей в зависимости от количества аватаров за последний год от тестирования. Было принято решение пользователей, у которых было более 20 аватаров объединить в одну группу.

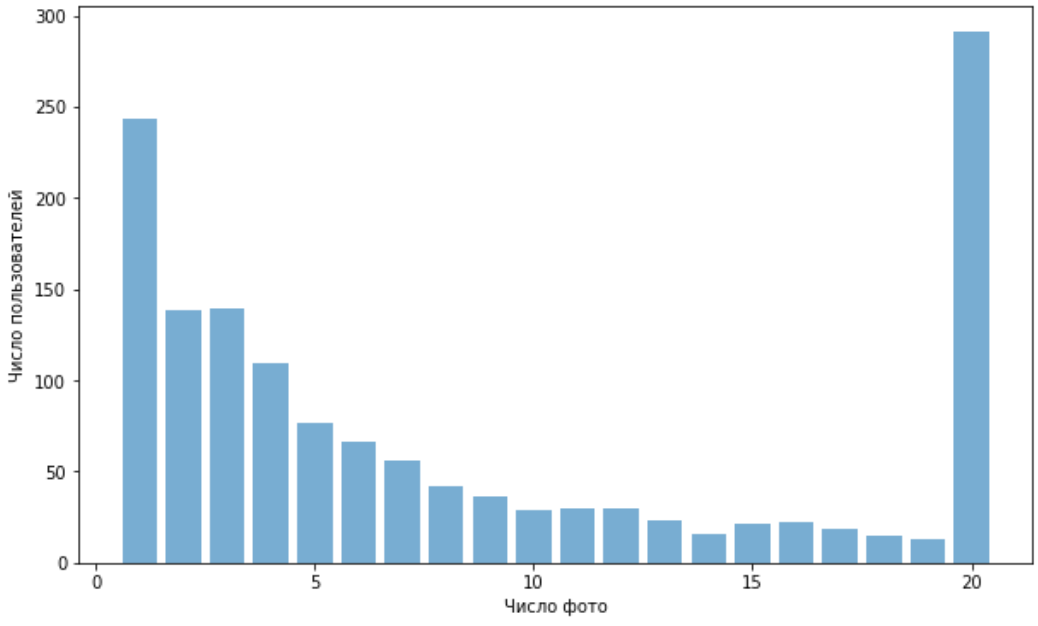


Рис. 1. Плотность распределения пользователей с разным количеством аватаров за последний год

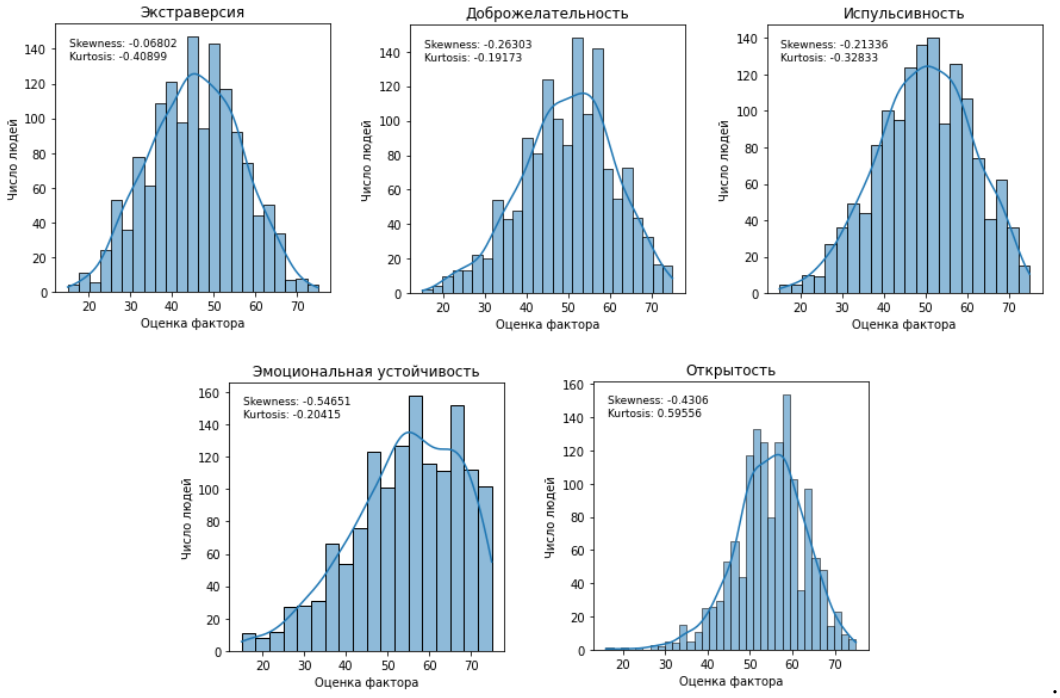


Рис. 2. Плотности распределения оценок по факторам 5PFQ

На рис. 2 представлены плотности распределения оценок по каждому фактору методики. Рассчитанные асимметрия и эксцесс, а также сглаженность свидетельствуют о почти нормальном распределении. Однако значение эксцесса для «Эмоциональной устойчивости» равняется -0.20415, что свидетельствует о большей удаленности распределения от нормального в сравнении с другими факторами личности, что может говорить о недостаточности данных или специфике выборки, однако ожидается, что подобное смещение не должно оказать значительного влияния на результат.

Для построения оценок выраженности черт личности в соответствии с указанной методикой необходимо из аватаров извлечь следующий набор признаков:

- Красочность [7];
- Цветовое разнообразие [8];
- Цветовая гармония [9];
- Шкала Pleasure Arousal Dominance (PAD) [10];
- Доли низкого, среднего и высокого значений компонент цветового пространства RGB на изображении;
- Доли низкого, среднего и высокого значений компонент цветового пространства HSV на изображении;
- Естественность [11];
- Контраст;
- Яркость [12].

В итоге подготовки данных был получен набор, состоящий из 12035 записей «№ пользователя – перечень цветовых характеристик i-го изображений – результат прохождения 5PFQ». Для всех аватаров пользователя был присвоен один и тот же результат прохождения тестирования.

Для построения автоматизированного средства оценки выраженности психологических особенностей пользователей социальных сетей по его аватару было решено построить предсказательную регрессионную модель на основе Gradient Boosting Tree, как одного из наиболее ярких и популярных представителей ансамблевых моделей для решения смежных задач [8]. К сожалению, в рамках данной задачи, нейронные сети показывали недостаточную точность, по причине нехватки данных для обучения.

Обучение происходило на упомянутом ранее наборе данных, при помощи GridSearch для получения лучших значений гиперпараметров модели и пятикратной перекрестной проверкой. Также при этом был проведен эксперимент по оценке качества предсказаний, относительно количества использованных фотографий. Вместе с тем было решено рассмотреть обе ситуации, когда записи по всем аватарам одного пользователя соответствуют одну и тому же результату прохождения тестирования и рассматриваются в отдельности, а также, когда характеристики изображений, принадлежавших одному пользователю, усредняются. При обучении выбирались подвыборки для 1-го, 3-х, 5-ти, 10-ти, 15-ти, 20-ти последний аватаров, размещенных пользователем за год. Количество уникальных пользователей убывало соответственно. Итоговые оценки точности по RMSE представлены в табл. 1.

Таблица 1

Усредненные значения метрики RMSE при обучении модели с кросс-валидацией для сравнения результатов

	по 5 фото, без усреднения	по 5 фото, с усреднением	по 10 фото, без усреднения	по 10 фото, с усреднением	по 20 фото, без усреднения	по 20 фото, с усреднением
Экстраверсия	0.190455	0.190725	0.194720	0.196456	0.233903	0.237436
Доброжелательность	0.184727	0.184244	0.182138	0.185547	0.185822	0.194954
Сознательность	0.189822	0.187141	0.188678	0.190307	0.211338	0.226094
Эмоциональная устойчивость	0.217383	0.218395	0.210016	0.210306	0.237186	0.222466
Открытость	0.135005	0.136693	0.147158	0.151561	0.167004	0.165517

Стоит отметить, что для краткости в таблице представлены наиболее значимые результаты. Подвыборки с 1 и 3 изображениями показали неудовлетворительный результат предсказания и были упразднены, а подвыборка с 15 аватарами не отличалась от результата с 10. Хуже себя показала подвыборка с 20 фотографиями за год, однако, этот может свидетельствовать о сокращении разнообразия в обучающих данных и как следствие снижение точности. Таким образом было экспериментально показано, что на основе 5-ти последних аватаров можно говорить о личностных особенностях пользователя и пытаться с высокой степенью точности предсказывать их выраженности. Стоит отметить, что значимых отличий в подходе с усреднением выявлено не было.

Заключение. В рамках данной работы была достигнута цель по формированию подхода с автоматизацией оценки выраженности психологических особенностей пользователей социальных сетей на основе цветовых характеристик изображений-аватаров их профилей. Полученный результат показал высокую точность, в особенности, учитывая специфику области психологии. Также было выяснено, что устойчивое представление о результатах прохождения пятифакторного опросника личности можно получить при рассмотрении 5 аватаров последних аватаров пользователя. Теоретическая и практическая значимости заключаются в том, что сформи-рован новый подход, отличающийся от известных задействованным в анализе перечнем данных, и построена предсказательная модель, позволяющая оценить выраженность личностных черт по 5 факторам на основе опубликованных изображений профиля в социальных медиа, что опосредованно в дальнейшем позволит строить оценки защищенности пользователя от социоинженерных атак, строить рекомендации по профориентации, настраивать таргетированную рекламу, точнее составлять кредитный скоринг клиента, а также продвинет исследования в областях психологии и социологии и разовьет сферу товаров и услуг.

Работа велась в рамках государственного задания СПб ФИЦ РАН № 0073-2019-003); при финансовой поддержке проекта РНФ № 23-21-00338, а также гранта Президента МК-5237.2022.1.6

СПИСОК ЛИТЕРАТУРЫ

1. Чернышенко сообщил, что почти 90% населения России пользуются интернетом // ТАСС [Электронный ресурс]. URL: https://tass.ru/obschestvo/15891729 (дата обращения: 20.06.2023).
2. «Цифровая экономика РФ» [Электронный ресурс] // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: [сайт]. URL: https://digital.gov.ru/ru/activity/directions/858/ (дата обращения: 20.06.2023).
3. Kemp S. DIGITAL 2023: GLOBAL OVERVIEW REPORT [Электронный ресурс] // DataReportal. URL: https://datareportal.com/reports/digital-2023-global-overview-report (дата обращения: 20.06.2023).
4. Алиуллов Ш. Самые популярные соцсети в России: рейтинг 2023 года [Электронный ресурс] // 4PDA:[сайт]. URL: https://4pda.to/2023/03/06/410508/samye_populyarnye_sotsseti_v_rossii_rejting_2023_goda/ (дата обращения: 20.06.2023).
5. Соколова А. Аудитория восьми крупнейших соцсетей в России в 2023 году: исследования и цифры [Электронный ресурс] // PPC.World. URL: https://ppc.world/articles/auditoriya-vosmi-krupneyshih-socsetey-v-rossii-issledovaniya-i-cifry/ (дата обращения: 20.06.2023).
6. Хромов А. Б. Пятифакторный опросник личности : учебно-метод. пособие. Курган : КГУ, 2000. 23 с.
7. Hasler D., Suesstrunk, S. Measuring Colourfulness in Natural Images. Proceedings of SPIE —The International Society for Optical Engineering. 2003. № 5007. Pp. 87-95.
8. Jang Hyun Kim, Yunhwan Kim. Instagram user characteristics and the color of their photos: Colorfulness, color diversity, and color harmony // Information Processing & Management. 2019. Vol. 56(4). Pp. 1494-1505.
9. Datta R., Joshi D., Li Jia, Wang J. Studying Aesthetics in Photographic Images Using a Computational Approach. Proceedings of the 9th European Conference on Computer Vision, (Graz). 2006. № 3., Pp. 288-301. doi: 10.1007/11744078_23.
10. Valdez P., Mehrabian A. Effects of color on emotions // Journal of experimental psychology. General, 1994. Vol. 123 № 4. Pp. 394-409.
11. Huang K. Q., Wang Q., Wu Z. Y.. Natural color image enhancement and evaluation algorithm based on human visual system// Comput. Vis. Image Underst. 2006. Vol. 103(1). Pp. 52–63.
12. Siersdorfer S., San P., Jose M., Sanderson M. Automatic Video Tagging using Content Redundancy, 2009. Pp. 395-402. 10.1145/1571941.1572010.

УДК 004.8

ФАКТОРЫ УСКОРЕНИЯ ГЛОБАЛЬНОГО АПОСТЕРИОРНОГО ВЫВОДА В АЛГЕБРАИЧЕСКИХ БАЙЕСОВСКИХ СЕТЯХ ЗА СЧЕТ ИСПОЛЬЗОВАНИЯ ТРЕТИЧНОЙ СТРУКТУРЫ

Вяткин Артём Андреевич, Абрамов Максим Викторович
СПИИРАН ─ СПб ФИЦ РАН
14-я лин. В. О., 39, Санкт-Петербург, 199178, Россия
e-mails: aav@dscs.com, mva@dscs.pro

Аннотация. В теории алгебраических байесовских сетей существуют два метода проведения глобального апостериорного вывода, использующие вторичную и третичную структуры. Данная статья направлена на определение факторов, которые способствуют ускорению проведения глобального апостериорного вывода за счет использования третичной структуры алгебраической байесовской сети по сравнению со вторичной структурой. Этими факторами, в результате, явились, необходимость построения вторичной структуры, требующей построения третичной, и, что имеет решающее значение, использование свидетельств с меньшей мощностью нагрузки. Помимо этого, приведен пример, показывающий распространение свидетельств с меньшим числом атомов при использовании третичной структуры.

Ключевые слова: алгебраические байесовские сети; вероятностные графические модели; фрагмент знаний; третичная структура; вторичная структура; глобальный апостериорный вывод; машинное обучение.

FACTORS OF ACCELERATING GLOBAL POSTERIOR INFERENCE IN ALGEBRAIC BAYESIAN NETWORKS BY USING TERTIARY STRUCTURE

Vyatkin Artyom, Abramov Maxim
SPIIRAN ─ SPb FRC RAS
39 V. I. 14th line, St. Petersburg, 199178, Russia
e-mails: aav@dscs.com, mva@dscs.pro

Abstract. In the theory of algebraic Bayesian networks, there are two methods of global posterior inference using secondary and tertiary structures. This paper aims to determine the factors that contribute to the acceleration of global posterior inference by using the tertiary structure of an algebraic Bayesian network compared to the secondary structure. These factors, as a result, were, the need to construct a secondary structure requiring the construction of a tertiary structure and, crucially, the use of evidence with less load cardinality. In addition, an example is given to show the propagation of evidence with fewer atoms when a tertiary structure is used.

Keywords: algebraic Bayesian networks; probabilistic graphical models; knowledge pattern; tertiary structure; secondary structure; global posteriori inference; machine learning.

Введение. Вероятностные графические модели на текущий момент находят широкое применение в контексте различных прикладных задач, которыми являются, например, определение человеческих эмоций [1], диагностирование неисправностей технологических процессов [2], прогнозирование распространения возбудителей болезней [3], анализ прочности материалов [4]. Подклассом вероятностных графических моделей являются алгебраические байесовские сети, определяемые как логико-вероятностные графические модели баз фрагментов знаний. В теории алгебраических байесовских сетей один из важных вопросов — вопрос проведения апостериорного вывода, пересчета оценок элементов сети на основе формализованной новой поступившей информации. Ранее были описаны два метода, использующие для проведения глобального апостериорного вывода вторичную и третичную структуры соответственно [5].

В статье [6] указывается, что при проведении глобального апостериорного вывода в алгебраических байесовских сетях, где число фрагментов знаний равно 5–150, алгоритм, использующий третичную структуру, работает в 1.15–2 раза быстрее, чем алгоритм, использующий вторичную структуру. Выявление же причин такого ускорения способствует дальнейшему поиску еще более быстрых алгоритмов и оптимизации текущих, что особенно важно в теории алгебраических байесовских сетей, где в основе многих методов работы с моделями лежит ресурсоемкая операция решения задач линейного программирования. Таким образом, цель данной статьи состоит в поиске факторов вышеописанного ускорения.

Теоретическая основа. Перед определением факторов, содействующих разнице во времени работы алгоритмов, необходимо определить основные рассматриваемые объекты, а также описать сами алгоритмы, чему и будет посвящен этот раздел.

Алгебраический баейсовские сети — графовые структуры, которые рассматриваются над отдельными, более мелкими объектами — фрагментами знаний. Сам же фрагмент знаний — структура, которая определяется, в частности, его нагрузкой, алфавитом (атомами). Например, алфавитом может служить множество $\{x_0, x_1\}$, при этом между фрагментами знаний будут определяться операции пересечения как между алфавитами, над которыми они построены. Более строго, фрагмент знаний может определяться, например, как набор квантов над собственным

алфавитом. Квант — конъюнкция атомов из алфавита, а также их отрицаний. Например, для алфавита $\{x_0, x_1\}$ набором квантов будет множество $\{\underline{x_1}x_0, \underline{x_1}x_0, x_1\underline{x_0}, x_1x_0\}$. Помимо этого, квантам сопоставляются скалярная или интервальная оценка вероятности их истинности. Апостериорным выводом в таком случае является пересчет оценок фрагмента знаний на основе поступившего *свидетельства – распространение, пропагация* свидетельства. В качестве свидетельства могут выступать другие фрагменты знаний, а также положительные и отрицательные означивания конкретных атомов. Такой апостериорный вывод зовется *локальным,* так как происходит на уровне конкретного фрагмента знаний.

Набор фрагментов знаний задает простейшую структуру алгебраической байесовской сети — первичную структуру. Вторичной же структурой является граф смежности, где вершины графа нагружены фрагментами знаний. Граф смежности — граф, где в первую очередь никакая нагрузка вершины не входит в нагрузку другой вершины, а также между любой парой вершин, которые содержат общие элементы, то есть пересечение алфавитов соответствующих фрагментов знаний не пусто, существует путь. В-третьих, наконец, каждая из вершин, которые находятся на этом пути, включает в себя пересечение крайних для пути фрагментов знаний.

С помощью вторичной структуры алгебраической байесовской сети можно проводить уже глобальный апостериорный вывод, то есть распространение влияния свидетельства во все фрагменты знаний сети. Опишем проведение апостериорного вывода в данном случае, не умаляя общности, сказав, что первоначальное свидетельство, которое необходимо учесть во всей сети, изначально включается в некоторый фрагмент знаний сети. Итак, во-первых, берется тот фрагмент знаний, в который включено свидетельство, и, далее, производится локальный апостериорный вывода для этого фрагмента знаний и первоначального свидетельства. Затем рассматриваются соседи данного фрагмента знаний, а также их пересечения с ним. Для каждого соседа рассматривается соответствующее пересечение, которое определяется как новое, виртуальное, свидетельство, далее распространяемое в фрагмент знаний-сосед. Таким образом происходит пропагация свидетельства в фрагмент знаний-сосед, что, рекурсивно, повторяется для остальных фрагментов знаний в сети. В данном случае будем рассматривать только ациклические алгебраические байесовские сети — сети, которые представимые в виде дерева смежности. Для таких сетей описанный алгоритм пропагации пройдет всегда корректно [5].

Наконец, третичной структурой алгебраической байесовской сети является диаграмма Хассе для множества непустых пересечений фрагментов знаний, объединенное с множеством фрагментов знаний сети, а также пустым множеством. Помимо фрагментов знаний и их пересечений будем также рассматривать однозначно с ними отождествляемые нагрузки. С помощью третичной структуры, как упоминалось ранее, можно также проводить глобальный апостериорный вывод, который состоит из следующих шагов [5]:

Шаг 1. Распространить u во все фрагменты знаний, содержащие u, где само u содержит нагрузку свидетельства. Повторное распространение свидетельства в фрагменты знаний не проводится.

Шаг 2. В третичной структуре пометить нагрузку u и всех ее потомков. При этом если обнаружилась нагрузка со всеми помеченными потомками, то ее также необходимо пометить.

Шаг 3. Выбрать непомеченную нагрузку максимальной мощности v, непосредственным потомком которой является некоторая помеченная нагрузка w. Если такую нагрузку найти не удается, то завершить алгоритм.

Шаг 4. Сформировать новое свидетельство, нагрузка которой совпадает с v, а оценки вероятности истинности взяты из какого-либо фрагмента знаний, содержащего w. Далее с новым свидетельством перейти к шагу 1.

Стоит отметить, что для вышеописанного алгоритма корректность работы также доказана только для ациклических алгебраических байесовских сетей.

Сравнение времен работы алгоритмов. Стоит сказать, что непосредственной пропагации свидетельства с использованием вторичной и третичной структуры, предшествует построение этих структур. При этом для формирования вторичной структуры необходимо использовать третичную [7], что, несомненно, является одним из факторов, способствующих более быстрому проведению глобального апостериорного вывода в случае третичной структуры. Однако были проведены экспериментальные исследования времени работы алгоритмов, которые показали, что этот фактор не является основополагающим при ускорении и дает выигрыш лишь в несколько процентов от общего времени работы. В результате проведенных экспериментов, где все алгоритмы реализовывались с использованием языка программирования Python, было установлено, что основное время занимает пропагация свидетельств в конкретные фрагменты знаний.

При пропагации свидетельства, представимого в виде фрагмента знаний, во времени работы его распространения важную роль играет мощность нагрузки этого свидетельства — время пропагации увеличивается экспоненциально относительно увеличения мощности нагрузки свидетельства [8]. При этом, как показали проведенные эксперименты, основное время работы алгоритма апостериорного вывода уходит на пропагацию свидетельства в фрагменты знаний, поэтому размер свидетельства является существенным фактором.

Проведение дальнейших экспериментов с обоими алгоритмами показало, что именно различные размеры свидетельств, которые распространяются в фрагменты знаний, имеют ключевую роль в разнице времени работы алгоритмов. Ускорение же алгоритма, использующего третичную структуры достигается за счет того, что при пропагации по диаграмме Хассе выбираются нагрузки, лежащие все ближе к вершине-пустой нагрузке, а значит

имеющие все меньшую и меньшую мощность. В то время как при пропагации во вторичной структуре выбираются нагрузки, лежащие на пересечениях фрагментов знаний, которые будут включать в себя нагрузки, выбираемые при пропагации с использованием третичной структуры, и часто имеющие большую мощность. Рассмотрим распространение свидетельства на примере алгебраической байесовской сети, состоящей из трех фрагментов знаний, построенных над алфавитами $\{x_0, x_1, x_2\}$, $\{x_0, x_1, x_3\}$, $\{x_1, x_2, x_4\}$. Вторичная структура над этими фрагментами знаний указана на рис. 1, соответствующая третичная же структура указана на рис. 2. Фрагменты знаний обозначены как атомы, над которыми они построены, заключенные в угловые скобки.

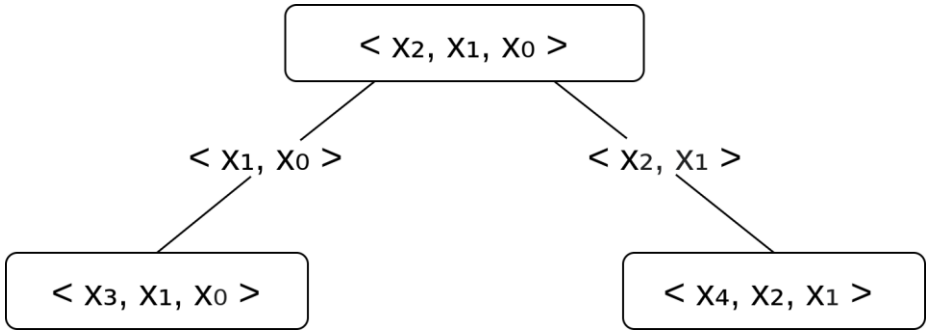


Рис. 1. Вторичная структура, представленная в виде дерева смежности

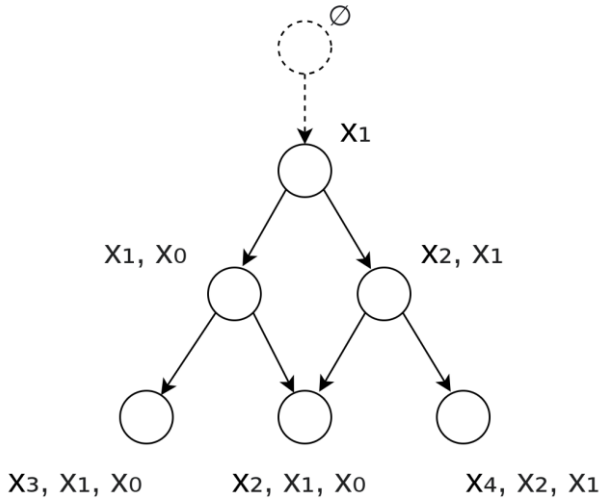


Рис. 2. Третичная структура

Предположим, что необходимо распространить свидетельство с нагрузкой, состоящей из одного атома x_1. Тогда, в случае вторичной структуры выбирается один фрагмент знаний, например $< x_0, x_1, x_2 >$, и свидетельство пропагируется в него. Затем выбираются пересечения этого фрагмента знаний и его соседей, составляются виртуальные свидетельства и далее распространяются уже они. Виртуальные свидетельства в данном случае будут иметь нагрузки $\{x_0, x_1\}, \{x_1, x_2\}$ и, соответственно, состоять из двух атомов. Подчеркнем, что независимо от выбора первоначального фрагмента знаний, в который будет распространятся свидетельство, виртуальные свидетельства для пропагации в остальные фрагменты знаний будут состоять из двух атомов.

Рассмотрим пропагацию свидительства с использованием третичной структуры. В этом случае на шаге 1 можно выбрать нагрузку, состоящую из одного атома x_1 и далее распространить соответствующее свидетельство во все фрагменты знаний, так как их нагрузки содержат x_1, после чего будет помечена вся третичная структура и алгоритм завершит свою работу. Таким образом, при использовании третичной структуры произошла пропагация свидетельств, состоящих только из одного атома, с использованием вторичной же структуры два виртуальных свидетельства имели по два атома. Поэтому в данной сети пропагация свидетельства произойдет быстрее с использованием третичной структуры.

Заключение. В данной работе определяются два фактора, за счет которых использование третичной структуры в задаче глобального апостериорного вывода дает выигрыш по времени по сравнению со вторичной структурой. Этими факторами являются, во-первых, необходимость построения вторичной структуры, которая требует построения третичной, и, во-вторых, что существеннее, пропагация свидетельств с меньшей мощностью нагрузки. Помимо этого, в работе описан пример, показывающий использование свидетельств меньшей мощности с применем третичной структуры.

В дальнейших исследованиях предполагается анализ выбросов, полученных при проведении эксперимента, указанного в статье [6], что также поможет определить дальнейшие пути по ускорению проведения алгоритма глобального апостериорного вывода, и что будет способствовать более активному внедрению алгебраических байесовских сетей в решение прикладных задач, связанных, например, с оценкой оценки защищенности систем от социоинженерных атак [9].

Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН СПИИРАН № FFZF-2022-0003.

СПИСОК ЛИТЕРАТУРЫ

1. Zhang L., Tong Y., Ji Q. Probabilistic graphical models and their applications in computer vision // Handbook of pattern recognition and computer vision. 2010. Pp. 129–156.
2. Amin M. T., Khan F., Ahmed S., Imtiaz S. A data-driven Bayesian network learning method for process fault diagnosis // Process Safety and Environmental Protection. 2021. Vol. 150. Pp. 110–122. DOI: 10.1016/j.psep.2021.04.004.
3. Wu Y., McLeod C., Blyth C., Bowen A., Martin A., Nicholson A., Mascaro S., Snelling T. Predicting the causative pathogen among children with osteomyelitis using Bayesian networks – improving antibiotic selection in clinical practice // Artificial Intelligence in Medicine. 2020. Vol. 107. Pp. 101895.
4. Petrolo M., Carrera E. On the use of neural networks to evaluate performances of shell models for composites // Advanced Modeling and Simulation in Engineering Sciences. 2020. Vol. 7. Pp. 1–28.
5. Вяткин А. А., Абрамов М. В., Харитонов Н. А., Тулупьев А. Л. Применение третичной структуры алгебраической байесовской сети в задаче апостериорного вывода // Вестник ЮУрГУ. Вычислительная математика и информатика. 2023. Т. 12. № 1. С. 61–88. DOI: 10.14529/cmse230104.
6. Vyatkin A. A., Tulupyev A. L. Statistical Comparison of the Running Times of Global Posteriori Inference Algorithms in Algebraic Bayesian Networks // 2023 XXVI International Conference on Soft Computing and Measurements (SCM), Saint Petersburg, Russian Federation. 2023. Pp. 24-28. doi:10.1109/SCM58628.2023.10159044.
7. Фильченков А. А., Фроленков К. В., Сироткин А. В., Тулупьев А. Л. Система алгоритмов синтеза подмножеств минимальных графов смежности // Информатика и автоматизация. 2013. № 27. С. 200–244. DOI: 10.15622/sp.27.17.
8. Тулупьев А. Л. Алгебраические байесовские сети: локальный логико-вероятностный вывод. СПб. : Анатолия, 2007. 80 с.
9. Khlobystova A. O, Abramov M. V. The models separation of access rights of users to critical documents of information system as factor of reduce impact of successful social engineering attacks // Russian Advances in Fuzzy Systems and Soft Computing: Selected Contributions to the 8th International Conference on «Fuzzy Systems, Soft Computing and Intelligent Technologies (FSSCIT 2020)». S., 2020. Pp. 264–268.

УДК 004.418

ПОДХОДЫ К РАЗРАБОТКЕ СЕРВИСА УЧЁТА РАСХОДОВ НА ТОПЛИВО И МАРШРУТНОЙ АДАПТАЦИИ С УЧЁТОМ ПОЛЬЗОВАТЕЛЬСКИХ ПАРАМЕТРОВ

Корепанова Анастасия Андреевна, Есин Максим Сергеевич, Сабреков Артём Азатович
СПИИРАН ─ СПб ФИЦ РАН
14 линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mails: aak@dscs.pro, mse@dscs.pro

Аннотация. В представленной работе освещается разработка и оптимизация сервиса, направленного на расчет стоимости автомобильных поездок с учётом стоимости дозаправки, с акцентом на внедрение механизма оптимизации маршрута и адаптации под пользовательские параметры: выбор конкретной топливной компании, типа топлива и начального его объема. Данная статья описывает актуальность задачи, исходные данные для реализации проекта и концепцию его исполнения, таким образом закладывая основу для дальнейших исследований.

Ключевые слова: оптимизация маршрута; расчет стоимости поездки; алгоритм Дейкстры; заправочные станции; стоимость топлива.

APPROACHES TO THE DEVELOPMENT OF A FUEL COST ACCOUNTING AND ROUTE ADAPTATION SERVICE ACCORDING TO USER PARAMETERS

Korepanova Anastasia, Esin Maksim, Sabrekov Artem
SPIIRAN ─ SPb FRC RAS
39 Vasilievsky Island 14th line, St. Petersburg, 199178, Russia
e-mails: aak@dscs.pro, mse@dscs.pro

Abstract. The article sheds light on the development and optimization of a service aimed at calculating the cost of car trips, taking into account the cost of refueling, with a focus on implementing a route optimization mechanism and adapting to user parameters: choosing a specific fuel company, type of fuel, and its initial volume. This article describes the relevance of the task, the initial data for implementing the project, and the concept of its execution, thus laying the foundation for further research.

Keywords: route optimization; trip cost calculation; Dijkstra's algorithm; gas stations; fuel cost.

Введение. В эпоху постоянной динамики цен на топливо и стремительной урбанизации глобального пространства, мобильность становится одним из ключевых аспектов повседневной жизни человека. Это

актуализирует вопрос оптимизации расходов на топливо, создавая почву для разработки технологических решений, способных минимизировать затраты водителей. Данная статья посвящена задаче разработки алгоритма автоматического построения маршрута, стратегически выгодного с точки зрения мест и объемов дозаправки. Главной задачей исследования является создание модели, способной анализировать текущие цены на топливо на различных заправочных станциях вдоль пути следования, и на основе этих данных строить оптимальный маршрут, не только учитывающий расстояние и время в пути, но и минимизирующий суммарные затраты на топливо, причем с учетом конкретных показателей каждого транспортного средства. Не менее важным является аспект удобства и доступности использования подобного сервиса для широкой аудитории автолюбителей, что обуславливает необходимость учета индивидуальных предпочтений пользователей, таких как выбор бренда топливных станций или типа топлива, а также дополнительных услуг, оказываемых на станциях. Ожидается, что предложенный алгоритм и реализующий его сервис станут ценным инструментом для экономии бюджетов автомобилистов, а также способствуют более рациональному использованию энергоресурсов на общественном уровне.

Данная работа выполняется в рамках сервиса Cargotime.ru [9], представляющего набор инструментов для участников логистического рынка, которые позволяют им более качественно и продуктивно взаимодействовать друг с другом.

На данный момент существует ряд сервисов, призванных облегчить жизнь автомобилиста, упростив процесс выбора и оплаты топлива. Drivvo [1] предоставляет инструментарий для управления финансовыми и эксплуатационными аспектами владения автомобилем, позволяя отслеживать расходы на топливо, регистрировать штрафы и хранить основную информацию о транспортном средстве. Функционал «Где дозаправка» дает возможность увидеть расположение ближайших АЗС и актуальные цены на топливо. Однако, несмотря на полезность представляемой информации, Drivvo не предоставляет возможности оптимизации маршрута с учетом расположения и цен на заправочных станциях. Сервис «Яндекс заправки» выходит за рамки простого информирования о стоимости топлива, предлагая возможность его оплаты без выхода из автомобиля на подключенных к сервису АЗС. Дополнительно, сервис может построить маршрут с учетом выбранной заправочной станции. Однако, его функционал ограничен построением маршрута только через одну АЗС, не обеспечивая полной оптимизации пути с учетом топливных расходов. FuelUP [2] ориентирован на оплату топлива без физического посещения кассы, предоставляя возможность оплаты прямо через приложение на участвующих в программе АЗС. Основными плюсами являются возможность оплаты топлива на расстоянии и фильтрации по типам топлива. Тем не менее, FuelUP не предлагает функциональности, связанной с планированием маршрута или поиском заправочных станций вдоль пути, ограничиваясь лишь базой данных АЗС, подключенных к сервису. Waze [3], в основном, фокусируется на навигации, помогая избежать пробок и предлагая оптимальные пути движения, благодаря активному участию сообщества водителей, которые делятся актуальной информацией о дорожной обстановке. В приложении есть возможность видеть ближайшие заправки и, благодаря пользователям, цены на топливо на них, что может быть полезно в пути. Но, несмотря на широкую базу данных, предоставляемую сообществом, она может содержать устаревшую информацию о ценах на топливо и, также как FuelUP, не предоставляет возможности оптимизировать маршрут с учетом расходов на топливо. Benzuber [4] фокусируется на удобстве топливных транзакций, позволяя осуществлять оплату бензина без посещения кассы, а также предлагая скидки от партнерских компаний. Сервис позволяет добавлять ближайшие заправочные станции в избранное и следить за динамикой цен на топливо. Однако, так же как и Drivvo, Benzuber не предоставляет инструментов для оптимизации маршрута в плане стоимости и расположения заправочных станций.

Как видно из обзора, существующие решения предоставляют ценную функциональность в определенных аспектах вождения и управления топливо заправкой, но не полностью решают проблему оптимизации маршрута с точки зрения экономии на топливе, что подчеркивает актуальность и значимость разработки нового, всеобъемлющего решения в этой области.

Для реализации первоначальной и доработанной версии приложения были выбраны следующие инструменты и технологии:

– Google Places API: Этот сервис обеспечивает доступ к данным о местоположении через HTTP-запросы и возвращает результаты в форматах XML или JSON. Он был использован для формирования маршрута и расчёта дистанции между заданными точками;

– TypeScript: Как строго типизированный язык, который расширяет функционал JavaScript, TypeScript поддерживает различные стили программирования и обеспечивает дополнительную безопасность типов данных. Компилируемый в JavaScript, он совместим с различными браузерами и может использоваться совместно с серверными платформами, например, Node.js;

– Node.js и NestJS: Node.js выступает в роли кросс-платформенной серверной среды, транслируя JavaScript в машинный код, а NestJS — это фреймворк, который обеспечивает удобную архитектуру для создания масштабируемых приложений, простоту разработки и управления на серверной стороне;

– MySQL и TypeORM: MySQL была выбрана в качестве системы управления реляционными базами данных из-за её использования в существующем проекте. В сочетании с TypeORM, который является объектно-реляционным отображением (ORM) и способен работать с различными платформами и языками

программирования, эта технология обеспечивает эффективное управление данными. TypeORM, в частности, является популярной библиотекой для проектов на TypeScript, облегчая взаимодействие с базой данных.

Таким образом, комбинация вышеупомянутых технологий создаёт надёжную и масштабируемую основу для разработки, которая обеспечивает гладкую интеграцию между различными аспектами приложения.

Данный проект продолжает уже имеющийся сервис. Ниже представлена его микросервисная архитектура.

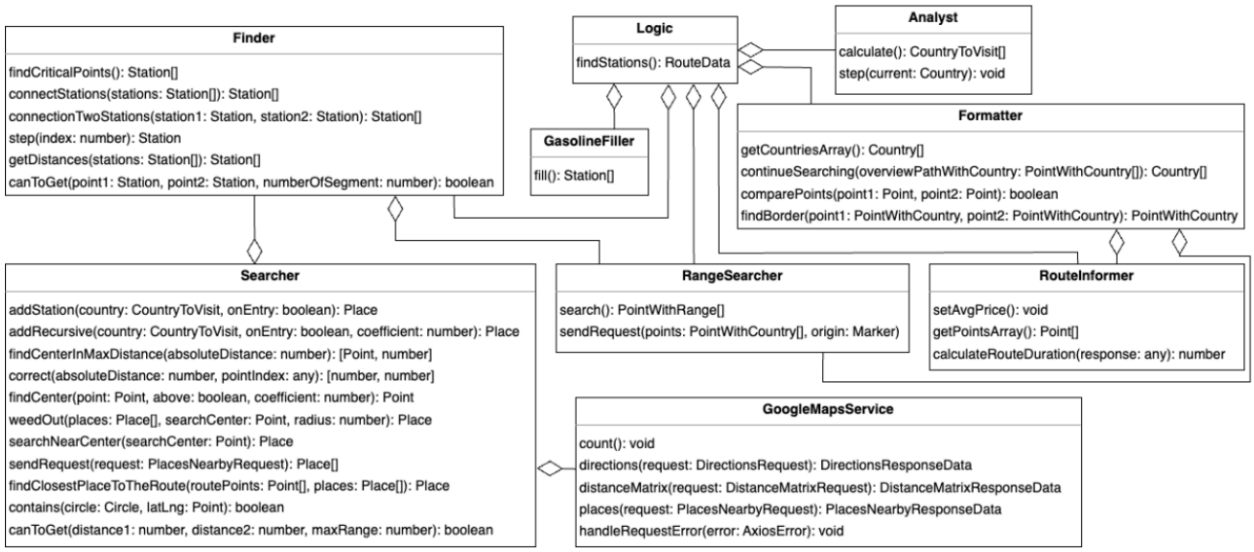


Рис. 1. Изначальная архитектура сервиса.

Ниже приведён обзор подходов, применяющихся для решения оптимизационных задач на графах.

Задача поиска кратчайшего пути долгое время оставалась в центре внимания исследователей, приведя к разработке множества алгоритмов. В исследовании [5], проведенном на основе реальных дорожных сетей, были сравнены результаты и эффективность алгоритма Дейкстры, его модификаций, алгоритма Беллмана — Форда и других алгоритмов. Далее мы подробнее рассмотрим алгоритмы Дейкстры, A* и Флойда — Уоршелла. Алгоритм Дейкстры выделяется как один из наиболее известных и широко применяемых алгоритмов поиска кратчайшего пути в графе. Он на каждом этапе выбирает вершину с наименьшим расстоянием до стартовой вершины, далее интегрируя её в дерево кратчайших путей. Его сложность составляет $O(|E| + |V| \log |V|$, где $|E|$ и $|V|$ — это количество рёбер и вершин графа соответственно. Модификации алгоритма используются в различных практических задачах, например, при построении маршрутов в сервисе Яндекс.Карты. Алгоритм A* служит для нахождения кратчайшего пути между двумя узлами взвешенного графа, применяя жадный метод и использование эвристики для оценки оставшегося расстояния до цели. Его сложность — O(bd), где b и d — среднее количество возможных действий на каждом узле и глубина решения соответственно. Алгоритм Флойда-Уоршелла, использующий метод динамического программирования, вычисляет кратчайшие расстояния между всеми парами вершин в графе, учитывая положительные и отрицательные веса рёбер. При сложности O(|V|^3), этот алгоритм не является оптимальным для создания экономически эффективного маршрута, поскольку не сохраняет данные о кратчайших путях и вычисляет расстояние между всеми парами вершин, тогда как для нашей задачи важно определить расстояние только между начальной и конечной точками.

На основании проведенного анализа, принято решение о применении алгоритма Дейкстры для формирования маршрута, который будет оптимальным по стоимости, учитывая отсутствие рёбер с отрицательным весом и способность алгоритма учитывать специфику рассматриваемого процесса.

Для дальнейшей разработки алгоритма необходимо было разработать концепцию получения, обработки и хранения данных о заправочных станциях. Информация о заправочных станциях аккумулируется в созданной таблице под названием «gas_station», в которой хранятся данные, такие как название станции, бренд, страна, регион, город, координаты (широта и долгота), а также цены на различные виды топлива и дополнительные услуги.

Данные для таблицы были получены из следующих ключевых источников:

– официальные сервисы АЗС [6, 7];
– сервисы, имеющие партнерские отношения с АЗС [8].

Официальные сервисы заправочных станций являются первоисточниками самых актуальных и надежных данных по заправкам, и поэтому при определении приоритетности использования данных, информация от официальных сервисов обрабатывается как наиболее достоверная и свежая.

Партнерские сервисы, в основном, фокусируются на предоставлении дисконтных карт для разнообразных брендов АЗС. Их цель сбора данных о заправочных станциях и стоимости топлива заключается в демонстрации различий в стоимости топлива с использованием и без использования их продуктов.

Заключение. В данной статье были заложены основы для дальнейшего исследования алгоритма оптимизации стоимости поездки на машине, а внимание было сосредоточено на определении оптимальных стратегий и методик для решения задач, связанных с построением маршрутов и обработкой данных. Алгоритм Дейкстры, несмотря на свои особенности и условности применения, был выбран в качестве основного инструмента для разработки экономически выгодных маршрутов, учитывая специфику рассматриваемого процесса. Также была обозначена значимость аккуратного и структурированного хранения информации о заправочных станциях для обеспечения точности и актуальности данных, взятых из различных источников.

На практике, внедрение оптимизированных алгоритмов поиска пути и эффективных систем управления данными в действующие логистические и транспортные системы может привести к значительному усовершенствованию в области планирования маршрутов и ресурсоемкости процессов. Дальнейшее исследование состоит в разработке аглгоритма оптимизации стоимости маршрута или переработке существующих алгоритмов под конкретную задачу. Результаты данной работы будут использоваться в рамках сервиса Cargotime.ru и поспособствуют развитию автоматизации сферы логистики в Российской Федерации.

Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН СПИИРАН № FFZF-2022-0003; при финансовой поддержке РФФИ, проект №20-07-00839

СПИСОК ЛИТЕРАТУРЫ

1. Drivvo — system for managing vehicle fleets, which gives the manager total control over vehicles and drivers : [сайт]. [Электронный ресурс]. URL: https://www.drivvo.com/en. (дата обращения 23.09.2023).
2. FUELUP — технологический топливный онлайн-сервис, который помогает заправлять автомобиль не покидая салона : [сайт]. [Электронный ресурс]. URL: https://fuelup.ru/ (дата обращения: 24.06.2023).
3. Waze — направление движения, дорожные условия и пробки: сайт [Электронный ресурс]. URL: https://www.waze.com/ru/live-map/(дата обращения: 24.06.2023).
4. Benzuber — онлайн-сервис для оплаты топлива на АЗС : сайт [Электронный ресурс]. URL: https://benzuber.ru/ (дата обращения: 24.06.2023).
5. Zhen B., Noon C. Shortest Path Algorithms: An Evaluation using Real Road Networks // Transportation Science. 1998. Pp. 65–73.
6. Сеть АЗС Газпром: сайт [Электронный ресурс]. URL: https://www.azsgazprom.ru/ azs-prices/ (дата обращения: 24.06.2023).
7. Сеть АЗС РосНефть [Электронный ресурс]. URL: https://www.rosneft-azs.ru/ Nasha-set/about (дата обращения: 24.06.2023).
8. КАРДЕКС — топливные карты для юридических лиц [Электронный ресурс]. URL: https://card-oil.ru/set_azs/(дата обращения: 24.06.2023).
9. Cargotime — единая грузовая служба [Электронный ресурс]. URL: https://cargotime.ru/ (дата обращения: 24.06.2023).

УДК 004.418

ЛОГИСТИЧЕСКИЙ ПОРТАЛ CARGOTIME.RU: АВТОМАТИЗАЦИЯ МОНИТОРИНГА СТАБИЛЬНОСТИ РАБОТЫ СЕРВИСА РАСЧЕТА СТОИМОСТИ ДОСТАВКИ

Назарова Полина Андреевна[1], Есин Максим Сергеевич[2], Сабреков Артём Азатович[3]
[1] Санкт-Петербургский национальный исследовательский Академический университет
имени Ж.И. Алферова Российской академии наук
Хлопина ул., 8, корп. 3, лит. А, Санкт-Петербург, 194021, Россия
[2] СПИИРАН ─ СПб ФИЦ РАН
В. О. 14 линия, 39, Санкт-Петербург, 199178, Россия
[3]Санкт-Петербургский государственный университет
Университетская наб., 7–9, Санкт-Петербург, 199034, Россия
e-mails: ktotochra9@gmail.com, mse@dscs.pro, aas@dscs.pro

Аннотация. В статье рассматривается концепция автоматизированной системы мониторинга стабильности работы сервиса стоимости доставки в контексте разработки логистического портала Cargotime.ru.

Ключевые слова: логистика; система автоматического мониторинга; мониторинг доступности веб-ресурсов; веб-разработка; парсеры.

AUTOMATED MONITORING SYSTEM FOR THE STABILITY OF DELIVERY COST CALCULATION SERVICE ON CARGOTIME.RU LOGISTICS PORTAL

Nazarova Polina[1], Esin Maxim[2], Sabrekov Artem[3]
[1] Saint Petersburg National Research Academic University of the Russian Academy of Sciences,
8/3 Hlopina St, St. Petersburg, 194021, Russia
[2] SPIIRAN ─ SPb FRC RAS
39 14th Line St, St. Petersburg, 199178, Russia
[3]St. Petersburg State University
7-9 Universitetskaya Emb, St Petersburg 199034, Russia
e-mails: ktotochra9@gmail.com, mse@dscs.pro, aas@dscs.pro

Abstract. The article discusses the concept of an automated monitoring system for the stability of the delivery cost service within the context of developing the Cargotime.ru logistics portal.

Keywords: logistics; automated monitoring system; web resource availability monitoring; web development; parsers.

Введение. В современном мире логистики, где скорость, точность и надежность играют важную роль в успехе бизнеса, логистические порталы становятся неотъемлемой частью операционных процессов множества компаний. Они предоставляют возможность эффективно управлять процессом грузоперевозок, что имеет прямое влияние на конечные результаты и удовлетворенность клиентов. В контексте этой динамичной среды, логистический портал Cargotime.ru [1], разрабатываемый на базе лаборатории теоретических и междисциплинарных проблем информатики [2], предлагает уникальные решения для сферы логистики.

Одним из ключевых инструментов, обеспечивающих успешное функционирование Cargotime.ru, является сервис расчета стоимости доставки грузов [3, 4]. Этот инструмент осуществляет сбор и анализ данных о стоимости и сроках доставки грузов с сайтов различных перевозчиков и представляет эту информацию в удобном и единообразном формате на портале Cargotime.ru. Кроме того, сервис позволяет минимизировать стоимость маршрута путём построения сложного маршрута, на котором груз перевозят несколько компаний вместо одной [5]. Однако, чтобы обеспечить стабильность работы сервиса и, следовательно, качество обслуживания пользователей, была разработана и внедрена система автоматического мониторинга работы данного сервиса. Именно этой системе посвящена данная статья.

На рис. 1. представлен принцип работы сервиса расчета стоимости доставки.

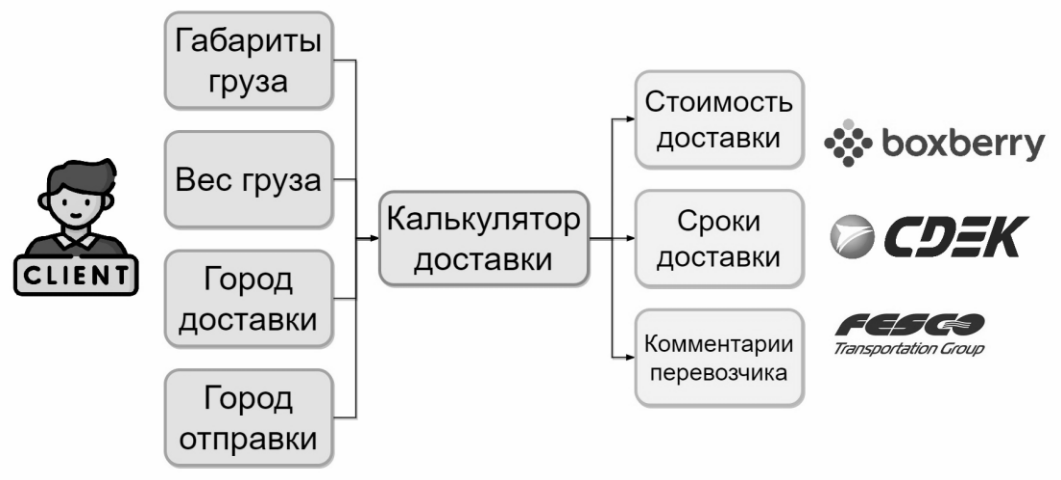


Рис. 1. Принцип работы сервиса расчета стоимости доставки

Научная актуальность данного исследования состоит в необходимости создания автоматизированной системы мониторинга, поскольку она играет важную роль в стабильности работы системы. Время и точность информации о стоимости доставки стали критически важными для принятия решений в бизнесе, и компании все больше ориентируются на логистические порталы, предоставляющие эту информацию в режиме реального времени. В условиях конкуренции на рынке логистики, сложно переоценить роль автоматизации мониторинга стабильности сервисов в обеспечении качественного обслуживания клиентов. Исследование системы автоматического мониторинга на примере сервиса расчета стоимости Cargotime.ru не только демонстрирует практическое применение современных технологий в логистике, но и открывает путь к дальнейшим научным исследованиям в области автоматизации и оптимизации логистических систем.

Формулировка задачи. Основной целью данного исследования является анализ и описание системы автоматического мониторинга работы сервиса расчета стоимости на портале Cargotime.ru. В рамках статьи будут рассмотрены технические детали и механизмы функционирования этой системы, а также выявлены преимущества, которые она приносит компании и ее клиентам.

Результаты данного исследования будут полезны как для технических специалистов, работающих в сфере логистики и информационных технологий, так и для предпринимателей и руководителей компаний, заинтересованных в оптимизации своих логистических процессов и обеспечении стабильности работы логистических порталов. Результаты и выводы данной статьи могут послужить основой для разработки и усовершенствования подобных систем в других сферах бизнеса, что делает исследование актуальным и значимым для широкой аудитории.

Концепция сервиса автоматического мониторинга.

Специфика предметной области. Для того, чтобы разработать систему автоматизации мониторинга, необходимо ознакомиться со спецификой предметной области, а именно — сервисом расчета стоимости доставки. Сервис расчета стоимости доставки на портале Cargotime.ru представляет из себя агрегатор калькуляторов, которые позволяют вычислить примерную стоимость и сроки доставки. Парсеры калькуляторов доставки, которые представляют из себя автоматизированные скрипты, как правило, состоят из нескольких запросов, таких как запрос аутентификации, запрос на получение грузовых лимитов, запросы на получение локаций и запросы стоимости и сроков доставки. Поскольку данный сервис взаимодействует с большим количеством различных веб-ресурсов и с каждого из них пытается получить данные, ошибки в парсерах возникают довольно часто и причиной этому могут служить как внешние причины (изменение API или фронтенда сайта компании, добавление нового уровня защиты или же временная недоступность страницы), так и внутренние (например, непредвиденная ошибка в коде самого парсера).

Механизмы работы сервиса. Сервис автоматического мониторинга предполагает работу в режиме реального времени и непрерывное отслеживание активности агрегатора калькуляторов стоимости доставки. Основные механизмы функционирования сервиса включают в себя проведение регулярных проверок, сбор и анализ данных. Более того, важной составляющей сервиса является система составления отчетности: в случае обнаружения непредвиденных событий и сбоев, система генерирует автоматические оповещения для технических специалистов, что позволяет им быстро реагировать и устранять проблемы. Это обеспечивает оперативное реагирование на проблемы и их немедленное устранение, минимизируя негативное воздействие на работу портала. Составление отчетности также позволяет иметь общее представление о стабильности работы парсеров (как часто они ломаются, по какой причине и насколько долго).

Классификация проверок. Система автоматического мониторинга включает в себя ряд проверок, совместно обеспечивающих бесперебойную работу агрегатора. Проверки можно разделить на две основные группы: частые и редкие. Частые проверки предназначены для мониторинга наиболее уязвимых мест в работе парсеров и выявления ошибок, требующих немедленного вмешательства. Они осуществляются в реальном времени и позволяют оперативно реагировать на проблемы. Редкие проверки, напротив, включают в себя регулярную проверку работоспособности всех парсеров для составления ежедневной отчетности. Эти проверки обеспечивают общее представление о работоспособности каждого из парсеров и позволяют выявить тенденции и потенциальные проблемы на более долгосрочной основе. Относя проверку к частой или редкой, необходимо также учитывать особенности сайтов компаний, с которых агрегируются данные: запросы к некоторым сайтам требуют дополнительных финансовых затрат, поэтому излишне частые проверки таких сайтов будут финансово невыгодными.

Одной из наиболее важных и необходимых проверок является мониторинг доступности веб-ресурсов, с которых осуществляется парсинг информации о доставке. В начале процесса проверки из базы данных системы расчета стоимости доставки портала Cargotime.ru достается информация о веб-ресурсах, с которых осуществляется сбор данных. Эта информация включает в себя название компании, ссылку на сайт и информацию о доступности ресурса на данный момент времени. Система автоматического мониторинга выполняет проверку доступности каждого из источников, данных. Этот процесс осуществляется с использованием специализированных скриптов и алгоритмов, которые отправляют запросы к каждому веб-ресурсу и анализируют ответы. Периодичность проверок может быть настроена в зависимости от требований, но оптимальным будет пометить данную проверку как частую и проводить ее через короткие интервалы времени, например, каждые 10 минут. После выполнения проверки доступности, система анализирует полученные результаты. В случае изменения статуса доступности ресурса, система посылает запрос на включение или отключение соответствующего парсера, чтобы обеспечить бесперебойность обслуживания пользователей. Система также включает в себя механизмы оповещения и алертов. На основе результатов проверки генерируется отчет, отправляемый техническим специалистам, что позволяет быстро реагировать на возможные сбои и минимизировать их воздействие на работу портала. Также важно поддерживать историю доступности каждого веб-ресурса. Это позволяет анализировать тенденции и определять потенциальные проблемы на основе прошлых событий. Исторические данные также могут быть использованы для оптимизации процесса мониторинга и планирования ресурсов.

Преимущества автоматизации мониторинга. Автоматизация мониторинга стабильности системы имеет несколько важных преимуществ.

Во-первых, это снижение риска ошибок и повышение надежности системы. Автоматический мониторинг уменьшает вероятность человеческих ошибок в процессе контроля работы сервиса и гарантирует, что система всегда доступна и работает корректно, что способствует снижению рисков и увеличению уровня доверия со стороны клиентов.

Во-вторых, это экономия времени и ресурсов. Автоматический мониторинг снижает необходимость в ручной проверке и вмешательстве, что освобождает ресурсы для других задач и позволяет сократить операционные расходы.

И, наконец, это повышение уровня обслуживания. Стабильный и точный расчет стоимости доставки улучшает опыт клиентов, что может привести к повышению их лояльности и росту популярности портала.

Перспективы развития сервиса автоматического мониторинга на портале Cargotime.ru.

Система автоматического мониторинга на портале Cargotime.ru не только успешно справляется с текущими задачами обеспечения стабильности и бесперебойной работы системы расчета стоимости доставки, но и открывает двери к множеству будущих перспектив.

Алгоритмы мониторинга в перспективе можно улучшить. С развитием технологий машинного обучения и анализа данных, система автоматического мониторинга может стать более интеллектуальной и способной прогнозировать возможные сбои и проблемы до их возникновения. Это позволит принимать предупреждающие меры и уменьшать риски.

Систему можно дополнить новыми функциями, такими как мониторинг производительности и оптимизация запросов к источникам данных. Это может повысить эффективность и скорость сбора информации.

Эти перспективы развития позволяют видеть в системе автоматического мониторинга на портале Cargotime.ru мощный инструмент, способный эволюционировать вместе с растущими потребностями и вызовами логистической отрасли, предоставляя пользователям более надежный и эффективный сервис доставки.

Заключение. В статье была описана система автоматического мониторинга стабильности работы сервиса расчета стоимости доставки на логистическом портале Cargotime.ru. Эта система представляет собой неотъемлемую часть инфраструктуры портала, обеспечивающую стабильную работу сервиса. Ее значимость заключается в постоянном контроле и обеспечении надежности сбора и выдачи данных о доставке, что имеет первостепенное значение для эффективного обслуживания клиентов.

В рамках статьи были подробно рассмотрены механизмы функционирования системы, включая регулярные проверки и алерты, а также классификацию проверок. Такой подход позволяет оперативно выявлять и устранять проблемы, обеспечивая высокую степень стабильности работы системы.

СПИСОК ЛИТЕРАТУРЫ

1. Логистический портал Cargotime.ru [Электронный ресурс]. URL: https://cargotime.ru/ (дата обращения: 25.09.2023).
2. Лаборатория теоретических и междисциплинарных проблем информатики [Электронный ресурс]. URL: https://dscs.pro (дата 28.09.2023).
3. Абрамов М. В., Есин М. С. Агрегация сведений и оценка параметров грузовых маршрутов на основе методов машинного обучения в условиях информационного дефицита // Информационная безопасность регионов России (ИББР-2021). XII Санкт-Петербургская межрегиональная конференция. Материалы конференции. СПб.: СПОИСУ, 2021. С. 328-330.
4. Калькулятор расчета стоимости доставки на портале Cargotime.ru [Электронный ресурс] URL: https://cargotime.ru/calc/ (дата обращения: 25.09.2023).
5. Есин М. С., Корепанова А. А., Сабреков А. А. Агрегация и анализ сведений логистических компаний для построения сложного маршрута перевозки груза // Программные продукты и системы. 2023. Том 36. № 2. С. 309-319.

УДК 004.023

ПОДХОД К ОЦЕНКЕ ВЫРАЖЕННОСТИ УЯЗВИМОСТЕЙ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ СОЦИОИНЖЕНЕРНЫМ АТАКАМ

Олисеенко Валерий Дмитриевич
СПИИРАН ─ СПб ФИЦ РАН
В.О. 14-я Линия, 39, Санкт-Петербург, 199178, Россия
e-mail: vdo@dscs.pro

Аннотация. В статье представлен подход к оценке выраженности уязвимостей пользователей информационных систем к социоинженерным атакам. В основе подхода используется предположение, что выраженность уязвимости пользователей к социоинженерным атакам напрямую связано с их публикацией контента на своей странице в социальной сети. В рамках предложенного подхода планируется использование машинного обучения для связывания контента с результатами теста, который определяется оценку выраженность уязвимости к тому или иному виду социоинженерной атаки.

Ключевые слова: социоинженерные атаки; уязвимости пользователя; информационные системы; кибербезопасность.

APPROACH TO ASSESSING THE SEVERITY OF VULNERABILITIES OF INFORMATION SYSTEM USERS TO SOCIAL ENGINEERING ATTACKS

Oliseenko Valerii
SPIIRAN ─ SPb FRC RAS
39 V. I. 14th l., St. Petersburg, 199178, Russia
e-mail: vdo@dscs.pro

Abstract. The paper presents an approach to assessing the severity of vulnerabilities of users of information systems to social engineering attacks. The approach is based on the assumption that the expression of users' vulnerability to social engineering attacks is directly related to their publication of content on their social network page. The proposed approach plans to use machine learning to link the content to the results of a test that determines an estimate of vulnerability to a particular type of social engineering attack.

Keywords: social engineering attacks; user vulnerabilities; information systems; cyber security.

Введение. В работе [1] был представлен подход, моделирующий систему «критичные документы — информационная система — пользователь — злоумышленник».

В рамках данного подхода оценивалось взаимодействие «пользователь — злоумышленник» через сущности «профиль уязвимостей пользователя», «профиль компетенции злоумышленника» и «связи между видами атакующих действий и уязвимостями пользователя». В рамках сущности «профиль уязвимости пользователя» [2,3] уязвимость пользователя могла быть опосредовано оценена через оценку выраженность его психологических особенностей. Такие психологические особенности человека как доверчивость, эмоциональная неустойчивость, низкая самооценка, неуверенность в себе, недостаток критического мышления и другие могут составлять профиль уязвимости пользователя и существенно влиять на успешность социоинженерной атаки на него [4].

Однако, данный подход имеет существенные недостатки т.к. фактически необходимо проводить два исследования — первое по оценки успешности конкретного вида социоинженерной атаки на пользователей, а второй со связью такой оценки с оценкой выраженности психологических особенностей пользователей. В данной статье будет предложен пример подхода к оценке выраженности уязвимостей пользователей информационных систем к социоинженерным атакам устраняющий указанный выше недостаток.

Основная часть. Авторы исследования [5] выделяют пять потенциальных уязвимостей пользователей: информационная неосмотрительность, слабый пароль, техническая халатность, техническая неопытность, техническая безграмотность.

Для оценки представленных уязвимостей может быть использован инструментарий в виде разработки теста. Тест может строится в соответствии со следующей схемой:

- Сбор информации о пользователях (возраст, пол, город проживания, ссылка на социальную сеть);
- Разработка некоторого количества вопросов, по каждой из оцениваемой уязвимости пользователей, с возможностью выбора ответа из нескольких возможных (3–5);
- Проверка согласованности ответов с помощью контрольных вопросов;
- Проведение тестирования на выборке пользователей;
- Обработка результатов тестирования и анализ ошибок.

После получения набора эмпирических данных (результатов теста) необходимо проанализировать информацию, которую пользователь размещает на своей странице в социальной сети, ссылку на которую было получена во время прохождения теста. В качестве такой информации может выступать биографические характеристики, посты, фотографии, видео и иной контент.

Для её получения может быть использован API социальной сети (при наличии) или программные модули для создания автоматизированных систем выгрузки информации при помощи get/post запросов к страницам пользователей. Важным вопроса сбора информации является законность данного действия.

Для соблюдения законодательства Российской Федерации при проведении исследования является согласие пользователей с участием в исследовании, а также соответствие п.9 ч.1 ст.6 Федерального закона №152-ФЗ Российской Федерации и правилам социальной сети.

В общем случае задача предсказания уязвимостей пользователей к социоинженерным атакам будет относиться к задаче обучения с учителем, а именно регрессии или классификации в зависимости от выбранной шкалы для оценки результатов теста.

Таким образом, на вход модели должен поступать информация, собранная на прошлом этапе (биографические характеристики, посты, фотографии, видео и т.д.), а на выход результаты прохождения теста. Однако в явном виде собранную информацию из профилей пользователей социальной сети может быть невозможно напрямую использовать для обучения модели машинного обучения, т.к. она будет «непонятна» модели. Поэтому необходима предварительная обработка данных.

В зависимости вида исследуемых данных будет различаться процесс предварительной обработки. Так для текстовых данных (постов пользователей), например, может быть использована токенизация, удаление стоп-слов, лемматизация и другие операции, после чего все данные пропущены через языковые модели BERT и превращены в эмбеддинги могут быть использованы в моделях для дальнейшего предсказания результатах теста. Для фотографий это могут методы выделения объектов (модели YOLOv7, EfficientDet, GroundingDINO и другие) для извлечения и последующего анализа признаков.

Таким образом полный процесс создания подхода к оценке выраженности уязвимостей пользователей информационных систем социоинженерным атакам можно изобразить схемой (рис. 1).

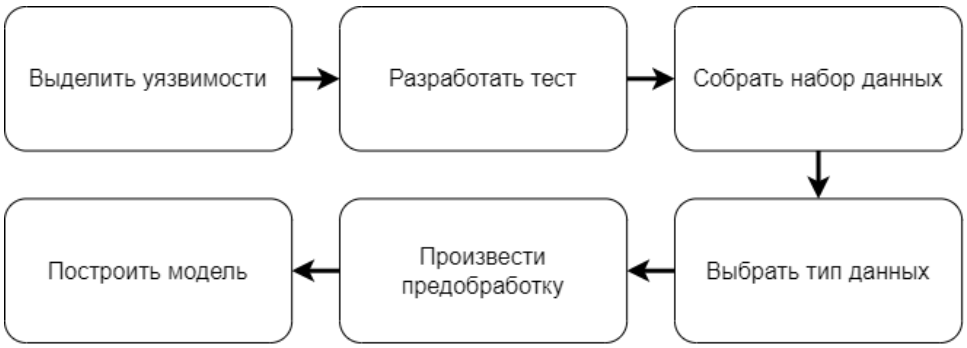


Рис. 1. Полный процесс создания подхода к оценке выраженности уязвимостей пользователей информационных систем социоинженерным атакам

Каждый блок схемы отражает этап подхода:

1.Выделить список уязвимостей пользователей к социоинженерным атакам.

2.Разработать метод (тест) для оценки выраженности уязвимостей к социоинженерным атакам.

3.Собрать набор данных в виде результата теста и информации со страниц респондентов.

4.Выбрать тип анализируемой информации со страниц респондентов.

5.Произвести предобработку набора данных, выбрать решаемую задачу (задача классификации или регрессии).

6.Построить предсказательную модель.

Стоит отметить, что наиболее сложным этапом описанного подхода является выделение уязвимостей пользователей к социоинженерным атакам, т.к. эту требует глубоких знаний в области психологии, кибербезопасности и социологии.

Заключение. Проведения исследований в области защиты от социоинженерных атак имеет высокую сложность в следствии отсутствия общепринятой системы к выделению типов и оценки их результативности. Однако общий подход к оценке выраженности уязвимостей пользователей информационных систем социоинженерным атакам может быть построен фактически для любого из типов и результатов оценки. В данной работе был представлен один из таких подходов.

Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН № FFZF-2022-0003; при финансовой поддержке гранта Президента МК 5237.2022.1.6.

СПИСОК ЛИТЕРАТУРЫ

1. Абрамов М. В., Тулупьева Т. В., Тулупьев А. Л. Социоинженерные атаки: социальные сети и оценки защищенности пользователей. СПб.: ГУАП, 2018. 266 с.
2. Возможности и опыт применения компьютерных инструментов в анализе цифровых следов студентов — пользователей социальной сети / Тулупьева Т. В. [и др.]. // Компьютерные инструменты в образовании. 2015. № 5. С. 3–13.
3. Социальнопсихологические факторы, влияющие на степень уязвимости пользователей автоматизированных информационных систем с точки зрения социоинженерных атак / Тулупьева Т. В. [и др.]. // Труды СПИИРАН. 2010. № 12. С. 200–214.
4. Тулупьева Т. В. Психологические аспекты информационной безопасности организации в контексте социоинженерных атак // Управленческое консультирование. 2022. № 2. С. 123–138.
5. Абрамов М. В., Тулупьев А. Л., Тулупьева Т. В. Психологические особенности, психические состояния пользователя и профиль его уязвимостей в контексте социоинженерных атак // Психология психических состояний. 2019. № 13. С. 312–317.

УДК 004.89

ПЕРСПЕКТИВЫ ПРОФОРИЕНТАЦИИ: ИНТЕГРАЦИЯ СОЦИОКОМПЬЮТИНГА В ПРИНЯТИЕ РЕШЕНИЙ О КАРЬЕРЕ

Хлобыстова Анастасия Олеговна
СПИИРАН ─ СПб ФИЦ РАН
14 линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: aok@dscs.pro

Аннотация. В работе рассматривается проблема принятия решений о карьере. Исследование опирается на модель профориентации RIASEC. Целью исследования является выявление взаимосвязей между результатами теста RIASEC, моделирующего профессиональные склонности пользователя, и школьными интересами. На основе множественного дисперсионного анализа (MANOVA) были выявлены статистически значимое влияние некоторых школьных предметов, выбранных как наиболее интересующие, на результаты теста Голланда.

Ключевые слова: профессиональная идентичность; профессиональная ориентация; выбор карьеры; социальные медиа; анализ данных; тест Голланда.

PERSPECTIVES ON CAREER GUIDANCE: INTEGRATING SOCIOCOMPUTING INTO CAREER DECISION-MAKING

Khlobystova Anastasiia
SPIIRAN ─ SPb FRC RAS
39 Line 14 V. I., St. Petersburg, 199178, Russia
e-mails: aok@dscs.pro

Abstract. The paper examines the problem of career decision making. The study is based on the RIASEC career guidance model. The aim of the study is to identify the relationships between the results of the RIASEC test modelling the user's occupational aptitudes and school interests. Based on multiple analysis of variance (MANOVA), statistically significant effects of some school subjects selected as the most interesting ones on the results of the Holland test were found.

Keywords: professional identity; career counseling; career choice; social media; Data Science; RIASEC.

Введение. Принятие решений о карьере является сложным процессом, который часто зависит от множества факторов. Одной из основных проблем в этой области является ограниченный доступ к высококачественным услугам по профориентации и консультированию в вопросах построения карьеры. При этом каждый шестой россиянин недоволен своей работой [1], что подчёркивает необходимость повышения поддержки в области профориентации. Современные тенденции в развитии технологий и социокомпьютинга предоставляют новые возможности для решения проблемы ограниченного доступа к высококачественным услугам профориентации [2–4]. Однако, для полноценного использования этих возможностей, необходимы дополнительные исследования.

Настоящая работа опирается на известную профориентационную модель Дж. Голланда — RIASEC, основанную на идее того, что в профессиональном контексте люди могут быть соотнесены с шести базовыми типам профессиональных интересов: R (Реалистичный), I (Интеллектуальный), A (Художественный), S (Социальный), E (Предприимчивый), C (Конвенциональный) [5]. В свою очередь определение доминирующего типа в рамках модели RIASEC может способствовать эффективному профориентационному консультированию. Целью настоящего исследования является выявление взаимосвязей между результатами теста RIASEC, моделирующего профессиональные склонности пользователя, и школьными интересами.

Методика исследования. Сбор ответов респондентов проводился через веб-приложение на базе сервиса VK Mini Apps социальной сети «ВКонтакте» «Психологические тесты» [6]. В ходе опроса респондентам было предложено пройти тест Голланда на определение их профессиональных склонностей, а также ответить на вопрос с множественным выбором: «Выберите из списка 3 предмета, которые вызывали у Вас наибольший интерес во время обучения в школе». Варианты ответов: математика, физика, химия, биология, история, иностранный язык, русский язык, география, информатика и ИКТ, литература, обществознание, изобразительное искусство/МХК. Анализируемый набор данных состоит из 3450 строк. Диаграмма распределения по полу и преобладающему профессиональному типу представлена на рис. 1, по выбранным предметам на рис. 2.

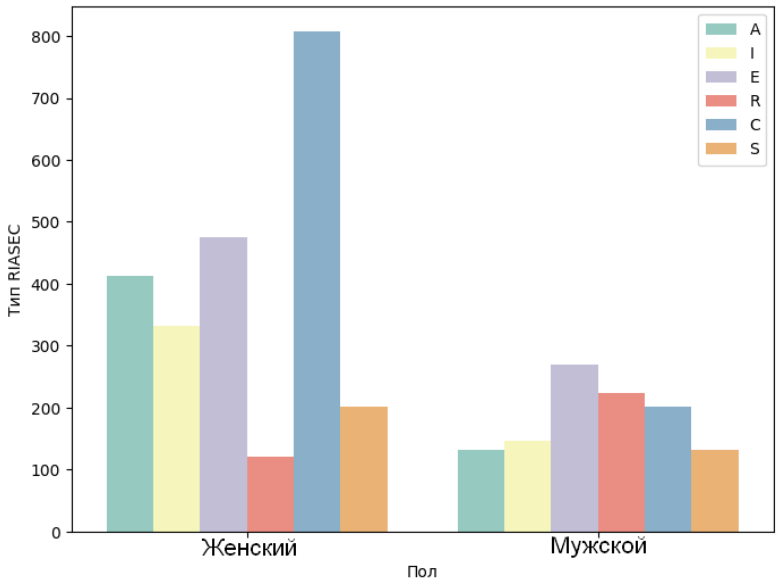


Рис.1. Распределение по преобладающему профессиональному типу.

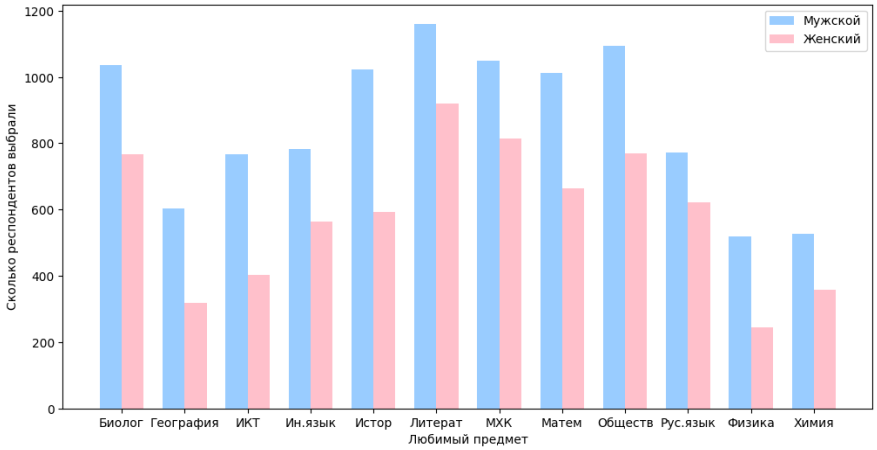


Рис.2. Распределения по предметам, вызывавшим наибольший интерес в школе.

Для анализа зависимости между предметами, которые вызывали наибольший интерес во время обучения в школе (бинарные переменные), и результатами теста Голланда, учитывая влияние переменной пола, был проведён множественный дисперсионный анализ (MANOVA). Результаты расчёта представлены в таблице 1, где value означает оценку влияния каждого из предметов на значение результатов теста Голланда, а Pr обозначает уровень статистической значимости.

Таблица 1

Результаты множественного дисперсионного анализа (MANOVA)

	R	I	A	S	E	C
Математика	Value: 0.0010 Pr: 0.1744	Value: 0.0016 Pr: 0.0658	Value: 0.0019 Pr: 0.0414	Value: 0.0021 Pr: 0.0261	Value: 0.0012 Pr: 0.1174	Value: 0.0052 Pr: 0.0001
Физика	Value: 0.0065 Pr: 0	Value: 0.0056 Pr: 0.0001	Value: 0.0055 Pr: 0.0001	Value: 0.0054 Pr: 0.0001	Value: 0.0055 Pr: 0.0001	Value: 0.0084 Pr: 0.0000
Химия	Value: 0.009 Pr: 0.2192	Value: 0.009 Pr: 0.2228	Value: 0.0014 Pr: 0.0939	Value: 0.0009 Pr: 0.2204	Value: 0.0014 Pr: 0.0831	Value: 0.0034 Pr: 0.0028
Биология	Value: 0.0004 Pr: 0.4649	Value: 0.0004 Pr: 0.4869	Value: 0.0009 Pr: 0.2118	Value: 0.0004 Pr: 0.5133	Value: 0.0005 Pr: 0.4434	Value: 0.0020 Pr: 0.0333
История	Value: 0.0039 Pr: 0.0012	Value: 0.0045 Pr: 0.0004	Value: 0.0050 Pr: 0.0002	Value: 0.0039 Pr: 0.0012	Value: 0.0049 Pr: 0.0002	Value: 0.0051 Pr: 0.0002
Иностранный язык	Value: 0.0006 Pr: 0.3651	Value: 0.0025 Pr: 0.0208	Value: 0.0020 Pr: 0.0304	Value: 0.0006 Pr: 0.3589	Value: 0.0013 Pr: 0.1097	Value: 0.0009 Pr: 0.2269
Русский язык	Value: 0.0002 Pr: 0.7357	Value: 0.0023 Pr: 0.0208	Value: 0.0014 Pr: 0.0836	Value: 0.0004 Pr: 0.4692	Value: 0.0013 Pr: 0.1028	Value: 0.0014 Pr: 0.0877
География	Value: 0.0041 Pr: 0.0008	Value: 0.005 Pr: 0.0002	Value: 0.0043 Pr: 0.0006	Value: 0.0044 Pr: 0.0005	Value: 0.0051 Pr: 0.0002	Value: 0.0048 Pr: 0.0003
Информатика и ИКТ	Value: 0.0056 Pr: 0.0001	Value: 0.0056 Pr: 0.0001	Value: 0.0052 Pr: 0.0001	Value: 0.0060 Pr: 0.0000	Value: 0.0052 Pr: 0.0001	Value: 0.0070 Pr: 0.0000
Литература	Value: 0.0001 Pr: 0.8073	Value: 0.0005 Pr: 0.4086	Value: 0.0006 Pr: 0.3341	Value: 0.0001 Pr: 0.8203	Value: 0.0003 Pr: 0.5954	Value: 0.0001 Pr: 0.8335
Обществознание	Value: 0.0008 Pr: 0.2325	Value: 0.0025 Pr: 0.0127	Value: 0.0033 Pr: 0.0035	Value: 0.0008 Pr: 0.2606	Value: 0.0033 Pr: 0.0032	Value: 0.0029 Pr: 0.0068
Изобразительное искусство/МХК	Value: 0.0005 Pr: 0.4196	Value: 0.0013 Pr: 0.1104	Value: 0.0002 Pr: 0.7475	Value: 0.0001 Pr: 0.8572	Value: 0.0001 Pr: 0.8494	Value: 0.0008 Pr: 0.2502

По результатам проведённого анализа можно сделать вывод о том, что существует статистически значимое влияние некоторых предикторов (предметов, которые вызывали наибольший интерес во время обучения в школе) на зависимую переменную (результат теста Голланда). А именно, статистически значимый результат показали такие предметы как физика, история, география, информатика и ИКТ.

Заключение. Таким образом, в ходе исследования были выделены некоторые взаимосвязи между результатами теста RIASEC, характеризующего профессиональные склонности личности, и школьными интересами. В свою очередь, информация о школьных интересах может содержаться в цифровых следах пользователя в онлайн социальных сетях, например, таких как тематики сообществ и публикуемые посты, и предсказана при помощи методов анализа данных и машинного обучения. Полученные результаты могут послужить основой для дальнейших исследований в области психологии и профессиональной ориентации, направленных на более глубокое понимание взаимосвязей между психологическими особенностями, интересами человека и его цифровой активностью.

Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН СПИИРАН № FFZF-2022-0003.

СПИСОК ЛИТЕРАТУРЫ

1. Опрос показал, сколько россиян недовольны своей работой [Электронный ресурс]. URL: https://ria.ru/20231010/rabota-1901650112.html (дата обращения:10.10.2023).
2. Dağıstanlı Ö., Erbay H., Kör H., YurttakalA. H. Reflection of people's professions on social media platforms //Neural Computing and Applications. 2022. Pp. 1–12. doi: 10.1007/s00521-022-07987-8.
3. Kern M .L., McCarthy P. X., Chakrabarty D., Rizoiu M. A Social media-predicted personality traits and values can help match people to their ideal jobs //Proceedings of the National Academy of Sciences. 2019. Vol. 116. №. 52. Pp. 26459-26464. DOI: 10.1073/pnas.1917942116.
4. José-García A., Sneyd A., Melro A., Ollagnier A., Tarling G., Zhang H., Stevenson M., Everson R., Arthur R. C3-IoC: A career guidance system for assessing student skills using machine learning and network visualisation //International Journal of Artificial Intelligence in Education. 2022. Pp. 1–28. doi: 10.1007/s40593-022-00317-y.
5. Holland J. L. Explorations of a theory of vocational choice and achievement: II. A four-year prediction study // Psychological reports, 1963. V 2. №. 2. Pp. 547–594.
6. Приложение «Психологические тесты» [Электронный ресурс]. URL: https://vk.com/app7794698_203437876 (дата обращения: 10.10. 2023).

УДК 004.8

РАЗРАБОТКА ПРИЛОЖЕНИЯ ВКОНТАКТЕ ДЛЯ АНАЛИЗА ТЕМАТИК СООБЩЕСТВ: ТРЕБОВАНИЯ К ФУНКЦИОНАЛЬНОСТИ И БЕЗОПАСНОСТИ

Чекалёв Артём Алексеевич[2], Хлобыстова Анастасия Олеговна[1,2]
[1] СПИИРАН ─ СПб ФИЦ РАН
14 линия В. О., 39, Санкт-Петербург, 199178, Россия
[2] Санкт-Петербургский государственный университет
Университетская наб., 7, Санкт-Петербург, 199034, Россия
e-mails: aok@dscs.pro, st087200@student.spbu.ru

Аннотация. В статье рассмотрена задача создания веб-приложения на платформе VK Mini Apps для предоставления пользователям информации о тематиках подписок и склонности к определенному профессиональному типу личности. Приложение разработано с использованием Python и интегрировано с VK API для выгрузки и обработки тематик групп. В статье приводится описание реализации серверной (backend) и клиентской (frontend) частей. Рассмотрены аспекты безопасности приложения.

Ключевые слова: социальные сети; ВКонтакте; веб-приложение; анализ социальных сетей; анализ подписок; тематики сообществ.

DEVELOPING AN APPLICATION WITHIN VKONTAKTE FOR ANALYSING COMMUNITY TOPICS: FUNCTIONALITY AND SECURITY REQUIREMENTS

Chekalev Artem [1], Khlobystova Anastasiia [1,2]
[1] SPIIRAN ─ SPb FRC RAS
39 Line 14 V. I., St. Petersburg, 199178, Russia
[2] Saint-Petersburg State University,
7 Universitetsky Av, St. Petersburg, Russia
e-mails: aok@dscs.pro, st087200@student.spbu.ru

Abstract. The article discusses the task of creating a web application on the VK Mini Apps platform to provide users with information about the activities of subscriptions and inclination towards a certain professional personality type. The application is developed using Python and integrated with VK API for uploading and processing group topics. The article describes the implementation of the server (backend) and client (frontend) parts. The security aspects of the application are considered.

Keywords: social network; VKontakte; web-application; social network analysis; analyzing groups; group themes.

Введение. Социальные сети становятся все более популярными и значимыми в жизни современного человека. Они предоставляют возможность поддерживать связь с близкими и друзьями, делиться своими мыслями, фотографиями и видео. В России среди онлайн социальных сетей особое место занимает «ВКонтакте», которую ежемесячно посещают более 79 миллионов пользователей [1], что в свою очередь делает её самой популярной соцсетью в стране [2]. Так, согласно официальным данным «ВКонтакте» за первый квартал 2023 года [3], средняя дневная аудитория достигла 53,6 млн посетителей. Привлекательность этой социальной сети заключается в ее доступности и удобстве использования. При этом объемы публикуемого контента в этой социальной сети достигают 6,3 миллиарда единиц в год [4].

Одним из популярных сервисов «ВКонтакте» является VK Mini Apps, содержащий огромное количество приложений, каждое из которых предоставляет пользователю различные возможности. Как сообщается на официальном сайте «ВКонтакте» [5], на январь 2023 года на платформе зарегистрировано 75000 мини-приложений, а число людей, которые пользовались ими, составило 45 миллионов в месяц. Одним из главных

преимуществ VK Mini Apps является простота использования. Пользователи могут получать доступ к мини-приложениям прямо из социальной сети, не тратя время на установку и загрузку отдельных приложений на свои устройства. В данном контексте актуальна задача разработки новых приложений внутри VK Mini Apps, способных не только предоставлять игровой контент, но и давать возможность узнать нестандартную информацию о себе, построенную на ассоциированном с пользователем контенте. В качестве такой системы предлагается разработка приложения на платформе VK Mini Apps, которое будет собирать и обрабатывать информацию о тематиках групп пользователей, а также на их основе выдавать предполагаемый профессиональный тип личности, к которому человек наиболее склонен.

Описание реализации. Процесс разработки приложения можно поделить на две части: серверную (backend) и клиентскую (frontend) части. Опишем каждый из этих этапов.

Реализация серверной части (backend) приложения была выполнена с использованием языка программирования Python, а также интеграции с VK API для получения информации о тематиках групп пользователей. Выгрузить и вывести статистику тематик групп можно в двух сценариях:

– на основе подписок самого пользователя, который использует приложение;

– на основе подписок любого другого пользователя, id которого будет введено в специальную текстовую форму.

Опишем, как работает приложение в каждом из вариантов.

1.Выгрузка тематик групп пользователя.

1.1.Аутентификация и получение токена

При нажатии на кнопку «Анализ моей страницы», пользователю предлагается открыть доступ к просмотру своих сообществ. Это необходимо для того, чтобы приложение могло собирать и выводить тематики групп. После этого, приложение проходит процесс аутентификации и получает токен пользователя, необходимый для выполнения запросов к VK API.

1.2.Запрос тематик групп

С использованием метода groups.get() VK API получает список групп пользователя и их тематик. По каждой тематике подсчитывается количество групп пользователя с такой тематикой. Полученные данные записываются в двумерный массив, элементами которого являются массивы вида [название тематики группы, количество групп с этой тематикой].

1.3.Обработка и анализ

Массив с тематиками групп с помощью API направляется в программу Python, в которой при помощи библиотеки gensim [6] методами искусственного интеллекта обрабатывается полученная информация. А именно рассчитывается семантическая близость тематик групп и ключевых слов профессиональных типов, доступных в базе данных по профессиям O*NET [7]. Результатом анализа является профессиональный тип личности, к которому наиболее склонен пользователь.

2.Выгрузка тематик групп пользователя.

2.1Аутентификация и получение токена

Если же пользователю нужно проанализировать страницу любого другого пользователя «ВКонтакте», ему необходимо ввести его id в форму для текста. Стоит отметить, что в общем случае id — это некоторое натуральное число, поэтому важной является обработка ситуации, когда в поле вводится что-то кроме цифры. В случае, если введены только цифры, текст из формы передается далее и обрабатывается методами VK Api; иначе, приложение сообщает пользователю, что данный id некорректен.

Запрос тематик групп. Список групп пользователя запрашивается также при помощи метода groups.get(). Однако в данном случае важен тип профиля другого пользователя. Если профиль пользователя является «открытым» для токена пользователя, который ввёл id страницы данного, то приложение произведёт подсчёт количества групп пользователя с той или иной тематиками; иначе приложение сообщит, что профиль недоступен для выгрузки групп, при этом указав причину: профиль закрыт, заблокирован или удалён.

Реализация клиентской части (frontend) включает создание удобного и интуитивно понятного интерфейса для взаимодействия с пользователями. Говоря о внешней составляющей приложения, все элементы реализованы с использованием VK UI [8]. Это библиотека react-компонентов, с помощью которой удобно создавать приложения на платформе VK Mini Apps.

Для наглядности отображения результатов приложение не только выводит список тематик групп пользователя, но и строит столбчатую диаграмму при помощи библиотеки chart.js, в которой отображены 3 наиболее часто встречаемые у пользователя тематики групп. На рис. 1 изображен интерфейс разработанного приложения.

Важным аспектом при разработке мини-приложения является соблюдение политик безопасности и конфиденциальности. В том числе, использование эффективных методов проверки подлинности данных, обеспечение безопасного хранения и использования ключей доступа, предотвращение SQL-инъекций и XSS-уязвимостей. Также важно обеспечивать надежную защиту приложения от возможных атак, таких как CSRF-атаки.

Для обеспечения необходимого уровня безопасности разработанного приложения в дальнейшем также планируется изучить источники [9−11].

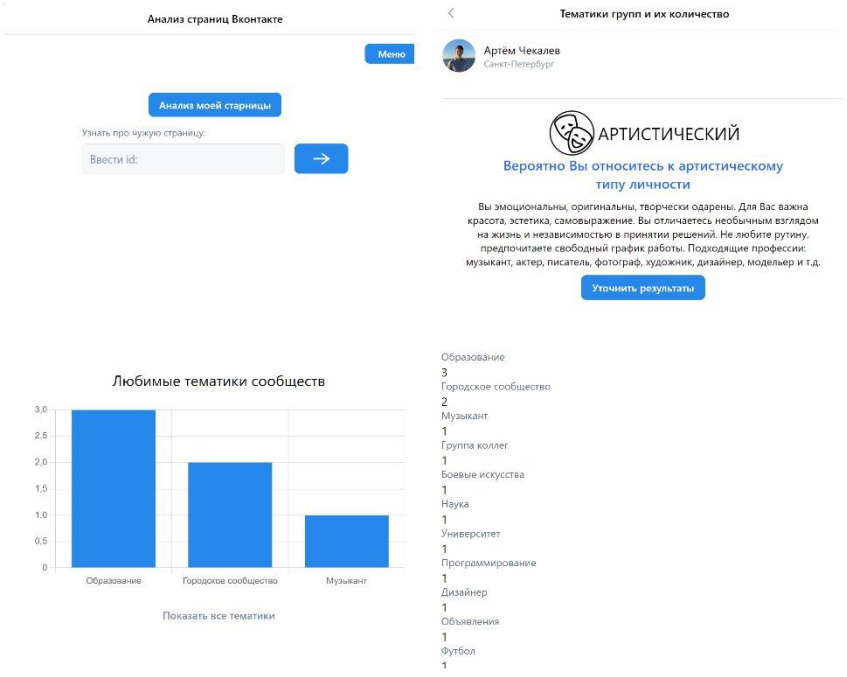


Рис. 1. Интерфейс приложения «Анализ страниц ВКонтакте»

Заключение. Таким образом, в статье была рассмотрена актуальная задача разработки системы, способной анализировать неявные предпочтения пользователей социальной сети. В качестве способа ее решения было разработано приложение VK Mini Apps, которое собирает информацию о тематиках групп пользователей и возвращает их в виде списка и диаграммы. Помимо этого, реализована возможность сопоставления тематикам групп профессионального типа личности, к которому наиболее склонен пользователь. В качестве профессиональных типов были использованы характеристики из теста Голланда. В дальнейшем планируется добавить в приложение дополнительную функциональность, а именно возможность просматривать пересечение тематик групп пользователя с тематиками групп его друзей. Также планируется выложить приложение в каталог сервисов ВКонтакте.

Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН № FFZF-2022-0003.

СПИСОК ЛИТЕРАТУРЫ

1. Статистика ВКонтакте в 2023 году [Электронный ресурс]. URL: https://inclient.ru/vk-stats/ (дата обращения: 08.10.2023).
2. Социальные сети в первом полугодии 2023 [Электронный ресурс]. URL: https://mediascope.net/news/1681112/ (дата обращения: 08.10.2023).
3. Результаты VK за первый квартал 2023 года [Электронный ресурс]. URL: https://vk.company/ru/investors/info/11481/ (дата обращения: 08.10.2023).
4. ВКонтакте подвела итоги контентной платформы [Электронный ресурс]. URL: https://vk.com/press/content-2022 (дата обращения: 08.10.2023).
5. Официальный сайт ВКонтакте [Электронный ресурс]. URL: https://vk.com/mini-apps (дата обращения 08.10.2023).
6. Gensim 4.3.2 [Электронный ресурс]. URL: https://pypi.org/project/gensim/ (дата обращения 08.10.2023).
7. O*NET [Электронный ресурс]. URL: https://www.onetonline.org/ (дата обращения 08.10.2023).
8. Библиотека VK UI [Электронный ресурс]. URL: https://github.com/VKCOM/VKUI (дата обращения 08.10.2023).
9. Критерии модерации [Электронный ресурс]. https://dev.vk.com/ru/mini-apps/catalog/criteria (дата обращения 08.10.2023).
10. Иконников М. А., Карманов И. Н. Меры и требования к защищенным веб-приложениям // Интерэкспо Гео-Сибирь. 2019. № 2. С. 13−19.
11. Хоффман Э. Безопасность веб-приложений. СПб., Питер, 2021. С. 221−251.

КИБЕРФИЗИЧЕСКИЕ И ГЕОИНФОРМАЦИОННЫЕ СИСТЕМЫ

УДК 004.89

ПРОБЛЕМА БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ЦИФРОВЫХ ДВОЙНИКОВ В МЕДИЦИНЕ И БИОМЕТРИИ И МЕТОДЫ ИХ ЗАЩИТЫ ОТ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Жумажанова Самал Сагидулловна, Ложников Павел Сергеевич, Зубович Никита Васильевич, Красотина Арина Игоревна
Омский государственный технический университет
пр. Мира, 11, Омск, 644050, Россия
e-mails: samal_shumashanova@mail.ru, lozhnikov@mail.ru, ankerov.n@mail.ru, arinakrasotina@mail.ru

Аннотация. В последнее время, в связи с ростом цифровых технологий, объединенных под общим названием «Индустрия 4.0», искусственный интеллект, машинное обучение, технологии обработки больших массивов данных, облачные технологии и элементы Интернета вещей, цифровые двойники, становятся мощной движущей силой. При этом концепция цифровых двойников является одной из основных технологий, включающей в себя как физические, так и виртуальные ресурсы, систему обслуживания, огромные объемы данных, методы и алгоритмы их обработки. Поэтому растущий интерес к цифровым двойникам ведет за собой также повышение внимания экспертов в области информационной безопасности, соответственно, вопросы кибербезопасности здесь стоят не на последнем месте. Цифровые двойники могут выступать в качестве потенциального источника утечки данных, а злоумышленники в свою очередь могут использовать обширные знания о физических процессах и устройствах, доступных через цифровые двойники. Настоящая работа посвящена анализу основных рисков информационной безопасности, направленных на цифровые двойники, используемые в биометрии и медицине.

Ключевые слова: цифровой двойник; анализ данных; искусственный интеллект; защита персональных данных; риски информационной безопасности; digital transformation.

THE PROBLEM OF INFORMATION SECURITY WHEN USING DIGITAL TWINS IN MEDICINE AND BIOMETRICS AND METHODS FOR THEIR PROTECTION FROM INFORMATION SECURITY THREATS

Zhumazhanova Samal, Lozhnikov Pavel, Zubovich Nikita, Krasotina Arina
Omsk State Technical University, 11 Mira Av, Omsk, 644050, Russia
e-mail: samal_shumashanova@mail.ru

Abstract. Recently, due to the growth of digital technologies, united under the general name «Industry 4.0», artificial intelligence, machine learning, technologies for processing large amounts of data, cloud technologies and elements of the Internet of things, digital twins, are becoming a powerful driving force. At the same time, the concept of digital twins is one of the main technologies, which includes both physical and virtual resources, a service system, huge volumes of data, methods and algorithms for processing them. Therefore, the growing interest in digital twins is also leading to an increase in the attention of experts in the field of information security; accordingly, cybersecurity issues are not in last place here. Digital twins can act as a potential source of data leakage, and attackers, in turn, can exploit the extensive knowledge of physical processes and devices available through digital twins. This work is devoted to the analysis of the main information security risks aimed at digital twins used in biometrics and medicine.

Keywords: digital twin; data analysis; artificial intelligence; personal data protection; information security risks; digital transformation.

Введение. Цифровой двойник (ЦД) — это виртуальная модель физического объекта, имеющая двунаправленный обмен данными между физическим объектом и его соответствующим двойником. ЦД имеют большой потенциал и позволяют открывать новые знания, а также проводить безопасные эксперименты с участием человека.

Согласно аналитическому отчету Spherical Insights & Consulting [1] в 2022 году рынок ЦД был оценен в 12,6 миллиарда долларов США, а к 2032 году может достичь 140,76 миллиарда долларов США. В свою очередь

компания MARKETSANDMARKETS [2] оценила объем рынка ЦД в 2023 году в 10,1 миллиарда долларов США, при этом прогнозируя ежегодный прирост рынка в 61,3% до 110 миллиарда долларов США в 2028 году.

Этот рост популярности ЦД можно обосновать тем, что они широко применяются в военной, авиационной, биомедицинской и других отраслях, в каждую из которых они вносят свои преимущества, например, позволяют разработчикам тестировать характеристики устройства, его использование и вносить своевременные изменения перед запуском устройства в производство. Это повышает безопасность конечного продукта. Однако, с вовлечением ЦД также возросли риски совершения кибератак и несоответствия ЦД принятым международным и локальным нормативным требованиям по защите информации.

Среди рисков наиболее опасными также могут быть намеренные или непреднамеренные искажения ЦД или объекта, ЦД которого разрабатывают, и это является основной причиной того, почему рынок данной технологии сдерживается большинством владельцев компаний, заинтересованных в ЦД. К тому же не все производители и пользователи могут доверять ЦД, поскольку не для всех них есть доказательства точности и степени близости ЦД его физическому аналогу.

При создании ЦД человека в биометрии или медицине необходимо обратить особое внимание на использованные сведения, которые представляют собой персональные данные, как правило, это категории специальных и биометрических ПДн. При широком внедрении ЦД обеспечение конфиденциальности таких данных может стать большой проблемой, которую необходимо решать врачам и медперсоналу, а также специалистам по информационной безопасности.

В настоящей работе проведен анализ рисков применения ЦД с точки зрения информационной безопасности и сделаны выводы о возможных методах противодействия данным рискам.

Технологии создания цифровых двойников. ЦД бесспорно являются удобным инструментов для прогнозирования разных ситуаций, которые могут возникнуть с реальным объектом, но перед тем как интегрировать двойника в систему для использования, его необходимо создать. Существует несколько подходов к созданию цифровых близнецов.

В основном выделяют следующие подходы:

- функционально-ориентированный;
- предметно-ориентированный;
- процессно-ориентированный;
- отраслевой.

Функционально-ориентированный подход рассматривает ЦД как набор функций, преобразующий поступающий поток информации в выходной поток. Процесс преобразования информации потребляет определенные ресурсы. Принципиальное отличие функционально-ориентированного от других подходов заключается в четком отделении методов обработки данных от самих данных.

Предметно-ориентированный – это подход, который привносит большую ценность и эффективность в двойники. Этот подход заключается в том, чтобы сосредоточиться на анализе и моделировании предметных областей, для которых создаются ЦД.

Процессно-ориентированный подход — это подход, который рассматривает данные, лежащие в основе ЦД как неизменные, и сосредотачивает внимание на процессах и преобразованиях, происходящих с этими данными.

Отраслевой подход подразумевает сосредоточение усилий по разработке ЦД на конкретной отрасли, а иногда - на конкретном предприятии, или, в случае персонализированной медицины - на конкретном человеке. ЦД, созданные с использованием отраслевого подхода, получаются более качественными, и реже дают сбои, однако их создание является более трудоемким, чем при использовании других подходов.

В зависимости от выбранного подхода можно использовать разные программные комплексы, приведенные в таблице 1.

Таблица 1

Программное обеспечение для реализации подходов к созданию цифровых двойников [3]

Подход	Программное обеспечение
Функционально-ориентированный	Autodesk Digital Twin, Bosch IoT Suite, AnyLogic, ANSYS Twin Builder и др
Предметно-ориентированный	SAP Leonardo Internet of Things, Oracle IoT Production Monitoring Cloud и др

Процессно-ориентированный	Cohesion, iTwins и др.
Отраслевой	Cerebra, Flutura Decision Science, Tekvel Park и др

ЦД используются в широком спектре отраслей, включая производство, энергетику, здравоохранение и городское планирование. Технологии на базе ЦД предлагают решения для прогнозирования и оптимизации работы объектов в режиме реального времени.

Вот некоторые примеры технологий на базе ЦД:

1. Индустрия 4.0: ЦД позволяют создавать виртуальные модели производственных предприятий, оптимизируя процессы и предсказывая возможные сбои. Это улучшает эффективность и гибкость в производстве [4, 5].

2. Энергетика: ЦД в энергетике используются для мониторинга и оптимизации систем энергоснабжения, позволяя операторам принимать грамотные решения в режиме реального времени для повышения энергоэффективности и надежности [6].

3. Здравоохранение: В ЦД здравоохранения объединяются данные пациентов, информация об оборудовании и окружающей среде, что позволяет создать модели для прогнозирования результатов лечения и оптимизации бизнес-процессов в области здравоохранения [7].

4. Городское планирование: ЦД городских систем собирают данные о транспорте, среде, зданиях и людях для предоставления городским планировщикам возможности моделирования и принятия решений на основе данных [8].

Риски и уязвимости, связанные с цифровыми двойниками. Так как ЦД являются носителями информации о физическом объекте, их использование тесно связано с множеством рисков информационной безопасности. К таким рискам относится нарушение целостности, конфиденциальности и доступности данных, на основе которых создан ЦД.

ЦД могут выступать в качестве потенциального источника утечки данных. Злоумышленники могут использовать знания о физических процессах и устройствах, доступных через ЦД, используя двухэтапную стратегию: использовать ключевой источник входных данных, а именно, ЦД, в небезопасном/уязвимом состоянии, а затем с помощью этого состояния скрытно манипулировать поведением основной физической системы или объекта. В случае персонализированной медицины любой из этих рисков может повести за собой ряд критических ошибок для медицинского персонала и серьёзных последствий для пациентов.

Более того, если случится утечка биометрических данных, использованных для создания двойника, возникнет угроза компрометации человека в любой информационной системе, где эти данные используются для идентификации личности. Таким образом, необходимым является защита ЦД от любых рисков и угроз информационной безопасности. Для обеспечения качественной защиты такого рода, необходимо чётко представлять, какие риски связаны с использованием двойников и как с ними наиболее эффективно бороться.

Наиболее серьёзные риски использования ЦД, а также рекомендованные методы противодействия им приведены в таблице 2.

Таблица 2

Риски информационной безопасности при использовании цифровых двойников

Риски информационной безопасности при использовании ЦД	Описание рисков информационной безопасности	Методы борьбы с рисками использования ЦД
Риск компрометации данных ЦД	Низкая безопасность сетевых соединений и протоколов передачи данных увеличивает риск уязвимости данных ЦД при передаче по сети. Недостаточная защита соединений или протоколов позволяет злоумышленнику перехватить, изменить или подменить данные, внедрив их в скомпрометированный ЦД. Это может привести к несанкционированному доступу или изменению информации, что может нанести серьезный ущерб [9]. Отсутствие шифрования данных. Если данные ЦД передаются или хранятся без шифрования,	Защита от несанкционированного доступа путем реализации механизмов аутентификации и авторизации. Шифрование данных ЦД для обеспечения их конфиденциальности. Использование цифровых подписей и цифровых сертификатов для обеспечения целостности данных [21].

	злоумышленник может получить доступ к ним и использовать конфиденциальную информацию. Шифрование предоставляет дополнительный уровень защиты и предотвращает несанкционированный доступ [10]. Недостаточная аутентификация пользователей и учетных записей. Слабая аутентификация пользователей и учетных записей в системе ЦД облегчает несанкционированный доступ и потенциальное вмешательство злоумышленников в данные.	
Риск внедрения злоумышленником вредоносного кода в компьютерные системы	Существует несколько сценариев внедрения: Использование слабых протоколов и алгоритмов безопасности. Если компьютерная система использует устаревшие или слабые протоколы и алгоритмы безопасности, злоумышленники могут внедрять вредоносный код путем перехвата и изменения данных, передаваемых по незащищенным каналам связи [11]. Использование уязвимостей программного обеспечения. Иногда в ПО обнаруживаются уязвимости, которые злоумышленники могут использовать для вторжения и установки вредоносного кода, например, уязвимость веб-сервера дает возможность получить несанкционированный доступ к системе [12]. Внедрение вредоносного кода через взаимодействие с другими системами. Высокая степень взаимодействия компьютерных систем увеличивает риски внедрения вредоносного кода [13].	Регулярное обновление программного обеспечения с целью устранения уязвимостей и обнаружения вредоносных программ. Использование антивирусного и антишпионского программного обеспечения для обнаружения и предотвращения внедрения вредоносного кода [21, 22].
Риск нежелательного доступа к ЦД.	Утечка данных ЦД через слабое управление правами доступа. ЦД может быть неправильно защищен или доступ к нему может быть предоставлен несанкционированным пользователям из-за недостаточно строгих правил доступа, что позволяет злоумышленникам получить нежелательную информацию [14]. Физический доступ к цифровому двойнику и его компонентам. Например, кто-то может получить физический доступ к серверу или устройству, на котором хранится или работает ЦД, и внести изменения или кражу данных [15]. Злоупотребление привилегиями доступа. Если у пользователя повышенные привилегии, он может незаконно получить доступ к защищенной информации или системе. Злоумышленники могут злоупотреблять таким доступом для кражи данных, изменения информации или нанесения ущерба системе [16].	Реализация строгих механизмов аутентификации и авторизации для предотвращения несанкционированного доступа к цифровым двойникам. Использование многоуровневых архитектур безопасности с ролевыми системами управления доступом [21, 22].
Риск подделки и злоупотребления ЦД	Создание фальшивых ЦД с целью замены оригинала. Подделка ЦД может привести к несанкционированному доступу к личным данным или финансам. Например, злоумышленник может использовать поддельный ЦД для получения доступа к банковскому аккаунту и махинации с финансами [17]. Злоупотребление функциями ЦД в криминальных целях. Подделка ЦД может привести к	Использование цифровых подписей и цифровых сертификатов для обеспечения подлинности и целостности ЦД. Регулярная проверка ЦД на предмет подделки и изменений [21, 22].

	несанкционированному доступу к информации, финансам или ресурсам, что может быть использовано злоумышленниками для кражи данных, нарушения целостности информации или совершения других преступных действий [18]. Использование ЦД для манипуляции с финансовыми данными. Злоумышленники могут использовать ЦД для подмены финансовых данных или изменения параметров транзакций. Это может привести к финансовым потерям клиентов, компаний или государственных организаций. Кроме того, использование ЦД для манипуляции с финансовыми данными может создать уязвимости в системах защиты данных и открыть дверь для дальнейших атак или злоупотреблений [19].	
Риск несоответствия ЦД оригиналу	Созданный ЦД может содержать ошибки, неточности или быть измененным по сравнению с оригинальными данными или системой. Это может привести к неправильным решениям, потере данных или нарушению целостности информации.	Разработка и внедрение систем синхронизации между ЦД и оригиналом.
Риски человеческого фактора при работе с ЦД	Ошибки внесения данных: Человеческий фактор может привести к неправильному внесению данных в ЦД, что может привести к неточным результатам и ошибочным решениям. Неправильное понимание и интерпретация данных: Люди могут неправильно понимать и интерпретировать данные, что может привести к неправильным выводам и решениям. Несоответствие между реальным миром и ЦД: Люди могут сделать неправильные или неточные моделирования и представления реального мира при создании ЦД, что может привести к ошибочным результатам и прогнозам. Недостаточная безопасность данных: Люди могут быть небрежными или недостаточно осторожными при обработке и хранении данных ЦД, что может привести к утечке и компрометации чувствительных данных. Непредсказуемость человеческого поведения: Человеческий фактор всегда неизвестен и непредсказуем, люди могут принимать неожиданные решения или вести себя непредсказуемо, что может негативно сказаться на работе с ЦД [20].	Проведение обучения и тренировок персонала для повышения осведомленности о безопасности и правильном использовании ЦД. Разработка и реализация строгой политики безопасности, включая установление правил и ограничений использования ЦД [22].

Резюмируя данные таблицы – несмотря на все преимущества ЦД, они имеют свои риски. Для защиты от рисков можно использовать надежные механизмы аутентификации и авторизации, шифрование данных и использование цифровых подписей. Регулярные обновления программного обеспечения и использование антивирусного ПО помогут предотвратить вредоносный код. Многоуровневые архитектуры безопасности и регулярная проверка на подделку также являются важными мерами. Образование персонала и разработка строгой политики безопасности также играют важную роль. Все эти меры помогут организациям использовать ЦД безопасно и надежно.

Заключение. ЦД представляют собой важную и перспективную технологию, которая имеет большой потенциал в различных отраслях. Они позволяют проводить безопасные эксперименты с участием человека и способствуют повышению безопасности конечных продуктов.

В данной научной статье проведен анализ рисков использования ЦД в медицине и биометрии с точки зрения информационной безопасности. Были выявлены основные угрозы информационной безопасности, связанные с применением ЦД и предложены методы защиты от них.

В свете проведенного анализа можно сделать вывод о необходимости дальнейшего исследования и разработки мер безопасности, которые бы позволили максимально обезопасить использование ЦД и защитить персональные данные, особенно в чувствительных отраслях, таких как персонализированная медицина.

Данные, представленные в статье, могут быть использованы для создания эффективных систем защиты и снижения рисков, связанных с использованием ЦД.

В результате ЦД смогут полностью раскрыть свой потенциал и стать неотъемлемым инструментом в различных областях.

СПИСОК ЛИТЕРАТУРЫ

1. Global Digital Twin Market Size To Exceed $140.76 Billion By 2032 - CAGR 27.29% | Spherical Insights [Электронный ресурс]. - Режим доступа: https://www.globenewswire.com/en/news-release/2023/04/21/2651928/0/en/Global-Digital-Twin-Market-Size-To-Exceed-140-76-Billion-By-2032-CAGR-27-29-Spherical-Insights.html. - (Дата обращения: 11.09.23г.).
2. MarketsandMarkets. Digital Twin Market [Электронный ресурс]. - Режим доступа: https://www.marketsandmarkets.com/Market-Reports/digital-twin-market-225269522.html. - (Дата обращения: 11.09.23г.).
3. CyberLeninka. (2022). Обзор программных продуктов разработки цифровых двойников [Электронный ресурс- Режим доступа: https://cyberleninka.ru/article/n/obzor-programmnyh-produktov-razrabotki-tsifrovyh-dvoynikov - (Дата обращения: 11.09.23г.).
4. Digital Twin Technology and Its Role in Industry 4.0 [Электронный ресурс]. - Режим доступа: https://www.researchgate.net/publication/316531103_Digital_Twin_Technology_and_Its_Role_in_Industry_40 (Дата обращения: 25.09.23г.)
5. Digital Twin Technologies: Definitions, Applications and Challenges [Электронный ресурс]. - Режим доступа: https://www.mdpi.com/2079-9292/9/3/498 (Доступ: [25.09.23г.]).
6. Digital Twin Technology in Energy Sector: A Comprehensive Overview [Электронный ресурс]. - Режим доступа: https://www.sciencedirect.com/science/article/pii/S2352340919310423 (Дата обращения: 25.09.23г.).
7. Digital Twin in Healthcare: A Survey [Электронный ресурс]. - Режим доступа: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6988490/ (Дата обращения: 25.09.23г.).
8. Digital Twins for Smart Cities: A Comprehensive Survey [Электронный ресурс]. - Режим доступа: https://www.researchgate.net/publication/321961716_Digital_Twins_for_Smart_Cities_A_Comprehensive_Survey (Дата обращения: 25.09.23г.)
9. Smith, J. (2017). Security Issues in Digital Twins of Cyber-Physical Systems. In Digital Twin Technologies and Smart Cities (pp. 17-30). Springer, Singapore.
10. Kowalski, M. R., & Toinin, P. (2018). Digital Twins: An Overview. In Proceedings of the International Workshop on Semantic Big Data (pp. 1-8). ACM.
11. Dey, N., Ashour, A. S., & Parvathi, K. R. (2019). Internet of Things, big data and analytics: the holy trinity in the industry 4.0 scenario. Journal of Ambient Intelligence and Humanized Computing, 10(6), pp. 2149-2167.
12. Munir, R., Ahmed, T., & Morrow, P. J. (2015). Security architecture for IoT smart gateway: Security-privacy trade-off. Procedia Computer Science, 52, 1066-1073.
13. Kaktas, R. N. (2019). Cyber Threats and Security Standards for Industry 4.0. In Industry 4.0: Trends and Challenges (pp. 135-154). Springer, Cham.
14. Li, B., Li, M., Chen, T., & Weng, J. (2018). A new service trust evaluation method for IoT network systems. Soft Computing, 22(7), 2163-2174.
15. Soldà, L., Jafari, M. A., Palombo, C., & Dini, G. (2017). Verifiable Use Case Access Control for Secure Data Storage in the Internet of Things. IEEE Internet of Things Journal, 5(5), pp. 3739-3747.
16. Ziegeldorf, J. H., Morchon, O. G., Wehrle, K., & Römer, K. (2014). Privacy in the Internet of Things: threats and challenges. Security and Communication Networks, 7(12), pp. 2728-2742.
17. Zhu, Q., Fitzgerald, J., Nahrstedt, K., & Lu, C. (2017). Cooperative and Secure Control of Vehicle Platoons Over Wide-Area Networks. IEEE Transactions on Vehicular Technology, 66(10), pp. 9704-9716.
18. Woychowski, C., Scott, D. C., & Sandel, R. (2018). Dancing with myself: a multi-view approach to creating digital avatars. ACM Transactions on Graphics (TOG), 37(4), pp. 1-14.
19. Sun, M., Kotagiri, R., & Li, J. (2014). A game-theoretic model for deception and deception detection in social networks. ACM Transactions on Intelligent Systems and Technology (TIST), 5(4), P. 72.
20. Santi, A., Restrepo, J. J., & Choca, C. E. (2018). Digital twin of manufacturing systems: a simulation model perspective. Journal of Ambient Intelligence and Humanized Computing, 9(5), pp. 1481-1495.
21. Alcaraz C., Lopez J. Digital Twin: A Comprehensive Survey of Security Threats // Proceedings of the International Conference on Cyber Security, Privacy, and Trust (CSP), 2019. - pp. 1-10.
22. Eckhart M., Ekelhart A. Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook // Journal of Computer Science and Cybernetics, vol. 4, no. 2, 2020. - pp. 45-62.

УДК 004.056

ВИДЫ КИБЕРАТАК И СПОСОБЫ ЗАЩИТЫ

Магера Марина Александровна
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий, пр., 3, Санкт-Петербург, 194064, Россия
e-mail: 19chapa99@gmail.com

Аннотация. В статье даны определения «кибератака» и «кибербезопасность», представлена статистика преступлений, совершенных с помощью информационных технологий, рассмотрены основные виды кибератак и способы защиты.

Ключевые слова: информационная безопасность; преступления в сфере информационных технологий; методы защиты информации; кибербезопасность; кибератаки.

TYPES OF CYBER ATTACKS AND METHODS OF PROTECTION

Magera Marina
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny,
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: 19chapa99@gmail.com

Absrtact. The article defines «cyber-attack» and «cyber security»; presents statistics of crimes committed with the help of information technology, discusses the main types of cyber-attacks and methods of protection.

Keywords: information security; crimes in the field of information technology; methods of information protection; cyber security; cyber-attacks.

Введение. Компьютерные сети являются неотъемлемой частью во всех сферах деятельности в современном обществе. Она представляет собой «объединение компьютеров и локальных сетей структурных подразделений организаций различных сфер деятельности на основе внутренних коммуникационных каналов и каналов сети Интернет» [1].

Компьютерные технологии позволили обрабатывать большое количество информации, хранить ее и передавать на дальние расстояния в мгновение ока, однако наличие единых баз данных, содержащие большой объем информации разного назначения, развитые системы коллективного пользования и широкое использование программ требуют определенного уровня защиты информации от кибератак. Компьютерная атака или кибератака — это «целенаправленное воздействие программными средствами, в том числе с использованием компьютерных вирусов, на информационно-телекоммуникационную систему, информационных систем, осуществляемое с целью нарушения конфиденциальности, целостности или доступности информации» [2]. Киберпреступления — это преступления, совершенные с помощью информационно-телекоммуникационных технологий или в сфере компьютерной информации.

Стоит отметить, что количество киберпреступлений растет с каждым годом. Согласно официальной статистике МВД РФ за январь-июль 2023 года в России было «зарегистрировано 371,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 27,9% больше, чем за аналогичный период прошлого года» [3]. Судебная и следственная практика показывает, что к наиболее распространенным преступлениям в сфере информационных технологий относятся:

- создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ);
- неправомерный доступ к компьютерной информации (ст. 272 УК РФ);
- мошеннические действия, совершенные с использованием электронных платежных средств (ст. 159.3 УК РФ).

Такой рост преступлений обусловлен быстрым развитием технологий, отсутствием эффективных мер по борьбе с киберпреступностью и необходимостью создания законодательной базы. Сказываются и особенности данных преступлений: преступник может находиться в любой точке мира и использовать не одну схему кибератак, а сразу несколько.

Виды кибератак можно разделить весьма условно: вредоносное ПО, DDos-атака, фишинг, атаки с использованием SQL-инъекций, межсайтовый скриптинг и ботнет. Ниже представлено описание каждого вида компьютерной атаки [4]:

Вредоносное ПО — это программа, созданная для внедрения в компьютерные систему, чтобы украсть конфиденциальную информацию, получить доступ к ней с последующей эксплуатацией либо вывести компьютерную систему из строя.

DDos-атака — это атака, при которой несколько зараженных компьютерных систем направлены на одну конкретную цель, например, сервер, веб-сайт или другой сетевой ресурс, перегружая его и замедляя либо вовсе останавливая работу системы.

Фишинг — это вид интернет-мошенничества, в котором злоумышленник притворяется доверенном лицом и обманом вынуждает жертву перейти по фальшивой ссылке, открыть зараженное вложение в электронном письме или самостоятельно сообщить конфиденциальные сведения.

SQL — это язык запросов, благодаря которому осуществляется управление базами данных и информацией, которая в них хранится. Так как большинство сайтов работают с базами данных, это делает их уязвимыми к атакам, совершенным с помощью SQL-инъекций. Злоумышленник вводит в поле ввода вредоносный запрос на SQL. После того как SQL-инъекция попадает в систему управления базами данных, она начинает работать. В результате преступник способен украсть личные данные клиентов, извлечь из базы объекты интеллектуальной собственности, секретные сведения и многое другое.

Межсайтовый скриптинг — один из видов кибератак, при котором сомнительный источник получает возможность внедрить свой код в веб-приложение, далеевредоносный код вместе с динамическим содержимым попадает в браузер жертвы. Это позволяет злоумышленнику выполнять в браузере другого пользователя вредоносные скрипты, написанные на различных языках, включая JavaScript, Java, Ajax, Flash и HTML. С помощью

межсайтового скриптинга злоумышленник может воровать cookie-файлы другого пользователя, после чего выдать себя за него и использовать для распространения вредоносного ПО, портить контент веб-сайтов, публиковать на них нежелательные материалы, совершать атаки на социальные сети, красть учетные данные и многое другое.

Ботнет — представляет собой сеть из нескольких подключенных к интернету зараженных компьютеров и устройств, которыми удаленно управляют злоумышленники. Как правило, ботнеты используются для рассылки спама, накручивания кликов и создания вредоносного трафика для DDoS-атак. Основной его цель — заразить как можно больше подключенных к интернету устройств, чтобы впоследствии можно было пользоваться их вычислительной мощностью и другими ресурсами для автоматизации и масштабирования вредоносной активности.

Таким образом, обеспечить полноценную и надежную кибербезопасность возможно, только если применять комплексный и системный подход. Система кибербезопасности должна включать не только все актуальные угрозы и уязвимости, но и угрозы, которые могут возникнуть в будущем. Контроль должен осуществляться непрерывно и обеспечивать поддержку на каждом этапе жизненного цикла информации.

Кибербезопасность — это «совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных» [5].

В зависимости от используемых методов, можно обозначить следующие средства защиты информации:

– организационные — комплекс мер и средств организационно правового и организационно-технического характера. К первым относят законодательные и нормативные акты, локальные нормативные документы организации. Второй тип — это меры по обслуживанию информационной инфраструктуры объекта.

– аппаратные (технические) — это специальное оборудование и устройство, предотвращающее утечки, защищающее от проникновения в IT-инфраструктуру;

– программные — это специальные ПО, предназначенные для защиты, контроля, хранения информации;

– программно-аппаратные — это специальные оборудования, оснащенные программными обеспечениями, для защиты данных.

Чтобы защитить информацию, находящуюся в современных сетях, большинство организаций используют широкий спектр специализированного программного обеспечения. Среди них можно выделить следующие типы программных средств защиты:

Антивирусное ПО. Программа, предназначенная для поиска, нейтрализации и удаления компьютерных вирусов. Они осуществляют проверку всех файлов, находящихся на компьютере, если антивирусное ПО видит подозрительную активность, то данный файл немедленно блокируется.

Облачные антивирусы (Cloud AV). Совокупность современных антивирусных программ и облачные технологии. К таким решениям относятся сервисы Crowdstrike, Panda Cloud Antivirus, Immunet и многие другие. Отличаются от обычных антивирусных ПО тем, что ПО размещен в облаке, а на защищаемое устройство устанавливается клиент-программа с минимальными техническими требованиями. Благодаря этому, клиент выгружает основную часть анализа данных в облачный сервер, что помогает обеспечить высокую степень защиты при минимальных технических нагрузках. Этот способ подходит для компьютерных систем, обладающих слабой вычислительной мощностью для обычного антивирусного ПО.

Решения DLP (Data Leak Prevention). Специализируются на защите информации от утечек данных. Он представляют собой комплекс технологий, эффективно защищающий организации от потери конфиденциальной информации в процессе различных видов кибератак. Внедрение и поддержка DLP требует достаточно больших вложений и усилий со стороны предприятия. Однако эта мера способна значительно уменьшить уровень информационных рисков для IT-инфраструктуры компании.

Системы криптографии. (DES — Data Encryption Standard, AES — Advanced Encryption Standard). Преобразуют данные, после чего их расшифровка может быть выполнена только с использованием соответствующих шифров. Помимо этого, криптография может использовать другие полезные приложения для защиты информации, в том числе дайджесты сообщений, методы проверки подлинности, зашифрованные сетевые коммуникации, цифровые подписи. Сегодня новые приложения, использующие зашифрованные коммуникации, например, Secure Shell (SSH), постепенно вытесняют устаревающие решения, не обеспечивающие в современных условиях требуемый уровень безопасности, такие как Telnet и протокол передачи файлов FTP. Для шифрования беспроводной связи широко применяются современные протоколы WPA/WPA2. Также используется и достаточно старый протокол WEP, который уступает по безопасности. ITU-T G.hn и другие проводные коммуникации шифруются при помощи AES, а аутентификацию и обмен ключами них обеспечивает X.1035. Для шифрования электронной почты используют такие приложения как PGP и GnuPG.

Межсетевые экраны (МСЭ). Решения, которые обеспечивают фильтрацию и блокировку нежелательного трафика, контролируют доступ в сеть. Различают такие виды файерволов, как сетевые и хост-серверы. Сетевые файерволы размещаются на шлюзовых ПК LAN, WAN и в интрасетях. Межсетевой экран может быть выполнен в формате программы, установленной на обычный компьютер или иметь программно-аппаратное исполнение. Программно-аппаратный файервол — это специальное устройство на базе операционной системы с установленным МСЭ. Помимо основных функций, межсетевые экраны предлагают ряд дополнительных решений для внутренней сети. Например, выступают в качестве сервера VPN или DHCP.

Виртуальные частные сети VPN (Virtual Private Network). Решение, использующее в рамках общедоступной сети частную сеть для передачи и приема данных, что дает эффективную защиту подключенных к сети приложений. При помощи VPN обеспечивается возможность удаленного подключения к локальной сети, создания общей сети для головного офиса с филиалами. Непосредственно для пользователей VPN дает возможность скрытия местоположения и защиты выполняемых в сети действий.

Прокси-сервер. Выполняет функцию шлюза между компьютером и внешним сервером. Запрос, отправляемый пользователем на сервер, вначале поступает на proxy и уже от его имени поступает на сервер. Возврат ответа производится также с прохождением промежуточного звена — proxy. Преимуществом является то, что кэш прокси-сервера доступен всем пользователям. Это повышает удобство в работе, поскольку наиболее часто запрашиваемые ресурсы находятся в кэше.

Решения SIEM. Системы мониторинга и управления информационной безопасностью. Специализированное ПО, которое берет на себя функцию управления безопасностью данных. SIEM обеспечивает сбор сведений о событиях из всех источников, поддерживающих безопасность, в том числе от антивирусного ПО, IPS, файерволов, а также от операционных систем и т. д. Также SIEM выполняет анализ собранных данных и обеспечивает их централизованное хранение в журнале событий. На основании анализа данных система выявляет возможные сбои, хакерские атаки, другие отклонения и возможные информационные угрозы.

В процессе анализа всех видов программных средств защиты данных к воздействиям кибератак были выявлены следующие недостатки [6]:

– - все программные средства требуют регулярных обновлений и модификаций, так как вредоносные ПО перманентно модернизируются;

– программные средства защиты, как и все программы, имеют уязвимые места для удаленных атак;

– модификация ПО большинства удаленных устройств не всегда физически реализуема.

Заключение. Таким образом, мы видим, что ни одна программа не способна противостоять всем видам компьютерных атак. Необходимо оценивать вероятность появления и реализации угроз при базовых и дополнительных средствах защиты. На основе полученной информации подбирать наиболее подходящий комплекс мер в зависимости от объекта защиты, технической мощности устройства и важности хранящейся на нем информации. А также периодически проводить экспертные проверки, которые проверяют все возможные угрозы, находят уязвимые места, составляют список предполагаемого ущерба в случае успешной атаки и вероятность возникновения данной угрозы.

СПИСОК ЛИТЕРАТУРЫ

1. Анисимов В. Г., Анисимов Е. Г., Сауренко Т. Н., Лось В. П. Оценка эффективности систем защиты компьютерных сетей от вирусных атак // Проблемы информационной безопасности. Компьютерные системы. 2022, № 1, С 11-17
2. Коллеров А. С., Синадский Н. И., Хорьков Д. А. Системы обнаружения атак : учеб. пособие для высших учебных заведений. М. : Горячая линия — Телеком, 2022. 124 с.
3. Состояние преступности в Российской Федерации за январь — июль 2023 года [Электронный ресурс]. URL: https://мвд.рф/reports/item/40874008 (дата обращения: 21.08.2023).
4. Что такое кибербезопасность? [Электронный ресурс] // Kaspersky Security Network. URL: https://www.kaspersky.ru-center/definitions/what-is-cyber-security (дата обращения: 21.08.2023).
5. Бусленко Т. О., Бусленко Е.О. Кибербезопасность. Виды киберугроз и контрмер [Электронный ресурс] // Молодой ученый: журнал. URL: https://moluch.ru/young/archive/66/3529/ (дата обращения: 22.08.2023).
6. Пузанов А .В., Пузанова К. А. Направления повышения кибербезопасности систем управления мобильной техники // Вопросы защиты информации. М.: НТЦ оборонного комлекса Компас, 2023. № 2 (141). С 66-70.

УДК 004.056

ЗАЩИТА СЕТЕЙ С АДАПТИВНОЙ ТОПОЛОГИЕЙ ОТ КИБЕРУГРОЗ НА ОСНОВЕ ИСКУССТВЕННОЙ ИММУНИЗАЦИИ

Павленко Евгений Юрьевич
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
e-mail: pavlenko@ibks.spbstu.ru

Аннотация. В статье рассматриваются глобальные и локальные стратегии искусственной иммунизации сетей с адаптивной топологией, направленные на их защиту от киберугроз путем наделения сети свойством устойчивости к различного рода атакам. Описана формальная постановка задачи создания механизма иммунизации, представлены шаги иммунизации различной динамической сетевой инфраструктуры — иерархической и одноранговой. Представлены результаты экспериментальных исследований по применению глобальных стратегий иммунизации для сетей с иерархической топологией, демонстрирующие состоятельность выбранных стратегий.

Ключевые слова: сеть с адаптивной топологией; искусственная иммунизация; глобальные стратегии иммунизации; локальные стратегии иммунизации; иерархическая сетевая топология.

ARTIFICIAL IMMUNIZATION-BASED THREAT PROTECTION OF NETWORKS WITH ADAPTIVE TOPOLOGY

Pavlenko Evgeny
Peter the Great St.Petersburg Polytechnic University (SPbPU)
29 Polytechnicheskaya St, St.Petersburg, 195251, Russia
e-mail: pavlenko@ibks.spbstu.ru

Abstract. The paper considers global and local strategies of artificial immunization of networks with adaptive topology aimed at protecting them from cyber threats by endowing the network with the property of resistance to various kinds of attacks. The formal formulation of the problem of creating an immunization mechanism is described, and the steps of immunization of different dynamic network infrastructures - hierarchical and peer-to-peer - are presented. The results of experimental studies on the application of global immunization strategies for networks with hierarchical topology are presented, demonstrating the validity of the selected strategies.

Keywords: network with adaptive topology; artificial immunization; global immunization strategies; local immunization strategies; hierarchical network topology.

Введение. Подобно тому, как иммунитет человека защищает его организм от различного рода деструктивных воздействий — внутренних и внешних — так и искусственный иммунитет представляет собой интеллектуальный механизм защиты для современных цифровых систем. Иммунизация таких систем позволит обеспечить их устойчивость к атакам, заключающуюся в сохранении их корректного функционирования. Стратегии иммунизации должны варьироваться в зависимости от типа систем и от их способности к перестроению, которая во многом определяется типом сетевой структуры, лежащей в основе системы. В работе представлена формальная постановка задачи создания механизма иммунизации, а также описан подход к иммунизации цифровых систем, базирующихся на иерархической и одноранговой сетевой топологии.

Первым шагом к формализации задачи является классификация видом современных цифровых систем в зависимости от типа их сетевой инфраструктуры. Выделяются 4 вида систем: системы с иерархической сетевой топологией, узлы сети статичны; системы с одноранговой сетевой топологией, узлы сети статичны; системы с иерархической сетевой топологией, узлы сети способны перемещаться в пространстве; системы с одноранговой сетевой топологией, узлы сети способны перемещаться в пространстве.

Для каждого вида цифровых систем, с учетом их специфики и назначения, подойдут различные стратегии иммунизации. Как правило, выделяют локальные и глобальные стратегии иммунизации, первые базируются на передаваемых по сети данных, а вторые работают на основе имеющихся знаний о структуре всей сети [1-3].

Формальная постановка задачи создания механизма иммунизации:

1. Пусть задана защищаемая система Sys, в состав которой входят компоненты $Nodes = \{Node_1, Node_2, \dots, Node_n\}$ и связи между ними $Edges$.

2. Для системы задается тип сетевой инфраструктуры $Type$ и целевая функция, в соответствии с которой работает система F: $Sys =< Nodes, Edges, Type, F >$.

3. Зададим функцию p, определяющую параметры значимых компонентов и связей между ними: $p(Nodes) = \{p_1^{Nodes}, p_2^{Nodes}, \dots, p_N^{Nodes}\}$ и $p(Edges) = \{p_1^{Edges}, p_2^{Edges}, \dots, p_M^{Edges}\}$.

4. Зададим функцию q, характеризующую качество реализации целевой функции: $q(F) = Q, Q \in [Q_{min}; Q_{max}]$. Здесь Q_{min} — минимально допустимое значение показателя качества работы системы.

5. Пусть множество Z — множество реализуемых атак: $Z = \{z_1, \dots, z_L\}$. Каждая атака $z_i \in Z$ описывается числом выведенных из строя объектов системы и снижением показателя качества ее работы Q. Воздействие множества атак описывается функцией $z(t)$.

6. Для защиты от киберугроз в системе реализован механизм иммунизации I, представляющий собой архитектурно заложенные на этапе проектирования или надстроенные средства обеспечения безопасности. Он включает 2 класса стратегий иммунизации — глобальные I^G и локальные I^L: $I = \{I^G, I^L\}$. Здесь глобальные стратегии оперируют множествами $Nodes$ и $Edges$, а также показателем Q, а локальные стратегии — множествами $Nodes$, $Edges$, $\{p_1^{Nodes}, p_2^{Nodes}, \dots, p_N^{Nodes}\}$, $\{p_1^{Edges}, p_2^{Edges}, \dots, p_M^{Edges}\}$ и показателем Q.

7. Процесс иммунизации выразим как функцию от времени $I(t)$, которая описывает восстановление поврежденных в ходе атаки компонентов системы и повышение значения Q.

Формально решение задачи иммунизации состоит в поиске оператора i, характеризующего стратегии иммунизации, такого, что одновременно выполняются следующие условия: $i: Z(t) - I(t) \to min$, минимизация числа зараженных объектов КФС; $i: I(t) \to Nodes_0 - Z(t)$, максимизация числа вылеченных компонентов КФС, здесь $Nodes_0$ — число компонентов системы до начала атаки; $i: |Q_0 - Q'| \to min$, максимизация значения Q или минимизация разницы между начальным значением $Q_0, Q_o \in [Q_{min}; Q_{max}]$ и значением Q', полученным в результате атаки.

Для сетей с адаптивной иерархической топологией, свойственной преимущественно промышленным системам, предлагается использовать глобальные стратегии иммунизации, в основе которых лежат графовые метрики центральности и критичности по связности (узел является критическим, если его удаление приведет к разрыву графа $G(s,d)$, где $G(s,d)$ есть успешные передачи сообщения от источника s к конечному получателю d) [4]. Для сетей с адаптивной одноранговой топологией более эффективными будут локальные стратегии иммунизации, в силу невозможности априорного знания структуры сети и ее постоянного изменения. Локальные стратегии будут носить вероятностный подход и затрагивать только определенную долю узлов.

Экспериментальные исследования проводились только для сетей с иерархической сетевой топологией. На основе системы, описанной в работе [5], был смоделирован иерархический граф. Показатель Q представлял собой эффективность передачи данных и варьировался в пределах $[80\,\%;\ 100\,\%]$. Смоделированные атаки имитировали воздействие на канал связи между узлами. Атака была обнаружена за счет изменений в значениях метрик центральности и снижения скорости передачи данных. Были применены глобальные стратегии иммунизации, состоящие в построении дополнительных связей между узлами, процесс иммунизации показан на рис. 1.

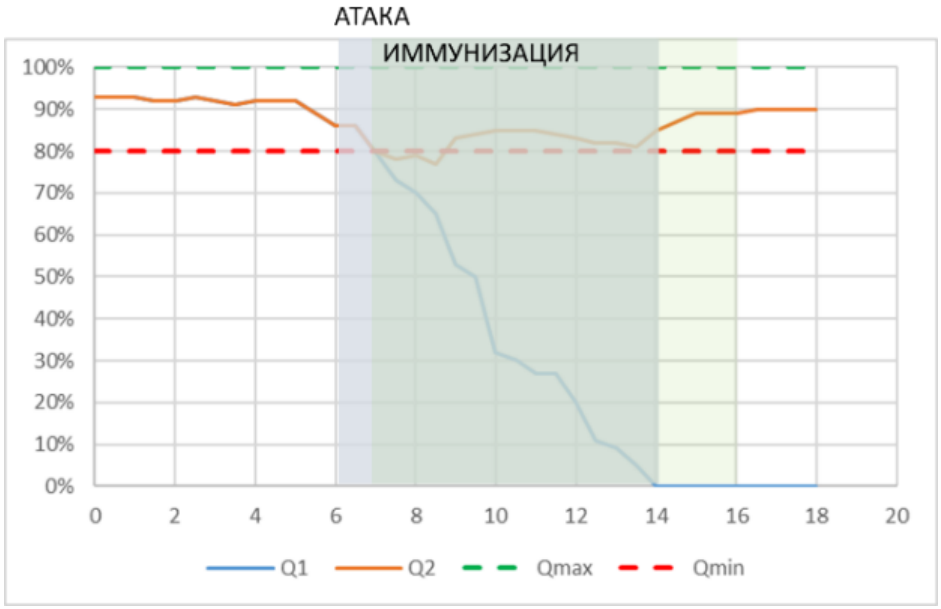


Рис. 1. Изменение показателя качества работы системы без иммунизации и при иммунизации

Из рисунка видно, что без иммунизации система бы деградировала очень быстро, в то время как применение даже первой стратегии иммунизации уже позволило противодействовать атаке и удержать значение Q в заданном диапазоне. Вторая стратегия была применена в момент времени 12, когда стало наблюдаться снижение значения Q и приближения его к минимальной отметке в 80 %.

Заключение. Предложен подход к иммунизации цифровых систем, базирующихся на иерархической и одноранговой сетевой топологии. В первом случае предложено использовать глобальные стратегии иммунизации, применяемые к узлам сети с высокой критичностью, где критичность определяется через метрики центральности и параметры связности сети. Во втором случае предложен вероятностный подход к выбору некоторого числа узлов, к которым будут применены защитные меры. Состоятельность подхода подтверждена экспериментально. Дальнейшие исследования должны быть направлены на установление зависимости между устойчивостью работы системы и локальными стратегиями иммунизации в случае одноранговой сетевой топологии.

Исследование выполнено в рамках гранта Президента РФ для государственной поддержки молодых российских ученых — кандидатов наук МК-3861.2022.1.6.

СПИСОК ЛИТЕРАТУРЫ

1. Wang C., Knight, J. C., Elder, M.C. On computer viral infection and the effect of immunization // 16th Annual Computer Security Applications Conference (ACSAC'00), IEEE. 2000. December. Pp. 246-256.
2. Bahashwan W. S., Al-Tuwairqi S. M. Modeling the Effect of External Computers and Removable Devices on a Computer Network with Heterogeneous Immunity // International Journal of Differential Equations. 2021. https://doi.org/10.1155/2021/6694098.
3. Ghalmane Z., Hassouni M. E., Cherifi H. Immunization of networks with non-overlapping community structure // Social Network Analysis and Mining. 2019. № 9, Pp. 1-22.
4. Khansari M., Kaveh A., Heshmati Z., Motlaq M. A. Centrality measures for immunization of weighted networks // Network Biology. 2016. № 6(1). Pp. 12-27.
5. Cohen R., Havlin S., Ben-Avraham D. Efficient immunization strategies for computer networks and populations. // Physical review letters, 2003. № 91(24), 247901.

УДК 004.056

СТРУКТУРНАЯ САМОРЕГУЛЯЦИЯ СЕТИ С АДАПТИВНОЙ ТОПОЛОГИЕЙ НА ОСНОВЕ ГРАФОВОГО АЛГОРИТМА ПРЕДСКАЗАНИЯ СВЯЗЕЙ

Павленко Евгений Юрьевич
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
e-mail: pavlenko@ibks.spbstu.ru

Аннотация. В статье рассматривается применение алгоритма предсказания связей (link prediction) в одноранговой сети с адаптивной топологией. Для работы алгоритма использованы значимые физические параметры устройств, а также метрика центральности по посредничеству, характеризующая значимость конкретного узла для передачи данных в сети. Корректность работы алгоритма подтверждена экспериментально: спрогнозированные ребра между вершинами графа, моделирующего сеть, действительно были построены, и процесс передачи и обмена данными не был нарушен.

Ключевые слова: сеть с адаптивной топологией; одноранговая сеть; саморегуляция; теория графов; алгоритм предсказания связей; метрика центральности.

STRUCTURAL SELF-REGULATION OF A NETWORK WITH ADAPTIVE TOPOLOGY BASED ON A GRAPH LINK PREDICTION ALGORITHM

Pavlenko Evgeny
Peter the Great St.Petersburg Polytechnic University (SPbPU)
29 Polytechnicheskaya St, St.Petersburg, 195251, Russia
e-mail: pavlenko@ibks.spbstu.ru

Abstract. The article discusses the application of link prediction algorithm in a peer-to-peer network with adaptive topology. The algorithm uses significant physical parameters of devices, as well as mediation centrality metric, which characterizes the importance of a particular node for data transmission in the network. The correctness of the algorithm was confirmed experimentally: the predicted edges between the nodes of the graph modeling the network were indeed constructed, and the process of data transmission and exchange was not disturbed.

Keywords: network with adaptive topology; peer-to-peer network; self-regulation; graph theory; link prediction algorithm; centrality metric.

Введение. Современные цифровые системы, построенные на базе сетей с адаптивной сетевой топологией, требуют создания новых подходов к обеспечению их защиты от киберугроз. Это обусловлено спецификой предметной области, заключающейся в мобильности узлов сети, а также непостоянном характере связности между узлами таких сетей. К особенностям обеспечения кибербезопасности рассматриваемых цифровых систем следует также отнести необходимость сохранения их корректного функционирования даже в условиях деструктивных воздействий. Для этого необходимо наделить защищаемую систему способностью к саморегуляции, как на уровне параметров устройств, так и на уровне структуры.

Способность системы корректно функционировать может быть выражена через целевую функцию системы. В терминах графовой модели, целевая функция представляет собой путь на графе, с учетом параметров дуг (ребер) и вершин графа, а также посещения определенных вершин графа [1]. С технической точки зрения, такие узлы могут представлять собой узлы, на которых происходит агрегация передаваемых данных от нескольких узлов сети или узлы, шифрующие накопленные данные.

Таким образом, при реализации киберугроз на сетевую инфраструктуру систему необходимо выполнить такие управляющие воздействия, которые бы обеспечивали выполнение целевой функции, то есть, возможность передачи данных с посещением обязательных узлов и одновременным сохранением значений параметров устройств в определенном диапазоне.

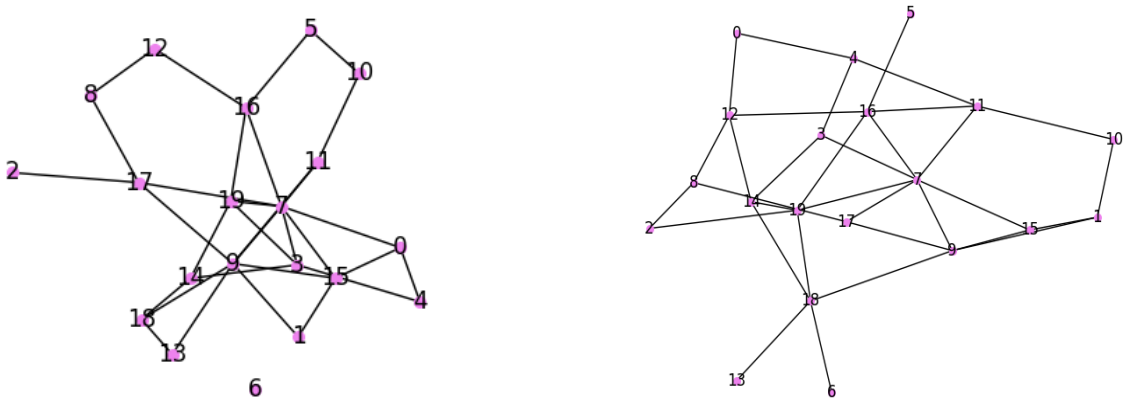
В данной работе внимание сосредоточено на структурной саморегуляции адаптивной сетевой топологии с использованием графового алгоритма предсказания связей (link prediction). Данный подход вдохновлен графовыми методами анализа взаимосвязей между пользователями в социальных сетях [2, 3]. Как правило, алгоритм предсказания связей направлен на прогнозирование «дружбы» между пользователями и его работа базируется на многих метриках, в том числе — общие друзья, одно и то же место учебы или работы в сочетании с похожим возрастом, схожие интересы и т.п. Для адаптации такого алгоритма к сетям с адаптивной топологией следует учитывать особенности функционирования защищаемой системы и тип сетевой топологии.

Представленное исследование сосредоточено на саморегуляции одноранговой сетевой топологии, выполняющей простейшую целевую функцию системы — передачу данных от одного конца сети до другого, подключенного к системе хранения данных. Такая целевая функция характерна для сенсорных сетей, расположенных в труднодоступных местах, где ключевая задача — сбор информации от сенсоров и ее передача в

хранилище данных для дальнейшего анализа [4, 5]. В таких условиях важна информация от всех (или от большинства) сенсоров, однако в случае разрыва связи между парой узлов необходимо, чтобы данные от узлов не были потеряны. Адаптивность сетевой топологии обеспечивает динамическое перестроение сети и появление новых связей в ответ на утраченные. Таким образом, такой тип сетевой инфраструктуры априори подходит для построения механизма саморегуляции. Однако ключевым вопросом остается выбор параметров узлов сети, в соответствии с которыми с большей вероятностью будут образовываться новые связи.

Разработанный алгоритм предсказания связей базируется на следующих параметрах: мощность сигнала устройства сети, его заряд батареи, критичность узла, выражаемая метрикой центральности по посредничеству. Предполагается, что выбранные параметры в случае с сенсорной сетью имеют ключевое значение для создания новых связей.

На рис. 1 показаны структуры сети до и после саморегуляции (а) и б), соответственно). Видно, что в случае а) имеется узел, данные от которого никуда не передаются, в случае б) это скорректировано за счет появления нового ребра (6, 18).



а) б)

Рис. 1. Структура одноранговой сети: а) до саморегуляции б) после саморегуляции

При работе алгоритма предсказания связей вероятность появления ребра между вершинами № 6 и № 18 составляла 0,97. При саморегуляции сети ребро между этой парой вершин действительно появилось, и этому есть обоснование в соответствии с принципами работы одноранговых сетей. На рис. 1 а) наблюдается граф довольно высокой связности, много вершин обладают степенью не менее 4. Однако подключение выполнено к узлу 18 в соответствии со следующими причинами:

– узел № 6 находился в радиусе передачи сигнала с узлами № 18, № 9 и № 15;

– у узла № 18 степень вершины ниже, чем у узлов № 9 и № 15 — степень узла № 18 составляет 3, а у двух других узлов — 6;

– несмотря на то, что в сети у мощных по уровню сигнала узлов допускается степень 7, заряд батареи у узла № 15 был существенно ниже, чем у узлов № 18 и № 9.

По совокупности параметров, для установки подключения к узлу № 6 был выбран узел № 18, и корректность работы алгоритма предсказания связей была подтверждена на практике, созданием такого ребра между вершинами, моделирующими узлы № 18 и № 9.

Таким образом, можно сделать вывод о том, что современные цифровые системы, построенные на базе сетей с адаптивной топологией, обладают способностью к саморегуляции, и повысить качество такой саморегуляции, достигая обеспечения корректного функционирования системы даже в условиях деструктивных информационных воздействий, можно, используя графовое представление такой сети. На основе значимых параметров устройств, представляющих собой вершины графа, и их характеристик, предоставляющих сведения о структуре сети, возможно корректное и обоснованное предсказание появления и разрыва сетевых соединений (ребер в графе). Использование для этого графового алгоритма предсказания связей позволит, с одной стороны, своевременно обнаруживать атаки на сеть, а с другой стороны — повысить эффективность саморегуляции за счет генерации множества графовых структур и их ранжирования.

Заключение. Обеспечение безопасности современных цифровых систем требует создания методов саморегуляции, позволяющих сохранить работу системы в условиях атак. Математические методы теории графов и совокупное использование физических характеристик устройств (уровень сигнала и заряда батареи) со структурными характеристиками (центральность узла в сети) представляют собой перспективный подход к саморегуляции динамических сетей, что подтверждено экспериментально на примере с одноранговыми сетями.

Финансирование: Исследование выполнено за счет гранта Российского научного фонда № 22-21-20008, https://rscf.ru/project/22-21-20008/. Исследование выполнено за счет гранта Санкт-Петербургского научного фонда в соответствии с соглашением от «15» апреля 2022 г. № 61/220.

СПИСОК ЛИТЕРАТУРЫ

1. Павленко Е. Ю. Модель функционирования адаптивной сетевой топологии крупномасштабных систем на основе динамической теории графов // Проблемы информационной безопасности. Компьютерные системы. 2022. № 3. С. 68-79. DOI 10.48612/jisp/tn56-xvah-7tf1.
2. Daud N. N. Applications of link prediction in social networks: a review / N. N. Daud, S. H. Ab Hamid, M. Saadoon, F. Sahran, N. B. Anuar // Journal of Network and Computer Applications, 2020. V. 166. Article 102716.
3. Qiu Z., Wu J., Hu W., Du B., Yuan G., Yu P. Temporal link prediction with motifs for social networks // IEEE Transactions on Knowledge and Data Engineering. 2021. Pp. 99.
4. Kandris D., Nakas C., Vomvas D., Koulouras G. Applications of wireless sensor networks: an up-to-date survey // Applied system innovation. 2020. 3, 14; doi:10.3390/asi3010014.
5. Kim M., Park S., Lee W. Energy and distance-aware hopping sensor relocation for wireless sensor networks. 2019. Sensors 19 (7), 1567. DOI:10.3390/s19071567.
6. Каширина И. Л., Ковун В. А. Количественный подход к оценке влияния литературных произведений с использованием теории графов // Вестник ВГУ. Серия: Системный анализ и информационные технологии, 2019. № 3. С. 177-185.

УДК 004.056

АРХИТЕКТУРА ЗАЩИЩЕННОЙ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ И ИНЦИДЕНТОВ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Штеренберг Станислав Игоревич
Ордена Трудового Красного Знамени Московский технический университет связи и информатики»
Авиамоторная ул., 8а, Москва, 111024, Россия
e-mail: shterenberg.stanislaw@yandex.ru

Аннотация. Цели архитектуры защищенной интеллектуальной системы обнаружения вторжений и инцидентов заключаются в том, чтобы предвидеть возможные угрозы безопасности информации, которые могут возникнуть в системе, и принимать меры по защите информации от возможных атак. Эта архитектура может использоваться для оценки уязвимостей в системе, выявления угроз и мер по их предотвращению, а также для обучения сотрудников организации правилам безопасности информации и процедурам защиты данных. Разработка технологии создания интеллектуальных систем защиты информации носит комплексный характер, в которой на первое место выносится квазибиологическая парадигма, где сперва представляется форма программирования информационных процессов, систем машинного обучения и построения нейронных систем и заканчивая архитектурой интеллектуальной системы обнаружения вторжений и инцидентов с встроенными механизмами обеспечения информационной безопасности.

Ключевые слова: искусственный интеллект; системы обнаружения вторжений; системы обнаружения инцидентов; нейросеть, распределённые информационные системы**.**

ARCHITECTURE OF A SECURE INTELLIGENT INTRUSION AND INCIDENT DETECTION SYSTEM IN DISTRIBUTED INFORMATION SYSTEMS

Shterenberg Stanislav
Moscow technical university of communications and informatics
8a Aviamotornaya St, Moscow, 111024, Russia
e-mail: shterenberg.stanislaw@yandex.ru

Abstract. The goals of the architecture of a secure intelligent intrusion and incident detection system are to anticipate possible threats to the security of information that may arise in the system and take measures to protect information from possible attacks. This architecture can be used to assess vulnerabilities in the system, identify threats and measures to prevent them, as well as to train the organization's employees in information security rules and data protection procedures. The development of technology for creating intelligent information security systems is complex in nature, in which a quasi-biological paradigm is put in the first place, where the form of programming information processes, machine learning systems and the construction of neural systems is first presented, and ending with the architecture of an intelligent intrusion and incident detection system with built-in information security mechanisms.

Keywords: artificial intelligence; intrusion detection systems; incident detection systems; neural network, distributed information systems.

Введение. В концепте архитектуры, где уже имеются предметы контроля «жизнеспособности» и кибербесопасности, основными достоинством будет являться установление коэффициента достижения порога насыщения, позволяющий контролировать распространения программных агентов в системе с обработкой механизмов Больших данных [1]. Обработка Больших данных [7] в дальнейшем будет влиять на приобретение

ассоциативной память у интеллектуальной системы обнаружения вторжений и инцидентов, а также обеспечивать синхронизацию компонентов мультиагентной нейронной системы, имеющая в основе квазибиологическую парадигму, которая позволяет определить условия сохранности интеллектуальной системы обнаружения вторжений и инцидентов от деструктивных действий. Представленный концепт YaVi имеет следующую схему (см. рис. 1) На схеме представлено большинство модулей и идейного программного обеспечения. За оранжевой чертой сверху рисунка представлены управляющие модули, а в синем овале рисунка представлены компоненты СУБД для всей системы концепта YaVi в целом.

Каждый модуль — эта программа и/или ПО («нейрон») со встроенными функциями сим защиты информации (далее — СЗИ), которые связаны единым процессом перцептрона, носящего название PiRun. В дальнейшем будет выстраиваться методология и защита ПО во всей распределенной информационной системе (далее — РИС). Суть этой концептуальной модели обеспечить зарождающийся ИИ математической методологией обработкой Больших данных для накопления ассоциативной памяти, проводить ассимиляцию дополнительных СЗИ и компонентов перцептрона, а также развивать и улучшать строящийся ИИ (ПО-программное обеспечение, ПА — программный агент, СУБД — система управление базой данных, БД — база данных).

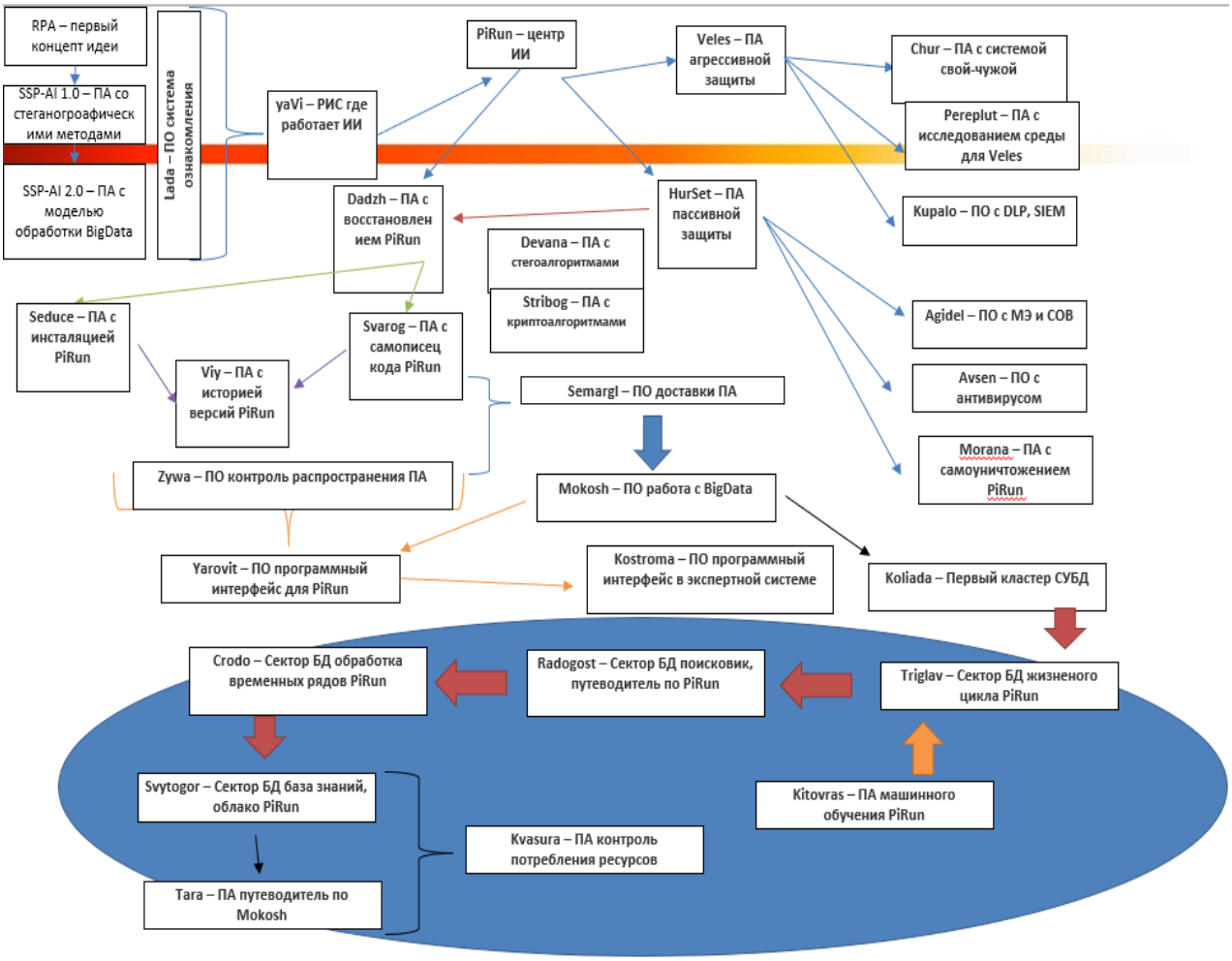


Рис. 1. Концептуальная схема YaVi - интеллектуальной системы обнаружения вторжений и инцидентов

В свою очередь PiRun программный агент — головной модуль принятия решений перцептрона. Принцип работы головного модуля принятия решений перцептрона включает в себя:

Сбор данных. Головным модулем производится сканирование сетевых ресурсов на наличие входных и выходных данных, изучается ход работы системы безопасности и т.д;

– Обработка данных. Головной модуль осуществляет предварительную обработку данных. Преобразовывает входные данные в приемлемый формат, что бы обученная модель их узнала. Также он осуществляет обработку входных данных: принимает входные данные, распознает их и классифицирует;

– Принятие решения. В зависимости от результата классификации, головной модуль принимает решение об одобрении или блокировке соответствующих действий;

– Итерация процесса. Процесс повторяется в цикле для построения новых моделей путем сбора новых данных и обучения головного модуля.

Таким образом, принцип работы головного модуля принятия решений перцептрона основан на алгоритмическом анализе входных данных, чтении данных из обученной модели, обработке и классификации этих данных и принятии решения на основании результатов. Принцип работы СУБД и базы знаний с ресурсами комплекса yaVi заключается в хранении и обработке информации о потреблении ресурсов и возможных уязвимостях для защиты РИС. Система регулярно обновляется, чтобы отслеживать изменения в состоянии системы и оперативно реагировать на уязвимости и угрозы. На основании описанных компонентов рассмотрим схему взаимодействия всех компонентов перцептронов (рис. 2).

Существует много причин для желания распространять интеллектуальные данные или справляться с многоагентными системами. Основные проблемы в исследованиях децентрализованной интеллектуальной системы состоят в следующем:

– Параллельное решение задач: в основном касается того, как можно модифицировать классические концепции искусственного интеллекта, чтобы можно было использовать многопроцессорные системы и кластеры компьютеров для ускорения вычислений;

– Распределенное решение проблем (DPS): концепция агента, автономных объектов, которые могут взаимодействовать друг с другом;

– Многоагентное моделирование (MABS): ветвь DAI, которая закладывает основу для моделирования, требующего анализа явлений не только на макроуровне, но и на микроуровне, как это происходит во многих сценариях социального моделирования.

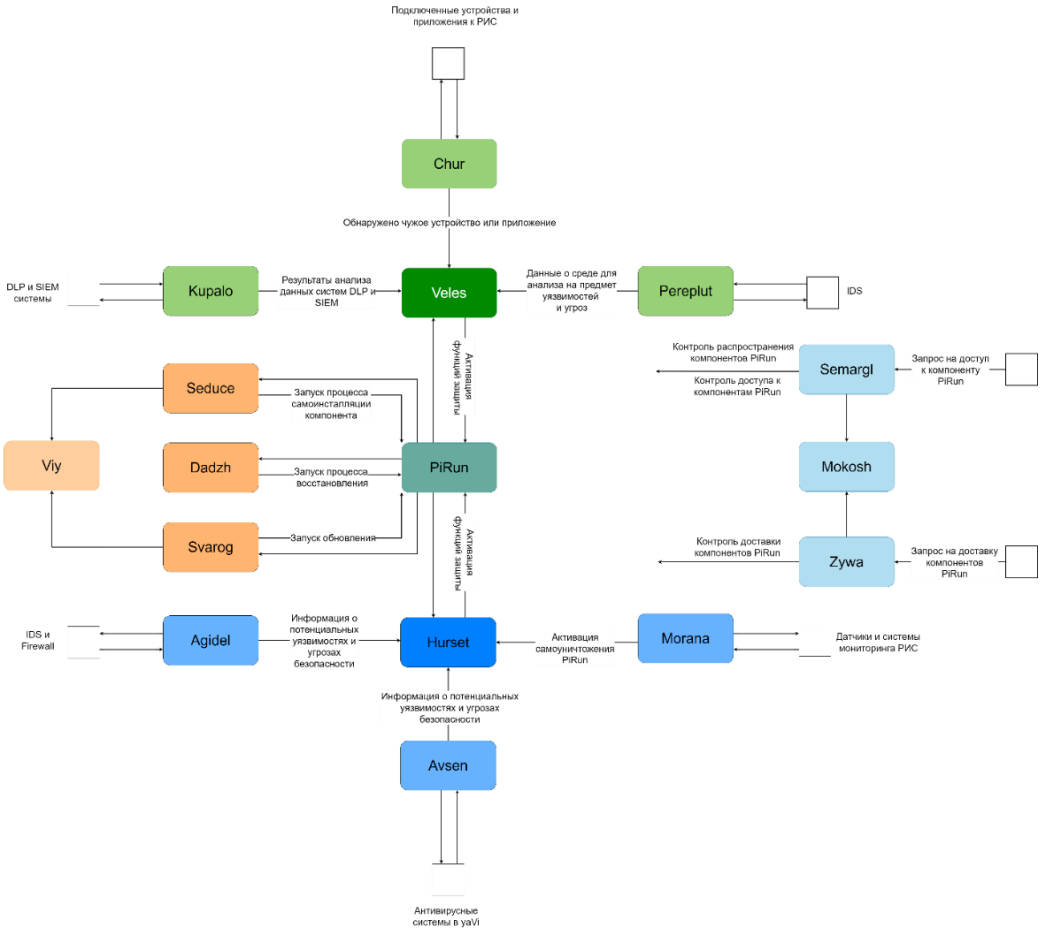


Рис. 2. Схема взаимодействия компонентов архитектуры yaVi.

Параметры, предоставленные всеми агентами, объединяются для получения глобальной модели. Более того, процесс объединения осуществляется не постоянным центральным координатором или сервером параметров, а временным ведущим агентом, динамически выбираемым среди всех активных, поэтому сеть роя является децентрализованной. За счет этого обеспечивается гораздо более высокая отказоустойчивость, чем в традиционных

платформах с серверами параметров. При использовании глобальной модели каждый агент получает в свое распоряжение все знания сети, при этом исходные данные не выходят за его пределы [2].

Идея обучения опирается на две проверенные технологии: распределенное машинное обучение и глубокое обучение. Алгоритм распределенного машинного обучения применяется для обучения общей модели на множестве агентов с подмножеством данных, находящихся в каждом агенте (в машинном обучении такой принцип называется парадигмой параллелизма по данным), но без центрального сервера параметров [3]. Процесс обучения архитектуры можно разделить на следующие этапы (см. рис. 3).

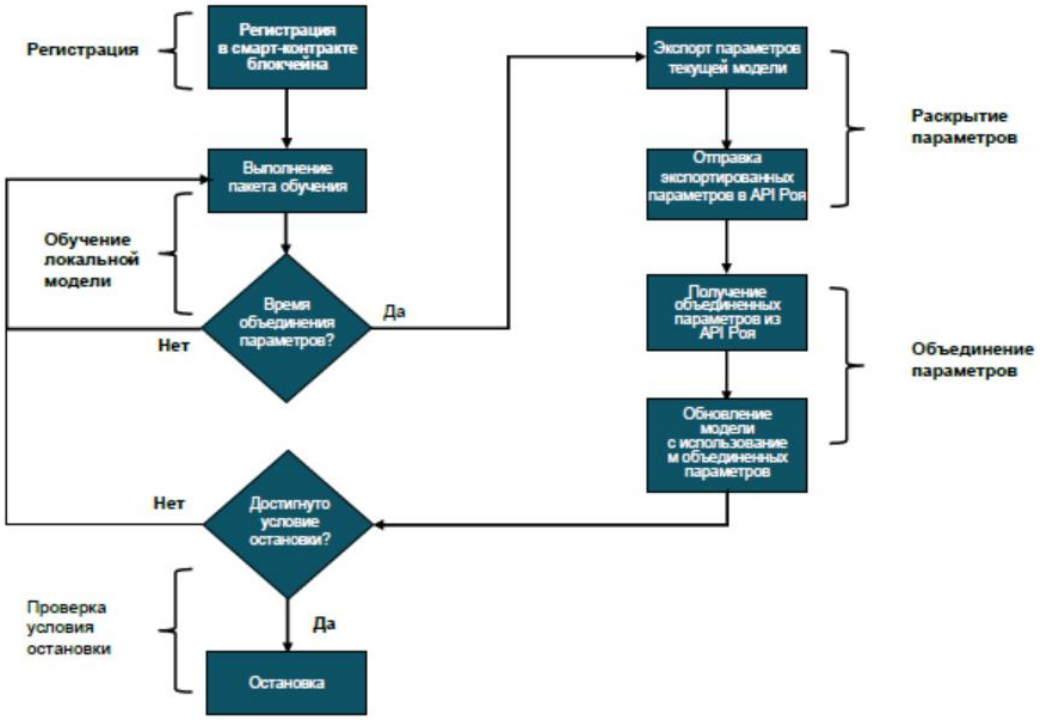


Рис. 3. Алгоритм обучения архитектуры yaVi

Рис. 4. Алгоритм распространения ПА в распределенной информационной системе со списком попаданий

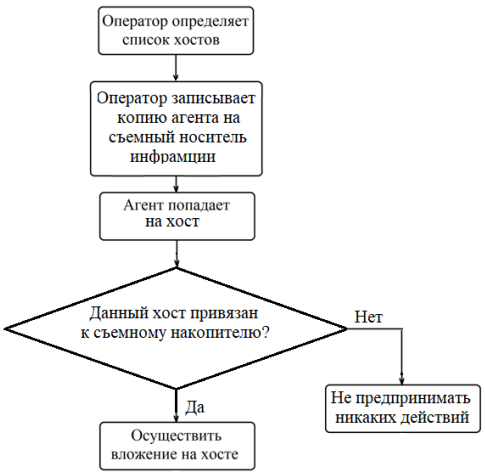


Рис. 5. Алгоритм распространения ПА в распределенной информационной системе со списком попаданий с автозапуском

Рис. 6. Алгоритм распространения ПА в распределенной информационной системе со списком попаданий, сканирующий тип

Для программного агента, в свою очередь, со списком попаданий характерно наличие списка, в котором указаны хосты, на которые требуется осуществить воздействие. Данный список составляется оператором агента до

его непосредственного запуска в распределенную информационную систему. Оператор, зная топологию сети, в которую будет запущен агент, составляет таблицу с IP-адресами и прописывает её в агенте. Данная таблица не должна занимать много места, чтобы не повысить вес самого агента, тем самым уменьшив показатель незаметности [1]. В отличие от сетевого червя, оператору которого перед запуском необходимо произвести сканирование сети для выявления нужных хостов, оператору агента сразу известны все хосты. На рис 4, 5 и 6 представлены различные способы распространения программных агентов по РИС.

В ходе разработки архитектуры были рассмотрены различные способы распространения агента в распределенной информационной системе [5]. В результате было выявлено три наиболее подходящих способа распространения агента:

1.Способ распространения агента со списком попаданий в распределенной информационной системе со списком попаданий. Данный способ будет наиболее эффективным в статичной сети, которая не подвергается каким-либо изменениям, например, масштабированию или изменению конфигурации хостов. В противном же случае, оператору придется вручную изменять список попаданий, что может повлечь за собой дополнительные расходы [6]. В случае, если сеть действительно является статичной, и в ней не вносятся изменения, то данный способ позволит с большой скоростью осуществлять работу агента, поскольку у него в наличии будут заранее построенные маршруты до определенных хостов, что даст возможность не тратить время на сканирование всех хостов в локальной сети.

2.Способ распространения агента с автозапуском в распределенной информационной системе. Данный способ будет эффективен только в той распределенной информационной системе, где необходимо достичь высокого уровня безопасности непосредственно внутри системы [8]. Хосты в таких системах не имеют выходов в интернет, а также не связаны между собой в сеть. В противном же случае, такой способ будет малоэффективен, поскольку имеет крайне низкую скорость и попросту неудобен как для оператора, так и для пользователей ввиду сложности журналирования и привязки хостов к определенным съемным носителям информации. В случае же, если распределенная информационная система построена таким образом, что хосты не имеют доступа друг к другу через сеть, такой способ распространения имеет место быть.

3.Способ распространения сканирующего агента в распределенной информационной системе. Данный способ будет эффективен в такой распределенной информационной системе, где необходимо распространить агента на каждый хост [9]. При этом не должна ставиться задача распространения агента в максимально быстрые сроки, поскольку с увеличение размера сети, скорость распространения будет падать и наоборот. В противном же случае использование данного способа нерационально, поскольку будет затрачено много ресурсов на «лишнее» копирование агента на хосты, которые этого не требуют, что повлечет за собой заметное увеличение времени распространения.

Анализируя вышеописанные способы распространения агента в распределенных информационных системах, можно разделить их по фактору требовательности к непосредственно самой системе и к пользователям, в том числе к оператору [10].

1)Способ распространения сканирующего агента. Данный способ является наименее требовательным к распределенной информационной системе и к пользователям данной системы, поскольку агент сам распространяется по системе без какой-либо помощи. Единственное, что требуется от оператора, это «запустить» агента в систему;

2)Способ распространения агента со списком попаданий. Данный способ требует от оператора агента точного знания, как топологии сети, так и всех используемых актуальных адресов хостов, на которые необходимо осуществить копирование агента, что уже устанавливает на оператора агента определенные требования;

3) Способ распространения агента с автозапуском. Данный способ является наиболее требовательным, поскольку для распространения агента в сети необходимо задействовать как оператора агента, так и простых пользователей. Для корректной работы оператору агента необходимо вести актуальную базу соответствия хостов и съемных носителей информации.

Заключение. В результате анализа данных способов распространения агента в распределенных информационных системах можно прийти к выводам о том, что способы распространения агента со списком попаданий и сканирующего агента являются наиболее эффективными, поскольку не требуют от оператора агента и пользователей строгих требований. ПА апробируют архитектуру с обновленными значениями параметров на локальных данных, проверяя модель по различным критериям (вычисляет проверочные метрики). Каждый ПА, завершив этот этап, оповещает РИС о том, что шаг обновления и проверки завершен. В это время ведущий агент продолжает проверять поступление сигнала «Обновление завершено» от каждого агента. Обнаружив, что все участники объединения сообщили о завершении, ведущий ПА объединяет показатели метрик от локальных проверок, чтобы вычислить общие показатели метрик.

Данное исследование выполнено при финансовой поддержке Минцифры России (грант ИБ) в рамках научного проекта, Доп. Соглашение №. 40469-05/2022-д/1 от 22.05.2023 г.

СПИСОК ЛИТЕРАТУРЫ

1. Цзэн Ю., Хайсюн С. Х. Сдерживание сетевых червей с помощью ограничения скорости для каждого процесса. 2008.
2. Роевое обучение: превратите распределенные данные в фактор успеха [Элекронный ресурс] // Hubr : [сайт]. 2021. URL: https://habr.com/ru/companies/hpe/articles/549100/ (дата обращения: 03.06.2023).
3. Лебедева А. Д. Концептуальная модель обеспечения защиты системы искусственного интеллекта мультиагентного типа // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2022) : сборник лучших докладов Всероссийской научно-технической и научно-методической конференции магистрантов и их руководителей.СПб. : СПбГУТ им. проф. М.А. Бонч-Бруевича. 2023. С. 203-206.
4. Миняев А. А., Красов А. В. Методика оценки эффективности системы защиты информации территориально-распределенных информационных систем // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 3. С. 26-32.
5. Билятдинов К. З., Красов А. В., Меняйло В. В. Исследование систем и анализ результатов: монография. СПб. : Астерион. 2019. 362 с.
6. Алгоритмы и методы защиты программного кода на базе обфускации / А. В. Красов [и др.] // I-methods. 2020. Т. 12. № 1. С. 1-12.
7. Дешевых Е. А. Ушаков И. А., Котенко И. В. Обзор средств и платформ обработки больших данных для задач мониторинга информационной безопасности // Информационная безопасность регионов России (ИБРР-2015) : Материалы конференции. СПб. : СПОИСУ, 2015. С. 67.
8. Ушаков И. А., Котенко И. В., Пелевин Д. В. Система обнаружения инсайдера в корпоративной компьютерной сети, используя алгоритмы, основанные на экспертных правилах: № 2019665940 : Свидетельство о государственной регистрации программы для ЭВМ № 2019666959 РФ. : заявл. 05.12.2019 : опубл. 17.12.2019 / заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ).
9. Коржик В. И., Кочкарев А. И., Флаксман Д. А. Система цифровых водяных знаков с повторным вложением информации по различным алгоритмам // Телекоммуникации. 2014. № 7. С. 22-33.
10. Цветков А. Ю., Эллауи Ю. Б. Поиск уязвимостей в программном обеспечении // Актуальные проблемы инфотелекоммуникаций в науке и образовании : сборник научных статей: в 4х т. СПб. : СПбГУТ им. проф. М.А. Бонч-Бруевича. 2021. Т. 1. С. 684-688.

ПОДГОТОВКА КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 811.116.1

ИНФОРМАЦИОННО-КОММУНИКАТИВНЫЕ ТЕХНОЛОГИИ В ОБУЧЕНИИ ЛИНГВИСТИЧЕСКИХ ДИСЦИПЛИН

Колоколова Лидия Петровна
Стерлитамакский филиал Уфимского университета науки и технологии
Ленина пр., 49, Стерлитамак, 453118, Россия
e-mails: kollidia@rambler.ru

Аннотация. В статье рассмотрены информационно-коммуникативные технологии, активно применяемые в учебной деятельности при изложении нового материала, на этапе закрепления изученного материала, при контроле и проверке, а также при самостоятельной работе. Процесс технологизации ускоряет передачу и освоение знаний, способствует формированию языковой картины мира, обеспечивает взаимодействие преподавателя и обучаемого в современных системах открытого и дистанционного образования.

Ключевые слова: информационно-коммуникативные технологии; компьютерное обучение; интерактивная доска; программное обеспечение.

ON THE QUESTION OF TECHNICAL MEANS OF LINGUISTIC DISCIPLINES

Kolokolova Lidia
Sterlitamak Branch of Ufa University of Science and Technology
49 Lenina Av, Sterlitamak, 453118, Russia
e-mail: kollidia@rambler.ru

Abstract. The article presents information and communication technologies, actively used in the educational activity in describing new material, at the stage of consolidation of the material, at controls and examination, as well as independent work. Process technologizing accelerate the transfer of knowledge and learning, promotes formation of a language picture of the world, provides interaction the teacher and the student in modern systems of open and distance education.

Keywords: Information and communication technologies; computer education; interactive whiteboard; software.

Введение. В современном образовании наблюдается устойчивый интерес исследователей к привлечению информационно-коммуникативных технологий в преподавание лингвистических дисциплин. Образовательная система в информационном обществе должна стать системой опережающей. Переход от консервативной образовательной системы к опережающей должен базироваться на опережающем формировании информационного пространства Российского образования.

Внедрение информационно-коммуникативных технологий (ИКТ) в образовательный процесс не столько насущная необходимость, сколько осознанный процесс технологизации рутинных процессов с целью высвобождения творческой энергии личности современного общества. Информационно-коммуникативные технологии в обучении русскому языку позволяют интегрировать в рамках одной программы тексты, графику, звук, анимацию, видеоклипы, высококачественные фотоизображения. Сфера использования информационно-коммуникативных технологий широка. Во-первых, названные технологии можно использовать при изучении нового материала: визуализация знаний (демонстрационно-энциклопедические программы, программы создания презентаций, интерактивная доска). Во-вторых, на этапе закрепления изученного материала (программы-тренажеры). В-третьих, при контроле и проверке изученного (программы для тестирования и контроля). В-четвертых, при самостоятельной работе учащихся (программы-репетиторы, электронные энциклопедии, развивающие программы). Наконец, для индивидуальной тренировки конкретных способностей учащегося: внимания, памяти, мышления и т.п.

С учетом актуального когнитивно-антропоцентрического взгляда на язык, в частности, и на весь комплекс гуманитарных наук, в целом, преподаватели-русисты считают возможным предложить некоторые новые требования и рекомендации к преподаванию русской словесности в школе и академических лингвистических курсов вузовской практике.

1.Преподавание словесности должно опираться прежде всего на классические тексты разных стилей и жанров, которые помимо фактуальной информации представляют определенную национальную культуру, особенности национальной картины мира, национального менталитета, в которых отражаются элементы духовной и материальной культуры народа в определенную историческую эпоху его существования.

2.Осуществлять преподавания словесности в соответствии с принципом системности, учить видеть в каждом отдельном факте языка сеть взаимосвязей его с фактами всех языковых уровней и экстралингвистическими категориями, понятиями и реалиями, которые получают отражение в данном языковом факте.

3.Ввести в лингвистический цикл предметов, преподаваемых в высших учебных заведениях, круг дисциплин, связанных с новыми направлениями современной филологии: лингвосемиотику, лингвокультурологию, риторику, теорию коммуникации, прикладную лингвистику.

Методологически внедрение ИКТ в процесс обучения ускоряет передачу и освоение знаний и способствует формированию языковой картины мира. Важным качеством современных ИКТ является их универсальность: они могут быть основой в организации любой деятельности, связанной информационным обменом, основой в создании общего информационного языкового пространства.

Наибольшую популярность среди технических приложений лингвистики получило компьютерное обучение. Компьютер является многофункциональным помощником, хорошим методическим инструментом наряду с другими средствами обучения. Актуальность компьютерных технологий в преподавании русской словесности налицо, так как новые условия, непринужденная обстановка, общение с компьютером, одобрение электронного помощника результатов труда имеют позитивную оценку. Студенты с разной степенью грамотности сосредотачиваются на ключевых моментах, так как машина идет вместе со студентом от незнания к знанию, акцентируя внимание на неусвоенном материале.

Для активизации учебной деятельности студентов создаются электронные учебники, позволяющие самостоятельно приобретать навыки грамотного письма, проверять собственные знания и подготавливаться к различным типам контрольных работ по русского языку.

Одним из последних по времени появления среди новых технических приложений лингвистики явилось применение интерактивных электронных досок. В процессе проведения учебных занятий использование интерактивной доски выводит на новый уровень подачу материала, создается комфортная среда при объяснении учебного материала и поддерживается атмосфера интересной познавательной беседы при обсуждении языковых явлений. В частности, в преподавании курса «Фонетическая система современного русского литературного языка» ключевым понятием является фонетическая транскрипция, представляющая собой передачу на письме графемами-буквами и специальными дополнительными знаками звучания различных по величине отрезков живой речи. Потребность в транскрипции была обусловлена зарождением сравнительно-исторического языкознания и развитием фонетики как науки. В специальных лингвистических трудах обычно применяется транскрипция Международной фонетической ассоциации, основанная на латинской графической системе. Бесспорно, используя интерактивные технические средства, можно детально представить фонетическое письмо и познакомить студентов с системой важных знаков транскрипции. Кроме того, интерактивная доска может быть использована при изучении артикуляционно-акустической системы современного русского литературного языка. Например, артикуляционная характеристика системы консонантизма предполагает следующие артикуляционные признаки:

1) характеристика согласных звуков по участию голоса и шума (сонорные и шумные);

2) характеристика согласных звуков по участию голосовых связок (шумные звонкие и шумные глухие: [б] — [п], [в] — [ф], [г] — [к], [з] — [с] и т.п);

3) характеристика согласных звуков по способу образования шума в полости рта (щелевые, смычные, аффрикаты (смычно-щелевые));

4) характеристика согласных звуков по месту образования шума в полости рта (переднеязычные (зубные, нёбные), среднеязычные, заднеязычные);

5) характеристика согласных звуков по наличию/отсутствию палатализации (мягкие и твердые: [б] — [б’], [в] — [в’], [г] — [г’], [д] — [д’] и т.п.).

Важно подчеркнуть, что применение технических средств находит отражение и в таком сложном разделе современного русского языка, как «Фонология». Фонема как основная единица фонологической системы должна быть изучена в соответствии со звуком, что дает студентам возможность понять соотношение этих единиц. В пределах одной фонемы оказывается целый ряд звуков, поэтому иногда говорят, что фонема — это группа звуков, заменяющих друг друга в различных фонетических условиях. Так, ударную фонему /а/ представляют звуки

[а], [˙а], [а˙], [ä]. Благодаря учению о чередовании звуков (альтернации звуков) И.А. Бодуэн де Куртенэ внес серьезный вклад в развитие научного представления о фонеме. Ученый исходил из положения о том, что все чередующиеся звуки в определенной позиции в одной и той же смысловой единице обладают способностью объединиться в нашем сознании в общее целое, т.е. создать идеальный портрет звука [1].

Таким образом, предложенная информация на занятиях по «Фонетике. Фонологии» современного русского литературного языка будет способствовать образному, зрительному восприятию учебного материала.

При изучении лексической системы современного русского литературного языка информационно-технические средства могут быть использованы при знакомстве с терминологическим аппаратом. В ходе занятий по разделу «Лексикология» студент должен овладеть определенным запасом довольно сложных лингвистических терминов, уметь профессионально квалифицировать языковые факты, формировать лингвистическое чутьё. Терминологический словарь составляет теоретическую основу изучаемой дисциплины, включает в себя словарные статьи по наиболее частотным терминам с дефинициями по теме «Лексикология. Фразеология. Лексикография», встречающимся в вузовских учебниках лингвистического цикла, лекционных курсах, на практических и семинарских занятиях, при изучении студентами курса сравнительной лексикологии и в школьной практике, при чтении периодических изданий не только популярных, но и академического типа. Помимо толкования терминов в терминологическом словаре приводятся примеры из ряда языков, особенно из истории развития русского языка, в его литературном варианте, просторечии и диалектах. Особенностью данного словаря является то, что он многофункционален (перевод терминов на изучаемые языки предваряется этимологическими сведениями). Например, в словарной статье «основные признаки слова (по теории А.И. Смирницкого)» представлены фонетические, лексико-грамматические и лексико-семантические признаки слова. В свою очередь, к фонетическим признакам слова относятся следующие особенности слова: 1) цельность и единооформленность; 2) фонетическая оформленность; 3) недвуударность; 4) непроницаемость; 5) постоянство звучания и значения.

Лексико-грамматическим признакам слова включают такие свойства слова, как 1) изолируемость; 2) цельность и единооформленность; 3) лексико-грамматическая отнесенность. К лексико-семантическим признакам относят 1) фразеологичность; 2) номинативность; 3) воспроизводимость; 4) семантическая валентность [2].

Все указанные признаки в терминологическом словаре представляют собой семантическое пространство, которое студент должен рассмотреть в течение определенного периода времени и использовать данную информацию на практических и семинарских занятиях. Более того, терминологический словарь содержит порядок и образец лексических, фразеологических и лексикографических анализов, используемых студентами при выполнении лабораторных работ.

Технические средства также успешно находят применение при составлении словарей разного типа. Например, по теме «Лексикография» важно учитывать следующие этапы работы: 1) предмет, объект, задачи изучаемой проблемы; 2) словарь, структура словаря; 3) понятие словарной статьи, структура словарной статьи; 4) функции словарей; 5) типология словарей; 6) лексикографический анализ слова. Интерактивная доска даёт возможность представить исследовательскую работу в целом и затем поэтапно рассматривать каждый отдельный информационный блок. Особенно этот вид деятельности характерен при анализе схемы комплексного лексикографического анализа, включающего следующие виды деятельности: 1) дать полное название словаря; 2) указать, выходные данные (авторы, год издания, место издания, издательство); 3) определить объект описания; 4) охарактеризовать структуру словарных статей и их содержание; 5) определить принцип построения словаря; 6) определить структуру словаря; 7) определить, на кого рассчитан словарь; 8) охарактеризовать объём словаря и специфику его оформления: таблицы, схемы, карты, иллюстрации, фото ит.п.; 9) описать словарную статью [3].

Более того, интерактивная доска позволяет демонстрировать слайды и видео, рисовать и чертить различные схемы, вносить любые изменения и сохранять их в виде компьютерных файлов для дальнейшего редактирования.

Заключение. Примером успешной реализации ИКТ в современном учебном процессе стало появление Интернета — всемирной компьютерной передачи с ее практически неограниченными возможностями сбора и хранения информации, передачи ее индивидуально каждому пользователю. Технология Интернет как среда коммуникации является посредником во включении студента в сетевые структуры, на основе которого он получает возможность эффективно использовать информацию, предоставляя ее заинтересованным людям в кратчайшие сроки. Таким образом, эффективность обучения может быть значительно повышена с помощью ИКТ, применяемых в различных оптимальных для данных занятий сочетаниях с другими средствами обучения.

СПИСОК ЛИТЕРАТУРЫ

1. Колоколова Л. П. Современный русский литературный язык: Фонетика : учеб. пособие для студ. высш. учеб. заведений. Уфа : РИЦ БашГУ, 2010. 143 с.
2. Колоколова Л. П. Современный русский язык. Лексикология. Фразеология. Лексикография: Учебное пособие для филол. фак. вузов. СПб. : Политехника-сервис, 2012. 147 с.
3. Современный русский литературный язык и методика его преподавания: учебный словарь. М. : ИПЦ Маска, 2015. 383 с.

УДК 811.116.1

ТЕХНИЧЕСКИЕ СРЕДСТВА ОБУЧЕНИЯ КАК ИНСТРУМЕНТАЛЬНАЯ СРЕДА ПОДДЕРЖКИ УЧЕБНОГО ПРОЦЕССА ПОДГОТОВКИ ФИЛОЛОГОВ

Колоколова Лидия Петровна
Стерлитамакский филиал Уфимского университета науки и технологии
Ленина пр., 49, Стерлитамак, 453118, Россия
e-mail: kollidia@rambler.ru

Аннотация. Рассматриваются технические средства обучения, активно применяемые в учебной деятельности при изложении нового материала, на этапе закрепления изученного материала, при контроле и проверке, а также при самостоятельной работе. Процесс технологизации ускоряет передачу и освоение знаний, способствует формированию языковой картины мира, обеспечивает взаимодействие преподавателя и обучаемого в современных системах открытого и дистанционного образования.

Ключевые слова: информационно-коммуникативные технологии; компьютерное обучение; интерактивная доска; программное обеспечение.

TECHNICAL TEACHING TOOLS AS A TOOL ENVIRONMENT FOR SUPPORTING THE EDUCATIONAL PROCESS OF PHILOLOGISTS TRAINING

Kolokolova Lidia
Sterlitamak Branch of Ufa University of Science and Technology
49 Lenina Av, Sterlitamak, 453118, Russia
e-mail: kollidia@rambler.ru

Abstract. Technical training aids are considered, actively used in the educational activity in describing new material, at the stage of consolidation of the material, at controls and examination, as well as independent work. Process technologizing accelerate the transfer of knowledge and learning, promotes formation of a language picture of the world, provides interaction the teacher and the student in modern systems of open and distance education.

Keywords: information and communication technologies; computer education; interactive whiteboard; software.

Введение. В российской системе образования наблюдается устойчивый интерес исследователей к привлечению информационно-коммуникативных технологий в преподавание лингвистических дисциплин. Внедрение технических средств обучения в образовательный процесс не столько насущная необходимость, сколько осознанный процесс технологизации рутинных процессов с целью высвобождения творческой энергии личности современного общества. Информационно-коммуникативные технологии в обучении русскому языку позволяют интегрировать в рамках одной программы тексты, графику, звук, анимацию, видеоклипы, высококачественные фотоизображения. Сфера использования информационно-коммуникативных технологий широка. Во-первых, названные технологии можно использовать при изучении нового материала: визуализация знаний (демонстрационно-энциклопедические программы, программы создания презентаций, интерактивная доска). Во-вторых, на этапе закрепления изученного материала (программы-тренажеры). В-третьих, при контроле и проверке изученного (программы для тестирования и контроля). В-четвертых, при самостоятельной работе учащихся (программы-репетиторы, электронные энциклопедии, развивающие программы). Наконец, для индивидуальной тренировки конкретных способностей учащегося: внимания, памяти, мышления и т. п.

Таким образом, одной из наиболее важных задач, стоящих перед российской системой образования, является обеспечение доступности и качества образовательного процесса, итогом которого должно быть формирование конкурентоспособного выпускника. Данная цель не может быть достигнута без широкого внедрения, без опоры на современные информационные технологии в образовании.

С учетом актуального когнитивно-антропоцентрического взгляда на язык, в частности, и на весь комплекс гуманитарных наук, в целом, преподаватели-русисты считают возможным предложить некоторые новые требования и рекомендации к преподаванию русской словесности в школе и академических лингвистических курсов вузовской практике.

1.Преподавание словесности должно опираться прежде всего на классические тексты разных стилей и жанров, которые помимо фактуальной информации представляют определенную национальную культуру, особенности национальной картины мира, национального менталитета, в которых отражаются элементы духовной и материальной культуры народа в определенную историческую эпоху его существования.

2.Осуществлять преподавания словесности в соответствии с принципом системности, учить видеть в каждом отдельном факте языка сеть взаимосвязей его с фактами всех языковых уровней и экстралингвистическими категориями, понятиями и реалиями, которые получают отражение в данном языковом факте.

3.Ввести в лингвистический цикл предметов, преподаваемых в высших учебных заведениях, круг дисциплин, связанных с новыми направлениями современной филологии: лингвосемиотику, лингвокультурология, риторику, теорию коммуникации, прикладную лингвистику.

Методологически внедрение технических средств в процесс обучения ускоряет передачу и освоение знаний и способствует формированию языковой картины мира. Важным качеством современных технических средств является их универсальность: они могут быть основой в организации любой деятельности, связанной информационным обменом, основой в создании общего информационного языкового пространства.

Наибольшую популярность среди технических приложений лингвистики получило компьютерное обучение. Компьютер является многофункциональным помощником, хорошим методическим инструментом наряду с другими средствами обучения. Актуальность компьютерных технологий в преподавании русской словесности налицо, так как новые условия, непринужденная обстановка, общение с компьютером, одобрение электронного помощника результатов труда имеют позитивную оценку. Студенты с разной степенью грамотности сосредотачиваются на ключевых моментах, так как машина идет вместе со студентом от незнания к знанию, акцентируя внимание на неусвоенном материале.

Для активизации учебной деятельности студентов создаются электронные учебники, позволяющие самостоятельно приобретать навыки грамотного письма, проверять собственные знания и подготавливаться к различным типам контрольных работ по русского языку.

Одним из последних по времени появления среди новых технических приложений лингвистики явилось применение интерактивных электронных досок. В процессе проведения учебных занятий использование интерактивной доски выводит на новый уровень подачу материала, создается комфортная среда при объяснении учебного материала и поддерживается атмосфера интересной познавательной беседы при обсуждении языковых явлений. В частности, в преподавании курса «Фонетическая система современного русского литературного языка» ключевым понятием является фонетическая транскрипция, представляющая собой передачу на письме графемами-буквами и специальными дополнительными знаками звучания различных по величине отрезков живой речи. Потребность в транскрипции была обусловлена зарождением сравнительно-исторического языкознания и развитием фонетики как науки. В специальных лингвистических трудах обычно применяется транскрипция Международной фонетической ассоциации, основанная на латинской графической системе. Бесспорно, используя интерактивные технические средства, можно детально представить фонетическое письмо и познакомить студентов с системой важных знаков транскрипции. Кроме того, интерактивная доска может быть использована при изучении артикуляционно-акустической системы современного русского литературного языка. Например, артикуляционная характеристика системы вокализма предполагает следующие артикуляционные признаки:

1)характеристика гласных звуков по степени подъёма спинки языка (гласные верхнего подъема: [и], [ы], [у]; гласные среднего подъема: [э], [о]; гласные нижнего подъема: [а]] и т.п);

2)характеристика гласных звуков по месту подъёма спинки языка (гласные переднего ряда: [и], [э]; гласные среднего ряда: [ы], [а]; гласные заднего ряда: [у], [о] и т.п);

3)характеристика гласных звуков по наличию/отсутствию лабиализации (лабиализованные и нелабиализованные гласные);

4)характеристика гласных звуков по наличию/отсутствию ударения (гласные полного образования и гласные редуцированные).

Таким образом, предложенная информация на занятиях по фонетической системе современного русского литературного языка будет способствовать образному, зрительному восприятию учебного материала.

При изучении лексической системы современного русского литературного языка информационно-технические средства могут быть использованы при знакомстве с терминологическим аппаратом. В ходе занятий по разделу «Лексикология» студент должен овладеть определенным запасом довольно сложных лингвистических терминов, уметь профессионально квалифицировать языковые факты, формировать лингвистическое чутьё. Терминологический словарь составляет теоретическую основу изучаемой дисциплины, включает в себя словарные статьи по наиболее частотным терминам с дефинициями по теме «Лексикология. Фразеология. Лексикография», встречающимся в вузовских учебниках лингвистического цикла, лекционных курсах, на практических и семинарских занятиях, при изучении студентами курса сравнительной лексикологии и в школьной практике, при чтении периодических изданий не только популярных, но и академического типа. Помимо толкования терминов в терминологическом словаре приводятся примеры из ряда языков, особенно из истории развития русского языка, в его литературном варианте, просторечии и диалектах. Особенностью данного словаря является то, что он многофункционален (перевод терминов на изучаемые языки предваряется этимологическими сведениями).

Например, в словарной статье «основные признаки слова (по теории А. И. Смирницкого)» представлены фонетические, лексико-грамматические и лексико-семантические признаки слова. В свою очередь, к фонетическим признакам слова относятся следующие особенности слова: 1) цельность и единооформленность; 2) фонетическая оформленность; 3) недвуударность; 4) непроницаемость; 5) постоянство звучания и значения.

Лексико-грамматическим признакам слова включают такие свойства слова, как 1) изолируемость; 2) цельность и единооформленность; 3) лексико-грамматическая отнесенность. К лексико-семантическим признакам относят 1) фразеологичность; 2) номинативность; 3) воспроизводимость; 4) семантическая валентность [2].

Все указанные признаки в терминологическом словаре представляют собой семантическое пространство, которое студент должен рассмотреть в течение определенного периода времени и использовать данную информацию на практических и семинарских занятиях. Более того, терминологический словарь содержит порядок и образец лексических, фразеологических и лексикографических анализов, используемых студентами при выполнении лабораторных работ.

Технические средства также успешно находят применение при составлении словарей разного типа. Например, по теме «Лексикография» важно учитывать следующие этапы работы: 1) предмет, объект, задачи изучаемой проблемы; 2) словарь, структура словаря; 3) понятие словарной статьи, структура словарной статьи; 4) функции словарей; 5) типология словарей; 6) лексикографический анализ слова. Интерактивная доска даёт возможность представить исследовательскую работу в целом и затем поэтапно рассматривать каждый отдельный информационный блок. Особенно этот вид деятельности характерен при анализе схемы комплексного лексикографического анализа, включающего следующие виды деятельности: 1) дать полное название словаря; 2) указать, выходные данные (автор (ы), год издания, место издания, издательство); 3) определить объект описания; 4) охарактеризовать структуру словарных статей и их содержание; 5) определить принцип построения словаря; 6) определить структуру словаря; 7) определить, на кого рассчитан словарь; 8) охарактеризовать объём словаря и специфику его оформления: таблицы, схемы, карты, иллюстрации, фото ит.п.; 9) описать словарную статью [3].

Более того, интерактивная доска позволяет демонстрировать слайды и видео, рисовать и чертить различные схемы, вносить любые изменения и сохранять их в виде компьютерных файлов для дальнейшего редактирования. Совершенно очевидно, что технические средства обучения — это широкий спектр цифровых технологий, используемых для создания, передачи и распространения информации и оказания услуг (компьютерное оборудование, программное обеспечение, телефонные линии, сотовая связь, электронная почта, сотовые и спутниковые технологии, сети беспроводной и кабельной связи, мультимедийные средства.

Примером успешной реализации технических средств обучения в современном учебном процессе стало появление Интернета — всемирной компьютерной передачи с ее практически неограниченными возможностями сбора и хранения информации, передачи ее индивидуально каждому пользователю. Технология Интернет как среда коммуникации является посредником во включении студента в сетевые структуры, на основе которого он получает возможность эффективно использовать информацию, предоставляя ее заинтересованным людям в кратчайшие сроки.

Технические средства активно используются в рамках дисциплины «Корпусная лингвистика», цель которой научить специалистов в области прикладной филологии базовым технологиям работы с различными корпусами с целью быстрого получения необходимого языкового материала. Национальный корпус русского языка, позволяющий по заданным лингвистическим — семантическим и грамматическим — параметрам в считанные минуты получить тысячи контекстов (в корпусе имеется возможность поиска и по заданной языковой единице разного формата).

Более того, информационно-коммуникативные технологии активно используются при знакомстве и историей создания электронных языковых корпусов, например, Брауновский корпус, Британский национальный корпус, Упсальский корпус русского языка, Хельсинкский аннотированный корпус русского языка, Фундаментальные корпусы других славянских языков: Чешский национальный корпус, Словацкий национальный корпус, Хорватский национальный корпус и др. [1].

Также студенты и магистранты могут работать с сайтом, посвященным семинару по корпусной лингвистике, побывать на форуме, где рассматриваются ключевые вопросы прикладной лингвистики, послушать видеолекцию В. А. Плунгяна «Почему современная лингвистика должна быть лингвистикой корпусов» и т. д.

Заключение. Совершенно очевидно, эффективность обучения может быть значительно повышена с помощью технических средств обучения, применяемых в различных оптимальных для данных занятий сочетаниях с другими средствами обучения.

СПИСОК ЛИТЕРАТУРЫ

1. Груднева Е.В. Корпусная лингвистика : учеб. пособие. 2-е изд., стер. М. : ФЛИНТА, 2012. 165 с.
2. Колоколова Л. П. Современный русский язык. Лексикология. Фразеология. Лексикография: Учебное пособие для филол. фак. вузов. СПб.: Политехника-сервис, 2012. 147 с.
3. Современный русский литературный язык и методика его преподавания: Учебный словарь. М. : ИПЦ «Маска», 2015. 383 с.

УДК 004 056.5

СОЦИАЛЬНЫЕ СЕТИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ВЫСШЕЕ ОБРАЗОВАНИЕ

Кононов Олег Александрович, Кононова Ольга Васильевна
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, Санкт-Петербург, 190000, Россия
e-mail: o2kon@mail.ru

Аннотация. В статье рассмотрены актуальные вопросы использования социальных сетей в высших учебных заведениях.

Ключевые слова: социальные сети; информационная безопасность; информационно-коммуникационные технологии; образовательная среда; высшее образование.

SOCIAL NETWORKS, INFORMATION SECURITY AND HIGHER EDUCATION

Kononov Oleg, Kononova Olga
Saint-Petersburg State University of Aerospace Instrumentation
67 Bolshaya Morskaya St, St. Petersburg,190000, Russia
e-mail: o2kon@mail.ru

Abstract. In article topical issues of using social networks in higher educational institutions are considered.

Keywords: social networks; information security; information and communication technologies; educational sphere; higher education.

Введение. Социальные сети в настоящее время для многих являются основным местом проведения времени в Интернете и позволяют совершенно незнакомым людям найти общий язык, как посредством общения, так и посредством открытой информации, которую оставляют пользователи. В тоже время социальные сети можно рассматривать как инструмент для продвижения как коммерческих, так и социальных проектов [1].

Активные пользователи и целевая аудитория. На начало 2023 года количество пользователей Интернета в мире составило 5,16 миллиарда или 64,4% мирового населения имеют доступ в Интернет. За год количество выросло на 1,9 %. При этом в 4 странах проникновение Интернета находится на уровне более 99, а в 24 странах — от 90 %. В России этот показатель составляет 88,2 % [2].

Почти 6 из 10 Интернет-пользователей трудоспособного возраста (57,8 %) обращаются к онлайн-ресурсам в поисках информации. Другими причинами использования Интернета являются: поддержание связи с друзьями и семьей (53,7 %); стремление быть в курсе новостей и текущих событий (50,9 %); желание просмотра видеороликов, сериалов или кино (49,7 %).

На начало 2023 года соцсети насчитывали 4,76 миллиарда пользователей, это почти 60 % от мирового населения, хотя темпы роста аудитории замедлились — за год составили всего 3 %. С начала пандемии общая аудитория соцсетей увеличилась почти на 30 %, что эквивалентно более чем 1 миллиарду новых пользователей за последние 3 года [2].

Темпы роста аудитории в последние годы также указывают на то, что COVID-19 ускорил распространение социальных сетей. При этом темпы роста в период с 2020 по 2021 год были почти в 2 раза выше, чем в предыдущие 12 месяцев, и рост продолжался двузначными темпами в период с 2021 по 2022 год. Однако за 2022 год темп замедлился и сейчас находится на самом низком уровне за всю историю наблюдений, при этом число пользователей всё ещё растет.

Сегодня люди проводят в соцсетях больше времени, чем когда-либо. При этом увеличение времени пребывания в соцсетях произошло на фоне сокращения общего количества времени, которое люди проводят онлайн. Так среднестатистический Интернет-пользователь трудоспособного возраста теперь тратит чуть больше 2,5 часов в день на социальные сети [2]. И хотя среднемировое значение всего на 3 минуты больше прошлогоднего, рост всё ещё наблюдается.

На сегодняшний день в мире существует множество социальных сетей от мега популярных и до совершенно неизвестных, в мире в целом насчитывается социальных сетей около пятисот. Одни сети развиваются, другие, наоборот, сокращают свою деятельность, есть социальные сети тематические, а есть просто для общения, выбор очень и очень велик.

Однако, нужно заметить, что лишь небольшая часть из них является международными. Всего таковых около 10 штук. К ним относятся, например, FaceBook, YouTube, WhatsApp, Instagram, WeChat и другие. В большинстве стран есть собственные социальные сети, такие, например, как российские Одноклассники.

В январе 2023 года в Российской Федерации насчитывалось 106,0 миллионов пользователей социальных сетей. Предполагаемая статистика использования цифровых устройств и Интернета в 2023 году жителями России приведена ниже [2].

- 88,2 % уровень проникновения Интернета в РФ;
- 92 % пользователей Интернета, используют смартфоны;

- 21,9 % прирост скорости мобильного Интернета;
- 73,3 % населения России есть в соцсетях;
- 8 часов — среднее время нахождения в сети;
- 10 % снижение трафика с десктопов и ноутбуков;
- 18 % прирост мобильного трафика;
- 18,5 % снижение трафика на поисковик Google из России;
- 81,7 % снижение трафика в Instagram;
- 36 % увеличение трафика Вконтакте;
- 56 % населения РФ есть в VK;
- 68 млн человек делают покупки в Интернет;
- 31 % снижение расходов на digital-маркетинг в России.

Среднесуточный охват пользователей соцсетей и мессенджеров в России [3] представлен на рис. 1.

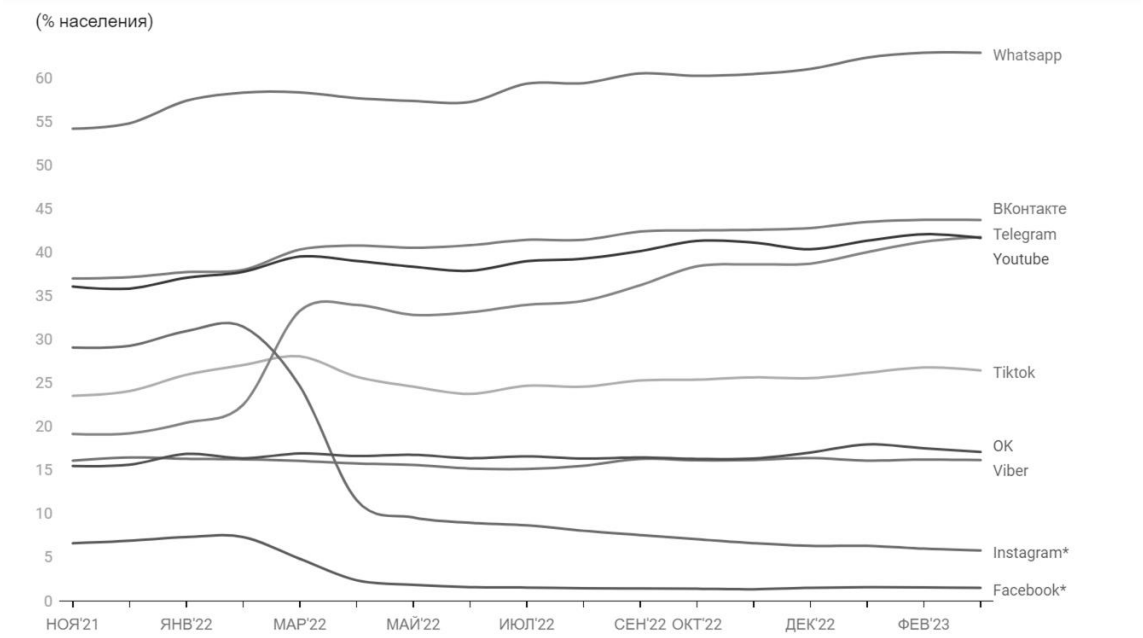


Рис. 1. Среднесуточный охват пользователей соцсетей и мессенджеров в России

Согласно графикам на рис. 1 в соцсеть Instagram в феврале 2023 году в среднем хотя бы раз в день (принадлежат компании Meta, которая была признана экстремистской и запрещена на территории России) заходили 6 % россиян старше 12 лет, что в 5 раз меньше, чем в феврале 2022-го (тогда среднесуточный охват сервиса составлял 31 %). Аудитория Facebook (также принадлежит Meta) за год снизилась в 3,5 раза — с 7 % до 2 %. Россияне также стали проводить меньше времени в Instagram и Facebook. Время потребления в первой соцсети за год упало в 2,4 раза, до 17 минут в день, второй — в 3 раза, до 5 минут. Посещаемость Facebook и Instagram в России резко упала после блокировки сервисов Роскомнадзором.

Главными бенефициарами блокировки Instagram и Facebook в России стали Telegram и «ВКонтакте». Среднесуточный охват Telegram в феврале 2023 года вырос к аналогичному месяцу предыдущего года почти в 1,8 раза — с 23 до 41 %. У «ВКонтакте» этот показатель увеличился в 1,15 раза — до 44 %, а у «Одноклассников» в 1,12 раза — до 18 %.

Охват TikTok остался прежним — 27 %, несмотря на ограничения для российских пользователей. В прошлом марте соцсеть запретила россиянам выкладывать новый контент и проводить прямые эфиры из-за закона о фейках про армию.

Кроме того, на динамику среднесуточного охвата пользователей соцсетей и мессенджеров в России будет влиять процесс совершенствования законодательства в области информационной безопасности и, в частности, например, Федеральный закон от 31.07.2023 № 408-ФЗ «О внесении изменения в Федеральный закон «Об информации, информационных технологиях и о защите информации» [4]. Таким образом, ужесточена ответственность владельцев площадок за нарушение их обязанностей.

Социальные сети стали своего рода Интернет-пристанищем, где каждый может найти техническую и социальную базу для создания своего виртуального образа. При этом каждый пользователь получает возможность не просто общаться и творить, но и делиться плодами своего творчества с многомиллионной аудиторией социальной сети [1].

Социальная среда вуза. В социальные сети приходят люди самых разных возрастов, политических взглядов, интересов, увлечений. Поэтому сайт любого направления будет интересен той или иной группе участников. Студенты, выпускники являются одними из наиболее активных пользователей компьютерных технологий вообще, а социальные сети — неотъемлемая часть этих технологий. Согласно ряду проведенных социологических исследований типичного пользователя социальной сети можно представить как человека 18-34 лет, получающего либо получившего высшее образование. Данная аудитория довольно обширна [1].

Сегодня создание социальной среды в вузе, мотивирующей сотрудников и студентов на постоянный рост собственных знаний и постоянное совершенствование процессов получения и закрепления новых знаний, является необходимым условием процветания.

В настоящее время в государственных и корпоративных, гражданских, научных, тематических и профессиональных сообществах приобрели популярность различные формы сетевого общения с использованием ИКТ, которые применяются в различных областях деятельности организаций, таких, как распространение информации внутри компании, коллективная разработка проектов, связи с клиентами, управление контентом, маркетинг и PR, а также в управлении знаниями [5].

Применительно к вузам основными процессами, где происходит извлечение, накопление и распространение знаний являются учебный процесс, научные исследования и разработки, материализация и коммерциализация результатов НИР и НИОКР, разработка учебных материалов.

Современный вуз по своему годовому финансовому обороту, по размерам, по объему и стоимости основных средств, по структуре ничем не отличается от крупных предприятий производства или сферы услуг.

Роли различных форм сетевого общения применительно к вузам приведены ниже [6]:

– создание книг и научных работ, каталогов ошибок и трудностей по проектам и направлениям, инструкций по процессам и программному обеспечению с реальными практическими примерами пользователей, документации по процессам;

– создание простых электронных курсов с комментариями слушателей, организацию коллективной работы слушателей, базы ресурсов и документов по тематике обучения;

– организация совместной работы над проектами, обсуждение проблем сотрудниками разного уровня и из разных регионов, мониторинг нового в отрасли, отслеживание интересов и профессионального развития сотрудников;

– обеспечение обучения на основе свежих ресурсов и формирование мнения о происходящем в обществе, работа группы над проектом в процессе обучения, подборка источников и построение взаимосвязи между ними, самостоятельная работа слушателей.

– создание информации о новых инструкциях и документах, рассылка новостей компании, рассылка вопросов сотрудников и проблем проектов, запись трансляций выступлений руководителей, сотрудников, организация асинхронных аудио-конференций;

– размещение информации о новостях курса или программы, информации о новых курсах, новых возможностях обучения, подписка на полезные для курса источники, вопросы слушателей, аудио-лекции, организация использования информации в свободном доступе для обучения.

Социальная структура. Социальную сеть можно определить как социальную структуру, объединяющую отдельных людей или даже целые организации [6].

Социальная сеть показывает, каким образом ее участники связаны друг с другом теми или иными отношениями — от случайных знакомств до тесных семейных связей.

В вузе объектами внимания должны становиться разномасштабные группы людей, причем в первую очередь такими объектами должны быть учебные группы студентов.

Связи в группах могут быть прямыми или косвенными, сильными или слабыми, односторонними или двусторонними. Персоны с большим количеством прямых связей играют важную роль в структуре взаимоотношений данной группы, часто демонстрируют большую продуктивность работы и большую удовлетворенность ею, чем участники сети с меньшим числом прямых связей. Эти персоны выполняют функции основных посредников между людьми, соединенными косвенными, непрямыми связями. Такое посредничество может оказывать как положительное, так и отрицательное влияние на взаимоотношения в социальной сети, помогая или, наоборот, препятствуя распространению информации либо налаживанию отношений между различными подгруппами сети. В структуре взаимоотношений данной группы желательно наличие преподавателей, включенных внутрь сетевого общения. Преподаватель не только является источником информации для остальных членов группы, но и сам черпает нужные ему сведения, обращаясь к коллегам. Преподавательский состав, включенный внутрь сетевого общения, должен существенно увеличить продуктивность работы группы и повысить удовлетворенность ею.

Важно соблюдать баланс между слабыми и сильными связями в социальных сетях — первые дают дополнительные источники инноваций, а вторые помогают создавать и поддерживать необходимый рабочий микроклимат.

Социальные сети могут выявить неформальные связи между участниками группы, что может оказаться полезным в организации образовательного процесса.

Социальные сети помогают наводить мосты между иерархической организационной структурой ВУЗа и неформальной горизонтальной структурой социальных связей для достижения стратегических целей обучения.

Исследование социальных сетей открывает резервы повышения эффективности совместной работы, позволяет лучше использовать таланты и знания участников группы, определять узкие места при реализации тех или иных решений, внедрении новаторских подходов и технологий.

Для идентификации социальных сетей с целью последующего анализа используются, как правило, интервью, опросы, специальные методы наблюдений. Множатся сайты, поддерживающие виртуальные сообщества.

ВУЗ объединяет людей, которые заинтересованы в приобретении и развитии знаний в определенной области, их использовании на практике, и для достижения этих целей постоянно взаимодействуют друг с другом. Вузовские сообщества, по сути, и осуществляют сегодня управление явным и неявным знанием. Члены вузовского сообщества хорошо понимают друг друга, поскольку работают над схожими проблемами. Они способны оценить уровень квалификации, проблемы и озарения коллег, получить друг от друга недостающие им знания. Эти знания являются основой для решения стоящих перед ними задач и базой для формирования новых знаний. А технологии, системы и структуры накопления и доступа к информации, такие как внутрикорпоративные сети, порталы и программные продукты совместной работы, обеспечивают инструментальную поддержку управления знаниями [6].

Опасности социальных сетей. Однако необходимо учитывать, что социальные сети, обеспечивая поддержание связи между людьми; создание групп по интересам, превращают нашу жизнь в открытую книгу, где информацию о нас могут прочесть не только наши друзья, но и недоброжелатели. Поэтому необходимо помнить о возможных угрозах со стороны социальных сетей.

Главные опасности, таящиеся в социальных сетях [6]:

- проблемы конфиденциальности;
- хакерство и взлом паролей;
- неадекватный взгляд на окружающий мир;
- Интернет-зависимость;
- потенциальные проблемы на рабочем месте;
- потенциальные проблемы дома.

Список может пополняться вместе с тем, как мы будем продолжать пользоваться социальными сетями, а они, в свою очередь, будут развиваться самым непредсказуемым образом вместе с новыми технологиями.

Согласно данным опроса [7], в общей сложности более двух третей сотрудников российских компаний открыто обсуждают рабочие вопросы с третьими лицами, причем 19 % из них признались, что спокойно могут описать нюансы своей деятельности в социальных сетях. 29 % «ради шутки» могут поделиться с друзьями забавными скриншотами или цитатами из переписки, а 24 % делятся только общими моментами, не затрагивающими деятельность предприятия. При этом основным корпоративным способом коммуникации в большинстве компаний является применение одного из стандартных мессенджеров (43 %) или этот способ никак не оговаривается (23 %). Только 21 % предприятий запрещают использование сервисов быстрых сообщений на рабочих устройствах, а в 13 % случаев используется внутренний корпоративный чат на рабочем портале. Далеко не во всех компаниях всё ПО устанавливается только через специальные технические службы и приобретаются лицензионные версии программ. Более половины (62 %) участников опроса призналась, что на домашнем компьютере обновляют ПО крайне редко, и только 26 % и 12 % соответственно следуют подсказкам системы или следят за безопасностью осознанно, своевременно обновляя программы и приобретая лицензионные версии.

Опрос также показал, что каждый второй работник (52 %) берет время от времени работу на дом, придумывая «обходные варианты», поскольку скачивать документы с рабочих устройств не разрешено. Около 38 % отметили, что работать из дома в их организации не принято, а остальные (10 %) спокойно могут взять работу домой, и, не скрываясь от начальства, воспользоваться необходимой внутренней информацией.

Особенно актуальной проблемой информационная безопасность становится в условиях перехода на удаленную занятость. При этом наряду с использованием специальных программных средств необходимо также уделять внимание вопросам совершенствования корпоративной культуры.

Применительно к вузам особое значение в борьбе с отмеченными угрозами приобретает практика соблюдения норм компьютерной этики, поскольку саморегуляция на основе нравственных норм является одним из естественных и эффективных способов защиты от антисоциального поведения пользователей социальных сетей [8].

Оценка применения социальных сетей в учебном процессе. Возможности применения социальных сетей в учебном процессе можно оценить по результатам проведенного в университете опроса, на основе которого был составлен график сравнения использования социальных сетей до и после пандемии (рис. 2).

Как показали результаты исследования, во время пандемии коронавируса социальные сети стали важным инструментом поддержания коммуникаций и обеспечения непрерывного обучения. Опыт использования

социальных сетей во время пандемии лёг в основу проекта «Цифровые Кафедры» в Санкт-Петербургском государственном университете аэрокосмического приборостроения, в рамках программы стратегического академического лидерства «Приоритет-2030».

В учебном 2022/2023 году студенты, попавшие в проект, бесплатно обучались востребованной цифровой профессии и получили не один, а целых два диплома. Обучение на «Цифровой Кафедре» проходило параллельно с освоением основной специальности, занятия были встроены в расписание. Это расширяет горизонт возможностей студентов после выпуска, повышает их востребованность и конкурентоспособность на рынке труда.

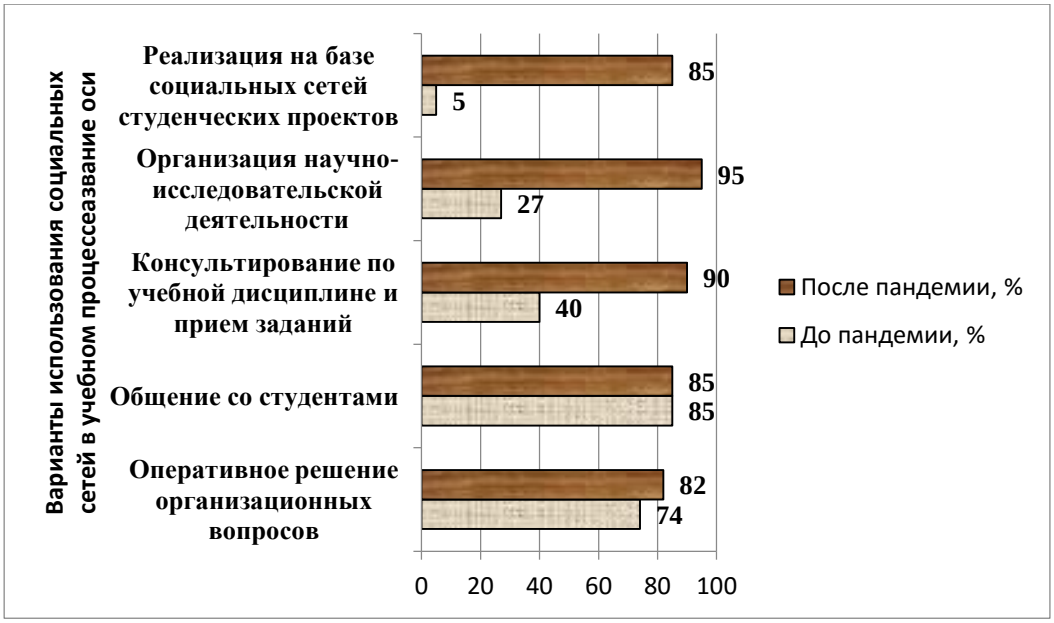


Рис. 2. Уровень использования социальных сетей в учебном процессе

Следует обратить внимание, что социальные сети в учебном процессе практически не влияют на мотивацию студентов, однако они увеличивают возможности продвижения соответствующего вуза. В тоже время они позволяют усилить влияние на социальный, психологический и этический аспекты учебного процесса в виде:

– увеличения частоты прохождения узконаправленных онлайн-курсов и, как следствие, расширения компетенций студентов в их профессиональном самоопределении;

– усиления интереса к дисциплинам, возрастания вовлеченности студентов в учебный процесс, развития креативности;

– приобретения опыта применения норм компьютерной этики.

Заключение. Опыт использования социальных сетей во время пандемии дал новый импульс развитию применения социальных сетей в образовании. Социальные сети, как элемент информационно-коммуникационных технологий при их умелом использовании могут и должны стать мощным инновационным ресурсом совершенствования различных сфер жизни, включая образование, однако необходимо учитывать таящиеся в них опасности.

СПИСОК ЛИТЕРАТУРЫ

1. Кононов О. А. Кононова О. В. Вопросы информационных отношений в подготовке кадров // Региональная информатика и информационная безопасность : сборник трудов. Вып. 10. СПб. : СПОИСУ, 2021. С. 225-228.
2. Статистика интернета и соцсетей на 2023 год — цифры и тренды в мире и в России. [Электронный ресурс]. URL: https://www.web-canape.ru/business/statistika-interneta-i-socsetej-na-2023-god-cifry-i-trendy-v-mire-i-v-rossii/ (дата обращения 18.08.2023).
3. Среднесуточный охват пользователей соцсетей и мессенджеров в России. [Электронный ресурс]. URL: https://www.tadviser.ru/images/8/89/Telegram_ohvat.png (дата обращения 18.08.2023).
4. О внесении изменения в Федеральный закон «Об информации, информационных технологиях и о защите информации»: Фед. закон от 31.07.2023 г. № 408-ФЗ. [Электронный ресурс]. URL: https://www.tadviser.ru/images/4/46/000120230731v0021.pdf. (дата обращения 19.08.2023).
5. Кононов О. А. Кононова О. В. Социальные сети и управление знаниями // Региональная информатика и информационная безопасность : сборник трудов. Вып. 2. СПб.: СПОИСУ, 2016. С. 245-249.
6. Кононов О. А., Кононова О. В. О социальных сетях вузов и информационной безопасности // Региональная информатика и информационная безопасность : сборник трудов. Выпуск 3. СПб.: СПОИСУ, 2017. С. 115-119.
7. Утечки данных в соцсетях [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/ (дата обращения 18.08.2023).
8. Кононов О. А., Кононова О. В. Социальные и этические аспекты обеспечения информационной безопасности // Проблемы управления. М. : ИПУ РАН, 2009. № 1. С. 76-80.

УДК 004 : 004.05 : 004.5

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ АВТОМАТИЗАЦИИ ПРОЦЕССОВ ОБУЧЕНИЯ IT-СПЕЦИАЛИСТОВ С УЧЕТОМ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сафронова Мария Вадимовна
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mail: maryaeihteen@gmail.com

Аннотация. В данной статье описываются этапы проектирования и разработки модулей «База данных», «Администрирование» и «Чат» для системы автоматизации процессов обучения IT специалистов, а также выбранные программные меры защиты от компьютерных атак.

Ключевые слова: автоматизация процессов; проектирование; разработка; обучение IT специалистов; информационная безопасность.

SOFTWARE OF TRAINING PROCESSES AUTOMATION OF IT SPECIALISTS WITH REQUIREMENTS OF INFORMATION SECURITY

Safronova Marya
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mail: maryaeihteen@gmail.com

Abstract. This article describes the stages of design and development of the modules «Database», «Administration» and «Chat» for the system of automation of IT specialists' training processes, as well as selected software protection measures against computer attacks.

Keywords: process automation; design; development; training of IT specialists; information security.

Введение. Одним из важных аспектов, утверждённой в 2017 году в Российской Федерации программы «Цифровая экономика Российской Федерации», является подготовка IT кадров. Ключевыми этапами обучения является получение теоретических и практических навыков будущими специалистами [1]. Таким образом, вопрос автоматизации процессов обучения является актуальным. Для автоматизации процессов получения специалистами практических навыков была разработана автоматизированная информационная система.

Разработанная система позволяет хранить большие объемы данных, отслеживать процесс выполнения заданий, предлагать задачи исполнителям в зависимости от уже имеющихся у них навыков, а также обмениваться сообщениями с наставниками, контролирующими процесс выполнения заданий, в реальном времени и создавать отчеты об успеваемости исполнителей. Система позволит значительно упростить процесс получения практических навыков обучающимися.

Было принято решения разработать систему как web-приложение, так как данная технология проста в реализации и удобна в использовании для большого количества пользователей, не требует установки отдельных программ и средств защиты для каждого клиента, доступ к системе может быть реализован посредством обычного браузера [2].

Разработка началась с проектирования системы. Средствами языка UML была построена диаграмма вариантов использования системы [3]. Данная диаграмма описывает функционал разрабатываемой программной системы доступный каждой группе пользователей. Были выделены 6 групп пользователей, которые могут взаимодействовать с системой:

1.Администратор — выполняет функции по настройке системы. Также администратор занимается исправлением и доработкой системы, тестированием и введением в эксплуатацию новых модулей.

2.Управляющий — выполняет функции обработки задачи, проводит оценку параметров исполнителя необходимых для выполнения данной задачи.

3.Заказчик — выполняет функции по первичной постановке задачи. Загружает ТЗ на работу в систему, устанавливает сроки выполнения задачи.

4.Исполнитель — выполняет задачи, поставленные системой. Делает пометки о ходе выполнения задачи. Мотивация — получение новых навыков.

5.Наставник — преподаватель, руководитель практики, обладающий знаниями и навыками для помощи Исполнителю в решении поставленной задачи.

6.Неавторизованный пользователь — пользователь, который не имеет прав в системе.

7.На рис. 1 представлена диаграмма вариантов использования системы.

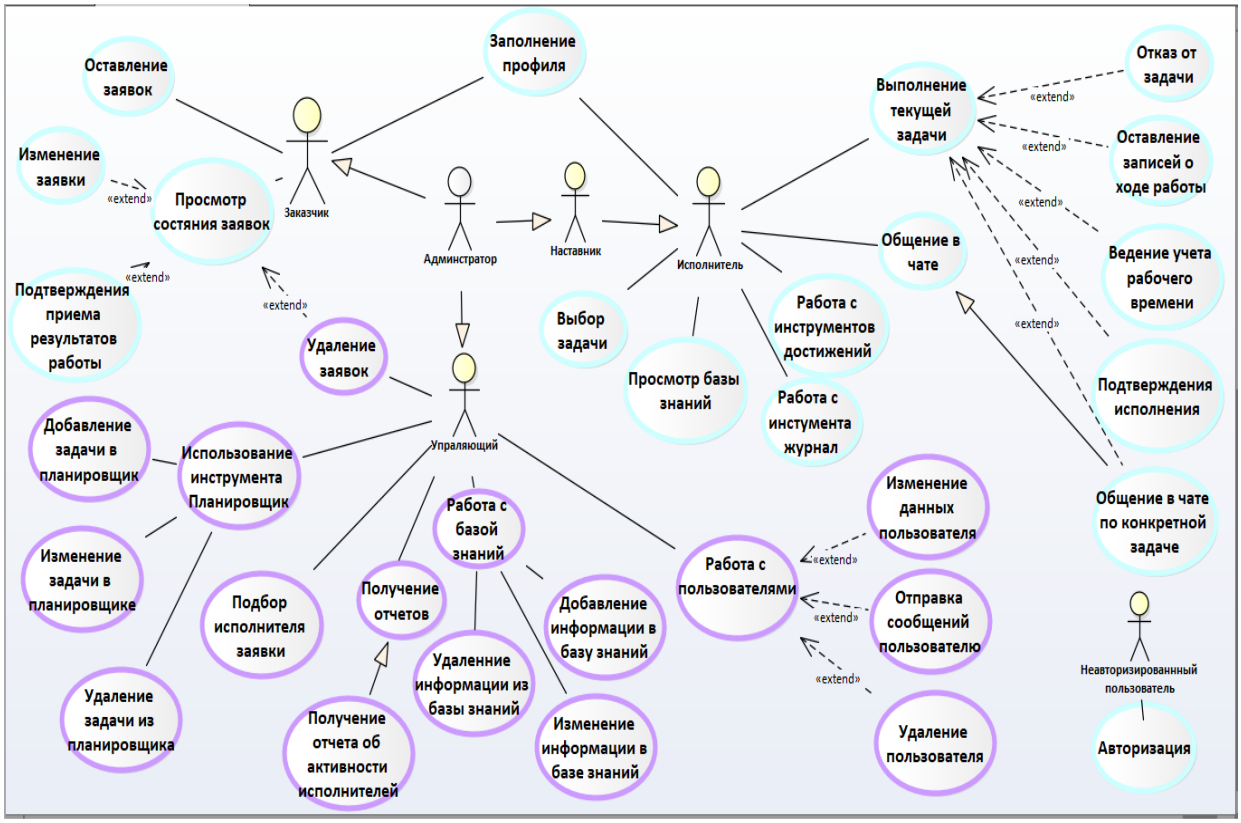


Рис.1. Диаграмма вариантов использования системы

Для более детального описания особенностей функционального поведения системы был разработан шаблон сценариев, описывающий действия пользователей и поведение моделируемой системы в форме обычного текста. Для каждого варианта использования в шаблоне сценариев представлен свой раздел, описывающий ход событий выполнения данного варианта использования и исключительные ситуации, которые могут возникнуть. В таблице 1 приведён Главный раздел сценария выполнения варианта использования «Общение в чате по конкретной задаче».

Таблица 1

Главный раздел сценария выполнения варианта использования «Общение в чате по конкретной задаче»

Вариант использования	Общение в чате
Актеры	Исполнитель, Наставник
Цель	Общение между исполнителем и наставником
Краткое описание	Исполнитель может задать вопросы наставнику по поводу выполнения задачи
Тип	Базовый
Ссылки на другие варианты использования	Выполнение текущей задачи
	Работа с инструментом чат

При разработке системы использовалась модель MVC (аббревиатура от «модель-представление-контроллер»). Это способ организации кода, который предполагает выделение блоков, отвечающих за решение разных задач.

Модель отвечает за данные и определяет структуру приложения.

Представление отвечает за взаимодействие с пользователем, определяет внешний вид приложения.

Контроллер отвечает за связь между моделью и представлением, определяет, как сайт реагирует на действия пользователя.

Данная модель повышает безопасность приложения за счет:

1.Разделение обязанностей между компонентами модели. Это облегчает управление и контроль над каждой составляющей приложения.

2.Централизованной проверки пользовательского ввода.

3.Упрощение тестирования: поскольку MVC обеспечивает разделение обязанностей, тестирование каждого из компонентов может быть проще и эффективнее, что может помочь в обнаружении и устранении уязвимостей безопасности [4].

Для разработки системы были выбраны следующие средства разработки:

1.Для проектирования базы данных была выбрана технология PostgreSQL — это мощная система объектно-реляционных баз данных с открытым исходным кодом, активно разрабатываемая более 35 лет и заслужившая прочную репутацию за надежность функций и производительность.

2.Для разработки серверной части приложения был выбран язык PHP. PHP — это распространённый язык программирования общего назначения с открытым исходным кодом. PHP специально сконструирован для веб-разработок и его код может внедряться непосредственно в HTML.

3.JavaScript — мультипарадигменный язык программирования. Поддерживает объектно-ориентированный, императивный и функциональный стили.

4.Centrifugo — Масштабируемый сервер обмена сообщениями в реальном времени [5].

5.При разработке модулей были учтены российские и мировые стандарты по безопасности, такие как OWASP Top 10, CAPEC (Common Attack Pattern Enumeration and Classification), CWE (Common Weakness Enumeration), CVE (Common Vulnerabilities and Exposures), Банк данных угроз безопасности информации ФСТЭК России, Mitre *Att&ck*, STIX (Structured Threat Information eXpression), WASC (Web Application Security Consortium), модель Kill Chain [6].

Для системы были разработаны следующие модули:

Модуль «База данных» — совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимо от прикладных программ [7]. Спроектированная база данных хранит информацию о пользователях системы, правах пользователей, выполняемых задачах, сообщениях пользователей, методических материалах для обучения.

Разработка модуля «Администрирование» включила в себя разработку инструментов «Заказчики», «Исполнители» и «Наставники», а также инструментов «Заявки», «Планировщик» и «Взаимодействие».

Инструменты «Заказчики», «Исполнители» и «Наставники» предназначены для работы с информацией о соответствующих участниках системы.

Инструмент «Заявки» служит для определения параметров подбора Исполнителя заявки.

Инструмент «Планировщик» поможет управляющему системой работать в соответствии с поставленным планом работы.

Инструмент «Взаимодействие» призван выступать неким коннектором между всеми инструментами модуля и модулем «База данных».

Модуль «Администрирование» расположен в защищенной части web-приложения, доступ к которой имеют только пользователи с правами «Администратор» и/или «Управляющий». Его интерфейс представлен на рис. 2.

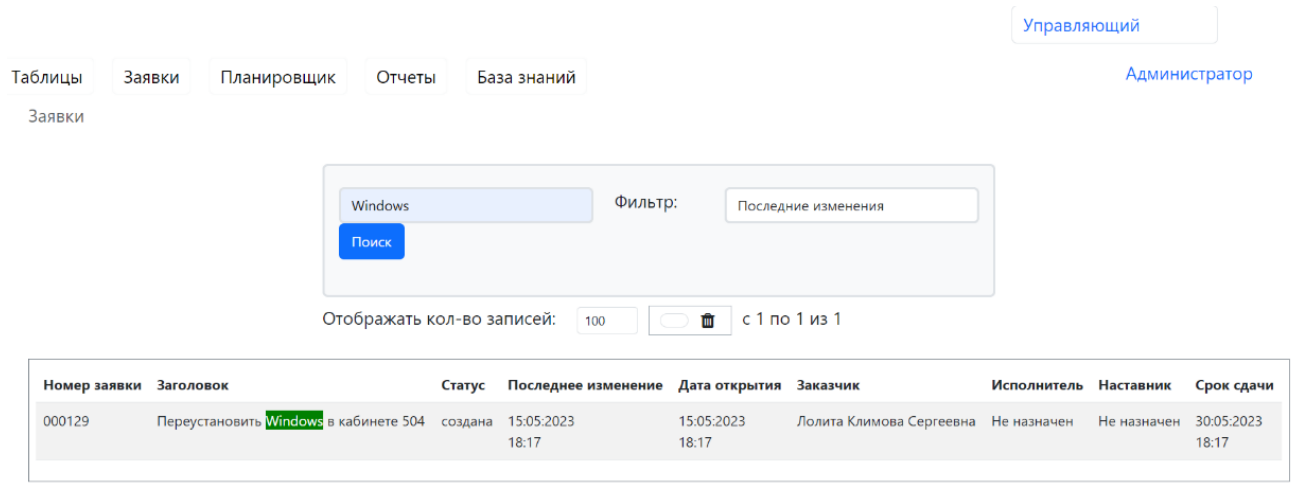


Рис. 2. Интерфейс модуля «Администрирование»

Разработка модуля «Чат» включает в себя создание модуля для быстрого обмена сообщениями между исполнителями и наставниками, методов для записи и получения сообщений из базы данных. Для получения сообщений в реальном времени используется протокол WebSocket (протокол связи поверх TCP-соединения, предназначенный для обмена сообщениями между браузером и веб-сервером, используя постоянное соединение). Соединения посредством web-сокетов реализуется на сервере Centrifugo.

Интерфейс данного модуля представлен на рис. 3.

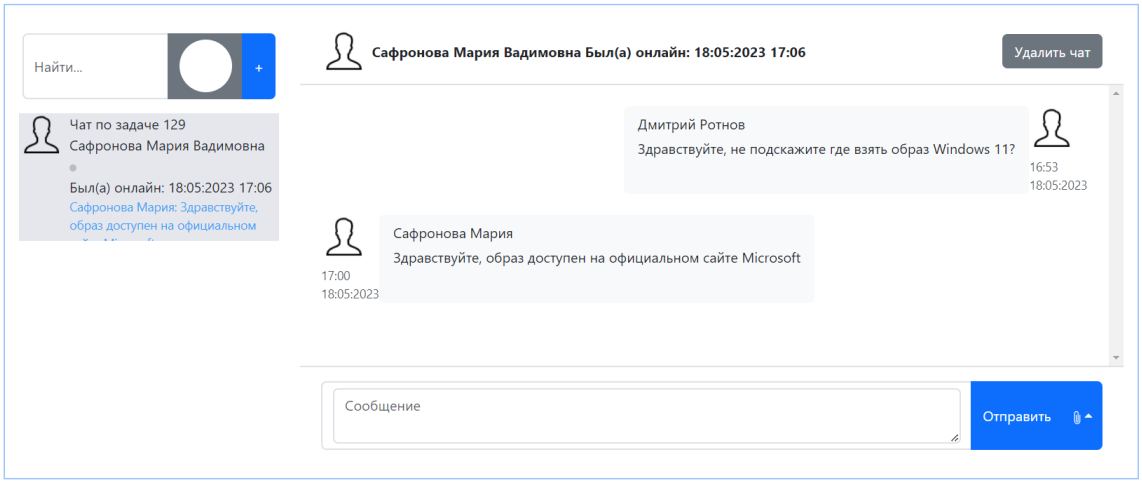


Рис. 3. Интерфейс модуля «Чат»

Для Безопасной интеграции модуля базы данных в систему были выбраны следующие средства:

1.Каждый сервис в системе разворачивать на отдельном docker контейнере, что повышает безопасность за счет изоляции частей системы и ограничения привилегий контейнера по умолчанию.

2.Для связи базы данных и серверной части используется библиотека PHP Data Objects (PDO) — универсальный интерфейс для работы с базами данных в PHP, поддерживающий подготовленные запросы, которые защищают приложение от SQL-инъекций.

Модуль «Чат» расположен в защищенной части web-приложения, доступ к которой имеют только авторизированные пользователи. Для того, чтобы пользователи получали сообщения в реальном времени они подключаются к серверу Centrifugo. Когда пользователь заходит на страницу чата, сервер генерирует ключи доступа пользователя к приватным каналам. Таким образом, пользователь может получать сообщения только из тех чатов, в которых он состоит.

Были реализованы программные меры защиты от типовых атак на web-приложение:

1. *Защита от угроз нарушения контроля доступа:*

Права доступа пользователей хранятся в базе данных. Для проверки прав пользователя на стороне сервера разработан специальный механизм, который по идентификатору пользователя получает его права из базы данных и проверяет является ли аккаунт пользователя активированным.

2.*Защита от SQL injections реализуется следующими мерами:* Передача данных на сервер методом POST, проверкой прав пользователя при каждом обращении к базе данных, данные подставляются в запрос только через подготовленные выражения, а также экранированием специальных символов и использованием регулярных выражений.

3.*Защита от XSS атак:* Защита от XSS атак реализована путем экранирования входных и выходных, указанием кодировки на каждой веб-странице, установкой флага HttpOnly (этот флаг делает клиентские куки недоступными через языки сценариев, такие как JavaScript), заданием списка желательных источников для загрузки контента с помощью заголовка Content Security Policy.

4.*Защита от CSRF атак:* Для защиты от CSRF атак используются CSRF-токены. CSRF-токены (или anti-CSRF-токены) напоминают cookies. Это такие же данные, которые сервер отправляет браузеру в ожидании получить их обратно, но отличие в следующем: сервер должен отправить браузеру уникальный токен и проверить, присылает ли его браузер в ответ в запросе. Если токены совпадают, запрос действителен, если нет — отклоняется.

5.*Регистрация и мониторинг событий в системе:* Для своевременного выявления нарушения безопасности в системе в базе данных ведется журнал аудита событий [8]. Данные в журнал вносятся с помощью, разработанной на языке plsql функции триггера, которая срабатывает при внесении изменений пользователей в систему. Код и работа данной функции представлены на слайде.

6.*Настройка безопасности на сервере:*

Служебный файл. haccess хранит расширенные параметры работы с веб-серверами (Apache и т. п.). Он необходим для корректного функционирования любого сайта. Когда web-сервер получает запрос по протоколу HTTP (или HTTPS) к какому-либо файлу на сервере (определенной странице сайта), он предварительно проверяет наличие файла .htaccess в той же папке (или в одной из вышестоящих по иерархии каталогов папок, начиная с корневого каталога сайта). Файл был дополнен настройками, которые дополнительно защищают приложение от xss атак и запрещают просмотр списка каталогов и файлов сервера.

7.*Защита от криптографических сбоев:* Защита от криптографических сбоев была реализована путем хэширования паролей безопасным к брутфорсу алгоритмом bcrypt.

8. *Защита от брутфорс атак* проводится путем проверки сложности и длины создаваемого пароля.

Была проведена проверка разработанных модулей на безопасность сканером уязвимостей OWASP ZAP. OWASP (Open Web Application Security Project) — всемирная некоммерческая организация, деятельность которой направлена на повышение безопасности ПО. OWASP ZAP — это один из самых популярных в мире инструментов безопасности с открытым исходным кодом. В результате сканирования: не найдены уязвимости, которые могут навредить системе, но найдена информация об используемых компонентах веб-сайта. Это можно исправить дополнительными настройками безопасности на сервере. На рис. 4 представлены результаты сканирования [6].

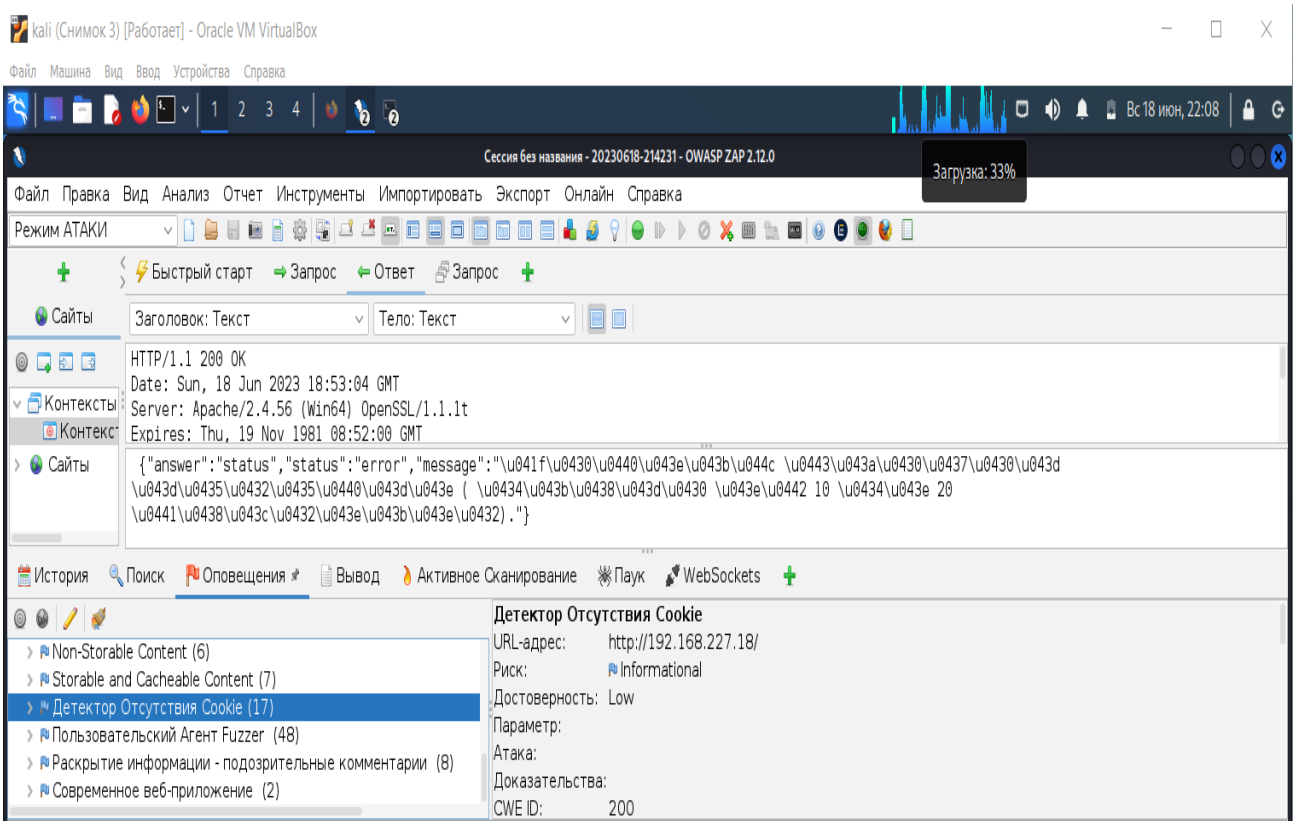


Рис. 4. Сканирование OwaspZap

Заключение. На данный момент разработанное программное обеспечение находится на этапе регистрации. Программную систему можно использовать для автоматизации процессов получения практических навыков IT-специалистами, а также для организации технической поддержки предприятия. Система обеспечивает непрерывный процесс получения практических навыков обучающимися, а также отслеживания их успеваемости. Представленные алгоритмы предотвращения компьютерных атак разрабатывались с учётом Российских и мировых стандартов по безопасности. Дальнейшие исследования будут связаны с повышением безопасности разработанной системы.

СПИСОК ЛИТЕРАТУРЫ

1. Цифровая экономика РФ [Электронный ресурс]. URL: https://digital.gov.ru/ru/activity/directions/858/?utm_referrer=https%3a%2f%2fwww.google.com%2f/ (дата обращения: 07.08.2023).
2. Ильина А. А., Шипунов И. С. Мобильное приложение для организации учебного процесса студента // Актуальные аспекты и приоритетные направления развития транспортной отрасли. СПб., 2019 года. С. 172-176.
3. Буч Г., Рамбо Д., Якобсон И. Введение в UML от создателей языка. 2017.496 с.
4. Архитектурный паттерн MVC. Веб-платформа. [Электронный ресурс].URL: https://doka.guide/tools/architecture-mvc/m (дата обращения: 07.08.2023).
5. Centrifugo introduction. CENTRIFUGO. Scalable real-time messaging server. Set up once and forever. [Электронный ресурс]. URL: https://centrifugal.dev/(дата обращения: 07.08.2023).
6. Общий обзор классификаций угроз безопасности: OWASP, CWE, CAPEC, WASC. Безопасность пользователей в сети Интернет. [Электронный ресурс]. URL: https://safe-surf.ru/specialists/article/5210/595970/ (дата обращения: 07.08.2023).
7. Нырков А.П., Нырков А. А. Сравнительная оценка математического обеспечения систем управления базами данных // Задачи контроля и управления. СПб.: СПГУВК, 1997. С. 142-145.
8. Нырков А.П., Рудакова С. А. Методика аудита объектов информатизации по требованиям информационной безопасности // Журнал университета водных коммуникаций. 2012. № 3. С. 146-149.

УДК 004.896

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В АВТОМАТИЗИРОВАННОЙ ТРЕНАЖЕРНО-ОБУЧАЮЩЕЙ СИСТЕМЕ

Юрий Николаевич Островский, Наталия Львовна Виткевич, Сергей Львович Хомутовский
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий, пр., 3, Санкт-Петербург, 194064, Россия
e-mails: ostrovskii_urii@mail.ru, tivatan@mail.ru, Sergey homutovsky99@mail.ru

Аннотация. В статье на основе анализа целей цифровой трансформации высшего образования обоснована актуальность и представлена архитектура автоматизированной тренажерно-обучающей системы военного вуза, а также предложены механизмы внедрения сквозных цифровых технологий и искусственного интеллекта для автоматизации и персонализации учебного процесса военно-инженерного вуза.

Ключевые слова: цифровая трансформация; интеллектуальная система; тренажерно-обучающая система; искусственный интеллект; сквозные цифровые технологии.

ARTIFICIAL INTELLIGENCE IN AUTOMATED SIMULATOR AND TRAINING SYSTEM

Ostrovsky Yuri, Vitkevich Natalia, Khomutovsky Sergey
The Military Academy of Telecommunications, named after
Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: ostrovskii_urii@mail.ru, tivatan@mail.ru, sergey_homutovsky99@mail.ru

Absrtact. The article, based on the analysis of the goals of digital transformation of higher education, substantiates the relevance and presents the architecture of the automated simulator-training system of a military university, and also suggests mechanisms for the introduction of end-to-end digital technologies and artificial intelligence to automate and personalize the educational process of a military engineering university.

Keywords: digital transformation; intelligent system; simulator-training system; artificial intelligence; end-to-end digital technologies.

Введение. Цифровая революция, глобализация и конкуренция за таланты привели к появлению относительно нового тренда в построении систем высшего образования — персонализации. Непрерывный процесс развития технических систем и аппаратных комплексов связи, увеличение числа объектов управления, рост скорости производственных процессов увеличивает сложность выполняемых операций для их обслуживания и эксплуатации, что влечет за собой повышение требований к качеству знаний и навыков военных специалистов [1].

Стратегические направления в области цифровой трансформации высшего образования на период до 2030 года утверждены Распоряжением Правительства Российской Федерации от 21.12.2021 №3759-р. В ходе реализации стратегического направления будут внедрены следующие технологии [2]:

– *искусственный интеллект* в части рекомендательных систем и интеллектуальных систем поддержки принятия решений, перспективных методов и технологий;

– *большие данные* в части использования методов интеллектуального анализа значительных объемов информации для поддержки принятия управленческих решений и повышения качества данных;

– *сквозные цифровые технологии* в части разработки инструментов по повышению уровня цифровых компетенций работников образовательных организаций высшего образования.

Указанные технологии будут применены в проекте «Единая сервисная платформа науки» в части формирования единой *экосистемы*. Основной целью создания *экосистемы* образования будет повышение качества образования, улучшение доступности образовательных ресурсов и средств обучения, а также повышение эффективности обучения и подготовки кадров. Одним из ключевых элементов экосистемы образования является использование новых цифровых технологий и искусственного интеллекта для оптимизации образовательных процессов, автоматизации рутинных задач, а также для поддержки принятия решений в образовательной сфере представленных на рис. 1.

Развитие образовательной деятельности военного вуза в цифровой среде является непременным условием успеха в развитии современной армии. Цифровая экономика считается новым этапом развития экономики, который связан с использованием сквозных цифровых технологий для создания продуктов и услуг. Это означает, что использование сквозных цифровых технологий во военном образовании является необходимым условием для подготовки военнослужащих к решению современных задач.

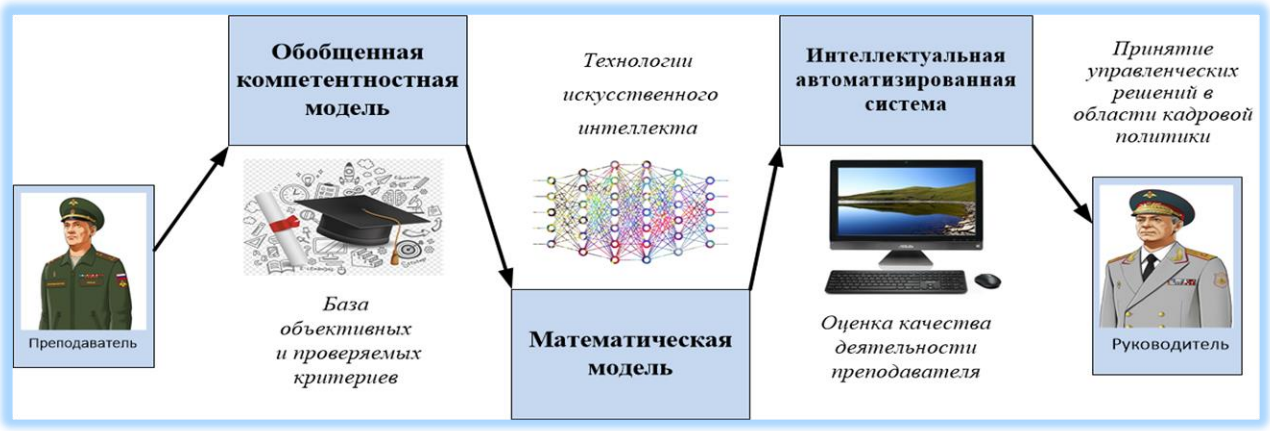


Рис. 1. Искусственный интеллект в экосистеме образования

Военный вуз МО РФ должен адаптировать программы обучения к новым цифровым технологиям и оборудованию, используемому в современных вооруженных конфликтах и специальных военных операциях. Например, средства радиосвязи, беспилотные летательные аппараты, кибератаки, война в космосе и другие виды новых угроз требуют новых знаний и навыков от будущих офицеров.

В настоящее время вопрос реализации экосистемного подхода в условиях цифровой трансформации военного профессионального образовании является относительно новой и недостаточно исследованной темой. Данный подход предполагает интеграцию различных компонентов образовательной системы, включая технологические, методические, организационные и социальные аспекты обучения, для достижения максимальной эффективности. Экосистемный подход предполагает рассмотрение системы, в которой различные элементы взаимодействуют друг с другом, как единый механизм.

В рамках данного подхода военный вуз должен рассматриваться как часть более широкой экосистемы, которая включает в себя различные учебные заведения, научно-исследовательские институты, военные подразделения и другие институты и организации, связанные с военной деятельностью. Все эти компоненты должны взаимодействовать между собой, чтобы обеспечить максимальное качество обучения и подготовки специалистов «на опережение».

Для реализации экосистемного подхода с внедрением искусственного интеллекта (ИИ) военный вуз должен использовать современные сквозные цифровые технологии и инструменты, такие как виртуальная и дополненная реальности, облачные вычисления, машинное обучение, генеративный и аналитический искусственный интеллект и т. д. Эти технологии могут быть использованы для разработки интеллектуальных тренажерно-обучающих систем, виртуальных лабораторий и тренажеров, которые позволят обучающимся получать профессионально-значимые компетенции.

Кроме того, важным аспектом *экосистемного подхода* является учет индивидуальных потребностей слушателей и курсантов. Военный вуз должен предоставлять различные варианты обучения, которые соответствуют потребностям и интересам обучающихся.

Военная педагогическая система практически не менялась с момента своего становления и уже не соответствует требованиям современного времени.

Это проявляется, в частности, в том, что Вооруженные Силы Российской Федерации оказались перед проблемой отсутствия достаточного числа кадров, способных сразу после окончания высшего военного учебного заведения компетентно работать в новых условиях, не тратя время на длительную адаптацию в войсках и в профессии. Ситуация, когда офицер-выпускник имеет конечный объем знаний по военно-профессиональным дисциплинам при отсутствии умений его использовать и пополнять, становится сдерживающим фактором развития безопасности и обороноспособности нашего государства. Девизом военного образования в России сейчас становятся слова В.В. Путина: «…Нам необходима инновационная армия, где к профессионализму, техническому кругозору и компетентности военных предъявляются требования принципиально иного, самого современного уровня… С учетом современных вызовов и угроз интересам нашей страны» [3].

Актуальность проведения исследований в области развития образовательной деятельности военного вуза в условиях цифровой трансформации и развития искусственного интеллекта обусловлена несколькими факторами.

Во-первых, цифровая трансформация и развитие искусственного интеллекта оказывают значительное влияние на современную военную доктрину и тактику ведения боевых действий. Развитие сквозных цифровых технологий привело к тому, что образовательный процесс в военных вузах стал меняться. Введение новых цифровых технологий и методов обучения требует анализа и оценки их эффективности в «контекстном обучении» [4] военных специалистов. В связи с этим, военным специалистам необходимо обладать профессионально-

значимыми компетенциями, чтобы адекватно реагировать на изменяющуюся обстановку и использовать современные технологии в своей работе.

Во-вторых, использование искусственного интеллекта и сквозных цифровых технологий в образовательном процессе может значительно улучшить качество обучения военных специалистов. Однако, для достижения наилучших результатов, необходимо проводить исследования по определению наиболее эффективных методов использования этих технологий в обучении.

В Послании Федеральному Собранию Российской Федерации 21 февраля 2023 года Президент России В.В. Путин обратил внимание на ряд вопросов, требующих существенных изменений в образовании: «в условиях новых требований, необходим синтез всего лучшего, что было в советской системе образования, и опыта последних десятилетий».

В-третьих, исследования развития образовательной деятельности военного вуза в условиях цифровой трансформации и развития искусственного интеллекта могут помочь выявить проблемы, связанные с использованием этих технологий в обучении, определить ключевые показатели оценки эффективности. Например, проблемы могут возникать из-за недостаточной квалификации преподавателей или из-за недостаточного доступа к оборудованию и программному обеспечению.

В своей речи на пленарном заседании XXVI Петербургского международного экономического форума В.В. Путин отметил: «Необходимо повысить ориентированность высших и средних специальных учебных заведений на результат, то есть на успешное трудоустройство выпускников. В связи с этим считаю правильным сделать две вещи, по крайней мере, две. Первое. Установить для учебных заведений *специальные ключевые показатели эффективности*. Главный из них — это качество занятости выпускников. На основе такого подхода предлагаю сформировать рейтинги учебных заведений профессионального образования. И второе. Предлагаю ежегодно готовить пятилетний прогноз потребности в кадрах на уровне всей экономики, чтобы максимально гибко учитывать меняющиеся тренды, новые запросы рынка труда и, конечно, наши приоритеты в развитии отраслей экономики».

В-четвертых, проведение исследований развития образовательной деятельности военного вуза в условиях цифровой трансформации и развития искусственного интеллекта может стать основой для разработки новых методик и подходов к обучению военных специалистов, которые будут соответствовать современным технологиям и требованиям.

Так в своей речи на пленарном заседании XXV Петербургского международного экономического форума В.В. Путин отметил: *«Многие российские решения по искусственному интеллекту и обработке больших данных являются лучшими в мире. Технологическое развитие — это сквозное направление, которое определит не только текущее десятилетие, но и весь 21 век.»*

В жизни нашего общества происходят крупные перемены в различных его сферах и, так как образование должно носить *опережающий характер* развития по отношению к социально-экономическому развитию общества, назрела необходимость законодательного определения и закрепления стратегии государства в развитии системы образования. Таким документом явилась Национальная доктрина образования в Российской Федерации на период до 2025 года [5], определившая стратегические цели образования, тесно увязанные с такими проблемами развития российского общества.

Сегодня знания и технологии быстро обновляются, для освоения передовых способов действий, для эффективного функционирования в динамично развивающейся профессиональной среде необходимо направлять учащихся на опережение, на выход за рамки действующих стандартов подготовки, профессиональных компетенций, подходов, решений. Достижение инновационного качества обучения, подготовка специалистов «с опережением», требует адекватных изменений в педагогических подходах, технологиях, решениях [6].

В системе военного образования, являющегося частью системы профессионального образования в целом, выросли требования к уровню подготовки офицеров, особенно в период *специальной военной операции* на Украине (СВО), как в одном из высокотехнологичных направлений развития и совершенствования Вооруженных Сил Российской Федерации.

В рамках Национальной технологической инициативы был поставлен вопрос об обеспечении технологической независимости России за счет развития сквозных цифровых технологий, которые были определены как ключевые научно-технические направления, оказывающие наиболее существенное влияние на развитие рынков и одновременно охватывающие несколько отраслей. Практически все виды таких технологий развиваются в военной отрасли промышленности и быстро проникают в сферу военного образования, меняя информационно-образовательную среду [7].

Дальнейшее развитие автоматизированной тренажерно–обучающей системы с применением искусственного интеллекта и сквозных цифровых технологий позволит создать интеллектуальную образовательную систему военного вуза представленной на рис. 2. Результатом данной системы станет получение прогноза и выдача корректирующих управленческих решений, предотвращения критических ситуаций, снижения рисков неблагоприятных последствий в образовательной и научной деятельности высших учебных заведений в условиях цифровой трансформации.

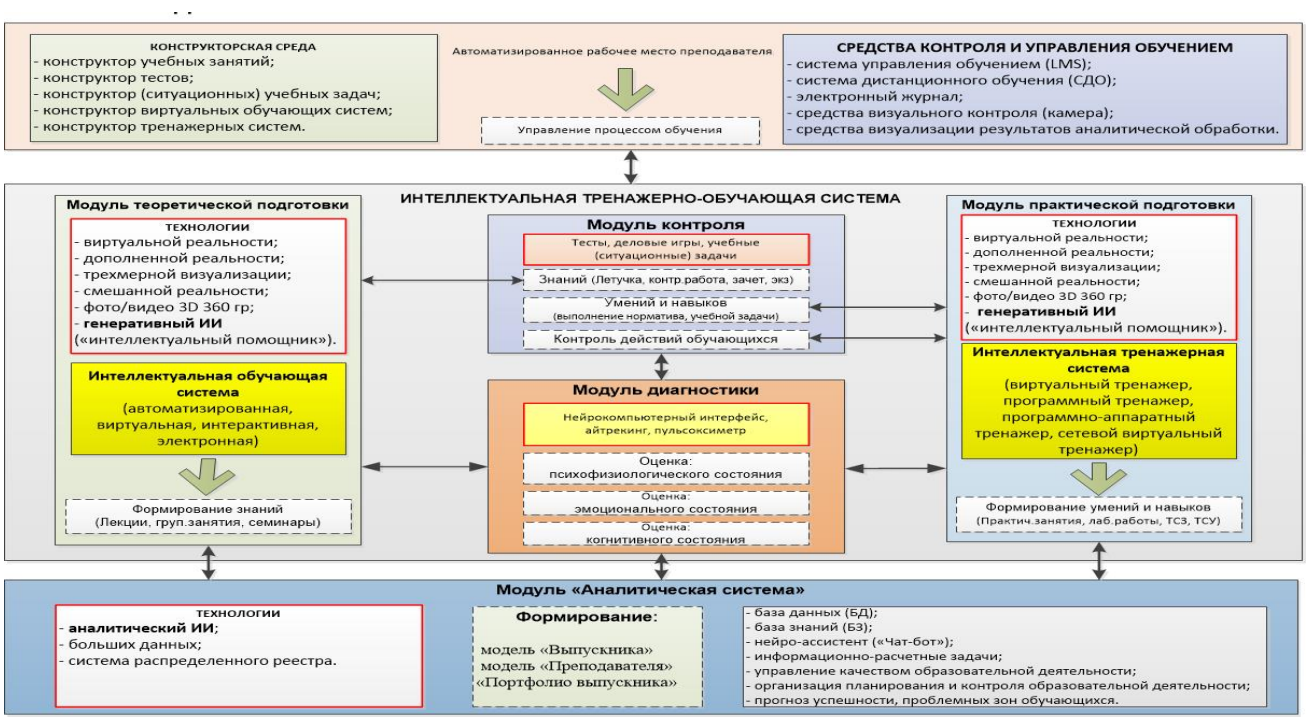


Рис. 2. Архитектура автоматизированной тренажерно-обучающей системы

Таким образом, развитие образовательной деятельности военного вуза в цифровой интеллектуальной образовательной системе является необходимым условием для подготовки военных кадров, способных эффективно решать современные задачи армии и флота Российской Федерации. Важно использовать все возможности новых цифровых технологий в обучении, таким образом, чтобы обучающиеся могли получить максимальную пользу от учебного процесса.

СПИСОК ЛИТЕРАТУРЫ

1. Соколова И. И, Островский Ю.Н., Виткевич Н.Л. Сквозные цифровые технологии в интеллектуальной тренажерно-обучающей системе. Технологии. Инновации. Связь. Сборник материалов научно-практической конференции. СПб., 2022. С. 136-143.
2. Распоряжение Правительства Российской Федерации от 21.12.2021 №3759-р Об утверждении стратегических направлений в области цифровой трансформации науки и высшего образования на период до 2030 года [Электронный ресурс] // Официальное опубликование правовых актов : [сайт]. URL: http://publication.pravo.gov.ru/Document/View/0001202112250002 (дата обращения 10.10.2023).
3. Путин В. В. Доклад на Госсовете РФ 8 февраля 2008 г. «О стратегии развития России до 2020 года». М., 2008. 26 с.
4. Вербицкий А. А. Компетентностный подход и теория контекстного обучения. М.: Исследовательский центр проблем качества подготовки специалистов, 2004.
5. Национальная доктрина образования в Российской Федерации [Электронный ресурс]. URL: http://dvgu.ru/umu/ZakRF/doktrinl.htm, (дата обращения: 30.08.2023).
6. Носкова Т. Н. Психодидактика информационно-образовательной среды : учеб. пособие. СПб. : Изд-во РГПУ им. А. И. Герцена, 2007. 171 с.
7. Островский Ю. Н., Соколова И. И. Перспективные тренажерно-обучающие системы в подготовке военных связистов : Материалы Международной научной конференции «Информатизация непрерывного образования — 2018». Москва, 14–17 октября 2018 г.: в 2 т. / под общ. ред. В. В. Гриншкуна. М. : РУДН, 2018. Т. 1. 760 с. С. 572-575.

УДК 004.056

МОДЕЛЬ ЗАЩИЩЕННОГО КАНАЛА ПЕРЕДАЧИ ИНФОРМАЦИИ В КОРПОРАТИВНОЙ СРЕДЕ С ПРИМЕНЕНИЕМ ОТКРЫТЫХ МЕССЕНДЖЕРОВ

Солодянников Александр Владимирович
Санкт-Петербургский государственный экономический университет
Грибоедова наб. кан., 30\32, Санкт-Петербург, 191023, Россия
e-mails: solod000@yandex.ru

Аннотация. Данная статья рассматривает проблему отсутствия защищенного мессенджера передачи коротких сообщений. Основная тема исследования — поиск возможностей, в нынешних условиях, создания защищенного канала передачи информации с применением существующих программных продуктов.

Ключевые слова: цифровой мессенджер; цифровые технологии; базы данных; система управления.

MODEL OF SECURE INFORMATION TRANSMISSION CHANAL IN A CORPORATE ENVIROMENT USING OPEN MESSENGERS

Solodyannikov Alexander
St. Petersburg State University of Economics
30/32 Griboedov's canal Emb, St. Petersburg, 191023, Russia
e-mails: solod000@yandex.ru

Abstract. This article examines the problem of the lack of a secure messenger for transmitting short messages. The main topic of the research is the search for opportunities, in the current conditions, to create a secure channel for transmitting information using existing software products.

Keywords: digital messenger; digital technologies; databases; management system.

Введение. В настоящее время вопрос конфиденциальности данных в социальных сетях стоит наиболее остро, так как довольно часто в сети Интернет случается кража или продажа личных данных. Сегодня абсолютно каждый пользуется смартфоном, компьютером, ноутбуком для передачи различной информации, будь то простое общение между людьми или, например, денежные операции. В связи с этим могут происходить различные утечки данных, как по вине злоумышленников, так и по неосторожности. Это ведет к большим финансовым потерям, а порой пропадает и действительно важная и достаточно ценная информация.

Основным средством общения людей являются сеть Интернет и телефонная связь, поэтому основные утечки различной информации происходят через них.

Целью исследования было поиск возможностей создания защищённого канала связи при помощи облачных серверов.

Для решения данной цели необходимо было решить следующие задачи:

- рассмотреть существующие подходы создания защищённого акустического канала связи и облачных серверов;
- обосновать выбор подходящих для выполнения обозначенной цели облачных серверов и мессенджеров;
- создать модель угроз и модель нарушителя для предлагаемого варианта;
- разработать общие принципы создания защищенного акустического канала связи на основе облачного сервера.

На рис. 1 показан принцип работы защищенного канала связи. Пользователь сканирует устройство с помощью антивирусной программы перед отправкой сообщения. Если сканирование прошло успешно, то можно отправить сообщение, не опасаясь, что оно будет перехвачено вредоносным ПО. Клиент Signal передает данные на облачный сервер, который также управляет серверной частью сигнального мессенджера. Правильное функционирование контролируется системным администратором. Файлы шифруются на сервере. Системный администратор также следит за безопасностью хранения данных, что выражается дополнительным шифрованием жестких дисков, на которых хранятся сообщения перед отправкой. Как только приемник доступен, немедленно начинается передача данных. Предполагается, что устройство получателя уже было проверено антивирусной программой и поэтому сообщение поступает в сигнальный клиент в зашифрованном виде, из которого информация считывается получателем. Преимущество использования облачного сервера в этой модели заключается в том, что системному администратору приходится отслеживать меньше настроек. Физическая безопасность сервера, является обязанностью поставщика услуг. Кроме того, почти все сервисы, реализующие облачные технологии, имеют возможность автоматического резервного копирования, а также настроены на защиту данных от потери во время хранения. Задачи системного администратора сводятся к проверке работоспособности сервера, обеспечению сетевой безопасности операционной системы и, пожалуй, самое главное, обеспечению безопасности файловых хранилищ с дополнительными шифрами. При этом необходимо обеспечивать контроль физического доступа к хранилищу данных.

Рис. 1. Принцип работы защищенного канала связи компании.

Важно понимать, что для достижения хорошего уровня защиты информации и избежания потенциальных утечек из-за человеческого фактора необходимо следовать строгим правилам. Руководящие документы должны описывать права и обязанности пользователя. В связи с тем, что устройства доверенные, первым шагом является предотвращение установки на них стороннего программного обеспечения. Кроме того, обязательства пользователя должны включать пункт о конфиденциальности данных по отношению к третьим лицам, которые не имеют на это полномочий. Поскольку устройства должны быть доверенными, следует также запретить использование сторонних сетей для подключения к Интернету. Необходимо добавить возможность использования этих устройств в защищаемых помещениях. Учитывая возможную уязвимость в регистрации пользователя при первом подключении к серверу, которая позволяет совершить атаку типа человека посередине, стоит рекомендовать обмен идентификационными ключами при контакте с 2 устройствами через камеру и QR-код, на котором отображается идентификационный ключ. В противном случае разрешение пользователю регистрироваться при первом входе в систему может быть дано только в том случае, если соблюдены все остальные критерии, важнейшим из которых является использование устройства в доверенной среде. Кроме того, необходимо установить обязанность проверять антивирусную программу на устройстве один раз в определенный промежуток времени.

Заключение. Данные меры позволят снизить вероятность утечки информации по техническим каналам.

СПИСОК ЛИТЕРАТУРЫ

1. Белов Е. Б., Лось В. П., Мещеряков Р. В., Шелупанов А. А. Основы информационной безопасности : учебн. пособие. М. : Горячая линия — Телеком,2011. 558 с.
2. Бузов Г. А., Калинин С. В., Кондратьев А. В. Защита от утечки информации по техническим каналам : учебн. пособие. М. : Горячая линия — Телеком, 2005. 416 с.
3. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. М. : Энергоатомиздат, 1994.
4. Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В Информационная безопасность открытых систем. Ч. 1 : учебник для вузов. М. : Горячая линия — Телеком, 2006. 686 с.
5. Малюк А. А., Пазизин С. В., Погожин Н. С. Введение в защиту информации в автоматизированных системах: Учебн. пособие для вузов. М. : Горячая линия — Телеком, 2004. 147 с.
6. Язов Ю. К. Основы методологии количественной оценки эффективности защиты информации в компьютерных сетях. Ростов-на-Дону : СКНЦ ВШ, 2006. 270 с.
7. Язов Ю. К., Аграновский А. В., Мамай В. И., Назаров И. Г. Основы технологий проектирования систем защиты информации в информационно-телекоммуникационных системах : монография. СКНЦ ВШ, 2006. 318 с.

УДК 004.41

ОСОБЕННОСТИ РАЗРАБОТКИ ИГРЫ

Турышева Светлана Вадимовна, Шалагина Алина Сергеевна
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: s.turysheva@gmail.com, shalaginaaaaa@yandex.ru

Аннотация. В исследовании проанализированы основные этапы разработки игры жанра light novella и представлены возможные программные обеспечения открытого доступа для проектирования игры.

Ключевые слова: light novella; игры; видеоигры; сценарий.

FEATURES OF GAME DEVELOPMENT

Turysheva Svetlana, Shalagina Alina
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, Saint-Petersburg, 198035, Russia
e-mails: s.turysheva@gmail.com, shalaginaaaaa@yandex.ru

Abstract. The study analyzes the main stages of the development of a game of the light novella genre and presents possible open access software for the design of the game.

Keywords: light novel; games; video games; script.

Введение. На данный момент информационные технологии активно развиваются в области создания IT-игр, которые могут привлечь внимание абитуриентов и студентов, способствуя их участию в студенческой жизни и образовательном процессе в университете. Сегодняшняя задача заключается в выборе программных обеспечений для разработки и реализации игры жанра «light novella».

Миссией данной игры является ознакомление студентов первого курса с аспектами университетской жизни, а использование жанра «light novella» позволяет обеспечить интерактивный опыт игроков. Таким образом, игра становится эффективным средством для овладения необходимыми знаниями и навыками.

Визуальная новелла — жанр, в котором история передается зрителю с помощью вывода текста и статичных (иногда анимированных) изображений, а также сопровождается звуковым и музыкальным сопровождением. Этот формат позволяет создать впечатляющий визуальный и аудиоэффект, обогащая повествование и создавая уникальную атмосферу для игрока.

Создание видеоигр — это сложный и трудоемкий процесс, о котором многие люди не догадываются. В связи с этим, чаще всего, разработкой игры занимается команда специалистов. Каждый член команды должен быть хорошо знаком со своей сферой: художники, программисты, тестировщики и другие специалисты.

Для упрощения процесса разработки игры можно выделить 4 основных этапа: разработка сюжета, дизайн игры, программирование и отладка.

На каждом этапе разработки игры требуются соответствующие навыки с работой в программных обеспечениях. Опишем каждый из этапов.

1 этап: Разработка сюжета. Начальный этап включает определение концепции игры и создание сценария, который будет использоваться в качестве основы для всей игры. Это включает выбор темы, сюжетных линий, персонажей, места действия и прочих элементов игры. Был произведен анализ программных средств для создания сценария по различным критериям.

Таким образом, сюжет разрабатывался и оформлялся в программном обеспечении ThinkComposer.

Thinkcomposer — приложение, позволяющее организовать большое количество мыслей, информации в виде взаимосвязанных элементов на схеме. Оно предназначено для создания концептуальных карт, карт мыслей, моделей, диаграмм с подробным или кратким контентом, описанием.

Основные черты:

– интеграция с пакетами Microsoft Office,
– готовые шаблоны,
– поддержка горячих клавиш,
– поддержка многими операционными системами.

На рис. 1 представлен отрывок сценария игры в программном обеспечении ThinkComposer.

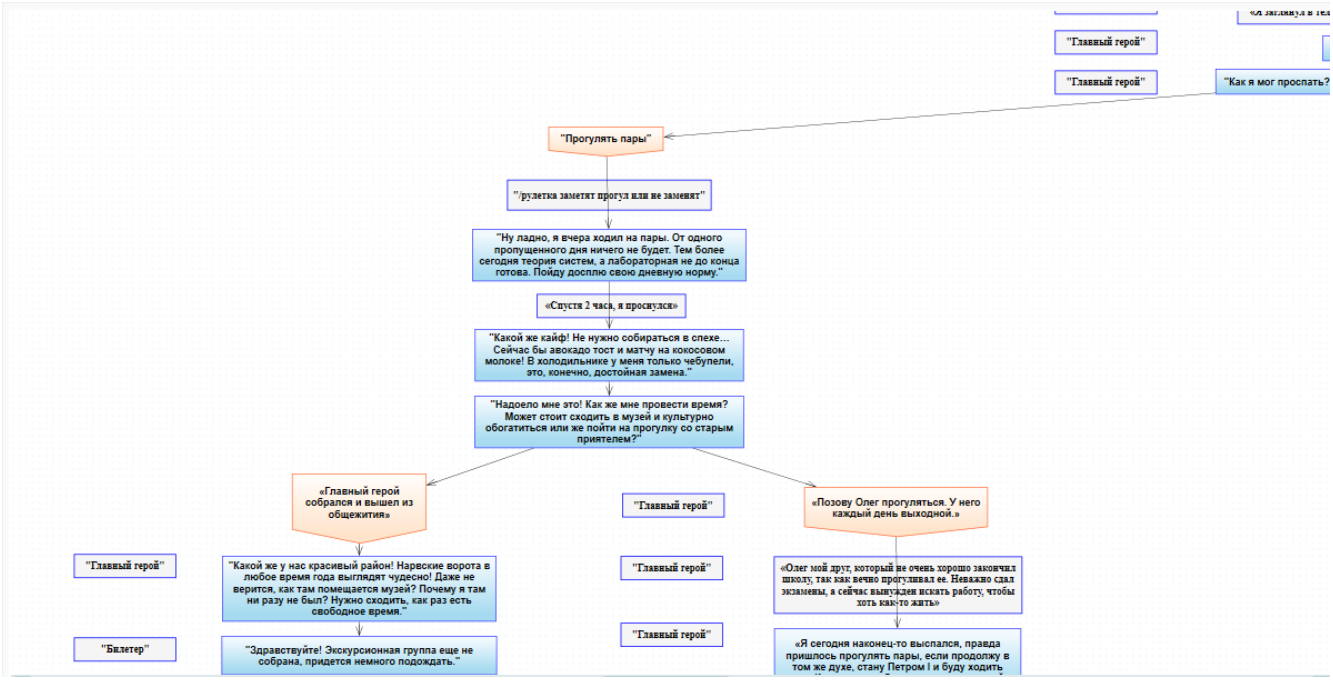


Рис. 1. Сценарий в ThinkComposer

2 этап: Дизайн игры и персонажей. Создавались концепт-арты, скетчи и прототипы, которые будут использоваться для создания окончательных моделей персонажей и окружения. При разработке персонажей использовался минималистичный стиль с небольшим количеством деталей и цветов. Изначально были созданы образы всех героев в Paint Tool SAI. Затем был разработан фон в соответствии с сюжетом игры и дизайн главного меню и всех элементов управления, включая всплывающий текст.

Для сохранения прозрачности фона персонажи были нарисованы в формате png, а для фоновых изображений был использован более высококачественный формат jpeg. При создании игры были взяты в качестве основы

реальные объекты, которые связаны с аудиториями и местами, которые студенты часто посещают в университете. Это позволяет создать более реалистичную и узнаваемую атмосферу в игре.

На рис. 2 представлен дизайн главного меню игры.

Рис. 2. Главное меню

3 этап: Программирование. Код для игры был создан в специальной оболочке Ren'py, которая основана на языке программирования Python. Большая часть кода занимается обработкой реплик героев, в то время как стилевое оформление и алгоритмическая логика составляют гораздо меньшую часть. В начале разработчики импортировали сценарий из внешнего приложения, затем добавляли логику и, в конечном итоге, применяли различные музыкальные и графические эффекты. На Ren`Py написаны большинство визуальных новел, такие, как «Бесконечное лето», «Суп бабочек», «Черный шкаф», «Волшебный дневник», «Игра в пятницу» и не только.

На рис. 3 представлен отрывок кода игры.

```
label get_out:
    scene bg narv
    show gg happy
    gg "Какой же у нас красивый район!"
    gg "Нарвские ворота в любое время года выглядят чудесно!"
    gg "Даже не верится, что там помещается музей."
    gg "Почему я там ни разу не был?"
    gg "Нужно сходить, как раз есть свободное время."
    hide gg
    show экскурс
    bileter "Здравствуйте!"
    bileter "Экскурсионная группа еще не собрана, придется немного подождать."
    hide экскурс
    show gg norm
    gg "Сколько нужно ждать?"
    hide gg
    show экскурс
    bileter "Минут 10-20, скоро должны подъехать школьники, будете с ними в одной группе."
    "Через 10 минут подошла группа школьников и началась экскурсия."
    "Экскурсоводом оказался мой старый приятель-старшекурсник Ваня, по совместительству сосед по этажу. "
    "После экскурсии я подошел к нему и начал разговор."
    hide экскурс
    show gg happy
    gg "Как же здорово! Не могу поверить, что раньше Нарвские ворота были деревянные."
    hide gg
    show i norm
```

Рис. 3. Код игры в Ren'py

Этап 4: Отладка. Самым сложным этапом является отладка, поскольку необходимо гарантировать соответствие сценария геймплею. Исправление ошибок осуществляется путем многократного итерационного проигрывания эпизодов, а также отправкой игры на тестирование сторонним лицам, которые предоставляют свои комментарии и предложения по внесению исправлений.

Для отладки программы применялась среда разработки PyCharm, которая обеспечивает удобство сравнения различных версий кода, поиск ошибок и возможность дополнения или интеграции.

Заключение. В исследовании были проанализированы этапы разработки игры, были выбраны основные программные обеспечения в связи с навыками команды и требованиями проекта по основным критериям. В результате была получена пошаговая инструкция разработки игры в жанре «light novella».

СПИСОК ЛИТЕРАТУРЫ

1. Выбор программного обеспечения для разработки сценария игры жанра light novella / С. В. Перевозчиков [и др.] // Молодой исследователь Дона. 2023. № 2(41). С. 72-77.
2. Суслова М. С. Обоснование выбора движка Ren'Py для создания игр формата визуальная новелла // Вестник научных конференций. 2020. № 9-3(61). С. 121-122.
3. Казачкова О. А., Козулина А. Н. Методы представления текста и графической составляющей в визуальных новеллах // Национальная научно-техническая конференция с международным участием. Перспективные материалы и технологии (ПМТ-2022). М. : МИРЭА — Российский технологический университет, 2022. С. 553-559.
4. Алексеев В. В., Карасева Е. И. Синтез и анализ вероятностей событий по нечисловой неточной и неполной экспертной информации // Проблемы анализа риска. 2014. Т. 11. № 3. С. 22-31.
5. Устюгова А. А. Особенности разработки 2D-игр в жанре визуальной новеллы // Медиа в информационном обществе: эффекты, возможности, риски : сборник научных трудов. Саратов: Саратовский государственный технический университет им. Гагарина Ю. А., 2022. Т. II. С. 97-100.

УДК 004.451:004.056

МЕТОДИКА ИЗУЧЕНИЯ МЕХАНИЗМОВ ПРОСТРАНСТВА ИМЕН «КОНТРОЛЬНЫЕ ГРУППЫ» В ДИСЦИПЛИНЕ «ОПЕРАЦИОННЫЕ СИСТЕМЫ» НАПРАВЛЕНИЙ «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ» И «КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ»

Частухин Даниил Алексеевич, Широков Владимир Владимирович, Щиголева Марина Андреевна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия
e-mails: dudypool@yandex.ru, vvshirokov@mail.ru, vvcehanovsky@mail.ru

Аннотация. Рассматривается раздел дисциплины «Операционные системы» направления «Информационные системы и технологии», в котором изучаются механизмы ограничения доступа к ресурсам. Технологии ограничения доступа к ресурсам позволяет повысить компьютерную безопасность. В числе механизмов таких технологий рассматривается пространство имен процессов «контрольные группы». Рассматриваются также программные интерфейсы перечисленных механизмов, позволяющие создавать системы защиты информации.

Ключевые слова: операционная система; технологии ограничения доступа; пространства имен процессов; программный интерфейс операционной системы; контрольные группы; компьютерная безопасность.

METHODOLOGY FOR STUDYING THE MECHANISMS OF THE NAME SPACE «CONTROL GROUPS» IN THE DISCIPLINE «OPERATING SYSTEMS» IN THE DIRECTION «INFORMATION SYSTEMS AND TECHNOLOGIES» AND «COMPUTER SECURITY»

Chastuhin Daniil, Shirokov Vladimir, Schigoleva Marina
Saint Petersburg Electrotechnical University
5 Professor’s Popov St, St. Petersburg, 197022, Russia
e-mails: dudypool@yandex.ru, vvshirokov@mail.ru, vvcehanovsky@mail.ru

Abstract. The section of the discipline «Operating systems» of the direction «Information systems and Technologies» is considered, in which the mechanisms of restricting access to resources are studied. Technologies for restricting access to resources can improve computer security. Among the mechanisms of such technologies, the process namespace «control groups» is considered. The program interfaces of the listed mechanisms are also considered, which allow creating information security systems.

Keywords: operating system; access restriction technologies; process namespaces; operating system programming interface; control groups; computer security.

Введение. Пространства имен операционной системы Linux предоставляют механизмы изоляции ресурсов дочерних процессов от ресурсов родительских процессов. Эти механизмы лежат в основе построения таких важнейших и широко распространенных средств обеспечения безопасности информационных систем, как контейнеры [1]. Поэтому изучение механизмов пространств имен в дисциплине «Операционные системы» обучающимися направлений подготовки «Информационные системы и технологии» и «Компьютерная безопасность» необходимо и актуально.

В настоящее время ОС Linux предлагает следующие типы пространств имен, позволяющих осуществлять изоляцию процессов по соответствующим видам ресурсов [2]:

1) IPC межпроцессное взаимодействие (очереди сообщений);
2) Network сетевые устройства, сетевые стеки, порты;
3) UTS имена хоста и домена;
4) PID идентификаторы процессов;
5) User идентификаторы пользователей и групп;
6) Mount точки монтирования файловых систем;
7) Cgroup корневые директории контрольных групп;
8) Time системные часы.

Перечисленные типы пространств имен можно разделить на три группы с точки зрения сложности освоения обучающимися при выполнении ими лабораторных работ:

1.Пространства имен IPC, Network, PID, UTS, для которых в функцию создания дочернего процесса достаточно ввести соответствующий флаг (CLONE_NEWIPC, CLONE_NEWNET, CLONE_NEWPID, CLONE_NEWUTC), чтобы получить возможность продемонстрировать работу процессов (родителя и потомка) в изолированных пространствах по соответствующим видам ресурсов;

2.Пространства имен Time, User, для которых недостаточно ввести флаг (CLONE_NEWTIME, CLONE_NEWUSER), но и необходимо произвести предварительную настройку определенных системных файлов. В первом случае это файл /proc/[pid]/timens_offsets, через который необходимо задать смещение системного времени процесса-потомка от системного времени процесса-родителя. Во втором случае это файлы /proc/[pid]/uid_мари /proc/[pid]/gid_map, через которые необходимо задать допустимые диапазоны идентификаторов пользователя и группы, которые могут быть установлены в процессе-потомке;

3.Пространства имен Mount, Cgroup, для которых установка соответствующего флага (CLONE_NEWNS, CLONE_NEWCGROUP) должна продемонстрировать отсутствие «видимости» процессами определенных ветвей файловой системы. В первом случае процесс-родитель «не видит» изменений файловой системы процесса-потомка, которые последний произвел путем вызова функции (команды) mount. Во втором случае процесс-потомок «не видит» ветку дерева файловой системы в каталоге /sys/fs/cgroup, описывающую контрольную группу процесса-родителя. Такая изоляция не позволяет процессу-потомку воздействовать на ресурсы процесса-родителя.

В данной публикации рассматривается методика изучения и проверки возможностей управления ресурсами процессов на основе контрольных групп и изоляции ресурсов с помощью механизма пространства имен Cgroup.

Методика может быть использована для проведения практических занятий и выполнения лабораторных работ обучающимися при изучении дисциплины «Операционные системы». Материал подобран таким образом, чтобы соответствовал двум направлениям подготовки «Информационные системы и технологии» и «Компьютерная безопасность» с учетом ранее изученных дисциплин программ подготовки. Материал методики включает ознакомительную составляющую по рекомендуемым программно-методическим источникам и процедурную составляющую с последовательными предписаниями выполнения заданий, процедурно подводящими к получению искомого результата — заключению по целевому преобразованию каталогов пространства имён.

Теоретическая предметная подготовка практических заданий:

– Изучение механизма создания контрольных групп;
– Изучение механизма пространства имен контрольной группы;
– Изучение программных интерфейсов: создания дочерних процессов; создания дочерних процессов с возможностью создания новой контрольной группы; создания дочерних процессов с продолжением своего выполнения в изолированном от процесса-родителя пространстве.

Выполненные задания:

– Создание контрольной группы по определенному виду ресурсов;
– Создание каталога в файловой заданной системе;
– Идентификация процессов и объёмов памяти: ограничения / отсутствие ограничений;
– Контроль хода обработки контрольной группы результатов выполняемых действий.

Вывод по результатам обработки контрольной группы: текущие каталоги контрольной группы становятся корневым каталогом нового пространства имен. На первом этапе изучения механизма контрольных групп обучающимся предлагается создать контрольную группу по определенному виду ресурсов. Наиболее наглядным для этой цели является ресурс памяти. Для этой цели необходимо создать каталог в файловой системе /sys/fs/cgroup/memory, например, /sys/fs/cgroup/memory/test_cgroup.

При создании каталога /sys/fs/cgroup/memory/test_cgroup в нем автоматически создается группа файлов, содержащих информацию о контрольной группе. Например, в файле cgroup.procs будут содержаться идентификаторы процессов, принадлежащих этой группе, а в файле memory.limit_in_bytes будет содержаться ограничение на объем памяти, которым могут пользоваться процессы, принадлежащие этой группе. При создании файла memory.limit_in_bytes в нем записаны данные, говорящие об отсутствии ограничений на размер памяти. Обучающимся может быть предложено задание по управлению контрольными группами, включающее перечисленные выше действия и наблюдение за результатами выполнения этих действий.

Следующим этапом работы является знакомство с механизмом пространства имен контрольной группы. Для этого необходимо предварительно ознакомиться с программными интерфейсами создания дочерних процессов с возможностью создания новой контрольной группы [3]. К таким интерфейсам относится функция clone(), в набор параметров которой могут входить перечисленные выше флаги типов пространств имен, в том числе и CLONE_NEWCGROUP. Другим видом интерфейса является совместное использование функций fork() и unshare(). То есть создаваемый функцией fork() дочерний процесс должен вызвать функцию unshare() с передачей флага типа пространства имен, и тем самым продолжить свое выполнение в новом, изолированном от процесса-родителя пространстве.

Как сказано в документации [4], «когда процесс создает новое пространство имен контрольной группы с помощью clone() или unshare() с флагом CLONE_NEWCGROUP, его текущие cgroups каталоги становятся корневым cgroup каталогом нового пространства имен». Вот этот факт и предстоит увидеть обучающимся на данном этапе работы.

Можно предложить следующие варианты проверки видимости каталогов cgroups в процессе-потомке:

1.Использование в процессе-потомке вызова функции system(«/bin/bash»). В этом случаепроцесс-потомок вызывает внутри себя командный интерпретатор. В нем необходимо с клавиатуры выдать команду «cd /proc/self» для перехода в каталоге /proc в подкаталог процесса-потомка /proc/[pid]. Затем выдать команду «cat cgroup», чтобы вывести на экран содержимое файла cgroup. Этот файл содержит путь в файловой системе /sys/fs/cgroup к подкаталогу, описывающему контрольную группу, в которую входит процесс-потомок. Затем необходимо выдать команду «exit», чтобы из командного интерпретатора вернуться в процесс-потомок.

2.Использование в процессе-потомке вызова функции system(«cat /proc/self/cgroup»). Этот вызов сразу выводит на экран содержимое файла cgroup каталога /proc/[pid].

3.Вызов функции system() не является предпочтительным в программах, которые требуют привилегий, а вызовы clone() и unshared() с флагом CLONE_NEWCGROUP требуют привилегий администратора (CAP_SYS_ADMIN). Поэтому для наблюдения за содержимым файла /proc/[pid]/cgroup целесообразно прямое открытие файла вызовом fopen() с последующим чтением содержимого функцией fread() и закрытием функцией fclose().

Что должен увидеть обучающийся в случаях, когда процесс-потомок выполняется в общем с процессом-родителем пространстве имен контрольных групп и в изолированном пространстве?

Если процесс-потомок выполняется в общем с процессом-родителем пространстве Cgroup, то через содержимое файла /proc/[pid]/cgroup ему доступен весь путь к каталогу, описывающему контрольную группу процесса-родителя, вплоть до каталога /sys/fs/cgroup. Это позволяет процессу-потомку воздействовать на ограничение ресурсов процесса-родителя вследствие ошибочных или умышленных действий.

Если процесс-потомок выполняется в изолированном от процесса-родителя пространстве Cgroup, то содержимое файла /proc/[pid]/cgroup — это корневой каталог. То есть процесс-потомок не может подняться по дереву файловой системы к ограничениям ресурсов процесса-родителя и, соответственно, не имеет возможности воздействовать на них.

Две строки, представленные ниже, иллюстрируют эти положения (строки получены при запуске программ в ОС LinuxUbuntu 22.10):

0::/user.slice/user-1000.slice/user@1000.service/app.slice/app-org.gnome.Terminal.slice/vte-spawn-f9dda2da-431f-4602-9678-3a42e3f931cb.scope

0::/

В первой строке представлен пример содержимого файла /proc/[pid]/cgroup дочернего процесса, когда отсутствует флаг CLONE_NEWCGROUP при вызове clone() или unshare(). То есть дочерний и родительский процессы выполняются в общем пространстве имен контрольных групп. Представленная строка — это подкаталог в файловой системе /sys/fs/cgroup. Содержимое этого подкаталога полностью описывает ограничения на ресурсы процесса-родителя.Во второй строке представлено содержимое файла /proc/[pid]/cgroup дочернего процесса, когда установлен флаг CLONE_NEWCGROUP при вызове clone() или unshare().

Вывод: дочерний процесс выполняется в изолированном пространстве имен контрольных групп. Представленная строка — это корневой каталог, а это значит, что процессу потомку недоступны данные об ограничениях ресурсов процесса-родителя.

При изучении механизмов пространства имен контрольных групп обучающимся необходимо самостоятельно получить результаты, подобные представленным, и выполнить анализ полученных результатов с точки зрения возможного воздействия процесса-потомка на ресурсы процесса-родителя.

Таким образом обучаемые проходят по заданной методологии достижения искомого результата, осваивают новый теоретический материал по сопровождению выполняемого задания, принимают программно-технические решения и выполняют их, самостоятельно и наглядно для себя достигают конечный результат проделанных преобразований.

Заключение. Разработанная методика изучения и проверки возможностей управления ресурсами процессов на основе контрольных групп и изоляции ресурсов с помощью механизма пространства имен Cgroup, ориентирована на проведение практических занятий и лабораторных работ, содержит необходимый ознакомительный материал и механизмы проверки возможностей управления ресурсами процессов. Раздел дисциплины «Операционные системы» на основе современных программно-технических решений реализации безопасных информационных технологий с применением контрольных групп и изоляции ресурсов с помощью механизма пространства имен Cgroup позволит обучающимся лучше понять внутренние механизмы функционирования контейнеров, одним из элементов построения которых являются пространства имен, рассмотреть его как средство решения задач ограничения доступа к ресурсам, что является необходимой составляющей при разработке и применении безопасных информационных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Райс Л. Безопасность контейнеров. Фундаментальный подход к защите контейнеризированных приложений. СПб. : Питер, 2021. 224 с. (Серия «Бестселлеры O'Reilly»).
2. Home DTOS Other Projects Knowledge Base Linux Manpages Community Contribute Указатели на информацию о различных типах пространств имен // Linux Manpages. Обучение системному программированию на Linux / UNIX: информационный портал [Электронный ресурс]. URL: https://man7.org/linux/man-pages/man7/namespaces.7.html (дата обращения 16.03.2023).
3. Широков В. В., Щиголева М. А. Методические рекомендации по практическому освоению программных интерфейсов пространств имен операционных систем // Современное программирование. III Всероссийская научно-практическая конференция. Нижневартовск, 2020. С. 295-299.
4. Cgroup_namespaces (7) [Электронный ресурс] // Обзор пространств имен cgroup в Linux: Описание. Обзор пространств имен: [сайт]. URL: https://man7.org/linux/man-pages/man7/cgroup_namespaces.7.html (дата обращения 16.03.2023).

УДК 004.056.5 (371.693.4)
ГРНТИ 81.93.29

РАЗРАБОТКА ВИРТУАЛЬНОГО ТРЕНАЖЁРА ПО ПРОВЕДЕНИЮ СПЕЦИАЛЬНОГО ОБСЛЕДОВАНИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Шейхов Глеб Вагифович, Липатников Валерий Алексеевич, Островский Юрий Николаевич, Васильев Никита Алексеевич, Ледовская Кристина Геннадьевна
Военная академия связи им. С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: gleb.sheyhov@yandex.ru, vasn2020@mail.ru

Аннотация. В данной статье описана модель виртуального тренажера по проведению специального обследования объектов информатизации. Актуальность темы обусловлена высокой стоимостью аппаратуры для проведения специального обследования помещений для учебных учреждений, что требует кардинального снижения стоимости и повышение качества обучающихся по вопросам проверки специализированных помещений.

Ключевые слова: информационная безопасность; специальное обследование; виртуальная реальность; виртуальные тренажеры, объекты информатизации

DEVELOPMENT OF A VIRTUAL SIMULATOR FOR CONDUCTING A SPECIAL SURVEY OF INFORMATIZATION OBJECTS

Sheikhov Gleb, Lipatnikov Valery, Ostrovsky Yuri, Vasilev Nikita, Ledovskaya Kristina
The Military Academy of Telecommunications, named S. M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: gleb.sheyhov@yandex.ru, vasn2020@mail.ru

Absrtact. This article describes a model of a virtual simulator for conducting a special survey of informatization objects. The relevance of the topic is due to the high cost of equipment for conducting a special examination of premises for educational institutions, which requires a drastic reduction in the cost and improvement of the quality of students on the inspection of specialized premises.

Keywords: information security; special examination; virtual reality; virtual simulators, informatization objects.

Введение. Повсеместное внедрение информационных технологий подарило людям огромное количество возможностей, однако и поставило перед ними новые задачи, связанные с безопасностью объектов информатизации. В современных реалиях защита объектов информатизации Российской Федерации является основополагающим критерием для развития и безопасности нашей страны. Мощные системы разведки иностранных государств, оснащённые современными техническими средствами и направленные на снятие информации, дают возможность непрерывно получать данные различного уровня секретности [1, 2].

Перехват информации осуществляется по техническим каналам утечки информации (ТКУИ). ТКУИ — способ утечки информации с объекта защиты системы закрытой связи, образованной совокупностью источников

информации, среды распространения сигнала и технические средства разведки злоумышленника. Среда распространения опасного сигнала — материальное вещество между источником сигнала и местом воздействия аппаратуры перехвата. В качестве среды распространения могут выступать проводники связи, электропитания, трубы систем вентиляции, окружающее пространство. Для обеспечения безопасности специализированных помещений и объектов информатизации, расположенных в них, проводится специальная проверка. Специальное обследование помещений нацелено на локализацию (обнаружение, устранение, ослабление) возможных каналов утечки секретной информации, ее кражи, потери, несанкционированного доступа (НСД) и уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования [3].

Анализ релевантных работ. Ни для кого не секрет, что получение информационного доступа к закрытым каналам передачи данных, секретной информации на данный момент реализуется с использованием современных технических средств радиоэлектронной разведки [4]. Этому способствует высокий уровень развития технологий в различных областях техники, которые позволяют создавать высокоэффективные автономные автоматические средства получения информационного доступа в портативном, малом и сверхмалом вариантах.

Данными проблемами и поиском их решения в своих работах выступали: А. П. Жук, Е. П. Жук, А. И. Тимошкин, О. М. Лепёшкин, А. А. Хорев.

Из проводимого анализа тенденций развития информационных систем, позволяющих сделать вывод о том, что в последние годы появилась и развивается новая современная технология — технология защиты информации в компьютерных информационных системах и в сетях передачи данных. Продвижение и развитие данной технологии требует больших финансовых затрат. Однако все это позволяет избежать значительных потерь и ущерба, которые могут возникнуть при реальной реализации угроз информационным системам (ИС) и информационным технологиям (ИТ) [5].

Также имеются рекомендации по обнаружению закладных устройств с применением организационно-технических мер, которые в определенной мере помогут решить эту проблему. В ней рассмотрен обширный список технических средств поиска электронных устройств перехвата информации, проведена их классификация и исследованы технические характеристики и особенности работы, даны рекомендации по использованию этих средств в практической деятельности органов защиты информации, а также о проведении специальных работ по методике проведения специального обследования [6].

Существенным недостатком данных работ считаю, отсутствие практической составляющей визуализации процесса обучения, что негативно сказывается на уровне усвоения материала обучающимися.

Также была рассмотрена статья С. Ф. Сергеев «Виртуальные тренажеры: проблемы теории и методологии проектирования», в которой рассматриваются актуальные системы виртуального обучения, а также проблемы их построения и реализации в системе обучения начинающих операторов.

Основываясь на вышеуказанном анализе, можно сделать вывод, что на данный момент создание виртуального тренажёра для обучения начинающих специалистов-операторов является актуальным вопросом и имеет положительные перспективы для его реализации.

Цель данной разработки состоит в повышении качества практической подготовки специалиста за счет погружения обучающегося в область предметных знаний изучаемой дисциплины с использованием технологий визуализации посредством виртуального тренажера для поиска закладных устройств, с одновременным снижением затрат на использование специализированного оборудования, за счет стереоскопической визуализации модели тренажера.

Задача заключается в разработке тренажёра, предназначенного для получения первичных навыков проведения специального обследования выделенных помещений и объектов информатизации с применением технологии Virtual Reality (VR).

Выбор метода решения задачи. Для решения поставленной цели и задачи мною был разработан алгоритм для успешного взаимодействия с виртуальным тренажёром. Обучающийся будет выполнять мероприятия по поиску закладных устройств посредством визуального осмотра, а также с использованием специальных технических средств. Погружаясь в виртуальное пространство, он видит перед собой смоделированное специальное помещение, где может перемещаться по сцене и выполнять все необходимые действия, такие как осмотр всех объектов помещения, столов, радиаторных батарей, электрооборудования, розеток, вентиляции, заземления. В данном проекте возможен не только визуальный осмотр помещения, но и использование специализированных устройств для поиска технического канала утечки информации, таких как «Нелинейный локатор NR-900EMS» и «Пиранья ST-033». Структура виртуального тренажера представлена на рис. 1.

Виртуальный тренажер выполняет функцию визуализации специального обследования помещения с помощью технических и программных средств. Моделирует виртуальное пространство, передаваемое человеку через зрение и слух, имитируя воздействие окружающей виртуальной реальности путем синтеза реакций и свойств в интерактивном мире, где все процессы рассчитываются, анализируются и выдаются как поведение в реальном времени. Данное устройство имитирует возможность поиска закладных устройств путём проведения специального обследования без прибора, а также поиск закладных устройств путём проведения специального обследования с использованием «Нелинейного локатора NR-900EMS» и «Пиранья ST-033». Отличительной особенностью

VR технологии является возможность при помощи специализированной гарнитуры, отслеживать положение обучающегося в пространстве, а именно повороты и наклоны головы, движение рук, возможность перемещаться в виртуальном пространстве, как в реальном [7-11].

Рис. 1. Структура виртуального тренажера

В тренажере используются виртуальные имитаторы измерительных приборов таких как «Пиранья ST-033» и как «Нелинейный локатор NR-900EMS». «Пиранья ST-033» — универсальный прибор обнаружения, который предназначен для поиска и локализации технических средств негласного получения информации, а также для решения ряда иных задач по защите информации. Изделие позволяет работать в таких режимах, как высокочастотный детектор-частотомер, СВЧ детектор, анализатор проводных линий, детектор инфракрасных-излучений, детектор низкочастотных магнитных полей и т.д. «NR-900EMS» — предназначен для поиска закладных технических средств съема информации, содержащих полупроводниковые компоненты, например, радиомикрофоны, проводные микрофоны, средства аудио и видеозаписи и др. Изделие позволяет выявлять указанные средства вне зависимости от их функционального состояния, т.е. находящиеся как во включенном, так и выключенном состоянии. Изделие обеспечивает эффективный поиск и достоверное определение местоположения объектов поиска в ограждающих строительных конструкциях (пол, потолок, стены), а также в мебели и других предметах интерьера. На рис.2 представлена модель выделенного помещения изнутри, разработанная в среде Unity [12, 13].

Рис. 2. Модель выделенного помещения изнутри

Проведение внешнего осмотра и подготовка к работе, включение тренажера, контроль его исправности. Управление тренажером осуществляется кнопками взаимодействия, расположенных на беспроводном контроллере. Для проведения специального обследования обучаемый открывает двери специализированной аудитории нажатием кнопки «Тачпад» на контролере управления, который отвечает за взаимодействие обучающегося с предметами. Далее производится осмотр помещения на наличие закладных устройств. Перемещение (телепортация) внутри аудитории осуществляется с использованием контроллера наведения на указанное место, с удержанием кнопки «Триггер». Взаимодействие со всеми объектами в виртуальном тренажере осуществляется с помощью нажатия и удерживания кнопки «Триггер». Предметы, размещённые на столах в виртуальном помещении, также можно перемещать и осматривать, путем зажатия кнопки «Триггер» и не отпуская ее перемещать данный предмет. Закладные устройства могут находится как в источниках электропитания, так и в вентиляции помещения.

Обучающийся подходит к электрощиту, нажимает и удерживает кнопку «Триггер» для открытия крышки электрического щита, затем осматривает его. Для поиска закладных устройств в вентиляциях, кондиционерах, потолочных плитах требуется переместить стул к вентиляции и произвести визуальный осмотр, далее выполнить аналогичные последовательные действия для взаимодействия с объектами. Обучаемый подходит к стулу и удерживая клавишу «Триггер» переносит стул в требуемое место отпускает кнопку «Триггер», после чего нажатием кнопки «Тачпад» перемещается на него. Обучаемый, увидев решётку вентиляции, нажимает «Триггер» для ее открытия. Для проведения спец. обследования помещения с использованием приборов, обучающийся подходит к столу, на котором лежат такие устройства как: «Нелинейный локатор NR-900EMS» и «Пиранья ST-033». После того как обучающийся становится напротив устройства, которым хочет воспользоваться, он нажимает кнопку «Триггер», чтобы подобрать упавший предмет. При выборе прибора «Пиранья ST-033» обучающийся проводит спец. обследование аудитории путем поиска «бликов», которые подсказывают о местонахождении закладного видеоустройства. Критерием оценки при выполнении данного учебного задания выступает временной промежуток, за который обучающийся должен обнаружить и собрать все закладные устройства [14].

Виртуальный тренажёр моделирует методику проведения специального обследования в выделенном помещении без использования специальных приборов, в том числе и с использованием виртуальных приборов по поиску закладных устройств различного типа [15].

Для оценки эффективности тренажера был проведен эксперимент на нескольких рабочих тестовых группах: первая группа при изучении темы использовала тренажер, а вторая нет. Оценка эффективности осуществлялась путем проведения теста на изученную тему. Результаты эксперимента, приведенные на рис. 3, показали, что группа № 1, использующая тренажер, заметно повысила свою успеваемость по сравнению с группой № 2, которая не использовала тренажер.

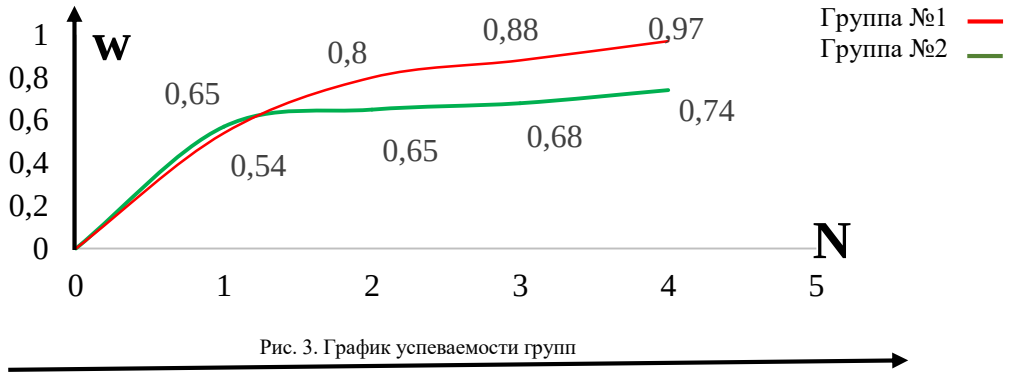


Рис. 3. График успеваемости групп

Заключение. Практическое применение виртуального тренажёра в учебном процессе позволит проводить мероприятия специального обследования без использования специализированного дорогостоящего оборудования такого, как «Нелинейный локатор 900EMS» и «Пиранья ST-033». Кроме того, для виртуального тренажера были дополнительно разработаны и установлены виртуальные закладные устройства несанкционированного съема информации. Применение данной методики позволит повысить качество практической подготовки военных специалистов, сократить затраты на их обучение, а также сократить эксплуатационный ресурс дорогостоящего специального оборудования.

СПИСОК ЛИТЕРАТУРЫ

1. Островский Ю. Н., Васильев Н. А. Используя цифровые технологии виртуальный тренажёр по развёртыванию аппаратной связи // Журнал Вестник военного образования. 2022. № 4 (37). С. 83-86.
2. Джонатан Л. Виртуальная реальность в Unity. ДМК Пресс, 2016. 313 с.
3. Безопасность информационных систем : учеб. пособие. М. : Флинта, Наука, 2015.184 с.
4. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Защита информации техническими средствами : учеб. пособие. СПб. : НИУ ИТМО, 2012. 416 с.
5. Жук И. Е. Концептуальные основы информационной безопасности // Информация и безопасность. 2010. 44 с.
6. Хорев А. А. Техническая защита информации. М. : НПЦ Аналитика, 2008. 436 с.
7. Пахомова А. С., Пахомов А. П., Разинкин К. А. К вопросу о разработке структурной модели угрозы компьютерной разведки // Информация и безопасность. 2013.Т. 16. № 1. С. 115-118.
8. Чаплыгина М. П. Методика контроля защищенности автоматизированной системы обработки конфиденциальной информации от несанкционированного доступа к информации // Молодой ученый. 2016. С. 169.
9. Костарев С. В., Карганов В. В., Липатников В. А., Технологии защиты информации в условиях кибернетического противоборства : науч. монография. СПб. : ВАС, 2020. 716 с.
10. Липатников В. А., Тихонов В. А. Распознавание вторжений нарушителя при управлении кибербезопасностью инфраструктуры интегрированной организации на основе нейро-нечетких сетей и когнитивного моделирования // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019) : сборник научных статей VIII Международной научно-технической и научно-методической конференции : в 4 т. 2019. С. 659–664.
11. Липатников В. А., Ломанов А. А. Способ обнаружения и классификации многоэтапной атаки на основе долгой краткосрочной памяти // Технологии. Инновации. Связь : сборник материалов научно-практической конференции. СПб., 2022. С. 104-108.

12. Lipatnikov V. A., Kuzin P.I., Rabin A. V. The method of increasing the reliability of noise immunity when receiving information in radio communication systems of the SHF and EHF ranges // Journal of Physics: Conference Series. K., 2020. Pp. 52100.
13. Rabin A. V., Lipatnikov V. A., Kuzin P. I. Signal protection methods in channels with Nakagami fading // JOP Conference Series: Metrological Support of Innovative Technologies. Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations. K., 2020. Pp. 52078.
14. Тренажерно-обучающие системы с применением технологий виртуальной и дополненной реальности / Осадчий А. И. [и др.] // Информация и космос. 2021. № 1. С. 65-72.
15. Островский Ю. Н., Шайсултанов М. Х. Нейрокомпьютерный интерфейс для обучающих систем военного назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сборник научных статей. 2018. С. 520-524.

УДК 37.01

ФИНАНСОВЫЕ И ПОЛИТИЧЕСКИЕ РИСКИ ИНФОРМАЦИОННОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ

Шубинский Максим Игоревич
Санкт-Петербургский государственный технологический институт (технический университет),
Московский просп., 24-26/49, Санкт-Петербург, 190013, Россия
e-mail: shubinskiy@gmail.com

Аннотация. В настоящей работе рассмотрена модель информационной образовательной среды с точки зрения обеспечения ее безопасности. Дано общее описание рисков ИОС. Подробно рассмотрены финансовые риски и политические риски информационной образовательной среды.

Ключевые слова: финансовые риски, политические риски, информационная образовательная среда.

FINANCIAL AND POLITICAL RISKS OF THE INFORMATION EDUCATIONAL ENVIRONMENT

Shubinskiy Maxim
St. Petersburg State Institute of Technology
24-26/49 Moscow's Av, St. Petersburg, 190013, Russia
e-mail: shubinskiy@gmail.com

Absrtact. This paper considers a model of the information educational environment from the point of view of ensuring its security. A general description of the information educational environment risks is given. Financial risks and political risks of the information educational environment are considered in detail.

Key words: management risks; financial risks; political risks; information educational environment.

Введение. Опишем упрощенную модель информационной образовательной среды образовательного учреждения с точки зрения обеспечения ее безопасности. Наша модель будет основываться на теории рисков.

Одно из ключевых понятий для модели безопасности информационно-образовательной среды — это понятие угрозы.

Под угрозой будем понимать потенциально возможное событие, которое может привести к нанесению ущерба. Риск — определяет степень опасности воздействия угрозы (или набора угроз) на систему (объект, ресурс или процесс).

Для каждой информационно-образовательной среды существуют риски, реализация которых приведет информационную среду в неработоспособное состояние или в состояние, в котором эффективность работы среды будет существенно снижена. Для каждого риска есть некоторый набор угроз.

Часть из этих угроз являются актуальными. Актуальными угрозами считается те угрозы, которые имеют высокую степень опасности воздействия на систему.

Под безопасной информационно-образовательной средой мы будем понимать такую информационную среду, для которой определен набор актуальных угроз наступления рисков и для каждой из угроз выбран способ защиты, позволяющий наиболее эффективно предотвратить угрозу или минимизировать возможные потери (рис. 1).

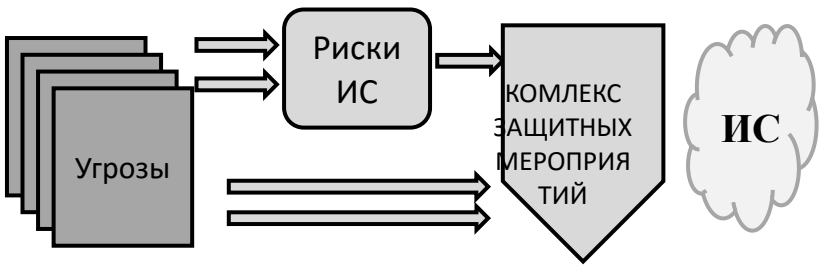


Рис. 1. Безопасная информационная среда

На рисунке видно, что выбранная защита, частично нейтрализует угрозы, а частично минимизирует потери от реализованных рисков. Таким образом, для получения конкретной модели безопасной информационно-образовательной среды необходимо описать возможные группы рисков данной среды, определить набор актуальных угроз, которые могут привести к реализации рисков и определить комплекс защитных мероприятий, позволяющих нейтрализовать угрозы или минимизировать их последствия. Необходимо отметить, что в комплекс мероприятий должны входить и технические, и педагогические и организационные действия.

Угрозы безопасности информационно-образовательной среды ОУ. Рассмотрим более подробно понятие угрозы и примем следующее определение. Угроза – это реально или потенциально возможные действия, приводящие к финансовым или репутационным потерям. В любой системе проводится процедура выявления опасностей, в отношении, процессов или ресурсов с целью определения угроз, влияющих на эти процессы и ресурсы в процессе их функционирования. В результате анализа проводится классификация угроз и описание характера их проявлений, позволяющая в последующем перейти к оценкам рисков.

Для построения верной модели безопасной информационно-образовательной среды ОУ главным является правильный анализ возможных угроз информационной безопасности. Принципы классификации угроз могут быть различны, но они должны иметь строгое описание условий классификации.

1.Классификация по принципу воздействия. Угрозы могут быть:

–умышленными, когда существует угроза, являющаяся результатом преднамеренных воздействий на информационную образовательную среду;

–непредумышленными, когда существует угроза, являющаяся результатом непреднамеренных или случайных воздействий.

2.Классификация по объектам воздействия:

–угрозы, направленные на порчу оборудования;

–угрозы, направленные на порчу программного обеспечения;

–угрозы, направленные на потерю данных, принадлежащих ОУ;

–угрозы, направленные на неправомерное использование данных, принадлежащих ОУ;

–угрозы, направленные на ухудшения имиджа учреждения;

–угрозы, направленные на нежелательные воздействия на учащихся и работников.

Для рассматриваемой нами модели безопасной образовательной среды, самой удобной будет являться:

3.Классификация угроз по требуемым мерам противодействия:

–угрозы для противодействия, которым надо применить технические решения;

–угрозы для противодействия, которым надо применить программные средства;

–угрозы для противодействия, которым надо применить организационные решения;

–угрозы для противодействия, которым надо применить педагогические решения;

–угрозы для противодействия, которым надо применять комбинацию разнообразных мер.

Для составления набора актуальных угроз возникновения рисков информационной среды ОУ, будем пользоваться последней из предложенных выше классификаций.

Для построения верной модели безопасной информационной среды нет смысла рассматривать все существующие угрозы. К сожалению, 152-ФЗ и иные нормативные документы придерживаются принципа избыточных требований, что является разумным для учреждений, например, оборонной промышленности, но неразумно для учреждений социальной сферы. Мы будем использовать принцип целесообразности, используемый в международных стандартах информационной безопасности, который не полностью стыкуется с российским законодательством в сфере информационной безопасности, но применим в условиях более широкой задачи — создать безопасную информационно-образовательную среду учреждения. Наша задача рассмотреть полный набор угроз, и выбрать из него те угрозы вероятность осуществления, которых наиболее велика.

Общее описание рисков ИОС. Рассмотрим риски информационной образовательной среды. В данной работе предлагается следующий критерий разбиения рисков на группы. Риски группируются в соответствии с объектом (субъектом) образовательного процесса, на который они воздействуют.

–Педагогические риски — отрицательные воздействия на учебный процесс;

–Психолого-медицинские риски — отрицательные воздействия на жизнь и здоровье учащихся и педагогов;

–Управленческие (или организационные) риски — отрицательное влияние на управленческие процессы;

–Финансовые риски — отрицательные воздействия на финансовое состояние учреждения (прямые финансовые потери);

–Политические риски — отрицательные воздействия на репутацию учреждения.

В группу педагогических рисков, включаются те риски, которые могут повлиять на учебный процесс. Здесь надо отметить риски, в результате реализации которых будет невозможно использовать компьютерное оборудования при ведении занятий. Стоит напомнить, что, согласно новым ФГОС, использование подобного оборудования является обязательным.

К группе психолого-медицинских рисков, прежде всего, относятся те риски, которые могут повлиять на здоровье, как учащихся, так и сотрудников ОУ. В группу управленческих рисков, включим те риски, которые

приведут к необходимости временной или постоянной перестройки организационной структуры образовательного учреждения. Ярким примером подобного риска может служить риск временной неработоспособности локальной сети учреждения при использовании системы фиксации хода образовательного процесса (например, электронный журнал).

В группу *финансовых рисков* включим все те риски, которые связаны с понесением учреждением финансового ущерба. Это в первую очередь порча оборудования и программного обеспечения. Вторая группа финансовых рисков связанна с вопросами госзаказа, начисления заработной платы и иных экономических вопросов. В группу *политических рисков* включим риски, отрицательно влияющие на имидж учреждения, что может сказаться на наборе желающих учиться в данном учреждении, и может привести либо к ухудшению контингента учащихся, либо даже к его уменьшению, что при нынешних принципах финансирования может серьезно сказаться на бюджете. Часть политических рисков связана с необходимостью выполнением ОУ федеральных и региональных законодательных актов, и иных нормативных документов, связанных с информатизацией, а также требований надзорных органов. Необходимо отметить, что иногда грани, отделяющие одну группу рисков от другой достаточно условны. Так, например, есть часть рисков, которые можно отнести и к педагогическим рискам, и к психолого-медицинским.

Еще один важнейшим фактором является то, что существуют угрозы, которые могут привести к реализации сразу нескольких рисков. Сгоревшее оборудование приведет как к отмене занятия (педагогический риск), так и к прямым финансовым потерям (финансовый риск). Конечно, конкретные наборы рисков могут отличаться в зависимости от региона, особенностей учреждения, его уровня информатизации, но значительная часть рисков, а также общие подходы к созданию безопасной информационной среды ОУ будут одинаковы.

В данной работе мы подробнее остановимся на не типичных для педагогики группах рисков. К сожалению, в большинстве статей, посвященных проблемам образования, не рассматриваются финансовые и политические риски образовательной среды. Именно данные риски являются основной темой сегодняшней работы.

Финансовые риски. Вспомним, что финансовые риски — это отрицательные воздействия на финансовое состояние учреждения (прямые финансовые потери). Финансовые риски, прежде всего, связаны с понесением учреждением финансового ущерба. В данном случае, мы имеем несколько групп рисков, связанных с вопросами работоспособности оборудования и программного обеспечения. Построим перечень подобных рисков.

Первая группа рисков будет касаться только неработоспособности целиком компьютеров.

–Риск прекращения работы (неработоспособность) студенческого (ученического) компьютера в компьютерном кабинете или медиатеке.

–Риск прекращения работы (неработоспособность) компьютера преподавателя, расположенного в каком-либо образовательном кабинете.

–Риск прекращения работы компьютера, расположенного в медиатеке или в преподавательской (учительской).

–Риск неработоспособности административного компьютера, то есть компьютера, за которым может работать декан, проректор, ректор (директор школы и его заместители), секретарь и другие сотрудники, не связанные непосредственно с образовательным процессом.

–Риск неработоспособности компьютера в бухгалтерии.

–Риск неработоспособности одного из серверов учреждения.

–Вторая группа рисков касается работы программного обеспечения компьютеров.

–Риск полного прекращения работы ученического(студенческого) компьютера из-за выхода из строя его операционного программного обеспечения.

–Риск полного прекращения работы компьютера преподавателя из-за выхода из строя его операционного программного обеспечения.

–Риск полного прекращения работы административного компьютера из-за выхода из строя его операционного программного обеспечения.

–Риск полного прекращения работы компьютера бухгалтеров из-за выхода из строя его операционного программного обеспечения.

–Риск полного прекращения работы одного из серверов учреждения из-за выхода из строя его операционного программного обеспечения.

–Риск частичного выхода из строя ученического (студенческого) компьютера из-за прекращения работы одного из важных приложений.

–Риск частичного выхода из строя компьютера преподавателя из-за прекращения работы одного из важных приложений.

–Риск частичного выхода из строя административного компьютера из-за прекращения работы одного из важных приложений.

–Риск частичного выхода из строя компьютера бухгалтеров из-за прекращения работы одного из важных приложений.

–Риск частичного выхода из строя одного из серверов учреждения из-за прекращения работы одного из важных приложений.

Все риски из данной группы достаточно реальны, но на них редко обращают внимание, поскольку чаще всего они устраняются системным администратором. Проблемой является наличие в школе ставок системного администратора и администратора серверов (в ВУЗах такой проблемы нет). Поскольку в их отсутствие, все вопросы будет решать учитель информатики, зачастую являющийся ответственным за все школьное «железо», что никак не следует из школьного расписания.

Третья группа финансовых рисков связанна с вопросами госзаказа, начисления заработной платы и иных экономических вопросов. Эта группа наиболее важная, однако, вопросы, касающиеся непосредственной работы бухгалтеров в образовательном учреждении, практически не рассматривались в литературе. Построим перечень финансовых рисков данной группы.

–Риск выхода из строя программного обеспечения, связанного с начислением заработной платы.

–Риск выхода из строя программного обеспечения, связанного с бухгалтерией и бухгалтерской отчетностью учреждения.

–Риск выхода из строя программного обеспечения, обеспечивающего вопросы государственного задания (в том числе обеспечивающего аукционы).

–Риск подключения в систему начисления заработной платы некоторого пользователя (зарегистрированного или незарегистрированного), который будет влиять на выплаты сотрудникам. Здесь возможно, как неоправданное увеличение, так и уменьшение выплат, и/или подключение еще одного или нескольких неработающих сотрудников.

–Риск проведения конкурса в системе государственного заказа незарегистрированным человеком с целями отличными от целей руководства учреждения.

–Риск использования программного обеспечения, связанного с бухгалтерией и бухгалтерской отчетностью, с целью причинения ущерба учреждению.

Если три первых риска третьей группы, отличаются от рисков второй группы только программным обеспечением, которое может выйти из строя, то следующие три привязаны к нарушителям, которые считаются готовыми пойти на данный риск.

Политические риски. Политические риски — это отрицательные воздействия на репутацию учреждения.

В группу политических рисков включим риски, отрицательно влияющие на имидж учреждения, что может сказаться на наборе желающих учиться в данном учреждении, и может привести либо к ухудшению контингента обучающихся, либо даже к его уменьшению, что при нынешних принципах финансирования может серьезно сказаться на бюджете. Часть политических рисков связана с необходимостью выполнением ОУ федеральных и региональных законодательных актов, и иных нормативных документов, связанных с информатизацией, а также требований надзорных органов.

Рассмотрим первую группу рисков. В данную группу обязательно включаются риски связанные с сайтом учреждения.

Риск отсутствия рабочей версии сайта учреждения. Конечно, в настоящее время, этот риск минимален для государственных образовательных учреждений, но некоторые частные учреждения вполне могут несколько месяцев обойтись без сайта.

Риск выхода из строя, как сайта целиком, так и части сайта, случающийся по техническим причинам. Это может быть выход из строя, небольшого раздела, который при этом посещается довольно часто, а может быть, будут испорчены или не будут открываться 3-4 раздела, которые крайне редко посещают, и в этом случае ОУ может не скоро узнать об этом факте. В данном случае, речь идет о случайном выходе из строя фрагмента (фрагментов) сайта.

Риск плохого (не полного, не аккуратного или не красивого) представления информации на сайте. Этот риск часто встречается в деятельности ОУ.

Риск выхода из строя как сайта целиком, так и части сайта, случающийся после преднамеренного воздействия учащихся или иных лиц. Этот риск включает в себя и злонамеренные действия людей непосредственно по сайту ОУ (более редкие, но более серьезные проблемы), и злонамеренные действия людей, направленные на целую группу разноплановых сайтов, в которую попадает и сайт ОУ.

Риск неправильной (устаревшей) информации об ОУ, размещенной на официальных сайтах муниципальной, районной, региональной или федеральной систем образования.

Рассмотрим вторую группу рисков. В нее включим риски, связанные с невыполнением ОУ федеральных законов, постановлений и других региональных нормативных актов, связанных с информатизацией образовательных учреждений. В этой группе может быть много рисков, связанных с тем или иным официальным документом, но мы будем рассматривать только три риска, которые отличаются друг от друга реальными возможностями ОУ.

Риск невыполнения ОУ федеральных законов, постановлений или другой нормативной документации из-за финансовой невозможности выполнения. Этот риск, вполне, реален и, например, все законодательные акты по обеспечению безопасности персональных данных при правильном их применении должны заставлять все школы и методические центры платить за обеспечение безопасности большие деньги.

Риск невыполнения ОУ федеральных законов, постановлений или другой нормативной документации из-за недостаточного уровня знаний работников ОУ. В данном случае, необходим специалист, который мог бы выполнять те или иные постановления, например, связанные с информационной безопасностью. Однако, обычно, такого специалиста в ОУ нет.

Риск невыполнения ОУ федеральных законов, постановлений или другой нормативной документации из-за собственных недоработок. Указанный риск отличается от предыдущего тем, что ОУ часто нарушают законы, зная, что так лучше не делать и зная, как можно сделать правильно и не дорого.

Конечно, нельзя сказать, что мы рассмотрели абсолютно все политические и финансовые риски информационно-образовательной среды. Однако по результатам данной работе видны и большая множественность возможных угроз ИОС и требуемое разнообразие необходимых защитных механизмов.

Заключение. Стоит отметить, что, когда мы говорим о рисках, нас интересуют не только причины возникновения тех или иных угроз, но и возможные последствия. Для минимизации возможных потерь имеет существенное значения не только причина, по которой, например, во время конкретного занятия отсутствует Интернет (это могут быть внутренние проблемы с оборудованием, технические проблемы провайдера, или даже неоплата услуг провайдера) но и последствия данного события.

Таким образом, для риска выхода из строя программного обеспечения, например, связанного с бухгалтерией и бухгалтерской отчетностью учреждения выбирается набор угроз. Затем, для минимизации потерь, надо определить перечень мероприятий, которые, с одной стороны, позволят уменьшить вероятность возникновения риска, а с другой избежать неприятностей с бухгалтерским программным обеспечением, если, несмотря на все принятые меры, проблемы возникнут.

Конечно, конкретные наборы рисков могут отличаться в зависимости от региона, особенностей учреждения, его уровня информатизации, но значительная часть финансовых и политических рисков, а также общие подходы к созданию безопасной информационной среды ОУ будут одинаковы.

СПИСОК ЛИТЕРАТУРЫ

1. Шубинский М.И. Информационная безопасность школы // Вестник ОГУ. 2013. № 1 С. 108-112.
2. Обеспечение безопасности детей в информационной сфере: методические рекомендации для педагогов, психологов, родителей и всех заинтересованных сторон // Центр исследований «Сандж». Казахстан. 2010. [Электронный ресурс] URL: http://www.pandia.ru/text/77/129/116.php (дата обращения :10.10.2023).
3. Климонтова Г. Н. Информационная безопасность в компьютерных системах. Выработка практических навыков учащихся // Народное образование. 2013. № 6. С. 265-270.
4. Бояров Е. Н. Ключевые проблемы информационной безопасности сферы образования // Педагогика высшей школы. 2016. С. 42-45.
5. Жарникова Ю. С. Угрозы информационной безопасности образовательного учреждения // Молодой ученый. 2017. С. 60-63.
6. Шубинский М. И. Педагогические риски информационной образовательной среды // Электронный журнал Экстернат. 2021. [Электронный ресурс]. URL: http://ext.spb.ru/index.php/17844 (дата обращения 10.10.2023).
7. Шубинский М. И. Риски информационной образовательной среды // Региональная информатика и информационная безопасность : сборник трудов. Вып. 11. СПб. : СПОИСУ, 2022. С. 394-398.

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «ИНТЕЛЛЕКТУАЛЬНЫЕ БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»

УДК 004.896

ИССЛЕДОВАНИЕ МЕТОДОВ ВИЗУАЛЬНОЙ НАВИГАЦИИ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ СРЕДСТВ В СЛОЖНЫХ УСЛОВИЯХ ЭКСПЛУАТАЦИИ

Беляев Павел Юрьевич, Зикратов Игорь Алексеевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, Санкт-Петербург, 193232, Россия
e-mails: Belyaev.edu@gmail.com, zikratov.ia@sut.ru

Аннотация. В статье рассматриваются основные методы визуальной навигации беспилотных летательных аппаратов в сложных условиях. Наиболее перспективными являются методы компьютерного зрения за счет минимизации проблем с накоплением ошибки и влияния шума.

Ключевые слова: визуальная навигация; распознавание объекта; сверточные нейронные сети; БПЛА; сенсоры.

ANALYSIS OF VISUAL NAVIGATION METHODS FOR UNMANNED AERIAL VEHICLES UNDER CHALLENGING OPERATING CONDITIONS

Belyaev Pavel, Zikratov Igor
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: Belyaev.edu@gmail.com, zikratov.ia@sut.ru

Abstract. The article discusses the main methods of visual navigation of drones in complex environments. The most promising are computer vision methods due to the minimization of problems with the accumulation of noise influence error.

Keywords: visual navigation; object detection; convolutional neural networks; UAVs; sensors.

Введение. В последние годы автономные робототехнические системы и беспилотные летательные аппараты (БПЛА) стали представлять все больший интерес в различных областях, таких как исследования, разведка, мониторинг, доставка грузов и другие ресурсоемкие задачи. Одной из ключевых задач в разработке таких систем является разработка эффективных методов навигации, которые позволят БПЛА безопасно и точно перемещаться в требуемой области. Визуальная навигация представляет собой перспективный подход, который использует визуальную информацию для определения положения и ориентации БПЛА в окружающей среде. Также, в последние годы сверточные нейронные сети продемонстрировали выдающуюся эффективность в задачах обработки изображений, что позволяет исследовать применение этой технологии в задачах визуальной навигации [1].

Использование методов оптической навигации БПЛА в сложной местности представляет значительные технические и вычислительные сложности. Сложная местность может включать нерегулярный рельеф, препятствия, изменчивые условия освещения, ограниченный обзор и видимость, а также непредсказуемые природные явления. Нерегулярный рельеф и наличие препятствий создают трудности навигации. Неровная поверхность и выступающие объекты могут затруднять извлечение признаков и точную локализацию, что влияет на надежность системы. Условия освещения в сложной местности могут быть непредсказуемыми и изменчивыми, что затрудняет обработку визуальных данных и усложняет определение положения и ориентации БПЛА. Такое же влияние имеет ограниченные обзор и видимость. Присутствие препятствий, таких как здания, деревья, горные склоны или другие, может ограничивать доступную визуальную информацию, что уменьшает точность определения положения. Кроме того, плохая видимость из-за тумана, дождя или снегопада также затрудняет навигацию напрямую воздействуя на оптику БПЛА, а также значительно понижает точность оптических методов. Сильный ветер или воздушные потоки, могут также оказывать влияние на оптическую навигацию. Эти факторы могут приводить к нестабильности и неопределенности в движении БПЛА, что усложняет точную локализацию и навигацию в целом.

Основными методами оптической навигации БПЛА служат: Оптический поток (Optical flow) [2-4], оптическое отслеживание (Optical Tracking) [5, 6], методы стереозрения [7, 8], лидарное зрение [9-11], компьютерное зрение [12, 13] и Simultaneous Localization and Mapping (SLAM) [14-16]. Оптический поток является методом, основанным на анализе движения пикселей на последовательных изображениях. Этот метод позволяет определить направление и скорость движения объектов с камеры БПЛА. Оптический поток широко используется для оценки скорости и контроля движения БПЛА.

Optical Tracking основан на использовании оптических датчиков (таких как камеры) для отслеживания и распознавания объектов в реальном времени. Оно позволяет БПЛА следить за выбранными объектами и управлять движением на основе их положения.

Методы стереозрения используют пару камер для восстановления трехмерной информации об окружающей среде. Анализируя смещение объектов на изображениях, полученных с разных камер, можно определить глубину и расстояние до объектов.

Лидарное зрение использует лазерные лучи для измерения расстояний до объектов и создания точной трехмерной карты окружающей среды.

Компьютерное зрение охватывает широкий спектр методов и алгоритмов для обработки и анализа изображений с целью извлечения полезной информации. В контексте оптической навигации БПЛА компьютерное зрение может быть использовано для обнаружения и распознавания объектов, извлечения признаков сцены, а также для обработки и интерпретации данных с других сенсоров.

SLAM представляет собой метод, который объединяет задачу определения положения и ориентации БПЛА с построением карты окружающей среды в режиме реального времени. SLAM использует комбинацию датчиков, таких как камеры, лидары, инерциальные измерительные устройства (IMU) и другие, для оценки положения БПЛА и создания трехмерной карты окружающей среды.

Каждый метод по-своему актуален исходя из входных данных для выполнения задачи, однако, большинство из них зависят от воздействия на сенсоры БПЛА и возможности работы в сложных условиях. Так же, при анализе подходов наиболее перспективным для сложных условий является подход на основе компьютерного зрения с применением сверточных нейронных сетей [17]. Метод автономной навигации БПЛА на основе сверточных нейронных сетей превосходит другие рассмотренные подходы благодаря своей способности эффективно анализировать и обрабатывать визуальную информацию. Также сверточные нейронные сети обладают высокой способностью извлекать признаки из изображений и обнаруживать сложные шаблоны и структуры, что позволяет методу данному подхожу достичь высокой точности в распознавании объектов, а также в определении положения и ориентации БПЛА на основе визуальных данных. Подробное сравнение методов представлено в таблице 1.

Таблица 1

Сравнение методов визуальной навигации БПЛА

Метод	**Преимущества**	**Недостатки**
Optical Flow	–Высокая скорость обработки; –Простота реализации; –Низкие вычислительные требования.	– Ограниченная точность в сложных условиях; –Проблемы с отслеживанием текстурно однородных областей; –Ошибки оценки движения объектов; –Накопление ошибки на больших расстояниях; –Влияние шума.
Optical Tracking	– Высокая точность; –Устойчивость к текстурным изменениям; –Возможность работы в режиме реального времени; –Гибкость в различных условиях.	–Зависимость от видимости объектов; –Влияние шума и ошибок измерений; –Ограниченная дальность отслеживания; –Проблемы с масштабированием.
Методы стереозрения	–Высокая точность в определении глубины; –Возможность оценки размеров объектов; –Работа в широком диапазоне условий; –Возможность работы в реальном времени.	– Ограниченная дальность; –Влияние на точность изображений; –Высокая вычислительная сложность.
Компьютерное зрение	–Гибкий анализ; –Возможность работы с различными типами данных; –Использование широкого спектра алгоритмов и моделей; –Возможность работы в режиме реального времени.	– Вычислительная сложность; –Необходимость обучения и настройки.
SLAM	–Одновременная локализация и построение карты; –Использование визуальной информации.	–Вычислительная сложность; –Накопление ошибок; –Зависимость от освещения и ландшафта.

При сравнении заметно, что большинство методов крайне зависимы от влияния шума, накопления ошибки и других осложнений. На основе этого наиболее перспективным в рамках автономной навигации являются методы на основе компьютерного зрения.

В работе [18] представлен метод автономной навигации, основанный на использовании глубоких сверточных нейронных сетей. Авторы предложили подход, в котором нейронная сеть обучается на большом объеме данных, включающих визуальную информацию с камер БПЛА и соответствующие команды управления. Глубокая сверточная нейронная сеть выполняет анализ входных изображений и выявляет характеристики, необходимые для принятия решений о навигации. Сеть обучается классифицировать различные элементы сцены, такие как земля, деревья, здания и другие препятствия. Она также способна определять положение БПЛА относительно этих элементов и принимать решения об управлении, чтобы избегать столкновений и успешно достигать целей навигации. В работе [19] предложен подход, в котором сверточные нейронные сети обучаются на обширном наборе данных, включающем визуальные изображения с различных ракурсов и условий освещения. Целью обучения является обнаружение хорошо сопоставляющихся областей, которые могут быть использованы для точного определения положения и ориентации БПЛА. В работе [20] рассматривается метод, основанный на комбинированной архитектуре нейронных сетей и применении программируемой логической матрицы (FPGA) для обеспечения наблюдения за вырубкой леса и визуальной навигации БПЛА. Авторы предлагают предлагается подход, в котором комбинированная архитектура весовых нейронных сетей используется для обнаружения и классификации областей вырубки леса на основе входных визуальных данных. Нейронные сети обучаются на большом объеме данных, чтобы определить характеристики, связанные с вырубкой леса, и принимать решения о наличии или отсутствии вырубки. В работе [21] предлагается подход, в котором используется сверточная нейронная сеть, основанная на методе Faster R-CNN, для обнаружения и классификации препятствий в окружающей среде БПЛА. Нейронная сеть обучается на разнообразном наборе данных, включающем изображения плантаций деревьев, чтобы научиться распознавать различные типы препятствий, такие как деревья, ветки и другие объекты. Полученные результаты отображаются на бортовой системе БПЛА, которая позволяет осуществлять навигацию и избегать препятствий в режиме реального времени. Такой подход позволяет БПЛА автономно планировать и корректировать свой путь, учитывая препятствия и обеспечивая безопасное перемещение в плантациях деревьев. В работе [22] авторы предлагают подход, основанный на сотрудничестве морских беспилотных плавсредств (МБП) и БПЛА для выполнения миссий по поиску и спасению в водной среде. В данной работе предлагается подход, в котором используются методы визуальной навигации и управления на основе обучения с подкреплением для координации действий. Управление на основе обучения с подкреплением позволяет системе учиться на опыте и принимать решения о наилучшей стратегии действий в реальном времени. Агенты взаимодействуют друг с другом и с окружающей средой, получая награды или штрафы в зависимости от эффективности своих действий. Таким образом, система постепенно улучшает свою производительность и способность выполнять сложные миссии по поиску и спасению.

Недостатки методов, описанных в статьях, включают в себя: зависимость от качества обучающих данных, вычислительную сложность, чувствительность к условиям окружающей среды, ограниченную обобщающую способность и требования к аппаратным ресурсам. При правильном подходе к созданию системы можно значительно снизить данные недостатки и повысить общую точность и стабильность системы автономной навигации.

На основе исследованных работ была сформирована начальная схема подхода к визуальной навигации БПЛА. Первоначально оператору необходимо определить задачу полета (поиск объекта, разведка), затем необходимо определить область работы — на этом этапе происходит предварительная разметка области интереса для формирования данных для дообучения нейронной сети. В дальнейшем происходит запуск БПЛА и проведение работ. Предварительная модель представлена на рис. 1.

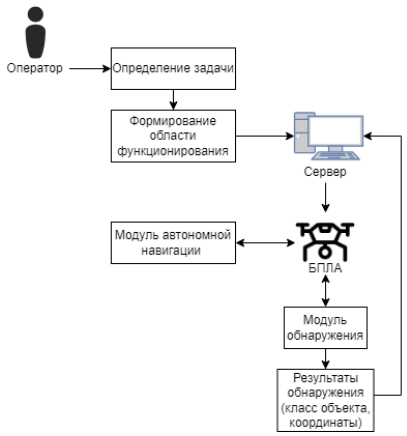


Рис. 1. Схема взаимодействия оператора с предложенной системы

Заключение. Таким образом, проведен анализ методов визуальной навигации беспилотных летательных аппаратов в задаче эксплуатации в сложной местности. В качестве перспективного был выделен метод на основе

компьютерного зрения исходя из того, что данный подход способен работать в сложных условиях без использования сложного оборудования, а также подстраиваться под изменяющуюся среду. В дальнейшем планируется реализация данного метода в симуляции и на реальных данных.

СПИСОК ЛИТЕРАТУРЫ

1. Object detection in optical remote sensing images: A survey and a new benchmark / Li K. [et al] // ISPRS journal of photogrammetry and remote sensing. 2020. Т. 159. С. 296-307.
2. Tchernykh V., Beck M., Janschek K. Optical flow navigation for an outdoor UAV using a wide angle mono camera and DEM matching // IFAC Proceedings Volumes. 2006. Т. 39. №. 16. С. 590-595.
3. Chao H., Gu Y., Napolitano M. A survey of optical flow techniques for UAV navigation applications // International Conference on Unmanned Aircraft Systems (ICUAS). IEEE, 2013. С. 710-716.
4. A comparative study of optical flow and traditional sensors in UAV navigation / Chao H. [et al] // American Control Conference. IEEE, 2013. С. 3858-3863.
5. Optical tracking system for multi-UAV clustering / Ming R. [et al] // IEEE Sensors Journal. 2021. Т. 21. №. 17. С. 19382-19394.
6. Laser tracking leader-follower automatic cooperative navigation system for UAVs / Ming R. [et al] // International Journal of Agricultural and Biological Engineering. 2022. Т. 15. №. 2. С. 165-176.
7. Combining stereo vision and inertial navigation system for a quad-rotor UAV / García Carrillo L. R. [et al] // Journal of intelligent & robotic systems. 2012. Т. 65. №. 1-4. С. 373-387.
8. Mustafah Y. M., Azman A. W., Akbar F. Indoor UAV positioning using stereo vision sensor // Procedia Engineering. 2012. Т. 41. С. 575-579.
9. A Global ArUco-Based Lidar Navigation System for UAV Navigation in GNSS-Denied Environments / Qiu Z. [et al] // Aerospace. 2022. Т. 9. №. 8. С. 456.
10. Cooperative navigation and guidance of a micro-scale aerial vehicle by an accompanying UAV using 3D LiDAR relative localization / Pritzl V. [et al] // International Conference on Unmanned Aircraft Systems (ICUAS). IEEE, 2022. С. 526-535.
11. UAV-based LiDAR Mapping with Galileo-GPS PPP Processing and Cooperative Navigation / Causa F. [et al] // International Conference on Unmanned Aircraft Systems (ICUAS). IEEE, 2022. С. 938-947.
12. A survey on vision-based UAV navigation / Lu Y. [et al] // Geo-spatial information science. 2018. Т. 21. №. 1. С. 21-32.
13. A simple visual navigation system for an UAV / Krajník T. [et al] // International Multi-Conference on Systems, Signals & Devices. IEEE, 2012. С. 1-6.
14. A survey of uav visual navigation based on monocular slam / Wei W. [et al] // IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC). IEEE, 2018. С. 1849-1853.
15. Nemra A., Aouf N. Robust cooperative UAV visual SLAM // IEEE 9th international conference on cyberntic intelligent systems. IEEE, 2010. С. 1-6.
16. Li X. Visual navigation in unmanned air vehicles with simultaneous location and mapping (SLAM). 2014.
17. Robust Autonomous Vehicle Computer-Vision-Based Localization in Challenging Environmental Conditions / Chuprov S. [et al] // Applied Sciences. 2023. Т. 13. №. 9. С. 5735.
18. Deep convolutional neural network based autonomous drone navigation / Amer K. [et al] //Thirteenth International Conference on Machine Vision. SPIE, 2021. Т. 11605. С. 16-24.
19. Shahoud A., Shashev D., Shidlovskiy S. Detection of good matching areas using convolutional neural networks in scene matching-based navigation systems // Proceedings of the 31st International Conference on Computer Graphics and Vision, Nizhny Novgorod, Russia. 2021. С. 27-30.
20. Combined weightless neural network FPGA architecture for deforestation surveillance and visual navigation of UAVs / Torres V. A. M. F. [et al] // Engineering Applications of Artificial Intelligence. 2020. Т. 87. С. 103-227.
21. Lee H. Y., Ho H. W., Zhou Y. Deep Learning-based monocular obstacle avoidance for unmanned aerial vehicle navigation in tree plantations: Faster region-based convolutional neural network approach // Journal of Intelligent & Robotic Systems. 2021. Т. 101. С. 1-18.
22. Cooperative USV–UAV marine search and rescue with visual navigation and reinforcement learning-based control / Wang Y. [et al] // ISA transactions. 2023.

УДК 004.946

ФОРМИРОВАНИЕ ЕДИНОЙ КИБЕРСРЕДЫ ПОСТИНДУСТРИАЛЬНОГО ОБЩЕСТВА НА БАЗЕ ЦИФРОВЫХ 5D-ДВОЙНИКОВ ПРОСТРАНСТВЕННО-РАСПРЕДЕЛЕННЫХ ОБЪЕКТОВ

Верхова Галина Викторовна, Акимов Сергей Викторович,
Прощенков Валерий Михайлович, Юрчик Даниил Сергеевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: galina500@inbox.ru, akimov-sv@yandex.ru, valery@proshchenkov.ru, urdanyrec@yandex.ru

Аннотация. Рассмотрены проблема геоинформационного обеспечения современного общества. Проанализировано современное состояние и перспективы развития цифровых двойников пространственных объектов. Представлена концепция эволюции цифровых 5D-двойников на примере продукта VELOCITY 5D. Рассмотрена проблема синтеза общесистемных и географических аспектов и пути ее решения в рамках многоаспектного геоинформационного моделирования.

Ключевые слова: цифровой двойник; пространственный объект; инфраструктура пространственных данных; многоаспектные геоинформационные модели; синтез общесистемных и географических аспектов; комплексные модели; модульное построение сложных систем; цифровой 5D-двойник.

FORMATION OF A SINGLE CYBER ENVIRONMENT OF A POST-INDUSTRIAL SOCIETY ON THE BASIS OF 5D DIGITAL TWINS OF SPATIALLY DISTRIBUTED OBJECTS

Verhova Galina, Akimov Sergei, Proshchenkov Valerii, Iurchik Daniil
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
22 Bol'shevikov Av., St. Petersburg, 193232, Russia
e-mails: galina500@inbox.ru, akimov-sv@yandex.ru, valery@proshchenkov.ru, urdanyrec@yandex.ru

Abstract. The problem of geoinformation support of modern society is considered. The current state and prospects for the development of digital twins of spatial objects are analyzed. The concept of the evolution of 5D digital twins is presented on the example of the VELOCITY 5D product. The problem of synthesis of system-wide and geographical aspects and ways of its solution within the framework of multidimensional geoinformation modeling are considered.

Keywords: digital twin; spatial object; spatial data infrastructure; multidimensional geoinformation models; synthesis of system-wide and geographic aspects; complex models; modular construction of complex systems; 5D digital twin.

Введение. В современных условиях государственным структурам и ведомствам, частным компаниям и отдельным гражданам необходима достоверная и полная информация о географических объектах. Учитывая важность проблемы, ее решение может быть эффективно выполнено только на государственном уровне путем формирования национальной инфраструктуры пространственных данных Российской Федерации, которая должна базироваться на инфраструктурах пространственных данных федерального, регионального и муниципального уровней с учетом общих принципов и стандартов. Национальная инфраструктура пространственных данных должна обладать свойством интероперабельности, гарантирующей возможность ее интеграции в глобальную инфраструктуру пространственных данных на основе использования международных стандартов. Одной из важнейших проблем при формировании национальной инфраструктуры пространственных данных, является наличие унифицированного качественного классификатора географических объектов, который допускает интеграцию в геоинформационные системы и базы данных всех уровней, от муниципального до государственного, и является совместимым с международными геоинформационными сервисами. Инфраструктура пространственных данных должно стать частью единой киберсреды постиндустриального общества, в которой будет выполнен системный синтез как общесистемных, так и географических аспектов в рамках перспективных 5D-цифровых двойников пространственно-распределенных объектов.

Современное состояние инфраструктуры пространственных данных рассмотрим на примере Регионального фонда пространственных данных Санкт-Петербурга [1], который включает в себя сеть референцных станций, градостроительный портал и веб-карту. Государственная спутниковая сеть точного позиционирования Санкт-Петербурга предназначена для обеспечения геодезических работ на территории Санкт-Петербурга и прилегающих районов Ленинградской области. Сеть референцных станций (рис. 1) обеспечивает получение информации спутниковыми навигационными и геодезическими приемниками, которая необходима для определения их координат как в режиме реального времени, так и в режиме постобработки. Данная сеть сертифицирована как средство измерений и на ее основе организовано предоставление корректирующей и измерительной информации для государственных структур, а также платных услуг для коммерческих организаций. В сети референцных станций используется система глобальной спутниковой навигации GNSS (Global Navigation Satellite System). Базовые станции оснащены спутниковыми геодезическими приемниками Leica GR10 и высокоточными антеннами Leica AR25 Choke Ring. Приёмник Leica GR10 поддерживает 120 каналов и способен отслеживать до 60 навигационных спутников, обеспечивая одновременную работу со спутниками GPS, ГЛОНАСС и Galileo. В системе можно создавать до 10 одновременных сеансов записи с частотой до 50 Гц.

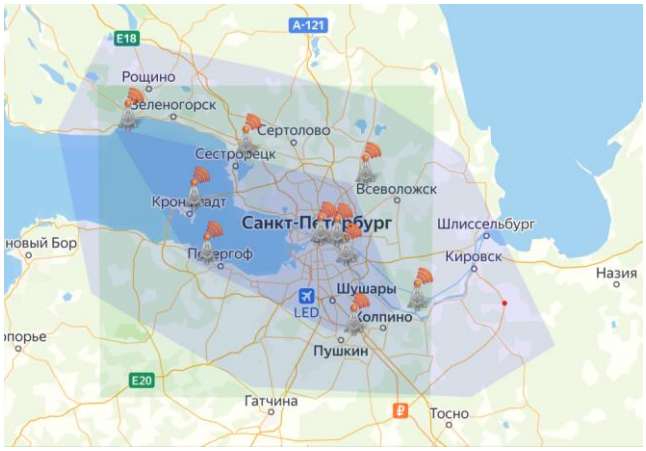


Рис. 1 Сеть референцных станций Санкт-Петербурга

Градостроительный портал Санкт-Петербурга [2] содержит различную геоинфомрацию, включая территориальное планирование, Генеральный план, объекты культурного наследия, пешеходные маршруты, объекты общественно-делового назначения, сведения о застроенных или подлежащих застройке земельных участков и т.п. На рис. 2 приведен пример слоев, отображающих пешеходные маршруты, включая концепцию пешеходного Петербурга, непрерывные маршруты движения пешеходов и проекты пешеходных зон.

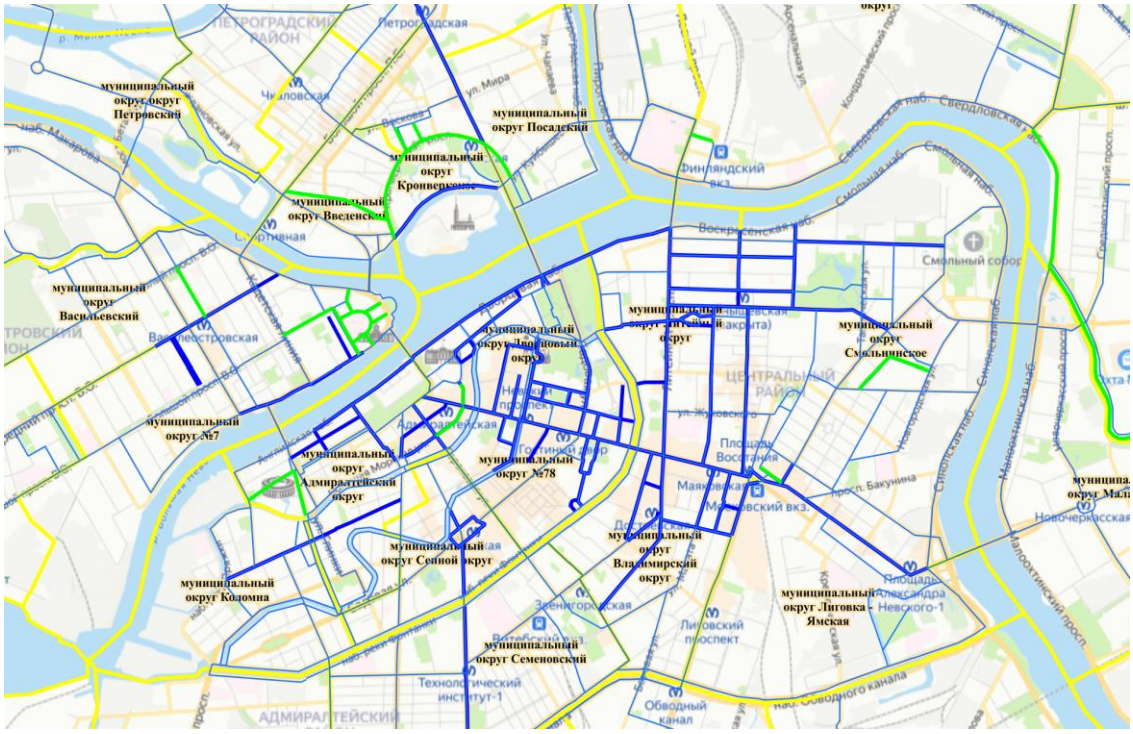


Рис. 2. Пешеходные маршруты на сайте Градостроительного портала Санкт-Петербурга

Региональный фонд пространственных данных Санкт-Петербурга представляет собой высокотехнологическую геоинформационную систему [3-6], обеспечивающую виртуальное представление пространственных объектов, а также точное позиционирование. Данные технологии должны развиваться в направлении повышения степени виртуализации и полноты отражения пространственных объектов Санкт-Петербурга и Ленинградской области, создавая киберсреду, не уступающую, а по некоторым показателям и опережающую лучшие мировые образцы. Создание такой среды возможно лишь на базе цифровых 5D-двойников с применением подходов построения модульных систем [7-8].

Концепцию и технологию цифровых 5D-двойников рассмотрим на примере VELOCITY 5D [9-11]. Канадская компания Presagis анонсировала гибкую и масштабируемую цифровую экосистему VELOCITY 5D, которая автоматически преобразует 2D- и 3D-данные ГИС в реалистичные цифровые двойники с широкими информационными возможностями предоставления о пространственных объектах в реальном масштабе времени. В VELOCITY 5D четвертое измерение подразумевает время, а пятое — контекст (рис. 3). Данная экосистема в первую очередь нацелена на повышение качества поддержки принятия решений.

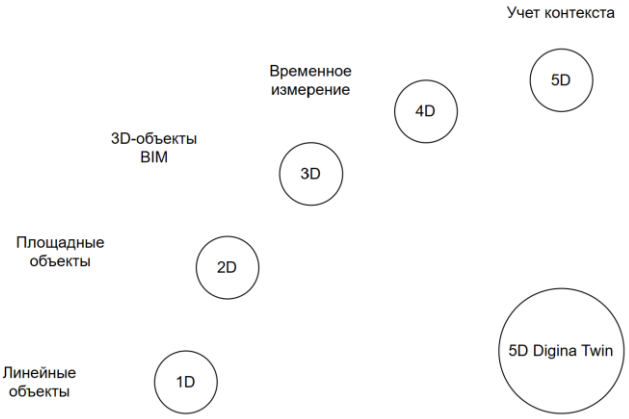


Рис. 3. Развитие размерности геоинформационных моделей

В VELOCITY 5D применяется искусственный интеллект для извлечения информации из цифровых двойников пространственных объектов, с целью выявления моделей взаимодействия людей, поведения толпы, движения транспортных средств и других объектов и отношений между ними. Это позволяет пользователям лучше

интерпретировать комплексную ситуацию в динамически меняющемся мире и моделировать будущие ситуации. Платформа VELOCITY 5D нацелена на реализацию возможности создания общенационального высокоточного цифрового двойника на основе данных ГИС масштаба страны в течение нескольких часов с последующем выполнение сценариев моделирования, визуализации, планирования и картирования.

Заключение. Развитие и массовое внедрение цифровых 5D-двойников требует моделей, позволяющих осуществить синтез общесистемных и географических аспектов, выполняемый с единых методологических позиций, а также технологий, обеспечивающих создание распределенной интероперабельной геоинформационной среды, являющейся частью киберсреды постиндустриального общества [12]. Такие модели могут быть сформированы путем обобщения методологии комплексных и интегративных моделей на случай моделирования пространственно-распределенных природных и техногенных объектов.

Проект реализуется победителем грантового конкурса для преподавателей магистратуры 2021/2022 Стипендиальной программы Владимира Потанина.

СПИСОК ЛИТЕРАТУРЫ

1. Официальный сайт Фонда пространственных данных Ленинградской области [Электронный ресурс]. URL: https://fpd.lenobl.ru/ (дата обращения: 29.06.2023).
2. Градостроительный портал Санкт-Петербурга [Электронный ресурс]. URL: https://portal.kgainfo.spb.ru/KGAMap/ (дата обращения: 29.06.2023).
3. Карпик А. П. Методологические и технологические основы геоинформационного обеспечения территорий :монография. Новосибирск: Сиб. гос. геодез. акад. (СГГА), 2004. 259 с.
4. Акинина Н. В., Курагин А. В., Колесенков А. Н., Костров Б. В. Разработка картографических веб-приложений на основе геоинформационных технологий // Телекоммуникации. 2023. № 2. С. 23-31.
5. Абрамов В. И., Кашироков А. С. Цифровые двойники — эффективные инструменты цифровой трансформации ЖКХ // Цифровая экономика и финансы. Материалы IV Международной научно-практической конференции : сборник. Санкт-Петербург, 2021. С. 139-143.
6. Харламов С. Ю. Цифровой двойник как элемент применения ГИС-технологий в развитии территории // Пространственное развитие территорий. III Международная научно-практическая конференция : сборник научных трудов / под общей ред. Е. А. Стрябковой, А. М. Кулик. Белгород, 2020. С. 189-192.
7. Кходер Х., Верхова Г. В., Акимов С. В. Модульная технология проектирования гибких сложных систем // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 9. С. 86-90.
8. Акимов С. В., Меткин Н. П. Архитектура среды многоаспектного моделирования для автоматизации решения задач исследования, проектирования и управления // Вопросы радиоэлектроники. 2013. Т. 1. № 1. С. 32-40.
9. Официальный сайт VELOCITY 5D [Электронный ресурс]. URL: https://www.velocity5d.com/ (дата обращения: 29.06.2023).
10. Официальный сайт компании Esri [Электронный ресурс]. URL: https://www.esri.com/ (дата обращения: 29.06.2023).
11. Collins M. Quickly creating large-scale digital twins with VELOCITY 5D // Geo Week News. 2023 [Электронный ресурс]. URL: https://www.geoweeknews.com/sponsored/quickly-creating-large-scale-digital-twins-with-velocity-5d (дата обращения: 29.06.2023).
12. Верхова Г. В., Акимов С. В. Многоагентный подход к формированию единой геоинформационной среды // Международная конференция по мягким вычислениям и измерениям. 2021. Т. 1. С. 286-289.

УДК 004.056.55

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ОПЕРАТИВНОГО УПРАВЛЕНИЯ ПРОЦЕССАМИ СТЕГАНОГРАФИИ

Волынкин Павел Александрович, Гибадуллин Альберт Артурович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Мойки р. наб., 61, лит. А, Санкт-Петербург, 191186, Россия
e-mails: pavelas@mail.ru, theelementoffire@mail.ru

Аннотация. В статье рассматривается задача реализации возможности динамического использования битов контейнеров для внедрения контента в зависимости от среднего цветового фона контейнера. Для осуществления исследований было использовано предварительно разработанное программное обеспечение.

Ключевые слова: адаптация; алгоритм управления; стеганография; графические контейнеры; экспертные оценки; цветовой фон контейнера.

RESEARCH OF THE POSSIBILITIES OF OPERATIONAL CONTROL OF STEGANOGRAPHY PROCESSES

Volynkin Pavel, Gibadullin Albert
The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
61 Moika Emb, letter A, St. Petersburg, 191186, Russia
e-mails: pavelas@mail.ru, theelementoffire@mail.ru

Abstract. The article deals with the problem of implementing the possibility of dynamic use of container bits for content injection, depending on the average background color of the container. To carry out the research, previously developed software was used.

Keywords: adaptation; control algorithm; steganography; graphics containers; expert assessments; color background of the container.

Введение. Сокрытие секретной информации в свободно распространяемых изображениях становится актуальной задачей во времена все большего распространения использования средств мобильной связи. При использовании стеганографии с применением графических контейнеров зачастую далеко не полностью используются младшие биты контейнеров для сохранения в них информации секретного контента [1-3].

В связи с этим ставится задача исследовать возможность максимально плотного внедрения скрываемой информации в контейнере с учетом особенностей самого контейнера.

Для решения поставленной задачи было разработано программное обеспечение для устройств мобильной связи (рис.1).

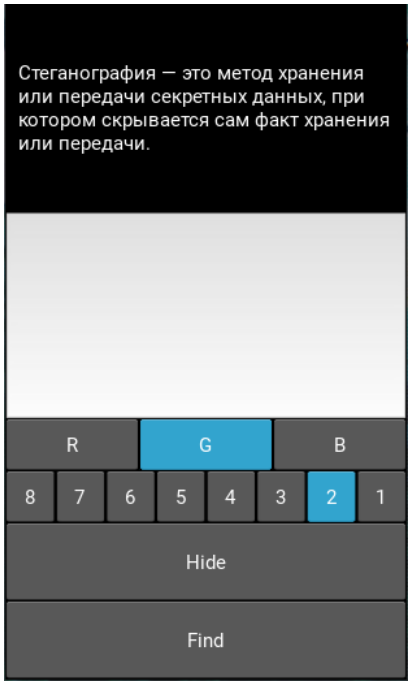


Рис. 1. Интерфейс разработанного мобильного приложения

С использованием разработанного приложения был проведен визуальный анализ изображений при использовании различных разрядов и каналов цветности. Для первой серии экспериментов исходное изображение до сокрытия информации в нем представлено на рис. 2а.

Рис. 2а. Исходное изображение контейнера

Рис. 2б. Сокрытие в младших битах R-канала

Скрываемый контент был загружен в младшие биты красного канала (рис. 2б). Визуально изображение для сокрытия сложно отличить от исходного, что подтверждает известное положение об эффективности использования младших битов контейнера.

Затем было исследовано сокрытие в старших битах каналов разного цвета: синего (рис.3а) и красного (рис. 3б.) каналов цветности.

Рис. 3а. Сокрытие в старших битах B-канала

Рис. 3б. Сокрытие в старших битах G-канала

Как и следовало ожидать, для синего и зеленого каналов сокрытие визуально обнаруживается довольно легко. При кодировании сообщения в старшие биты синего канала цветности после очищения бит нужного разряда для сокрытия информации в дальнейшем, изображение потеряло оттенки синего цвета и стало выглядеть желтым, по причине преобладания красного и зеленого оттенков (рис.3а.). Также явными становятся белые точки в левой части изображения, которые являются битами информации. Таким образом можно сделать вывод, что сокрытие информации в старшие биты изображения не только раскрывает факт манипуляции с изображением, но и выдает информацию, сокрытую в нем.

При кодировании сообщения в старшие биты красного канала цветности после очищения бит нужного разряда изображение потеряло оттенки красного цвета и стало выглядеть синим, по причине преобладания синего и зеленого оттенков (рис.3б.). Данное изображение не только компрометирует факт присутствия манипуляций, как и предыдущее, но и делает это более явно, так как синий цвет неестественен для человеческого глаза в данном случае.

Восприятие цвета играет важную роль в стеганографии графических контейнеров. Некоторые цвета в определенных изображениях могут быть менее заметными для человеческого глаза, что позволяет использовать их для скрытой передачи информации. Понимание особенностей восприятия человеком помогает улучшить стеганографический процесс. Для исследования этого фактора была проведена вторая серия экспериментов. Для наглядности было взята фотография зеленого леса (рис. 4).

Рис. 4. Исходное изображение-контейнер

На данном изображение преобладает зеленый цвет, а именно, средним цветом изображения является в модели цвета RGB #58692B, что составляет 34.5% красного, 41.2% зеленого и 16.9% синего. Для демонстрации изменения изображения размером 350x233 пикселей была проведена поочередная запись текста из 2855 символов в определенный цветовой канал с пошаговым увеличением значимости бит.

Выбор размера изображения и количества символов обусловлен тем, что зашифрованное сообщение занимает примерно половину изображения.

Были проведены записи контента в 5-й и 6-й биты зеленого и синего каналов (рис. 5а).

Рис. 5. Изображение-контейнер с внедренной информацией в зеленый канал (в 5-й бит (слева) и в 6-й бит (справа)

Рис. 5б. Изображение-контейнер с внедренной информацией в синий канал (в 6-й бит (слева) и в 7-й бит (справа)

Для внедрения в 5-й бит зеленого канала наблюдается шум в левой части изображения, так как в ней сокрыты биты информации. Правая часть изображения стала темнее оригинала по причине очистки бит выбранной разрядности. При недлительном или отдаленном наблюдении данные изменения могут остаться незамеченными. При внедрении в 6-й бит на изображении наблюдается явный шум, выдающий наличие скрытой информации в левой части изображения (рис. 5б). Правая часть изображения стала еще темнее, с сильными потерями зеленых оттенков. Данные изменения сильно заметны, даже при невнимательном осмотре. Естественно, что попытка внедрять контент в самые старшие биты (7-й и 8-й) дают еще более неутешительные результаты.

При внедрении контента в синий канал, который в меньшей степени задействован в контейнере, при внедрении в 6-й бит наблюдается легкий шум слева, который можно спутать с туманом, учитывая содержимое изображения. Изменения в правой части изображения остаются практически незаметными. Разницу с оригинальным изображением сложно заметить несмотря на то, что запись была произведена в 6 разряд. При записи в 7-й бит шум слева становится сильным, явно выдавая скрытую информацию. Правая часть изображения визуально выглядит насыщенней. Данное изображение явно выдает наличие в нем скрытых бит информации.

Таким образом, целесообразно проводить внедрение контента в тот канал, который в минимальной степени задействован в модели среднего фона контейнера.

Кроме того, были проведены экспертные оценки эффективности сокрытия контента при различной задействованности битов того или иного канала (рис.6).

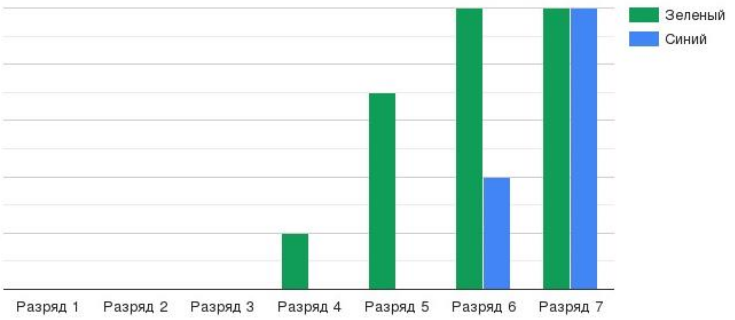


Рис. 6. Зависимость степени «разоблачения» факта сокрытия секретной информации от цвета и номера разряда байта цвета

Выбор правильного цвета для сокрытия информации позволяет увеличить количество разрядов, в которые может быть сокрыта информация. В случае с выбором минимально значимого цвета с небольшим количеством информации можно использовать большее количество разрядов, так как неиспользуемое пространство визуально будет казаться более насыщенным.

Заключение. В результате проведенных исследований делается вывод о возможности автоматической оценки среднего цветового фона изображения-контейнера и в зависимости от этой оценки автоматического выбора оптимального сочетания рабочих бит для каждого из RGB-каналов. Такое сочетание каналов и битов фактически станет ключом для извлечения скрытой информации у адресата. Такой подход позволит максимально уплотнить процесс упаковки контента в контейнерах.

СПИСОК ЛИТЕРАТУРЫ

1. Волынкин П. А., Севостьянова А. С. Исследование принципов шифрования мультимедиа информации в графических файлах // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. 2018. С. 203-206.
2. Волынкин П. А., Кононюк О. А. Исследование стеганографического метода LSB с использованием ключей для определения области встраивания данных в графических контейнерах. // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). Сборник научных статей IX Международной научно-технической и научно-методической конференции. СПб., 2020. С. 186-190.
3. Волынкин П. А., Кононюк О. А. Исследование стеганографического метода LSB с адаптивным поиском областей встраивания данных в растровых графических контейнерах. // Актуальные проблемы инфотелекоммуникаций в науке и образовании. СПб., 2021. С. 159-163.

УДК 004.934

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ КОМПЛЕКСНОЙ МЕТОДИКИ| ОЦЕНКИ КАЧЕСТВА АЛГОРИТМОВ КРИПТОГРАФИИ

Волынкин Павел Александрович, Кузнецов Вадим Всеволодович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Мойки реки наб, 61, лит. А, Санкт-Петербург, 191186, Россия
e-mails: pavelas@mail.ru, vadim.kuznetsov.2001@gmail.com

Аннотация. В статье рассматривается задача реализации возможности и результаты исследований комплексной оценки алгоритмов криптографии на основе энтропии, битовых карт и дисперсии. Для осуществления исследований было использовано предварительно разработанное программное обеспечение.

Ключевые слова: криптография; методы оценки алгоритмов; программное обеспечение; энтропия; битовые карты; дисперсия.

STUDY OF THE EFFICIENCY OF USING A COMPLEX METHOD FOR ASSESSING THE QUALITY OF CRYPTOGRAPHY ALGORITHMS

Volynkin Pavel, Kuznetsov Vadim
The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
61 Moyka r. Emb, letter A, St. Petersburg, 191186, Russia
e-mails: pavelas@mail.ru, vadim.kuznetsov.2001@gmail.com

Abstract. The article deals with the problem of realizing the possibility and the results of research on the complex evaluation of cryptography algorithms based on entropy, bitmaps and variance. To carry out the research, previously developed software was used.

Keywords: cryptography; methods for evaluating algorithms; software; entropy; bitmaps; dispersion.

Введение. Криптографические алгоритмы, каждый из которых имеет свои уникальные характеристики и стойкость, требуют эффективной оценки качества шифрования с точки зрения стойкости к атакам и возможности обнаружения. На основе разработанной ранее методики, алгоритмов и программного обеспечения были проведены исследования по анализу криптографических алгоритмов с целью определения их качества и стойкости.

Для проведения анализа были выбраны несколько популярных криптографических алгоритмов, включая шифры Цезаря, Вижинера, Хилла, Плейфера и AES. Были собраны зашифрованные данные с использованием каждого алгоритма и произведен расчет байтовой энтропии, дисперсии n-грамм и произведен анализ битовых карт для каждого набора данных. Пользователю представлена возможность анализа результатов работы алгоритмов шифрования, выбрать алгоритм шифрования и ввести ключ, для кодировки исходного текста из файла. Если нужный пользователю алгоритм шифрования в программе отсутствует — у него будет возможность закодировать сообщение самому для его дальнейшего анализа. После нажатия на кнопку расчета на экран выводятся рост энтропии и дисперсия n-грамм исходного и зашифрованного сообщения, а также битовая карта обоих сообщений (рис.1).

Рис. 1. Интерфейс разработанного приложения

Высокий рост энтропии свидетельствует о высокой стойкости выбранного алгоритма шифрования. Нулевая дисперсия n-грамм свидетельствует о том, что в тексте все n-граммы встречаются не более 1 раза, что демонстрирует высокую стойкость алгоритма шифрования.

Таким образом, чем лучше выбранный алгоритм шифрования, тем больше рост энтропии закодированного текста, и тем ближе к нулю дисперсия его n-грамм. Битовая карта, в свою очередь, поможет визуально оценить приближение зашифрованного сообщения к «белому шуму», что сильно затруднит процесс его декодирования.

Байтовая энтропия рассчитывается на основе формулы Шеннона-Виенера, используя вероятность p для каждого значения байта [1-3]. Приложение также предоставляет возможность визуализации исходного и зашифрованного текстов, в виде битовой карты. Текст представляется в виде изображения, где каждый пиксель представляет собой 0 или 1, соответствующие битам текста [4].

Сравнительные результаты для различных методов шифрования представлены на рис. 2.

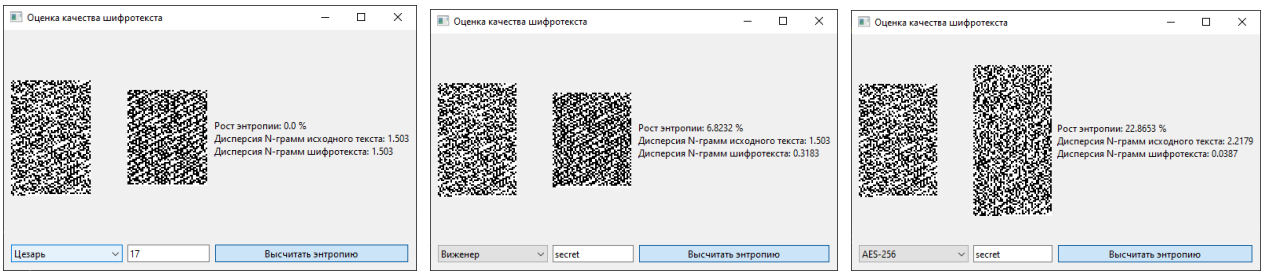


Рис. 2. Результаты оценки качества методов криптографии: Цезаря, Вижинера и AES-256

При шифровании методом Цезаря энтропия и дисперсия исходного и зашифрованного сообщения оказались одинаковыми, так как в этом случае применяется простое правило сдвига символов в сообщении на фиксированное количество позиций. Иными словами, каждый символ в исходном сообщении будет иметь однозначное соответствие с символом в зашифрованном сообщении. Поэтому частота появления символов в обоих сообщениях остается примерно одинаковой, что приводит к одинаковым значениям энтропии и дисперсии. Из-за этих особенностей алгоритм Цезаря является достаточно уязвимым для атак перебором и анализом статистики символов. В случае же шифрования методом Вижинера наблюдается рост показателя энтропии, и снижение дисперсии n-грамм шифротекста (примерно в 5 раз). Наилучшие результаты в приведенных примерах показало шифрование методом AES-256. При данном алгоритме наблюдается сильное улучшение показателей роста энтропии и дисперсии (почти на 2 порядка). Результаты оценки роста энтропии сведены на рис.3, а дисперсии — на рис. 4.

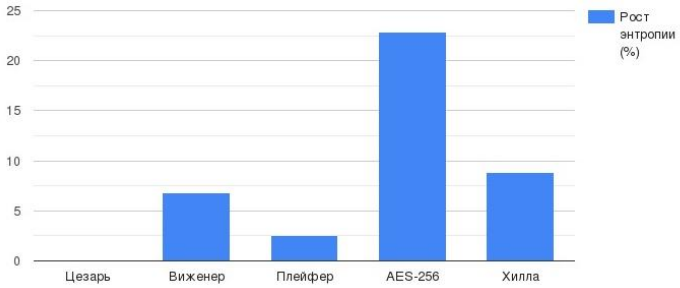


Рис. 3. Результаты оценки роста энтропии для методов Цезаря, Вижинера, Плейфера, AES-256 и Хилла

Показатель роста энтропии был получен путем вычитания относительной энтропии исходного текста из энтропии зашифрованного. Относительная энтропия, в свою очередь, была получена путем деления энтропии полученного шифротекста на значение максимальной возможной энтропии при текущей размерности алфавита. Таким образом, рост энтропии шифротекста свидетельствует о стойкости алгоритма, с помощью которого он был получен. Наибольший показатель роста энтропии, среди выбранных алгоритмов, можно наблюдать у алгоритма AES-256.

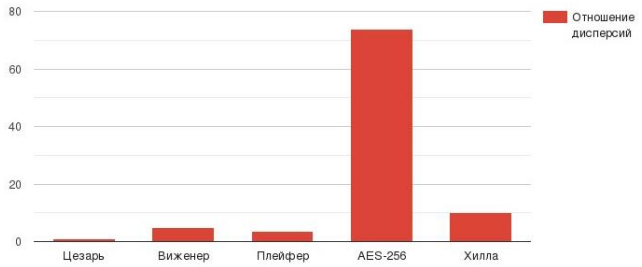


Рис. 3. Результаты оценки дисперсии для методов Цезаря, Вижинера, Плейфера, AES-256 и Хилла

Также было исследовано отношение дисперсий n-грамм исходного и зашифрованного текстов. Данное отношение было получено путем деления дисперсии исходного текста на дисперсию зашифрованного. При условии того, что при выборе лучшего алгоритма дисперсия n-грамм полученного с его помощью шифротекста стремится к нулю, можно сделать вывод, что большее значение полученного отношения свидетельствует о более высокой стойкости алгоритма. И в этом случае алгоритм AES-256 показал наилучший результат.

Заключение. В данной работе был предложен метод анализа криптографических алгоритмов с использованием байтовой энтропии и дисперсии n-грамм. Результаты экспериментального исследования подтвердили, что эти показатели могут служить хорошими метриками для определения стойкости алгоритмов. Дальнейшие исследования могут быть направлены на разработку более точных моделей и методов анализа, а также внедрение данной методики для оценки новых криптографических алгоритмов.

СПИСОК ЛИТЕРАТУРЫ

1. Зарипов Р. Г. Новые меры и методы в теории информации. Казань : КГТУ, 2005. 364 с.
2. Кац Дж., Линделл Ю. Введение в современную криптографию. CRC Press, 2014. 598 с.
3. Лавасани А., Эглидос Т. Практический тест следующего бита для оценки псевдослучайной последовательности // Scientia Iranica : научный журнал. 2009. Т. 16. Вып. 1.
4. Сен Н. Д., Котляров В. П., Григорьев Я. Ю. Применение оценок на основе энтропии для сравнения криптостойкости алгоритмов шифрования // Современные наукоемкие технологии : научный журнал. 2013. № 2. С. 105-106.

УДК 004.056.53

ИССЛЕДОВАНИЕ МЕТОДА ОБНАРУЖЕНИЯ АТАК НА TDLS: АНАЛИЗ УЯЗВИМОСТЕЙ И ПРЕДЛАГАЕМЫЕ РЕШЕНИЯ

Дрепа Владислав Евгеньевич, Ковцур Максим Михайлович,
Сахаров Дмитрий Владимирович, Шарапов Роман Игоревич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп.1, лит. А, Ж, Санкт-Петербург, 193232, Россия
e-mails: vladikdrepa@mail.ru, maxkovzur@mail.ru, sguard7@mail.ru, sharapov.roman@list.ru

Аннотация. С увеличением использования технологий беспроводной передачи данных, в особенности Wi-Fi, важность обеспечения безопасности передаваемых данных становится все более значимой. В частности, в корпоративных сетях, где конфиденциальность информации является приоритетом, необходимо обнаруживать и предотвращать возможные сетевые атаки. Данная статья представляет исследование методов обнаружения атак на TDLS (Tunneled Direct Link Setup) в беспроводных сетях. Рассматривается чипсет Broadcom — одного из крупнейших поставщиков чипсетов для беспроводных устройств. В силу широкого распространения данных чипсетов, они могут стать привлекательной целью для злоумышленников. Цель данной работы — исследовать уязвимости, связанные с чипсетами Broadcom, и разработать предлагаемые решения для обнаружения и предотвращения атак на TDLS. В статье представлен анализ существующих уязвимостей и предложены методы обнаружения атак на TDLS. Результаты исследования представляют практическую ценность для специалистов по информационной безопасности и сетевых администраторов, предоставляя дополнительные инструменты и рекомендации для защиты вверенных им сетей от потенциальных атак.

Ключевые слова: аппаратные уязвимости WLAN чипсетов; исследование чипсетов; Wi-Fi exploit; Broadcom; прошивка; reverse-engineering; TDLS.

THE RESEARCH OF TDLS ATTACKS DETECTION METHOD: VULNERABILITY ANALYSIS AND PROPOSED SOLUTIONS

Drepa Vladislav, Kovtsur Maxim, Sakharov Dmitry, Sharapov Roman
The Bonch-Bruevich St Petersburg State University of Telecommunications
22 Bolshevikov Av, bld. 1, St Petersburg, 193232, Russia
e-mails: vladikdrepa@mail.ru, maxkovzur@mail.ru, sguard7@mail.ru, sharapov.roman@list.ru

Abstract. With the increasing use of wireless data transmission technologies, especially Wi-Fi, the importance of ensuring the transmitting data security of is becoming increasingly important. Particularly in corporate networks, where information privacy is a priority, it is necessary to detect and prevent possible network attacks. This article presents a reasearch of TDLS (Tunneled Direct Link Setup) attack detection methods in wireless networks. It looks at the Broadcom chipset, one of the largest vendors of wireless devices chipsets. Because of the widespread availability of these chipsets, it can be an attractive target for attackers. The purpose of this article is to investigate vulnerabilities associated with Broadcom chipsets and develop proposed solutions to detect and prevent TDLS attacks. The article presents an analysis of existing vulnerabilities and proposes detecting TDLS attack methods. The results are of practical value to IT security specialists and network administrators, providing additional tools and guidance for protecting their networks from potential attacks.

Keywords: WLAN chipset hardware vulnerabilities; chipset research; Wi-Fi exploit; Broadcom; firmware; reverse-engineering; TDLS.

Введение. Аппаратные уязвимости WLAN чипсетов представляют серьёзную опасность для широкого спектра устройств, использующих беспроводные сети. Данные с сайта cve.mitre.org указывают на обнаружение около 30 аппаратных уязвимостей в различных чипсетах только за первую половину 2023 года. Эти уязвимости могут быть использованы злоумышленниками для несанкционированного доступа, манипуляции устройствами или кражи конфиденциальных данных.

Для выявления аппаратных уязвимостей проводится анализ кода, который хранится в постоянном запоминающем устройстве (ПЗУ) и оперативном запоминающем устройстве (ОЗУ) WLAN чипсета. Для этой цели используются утилиты nexmon, специально разработанные для анализа и модификации чипсетов Broadcom. С помощью данных утилит можно получить доступ к содержимому ПЗУ и ОЗУ, что позволяет детально проанализировать код и выявить потенциальные уязвимости. Анализ аппаратных уязвимостей является критически важной задачей для обеспечения безопасности систем, работающих на WLAN чипсетах. Он позволяет идентифицировать уязвимые места в чипсетах и разработать соответствующие меры по устранению уязвимостей. Это включает обновление и патчинг уязвимых частей кода, внедрение дополнительных механизмов защиты и улучшение общей безопасности устройств.

Систематический анализ аппаратных уязвимостей является неотъемлемой частью работы производителей чипсетов, разработчиков драйверов и обеспечения безопасности. Это помогает предотвращать потенциальные атаки и обеспечивать защиту конфиденциальных данных, особенно в корпоративных сетях, где защита информации имеет высокий приоритет [1-3]. Изучив данные из ПЗУ и ОЗУ Wi-Fi чипсета было выявлено, что исследуемый телефон поддерживает функцию TDLS (рис. 1).

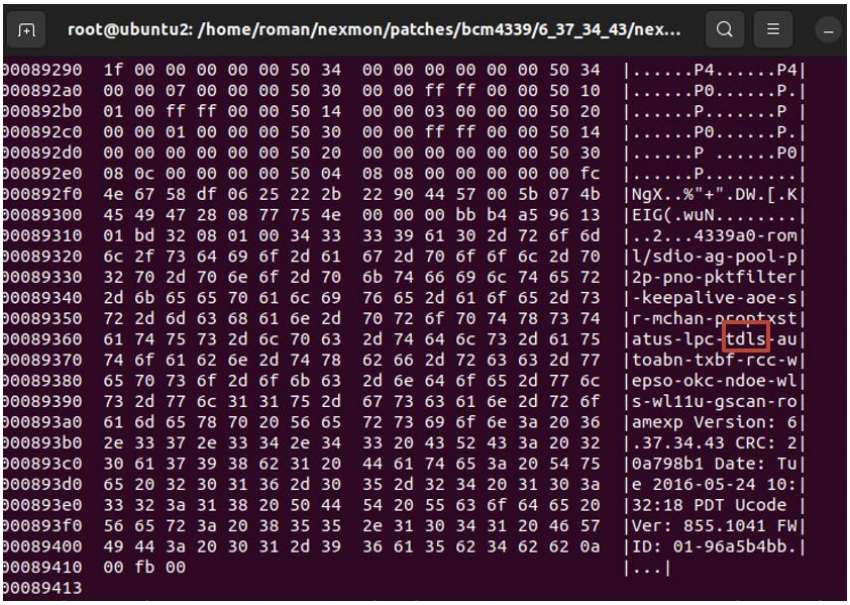


Рис.1. Наличие функции TDLS

В ходе исследования протокола TDLS в стандарте IEEE 802.11 была обнаружена уязвимость, связанная с функцией, ответственной за анализ сообщений точки доступа в процессе «рукопожатия» [4]. При обмене сообщениями точка доступа не проверяет длину поля, следующего за полем RSN (Robust Security Network). Это открывает возможность злоумышленнику удалённо изменить значение поля WPA Key Data Length на значение, превышающее допустимую длину в 63 байта. Изменение значения поля WPA Key Data Length в третьем сообщении четырёхэтапного рукопожатия свыше допустимой длины приводит к переполнению буфера данных в точке доступа, что может привести к отказу в обслуживании Wi-Fi. Эксплуатация данной уязвимости позволяет злоумышленнику привести к недоступности беспроводной сети, что создаёт серьёзные проблемы для пользователей, зависящих от надёжного соединения [5]. Такая атака может быть осуществлена удалённо, без физического доступа к точке доступа [6].

На рис. 2 можно увидеть, что для выполнения атаки необходимо изменить поля WPA Key Data Length, WPA Key Data и размер всего пакета. После изменения полей необходимо отправить пакет в трафик, и атака будет считаться совершённой. Принцип данной атаки представлен на рис. 3.

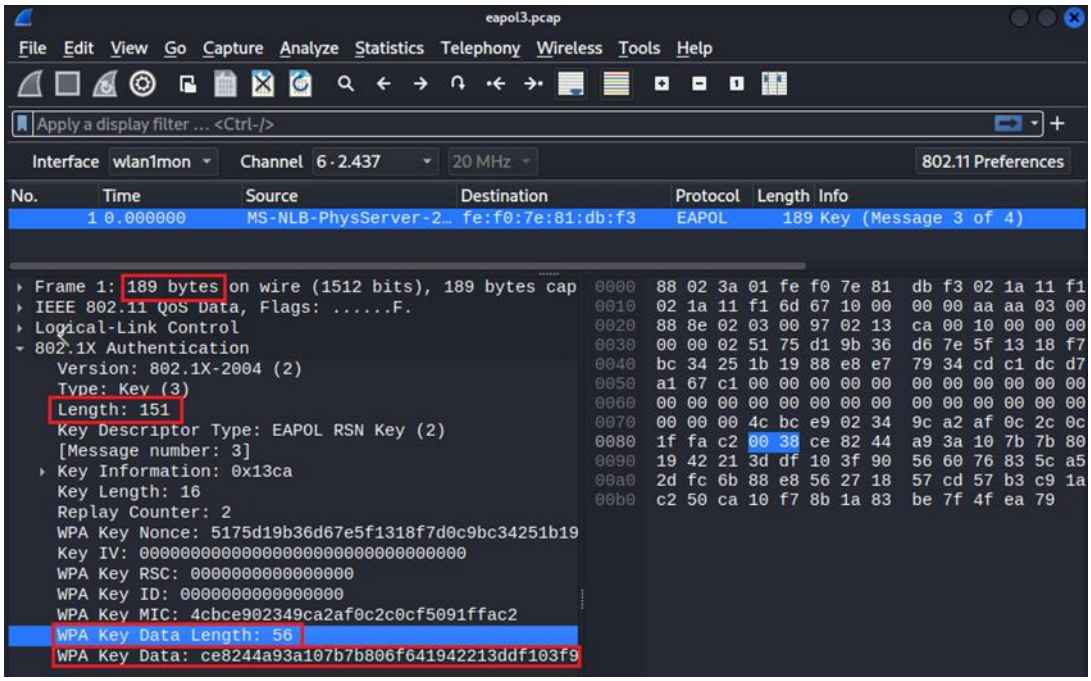


Рис. 2. Демонстрация полей, подвергающимся изменению

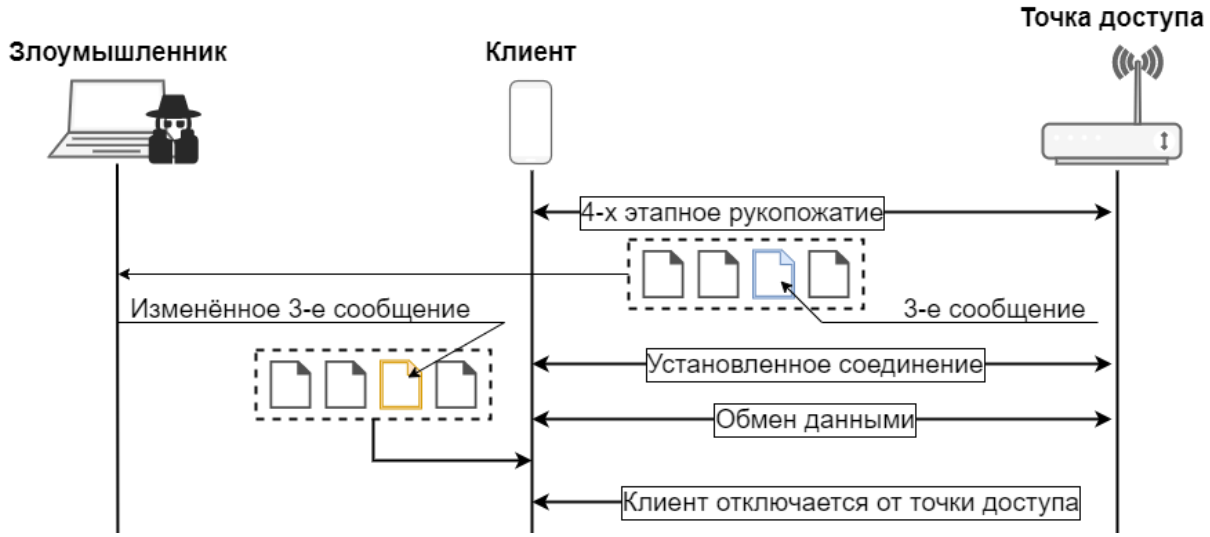


Рис. 3. Принцип атаки на TDLS

Для обнаружения атаки, связанной с изменением поля WPA Key Data Length, можно использовать фильтр в сетевом анализаторе Wireshark. Фильтр «(wlan_rsna_eapol.keydes.msgnr == 3) && (wlan_rsna_eapol.keydes.data_len > 63)»

позволяет выявить подозрительные пакеты, которые могут указывать на проведение такой атаки. Ниже поэтапно для более подробного разъяснения представлены составляющие указанного фильтра:

1) «wlan_rsna_eapol.keydes.msgnr == 3» — данная часть фильтра выделяет поле «msgnr» (номер сообщения) в кадре EAPoL (Extensible Authentication Protocol over LAN). Значение «3» указывает на третье сообщение рукопожатия WPA (четырёхэтапный процесс аутентификации в защищённой беспроводной сети);

2) «&&» — логическое «И»;

3) «wlan_rsna_eapol.keydes.data_len > 63» — в этой части фильтра проверяется поле «data_len» (длина данных) в поле «keydes» (ключевая информация) кадра EAPoL. Условие «data_len > 63» означает, что нас интересуют пакеты, где значение длины данных превышает 63 байта.

При использовании сетевого анализатора Wireshark с применением данного фильтра, можно отслеживать и анализировать пакеты, соответствующие данному критерию, что позволяет обнаружить атаки на поле WPA Key Data Length и принять соответствующие меры для защиты беспроводной сети [7].

Заключение. Исследование методов обнаружения атак на TDLS и анализ уязвимостей является важным шагом в повышении безопасности беспроводных сетей. Это способствует защите конфиденциальности и целостности данных, а также обеспечению бесперебойного функционирования сетевой инфраструктуры. Дальнейшие исследования и разработки в этой области будут способствовать созданию более надёжных и безопасных беспроводных сетей для использования в различных сферах, включая корпоративные и домашние сети. В статье рассмотрены подходы к анализу WLAN чипсетов для выявления аппаратных уязвимостей, а также продемонстрирована атака на протокол TDLS и метод обнаружения данной атаки на беспроводное устройство.

СПИСОК ЛИТЕРАТУРЫ

1. Reverse-engineering Broadcom wireless chipset // Quarkslab's blog URL: https://blog.quarkslab.com/reverse-engineering-broadcom-wireless-chipsets.html (дата обращения: 02.02.2023).
2. Over The Air Vol. 2, Pt. 1: Exploiting The Wi-Fi Stack on Apple Devices // Project Zero [Электронный ресурс]. URL: https://googleprojectzero.blogspot.com/2017/09/over-air-vol-2-pt-1-exploiting-wi-fi.html (дата обращения: 05.02.2023).
3. Сахаров Д. В., Красов А. В., Ушаков И. А., Бирих Э. В. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе IPV6 // Защита информации. Инсайд, 2020. № 1 (91). С. 51-57.
4. Киструга А. Ю., Ковцур М. М., Петров М. П., Шабанов В. П. Методика обнаружения местоположения нарушителя, реализующего атаку деаутентификации на сеть IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция. Т. 1 : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2022. С. 561-564.
5. Лаврова Д. С., Попова Е. А., Штыркина А. А., Штеренберг С. И. Предупреждение DoS-атак путем прогнозирования значений корреляционных параметров сетевого трафика // Проблемы информационной безопасности. Компьютерные системы, 2018. № 3. С. 70-77. EDN VOHMBC.
6. Ковцур М. М., Герлинг Е. Ю., Коновалова В. В., Киструга А. Ю. Исследование способов удаленного перехвата трафика в корпоративных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки, 2021. № 4. С. 68-75. DOI 10.46418/2079-8199_2021_4_10. EDN SWFHMM.
7. Федорова А. Э., Герлинг Е. Ю., Ахрамеева К. А., Андрианов В. И. Разработка веб-интерфейса для системы мониторинга беспроводных сетей семейства IEEE 802.11 // Региональная информатика и информационная безопасность : Сборник трудов XII Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 27–29 ноября 2021 года. Выпуск 10. Санкт-Петербург: Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2021. С. 381-385. EDN DXLBVX.

УДК 004.056

ВНЕДРЕНИЕ ЦИФРОВОГО ВОДЯНОГО ЗНАКА В МОДУЛЬ ЯДРА ОПЕРАЦИОННОЙ СИСТЕМЫ LINUX И УСТОЙЧИВОСТЬ К КОМПОНОВКЕ

Коньков Владимир Владимирович, Кузнецов Владимир Александрович, Красов Андрей Владимирович

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиковпр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: no0bot2001@mail.ru, kuznetsov_v2001@mail.ru, krasov@inbox.ru

Аннотация. В данной статье рассматривается проблема внедрения цифрового водяного знака (ЦВЗ) в модуль ядра операционной системы Linux и его устойчивость при процессе компоновки. Цифровой водяной знак является эффективным методом защиты интеллектуальной собственности и подтверждения подлинности кода. Основной фокус исследования состоит в определении влияния оптимизаций компоновки на сохранение ЦВЗ.

Ключевые слова: ЦВЗ; компоновка; ОС Linux; внедрение; вложение; эффективность.

DIGITAL WATERMARK INJECTION INTO LINUX OPERATING SYSTEM KERNEL MODULE AND LINK RESISTANCE

Konkov Vladimir, Kuznetsov Vladimir, Krasov Andrey

St. Petersburg State University of Telecommunications named after Professor M. A. Bonch-Bruevich
22 Bolshevikov Av, building 1, St. Petersburg, 193232, Russia
e-mails: no0bot2001@mail.ru, kuznetsov_v2001@mail.ru, krasov@inbox.ru

Abstract. This article explores the integration of a digital watermark into a Linux kernel module and its resilience during the compilation process. Digital watermarking serves as an effective method for protecting intellectual property and verifying code authenticity. The primary focus of this research is to examine the impact of compilation optimizations on watermark preservation.

Keywords: CVZ; layout; Linux OS; implementation; investment; efficiency.

Введение. В современном цифровом мире вопросы обеспечения авторских прав и защиты интеллектуальной собственности стали еще более острыми, особенно в области программного обеспечения. Методы внедрения цифровых водяных знаков в код программ, которые могут помочь идентифицировать автора и гарантировать целостность кода, активно разрабатываются и становятся все более важными инструментами защиты. Особый интерес представляет внедрение цифрового водяного знака в модуль ядра — основной компонент любой операционной системы. Этот подход позволяет обеспечить высокую устойчивость и защиту от несанкционированных изменений [1, 2]. Но появляется новый вызов — устойчивость водяного знака при компиляции и компоновке модулей с использованием различных оптимизаций. Оптимизация кода — это распространенная практика, направленная на увеличение эффективности исполнения программ, однако она может значительно изменить структуру исходного кода, что, в свою очередь, может повлиять на сохранность водяного знака. В данной статье обсуждается метод внедрения цифрового водяного знака в модуль ядра и рассмотрим его устойчивость при компоновке с оптимизацией и без нее.

Основная часть. Executable and Linkable Format (ELF) — это универсальный формат файлов для хранения исполняемых файлов, объектных файлов, общих библиотек и дампов памяти, разработанный и внедренный в рамках проекта Unix System V. Он широко используется в большинстве современных операционных систем на базе Unix, включая Linux, BSD и Solaris [3]. ELF файлы играют ключевую роль в процессе создания исполняемых программ и модулей ядра, они содержат в себе всю необходимую информацию, которая используется компоновщиком и загрузчиком программы, включая секции с исходным кодом, данные и информацию о ресурсах.

Бинарные файлы, в свою очередь, являются формой хранения данных, который можно прочитать, исполнить или обработать программным обеспечением. В контексте операционных систем, бинарные файлы часто указывают на исполняемые файлы — программы, которые компьютер может выполнять. Исполняемые бинарные файлы могут содержать в себе как исходный код, так и ресурсы программы, включая изображения, текст и другие данные.

В контексте нашей работы с модулями ядра и водяными знаками нам также приходится работать с различными компонентами, включая секции кода и данных ELF файлов, хеш-функции для создания водяного знака, алгоритмы внедрения знака в исходный код, и инструменты для анализа и оптимизации кода. Все эти компоненты вместе образуют сложную систему, которую мы используем для защиты авторских прав на программное обеспечение и обеспечения его целостности.

Данный способ основан на особенностях кодировки инструкций x86 архитектуры. В частности, была рассмотрена структура Opcode и ModRM байтов. ModRM-байт определяет используемый режим адресации, операнд регистр и операнд регистр/память [4]. Opcode-байт определяет тип исполняемой инструкции и содержит 2 дополнительных бита — бит направления и бит размерности операндов. В ходе исследования была выявлена дуальность кодировки некоторых инструкций. Было установлено, что для инструкций с 2 операндами, где оба из них — регистры, изменение порядка следования операндов в ModRM-байте и соответствующее изменение бита направления операции в Opcode-байте не изменяет результат дизассемблирования инструкции. Предложенный метод цифровой подписи исполняемых файлов использует данную особенность, где контейнером для цифрового водяного знака являются биты направления в Opcode-байте.

Алгоритм подписи, следующий:

1. Анализ структуры формата исполняемого файла (ELF) и последующее извлечение адреса и размера текстового сегмента файла;
2. Дизассемблирование инструкций текстового сегмента (для декодирования инструкций x86-64 архитектуры использовалась библиотека Zydis);
3. Анализ инструкций на возможность использования в качестве контейнера для цифрового водяного знака;
4. Составление выборки подходящих для цели инструкций;
5. Последовательное сравнение битов цифрового водяного знака с битами направления инструкций из составленной выборки;
6. В случае соответствия вышеуказанных битов, инструкция пропускается. В противном случае, инструкция модифицируется согласно вышеуказанной методике;
7. В случае, когда количество битов контейнера превышает количество битов цифрового водяного знака, биты цифрового водяного знака дублируются, заполняя собой все пространство контейнера.

Был создан основной бинарный файл, написанный на языке C. Предназначен для внедрения и проверки ЦВЗ в исполняемый файл.

Адрес и размер текстовой секции нужен для того, чтобы знать какие биты нужно анализировать. Адрес и размер сегмента данных нужен для того, чтобы относительно них посчитать SHA256-хэш и в последствии составить из него водяной знак [4]. На рис. 1 представлен вывод команды test, программа выводит хэш код нашей надписи, которая была прописана в программе, хэш код сегмента данных, права доступа которого предназначены для чтения и записи, а также хэш код нашего цифрового водяного знака.

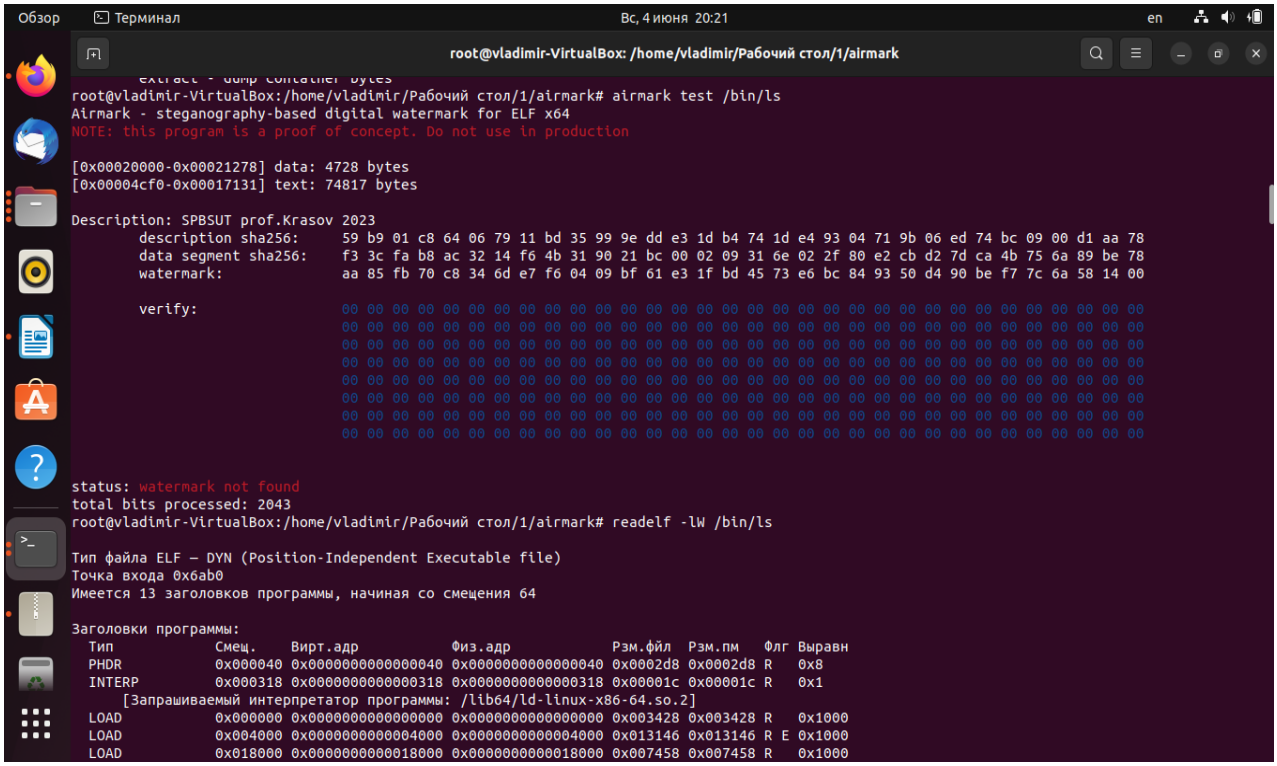


Рис. 1. Команда test

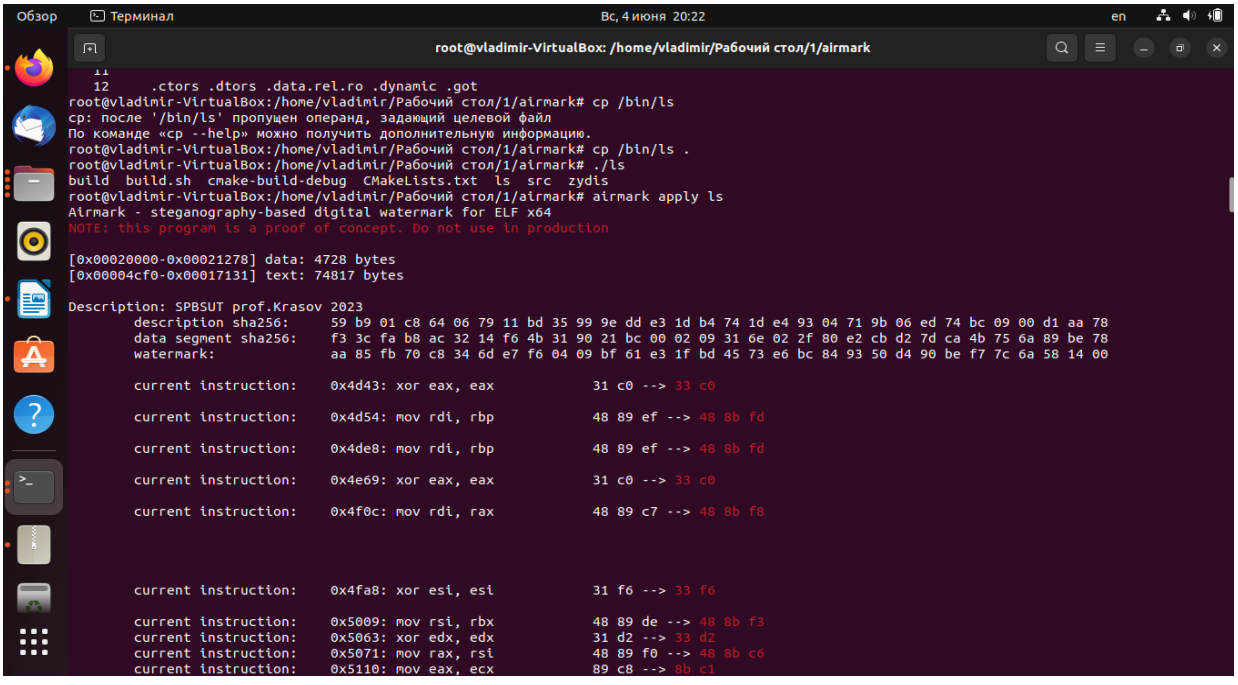


Рис. 3. Замена битов

Далее выбираем ранее считанный адрес и размер текстовой секции, набор байтов, который представляет собой инструкции и дизассемблируем их с помощью библиотеки Zydis. Данная библиотека позволяет нам работать не с сырым набором байтов, а с каждой инструкцией по отдельности. Значит, если у нас в файле есть байты 31 c0,

то это не сырые байты, а наша библиотека говорит на прямую, что эти байты обозначают инструкцию xor eax,eax и уже можно доставать конкретно нужные нам инструкции.

Так проходясь по всем инструкциям из текстовой секции мы достаем из них то, что нам нужно — это байт опкода и ModRM байт. Проверяем, что если изменить эту инструкцию по принципу замены бита направление изменения порядков операндов, то останется та же самая инструкция.

Дальше необходимо пройтись по всем отдельным битам водяного знака и выставить такие же значения битов направления в самих инструкциях и так зацикливаем водяной знак до конца текстовой секции [1]

Когда был выполнен проход по всем инструкциям и произошла замена всех битов в соответствии с водяным знаком, программа завершает работу. Рис. 3 показывает, как программа выводит на экран замену битов в инструкциях.

Вводим airmark test /bin/ls программа высчитывает все хэши находит адреса нужных секций и сегментов, только вместо того, что мы будем менять биты мы считываем биты направления в одну цепочку и делаем поиск цифрового водяного знака по ней. ЦВЗ найдено как показано на рис. 4.

```
total bits processed: 2043
root@vladimir-VirtualBox:/home/vladimir/Рабочий стол/1/airmark# airmark test /bin/ls
Airmark - steganography-based digital watermark for ELF x64
NOTE: this program is a proof of concept. Do not use in production

[0x00020000-0x00021278] data: 4728 bytes
[0x00004cf0-0x00017131] text: 74817 bytes

Description: SPBSUT prof.Krasov 2023
        description sha256:     59 b9 01 c8 64 06 79 11 bd 35 99 9e dd e3 1d b4 74 1d e4 93 04 71 9b 06 ed 74 bc 09 00 d1 aa 78
        data segment sha256:    f3 3c fa b8 ac 32 14 f6 4b 31 90 21 bc 00 02 09 31 6e 02 2f 80 e2 cb d2 7d ca 4b 75 6a 89 be 78
        watermark:              aa 85 fb 70 c8 34 6d e7 f6 04 09 bf 61 e3 1f bd 45 73 e6 bc 84 93 50 d4 90 be f7 7c 6a 58 14 00

        verify:                 aa 85 fb 70 c8 34 6d e7 f6 04 09 bf 61 e3 1f bd 45 73 e6 bc 84 93 50 d4 90 be f7 7c 6a 58 14 00


status: watermark found
total bits processed: 2043
root@vladimir-VirtualBox:/home/vladimir/Рабочий стол/1/airmark#
```

Рис. 4. Вывод команды test

Во время компоновки исполняемого файла, компилятор может использовать различные стратегии оптимизации, чтобы улучшить производительность или уменьшить размер результирующего исполняемого файла. Два наиболее общих вида оптимизации — это оптимизация по времени и оптимизация по размеру [3].

Оптимизация по времени фокусируется на увеличении скорости исполнения программы, что может включать в себя предварительное вычисление выражений, удаление неиспользуемого кода и разворачивание циклов. В контексте компиляции с оптимизацией по времени на GCC, мы можем использовать флаг -O3, который активирует все оптимизации, направленные на ускорение выполнения кода.

Оптимизация по размеру, с другой стороны, старается минимизировать размер исполняемого файла. Это может включать в себя упаковку данных, удаление неиспользуемого кода и сокращение размера инструкций. В контексте компиляции с оптимизацией по размеру на GCC, мы можем использовать флаг -Os, который активирует все оптимизации, направленные на минимизацию размера результирующего исполняемого файла [2].

В статье была выполнена компановка модуля ядра операционной системы Linux с оптимизацией как по скорости, так и по размеру. Применение оптимизации по скорости позволило улучшить производительность модуля, сократив время выполнения операций. Оптимизация по размеру, в свою очередь, позволила уменьшить размер модуля, что может быть важно в случае ограниченных ресурсов.

После проведенных оптимизаций, цифровой водяной знак (ЦВЗ) сохраняется на определенный процент. Результаты экспериментов показали, что при оптимизации по скорости ЦВЗ сохраняется на 70 % от исходного значения. В то же время, при оптимизации по размеру, ЦВЗ сохраняется на 80% от исходного значения. Так же без оптимизации ЦВЗ сохраняется на 100 %.

Заключение. Применение оптимизации при компоновке модуля ядра позволяет достичь баланса между производительностью и размером модуля, сохраняя цифровой водяной знак в соответствующей степени. Эти результаты подчеркивают важность выбора оптимальной стратегии компоновки в контексте внедрения цифрового водяного знака в модуль ядра операционной системы Linux.

СПИСОК ЛИТЕРАТУРЫ

1. Цифровые водяные знаки / В. И. Коржик [и др.]. // Цифровая стеганография и цифровые водяные знаки : в 2 ч. СПб : СПбГУТ, 2017. Ч. 2. С. 5-6.
2. Штеренберг С. И., Красов А. В. Разработка методики построения доверенной среды на основе скрытого программного агента. Ч. 3. Принцип действия программного агента и проверка его работоспособности // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 4. С. 34-40.
3. Красов А. В. Исследование применимости известных методов внедрения цифровых водяных знаков к исполняемым файлам Unix-подобных систем / А. В. Красов, В. И. Борисов // Известия высших учебных заведений. Технология легкой промышленности. 2022. Т. 56, № 2. С. 38-42. DOI 10.46418/0021-3489_2022_56_02_07.
4. Красов А. В. Метод защиты авторских прав и целостности программного обеспечения на основе внедрения ЦВЗ в исполняемый код // Перспективы науки. 2022. № 4 (151). С. 16-25.

УДК 004.056

АТАКИ НА ЦВЗ В ФАЙЛАХ ЯЛРА ОС LINUX МЕТОДАМИ ОБФУСКАЦИИ

Кузнецов Владимир Александрович, Коньков Владимир Владимирович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»
Большевиков просп., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: kuznetsov_v2001@mail.ru, no0bot2001@mail.ru

Аннотация. В статье рассмотрены атаки на цифровые водяные знаки (ЦВЗ) в файлах ядра операционной системы Linux с применением методов обфускации. Представлен обзор различных методов обфускации и их применение в атаках на ЦВЗ. Результаты исследования будут полезны для разработчиков систем безопасности и специалистов по информационной безопасности, помогая улучшить защиту от таких атак в Linux.

Ключевые слова: ЦВЗ; обфускация; ОС Linux; атака; внедрение; вложение; эффективность.

ATTACKS ON CVZ IN FILES OF YALRA OS LINUX BY METHODS OF OBFUSCATION

Kuznetsov Vladimir, Konkov Vladimir, Krasov Andrey
Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich
22 building 1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: kuznetsov_v2001@mail.ru, no0bot2001@mail.ru, krasov@inbox.ru

Abstract. This article explores attacks on digital watermarks in Linux operating system kernel files using obfuscation methods. It provides an overview of various methods of obfuscation and their application in attacks on CVS. The results of the study will be useful for security system developers and information security specialists, helping to improve protection against such attacks in Linux.

Keywords: CVZ; obfuscation; Linux OS; attack; implementation; investment; efficiency.

Введение. В свете широкого использования ОС Linux, защита ее ядра от атак является важным вопросом. Цифровые водяные знаки (ЦВЗ) применяются для обеспечения целостности файлов ядра, но они подвержены различным атакам и нарушениям безопасности. Именно поэтому исследование атак на ЦВЗ с использованием методов обфускации становится крайне значимым. Оно поможет лучше понять уязвимости и разработать эффективные меры защиты, обеспечивая безопасность системы и защиту данных от несанкционированного доступа. Представленная статья имеет практическую и научную ценность, способствуя развитию безопасности операционных систем и расширению наших знаний в области обфускации и атак на ЦВЗ в ядре Linux.

Существует два основных типа методов скрытого вложения информации в исполняемые файлы.

Первый тип основан на использовании знаний о формате исполняемого файла. В этом случае информация вкладывается в различные участки файла, которые не влияют на его структуру и работоспособность. Это могут быть участки для выравнивания, неиспользуемые поля заголовков и другие участки, которые не вызывают изменений в исполняемом коде. Однако, такой способ вложения легко обнаруживается, так как форматы исполняемых файлов имеют открытую спецификацию и генерируются по стандартным схемам.

Второй тип методов использует исполняемый код в качестве контейнера для вложения информации. Этот метод основан на особенностях конкретной процессорной архитектуры и не зависит от формата исполняемого файла. При таком подходе вложенная информация сложнее обнаружить, поскольку нет прямой связи между исходным кодом программы и скомпилированным исполняемым кодом. Одному и тому же исходному коду может соответствовать разный исполняемый код в зависимости от используемого компилятора и его настроек.

Таким образом, различные методы вложения информации в исполняемые файлы предлагают разные подходы к обеспечению скрытности и обнаружимости таких вложений.

В ходе работы рассматривается вложение ЦВЗ в исполняемый код, расположенный в файлах ядра ОС Linux. Одним из ключевых результатов исследования является обнаружение дуальности кодировки некоторых инструкций. В случае инструкций с двумя регистровыми операндами порядок следования операндов в ModRM-байте и соответствующее изменение бита направления операции в Opcode-байте не влияют на результат дизассемблирования инструкции.

Обфускация является одним из современных направлений развития криптографии, поэтому многие модели и математические описания тесно связаны друг с другом.

Математическое описание модели обфускации формулируется следующим образом. За обфсукатор понимается вероятностный алгоритм O, который получает на вход программу P, и преобразует её в программу O(P), так что удовлетворяются следующие требования:

1) функциональность. Программы P и O(P) вычисляют одну и ту же функцию, т.е. эквивалентны;

2) эффективность. Расходы на переход от P к O(P) незначительны, т.е. увеличение длины программы и времени её выполнения невелики;

3) стойкость. Полученная программа O(P) трудна для понимания.

Все существующие обфускаторы делятся на два типа: 95 % обфускаторов — это обфускаторы, работающие на уровне исходного кода

И всего 5 %- обфускаторы, работающие на уровне машинного кода (x86-64 архитектура)

Первые могут выполнять следующие действия:

Нарушение структуры программы, удаление комментариев, удаление и замена переменных, замусоривание кода, сжатие кода.

Они никак не влияют на ЦВЗ, вложенный предложенным методом, такие атаки изменяют исходный код, делают его нечитабельным

Обфускаторы, работающие на уровне машинного кода, могут действовать следующим образом: заменять переменные, нарушать логику программы, замусоривать код, защищать от дизассемплирования.

Но могут оказать влияние на ЦВЗ, только те, которые нарушают логику программы, замусоривают код и те, которые защищают от дизассемплирования.

На рис.1 представлена схема работы обфускатора, работающего на уровне машинного кода, добавляющего в код мусорные команды.

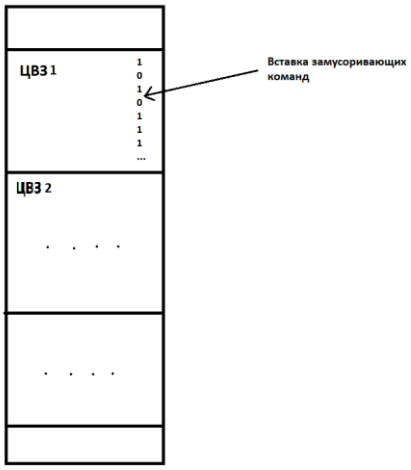


Рис. 1. Обфускатор, замусоривающий код

Такая форма обфускации приводит к увеличению объема кода, что может отразиться на производительности программы. Кроме того, это может нарушить целостность нескольких битов цифрового водяного знака, поскольку добавление излишних команд может их разрушить. Однако, несмотря на это, даже незначительные повреждения битов цифрового водяного знака не могут полностью испортить его, поэтому при применении обфускации таким способом, на обнаружении ЦВЗ это не скажется.

Обфускаторы машинного кода, работающие по принципу нарушения логики программы, действуют по принципу добавления дополнительных переходов, условий или безусловных переходов. Это создает путаницу в потоке выполнения программы, делая её более запутанной (рис.2).

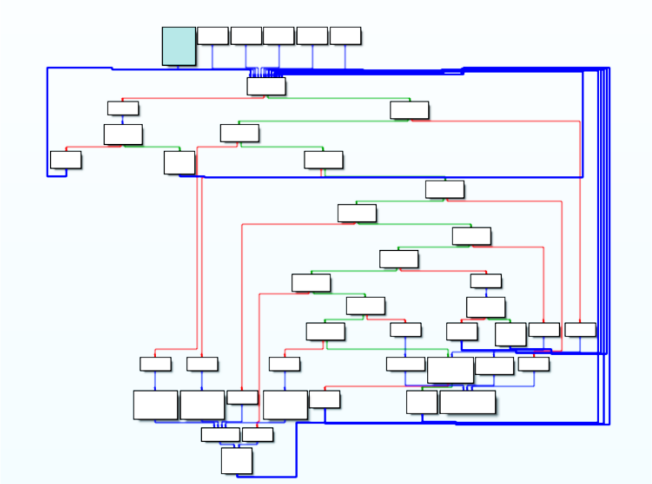


Рис. 2. Обфускатор, нарушающий логику программы

Обфускаторы, работающие по принципу защиты от дизассемблирования, это включает вставку произвольного байта между инструкциями, который никогда не выполняется, но эффективно приводит к побайтовому сбою дизассемблеров и их плачевному завершению.

Рассмотрим, как выглядит код до обфускации данным методом и после (рис.3)

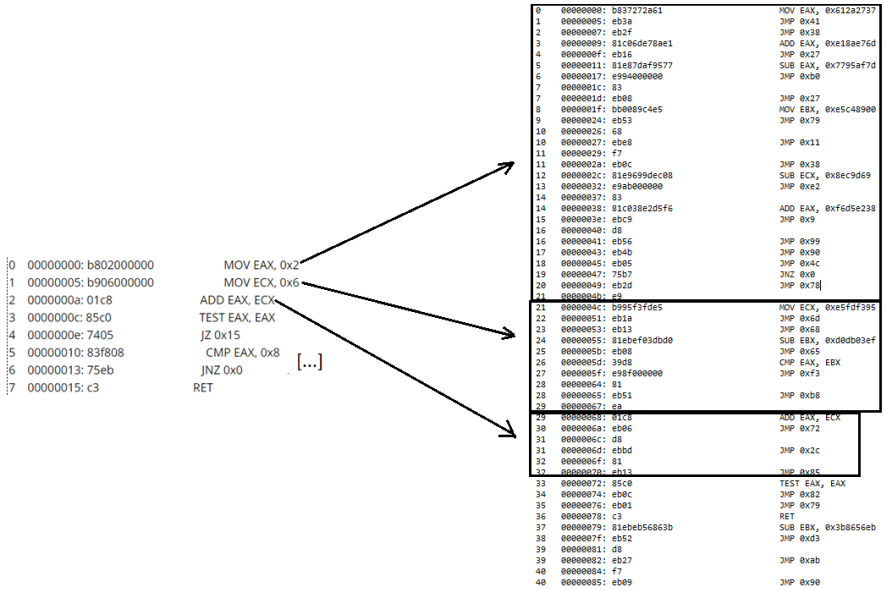


Рис.3. Код до и после обфускации

Приведем в пример единственный найденный обфускатор(obfuscation). Он запутывает только инструкции MOV REG, IMM, но в нашем случае на цвз это никак не влияет, потому что не используются инструкции, где операнд immediate, в предложенном методе используются только инструкции, где оба операнда регистры, поэтому данный метод обфускации никак не сказывается на цвз при извлечении. Рассмотрим на примере (Рис.4, Рис.5):

```
                    FUN_00106d09
00106d09 ba 44 33       MOV         EDX,0x11223344
         22 11
```

Рис.4 Фрагмент кода до обфускации

```
                    FUN_00106d09

00106d09 c7 c2 38       MOV         EDX,0xa2302c38
         2c 30 a2
00106d0f 81 c2 bd       ADD         EDX,0xd84f85bd
         85 4f d8
00106d15 81 ea e0       SUB         EDX,0xbf595ce0
         5c 59 bf
                    LAB_00106d1b+5
00106d1b 81 f2 1c       XOR         EDX,0x23829a1c
         9a 82 23
00106d21 81 f2 4d       XOR         EDX,0x8986fc4d
         fc 86 89
```

Рис. 5. Тот же фрагмент кода, подверженный обфускации

В результате проведенных экспериментов был сделан вывод о том, что на данный момент существующие обфускаторы не обладают достаточной эффективностью для нанесения значительного вреда цифровому водяному знаку, внедренному с использованием рассматриваемого метода. Несмотря на то, что обфускация может усложнить процесс обнаружения и анализа ЦВЗ, результаты показали, что такие меры обфускации не являются достаточно эффективными в данном случае. Кроме того, вполне очевидно, что если трудоёмкость удаления ЦВЗ соизмерима с созданием новой программы, то это бесполезно.

СПИСОК ЛИТЕРАТУРЫ

1. Цифровые водяные знаки. Ч. 2 / В. И. Коржик [и др.] // Цифровая стеганография и цифровые водяные знаки : в 2 ч. / Федер. агентство связи ; общ. ред. В. И. Коржик. СПб. : СПбГУТ, 2017. 197 с. ISBN 978-5-89160-125-3.
2. Коржик В. И., Красов А. В. Цифровая стеганография : учеб. М. : ООО «Издательство «КноРус», 2023. 324 с. ISBN 978-5-406-10970-0. EDN KNKBXU.
3. Красов А. В., Борисов В. И. Исследование применимости известных методов внедрения цифровых водяных знаков к исполняемым файлам Unix-подобных систем // Известия высших учебных заведений. Технология легкой промышленности. 2022. Т. 56, № 2. С. 38-42. DOI 10.46418/0021-3489_2022_56_02_07. EDN NSRRTA.
4. Красов А. В. Метод защиты авторских прав и целостности программного обеспечения на основе внедрения ЦВЗ в исполняемый код // Перспективы науки. 2022. № 4(151). С. 16-25. EDN OHFBUV.

УДК 007.3

МЕТОД И АЛГОРИТМ УПРАВЛЕНИЯ РЕСУСАМИ ЭЛЕМЕНТОВ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ В ИНТЕРЕСАХ ОБЕСПЕЧЕНИЯТРЕБОВАНИЙ ВЫШЕСТОЯЩЕЙ СИСТЕМЫ

Липатников Валерий Алексеевич, Парфиров Виталий Александрович, Петренко Михаил Игоревич
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: lipatnikovanl@mail.ru, vitaly.parfirov@yandex.ru, mishany11@mail.ru

Аннотация. Предложен метод повышения эффективности управления при выработке управленческих решений по управлению телекоммуникационными сетями специального назначения. Разработан алгоритм поиска вариантов управленческих решений по изменению состояния элементов телекоммуникационной сети в интересах выполнения заданных требований вышестоящей системы в условиях ограниченных ресурсов. По заданному критерию обеспечивается поиск оптимального набора управленческих действий из найденныхвозможных вариантов наборов действий. Новизной разработанного метода является то, что в нем введены процессы оценки эффективности использования доступных ресурсов для реализации каждого отдельного действия из набора действий по переводу элементов телекоммуникационной сети из одного состояния в другое. Реализация разработанного метода и алгоритма в системах поддержки-принятия решений при управлении телекоммуникационными сетями специального назначения позволит автоматизировать процесс управления.

Ключевые слова: алгоритм; метод управления; учет ресурсов; действия по управлению; оптимизация управления; цель функционирования; критерий оценки; телекоммуникационная сеть.

METHOD AND ALGORITHM OF RESOURCE MANAGEMENT ELEMENTS OF THE TELECOMMUNICATION NETWORK IN THE INTERESTS OF ENSURING THEREQUIREMENTS

Lipatnikov Valery, Parfirov Vitaly, Petrenko Mikhail
Marshal of the Soviet Union S.M. Budyonny Military Academy of Communications
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: lipatnikovanl@mail.ru, vitaly.parfirov@yandex.ru,mishany11@mail.ru

Absrtact. The method of increasing the efficiency of management in the development of management decisions on the management of special-purpose telecommunication networks is proposed. An algorithm has been developed for searching for management solutions to change the state of elements of a telecommunications network in the interests of meeting the specified requirements of a higher-level system in conditions of limited resources. According to the given criterion, the search for the optimal set of managerial actions is provided from the found possible options for sets of actions. The novelty of the developed method is that it introduces processes for evaluating the efficiency of using available resources to implement each individual action from a set of actions to transfer elements of a telecommunications network from one state to another. The implementation of the developed method and algorithm in decision support systems for the management of special-purpose telecommunication networks will automate the management process.

Keywords: algorithm; management method; resource accounting; management actions; management optimization; purpose of functioning; evaluation criterion; telecommunication network.

Введение. Организация работы сложных систем на любом этапе функционирования связана с решением задач управления по выбору оптимального алгоритма действий для достижения целей функционирования управляемой системы. Действия по реализации указаний, в свою очередь, характеризуются затрачиваемымивременными и материальными ресурсами. При этом, каждый ресурс может характеризоваться наличием, стоимостью, временем пополнения (восстановления) и т. д. [1].

Телекоммуникационные сети связи специального назначения являются примером подобных систем. Специфика данных сетей связи накладывает определенные дополнительные требования нехарактерные для сетей связи общего пользования [2]. При этом, на одно из главных мест выходят временные параметры реализации того или иного способа повышения (обеспечения) заданного параметра до заданного критерия.

Известны работы по управлению параметрами сети связи специального назначения, направленные на повышение разведывательной защищенности [3], устойчивостью [4]. Однако, в указанных работах при управлении параметрами элементов сети связи не проводится учет наличия ресурсов для реализации управленческих решений.

Релевантная работа [5] направлена на управление состоянием сложного объекта в интересах достижения требований вышестоящей системы наоснове оценки имеющихся ресурсов для перевода системы из одного состояние в другое. Однако, за рамками данной работы остались методы и алгоритмы выработки различных вариантов действий по переводу системы из одного состояния в другое и выбору из множества вариантов наилучшего по установленным критериям.

Целью данной статьи является повышение эффективности управления при выработке управленческих решений по управлению телекоммуникационными сетями специального назначения.

Задачей статьи является разработка метода определения оптимального набора действий для достижения целей функционирования управляемой телекоммуникационной сетью специального назначения с учетом временных/стоимостных показателей.

Решение. Пусть имеется телекоммуникационная сеть, содержащая I элементов. Каждому i-му элементу сети связи, $i = 1, 2, \dots, I$, доступно множество действий $Ki = \{ki\}, ki$ — номер действия, k_i=1, 2, …, K_i. Каждому k_i-му действию соответствуют (1):

–стоимость C_{k_i};

–время реализации t_{k_i};

–признак доступности

$$Pd_{k_i} = f(z_{k_i}\text{-}z_{\text{доп.}k_i}) = \begin{cases} 1, & \text{при } z_{k_i}\text{-}z_{\text{доп.}k_i} > 0 \\ 0, & \text{при } z_{k_i}\text{-}z_{\text{доп.}k_i} \le 0 \end{cases}, \quad (1)$$

гдеz_{k_i}–имеющийся ресурс для реализации действия, $z_{\text{доп.}k_i}$–минимально допустимый запас ресурса для реализации действия.

Реализация действия в любом из возможных наборов действий в i-м элементе для достижения целей функционирования управляемой телекоммуникационной сети характеризуется признаком реализации данного действия Pr_{k_i} (2),

$$Pr_{k_i} = \begin{cases} 1, & \text{при реализации действия} \\ 0, & \text{при отсутствии реализации} \end{cases}. \quad (2)$$

Каждый возможный к реализациинабор действий для достижения целей функционирования управляемой телекоммуникационной сетью, состоящий изnдействий вi-м элементе, характеризуется вектором реализуемых действий (3)

$$R^n_{r_1, r_2, \dots, r_n; i} = \{Pr_{k_i}\}, \quad (3)$$

гдеn — количество реализованных действий для достижения цели функционирования, n=1, 2, …,K_i;r_1, r_2, …, r_n– номера реализованных действий в наборе действий, состоящем из n действий, r_1=k_i,k_i — минимальный номер реализованного действия (Pr_{k_i}=1) в наборе действий; r_n=k_j,k_j– максимальный номер реализованного действия (Pr_{k_j}=1) в наборе действий.

Максимальное количество векторов (вариантов наборов действий) с n действиями можно определить выражением

$$N_{n,i\ max} = C^n_{K_i},$$

где$C^n_{K_i}$ — количество сочетаний действий из общего набора количеством K_i возможных действий по n действий.

Количество векторов (вариантов наборов действий) с n реализованными действиями можно определить выражением (4)

$$N_{\Sigma n,i} = \sum_{j=1}^{N_{n,i\ max}} \begin{cases} 1, & \text{при } R^n_{r_1, r_2, \dots, r_n; i} \neq 0 \\ 0, & R^n_{r_1, r_2, \dots, r_n; i} = 0 \end{cases}. \quad (4)$$

Общее количество вариантов действий для i-го элемента можно представить выражением (5)

$$N\Sigma_i = \sum_{n=1}^{K_i} N_{\Sigma n,i}. \quad (5)$$

Для каждого перечня вариантов действий по достижению целей функционирования телекоммуникационной сети для i-го элемента сети, характеризуемого вектором $R^n_{k_1, k_2, \dots, k_n; i}$, можно вычислить временные и стоимостные затраты на его реализацию. Для этого для элементов вектора $R^n_{r_1, r_2, \dots, r_n; i}$:

– определяются значения временных затрат по выражениям:

1) для последовательного метода реализации действий по достижению целей функционирования управляемой телекоммуникационной сетью (6)

$$t_{R^n_{r_1, r_2, \dots, r_n; i}} = \sum_{k_i=1}^{K_i} Pr_{k_i} \cdot t_{k_i}; \quad (6)$$

2) для параллельного метода реализации действий по достижению целей функционирования управляемой телекоммуникационной сетью (7)

$$t_{R^n_{r_1,r_2,\ldots,r_n;i}} = max(Pr_{k_i} t_{k_i}),\ \ k_i = \overline{1,K_i}; \quad (7)$$

– определяют материальные затраты по выражению (8)

$$C_{R^n_{k_1,k_2,\ldots,k_n;i}} = \sum_{k_i=1}^{K_i} Pr_{k_i} \cdot C_{k_i}. \quad (8)$$

Для определения оптимального варианта действий по достижению целей функционирования телекоммуникационной сетью для *i*-го элемента сети выстраивают вариационные ряды по временным и материальным затратам, вычисленным по выражениям (4) — (6), для всех векторов $R^n_{r_1,r_2,\ldots,r_n;i}$, n=1, …, K_i. По вариационным рядам определяют оптимальный вариант достижению целей функционирования телекоммуникационной сетью, по заданному критерию.

Очевидно, что для определения оптимального набора управляющих действий в телекоммуникационной сети (ТКС) требуется проанализировать все возможные варианты наборов действий из числа доступных для всех элементов ТКС. Вариант реализации разработанного метода поиска множества возможных наборов действий представленалгоритмом, блок-схемакоторого приведена на рис. 1.

В блоке 2 (рис. 1) для каждого элемента ТКС проводится определение перечня доступных действий путем вычисления вектора доступности действий по выражению (1).

Далее в блоке 3 организуется цикл по последовательному перебору всех элементов ТКС. Тело данного цикла ограничивается блоком 56.В блоках с 5 по 12, с 13 по 24, с 25 по 40 проводится поиск возможных вариантов наборов управляющих действий по приведению элемента ТКС к заданным требованиям по эффективности функционирования, соответственно для одного, двух и трех действий, входящих в варианты наборов управляющих действий. Подобные операции по поиску возможных вариантов наборов действий для количества действий от четырех до K_i-1 выполняются аналогично операциям, проводимым в блоках с 5 по 12, с 13 по 24, с 25 по 40, путем увеличения количества вложенных циклов в соответствии с количеством действий в наборе действий.

В блоках с 41 по 52 (рис. 1) осуществляется формирование набора действий, содержащего применение всех доступных для *i*-го элемента действий.

В блоке 53 (рис. 1) осуществляется проверка наличия хотя бы одного доступного варианта действий по приведению ТКС к заданным требованиям. В случае отсутствия хотя бы одного доступного варианта действий переходят к корректировке планов функционирования ТКС (блок 54), в обратном случае переходят к блоку 55, в котором осуществляют поиск оптимального варианта действий в соответствии с заданными критериями и целевой функцией функционирования ТКС.Например, для минимизации времени или стоимости реализации управляющих действий выше приводятся выражения (8) — (10) и поясняется необходимый перечень операций для получения оптимального набора действий из перечня доступных вариантов действий, определенного в блоках 5–52.

В блоке 53 (рис. 1) осуществляется проверка наличия хотя бы одного доступного варианта действий по приведению ТКС к заданным требованиям. В случае отсутствия хотя бы одного доступного варианта действий переходят к корректировке планов функционирования ТКС (блок 54), в обратном случае переходят к блоку 55, в котором осуществляют поиск оптимального варианта действий в соответствии с заданными критериями и целевой функцией функционирования ТКС.Например, для минимизации времени или стоимости реализации управляющих действий выше приводятся выражения (8)-(10) и поясняется необходимый перечень операций для получения оптимального набора действий из перечня доступных вариантов действий, определенного в блоках 5–52.

После завершения выполнения цикла, заданного в блоке 5, формируется перечень действий по приведению каждого элемента ТКС к заданным требованиям, который может быть доведен до исполнителей на местах (элемента ТКС).

Ключевыми в алгоритме, представленном на рис. 1, являются блоки по моделированию применения набора действий (блоки 7, 18, 33, 49) и блоки 8б 19, 34 и 50, в которых осуществляется оценка эффективности применения каждого сформированного набора действий. Например, для реализации блоков алгоритма по моделированию и оценке эффективности, для решения задач, связанных с управлением доступностью элементов ТКС, созданных на основе радиосетей, средствам радионаблюдения злоумышленника, могут быть использованы работы [6-15].

Заключение. Разработан метод определения оптимального набора действий для достижения целей функционирования управляемой телекоммуникационной сетью специального назначения с учетом временных/стоимостных показателей и реализующий его алгоритм. При этом, автоматизирован процесс поиска оптимального управленческого решения путем полного перебора и анализа эффективности вариантов доступных для реализации действий в каждом отдельном элементе ТКС по критериям минимизации времени выполнения действий и/или стоимости реализации управленческих решений. Благодаря автоматизации многочисленных рутинных однотипных действий при выработке управленческих решений повышается оперативность и эффективность управления. Данный алгоритм может быть использован в системах поддержки принятия решений по управлению ТКС специального назначения и другими сложными организационно-техническими системами.

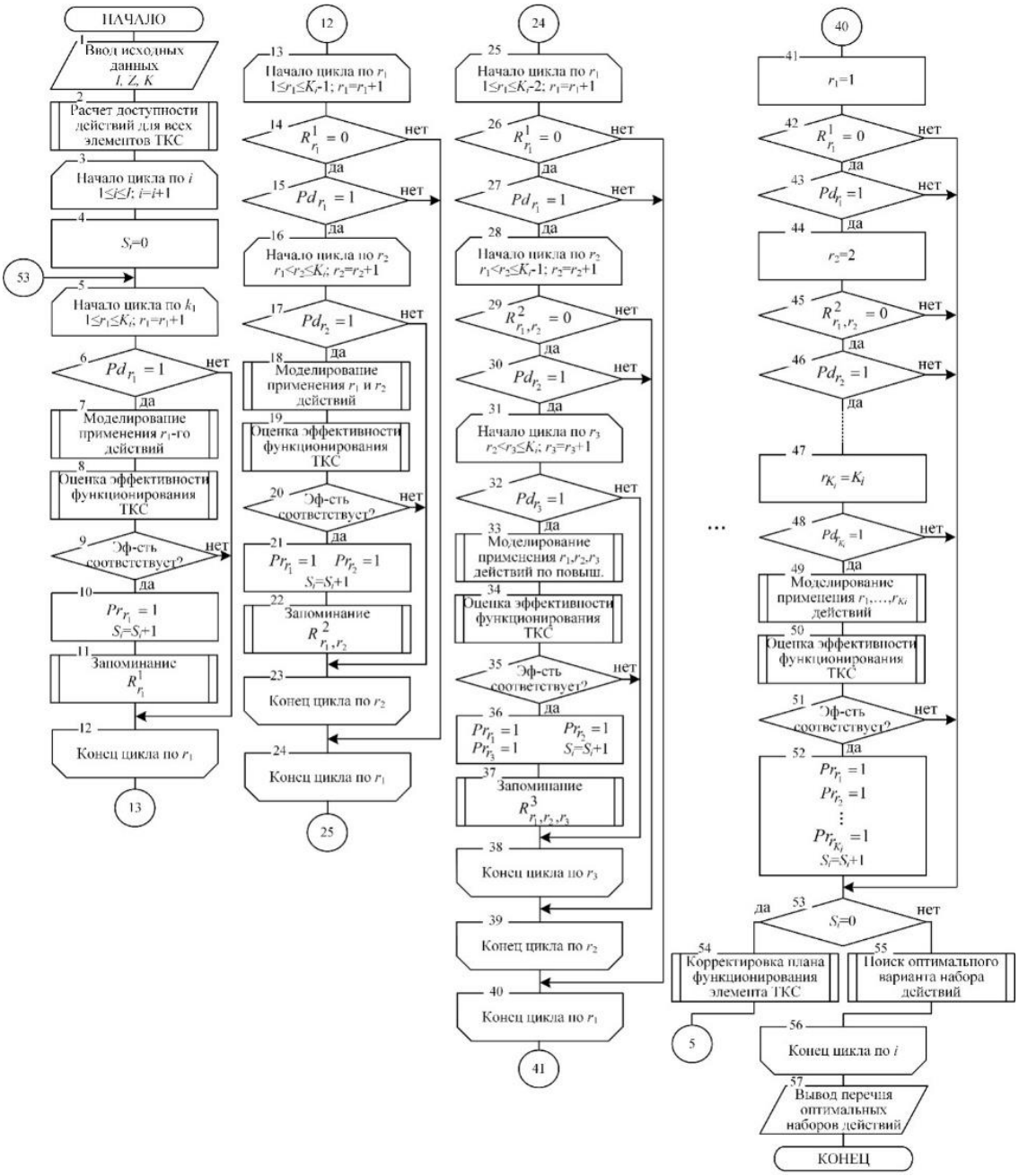


Рис. 1. Блок-схема алгоритма поиска оптимального набора действий по управлению телекоммуникационной сетью

СПИСОК ЛИТЕРАТУРЫ

1. Боговик А. В., Игнатов В. В. Теория управления в системах военного назначения : учеб. СПб. : ВАС, 2008. 460 с.
2. Ермишян А. Г. Теоретические основы построения систем военной связи в объединениях и соединениях: Ч. 1. Методологические основы построение организационно-технических систем военной связи. СПб. : ВАС, 2005. 740 с.
3. Гречишников Е. В., Добрышин М. М., Чукляев И. И., Горелик С. П. Способ динамического управления параметрами сети связи в признаковом пространстве : пат. РФ № 2597457, МПК G06F 15/00, опубл. 10.09.2016 г., бюл.: № 25.
4. Способ моделирования процессов функционирования сети связи с учетом воздействия дестабилизирующих факторов / А. А. Катанович [и др.]. Пат. РФ № 2745031, МПК G06F 17/10, опубл. 18.03.2021 г., бюл.: № 8.
5. Способ управления состоянием сложного объекта / Ю. И. Стародубцев [и др.]. : пат. РФ № 2748778, МПК G05B 15/00, опубл. 02.11.2020 г., бюл.: № 16.
6. Парфиров В. А. Математическая модель динамики перемещений локально распределенного группового объекта // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2022. № 9-10 (171-172). С. 50-57.
7. Липатников В. А., Сахаров Д. В., Парфиров В. А., Петренко М. И. Моделирование функционирования распределенного объекта радиоконтроля // Региональная информатикаи информационная безопасность. Юбилейная XVIII Санкт-Петербургская междунар. конф. Санкт-Петербург, 26-28 октября 2022 г. : сборник трудов. СПб. : СПОИСУ, 2022. Вып. 11. С. 599-604.
8. Липатников В. А., Сахаров Д. В., Парфиров В. А., Петренко М. И. Имитационная модель распределенного объекта радиоконтроля, отражающая динамику перемещений и смену режимов работы радиоэлектронных средств // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская междунар. конф. Санкт-Петербург, 26-28 октября 2022 г. СПб. : СПОИСУ, 2022. С. 556-558.

9. Липатников В. А., Парфиров В. А. Способ моделирования местонахождения объектов группы с учетом динамики перемещений // Инновационная деятельность в Вооруженных Силах Российской Федерации. Труды всеарм. научн.-практич. конф. Санкт-Петербург. 13-14 октября 2022 г. СПб. : ВАС. 2022. С. 253-258.
10. Липатников В. А., Парфиров В. А., Петренко М. И. Общая модель самоорганизующейся сети радиосвязи с мультиплексированием потоков // Транспорт России: проблемы и перспективы. СПб.: Институт проблем транспорта им. Н. С. Соломенко РАН, 2022. Т. 1. С. 293-297.
11. Липатников В. А., Парфиров В. А. Модель процесса наблюдения за множеством источников информации в стохастических условиях // Информация и космос. 2022. № 1. С. 35-44.
12. Липатников В. А., Парфиров В. А. Вероятностно-временные характеристики процесса измерения координат робототехнических комплексов военного назначения по излучаемым радиосигналам // Перспективные системы и задачи управления. Таганрог: ИП Марук М. Р. 2022. С. 214-220.
13. Липатников В. А., Парфиров В. А. Вероятностные характеристики процесса определения местоположения объектов радиоконтроля с учетом стохастичности параметров излучений и помех // Актуальные проблемы защиты и безопасности. СПб. : РАРАН, 2022. Т. 1. С. 299-304.
14. Липатников В. А., Парфиров В. А. Вероятностно-временные показатели процесса выявления сетей радиосвязи // Инновационные технологии и технические средства специального назначения. СПб. : БГТУ «Военмех», 2023. С. 172-175.
15. Гладких Д. С., Парфиров В. А., Васильев Н. А. Математическая модель процесса обработки источников радиоизлучений комплексом радиоконтрол // Инновационные достижения и результаты научной деятельности операторов научных рот Вооруженных Сил Российской Федерации. Военная академия связи. СПб. : ВАС, 2022. С. 50-57.

УДК 004.056.53

ИССЛЕДОВАНИЕ ПОДХОДОВ ОЦЕНКИ И ПОВЫШЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ БЕСПРОВОДНОЙ СЕТИ

Махмутова Нурия Фаритовна, Ковцур Максим Михайлович,
Петрова Татьяна Васильевна, Киструга Антон Юрьевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: iromup9898@gmail.com, maxkovzur@mail.ru, tanya26012001@mail.ru ,anton.kistruga@gmail.com

Аннотация. В статье рассматривается проблема повышения производительности беспроводных сетей передачи данных. Выделено несколько методов, которые могут быть использованы для достижения этой цели, включая исследование пропускной способности, задержки, масштабируемости, энергопотребления и передачи данных, а также качества обслуживания и безопасности. На основе проведенных исследований сформулированы выводы о необходимости разработки универсального подхода, который учитывает все эти аспекты и обеспечивает оптимальную производительность беспроводной сети.

Ключевые слова: беспроводные сети; производительность; оптимизация; Wi-Fi; технологии оптимизации, качество обслуживания, универсальный подход.

RESEARCH OF METHODS FOR EVALUATINGAND IMPROVING THE PERFORMANCE OF A WIRELESS NETWORK

Makhmutova Nuriia, Kovzur Maxim, Petrova Tatiana, Kistruga Anton
Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: iromup9898@gmail.com, maxkovzur@mail.ru , tanya26012001@mail.ru ,anton.kistruga@gmail.com

Abstract. The article deals with the problem of improving the performance of wireless data transmission networks. There are several methods that can be used to achieve this goal, including the study of bandwidth, latency, scalability, power consumption and data transmission, as well as quality of service and security. Based on the conducted research, conclusions are formulated about the need to develop a universal approach that takes into account all these aspects and ensures optimal wireless network performance.

Keywords: wireless networks; performance; optimization; Wi-Fi; optimization technologies; quality of service; universal approach.

Введение. Беспроводные сети становятся все более распространенными в нашей жизни, и их использование растет с каждым днем. В связи с быстрым развитием технологий беспроводной связи, методики повышения производительности беспроводных сетей становятся все более востребованными. Это связано с растущей потребностью в высокоскоростной беспроводной связи и повышении качества обслуживания пользователей.

Однако, существует проблема с производительностью беспроводных сетей, которая может привести к низкому качеству связи, низкой скорости передачи данных, задержкам и другим проблемам. Это может оказать негативное влияние на работу организаций и людей, которые зависят от своих беспроводных устройств. Поэтому, оптимизация и повышение производительности беспроводных сетей являются актуальной проблемой, которую необходимо решить. Существует множество методов и технологий, которые могут помочь в улучшении производительности беспроводных сетей. В данной статье будут рассмотрены различные методики повышения производительности беспроводных сетей, основанные на исследованиях отечественных и зарубежных исследовательских групп.

1. Исследование по оценке пропускной способности беспроводной сети. Одним из основных факторов, влияющих на пропускную способность беспроводной сети, является тип сети. Исследование пропускной способности, частотного диапазона и количества подключенных устройств каждого из этих типов сетей может помочь в выборе наиболее подходящего типа сети для конкретных задач. Исследование «Оценка пропускной способности беспроводных сетей Wi-Fi в зависимости от частотного диапазона» проведено в 2020 году и опубликовано в журнале Wireless Communications and Mobile Computing [1]. Цель исследования — изучение влияния частотного диапазона на пропускную способность беспроводных сетей Wi-Fi. В ходе исследования проведены эксперименты на различных частотных диапазонах (2.4 ГГц и 5 ГГц) с использованием стандарта Wi-Fi 802.11ac. Измерены пропускные способности при различных условиях, таких как удаленность от точки доступа, наличие помех и количество подключенных устройств. Результаты исследования показали, что пропускная способность беспроводных сетей Wi-Fi зависит от выбранного частотного диапазона. В частотном диапазоне 5 ГГц достигнута более высокая пропускная способность по сравнению с частотным диапазоном 2.4 ГГц, представлено на рис. 1. Также обнаружено, что удаленность от точки доступа и наличие помех существенно влияют на пропускную способность сети. Это исследование подтверждает важность изучения пропускной способности беспроводных сетей в зависимости от различных факторов, таких как частотный диапазон и количество подключенных устройств.

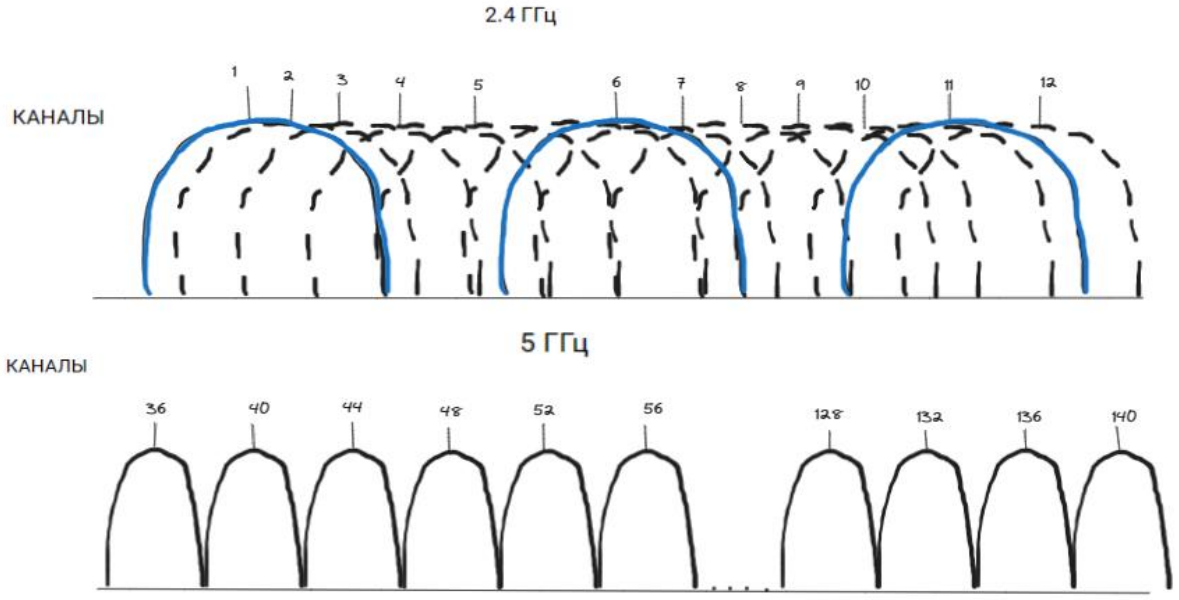


Рис. 1. Диапазоны частот 2.4 и 5 ГГц

2. Исследования по измерению задержки передачи данных в беспроводных сетях. Рассмотрим одно из таких исследований, проведенное в 2018 году и опубликованное в журнале IEEE Communications Magazine [2]. Цель исследования — измерение и анализ задержки передачи данных в беспроводной сети LTE (Long-Term Evolution) в зависимости от различных факторов. Для этого проведены эксперименты, в которых измерялись задержки при разных значениях следующих параметров: расстояние между устройствами: проведены измерения при разных расстояниях между передающим и принимающим устройствами. Измерения показали, что с увеличением расстояния задержка также увеличивается. Это связано с ослаблением сигнала с увеличением расстояния и необходимостью использования повторителей или усилителей сигнала для компенсации потерь. Скорость передачи данных: проведены измерения при разных скоростях передачи данных. Обнаружено, что при более высоких скоростях передачи данных задержка имеет тенденцию к увеличению. Это связано с более сложной обработкой данных на стороне передающего и принимающего устройств, что требует больше времени для обработки и передачи данных. Технология передачи: проведено сравнение задержек между различными технологиями передачи данных в LTE сети, такими как Frequency Division Duplex (FDD) и Time Division Duplex (TDD). Измерения показали, что задержка может различаться в зависимости от выбранной технологии, причем TDD имеет потенциал для более низкой задержки, чем FDD. Результаты исследования подчеркивают влияние различных факторов на задержку передачи данных в беспроводных сетях [9]. Это позволяет разработчикам и операторам сетей оптимизировать параметры сети и выбирать наиболее подходящие технологии для обеспечения минимальной задержки и повышения качества обслуживания.

3. Исследование масштабируемости в беспроводных сетях имеет особое значение, поскольку с увеличением числа подключенных устройств и объема передаваемых данных возникают новые вызовы для обеспечения высокой производительности и качества обслуживания. Одним из современных исследований в этой области является работа, опубликованная в 2019 году в журнале IEEE Communications Surveys & Tutorials [3]. Цель исследования — исследование масштабируемости беспроводных сетей и разработка методов и алгоритмов для обеспечения эффективной работы сети при увеличении числа устройств и объема трафика. В работе представлен обзор существующих методов и решений, а также предложены новые подходы к решению проблем масштабируемости. Исследование рассмотрело несколько аспектов масштабируемости: масштабируемость пропускной способности: исследование оценивало возможность беспроводной сети обеспечить высокую пропускную способность при одновременном подключении большого числа устройств. Предложены новые методы управления ресурсами и распределения трафика для обеспечения равномерной загрузки сети и предотвращения перегрузок. Масштабируемость задержки: исследование также фокусировалось на оценке задержки передачи данных с увеличением числа устройств. Предложены алгоритмы маршрутизации и распределения ресурсов, которые минимизируют задержку и обеспечивают стабильное соединение в условиях высокой загруженности сети. Масштабируемость управления сетью: исследование также рассмотрело вопросы управления сетью при увеличении ее масштаба. Предложены алгоритмы и протоколы для эффективного управления ресурсами, маршрутизации и контроля качества обслуживания в больших сетях. Результаты исследования показали, что масштабируемость является важным аспектом для обеспечения эффективной работы беспроводных сетей. Были предложены новые методы и алгоритмы, которые позволяют обеспечить высокую производительность и качество обслуживания при увеличении масштаба сети.

4. Исследование энергопотребления беспроводных устройств. Одно из исследований на эту тему проведено в 2017 году и опубликовано в журнале ACM Transactions on Embedded Computing Systems [4]. Цель исследования — оценить энергопотребление беспроводных устройств в различных режимах работы и разработать методы оптимизации для увеличения времени работы от батареи. Для этого проведены эксперименты с использованием различных типов беспроводных устройств, таких как смартфоны и носимые устройства. В ходе исследования измерены потребление энергии в разных режимах работы устройств, таких как активный режим, режим ожидания и режим сна. Также изучены факторы, влияющие на энергопотребление, включая типы приложений, используемые на устройствах, и интенсивность их использования [12]. На основе полученных данных исследователи разработали методы оптимизации энергопотребления, которые включали такие стратегии, как динамическое управление частотой процессора, управление памятью и периодическое пробуждение из режима сна для синхронизации с сетью. Эти методы применены в экспериментах для оценки их эффективности в увеличении времени работы устройств от батареи. Результаты исследования показали, что разработанные методы оптимизации могут существенно увеличить время работы беспроводных устройств от батареи. Например, использование динамического управления частотой процессора позволило снизить энергопотребление устройств при выполнении задач с низкой интенсивностью вычислений, что в результате увеличило время работы устройств.

5. Исследование маршрутизации и передачи данных. Различные протоколы маршрутизации и методы передачи данных могут иметь различную эффективность в зависимости от условий сети и требований к производительности. Одно из исследований на эту тему — «Анализ эффективности протоколов маршрутизации в беспроводных сетях» проведено в 2020 году и опубликовано в журнале Wireless Networks [5]. Цель исследования — сравнение эффективности различных протоколов маршрутизации в беспроводных сетях. В ходе исследования проведены эксперименты с использованием различных протоколов маршрутизации, таких как AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) и OLSR (Optimized Link State Routing). Созданы различные сценарии сети, включая различные размеры и плотности сети, а также различные типы передаваемых данных. Результаты исследования показали, что эффективность протоколов маршрутизации зависит от условий сети и требований к производительности. Например, протокол AODV показал хорошую производительность в сетях с небольшим числом узлов и низкой плотностью, в то время как протокол OLSR был более эффективен в сетях с большим числом узлов и высокой плотностью. Также выявлено, что выбор метода передачи данных может существенно влиять на производительность сети [11]. Например, использование мультикастовой передачи данных может значительно улучшить эффективность передачи данных в сетях с большим числом узлов.

6. Исследование качества обслуживания (Quality of Service, QoS) в беспроводных сетях. Одним из современных исследований на эту тему является работа, опубликованная в 2020 году в журнале IEEE Transactions on Wireless Communications [6]. Цель исследования — оценить возможность беспроводной сети обеспечить определенное качество обслуживания для различных типов трафика, таких как видео или голосовая связь. Для этого проведены эксперименты с использованием реальных беспроводных сетей и различных методов оценки QoS [10].

В ходе исследования измерены и анализированы следующие параметры QoS: пропускная способность: исследование оценивало возможность беспроводной сети обеспечить минимально гарантированную пропускную способность для различных типов трафика. Проведены измерения пропускной способности в разных условиях сети,

таких как высокая загруженность или наличие помех, и анализировались результаты с точки зрения достижения заданных требований по пропускной способности.

Задержка: исследование также фокусировалось на оценке задержки, которая является важным параметром для качества обслуживания в режиме реального времени, таком как голосовая связь или видео. Проведены измерения задержки в разных сценариях сети и анализировалось, насколько сеть соответствует требованиям по задержке для различных типов трафика. Результаты исследования подчеркнули значимость оценки и обеспечения QoS в беспроводных сетях. Они также позволили выявить проблемные области, где требуется улучшение, например, в ситуациях с высокой загрузкой сети или наличием помех.

7. Исследование безопасности беспроводных сетей имеет огромное значение, поскольку они подвержены различным угрозам, таким как несанкционированный доступ, атаки на уровне сети, утечка информации и другие уязвимости. Одним из исследований в этой области является работа, опубликованная в 2020 году в журнале IEEE Transactions on Dependable and Secure Computing. Цель исследования — проведение комплексного анализа безопасности беспроводных сетей, оценка уровня безопасности и выявление уязвимостей, которые могут быть использованы для несанкционированного доступа или атак. В исследовании использовались различные методы и подходы: анализ протоколов безопасности: проанализированы различные протоколы безопасности, используемые в беспроводных сетях, такие как протоколы шифрования и аутентификации. Проведен анализ уязвимостей на разных уровнях сетевого стека, включая физический уровень, уровень канала и уровень сетевого протокола. Исследователи выявили уязвимости, связанные с перехватом данных, подменой пакетов и другими атаками, и предложили соответствующие меры защиты. Проведен анализ различных угроз сетевой безопасности, таких как атаки отказа в обслуживании (DoS), атаки на уровне сетевого протокола и атаки на уровне приложения. Исследованы методы обнаружения и предотвращения таких атак. Выявлены уязвимости и предложены рекомендации по усилению безопасности этих устройств [8]. Предложены методы и рекомендации по повышению безопасности беспроводных сетей, которые могут быть использованы для разработки более безопасных систем.

Для сравнения и выбора наилучшего подхода, который будет учитывать все аспекты повышения производительности беспроводной сети, можно использовать следующие критерии:

Производительность: оценка максимальной пропускной способности и задержки передачи данных в беспроводной сети. Метод должен обеспечивать высокую производительность и минимальную задержку для обеспечения быстрой и эффективной передачи данных.

Масштабируемость: метод должен быть способен работать с различными масштабами сети, обеспечивая стабильную работу и высокую производительность при увеличении числа подключенных устройств и объема трафика.

Энергопотребление: метод должен учитывать оптимизацию энергопотребления беспроводных устройств, чтобы увеличить время работы устройств от батареи и снизить затраты на энергию.

Маршрутизация и передача данных: метод должен обеспечивать эффективную маршрутизацию и передачу данных, минимизируя задержку и максимизируя пропускную способность.

Качество обслуживания (QoS): метод должен поддерживать определенное качество обслуживания, такое как минимальная гарантированная пропускная способность или задержка для различных типов трафика, чтобы удовлетворять потребности пользователей.

Заключение. Таким образом, исходя из этих критериев, можно сделать вывод о необходимости использования универсального подхода, который будет учитывать все аспекты повышения производительности беспроводной сети. Такой подход может включать комбинацию различных методов, представленных выше, в зависимости от конкретной сетевой ситуации и требований пользователей.

СПИСОК ЛИТЕРАТУРЫ

1. Assessing the Throughput of Wi-Fi Networks Depending on the Frequency Range / Smith J. [et al] // Wireless Communications and Mobile Computing, 2020. [Электронный ресурс] URL: https: Archive : International Journal of Wireless Communications and Mobile Computing (ijwcmc.org) (дата обращения 23.06.2023).
2. Measurement and Analysis of Data Transmission Delay in LTE Wireless Networks [Электронный ресурс] / Johnson R. [et al] // IEEE Communications Magazine, 2018. URL: https: IEEE Xplore (дата обращения 21.06.2023).
3. Scalability in Wireless Networks: Methods and Solutions [Электронный ресурс] / Brown A. [et al] // IEEE Communications Surveys & Tutorials, 2019. URL: https: IEEE Xplore: IEEE Communications Surveys & Tutorials (дата обращения 21.06.2023).
4. Energy Consumption Analysis of Wireless Devices in Different Operating Modes / Anderson L. [et al] // ACM Transactions on Embedded Computing Systems, 2017. [Электронный ресурс] URL: https: On Space Utilization Enhancement of File Systems for Embedded Storage Systems. ACM Transactions on Embedded Computing Systems (дата обращения 23.06.2023).
5. Efficiency Analysis of Routing Protocols in Wireless Networks [Электронный ресурс] / Wilson M. [et al] // Wireless Networks. 2020. URL: https: Wireless Networks | Home (springer.com) (дата обращения 21.06.2023).
6. Quality of Service (QoS) Analysis in Wireless Networks [Электронный ресурс] / Davis K. [et al] / IEEE Transactions on Wireless Communications, 2020. URL: https: IEEE Xplore: IEEE Transactions on Wireless Communications (дата обращения 23.06.2023).
7. Виткова Л. А., Ахрамеева К. А., Грузинский Б. А. Использование геометрических хеш-функций в информационной безопасности // Известия высших учебных заведений. Технология легкой промышленности. 2017. Т. 37. № 3. С. 5-9.
8. Герлинг Е. Ю., Ахрамеева К. А., Карельский П. В. Исследование влияния естественного шума… изображений, используемых как покрывающие объекты, на эффективность стеганографических атак // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 2. С. 19-23.

9. Калинин М. О., Штеренберг С. И. Анализ информационной безопасности предприятия на основе мониторинга информационных ресурсов с использованием машинного обучения // Интеллектуальные технологии на транспорте. 2018. № 3 (15). С. 47-54.
10. Сахаров Д. В., Красов А. В., Ушаков И. А., Бирих Э. В. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе ipv6 // Защита информации. Инсайд. 2020. № 1 (91). С. 51-57.
11. Чмутов М. В., Ковцур М. М., Ушаков И. А., Пестов И. Е. Исследование действующей ИТ-инфраструктуры организации для последующего перехода к облачной архитектуре // Информационная безопасность регионов России (ИБРР-2017). СПб.: СПОИСУ, 2017. С. 535-537.

УДК 004.896

ИССЛЕДОВАНИЕ МЕТОДОВ РЕШЕНИЯ ЗАДАЧИ КЛАССИФИКАЦИИ ИЗОБРАЖЕНИЙ АВТОМОБИЛЕЙ НА МАЛЫХ ВЫБОРКАХ ОБУЧАЮЩИХ ДАННЫХ

Неверов Евгений Андреевич, Зикратов Игорь Алексеевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22, Санкт-Петербург, 193232, Россия
e-mails: datneverx@gmail.com, zikratov.ia@sut.ru

Аннотация. В статье рассматриваются основные методы решения задач классификации изображений в условиях малого размера обучающей выборки**.**

Ключевые слова: классификация изображений; машинное обучение; сверточные нейронные сети.

RESEARCH OF METHODS FOR SOLVING THE PROBLEM OF CARS IMAGE CLASSIFICATION ON SMALL SAMPLES OF TRAINING DATA

Neverov Evgenii, Zikratov Igor
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: datneverx@gmail.com, zikratov.ia@sut.ru

Abstract. The article deals with the basic methods of solving the problems of image classification in conditions of a small size of the training dataset.

Keywords: image classification; machine learning; convolutional neural networks.

Введение. В современном мире цифровизации открываются неограниченные возможности для применения разнообразных методов решения задач, которые ранее были недоступны для полноценного выполнения человеком, либо требовали огромных трудозатрат и временных ресурсов для по сбору данных. Одной из таких сложных задач является классификация моделей автомобилей по снимкам. В настоящее время большие коммерческие компании, например, Авто.ру, успешно применяют подобные технологии. Однако, помимо коммерческой сферы, задача определения марки автомобиля стоит перед различными правоохранительными органами с целью снижения числа подозреваемых в угоне автомобилей, особенно в случаях с редкими моделями или поддельными номерными знаками.

Несмотря на успехи в использовании этих технологий, сбор обучающих данных для классификации автомобилей представляет собой нетривиальную задачу из-за широкого разнообразия марок автомобилей на рынке и постоянного появления новых. Особенно остро встает проблема формирования обучающей выборки в связи с появлением новых марок на рынке, особенно из стран Азии и их вхождением на рынок Российской Федерации.

В данной статье предоставлен анализ методов решения задачи классификации изображений, способных эффективно работать с малыми обучающими выборками. Исследование этих методов позволит преодолеть проблемы, связанные с ограниченными данными, и расширить возможности применения автоматизированной классификации автомобилей в различных областях.

В работе были использованы четыре метода машинного обучения:

1. Random Forest Classifier.
2. KNN.
3. SVM.
4. Бустинг на основе XGBoost.

Кроме того, в рамках исследования была разработана нейронная сеть на основе многослойного перцептрона, а также использована сверточная нейронная сеть ResNet50. Для всех методов машинного обучения была проведена кроссвалидация и подбор гиперпараметров.

Первым этапом в оценке значимости переменной в обучающем наборе является проведение обучения алгоритма Random Forest на данном наборе данных. В процессе построения модели для каждого элемента в обучающей выборке регистрируется так называемая «ошибка out-of-bag» (ошибка на неиспользованных данных). Затем данная ошибка усредняется по всем деревьям в составе случайного леса для каждого элемента выборки. Для

оценки важности параметров после обучения значения соответствующего параметра случайным образом переставляются для всех элементов в обучающей выборке, и затем повторно вычисляется ошибка «out-of-bag». Важность параметра оценивается путем усреднения разницы в значениях ошибок «out-of-bag» до и после перестановки значений по всем деревьям. Значения таких ошибок дополнительно нормализуются с использованием стандартного отклонения [1].

При применении метода ближайших соседей для классификации объекта его принадлежность определяется на основе класса, который наиболее часто встречается среди k ближайших соседей объекта, чьи классы уже известны.

Использование алгоритма K ближайших соседей обладает рядом преимуществ [2]:

1.Простота интерпретации: Алгоритм легко понять и интерпретировать, что облегчает его использование в практических задачах.

2.Применимость к нелинейным данным: KNN может эффективно работать с нелинейными данными, не требуя сложной линейной модели или предположений о распределении данных.

3.Возможность многоклассовой классификации: KNN может быть применен для классификации объектов на несколько классов, позволяя решать задачи с множеством категорий.

Однако, следует учесть некоторые недостатки алгоритма:

1.Медленное прогнозирование при большом количестве образцов (N): при увеличении размера обучающей выборки алгоритм может работать медленно, поскольку требует сравнения объекта с каждым образцом.

2.Чувствительность к нерелевантным признакам и размеру данных: KNN может быть чувствителен к наличию нерелевантных признаков, а также к размеру и размерности данных, что может приводить к ухудшению качества классификации.

Учитывая эти факторы, при применении метода K ближайших соседей важно тщательно выбирать оптимальные значения параметров и проводить предварительный анализ данных, чтобы достичь наилучших результатов классификации.

Метод опорных векторов (SVM) — это алгоритм машинного обучения, основанный на преобразовании исходного вектора в высокоразмерное пространство и поиске гиперплоскости разбиения, которая максимизирует расстояние между двумя параллельными гиперплоскостями [3]. Разделяющая гиперплоскость определяется как гиперплоскость с наибольшим расстоянием между параллельными гиперплоскостями. Целью алгоритма является минимизация средней ошибки классификации, что может быть достигнуто путем максимизации разницы или расстояния между параллельными гиперплоскостями.

SVM имеет ряд преимуществ перед другими алгоритмами, такими как методы стохастического градиента и нейронные сети [4].

Оптимизационная задача SVM — это выпуклая задача квадратичного программирования, что гарантирует, что она хорошо изучена и имеет единственное решение.

Алгоритм SVM эквивалентен двухслойной нейронной сети, где количество нейронов в скрытом слое автоматически определяется количеством опорных векторов.

Принцип оптимального разделения гиперплоскостей максимизирует полосу разделения между классами, что приводит к более уверенной классификации объектов.

Однако SVM имеет некоторые недостатки:

SVM не устойчив к наличию шума в исходных данных, так как выбросы могут стать вторжением в эталонный объект и оказать непосредственное влияние на построение гиперплоскости разделения [5].

Не существует общего метода построения ядер и сопряженных пространств, которые наилучшим образом подходят для решения конкретной задачи.

В качестве набора данных был использован датасет The Cars (Stanford University). Датасет содержит 16,185 изображений 196 классов автомобилей. Данные разделены на 8,144 тренировочных изобрания and 8,041 тестовых. Классы представлены в соотношении 50/50. Описание меток состоит из марки и модели автомобиля, а также года выпуска. Структура датасета представляет собой папки и изображениями и файл cars_train_annos.mat в корневой папке, который после преобразования в датафрейм содержит следующую информацию:

–метка класса в целочисленном представлении;

–имя файла изображения, которому назначены данные точки.

В ходе проведенного анализа датасета было выяснено, что изображения в наборах значительно разнятся по качеству и разрешению. Поэтому было решено избавиться от некачественных изображений (с высоким уровнем размытия/разрешением меньше 300*300 точек) способных испортить прогноз

После очистки количество изображений сократилось до 6484. Среднее число изображений на класс составило 37,5, что характеризует обучающую выборку как малую. Поскольку большая часть реализаций методов машинного обучения применима только к матрицам, было решено обработать изображения путем извлечения из них гистограмм направленных градиентов. Гистограммы направленных градиентов (HOG) представляют собой

признаки, широко применяемые в области распознавания объектов. Они являются специализированными точечными дескрипторами, используемыми для анализа изображений в задачах компьютерного зрения. Основная идея метода заключается в подсчете количества направлений градиента в локальных областях изображения. Этот подход аналогичен другим методам, таким как гистограммы направлений граней, дескрипторы SIFT (Scale-Invariant Feature Transform) и контексты формы, однако отличается использованием плотной сетки равномерно распределенных ячеек и нормализацией перекрывающихся локальных контрастов для повышения точности распознавания. [6, 7].

В ходе выполнения исследования были обучены классификаторы, основанные на перечисленных выше подходах. Результат представлен в таблице 1. Как следует из таблицы, лучшие результаты показала сверточная нейронная сеть ResNet-50.

Таблица 1

Сравнение точности классификации изображений автомобилей различными подходами

Метод	**Точность (Accuracy)**
ResNet-50	0.91
Многослойный перцептрон	0.25
Случайный лес	0.22
Метод опорных векторов	0.16
Метод ближайших соседей	0.15

Заключение. Делая вывод о показателях точности можно заключить, что аугментация изображений может значительно улучшить точность классификации, однако в рамках исследования стояла задача изучить возможность классификаторов показывать удовлетворительные результаты в рамках низкого числа изображений на класс. Из-за специфичности данных, методам машинного обучения было недостаточно признаков для обучения, в связи с чем они недообучались и выдавали плохие прогнозы.

СПИСОК ЛИТЕРАТУРЫ

1. The elements of statistical learning: data mining, inference, and prediction / Hastie T. [et al.]. New York : Springer, 2009. T. 2. C. 1-758.
2. Cutler A., Cutler D. R., Stevens J. R. Random forests // Ensemble machine learning: Methods and applications. 2012. C. 157-175.
3. Murphy K. P. Machine learning: a probabilistic perspective. MIT press, 2012.
4. Müller A. C., Guido S. Introduction to machine learning with Python: a guide for data scientists. O'Reilly Media, Inc. 2016.
5. Вьюгин В. Математические основы теории машинного обучения и прогнозирования. МЦМНО, 2013. 390 с.
6. Kobayashi T., Hidaka A.i, Kurita T. Selection of Histograms of Oriented Gradients Features for Pedestrian Detection, 2007.
7. Dalal N., Triggs B. Histograms of Oriented Gradients for Human Detection, 2013.

УДК 004.053

АКТУАЛЬНЫЕ ВОПРОСЫ ПОДДЕРЖАНИЯ И СОПРОВОЖДЕНИЯ ЧИТАЕМОСТИ ИСХОДНОГО КОДА ПРОГРАММНЫХ ПРОЕКТОВ ВЫСОКОЙ СЛОЖНОСТИ

Поведайко Максим Дмитриевич, Алексеев Евгений Александрович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: mpovedaiko@yandex.ru, ea.alekseev.02@gmail.com

Аннотация. Рассматриваются методы и способы поддержания читаемости программного кода.

Ключевые слова: рефакторинг; антипаттерны; Brain Method и Data Class; Code Smells**.**

CURRENT ISSUES OF MAINTAINING AND MAINTAINING THE READABILITY OF THE SOURCE CODE OF SOFTWARE PROJECTS OF HIGH COMPLEXITY

Povedayko Maxim, Alekseyev Evgeny
Federal State Budget-Financed Educational Institution of Higher Education The Bonch-Bruevich
Saint-Petersburg State University of Telecommunications
22 Bolshevikov Av, letter 1, St. Petersburg, 193232, Russia
e- mails: mpovedaiko@yandex.ru, dimonqwerty368@gmail.com

Absrtact. The methods and methods of maintaining the readability of the program code are considered.

Keywords: refactoring; antipatterns; Brain Method и Data Class; Code Smells.

Введение. Большинство программистов, работающих над реальными большими проектами, всё чаще занимаются доработкой или оптимизацией уже ранее написанного кода. В настоящее время мало кто создает совершенно новые программы действительно с нуля. В результате этого можно утверждать, что поддержание читаемости исходного кода программного обеспечения — одна из важнейших задач в разработке программного обеспечения. Привлечение специалистов по рефакторингу на этапе производства программного кода приводит к значительному увеличению времени разработки, так как поиск антипаттернов и простое повышение читаемости кода путём его исправления требует большого количества усилий.

Одним из простейших путей к решению этой задачи является автоматизация поиска «проблемных» участков исходного кода. Американский программист, автор ряда книг и статей по архитектуре ПО Мартин Фаулер повторяющиеся признаки слабого проектирования и кодирования назвал Code Smells (запахи кода) [1]. Фаулер в своей книге утверждает, что антипаттерны являются неправильными или рискованными решениями существующих проблем.

Нашей задачей при рассмотрении нижеизложенного материала является определение факторов, приводящих к появлению Code Smells и антипаттернов, а затем поиск признаков, используя которые можно будет создать систему автоматического поиска антипаттернов.

Наиболее эффективно система будет искать антипаттерны, к которым можно применить некоторые методы базовых измерений. К ним относятся Brain Method и Data Class.Brain Method (Метод-Мозг) — это метод, который пытается централизировать функциональность класса, к которому он принадлежит. Обычно такой метод занимает много строк, имеет много условных ветвлений и глубокую вложенность.

Большой размер метода-мозга отрицательно влияет на степень читаемости кода и возможности его повторного использования, а длинные цепочки условных операторов и слишком глубокая вложенность требует большего внимания на этапе тестирования.

Data Class (Класс Данных) — это класс, который предоставляет только данные без какой-либо функциональности. Их уровень инкапсуляции низок, а функциональность недостаточна [1].

Для автоматического обнаружения могут использоваться измерения параметров исходного кода.

Для поиска Brain Method:

1.Цикломатическая сложность. Это показатель сложности исходного кода программы, который связан или коррелирует с вероятностью возникновения ошибок (багов) в программе. Показатель цикломатической сложности вычисляется через граф потока управления (Control flow graph, CFG), который отображает количество линейно-независимых путей выполнения в программе;

2.Число строк;

3.Число методов;

4.Максимальный уровень вложенности условных операторов;

5.Число переменных.

6.Для поиска Data Class:

7.Цикломатическая сложность.

8.Число методов доступа к полям класса (get/set).

9.Число переменных с модификатором доступа public.

10.Связи между классами объектов.

На основе приведенных выше методов базовых измерений можно создать нейронную сеть, определяющую антипаттерны на их основе.

Чтобы находить Brain Method, в первую очередь стоит ориентироваться на число строк в кандидатах, ведь чем больше в методе строк, тем сложнее он является. Еще один частый признак метода-мозга — огромное количество локальных переменных, чем их больше, тем более вероятно можно относить метод к антипаттерну. Также необходимо, чтобы сеть анализировала цикломатическую сложность, которую можно определить по количеству условных операторов в методе [2]. Последним признаком Brain-Method является высокий уровень вложенности условных операторов. Сравнив каждое из вычисленных значений с пороговыми, сеть помечает или не помечает метод как Brain-Method.

Для обнаружения Data Class надо понимать, что такой класс ориентирован исключительно на хранение данных. Сначала сеть посчитает количество методов доступа к полям, число публичных переменных, цикломатическую сложность. Но в этом случае последняя ожидаемо будет ниже, так как Data Class дает минимальную функциональность. Затем отслеживается количество связей с другими классами. Все результаты снова сравниваются с пороговыми, и сеть выносит решение.

В своей работе для 15-ой Международной конференции по исследованиям, управлению и применению программной инженерии (SERA) Севилай Велиоглу и Юнус Эмре Сельчук [3] сравнивают два похожих инструмента автоматического анализа кода: IPlasma [4] и Essere (Essere Code Smell Detector).

Ниже в таблице 1 приведены результаты сравнений, проводимых на основе тестов, в которых использовался код, оцененный реальными специалистами частной IT-компании.

Таблица 1

Сравнение эффективности обнаружения антипаттернов Brain Method и Data Class

Антипаттерн	IPlasma	Essere
Brain Method	72,7% (8/11)	Не поддерживается
Data Class	66,7% (12/18)	33,3% (6/18)

Essere, являясь коммерческим продуктом, к сожалению, не поддерживает обнаружение такого популярного антипаттерна, как Brain Method, и при этом не показывает впечатляющих результатов при обнаружении Data Class.

IPlasma же показывает более обнадеживающие результаты, но при этом работает лишь с C++ и Java, но недостаточно хорошо работает на таком языке, как C#, и совсем неудовлетворительно на Pyton. К тому же IPlasma является некоммерческим проектом, в результате чего его основным недостатком является быстрая потеря актуальности вследствие недостаточной поддержки разработчиком.

Заключение. Таким образом, можно сделать следующее утверждение: так как обнаружение известных антипаттернов в коде является задачей распознавания образов, то для создания программы обнаружения известных антипаттернов стоит использовать методы обучения с учителем. К этой категории обучающих алгоритмов принадлежит многослойный персептрон (MLP), традиционная модель нейронной сети с прямой связью. Её работа заключается в следующем: на входной слой сеть получает вышеуказанные метрические параметры, на выходном слое выводится значение целевой переменной. Значением целевой переменной будет вид обнаруженного антипаттерна. Количество скрытых слоев MLP и их размер для оптимальной точности предсказания будут определяться эмпирически и станут зависеть во многом от числа входных параметров. Как правило, для сложных задач рекомендуется иметь как минимум два скрытых слоя [5], при этом не следует создавать их чрезмерное количество, необходимо ограничиться рабочей архитектурой с минимумом скрытых слоев.

СПИСОК ЛИТЕРАТУРЫ

1. Фаулер М. Рефакторинг. Улучшение существующего кода. СПб. : Символ-Плюс, 2003. 432 с.
2. McCabe T. J. A Complexity Measure // IEEE Transactions on Software Engineering: journal. 1976. Pp. 308-320.
3. Velioğlu S., Emre Selçuk Y. An automated code smell and anti-pattern detection approach // IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA). 2017.
4. Marinescu C., Marinescu R., Mihancea P. F., Ratiu D., Wettel R. iPlasma: An Integrated Platform for Quality Assessment of Object-Oriented Design // LOOSE Research Group «Politehnica» University of Timisoara Romania. [Электронный ресурс]. URL: https://wettel.github.io/download/iPlasma-tooldemo.pdf (дата обращения: 01.09.2023).
5. Lippmann R. P. An Introduction' to Computing with Neural Nets // IEEE ASSP Magazine. [Электронный ресурс]. URL: https://www2.cs.sfu.ca/CourseCentral/414/li/material/refs/Lippmann-ASSP-87.pdf (дата обращения: 01.09.2023).

УДК 004.056.52

АКТУАЛЬНЫЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ НЕЙРОННЫХ СЕТЕЙ В СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Поведайко Максим Дмитриевич, Карташев Валерий Игоревич, Самсонов Дмитрий Эдуардович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: mpovedaiko@yandex.ru, vlrkrtshv@yandex.ru, dimonqwerty368@gmail.com

Аннотация. Рассматриваются особенности применения нейронных сетей для совершения мошеннических действий.

Ключевые слова: нейронные сети; защита; доступ к информации; противодействие краже информации в информационных системах; социальная инженерия.

CURRENT ISSUES THE USE OF NEURAL NETWORKS IN SOCIAL ENGINEERING

Povedayko Maxim, Kartashev Valery, Samsonov Dmitry
Federal State Budget-Financed Educational Institution of Higher Education The Bonch-Bruevich
Saint-Petersburg State University of Telecommunications
22 Bolshevikov Av, letter 1, St. Petersburg, 193232, Russia
e- mails: mpovedaiko@yandex.ru [1], vlrkrtshv@yandex.ru [2], dimonqwerty368@gmail.com

Absrtact. The features of the use of neural networks for committing fraudulent actions are considered**.**

Keywords: neural networks; protection; access to information; countering information theft in information systems; social engineering.

Введение. В последние годы наблюдается интенсивное развитие нейронных сетей. Нейронные сети начали массово применяться для анализа существующей информации, поиска закономерностей и составления прогноза будущей информации. Благодаря огромному массиву данных, накопленному в сети, нейронные сети могут быть также использованы в рамках социальной инженерии.

Понятие нейронной сети раскрывать не станем, но необходимо упомянуть о её компонентах.

Основные компоненты нейронной сети включают в себя:

1)нейроны;

2)веса;

3)функции активации;

4)слои.

Обучение нейронной сети происходит путем настройки весов и параметров таким образом, чтобы сеть могла выполнять конкретную задачу, например, классификацию изображений или прогнозирование временных рядов. Нейронные сети широко применяются в современных технологиях и являются ключевым компонентом многих систем машинного обучения и искусственного интеллекта.

Нейронные сети уже задействованы в процессе генерации речи, этот процесс обычно осуществляется в несколько этапов:

1.Подготовка аудиоданных. Аудиоданные (например, текстовая информация, которую нужно озвучить) обрабатываются и предварительно анализируются. Это может включать в себя преобразование текста в фонемы (минимальные звуковые единицы), извлечение мел-частотных кепстральных коэффициентов (MFCC) или другие методы представления аудиоинформации.

2.Синтез речи на основе предварительно подготовленных данных. Существует несколько методов синтеза речи с использованием нейронных сетей. Одним из наиболее популярных методов является генерация речи с помощью глубоких рекуррентных нейронных сетей (RNN) или трансформеров. В таких сетях модель получает на вход текстовое описание и генерирует соответствующую аудиозапись речи.

Необходимо сказать, что процесс обучения такой нейронной сети часто требует больших объемов данных, включая текст и соответствующие аудиозаписи. Нейронная сеть обучается выявлять связи между текстом и звуком, чтобы создавать натурально звучащую речь.

Важно отметить, что современные системы синтеза речи обычно используют глубокое обучение и многослойные нейронные сети для достижения высокого качества синтеза голоса. Глубокие нейронные сети позволяют модели учиться на основе большого объема данных и улучшать качество сгенерированной речи по мере обучения.

В настоящее время утверждается, что генеративные нейронные сети используют интеллектуальную собственность художников для генерации изображений. Это не совсем так, так как нейронные сети не используют повторно и не хранят изображения, на которых они обучались, а генерируют новые на основе весов и связей, полученных в результате обучения. Изображения генерируются обезличенно и не могут быть связаны с определенным человеком (художником) [1].

С другой стороны, можно утверждать, что генерация голоса чаще всего носит персональный характер. В большинстве генераторов, которые доступны сейчас, есть генерации по известным личностям, таким как актёры, персонажи фильмов и игр, озвученные актерами дубляжа. Такие голоса персонализированы и могут быть отождествлены с определенным человеком. Для генерации голоса необходимо определённое количество записанных аудио с разметкой текста, чтобы на основе этих записей можно было обучить нейронную сеть для последующей генерации голосового сообщения из текста.

Такие аудио могут быть получены разными способами, рассматривать их не станем.

Со слов создателей таких нейросетей известно, что для генерации голоса достаточно несколько десятков минут записанного аудио, которого достаточно имеется в открытых источниках [2].

Аудиосообщения, сгенерированные на основе голосовой модели, которая была обучена на данных одного человека, будут похожи по звучанию на самого человека, а при наличии достаточного количества чистого материала практически неотличимы на слух от реального человека.

Примером может послужить ситуация, с которой столкнулась Алёна Сергеевна Андронова. Она является актёром дубляжа. В её случае был записан многочасовой объём текста для внутреннего использования. Затем на основе данных записей была составлена модель и позже была предоставлена возможность генерировать аудио по любому тексту. Среди нескольких примеров использования есть озвучивание рекламных роликов, в том числе для приложений с контентом для взрослых. О данных рекламных материалах стало известно от знакомых Алёны, которые спрашивали у неё, занималась ли она озвучиванием материалов для данных проектов [3].

Было установлено, что люди, знакомые с указанным человеком лично, не смогли отличить специально записанные и сгенерированные нейросетью записи голоса. Можно предположить, что, если родственникам

Алёны позвонит злоумышленник и голосом, сгенерированным нейросетью, будет просить о материальной помощи, то, скорее всего, она будет получена.

Подобный способ мошенничества пока без использования нейросетей уже практикуется довольно давно. Но, если к этому подключить обученную нейронную модель на подобие ChatGPT, которая будет генерировать текст, и голосовую модель, обученную на определённом человеке, на практике, вне всяких сомнений, действительно получится максимально эмоционально надавить на родственника этого человека для получения любого типа выгоды. Аналогичным образом, но скорее с возрастающей частотой будут идти дела в финансовой сфере, предприятиях и организациях или в сфере услуг. Количество обманутых людей может значительно возрасти, так как многие могут не предполагать, что на другом конце телефона может быть не человек со знакомым голосом, а нейросеть, что лишь притворяется им.

Нейронные сети уже способны заменить человека «в разговоре», а Российское законодательство не поспевает. Да, есть законы, которые устанавливают порядок работы с биометрическими данными человека, такие как Федеральный закон «Об информации, информационных технологиях и о защите информации», Федеральный закон «О персональных данных», Указы Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» и «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», а также другие.

Однако можно утверждать, что разработанные законы и акты необходимо пересматривать. К примеру, используя технологии Deep Fake, возможна подмена с использованием глубокого обучения. Можно заменять лицо в видеороликах, при этом без или с минимальной коррекцией человеком.

Примером может послужить замена лица солиста группы «Земляне» Сергея Скачкова в клипе песни «Трава у дома» на лицо предпринимателя Илона Маска.

Сопоставив всё воедино, допустим, что можно применять комплексно: группы нейронных сетей, состоящих из перевода речи в текст, генерации ответа на сообщение, перевода текста в речь и замены лица. В таком случае появляется достаточно мощный инструмент обмана в режиме реального времени.

Таким образом, в результате сказанного можно утверждать, что нейронные сети не только ворвались с прекрасными возможностями для автоматизации огромного количества процессов, которые раньше было сложно или невозможно автоматизировать, но они способны создать огромную опасность в случае применения их в сфере мошенничества.

Заключение. Для нивелирования возможности мошенничества в этой сфере предлагается:

1.Своевременно создавать и постоянно модернизировать инструменты, которые помогли бы определять сгенерированную или измененную информацию, в том числе в реальном времени, так как развитие нейронных сетей продолжается, и результаты их работы всё труднее отличить неподготовленному пользователю от реальности.

2.Заблаговременно продумать и провести консультации со специалистами, работающими в данной области для внесения поправок и изменений в существующие законы, распоряжения и законодательные акты для предотвращения противоправных действий со стороны мошеннических лиц и организаций.

СПИСОК ЛИТЕРАТУРЫ

1. Меня зовут Алена Андронова и этот голос является синтезом речи [Электронный ресурс]. URL: https://youtu.be/xfhPMKpPQng?si=Dusu_ggDYZUrtUad (дата обращения: 02.09.2023).
2. Как ваш голос может стать не вашим? Говорим с пострадавшими и разработчиками нейросетей [Электронный ресурс]. URL: https://youtu.be/rHeYWhaCAIA?si=v-f2w2syENjJGoAT (дата обращения: 02.09.2023).
3. Алена Андронова — Синтез Голоса и Право [Электронный ресурс]. URL: https://www.youtube.com/watch?v=_eX6_naRei8 (дата обращения: 02.09.2023).

УДК 004.056.52

ПОВЫШЕНИЕ УРОВНЯ БЕЗОПАСНОСТИ ПОСРЕДСТВОМ ПРИМЕНЕНИЯ РАДИОЧАСТОТНОЙ ИДЕНТИФИКАЦИИ

Поведайко Максим Дмитриевич, Карташев Валерий Игоревич, Самсонов Дмитрий Эдуардович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: mpovedaiko@yandex.ru, vlrkrtshv@yandex.ru, dimonqwerty368@gmail.com

Аннотация. Рассматриваются методы и способы технической защиты документов.

Ключевые слова: защита; доступ к информации; противодействие краже информации в информационных системах.

INCREASING THE LEVEL OF SECURITY THROUGH THE USE OF RADIO FREQUENCY IDENTIFICATION

Povedayko Maxim, Kartashev Valery, Samsonov Dmitry
Federal State Budget-Financed Educational Institution of Higher Education The Bonch-Bruevich Saint-Petersburg State University of Telecommunications
22 Bolshevikov Av, 1 letter, St. Petersburg, 193232, Russia
e- mail: mpovedaiko@yandex.ru, vlrkrtshv@yandex.ru, dimonqwerty368@gmail.com

Absrtact. Methods and methods of technical protection of documents are considered**.**

Keywords: protection; access to information; countering information theft in information systems.

Ведение. Удостоверения личности различного рода играют ключевую роль в идентификации гражданина. С ростом технологических возможностей и повышением требований безопасности к такого рода документам радиочастотная идентификация (RFID) стала надежным инструментом для установления подлинности документа. Рассмотрим, как технология RFID способна идентифицировать поддельные удостоверения личности, обеспечивая высокую степень безопасности и конфиденциальности легальных документов.

RFID (радиочастотная идентификация) — это беспроводная связь для идентификации объектов или людей. RFID позволяет осуществлять идентификацию на расстоянии, то есть для считывания нет необходимости в том, чтобы передатчик находился в зоне прямой видимости считывателя. Система RFID включает в себя RFID-чип, RFID-считыватель, внутреннюю базу данных и блок управления [4].

В системах RFID предметы помечаются при помощи чипов, содержащих транспондеры, которые передают сообщения, считываемые специализированными RFID-считывателями. Считыватель извлекает из базы данных информацию об идентификационном номере, после чего использует ее для дальнейших действий. Кроме того, RFID-чипы могут быть оборудованы записываемой памятью, в которой хранится информация, предназначенная для передачи различным RFID-считывателям в разных местах. Это позволяет редактировать информацию, хранящуюся на RFID-чипах [1].

RFID-чипы принято разделять на две основные категории: активные и пассивные. Считыватели RFID также могут быть активными и пассивными в зависимости от типа применяемого чипа. Кроме того, чипы и считыватели разделяют на низкочастотные, высокочастотные, сверхвысокочастотные и ультравысокочастотные [2].

Внедрение технологии радиочастотной идентификации, которое продвигается в нашей стране, в области удостоверений личности имеет широкий спектр практических применений и преимуществ.

Внедрение радиочастотных чипов в государственные паспорта не является инновационным решением для идентификации граждан. Такие чипы могут содержать различные данные о владельце паспорта, такие как фотография, имя, фамилия, дата рождения и идентификационный номер.

Электронные чипы встраиваются в э-документ и могут быть считаны только при помощи авторизованных RFID-считывателей, что значительно повышает уровень безопасности, так как подделка данного документа становится крайне сложной задачей. Конечно, всегда существует возможность воровства, однако такие устройства достаточно легко заблокировать. В случае физического повреждения документа встроенный чип также может остаться работоспособным, т.к. современная электроника способна противостоять не только атмосферным явлениям, но и механическим повреждениям.

В случае заграничных паспортов применение RFID-технологии также предоставляет значительные преимущества. Помимо фотографии, имени, фамилии, даты рождения и идентификационного номера чипы в заграничных паспортах могут содержать биометрические сведения, такие как отпечатки пальцев или сканирование сетчатки глаза своего владельца, что делает их еще более защищенными от подделок и мошенничества. Помимо этого, данные паспорта позволяют пограничным контрольным пунктам быстро и точно проверить личность владельца при пересечении границы.

Использование RFID-технологии в медицинских полисах позволяет управлять медицинскими записями и обеспечивает доступ к медицинской информации, такой как группа крови, масса тела или наличие аллергии на медицинские препараты, что может уменьшить время и улучшить качество медицинской помощи, особенно в случаях, когда пациенту требуется экстренное медицинское вмешательство [3].

Водительские удостоверения с RFID-чипами помогают повысить безопасность на дорогах и улучшить эффективность правоохранительных органов. Электронные чипы могут содержать информацию о водителе, его водительском удостоверении и истории нарушений, медицинских показателях, о которых необходимо знать или учитывать при оказании первой медицинской помощи. Это позволяет полиции быстро и точно проверить легальность вождения и выявить нарушения, такие как вождение без водительских удостоверений или участие в дорожных происшествиях в случае розыска.

Применение RFID в удостоверениях личности открывает дверь для инноваций и улучшения процессов идентификации и безопасности в различных сферах жизни.

При использовании RFID в удостоверениях личности риск кражи персональных данных всё же остаётся. Злоумышленники могут перехватывать радиочастотные сигналы, передаваемые между чипом и считывателем, что позволит им получить доступ к личной информации владельца. Этот факт затрагивает актуальный вопрос о защите персональных данных и обеспечении конфиденциальности.

Для предотвращения воровства данных в подобных удостоверениях личности за рубежом применяются различные методы защиты и мониторинга, что необходимо внедрить и отечественным специалистам [5]:

1.Шифрование данных. Позволяет защитить данные на RFID-чипах от несанкционированного доступа. Перед отправкой данных с чипа на считыватель они шифруются, чтобы получить доступ к данным смог только авторизованный считыватель, обладающий ключом доступа.

2.Аутентификация. Требуется, чтобы чип и считыватель обменивались ключами или паролями для подтверждения их легитимности. Таким образом, только считыватель, который знает правильный ключ, сможет взаимодействовать с чипом и получить доступ к данным.

3.Защита чипов на физическом уровне. Подразумевается использование специальных оболочек (обложек для документа), которые мешают несанкционированному доступу к чипу.

4.Мониторинг и анализ активности. Когда система документирует параметры всех обращений к чипу, в результате чего отслеживать попытки несанкционированного доступа станет намного проще.

5.Регулярное обновление и смена ключей доступа. Позволят предупредить попытку взлома и лишить злоумышленника возможности получить доступ к персональным данным.

6.Идентификационный номер должен быть уникален и связан с конкретным владельцем. Подделка уникального идентификационного номера является крайне сложной задачей, так как для этого злоумышленникам необходимо получить доступ к специализированным программаторам.

7.Защита от копирования и клонирования чипов. Создание дубликатов документов должно контролироваться исключительно государством.

8.Биометрические данные личности должны выступать дополнительным слоями защиты и обеспечивать гарантированное подтверждение личности.

9.Использование специальных считывателей. Доступ к данным должен иметь уполномоченный персонал и органы правопорядка, что также позволит своевременно выявлять поддельные документы.

Таким образом, в рассмотренном материале был поднят актуальный вопрос внедрения радиочастотной идентификации личности.

Внедрение данной технологии обоснованно не только для облегчения работы силовых структур государства в процессе поиска и идентификации разыскиваемых лиц, оно также снизит административную нагрузку при опознании человека сотрудниками других структур государства, таких как банковские работники.

Кроме того, использование технологии RFID поспособствует значительному сокращению бумажной документации, поскольку большой объём данных будет дополнительно храниться в электронном формате на RFID-чипе, что позволит уменьшить издержки на печать и оптимизировать хранилища бумажной документации.

Заключение. В результате вышесказанного можно утверждать, что 100 % интеграция радиочастотной идентификации в удостоверения личности (паспорта, водительские удостоверения, медицинские книжки) не только окажет положительное воздействие на безопасность, но и позволит оптимизировать административные процессы, а также усложнит работу злоумышленникам, специализирующимся на краже конфиденциальной информации.

СПИСОК ЛИТЕРАТУРЫ

1. Таненбаум Э., Уэзеролл Д. Компьютерные сети : 5-е изд. СПб. : Питер, 2022. 960 с.
2. Финкенцеллер К. RFID-технологии : справочное пособие. М. : Додека XXI век, 2016. 490 с.
3. Bhite T. RFID Based E-Passport System // Journal of Emerging Technologies and Innovative Research. 2019. № 6. С. 324-325.
4. RFID РАДИОЧАСТОТНАЯ ИДЕНТИФИКАЦИЯ [Электронный ресурс] // ДатаКрат. URL: https://www.datakrat.ru/technology/rfid-radiochastotnaya-identifikatsiya (дата обращения: 2.09.2023).
5. Черепков С. Технология RFID. Опыт использования и перспективные направления // Компоненты и технологии. 2005. № 9. С. 154-157.

УДК 004.7

АРХИТЕКТУРА ИНФОРМАЦИОННЫХ СИСТЕМ ПРОГНОЗА БИРЖЕВЫХ КОТИРОВОК

Птицын Никита Алексеевич, Птицына Лариса Константиновна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Мойки р. наб, 61, Санкт-Петербург, 191186, Россия
e-mails: nikita_pti@inbox.ru, ptitsina_lk@inbox.ru

Аннотация: Актуализирован процесс разработки интеллектуальных информационных систем для прогноза биржевых котировок. Описаны основные понятия деятельности по анализу биржевых котировок. Выделены технологические основания для предлагаемой разработки. Изложена концепция формирования архитектуры интеллектуальной информационной системы для прогноза биржевых котировок. Определен состав

математического обеспечения интеллектуальной информационной системы для прогноза биржевых котировок. Представлены модели и методы обработки моделей структурированной и слабоструктурированной информации о поведении биржевых котировок. Приведен перечень моделей описания поведения биржевых котировок. Раскрыт технологический базис для разработки программных средств прогнозирования биржевых котировок. Проанализированы результаты экспериментального оценивания точности прогнозирования цены облигаций. Описана научная и практическая значимость полученных результатов исследования.

Ключевые слова: информация; информационная система; архитектура; котировки; прогноз; модели; методы; машинное обучение; программные средства.

ARCHITECTURE OF INFORMATION SYSTEMS FOR FORECASTING EXCHANGE QUOTATIONS

Ptitsyn Nikita, Ptitsyna Larisa
Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich
61 Moika River Emb, St. Petersburg, 191186, Russia
e-mails: nikita_pti@inbox.ru, ptitsina_lk@inbox.ru

Abstract: The process of developing intelligent information systems for forecasting stock quotes has been updated. The basic concepts of activity on the analysis of exchange quotations are described. Technological grounds for the proposed development are highlighted. The concept of forming the architecture of an intelligent information system for forecasting stock quotes is presented. The composition of the software for the intellectual information system for forecasting stock quotes has been determined. Models and methods for processing models of structured and semi-structured information about the behavior of exchange quotations are presented. A list of models for describing the behavior of stock quotes is given. The technological basis for the development of software tools for forecasting stock quotes is disclosed. The results of experimental evaluation of the accuracy of bond price forecasting are analyzed. The scientific and practical significance of the obtained research results is described.

Keywords: information; information system; architecture; quotes; forecast; models; methods; machine learning; software.

В современном мире наблюдается повышение значимости рыночных отношений в условиях интенсивного развития цифровой экономики.

В контексте различного целеполагания проявляется востребованность анализа поведения показателей биржевых котировок. Выявленная востребованность подтверждается разнообразием контента проводимых исследований по автоматизации прогноза [1-7].

Благодаря современным достижениям в теории и практике применения интеллектуальных информационных технологий создаются благоприятные условия для актуализации различных подходов к формированию архитектуры информационных систем для прогноза биржевых котировок.

Многообразие подходов обеспечивается обширностью результатов теоретических исследований в области искусственного интеллекта и расширенностью возможностей моделирования высокотехнологичных информационных инфраструктур.

В представляемом исследовании проводится анализ современных направлений развития методов и средств для прогноза биржевых котировок. Вслед за этим анализом предлагается концепция формирования архитектуры информационной системы для прогноза биржевых котировок.

При разработке концепции архитектуры информационной системы предусматривается её предназначение для трейдеров, инвесторов, банкиров, бизнесменов, брокеров, специалистов по подбору кредитов, системных аналитиков, экспертов, занимающихся трейдингом финансовых рынков.

Биржевая котировка представляется как цена актива, которая используется в торгах актива на бирже по определенным правилам. При этом считается, что котировка может соответствовать любому активу, торгующемуся на биржах. Среди биржевых котировок различаются прямые и обратные котировки.

Формирование архитектуры информационной системы для прогноза биржевых котировок осуществляется в ориентации на интеллектуальные сервис-ориентированные системы, реализуемые с помощью многокомпонентного программного обеспечения.

Предлагаемая концепция раскрывается в формате описания концептуальных моделей. В концепции выделяются две группы принципов. Первая группа принципов рассматривается как опорная. Вторая группа принципов относится к альтернативным подходам к интеллектуализации архитектуры информационной системы для прогноза биржевых котировок.

При формировании архитектуры информационной системы для прогноза биржевых котировок систематизированы:

– методы прогнозирования, основанные на обработке структурированной информации о поведении биржевых котировок.

– методы прогнозирования, ориентированные на обработку представлений слабоструктурированной информации о поведении биржевых котировок.

По результатам проведенного анализа методов и средств прогноза биржевых котировок образуется опорный базис математического обеспечения интеллектуальных информационных систем трейдинга.

В опорный базис математического обеспечения вводятся методы алгоритмического анализа данных, методы анализа данных, использующих машинное обучение, и методы обнаружения изменений в поведении биржевых котировок. Для каждой категории методов выстраивается соответствующая система моделей описания данных и система описания информации, а также система условий, допускающих их использование.

В опорный базис вводятся следующие модели поведения биржевых котировок:

– авторегрессионная модель (AR);
– модель скользящего среднего (MA);
– модель ARMA (авторегрессия-скользящее среднее);
– модель ARIMA (авторегрессия-интегрирование-скользящее среднее);
– модель SARIMA (сезонная ARIMA);
– модель SARIMAX (сезонная ARIMA с регрессорами);
– модели ARCH (авторегрессионная гетероскедастичности);
– VAR-модели (VAR);
– SVR-модель;
– модель деревьев решений;
– модель случайный лес;
– нейросетевая модель MLP;
– инновационная модель описания поведения биржевых котировок.

Инновационная модель описания поведения биржевых котировок построена на основе интеграции современных методов машинного обучения (LSTM, MLP, SVR). При разработке инновационной модели описания поведения биржевых котировок взяты за основу следующие принципы:

– увеличение количества признаков обучения за счет технических показателей, вычисляемых из базовых значений котировки;

– использование метода скользящего окна для увеличения связности данных и увеличения количества признаков;

– удаление невалидных данных во время обучения;
– преобразование прогнозируемого признака к стационарному виду;
– нормализация данных.

При разработке и исследовании программ оценивания и прогноза биржевых котировок использовалась среда Google Colaboratory и следующие средства:

– язык программирования Python;
– открытая программная библиотека для машинного обучения TensorFlow;
– библиотека Scikit-learn на языке Python для машинного обучения;
– библиотека NumPy на языке Python для поддержки многомерных массивов и данных;
– библиотека Pandas на языке Python для обработки и анализа данных;
– приложение Yfinance для отслеживания рынков и экономики;
– общие финансовые технические индикаторы FinTA;

– библиотека Matplotlib на языке программирования Python для визуализации данных двумерной и трёхмерной графикой.

В исследованиях в качестве исходной информации применялась базовая информация о котировке за задаваемый промежуток времени: цена открытия, закрытия, наибольшее и наименьшее значение, объем торгов.

Обрабатываемые данные извлекались из информационных ресурсов бирж с помощью провайдера финансовой информации Yahoo Finance.

Проведенные эксперименты по исследованию качества прогноза биржевых котировок проводились применительно к цене облигаций компании Google при описании ее поведения выше приведенными моделями.

В качестве характеристики качества прогнозирования задействовано оцениваемое во время экспериментов RMSE среднеквадратическое отклонение ошибки оценивания. В исследованиях разработанных программ выполнен сравнительный анализ точности прогнозирования облигаций компании Google.Для выявления эффективности применения различных моделей поведения цены облигаций сравнивались RMSE среднеквадратичные ошибки между прогнозируемыми и истинными данными.

Полученные результаты экспериментов приведены на рис. 1.

Название модели	RMSE (Среднеквадратичное отклонение прогнозов от истины)
ES	3.14092
AR	3.10032
MA	2.26325
ARMA	3.09127
ARIMA	2.29551
SARIMAX	3.20979
SVM (SVR)	2.47113
Дерево решений	2.18947
Случайный лес	1.75328
MLP	2.30737
Итоговая модель	0.55926

Рис. 1. Результаты оценивания ошибки прогноза

Сравнение экспериментальных результатов показывает, что точность прогнозирования цены облигаций Google с помощью разработанной инновационной модели описания её поведения повышается в 3.13 раза.

Научная новизна представляемых результатов исследований заключается:

– в разработке концепции архитектуры интеллектуальных информационных систем для прогноза биржевых котировок;

– в содержании опорного базиса математического обеспечения информационных систем для прогноза биржевых котировок;

– в сквозном связывании моделей, методов оценивания и прогноза биржевых котировок и моделей, методов обнаружения изменений в их поведении;

– в функциональных спецификациях разработанных программных средств прогноза биржевых котировок с применением моделей и методов машинного обучения;

– в расширении знаний о сравнительном качестве прогноза биржевых котировок с применением методов и средств интеллектуальных информационных технологий.

– Практическая значимость предопределяется:

– открытостью архитектуры интеллектуальных информационных систем для прогноза биржевых котировок, позволяющей непрерывно расширять их функциональные возможности;

– предоставлением возможности оценивания и сравнения качества прогноза биржевых котировок при использовании альтернативных моделей, методов и средств прогноза биржевых котировок;

– повышением степени комплексности и автоматизации трейдинга финансовых рынков;

– повышением качества прогноза биржевых котировок.

СПИСОК ЛИТЕРАТУРЫ

1. Птицына Л. К., Птицын Н. А. Расширение знаний о раннем обнаружении появляющихся изменений // Наука. Информатизация. Технологии. Образование. Материалы XIII международной научно-практичю конф. «Новые информационные технологии в образовании и науке НИТО 2020» 24–28 февраля 2020 г. Екатеринбург. Екатеринбург : ФГАОУ ВО «Российский государственный профессионально-педагогический университет», 2020. С. 248-252.
2. Нильсен Э. Практический анализ временных рядов : прогнозирование со статистикой и машинное обучение : перевод с английского . М. ; СПб. : Диалектика, 2021. 538 с.
3. Птицын Н. А. Птицына Л. К. Автоматическое отслеживание изменений показателей профессиональной деятельности // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2022). СПб.: СПбГУТ, 2023. С. 343-347.
4. Введение в анализ временных рядов : учеб. пособие для вузов / Н. В. Артамонов [и др.]. Вологда : ВолНЦ РАН, 2021. 134 с.
5. Прогнозирование котировок фьючерсов на индекс РТС на основе машинного обучения / Н. В. Воинов [и др.] // Материалы международной конференции по мягким вычислениям и измерениям. 2021. Т. 1. С. 271–274.
6. Дорошенко С. Н., Прийма К. А., Ляшенко А. Я. Анализ рынка акций на примере российских горнодобывающих компаний // Актуальные проблемы экономики и управления. 2022. № 1 (33). С. 3-7.
7. Французенко П. С. Исследование изменений индекса Мосбиржи в зависимости от количества зарегистрированных пользователей // Вестник Академии знаний. 2022. № 48 (1). С. 461-466.

УДК 004.045

ПРОТОТИП МИКРОПРИЛОЖЕНИЯ ХРАНЕНИЯ И ОБРАБОТКИ ИНФОРМАЦИИ О НАУЧНЫХ ПУБЛИКАЦИЯХ

Уласик Вероника Валерьевна, Восьмаков Дмитрий Иванович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича,
Большевиков пр., 22, корп. 1, Санкт-Петербург, Россия, 193232
e-mails: nika.ulasik@gmail.com, vosmakovd@mail.ru

Аннотация. Предложена концепция микроприложения, автоматизирующего процесс концентрации информации о публикациях отдельных авторов, авторских коллективов, структурных подразделений и организаций. Рассмотрены принципы функционирования программного решения, предложен вариант реализации системы на основе распределённой архитектуры.

Ключевые слова: микроприложение; распределенная система; интероперабельность; наукометрия.

PROTOTYPE OF MICROAPPLICATION FOR STORAGE AND PROCESSING OF INFORMATION ON SCIENTIFIC PUBLICATIONS

Ulasik Veronica, Vosmakov Dmitry
Federal State Budget-Financed Educational Institution of Higher Education
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: nika.ulasik@gmail.com, vosmakovd@mail.ru

Abstract. A concept of a microapplication is proposed to automate the process of gathering information about publications from individual authors, author groups, structural units, and organizations. The principles of the software solution's functioning are examined, and an implementation option of the system based on a distributed architecture is proposed.

Keywords: microapplication; distributed system; interoperability; scientometrics.

В настоящее время остро стоит проблема автоматизации работы с документами, создания отчётов, хранения больших массивов данных. Так, в образовательных и научных учреждениях Российской Федерации работа по формированию отчётной документации о результатах научной деятельности отдельных авторов, структурных подразделений и организаций выполняется вручную с минимальной степенью автоматизации. Данный процесс является рутинным и отнимает существенную часть рабочего времени у научно-педагогических работников, а также сотрудников, отвечающих за формирование отчетов.

Эта проблема может быть решена путём создания интероперабельных информационных систем, допускающих глубокую интеграцию в единую киберфизическую среду постиндустриального общества. Как и любая составляющая киберфизической среды, микроприложение хранения и обработки информации должно строится на трех базовых принципах: агентности, информационного самообслуживания и управляемой информационной открытости [1]. Интероперабельность подразумевает сквозное информационное взаимодействие и функциональную совместимость систем вне зависимости от их внутреннего устройства.

Целью создания микроприложения является сокращение времени на формирование отчетов о публикационной активности, а также на включение информации в портфолио за счет реализации одного из базовых принципов информационных технологий — DRY (don't repeat yourself — «не повторяйся») [2]. При этом каждый участник (физическое или юридическое лицо), представленный в системе агентом, имеет возможность распоряжаться информацией в рамках указанной лицензии (управляемая информационная открытость).

Исходя из перечисленных выше базовых принципов построения системы разработан следующий вариант реализации программного решения. Система функционирует по принципам, схожими с принципами, на основе которых построены распределённые системы управления версиями [3]: у каждого из пользователей имеется своя реплика информации о публикациях; синхронизация между несколькими экземплярами программы выполняется путём импорта или экспорта информации о публикациях в другие системы. По умолчанию пользователь работает с локальным набором данных в своей системе. В этом заключается научная новизна решения.

Микроприложение должно обеспечить добавление, редактирование и удаление информации о научных публикациях, а также экспорт информацию в формате, удобном для обмена между несколькими развёрнутыми копиями системы. Микроприложение должно иметь функционал по фильтрации и отображению списка библиографических источников, вывод подробной информации о каждом источнике и копирование библиографического описания в рекомендованном формате для вставки в список цитирования.

Прототип микроприложения хранения и обработки информации о научных публикациях состоит из микросервиса ASP.NET Core и микрофронтенда, реализованного на Blazor. В роли объектно-реляционного преобразователя выступил Entity Framework Core. В рамках студенческой научно-исследовательской работы

предполагается на базе данного прототипа создать интероперабельное микроприложение, которое может быть интегрировано в любые киберсреды, построенные на базе принципов агентности, информационного самообслуживания и управляемой информационной открытости.

В дальнейшем на основе данных принципов и на базе отработанной технологии планируется создать семейство программных продуктов для учета личных достижений и результатов научно-исследовательской деятельности, включая участие в конкурсах, прохождения курсов повышения квалификации и стажировок, свидетельств о государственной регистрации.

СПИСОК ЛИТЕРАТУРЫ

1. Верхова Г. В., Акимов С. В. Интеграция локальных интероперабельных киберсред виртуальных организаций в единую киберсреду постиндустриального общества // Волновая электроника и инфокоммуникационные системы. СПб., 2021. С. 34-39.
2. Haoyu W., Haili Z. Basic Design Principles in Software Engineering // Fourth International Conference on Computational and Information Sciences, Chongqing, China. 2012. Pp. 1251-1254.
3. Москалева Ю. П., Сейдаметова З. С. Централизованные и распределенные системы управления версиями как учебная платформа // Информационно-компьютерные технологии в экономике, образовании и социальной сфере. 2017. № 3 (17). С. 112-116.
4. Эванс Э. Предметно-ориентированное проектирование (DDD): структуризация сложных программных систем / пер. с англ. М.: И. Д. Вильямс, 2011. 448 с.

ОГЛАВЛЕНИЕ

CONTENTS