САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
РЕГИОНАЛЬНАЯ ИНФОРМАТИКА

Сборник трудов

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Выпуск 10

Санкт-Петербург
2021

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
РЕГИОНАЛЬНАЯ ИНФОРМАТИКА

Сборник трудов

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Выпуск 10

Санкт-Петербург
2021

УДК (002:681):338.98

Р32

Региональная информатика и информационная безопасность.
Р32 Сборник трудов. Выпуск 10 / СПОИСУ. – СПб., 2021. – 406 с.
ISBN 978-5-001820-20-8

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; Телекоммуникационные сети и технологии; Информационная безопасность; Информационно-психологические и правовые аспекты информационной безопасности; Информационные технологии в экономике; Информационные технологии на транспорте; Информационные технологии в образовании; Информационные технологии управления объектами морской техники и морской инфраструктуры; Информационные технологии в социокомпьютинге; Информационные технологии в критических инфраструктурах; Безопасные интеллектуальные информационные системы и технологии (молодежная научная школа).

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*

ISBN 978-5-00182-020-8

Публикуется в авторской редакции

Подписано в печать 15.11.2021. Формат 60x84⅛. Бумага офсетная.
Печать – ризография. Усл. печ. л. 46,9. Тираж 400 экз. Заказ № 1685
Отпечатано в ООО «ИПЦ «Измайловский»
190005, Санкт-Петербург, Измайловский пр., 18-д

ISBN 978-5-001820-20-8

ST. PETERSBURG INTERREGIONAL CONFERENCE
INFORMATION SECURITY OF RUSSIAN REGIONS

ST. PETERSBURG INTERNATONAL CONFERENCE
REGIONAL INFORMATICS

Proceedings

REGIONAL INFORMATICS AND INFORMATION SECURITY

The Issue No 10

St. Petersburg
2021

ГОСУДАРСТВЕННАЯ ПОЛИТИКА В СФЕРЕ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 332.14

ОСНОВНЫЕ ПАРАДИГМЫ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА ГОСУДАРСТВ АРКТИЧЕСКОГО БАССЕЙНА

Митько Арсений Валерьевич[1], Сидоров Владимир Константинович[2]
[1] Санкт-Петербургская Арктическая общественная академия наук
Искровский пр., 22, Санкт-Петербург, 193168, Россия
[1] Всероссийский научно-исследовательской институт метрологии имени Д.И. Менделеева
Московский пр., 19, Санкт-Петербург, 190005, Россия
[2] Санкт-Петербургский университет государственной противопожарной службы МЧС России
Московский пр., 149, Санкт-Петербург, 196105, Россия
e-mails: arseny73@yandex.ru, hamradio-spb@yandex.ru

Аннотация. В статье рассматриваются проблемы социально-экономического развития Арктического региона. В настоящее время наблюдается активизация деятельности всех без исключения государств, граничащих с Арктикой. Безусловно, во главе угла экономический потенциал Арктического шельфа, его освоение и защита национальных интересов. Перспективы развития Северного морского пути и становление цифровой экономики в Арктике также являются основополагающим направлением деятельности заинтересованных игроков.

Ключевые слова: цифровая экономика; Арктика; Северный морской путь; энергетический баланс; информационные технологии; связь.

MAIN PARADIGMS OF DEVELOPMENT OF THE INFORMATION SOCIETY OF THE STATES OF THE ARCTIC BASIN

Mitko Arseny[1], Sidorov Vladimir[2]
[1] Saint Petersburg Arctic Public Academy of Sciences
22 Iskrovsky Av, St. Petersburg, 193168, Russia
[1] D. I. Mendeleev All-Russian research institute of metrology
19 Moskovskij Av, St. Petersburg, 190005, Russia
[2] Saint-Petersburg University of State Fire Service of EMERCOM of Russia
149 Moskovskiy Av, St. Petersburg, 196105, Russia
e-mails: arseny73@yandex.ru, hamradio-spb@yandex.ru

Abstract. The article deals with the problems of socio-economic development of the Arctic region. Currently, there is an intensification of the activities of all states bordering the Arctic without exception. Of course, the economic potential of the Arctic shelf, its development and protection of national interests are at the forefront. The prospects for the development of the Northern Sea Route and the formation of a digital economy in the Arctic are also the fundamental areas of activity for interested players.

Keywords: digital economy; Arctic; Northern Sea Route; energy balance; information technology; communications.

Введение. На развитие Арктической зоны Российской Федерации приходится около 20% ВВП России, при том, что на территории Российской части Арктического региона проживает 2 % населения. Геологической службой США подсчитано, что на Арктику приходится около 22% мировых неразведанных ресурсов: 90 млрд. баррелей нефти (13% мировых неразведанных запасов); 1699 трлн. кубических футов, что эквивалентно 48,13 трлн. кубических метров, природного газа (30% мировых неразведанных запасов); 44 млрд. баррелей газового конденсата (20% мировых неразведанных запасов).

Для освоения ресурсов Арктической зоны Российской Федерации (далее АЗРФ) Россия сталкивается с многими проблемами:

– удаленность от основных промышленных центров, высокая ресурсоемкость и зависимость от поставок из других регионов;

– критическое состояние объектов жилищно-коммунального хозяйства и отрицательные демографические процессы;

– отсутствие Российских современных технических средств и техники для поиска, разведки и освоения морских месторождений углеводородов;

– неразвитость и износ инфраструктуры;

– отсутствие средств постоянного комплексного космического мониторинга, зависимость от иностранных средств;

– недостаточная развитость навигационно-гидрографического обеспечения мореплавания.

Международное энергетическое агентство (МЭА) в 2017 году представило очередной прогноз развития мировой энергетики до 2040 года.

В базовом сценарии New Policies Scenario, предусматривающем реализацию всех существующих и анонсированных экономико-политических мер по трансформации энергетического сектора, отмечается, что потребление газа вырастет на 45 % к 2040 году. Россия является одним из крупнейших игроков на рынке СПГ. По материалам Центрального диспетчерского управления (далее ЦДУ) ТЭК экспорт СПГ из России в страны Азиатско-Тихоокеанского региона за период с января по август 2018 года вырос на 48,2 % в годовом сопоставлении, до 15 млрд. куб. м. При этом в августе экспорт СПГ сократился по сравнению с прошлогодним августом на 22 %, до 0,9 млрд. куб. м.

Одним из главных конкурентов для поставок СПГ для России остаются США. Соединенные Штаты вышли на 1-ое место в мире по добыче нефти - почти 11 млн. баррелей в день. На 15 участках шельфа в Арктике, предусматривается разработка в 2019-2024 гг., в том числе на шельфе пограничного с Россией Чукотского моря. Однако сейчас действует ограничение на разработку природных ресурсов в Арктике. В свое время, Указ бывшего президента США Дональда Трампа о снятии запрета на добычу нефти на шельфе в марте 2019 года, Федеральный окружной суд Аляски признал незаконным.

Самыми богатыми в Арктическом регионе считаются запасы Баренцева и Карского морей. С момента подписания договора о морской границе между Россией и Норвегией в 2011 году в Баренцевом море не осталось неурегулированных территориальных споров. В юго-западной части Карского моря, у полуострова Ямал, разведаны крупные шельфовые месторождения природного газа и газового конденсата. Крупнейшие из них - Ленинградское (предварительно оцененные (ABC1+C2) запасы газа - более 1 трлн м³ и Русановское (780 млрд. м³). Освоение шельфовых месторождений планируется начать после 2025 года.

Планируется довести мощности на 2 проектах по добыче СПГ: «Ямал - СПГ» и на «Сахалин - 2». Проект завода по производству СПГ мощностью 16,5 млн. тонн, ресурсной базой которого станет Южно-Тамбейское месторождение полуострова Ямал с запасами 927 млрд. куб. м по классификации PRMS (по состоянию на 31.12.2013 г.). Оператор проекта - компания «Ямал СПГ», ее акционерами являются «Новатэк» (с долей 50,1 %), Total (20 %), CNPC (20 %) и китайский Фонд шелкового пути (9,9 %). Стоимость - 26,9 млрд. долл. США. Также в планах расширение морского порта Сабетта и строительство международного аэропорта Сабетта. «Сахалин - 2» - завод по производству СПГ проектной мощностью 9,6 млн. тонн на ресурсной базе Лунского месторождения острова Сахалин. Оператор проекта – компания Sakhalin Energy, совладельцами которой являются «Газпром» (50 % плюс одна акция), Shell (27,5 % минус одна акция), Mitsui (12,5 %) и Mitsubishi (10 %). Проект «Сахалин-2» предусматривает разработку Пильтун-Астохского и Лунского месторождений на Северо-восточном шельфе острова Сахалин. Объем производства СПГ в рамках проекта «Сахалин-2» в 2015 году составил 10,8 млн. тонн.

Помимо существующих проектов Россия планирует внедрить новые проекты СПГ:

– «Арктик СПГ-2» - срок ввода 2023 год, проект завода по производству СПГ на Гыданском полуострове, который реализует «Новатэк». Проект завода по производству СПГ из трех очередей общей мощностью до 18 млн. тонн. Ресурсной базой должно будет стать Утреннее месторождение с доказанными запасами 388,5 млрд. куб. м (согласно классификации SEC по состоянию на 31 декабря 2019 г.), расположенного на соседнем с Ямалом Гыданском полуострове. Лицензией на него владеет «дочка» «Новатэка» «Арктик СПГ-2». Предполагается освоение совместно с Китайской Народной Республикой.

– «Балтийский СПГ» в порту Усть-Луга Ленинградской области, для поставки в Атлантику, в Южную Азию - срок 2023 год совместно с Shell. Мощность завода составляет 10 млн. тонн. Договор подписан в 2017 году между «Газпром» и «Shell». Роль ресурсной базы будут выполнять не конкретные месторождения, а поставки из единой системы газоснабжения (ЕСГ) «Газпрома».

– «Дальневосточный СПГ» - «Сахалин - 1» (307 млн. тонн нефти и 485 млрд. куб. м. газа) расчет 6,2 млн. тонн. Предполагается строительство порта отгрузки СПГ для «Сахалин - 1». Акционеры – «Эксон Мобил» США - 30 %, «Роснефть» - 20 %, «ONGC Videsh» Индия - 20 %, «Содеко» Япония - 30 %. «Эксон Мобил» с 1995 года оператор «Сахалин -1» с долей - 30 %. В 2018 году «Эксон Мобил» вышли из проектов по геологоразведке совместных с компанией «Роснефть» из-за санкций.

– проект «Сахалин-3» 255 млн. тонн и ввод нефтеналивного терминала Ворота Арктики (Обская губа). Проект завода по производству СПГ мощностью 5 млн т в год с возможностью расширения до 10 млн. тонн. Его ресурсной базой должны будут стать месторождения проекта «Сахалин-1» - Чайво (введен 2005 году), Одопту (введен в 2010 году)

и Аркутун-Даги (введено в 2015 году) с запасами 307 млн. тонн нефти и 485 млрд. куб. м газа, которые разрабатываются консорциумом «Эксон Нефтегаз Лимитед» (по 30 % - у «Эксон Мобил» и японской «Содеко», по 20 % - у «Роснефти» и индийской ONGC).

Среди других проектов СПГ в Российской Арктике упоминаются:

– «Штокмановский СПГ» - проект завода по производству СПГ мощностью 7,5 млн. тонн на ресурсной базе Штокмановского месторождения шельфа Баренцева моря с запасами 38 трлн. куб. м газа. Оператором проекта должна была стать компания Shtokman Development AG, в которой 51 % принадлежал «Газпрому», 25 % – французской Total и еще 24 % – норвежской Statoil Hydro.

– «Печора СПГ» - Проект завода по производству СПГ мощностью 4 млн т на ресурсной базе Кумжинского и Коровинского месторождений Ненецкого автономного округа с общими запасами 165 млрд. куб. м газа по категории ABC1+C2. Оператор проекта – совместное предприятие «Роснефти» и группы «Аллтек», созданное в 2015 году.

Вместе с тем, идет борьба за рынок СПГ Европы. 26 марта 2019 г. палата представителей Конгресса США приняла законопроект о противодействии энергопоставкам России в Европу. Документ носит название «О приоритете усилий по укреплению сотрудничества учреждений США с целью убедить страны Центральной и Восточной Европы диверсифицировать источники энергии и маршруты поставок, укрепить энергобезопасность Европы и помочь США достичь своих целей в области глобальной энергетической безопасности». За него проголосовал 391 депутат, против были 24.

Законопроект призван:

– сокращать зависимость стран региона от Российских поставок газа;
– увеличивать конкуренцию на рынке;
– поощрять инвестиции Американских фирм в энергетическую инфраструктуру в Европе;
– увеличивать экспорт энергии и технологий из США.

На этом фоне следует ожидать укрепления российско-китайского сотрудничества в Арктике. Китай уже считает проект Ямал СПГ - на 1/3 принадлежит КНР - китайским, как и порт Сабетта, которые входят в глобальный интеграционный и логистически-коммуникационный проект Китая «Один пояс - один путь» (в Ямал СПГ: 30 % у КНР, 19 % - у Тоталь). Следует помнить о том, что Китай будет участвовать в проекте «Арктик СПГ-2».

Среди других проектов, которые могут быть реализованы с КНР - ж/д «Белкомур» и порт Архангельск. России необходимо привлекать в Арктические энергетические проекты иностранных инвесторов, при этом соблюсти национальные интересы и интересы национальной безопасности.

В январе 2018 г. пресс-канцелярия Госсовета КНР обнародовала первую Белую книгу об Арктической политике Китая, в которой говорится, что Пекин является важной заинтересованной стороной в делах Арктики. Китай не имеет территорий в Арктике, но Госсовет отмечает его «географическую близость» к полярным областям. КНР в своей стратегии определил, что «Полярный Шелковый путь» является частью более широкой китайской программы «Один пояс - один путь». КНР рассматривает возможность участия в строительстве ж/д магистрали «Белкомур» в Архангельской области «Белое море - Коми - Урал» - ОАО «Белкомур» через сотрудничество китайской корпорацией «Poly Technology» и ОАО «РЖД». А также в строительстве порта Архангельск через китайскую компанию COSCO. Среди китайских грузовых судов первым Северный морской путь (Северо-Восточный проход) в 2013 году освоил «Yong Sheng». Летом 2017 года этим маршрутом прошли еще шесть китайских судов. В сентябре 2017 года китайское исследовательское судно «Xue Long» впервые осуществило рейс Северо-Западным проходом вдоль северного побережья Канады, сократив время в пути из Нью-Йорка в Шанхай на семь суток по сравнению с маршрутом через Панамский канал.

Из стратегии России, относительно развития АЗРФ до 2035 года следует, что главными задачами для развития Арктического региона являются:

– создание ИТ- инфраструктуры;
– обеспечение экологической безопасности;
– развитие международного сотрудничества в Арктике;
– обеспечение военной безопасности и защита границы.

Следующим этапом развития Российской Арктики будет увеличение транзитного потенциала СМП, строительство логистических терминалов и совершенствование нормативно-правовой базы. Для обеспечения безопасности СМП Россия может утвердить необходимость сопровождения всех иностранных судов в акватории Арктических морей. Необходимо создание системы комплексной безопасности АЗРФ [2].

Вывод. Несмотря на санкции, между Арктическими странами не было охлаждения отношений. Возможно, что можно будет договориться о Соглашении по ключевым принципам обеспечения безопасности связи и подписать соответствующий Договор об общих правилах.

СПИСОК ЛИТЕРАТУРЫ

1. Стратегия развития Арктической зоны Российской Федерации и обеспечения национальной безопасности на период до 2035 года (Указ Президента РФ № 645 от 26.10.2020 г.).
2. Основы государственной политики Российской Федерации в Арктике на период до 2035 года. (Указ Президента РФ № 164 от 05.03.2020 г.).

УДК 681.883.04

ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМ УПРАВЛЕНИЯ И СВЯЗИ В АРКТИЧЕСКОЙ ЗОНЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Митько Арсений Валерьевич[1], Сидоров Владимир Константинович[2]
[1] Санкт-Петербургская Арктическая общественная академия наук
Искровский пр., 22, Санкт-Петербург, 193168, Россия
[1] Всероссийский научно-исследовательской институт метрологии имени Д.И. Менделеева
Московский пр., 19, Санкт-Петербург, 190005, Россия
[2] Санкт-Петербургский университет государственной противопожарной службы МЧС России
Московский пр., 149, Санкт-Петербург, 196105, Россия
e-mails: arseny73@yandex.ru, hamradio-spb@yandex.ru

Аннотация. В статье рассматриваются проблемы информационного обеспечения Арктического пространственного планирования, приводятся результаты исследований возможных механизмов реализации комплексирования средств мониторинга различных организационных структур. В качестве одного из примеров рассматривается принцип объединения систем управления и региональных интегральных автоматизированных систем мониторинга обстановки (РИАСМО) путём объединения информации ведомственных АСМО, совместно действующих в едином регионе. Основные результаты получены в совместных разработках Арктической общественной академии наук и Санкт-Петербургского университета ГПС МЧС России.

Ключевые слова: мониторинг; комплексирование; Арктика; пространственное планирование; информационные технологии; связь.

PROSPECTS FOR THE DEVELOPMENT OF CONTROL AND COMMUNICATION SYSTEMS IN THE ARCTIC ZONE OF THE RUSSIAN FEDERATION

Mitko Arseny[1], Sidorov Vladimir[2]
[1] Saint Petersburg Arctic Public Academy of Sciences
22 Iskrovsky Av, St. Petersburg, 193168, Russia
[1] D. I. Mendeleev All-Russian research institute of metrology
19 Moskovskij Av, St. Petersburg, 190005, Russia
[2] Saint-Petersburg University of State Fire Service of EMERCOM of Russia
149 Moskovskiy Av, St. Petersburg, 196105, Russia
e-mails: arseny73@yandex.ru, hamradio-spb@yandex.ru

Abstract. The article discusses the problems of information support for Arctic spatial planning, provides the results of studies of possible mechanisms for the implementation of the integration of monitoring tools for various organizational structures. As one of the examples, the principle of combining control systems and regional integrated automated systems for monitoring the situation (RIASMO) by combining information from departmental ASMOs jointly operating in a single region is considered. The main results were obtained in joint developments of the Arctic Public Academy of Sciences and St. Petersburg State Fire Service EMERCOM of Russia.

Keywords: monitoring; integration; Arctic; spatial planning; information technologies; communication.

Введение. Радикальные изменения геополитической обстановки, содержания задач и условий обеспечения социально-экономического развития Арктических регионов определяют основное содержание комплексной арктической реформы - составной части и приоритетной задачи современного этапа арктического строительства. В рамках арктической реформы осуществляется взаимосвязанное, скоординированное реформирование Арктической системы управления и пространственного планирования, транспортно-коммуникационной системы и других компонентов арктической организации государства, а основным стимулом (мотивацией) вхождения в состав кластера станет необходимость быть в структуре, обещающей полноценное функционирование, общественную, административную и бизнес-поддержку, включая российские и зарубежные инвестиции в проекты различного масштаба, например, развитие Северного морского пути, формирование единого информационного пространства Арктики, международной системы обеспечения глобальной, региональной и национальной безопасности в регионе.

Эффективность реализации разработанных предложений по созданию Государственной интегральной автоматизированной системы мониторинга обстановки в Арктике с учётом геополитических факторов циркумполярного, федерального и регионального масштабов состоит в значительном повышении качества информационного обеспечения системы управления Арктической зоной Российской Федерации (далее АЗРФ).

Область применения:

– в проектных и конструкторских организациях при разработке схем территориального планирования АЗРФ;

– в государственных структурах при разработке документов информационного обеспечения планирования и управления процессами социально-экономического развития;

– в бизнес-структурах регионов АЗРФ и других регионов Российской Федерации и зарубежья при планировании инвестиционных мероприятий и развитии делового и научно-технического сотрудничества [1].

«Стратегия национальной безопасности Российской Федерации», утвержденная Указом Президента Российской Федерации №683 от 31.12.2015 определяет необходимость развития системы обеспечения национальной безопасности, одной из важнейших задач которой является обеспечение безопасности жизнедеятельности важных хозяйственных, оборонных и др. объектов.

В принципе, обеспечение безопасности жизнедеятельности осуществляется путем:

– контроля исполнения правил безопасности (далее ИПБ) – автоматизированные системы контроля движения транспорта и др.,

– охраны важных объектов (далее ОВО) от террористических и криминальных угроз;

– предупреждения чрезвычайных ситуаций (далее ПЧС), в том числе угроз геофизического характера.

Системы ИПБ, ОВО и ПЧС состоят из двух подсистем:

1) автоматизированная система мониторинга обстановки (далее АСМО);

2) система противодействия угрозам и нарушителям (далее СПУН).

АСМО создаются внутри ведомств на трех уровнях:

– государственном - ведомственные АСМО (далее ВАСМО),

– региональном - региональных АСМО (далее РАСМО),

– локальном/объектовом - локальные/объектовые АСМО (далее ЛАСМО).

В настоящее время, на основании действующих федеральных документов – «Стратегия национальной безопасности Российской Федерации», законы №ФЗ-16 «О транспортной безопасности», №ФЗ-35 «О противодействии терроризму», №ФЗ-261 «О морских портах в Российской Федерации…», Указ Президента РФ №1167 «О неотложных мерах по повышению борьбы с терроризмом» различные ведомства самостоятельно и независимо друг от друга развивают автоматизированные системы мониторинга обстановки для обеспечения безопасности мореплавания и охраны важных морских объектов от внешних угроз террористического и криминального характера.

Состав предлагаемой ГИАСМО:

Интегральные межведомственные АСМО практически могут быть созданы только путем организации обмена информацией между участвующими в ней ВАСМО, РАСМО или ЛАСМО, т.е. без использования межведомственного звена интеграции информации. В таком случае в состав ГИАСМО должны входить (рис.1):

– все ВАСМО, включенные в состав ГИАСМО;

– главный информационно-командный центр (далее ГИКЦ) для аппарата президента/правительства РФ, однако в нем не требуется реализация функции интеграции информации всех ВАСМО, а достаточно отображения информации одной или нескольких ВАСМО по выбору;

– центральная сеть обмена информацией между ВАСМО и ГИКЦ.

Также, совместно действующие на конкретном объекте ЛАСМО различных ведомств, следует объединять локальными каналами обмена информацией в ЛИАСМО.

Достоинства предлагаемой ГИАСМО:

– исключается необходимость создания межведомственных центров интеграции информации на локальном, региональном и верхнем уровнях, определения юридической базы их функционирования, эксплуатирующих организаций и т.п.;

– для управления ГИАСМО, РИАСМО и ЛИАСМО достаточно создать межведомственный орган научно-методического сопровождения согласованного развития участвующих в них ВАСМО;

– обеспечивается возможность создания ВАСМО, РАСМО и ЛАСМО с учетом их взаимодействия (обмена информацией) с соседними АСМО, что позволит существенно сократить требуемые совместные объемы оборудования, финансирования и сроки их строительства;

– открывается перспектива унификации системных решений ВАСМО, РАСМО и ЛАСМО, применяемых в них технических средств, что обеспечит возможность использования только одобренных (сертифицированных) технических решений и средств, позволит существенно сократить их номенклатуру;

– обеспечивается возможность организации эффективного взаимодействия с СПУН различных ведомств, а также подключения сил и средств оборонных ведомств к защите важных гражданских объектов.

Состав базовой РИАСМО:

В полнофункциональную (базовую) РИАСМО должны входить:

– все РАСМО различных ведомств, включенные в РИАСМО;

– региональный информационно-командный центр (далее РИКЦ);

– межведомственная региональная сеть обмена информацией между РАСМО и РИКЦ.

РИКЦ предназначен для использования в аппарате руководства региона, освобожден от функции интеграции всей получаемой в РИАСМО информации, но обеспечивает отображение информации одной или нескольких РАСМО или ЛАСМО по выбору.

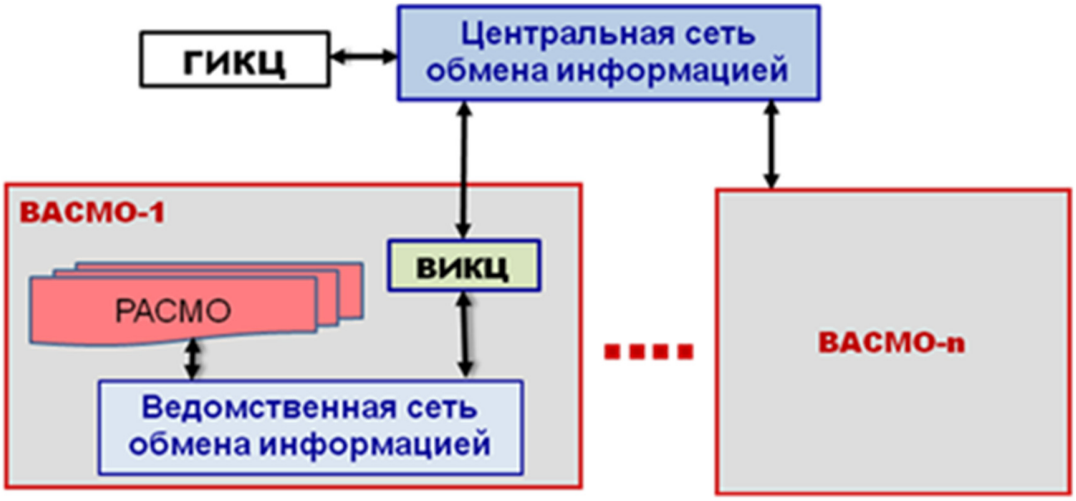


Рис.1. Структурная схема ГИАСМО

Состав базовой ЛИАСМО:

По аналогии с РИАСМО в базовую ЛИАСМО должны входить:

- все ЛАСМО различных ведомств, включенные в ЛИАСМО;
- локальный информационно-командный центр (далее ЛИКЦ);
- межведомственная локальная сеть обмена информацией между ЛАСМО и ЛИКЦ.

ЛИКЦ предназначен для использования в аппарате руководства обслуживаемого объекта и обеспечивает отображение информации одной или нескольких действующих на объекте ЛАСМО по выбору. В базовую ВАСМО должны входить:

- все РАСМО данного ведомства, включенные в ВАСМО;
- ведомственный информационно-командный центр (далее ВИКЦ);
- ведомственная сеть обмена информацией между РАСМО и ВИКЦ.

В базовую РАСМО входят:

- все включенные в нее ЛАСМО;
- ведомственный региональный информационно-командный центр (далее ВРИКЦ);
- ведомственная региональная сеть обмена информацией между ЛАСМО и ВРИКЦ.

ВРИКЦ предназначается для использования аппаратом руководства (правительства) региона, при этом в нем реализуются функции отображения и архивации информации одной или нескольких ЛАСМО, по выбору, или – интегральной информации всех ЛАСМО в составе РАСМО.

Для удобства реализации и обслуживания всех видов информационно-командных центров целесообразно в них применить единый базовый состав, включающий в себя АРМ начальника центра (далее АРМ-Н), одно или несколько АРМ дежурных (далее АРМ-Д) и технологическое АРМ (далее АРМ-Т), соединенные ЛВС.

АРМ-Н аналогичен АРМ-Д, но дополнительно оборудовано настенным экраном, на котором отображается ситуация на электронной карте всей зоны контроля.

АРМ-Т является рабочим местом сервисного инженера системы, обеспечивает управление и контроль работоспособности ее оборудования, регистрацию и архивацию информации.

Российская Федерация исходит из необходимости обладать потенциалом, достаточным для осуществления своей арктической политики, способным гарантированно обеспечить защиту национальных интересов в Арктике в любых условиях обстановки. Российская Федерация оставляет за собой право на применение всех имеющихся возможностей, включая силовые методы в критических ситуациях для национальной безопасности Российской Федерации в Арктике [2].

Заключение. Вместе с тем, в соответствии с Концепцией формирования и развития единого информационного пространства РФ, одобренной Решением Президента РФ №Пр-1694, при создании различных ведомственных СИОБ необходимо осуществлять их интеграцию, то есть создавать межведомственные единые СИОБ (ЕСИОБ) на государственном (ГЕСИОБ), региональном (РЕСИОБ) и локальном (ЛЕСИОБ) уровнях. Отсутствие такой интеграции приводит к дублированию различными ведомствами работ по созданию СОНБ, распылению государственных ресурсов.

СПИСОК ЛИТЕРАТУРЫ

3. Митько А.В. Основные направления формирования Арктической доктрины России/Научный вестник Ямало-Ненецкого автономного округа № 4 (105): 2019. С.25-29.
4. Митько А.В. Труды Международной молодежной научной конференции «Волновая электроника и ее применения в информационных и телекоммуникационных системах» СПБ.: ГУАП, - 2017. С. 113-118.

УДК 681.3.004.8

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЗДАВАЕМЫХ АВТОМАТИЗИРОВАННЫХ СТРАТЕГИЧЕСКИХ СИСТЕМАХ УПРАВЛЕНИЯ РАЗВИТИЕМ СУБЪЕКТОВ РОССИЙСКОЙ ФЕДЕРАЦИИ: ПРОБЛЕМЫ И РЕШЕНИЯ

Соколенко Виктор Николаевич
Северо-Западный институт управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации»
Средний проспект, 57, В.О., Санкт-Петербург, 199178, Россия
e-mails: sokolenko-vn@ranepa.ru

Аннотация. В статье рассматриваются проблемы информационной безопасности в создаваемых автоматизированных стратегических системах управления развитием субъектов Российской Федерации и их решение на основе использования методов ситуационного управления по прогнозированию состояния информационной безопасности.

Ключевые слова: информационная безопасность; прогнозирование состояния информационной безопасности; ситуационное управление; автоматизированная система стратегического управления; развитие территорий.

INFORMATION SECURITY IN AUTOMATED STRATEGIC DEVELOPMENT MANAGEMENT SYSTEMS OF THE CONSTITUENT ENTITIES OF THE RUSSIAN FEDERATION: PROBLEMS AND SOLUTIONS

Sokolenko Viktor
The North-West Institute of Management of RANEPA
57/43 Sredny Av, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: sokolenko-vn@ranepa.ru

Abstract. The article discusses the main problems of creating systems for strategic management of social and economic development of the constituent entities of the Russian Federation.

Keywords: information security; predicting the state of information security; situational management; automated strategic management system; development of territories.

Введение. Развитие информационных технологий в мире и, соответственно, в Российской Федерации (РФ) позволили расширить практику применения автоматизированных систем управления (АСУ) при подготовке и принятия управляющих решений по стратегическому развитию территорий субъектов РФ. Для этого стали создаваться автоматизированные стратегические системы управления (АССУ) развитием субъектов РФ. Причем характерной особенностью при проектировании и создании таких АСУ является обязательное наличие подсистемы прогнозирования внешних информационных воздействий (ВИВ), которые носят, как правило, стохастический характер при функционировании АССУ. Отсюда возникает ряд проблем при разработке этой подсистемы в таких АСУ, которые будут использоваться в процессе государственного и муниципального управления (ГМУ) развитием территорий субъектов РФ. Поэтому при прогнозировании состояния и обеспечению информационной безопасности (ИБ) в АССУ необходимо учитывать, что современное информационное пространство (ИП) настолько доступно и открыто, что возможности по представления информации и злоупотребления в нем фактически не ограничены. Следовательно, при создании единого ИП в субъектах РФ в интересах принятия управленческих решения по развитию их территорий появляется проблема, носящая объективный характер и связанная со специфическим представлением различных видов информации (текстовой, аудио, видовой, графической и т. д.), а также с наличием различных форматов представления электронной информации в современных аппаратно-программных системах и отсутствием единой информационной политики в различных субъектах при создании единого ИП.

Следует отметить, что формирование информационных ресурсов (ИР) для принятия управленческих решений по развитию территорий в субъектах РФ является частью проблемы формирования единого ИП. В общем случае, ИР формируются в результате деятельности, как органов государственной власти, так и государственных и негосударственных предприятий, научных, учебных и общественных организаций. Они включают информацию и знания, а также лингвистические средства, применяемые для описания конкретной предметной области и для доступа к информации и знаниям. В процессе формирования и использования ИР при прогнозировании состояния и обеспечению ИБ в таких АСУ, осуществляется сбор, обработка, хранение, поиск и выдача информации по запросам и регламенту. Указанная проблема обостряется из-за быстрого роста информационных потоков, циркулирующих в обществе. Всё это требует развития информационной инфраструктуры в субъектах РФ, которая характеризуется качественным и количественным составом элементов, информационной производительностью их и инфраструктуры в целом. И новым элементом информационной инфраструктуры становятся сети знаний, создание которых решается посредством социального взаимодействия и мобилизации ИР, находящихся в распоряжении владельцев этих ресурсов. Примерами такой сети знаний являются, прежде всего, интеллектуальные организации: технопарки, технополисы, наукограды,

бизнес-инкубаторы, информационно-аналитические центры. Учитывая это, поиск требуемой информации для функционирования таких объектов становится актуальным в связи с неконтролируемым ростом ненужного (а иногда и опасного) информационного «мусора» и недостатком актуальной деловой и коммерческой информации.

В перспективе, эффективный поиск требуемой информации может быть решен только с использованием АССУ, которые должны будут автоматически адаптироваться с учетом уровня знаний и запросов конкретных пользователей, воспринимать запросы на естественном языке и, используя методы ситуационного управления, выдавать им соответствующую информацию. Так как при определении информации ограниченного доступа и ее защиты необходимо помнить, что постоянная утечка информации ограниченного доступа (публикация сведений, составляющих государственную тайну, факты «взлома» интернет сайтов, переписки мобильных телефонов и т. п.) обостряет проблему ее защиты, для решения которой необходимо:

– дальнейшее развитие теоретических основ и формирование научно-методологического базиса, позволяющих адекватно описывать процессы в условиях значительной неопределенности и непредсказуемости проявления дестабилизирующих факторов (информационных угроз);

– разработать новые, научно обоснованные нормативно-методические документы по обеспечению ИБ на базе исследования и классификации угроз информации и выработки стандартов требований к ее защите;

– иметь стандартизацию подходов к созданию систем защиты информации (СЗИ) и рационализацию схем и структур управления защитой на объектовом, региональном и государственном уровнях;

– не допускать использования информации в разрушительных целях (вирусов) и отдельных видов электронной информации для вывода из строя (разрушения) компьютерных систем различного назначения: от отдельных частных компьютеров до специализированных АСУ.

Наряду с вышеизложенными проблемами необходимо при разработке подсистемы прогнозирования влияния ВИВ в АССУ учитывать и основные проблемы общественно-социального характера, которые были рассмотрены с участием автора в [3], и отмечено, что в постиндустриальном обществе наличие информации с точки зрения государственной и экономической безопасности выступает в двух категориях: как основа формирования угроз во всех сферах общественной деятельности и как один из основных экономических продуктов и товаров, обеспечивающих развитие важнейшей составляющей постиндустриального общества — единого ИП. Для решения рассмотренных проблем в интересах повышения эффективности ГМУ, достижения устойчивого развития субъектов РФ и обеспечения национальной безопасности в стране созданы и успешно функционируют ситуационные центры, деятельность которых в субъектах РФ рассмотрена в [1]. Они являются основой для проектирования и создания АССУ развитием территорий субъектов РФ в интересах обеспечения реализации полномочий органов государственной власти и местного самоуправления в соответствии с целями, установленных федеральными законами, в первую очередь, федеральным законом № 172 от 28 июня 2014 года «О стратегическом планировании». На них также возлагается информационный обмен между соответствующими уровнями управления.

Владение информацией необходимого качества в нужное время и в нужном месте, несомненно, является залогом успеха в любом виде деятельности, особенно, в управленческой и хозяйственной деятельности. Но можно утверждать, что в создаваемых АССУ субъектов РФ необходимо, в первую очередь, обеспечить ИБ при их функционировании. Под ИБ, в широком смысле, понимается состояние защищенности важнейших интересов государства, общества и личности в информационной среде. И поэтому проблема обеспечения ИБ становится особенно актуальной при создании АССУ субъектов РФ с целью поддержания должного уровня качества управления, которая не снимается и сегодня с повестки дня. Предложения по основам проектирования и создания АССУ в субъектах РФ сформулированы с участием автора в [2]. Но в связи с развитием процессов цифровизации ГМУ в настоящее время имеются актуальные и нерешенные информационные проблемы, рассмотренные выше.

Следует отметить, что в настоящее время СЗИ в АСУ регионального уровня, используемые в интересах повышения эффективности ГМУ, достижения устойчивого развития и обеспечения ИБ при создании АССУ в субъектах РФ, имеют ряд существенных недостатков, которые не позволяют эффективно решать вопросы по обеспечению заданного уровня защищенности информации в течение всего жизненного цикла и модернизации таких аналогичных систем. Это объясняется сложившимися требованиями к архитектуре больших АСУ. Существующие методы и средства защиты информации АСУ регионального значения, в основном, обеспечивают защиту информации лишь от известных угроз. Это определяет низкую эффективность применения имеющихся средств и СЗИ в настоящее время с учетом стохастического и практически постоянного появления новых угроз и увеличением их числа реализаций. Для повышения эффективности защищенности информации в создаваемых АССУ в субъектах РФ необходимо при их проектировании закладывать упреждающие способы защиты информации, способные адаптироваться к любым изменениям ВИВ. Поэтому для эффективной защиты информации в таких системах необходимо использовать особые подходы, учитывающие особенности влияния условий ВИВ на информационные подсистемы в создаваемых АССУ в субъектах РФ. На основе анализа информации в [4, 5], можно выделить следующие особенности влияния условий ВИВ на АССУ в субъектах РФ:

– проведение негативных воздействий на ограниченное число элементов АССУ определенного уровня, как правило, нижнего. Это объясняется тем, что применение ВИВ на элементы всех уровней АССУ требует привлечения большого объема ресурсов;

– большая степень неопределенности ВИВ в целом на АССУ. Это связано с разнообразием её элементов, широким спектром хаотических воздействий и сложностью в их согласовании как по времени, так и по пространству, при масштабном применении;

– проведение ВИВ с учетом потенциальной возможности оперативного оповещения о нем на один из элементов АССУ всех других её элементов и актуализации базы описаний ВИВ в каждом элементе системы, что связано с наличием разветвленных связей между элементами АССУ;

– различная важность элементов АССУ и разные подходы к обеспечению их ИБ, что предполагает выявление наиболее уязвимых элементов и сосредоточение ВИВ на них.

С учетом вышеизложенных особенностей для обеспечения ИБ при создании АССУ в субъектах РФ необходимо разработать следующие методические положения:

– по выбору оптимальной стратегии реагирования АССУ на ВИВ;

– по изменению свойств и параметров подсистемы защиты информации в АССУ;

– по количественной оценке уровня защищенности элементов АССУ.

При разработке этих методических положений целесообразно ориентироваться на их максимально возможную формализацию с целью создания на их основе алгоритмов системы поддержки принятия решений по управлению защитой информации в этой АССУ. В целом, разработка указанных методических положений необходима для создания способа построения и управления подсистемой защиты информации в АССУ на основе теории ситуационного управления с распознаванием ВИВ и прогнозированием ИП, а также самоадаптацией и обоснованием автоматического приспособления к непредвиденным изменениям параметров АССУ и внешней среды, который должен послужить основой для программно – аппаратной реализации.

Одним из вариантов, который может быть положен в основу такого способа, целесообразно рассмотреть методические положения, изложенные в [6], существо которых состоит в следующем. Повышение вероятности защищенности АССУ может достигаться за счет определения угроз вторжений и состояния ИБ с помощью математических алгоритмов, разработанных на основе древовидного классификатора и карт Кохонена. И тогда алгоритм управления должен включать: наблюдение и выделение признаков цифровых потоков с протоколами передачи данных, поступающих в ИВС и в используемый сервер, распознавание вторжения, выбор и реализация способа защиты. Предложенное в [7], в отличие от известных, должно позволить в создаваемых АССУ в субъектах РФ:

– учесть динамику и стохастическую неопределенность основных процессов защиты информации в этих системах;

– проводить мониторинг, распознавание вторжений и прогнозировать состояния при интеллектуальных процессах защиты;

– обеспечивать возможность обоснованного принятия решения на проведение мероприятий по предотвращению реализации угроз безопасности АССУ в субъектах РФ за счет прогнозирования состояния ИБ.

Заключение. Рассмотренные проблемы и предлагаемое решение обеспечения ИБ в создаваемых АССУ развитием территорий субъектов РФ позволит осуществить оперативное перестроение структуры СЗИ элемента, подвергнувшегося ВИВ, а также произвести подготовку решения о возможном изменении структуры СЗИ остальных элементов ССУ, в случае необходимости реагирования на ВИВ. Кроме того, это должно сопутствовать повышению качества управления при функционировании АССУ в субъектах РФ, имея в виду перспективу полного перехода управленческих структур на платформу стратегического видения будущего и его конструирования в интересах повышения качества жизни населения в субъектах РФ.

СПИСОК ЛИТЕРАТУРЫ

1. Лисенкова А.А, Левкин И.М. Обеспечение информационной безопасности государственных информационных систем - Труды Всероссийского Форума, Санкт - Петербург, 25-27 октября 2017г. «Система распределенных ситуационных центров как основа цифровой трансформации государственного управления «СРСЦ–2017». /Научный совет по информатизации Санкт - Петербурга. - СПб.: ООО «Политехника Сервис». 2018. с.179 - 181
2. Баранец С.Н., Соколенко В.Н. Основы проектирования и создания стратегической системы управления экономическим и социальным развитием субъекта Российской Федерации – Материалы Всероссийской научно-практической конференции «Современное управление: векторы развития» – Калининград: ЗФ РАНХиГС, 2021. С. 239 – 245.
3. Баранец С.Н., Соколенко В.Н. Проблемы создания стратегической системы управления экономическим и социальным развитием субъекта Российской Федерации – Материалы XV Международной научно-практической конференции «Цифровые трансформации в развитии экономики и общества» 21 апреля 2021 г. – Воронеж: НАУКА-ЮНИПРЕСС, 2021. С. 339 - 346.
4. Володина А.А., Левкин И.М. Оценка эффективности процесса отражения информационных угроз в больших информационных системах// Приборостроение № 5, 2016, с. 335-341.
5. Рахимов Е.А. Модели и методы поддержки принятия решений в интеллектуальной системе защиты информации: дис. Канд.техн.наук: 05.13.19. Уфа, 2006, с.237. РГБ ОД, 61:07-5/726.
6. Создание систем защиты информации государственных информационных систем [Электронный ресурс]. URL: http:// www.dialognauka.ru/solutions/ security_ gosinfosystem/(дата обращения 12.07.2020г.).
7. Липатников В.А., Литвинов А.А., Сахаров Д.В. Управление информационно – вычислительной сетью с распознаванием вторжений и прогнозированием состояния информационной безопасностью - Труды Всероссийского Форума, Санкт - Петербург, 25-27 октября 2017 г. «Система распределенных ситуационных центров как основа цифровой трансформации государственного управления «СРСЦ–2017». /Научный совет по информатизации Санкт - Петербурга. - СПб.: ООО «Политехника Сервис». 2018. с.176 – 179.

УДК 004.056

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ ПО ОЦЕНКЕ ПОКАЗАТЕЛЕЙ КРИТЕРИЕВ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Сторожик Виктор Сергеевич[1], Щелокова Екатерина Кристиановна[2]
[1] Арктическая общественная академия наук
Беринга, ул., 38, Санкт-Петербург, 199397, Россия
[2] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: vstorozhik@yandex.ru, kece7980@gmail.com

Аннотация. Рассматриваются особенности реализации требований нормативных правовых актов и методических документов, определяющих порядок оценки показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации.

Ключевые слова: безопасность; значимый объект; категория значимости; критерий значимости; критическая информационная инфраструктура; показатель; субъект; угроза безопасности информации.

FEATURES OF THE IMPLEMENTATION OF REQUIREMENTS FOR THE EVALUATION OF INDICATORS CRITERIA FOR THE SIGNIFICANCE OF OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION

Storozhik Viktor[1], Shchelokova Ekaterina[2]
[1] The Arctic Public Academy of Sciences
38 Bering St, St. Petersburg, 199397, Russia
[2] The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: vstorozhik@yandex.ru, kece7980@gmail.com

Abstract. The features of the implementation of the requirements of regulatory legal acts and methodological documents defining the procedure for evaluating the indicators of the criteria for the significance of objects of the critical information infrastructure of the Russian Federation are considered.

Keywords: security; significant object; category of significance; criterion of significance; critical information infrastructure; indicator; subject; threat to information security.

Введение. В Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, к основным национальным интересам в информационной сфере отнесено обеспечение устойчивого и бесперебойного функционирования критической информационной инфраструктуры (КИИ) в условиях проведения компьютерных атак [1].

В Стратегии национальной безопасности Российской Федерации указано, что использование иностранных информационных технологий и телекоммуникационного оборудования повышает уязвимость российский информационных ресурсов, включая объекты КИИ, к воздействию из-за рубежа, а также поставлена задача развития системы прогнозирования, выявления и предупреждения угроз информационной безопасности Российской Федерации, определения их источников и оперативной ликвидации последствий реализации таких угроз [2].

В рамках реализации требований Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [3] Постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 утверждены Правила категорирования объектов критической информационной инфраструктуры Российской Федерации и перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений [4].

Под категорированием понимается установление соответствия каждого объекта КИИ критериям значимости и их показателям. Категорирование осуществляется субъектами КИИ в отношении принадлежащих им на праве собственности, аренды или ином законном основании объектов КИИ.

Определение категорий значимости объектов КИИ (КЗ) осуществляется на основании показателей критериев значимости объектов КИИ (ПКЗ) и их значений, предусмотренных перечнем ПКЗ объектов КИИ и их значений. Объекту КИИ по результатам категорирования присваивается в соответствии с перечнем ПКЗ категория значимости с наивысшим значением. Устанавливаются три КЗ: самая высокая категория – первая, самая низкая – третья. В случае если ни один из ПКЗ неприменим для объекта КИИ или объект КИИ не соответствует ни одному ПКЗ и их значениям, КЗ не присваивается [4].

В соответствии с федеральным законом от 26 июля 2017 г. № 187-ФЗ значимым объектом КИИ является объект, которому присвоена одна из КЗ и который включен в реестр значимых объектов КИИ [3, 5].

В процессе категорирования объекта КИИ комиссией по категорированию оцениваются: социальная, политическая, экономическая, экологическая значимость, а также значимость для обеспечения обороны страны, безопасности государства и правопорядка.

Оценка производится в соответствии с перечнем ПКЗ, при этом определяется масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ, а также определяются значения каждого из ПКЗ или обосновывается их неприменимость. Рассматривается наихудший сценарий (целенаправленная атака) с максимально возможным ущербом. Наличие цифровых систем резервирования, защит и противоаварийной автоматики не учитываются.

Рассмотрим особенности оценки каждого из показателей значимости объектов КИИ.

Показатели критерия социальной значимости:

1. Причинение ущерба жизни и здоровью людей (человек).

Значение показателя: I категория – более 500; II категория – более 50, но менее или равно 500; III категория – более или равно 1, но менее или равно 50.

Причинение ущерба жизни людей – гибель.

Причинение ущерба здоровью людей – нарушение анатомической целостности и физиологической функции органов и тканей человека в результате воздействия физических, химических, биологических и психических факторов внешней среды (в соответствии с правилами определения степени тяжести вреда, причиненного здоровью человека, утв. постановлением Правительства РФ от 17 августа 2007 г. № 522 [6].

Показатель оценивается по результатам анализа последствий возможных аварий или иных инцидентов, связанных с негативным физическим, химическим, радиационным или иным воздействием на людей, которое может быть оказано в результате нарушения функционирования объекта КИИ.

2. Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, оцениваемые:

а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения;

Значение показателя: I категория – выход за пределы территории одного субъекта РФ или территории города федерального значения; II категория – выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта РФ или территории города федерального значения; III категория - в пределах территории одного муниципального образования (численностью от 2 тыс. человек) или одной внутригородской территории города федерального значения. При оценке значений данного показателя необходимо руководствоваться нормами Федерального закона от 6 октября 2003 г. N 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» [7].

б) по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек).

Значение показателя: I категория – более или равно 5000; II категория – более или равно 1000, но не менее 5000; III категория - более или равно 2, но менее 1000. При определении значения данного показателя необходимо избежать его несоответствия со значением показателя 2а), учитывая данные о численности населения муниципальных образований РФ, которые представлены Федеральной службой государственной статистики (http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/population/demography/).

3. Прекращение1 или нарушение функционирования2 объектов транспортной инфраструктуры, оцениваемые:

а) на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг;

Значение показателя: I категория – выход за пределы территории одного субъекта РФ или территории города федерального значения; II категория – выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта РФ или территории города федерального значения; III категория – более или равно 2, но менее 1000.

Под транспортной услугой понимается результат деятельности исполнителя транспортной услуги по удовлетворению потребностей пассажира, грузоотправителя и грузополучателя в перевозках в соответствии с установленными нормами и требованиями [8]. Порядок установления количества категорий и критериев категорирования объектов транспортной инфраструктуры и транспортных средств утвержден приказом Минтранса России от 21 февраля 2011 г. N 62 [9].

Объекты транспортной инфраструктуры категорируются согласно статье 6 Федерального закона от 09.02.2007 N 16-ФЗ «О транспортной безопасности» [10].

б) по количеству людей, для которых могут быть недоступны транспортные услуги (тыс. человек).

Значение показателя: I категория – более или равно 5000 (5 млн. чел.); II категория – более или равно 1000, но менее 5000; III категория – более или равно 2, но менее 1000 (1 млн. чел.).

4. Прекращение1 или нарушение функционирования2 сети связи, оцениваемые по количеству абонентов, для которых могут быть недоступны услуги связи (тыс. человек).

Значение показателя: I категория – более или равно 5000; II категория - более или равно 1000, но менее 5000; III категория – более или равно 3, но менее 1000.

Сеть связи – технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи. Услуга связи – деятельность по приему, обработке, хранению, передаче, доставке сообщений электросвязи или почтовых отправлений (в соответствии с Федеральным законом от 7 июля 2003 г. №126-ФЗ

«О связи») [11]. Выделяют следующие услуги связи: подвижная радиотелефонная связь (сотовая); телефонная (междугородняя, международная, местная, внутризоновая, выделенная сеть, таксофонная); радиосвязь (подвижная радиосвязь в сети связи общего пользования, подвижная радиосвязь в выделенной сети связи, подвижная спутниковая связь); каналы предоставления доступа к сети Интернет; вещание (кабельное, проводное радиовещание, эфирное вещание); почта; телеграф.

Реестр лицензий в области связи, осуществляет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) https://rkn.gov.ru/communication/register/license.

5. Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов).

Значение показателя: I категория – менее или равно 6; II категория - менее или равно 12, но более 6; III категория – менее или равно 24, но более 12.

Государственная услуга – деятельность по реализации функций соответственно федерального органа исполнительной власти, государственного внебюджетного фонда, исполнительного органа государственной власти субъекта Российской Федерации, а также органа местного самоуправления при осуществлении отдельных государственных полномочий, которая осуществляется по запросам заявителей в пределах установленных полномочий органов, предоставляющих государственные услуги [12].

Реестр государственный услуг (федеральных и муниципальных) (доступ ограничен) https://frgu.gosuslugi.ru.

Портал государственных услуг Российской Федерации (доступ свободный) https://gosuslugi.ru.

Показатели критерия политической значимости:

6. Прекращение1 или нарушение функционирования2 государственного органа в части невыполнения возложенной на него функции (полномочия).

Значения показателя: I категория – прекращение или нарушение функционирования Администрации Президента, Правительства, Федерального Собрания, Совета Безопасности, Верховного Суда, Конституционного суда РФ; II – категория прекращение или нарушение функционирования федерального органа государственной власти; III – прекращение или нарушение функционирования органа государственной власти субъекта РФ, города федерального значения.

Орган государственной власти (государственный орган) – это часть государственного аппарата, наделённая государственно-властными полномочиями и осуществляющая свою компетенцию по уполномочию государства в установленном им порядке

7. Нарушение условий международного договора РФ, срыв переговоров или подписания планируемого к заключению международного договора РФ, оцениваемые по уровню международного договора РФ.

Значения показателя: I категория – нарушение условий межгосударственного договора (срыв переговоров или подписания); II – нарушение условий межправительственного договора (срыв переговоров или подписания); III – нарушение условий договора межведомственного характера (срыв переговоров или подписания).

Международный договор РФ – международное соглашение, заключенное РФ с иностранным государством (или государствами), с международной организацией либо иным образованием, обладающим правом заключать международные договоры [13].

Показатели критерия экономической значимости:

В соответствии с полномочиями Федеральной службой по техническому и экспортному контролю (ФСТЭК России) [14] разработан проект методического документа «Рекомендации по оценке показателей критериев экономической значимости объектов КИИ РФ» [15, 16]. Документ детализирует порядок оценки показателей критериев экономической значимости объектов КИИ, проводимой в соответствии с Правилами категорирования объектов КИИ, утвержденными постановлением Правительства Российской Федерации от 8 февраля 2018 г. N 127. Проект методического документа предназначен для обеспечения единого подхода к оценке показателей критериев экономической значимости при проведении работ по категорированию объектов КИИ [16].

8. Возникновение ущерба субъекту КИИ, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов от годового объема доходов, усредненного за прошедший 5-летний период).

Значения показателя: I категория – более 20 (% годового дохода); II – более 10 (% годового дохода), но менее или равно 20 (% годового дохода); III – более или равно 1 (% годового дохода), но менее или равно 10 (% годового дохода).

Данный показатель применяется к субъектам КИИ: государственным корпорациям, государственным унитарным предприятиям, государственным компаниям, статистическим акционерным обществам, включенных в перечень стратегических предприятий и стратегических акционерных обществ, утвержденный Указом Президента РФ от 4 августа 2004 г. № 1009 [17].

9. Возникновение ущерба бюджетам РФ, оцениваемого в снижении выплат (отчислений) в бюджеты РФ, осуществляемых субъектом критической информационной инфраструктуры (процентов прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период).

Значения показателя: I категория – более 0,1 (% годового дохода); II – более 0,05 (0,005) (% годового дохода), но менее или равно 0,1 (% годового дохода); III – более 0,001 (% годового дохода), но менее или равно 0,05 (% годового дохода).

Показатель применяется к следующим субъектам КИИ: государственным органам, государственным учреждениям, российским юридическим лицам, индивидуальным предпринимателям [16].

10. Прекращение1 или нарушение2 проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством РФ системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемые среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций (млн. единиц) (расчет осуществляется по итогам года, а для создаваемых объектов - на основе прогнозных значений).

Значения показателя: I категория – более 120 (млн. единиц); II – более 70 (млн. единиц), но менее или равно 120 (млн. единиц); III – более 3 (млн. единиц), но менее или равно 70 (млн. единиц).

Данный показатель применяется к системно значимым кредитным организациям, операторам услуг платежной инфраструктуры, системно и (или) социально значимым платежным системам, к системно значимым инфраструктурам организации финансового рынка.

При оценке данного показателя используются следующие понятия и определения:

Оператор услуг платежной инфраструктуры – операционный центр, платежный клиринговый центр и расчетный центр [18].

Платежная система – совокупность организаций, взаимодействующих по правилам платежной системы в целях осуществления перевода денежных средств, включающая оператора платежной системы, операторов услуг платежной инфраструктуры и участников платежной системы, из которых как минимум три организации являются операторами по переводу денежных средств [18].

Значимая платежная система (системно значимая платежная система, социально значимая платежная система, национально значимая платежная система) – платежная система, отвечающая критериям, установленным Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе». Критерии признания платежной системы значимой установлены в указании Банка России [19].

Реестр значимых платежных систем, операторов услуг платежной инфраструктуры и операторов платежных систем размещен на официальном сайте Банка России [20].

Системно значимая кредитная организация – кредитная организация, которая признается в соответствии с Указанием Банка России от 22.07.2015 № 3737-У «О методике определения системно значимых кредитных организаций» системно значимой [19].

Банком России утвержден перечень следующих системно значимых кредитных организаций (по информации пресс-службы от 13 сентября 2017 г.): АО ЮниКредит Банк; Банк ГПБ (АО); БАНК ВТБ (ПАО); АО «АЛЬФА-БАНК»; ПАО Сбербанк; ПАО «Московский Кредитный Банк»; ПАО Банк «ФК Открытие»; ПАО РОСБАНК; ПАО «Промсвязьбанк»; АО «Райффайзенбанк»; АО «Россельхозбанк» (на долю системно значимых кредитных организаций приходится более 60% совокупных активов российского банковского сектора).

Системно значимая инфраструктурная организация финансового рынка – признанная Банком России системно значимой на основании критериев, установленных указанием Банка России от 25 июля 2014 г.

№ 3341-У «О признании инфраструктурных организаций финансового рынка системно значимым» [21].

Инфраструктурная организация финансового рынка – центральный контрагент, центральный депозитарий, расчетный депозитарий, саморегулируемая организация, клиринговая организация или биржа [21].

Банк России в течение 10 рабочих дней с даты принятия решения о признании ИОФР системно значимой размещает соответствующую информацию на официальном сайте Банка России (https://cbr.ru) и опубликовывает ее в «Вестнике Банка России».

Показатели критерия экологической значимости:

11. Вредные воздействия на окружающую среду, оцениваемые:

а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям;

Значения показателя: I категория – выход за пределы территории одного субъекта РФ или территории города федерального значения, с выходом вредных воздействий за пределы территории субъекта КИИ; II – выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта РФ или территории города федерального значения, с выходом вредных воздействий за пределы территории субъекта КИИ; III – в пределах территории одного муниципального образования или одной внутригородской территории города федерального значения, с выходом вредных воздействий за пределы территории субъекта КИИ.

б) по количеству людей, которые могут быть подвержены вредным воздействиям (тыс. человек).

Значения показателя: I категория – более или равно 5000 (5 млн. чел.); II – более или равно 1000

(1 млн. чел.), но менее 5000 (5 млн. чел.); III – более или равно 2 (2 тыс. чел.), но менее 1000 (1 млн. чел.).

Показатели критерия значимости для обеспечения обороны страны, безопасности государства и правопорядка:

12. Прекращение1 или нарушение функционирования2 (невыполнение установленных показателей) пункта управления (ситуационного центра), оцениваемые в уровне (значимости) пункта управления или ситуационного центра.

Значение показателя: I категория – прекращение или нарушение функционирования пункта управления государством или ситуационного центра Администрации Президента, Правительства, Федерального Собрания, Совета Безопасности, Верховного Суда, Конституционного Суда РФ; II – прекращение или нарушение функционирования пункта управления или ситуационного центра федерального органа государственной власти или государственной корпорации; III – прекращение или нарушение функционирования пункта управления или ситуационного центра органа государственной власти субъекта РФ или города федерального значения.

13. Снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом КИИ, оцениваемое:

а) в снижении объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции);

Значения показателя: I категория – более 15 (% объема продукции); II – более 10 (% объема продукции), но менее или равно 15 (% объема продукции); III – более 0 (% объема продукции), но менее или равно 10 (% объема продукции).

б) в увеличении времени выпуска продукции (работ, услуг) с заданным объемом (процентов установленного времени выпуска продукции).

Значения показателя: I категория – более 40 (% времени выпуска); II – более 10 (% времени выпуска), но менее или равно 40 (% времени выпуска); III – более 0 (% времени выпуска,) но менее или равно 10 (% времени выпуска).

14. Прекращение1 или нарушение функционирования2 (невыполнение установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, оцениваемые в максимально допустимом времени, в течение которого информационная система может быть недоступна пользователю (часов).

Значения показателя: I категория – менее или равно 1 (часа); II – менее или равно 2 (часов), но более 1 (часа); III – менее или равно 4 (часов), но более 2 (часов).

Заключение. Оценка показателей критериев значимости объектов КИИ позволяет постоянно действующей комиссии по категорированию субъекта КИИ принять решение по присвоению каждому из объектов КИИ одной из категорий значимости либо принять решение об отсутствии необходимости присвоения им одной из категорий значимости. В процессе принятия указанных решений комиссия должна руководствоваться требованиями рассмотренных в статье нормативных правовых актов и методических документов, регламентирующих порядок оценки показателей критериев значимости объектов КИИ.

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. Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
4. Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «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 ред. Постановления Правительства РФ от 13.04.2019 г. N 452).
5. Приказ ФСТЭК России от 6 декабря 2017 г. № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации».
6. Постановление Правительства РФ от 17 августа 2007 г. N 522 «Об утверждении Правил определения степени тяжести вреда, причиненного здоровью человека» (с изменениями и дополнениями).
7. Федеральный закон от 6 октября 2003 г. N 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» (с изменениями).
8. ГОСТ Р 51006-96 Услуги транспортные. Термины и определения.
9. Приказ Минтранса России от 21.02.2011 N 62 (ред. от 10.10.2013) «О Порядке установления количества категорий и критериев категорирования объектов транспортной инфраструктуры и транспортных средств компетентными органами в области обеспечения транспортной безопасности».
10. Федеральный закон от 9 февраля 2007 г. N 16-ФЗ «О транспортной безопасности» (с изменениями и дополнениями).
11. Федеральный закон от 7 июля 2003 г. №126-ФЗ «О связи» (с изменениями).
12. Федеральный закон от 27 июля 2010 г. N 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (с изменениями и дополнениями).
13. Федеральный закон от 15 июля 1995 г. N 101-ФЗ «О международных договорах Российской Федерации» (с изменениями и дополнениями).
14. Положение о Федеральной службе по техническому и экспортному контролю (утв. Указом Президента Российской Федерации от 16 августа 2004 г. N 1085 «Вопросы Федеральной службе по техническому и экспортному контролю»).
15. Информационное сообщение о разработке проекта методического документа ФСТЭК России «Рекомендации по оценке показателей критериев экономической значимости объектов критической информационной инфраструктуры Российской Федерации» от 16 февраля 2021 г. № 240/84/18.
16. Проект методического документа ФСТЭК России «Рекомендации по оценке показателей критериев экономической значимости объектов критической информационной инфраструктуры Российской Федерации» - Режим доступа: https://fstec.ru/teknicheskaya-zaschita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/338-proekty/ - Загл. с экрана.
17. Указ Президента РФ от 4 августа 2004 г. N 1009 «Об утверждении перечня стратегических предприятий и стратегических акционерных обществ» (с изменениями и дополнениями).
18. Федеральный закон от 27 июня 2011 г. N 161-ФЗ «О национальной платежной системе» (с изменениями и дополнениями).
19. Указание Банка России от 22.07.2015 № 3737-У «О методике определения системно значимых кредитных организаций».
20. Реестр платежных систем [Электронный ресурс]: база данных Банка России - Режим доступа: https://cbr.ru/PSystem/?PrtId=rops/ - Загл. с экрана.
21. Указание Банка России от 25 июля 2014 г. № 3341-У «О признании инфраструктурных организаций финансового рынка системно значимым».

ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И ТЕХНОЛОГИИ

УДК 004.056.5

ИССЛЕДОВАНИЕ ВОЗДЕЙСТВИЯ АТАК НА ТОЧКИ ДОСТУПА UBIQUITI NETWORKS

Бабков Иван Николаевич, Абраменко Георгий Тимофеевич, Коновалова Виктория Вадимовна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: ib9809@mail.ru, georgabramenko@gmail.com, konovalova.viktoriya.99@mail.ru

Аннотация. В статье рассматриваются атаки на беспроводные сети, соответствующие угрозам из банка данных угроз ФСТЭК России. Исследованы возможности эксплуатации уязвимостей, приводящих к реализации данных атак. В результате смоделированных атак, зафиксировано и оценено их влияние на точки доступа с помощью специальных средств мониторинга.

Ключевые слова: IEEE 802.11; Wi-Fi; безопасность беспроводных сетей; evil twin; dos; arp-spoofing.

A RESEACH OF THE IMPACT OF ATTACKS ON UBIQUITI NETWORKS ACCESS POINTS

Babkov Ivan, Abramenko Georgii, Konovalova Viktoria
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: ib9809@mail.ru, georgabramenko@gmail.com, konovalova.viktoriya.99@mail.ru

Abstract. The article discusses attacks on wireless networks that correspond to threats from the FSTEC of Russia threat databank. Possibilities of exploiting vulnerabilities leading to the implementation of these attacks have been investigated. As a result of simulated attacks, their impact on access points was recorded and evaluated using special monitoring tools.

Keywords: IEEE 802.11; Wi-Fi; wireless security; evil twin; dos; arp-spoofing.

Введение. Альтернативой кабельного решения для построения локальных сетей в настоящее время являются беспроводные локальные сети, использующие вместо кабеля — радиоэфир. В подавляющем большинстве случаев такие сети создаются как беспроводные локальные сети, основанные на стандартах IEEE 802.11. Технологии беспроводных локальных вычислительных сетей (Wireless Local Area Network – WLAN) развиваются с каждым днём и стали неотъемлемой частью жизни общества. WLAN открывают новые возможности для их пользователей – прежде всего мобильность терминалов и простоту изменения конфигурации сети. К достоинствам беспроводных сетей следует отнести: мобильность пользователей; отсутствие необходимости монтажа кабельной системы; простота подключения пользовательских устройств.

Даже крупные корпорации организуют свои сети с возможностью беспроводного подключения, в рамках концепции BYOD (Bring Your Own Device) [1]. Концепция подразумевает, что каждый сотрудник может принести и использовать своё собственное мобильное устройство для работы, а также использовать проводную или беспроводную сеть.

Не только в компаниях, но и в повседневной жизни люди сталкиваются с беспроводными сетями повсюду. Почти у каждого в доме установлен Wi-Fi роутер или точка доступа (ТД), также есть возможность подключения к бесплатным Wi-Fi сетям в ресторанах, гостиницах, в зданиях муниципалитета и даже в метро. Однако при этом необходимо учитывать проблему слабой защищенности беспроводных сетей. Так, например, согласно данным исследований Positive Technologies, 7 из 8 корпоративных беспроводных сетей были доступны за пределами контролируемой зоны, что потенциально позволяет проводить атаки [2]. Так как исследования работы ТД во время атак проводятся в рамках различных аудитов по информационной безопасности сети, зачастую, конкретные данные по таким исследованиям имеют ограниченный доступ.

Исследование работы точек доступа можно выполнить с помощью пентеста. Основная цель пентеста — подтвердить или опровергнуть риски несанкционированного доступа к защищаемой информации с помощью найденных уязвимостей. А главный принцип выполнения — обеспечить необходимую доказательность путем применения техник, методов и инструментария, используемых злоумышленниками. Зачастую злоумышленник

проникает во внутреннюю сеть атакуемой компании, используя внешние объекты в качестве опорной платформы для развития и расширения поверхности атаки. Большинство компаний не готовы отразить такие нападения. Тестирование на проникновение помогает предприятию выстроить эффективные процессы обеспечения безопасности. В связи с этим, существует необходимость изучения работы точек доступа в специально смоделированной среде, где не будет затронута ничья конфиденциальность.

Для исследования воздействия атак на точки доступа было выбрано оборудование от компании Ubiquiti Networks (UN), которое является довольно популярным в наше время. Согласно данным IDC за 2020 год Топ-3 производителей оборудования для локальных беспроводных сетей замыкает компания Ubiquiti, на которую пришлось 8,4% всех продаж [3].

В ходе работы, был организован лабораторный стенд с двумя точками доступа: UniFi AP-AC-Lite (UAP-AC-Lite) и NanoStation (NS) Loco M2. Также в состав стенда входят 2 машины с операционными системами: Kali Linux и Windows 7 с возможностью беспроводного подключения. Помимо этого, Windows 7 осуществляет управление UAP-AC-Lite через программный контроллер. Kali Linux в данной схеме играет роль нарушителя. Схема вышеописанного стенда представлена на рис. 1.

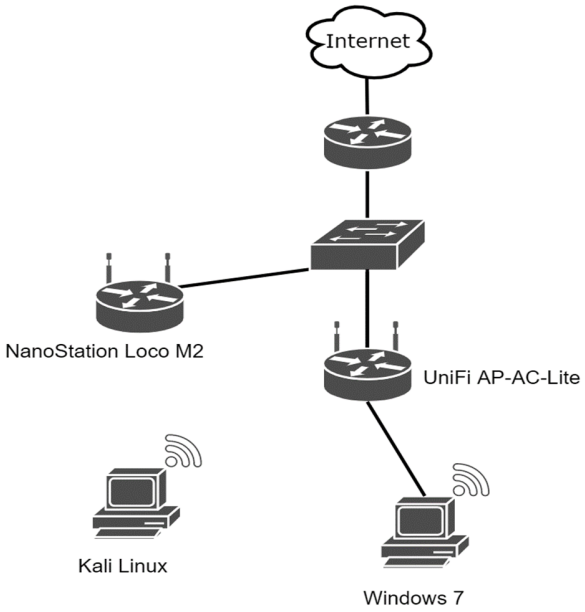


Рис. 1. Схема стенда тестируемой сети.

Для исследования уязвимостей точек доступа были выбраны следующие деструктивные атаки на Wi-Fi сети:

DoS (отказ в обслуживании), создается множество пакетов, которые тем или иным способом выводят из строя или замедляют работу точки доступа, что может привести к замедлению работы участка или всей сети.

Evil Twin (с англ. «злой двойник») подразумевает создание и использование мошеннической точки доступа с идентичными параметрами. Созданная паразитная точка доступа может забирать клиентов у существующей легитимной точки доступа [4].

ARP-Spoofing (с англ. «подмена ARP»), нарушитель осуществляет инъекцию пакетом, в результате чего изменяется запись в таблице ARP и перенаправляется весь трафик с точки доступа через нарушителя [5].

Приведенные выше атаки были выбраны в связи с простотой их реализации и их популярностью. Согласно данным Yandex.wordstat за последние 2 года количество запросов по выбранным типам атак не уменьшается, что доказывает их актуальность.

Помимо статистики запросов, в открытом доступе существует достаточно большое количество материала по беспроводным атакам, например, в [6].

Также, атаки Evil Twin и DoS соответствуют угрозам, приведенным в банке данных угроз ФСТЭК России: УБИ.126 «Угроза подмены беспроводного клиента или точки доступа» [7] и УБИ.140 «Угроза приведения системы в состояние «отказ в обслуживании» [8], соответственно. Частично к угрозе УБИ.126 можно отнести атаку ARP-Spoofing, в результате которой также возможно осуществление подмены беспроводного клиента или точки доступа.

Для моделирования атаки DoS на UAP-AC-Lite было отправлено с Kali Linux 1500 пакетов деаутентификации, чего было достаточно для введения точки доступа в состояние отказ в обслуживании.

Благодаря настроенным средствам мониторинга в программном контроллере (Unifi Controller v.5), удалось снять график загрузки ЦП (CPU), помимо этого на том же графике отражена загрузка оперативной памяти (Memory).

На рис. 2 отображены параметры загрузки CPU и Memory, снятые непосредственно с точки доступа через Unifi Controller.

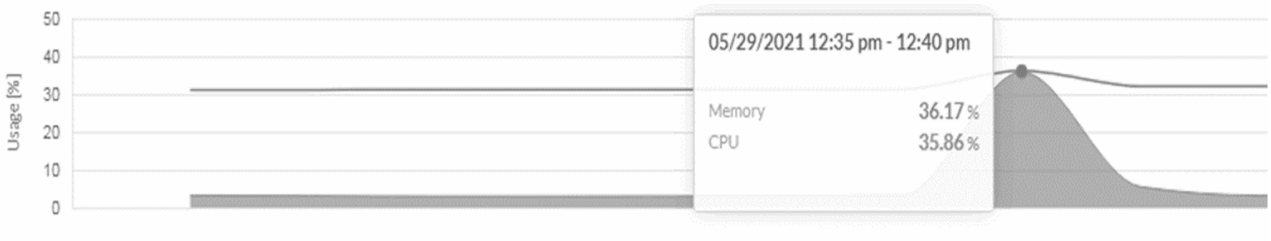


Рис. 2. Мониторинг загрузки CPU и Memory через Unifi Controller.

Как можно увидеть из графика, при атаке 5 пакетов в секунду на протяжении 5 минут было достаточным, чтобы перегрузить процессор почти на 36%, что ввело ТД в состояние «отказ в обслуживании».

В целях исследований было проведено несколько вариантов проведения атаки Evil Twin. В случае, когда контроллер обнаружил ТД только с идентичным именем (SSID), было выведено соответствующее предупреждение (рис. 3):

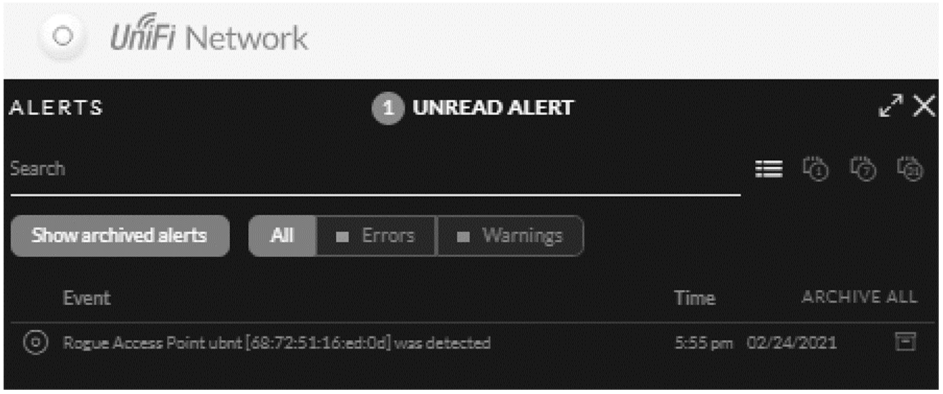


Рис. 3. Уведомление об обнаружении паразитной точки доступа.

Также удалось детектировать такой вариант атаки с помощью средств логирования. Записи об обнаружении представлены на рис. 4.

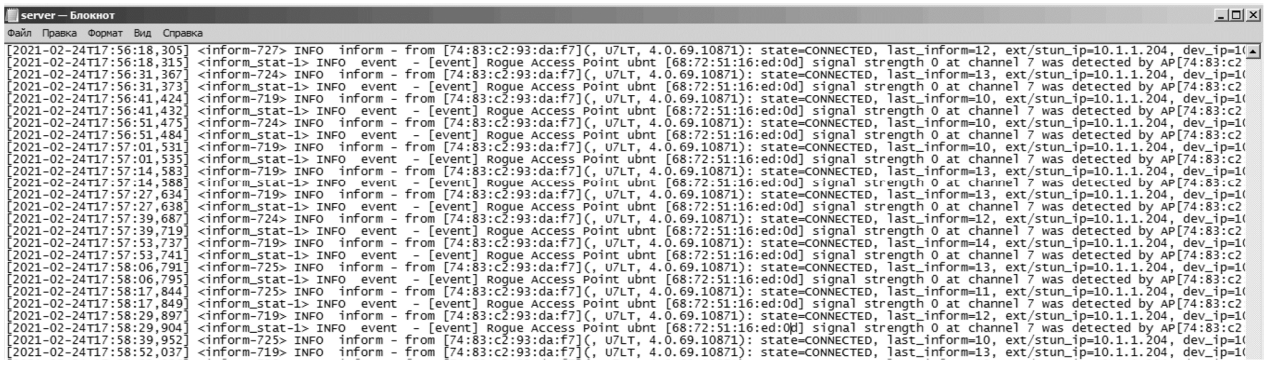


Рис. 4. Записи о детектировании паразитной точки доступа.

Влияние на точку доступа в таком варианте атаки Evil Twin не было зафиксировано. Но в других рассмотренных случаях, когда паразитная и легитимная точки доступа имели одинаковые параметры по безопасности (с паролем, и без него) и режиму шифрования, атака проходила успешно – все клиенты переходили к «злому двойнику».

Чтобы продемонстрировать влияние атаки, направленной на таблицу ARP, необходимо представить текущие параметры ARP таблицы, которые показаны на рис. 5.

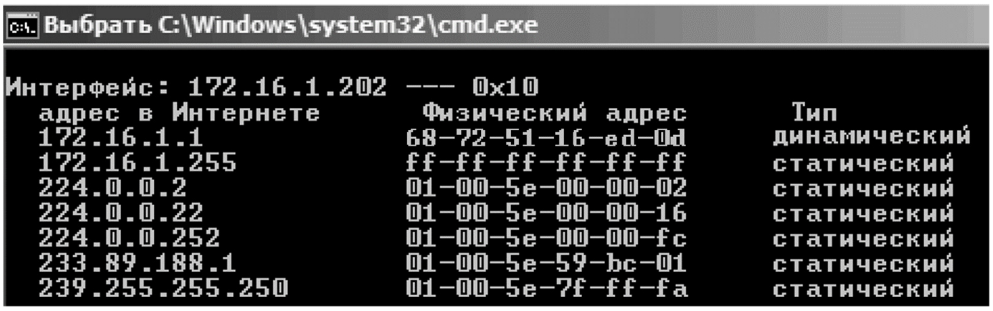


Рис. 5. Таблица ARP сети.

Нарушитель (Kali Linux), с помощью известных утилит осуществлял внедрение пакетов, благодаря которому удалось повлиять на таблицу ARP и внести MAC адреса нарушителя.

MAC адрес беспроводного интерфейса нарушителя представлен на рис. 6.

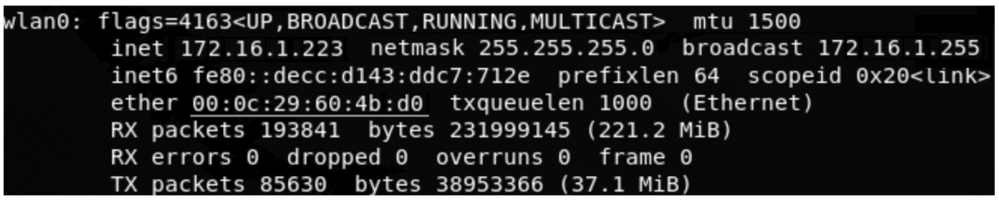


Рис. 6. Параметры интерфейсов нарушителя.

Результат успешной атаки представлен на рис. 7.

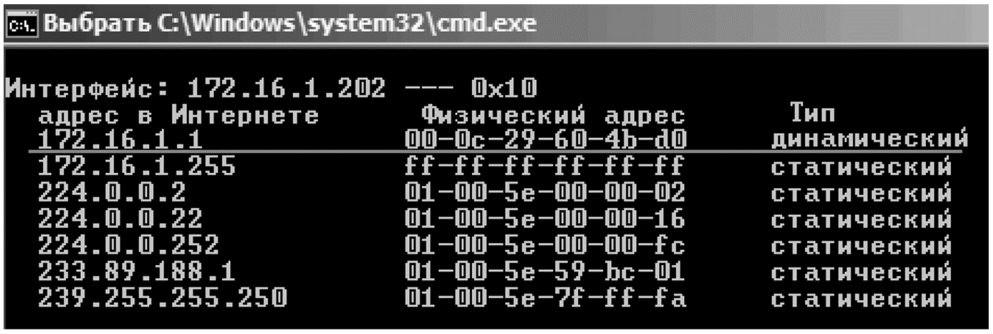


Рис. 7. ARP таблица после атаки.

Результатом такого изменения MAC адреса является изменение основного шлюза, что позволяет перенаправлять трафик через нарушителя, а затем на точку доступа. Данная атака называется «человек посередине» (man in the middle – MITM) [9]. В данном примере таким «человеком», прослушивающим весь трафик, являлась атакующая машина Kali Linux.

Вышеприведенная атака была осуществлена по беспроводному интерфейсу, но она также может использовать и проводной.

В качестве защиты от DoS атак можно дать следующие рекомендации:

IPS/IDS. Системы обнаружения и предотвращения вторжений в проводных сетях, которые способны отбрасывать излишние пакеты из беспроводных сетей. Как правило настройка осуществляется на маршрутизаторах и включается на точках доступа [10].

Стандарт 802.11w. Отдельный стандарт семейства IEEE, который позволяет защищать кадры управления, а именно: игнорирование сторонних пакетов с кадрами управления и отключение устройства из сети, если оно присылает больше, чем 1 пакет с управлением.

Мониторинг сетей и сетевых устройств. Позволяет отследить нагрузку на ЦП/ОЗУ ТД. В случае изменения нормальных данных, это может послужить сигналом о возможной атаке. Различные средства мониторинга могут быть как предустановленными (на программном контроллере, рис. 2), так и дополнительными, например, настройка протокола SNMP на сетевые устройства и выделенный сервер, на котором установлена ловушка SNMP, где собираются данные со всей локальной сети.

WIPS. Данная беспроводная система предотвращения вторжений отделяется от других систем, так как она может быть выделенной или гибридной беспроводной инфраструктурой сети. Основным преимуществом WIPS

является работа с трафиком в радиоэфире, тем самым обеспечивая более быструю реакцию на атаки, что критически важно для беспроводных устройств. Такая система будет детектировать и остальные рассмотренные в статье атаки.

Для защиты от атаки Evil Twin рекомендуется:

– Радио-мониторинг, который позволит обнаружить паразитную ТД, после чего администратор сети может принять соответствующие меры.

– Syslog или иные уведомления также могут сигнализировать об обнаружении паразитной ТД. В статье был рассмотрен вариант с программным контроллером, который вывел уведомление и сообщение (рис.3, рис. 4).

– Система WIPS, о преимуществах которой говорилось выше.

В качестве защиты от ARP-Spoofing рекомендуется:

– Изоляция клиентов (с целью защиты трафика между клиентами). В таком варианте сообщения от одного клиента не поступают остальным в локальной беспроводной сети.

– Мониторинг таблицы ARP на предмет новых записей или изменение параметров.

– Настройка систем мониторинга. Такими системами мониторинга могут являться: IDS, Syslog и другие специально настроенные системы.

Заключение. В целях проведения исследований был смоделирован лабораторный стенд с двумя точками доступа. Исследовано и проведена оценка влияния выбранных актуальных атак на ТД от компании UN. Лабораторный стенд возможно использовать в будущем для исследования влияния других атак на выбранное оборудование. Также, в рамках организованного стенда можно осуществлять лабораторные работы по дисциплине «Безопасность беспроводных сетей». Разработанный лабораторный стенд позволяет исследовать влияние атак на оборудование и методы защиты на участке или всей локальной сети. Стенд может быть организован как удаленно, так и локально, что позволит познакомиться с настройкой контрольных и не контроллерных точек доступа UN [11-13].

СПИСОК ЛИТЕРАТУРЫ

1. Красов, А. В., Рогова А. Н. Риски при реализации технологии BYOD в организациях и решения для их минимизации. Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. Т. 1. С. 506–510.
2. Positive Technologies. Уязвимости корпоративных информационных систем. [Электронный ресурс] URL: https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2019/?sphrase_id=88725 (дата обращения 3.06.2021).
3. Tadviser. Оборудование для беспроводных сетей (WLAN) мировой рынок [Электронный ресурс] URL: https://www.tadviser.ru/a/265124 (дата обращения 3.06.2021).
4. Ковцур М. М., Симанов М. С. Анализ особенностей организации авторизации пользователей в сетях коллективного доступа стандарта IEEE 802.11. Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 4. С. 537–541.
5. Инструменты Kali Linux. Атака на Wi-Fi [Электронный ресурс] URL: https://www.kali.tools/?tag=атака-на-wi-fi (дата обращения 5.06.2021).
6. Ковцур М. М., Кируга А. Ю., Ворошнин Г. Е., Федорова А. Э. Исследование атак authentication failure и Arp inject и методов их обнаружения в сетях семейства IEEE 802.11 // Информационные технологии и телекоммуникации. 2021. Т. 9. № 1. С. 87–98.
7. БДУ ФСТЭК России. УБИ.140 [Электронный ресурс] URL: https://bdu.fstec.ru/threat/ubi.140 (дата обращения 7.06.2021).
8. БДУ ФСТЭК России. УБИ.126 [Электронный ресурс] URL: https://bdu.fstec.ru/threat/ubi.126 (дата обращения 7.06.2021).
9. Козлов В. А., Рындюк В. А., Воробьев Г. А., Чернышев А. Б. Модели и методы защиты от атак «man in the Middle» (MITM). Современные фундаментальные и прикладные исследования. 2017. № 1(24). С. 27–35.
10. Зуев И. П., Карельский П. В., Ковцур М. М., Юркин Д. В. Разработка методики проведения испытаний IPS модулей. Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020): IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. Т.1. С. 492–496.
11. Бабков И. Н., Абраменко Г. Т., Храмцов Д. О., Оганесян А. Г. Оценка воздействия различных атак на точки беспроводного доступа Ubiquiti networks. Заметки ученого. 2021. Т.1 № 4. С. 67–70.
12. Александрова Е.С., Иванов Г.Н., Ковцур М.М. Анализ механизмов защиты Wi-Fi сетей. // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). С 47-51.
13. Петров В.А., Ковцур М.М., Кируга А.Ю. Исследование методов дальнометрии в беспроводных сетях. // REDS: Телекоммуникационные устройства и системы. С 42-49.

УДК 004.056.5

ТРЕБОВАНИЯ К ПОКАЗАТЕЛЯМ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫМИ СЕТЯМИ И ФОРМУЛИРОВКА ИХ ИНФОРМАТИВНОЙ ЗНАЧИМОСТИ

Башкирцев Андрей Сергеевич, Паращук Игорь Борисович, Беляев Сергей Валерьевич, Боголепов Григорий Сергеевич

Военная академия связи им. Маршала Советского Союза С.М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: ab098@yandex.ru, shchuk@rambler.ru, goshaceh@mail.ru, bogolepov@inbox.ru

Аннотация. Рассмотрен комплекс современных требований к защищенности автоматизированных систем управления телекоммуникационными сетями. Проведен анализ общих требований к показателям защищенности,

выполнение которых призвано обеспечить своевременное и устойчивое управление защитой информации, циркулирующей в системах контроля и мониторинга телекоммуникационных сетей в современных условиях. Показано, что на основе оценок относительной информативности требований к безопасности информации могут быть сформированы требования к показателям защищенности АСУ ТКС, причем с учетом их адаптации при изменении внешних условий функционирования и разработки системы.

Ключевые слова: требования; защищенность; показатель; автоматизированная система управления; телекоммуникационная сеть; информативность; идентификация; ранжирование.

REQUIREMENTS FOR SECURITY INDICATORS OF AUTOMATED TELECOMMUNICATIONS NETWORK MANAGEMENT SYSTEMS AND THEIR FORMULATION THEIR INFORMATIVE SIGNIFICANCE

Bashkirtsev Andrey, Parashchuk Igor, Belyaev Sergey, Bogolepov Grigory
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: ab098@yandex.ru, shchuk@rambler.ru, goshaceh@mail.ru, bogolepov@inbox.ru

Abstract. The complex of modern requirements for the security of automated control systems of telecommunications networks is considered. The analysis of the general requirements for security indicators, the implementation of which is designed to ensure timely and sustainable management of the protection of information circulating in the control and monitoring systems of telecommunications networks in modern conditions, is carried out. It is shown that on the basis of estimates of the relative informativeness of information security requirements, requirements for the security indicators of the automated control system can be formed, taking into account their adaptation to changes in the external conditions of the system operation and development.

Keywords: requirements; security; indicator; automated control system; telecommunications network; informative significance; identification; ranking.

Введение. Автоматизированные системы управления (АСУ) телекоммуникационными сетями (ТКС) призваны повысить качество функционирования ТКС, повысить своевременность и обоснованность принятия решений администратором сети, их деятельность служит снижению численности управленческого персонала и улучшению качества управления сетями такого класса в целом [1, 2].

Автоматизированные системы управления должны обеспечивать достижение целей создания, развития и функционирования сложных управляемых ТКС, причем надежность и адаптивность АСУ должны быть достаточными для достижения установленных целей функционирования ТКС в заданном диапазоне изменений условий применения. Помимо этого, в АСУ ТКС должны быть предусмотрены контроль правильности выполнения автоматизируемых функций и диагностирование с указанием места, вида и причины возникновения нарушений правильности функционирования автоматизированной системы [3].

Данная система управления должна в автоматизированном режиме выполнять: сбор, обработку и анализ информации (сигналов, сообщений, документов и т.п.) о состоянии ТКС; выработку управляющих воздействий (программ, планов и т.п.); передачу управляющих воздействий (сигналов, указаний, документов) на исполнение и ее контроль; реализацию и контроль выполнения управляющих воздействий, а также обмен информацией (документами, сообщениями и т.п.) с взаимосвязанными автоматизированными системами [4].

Важным элементом системы требований к АСУ ТКС являются требования по защищенности информации, циркулирующей в системах такого класса. В АСУ ТКС объектами защиты являются: информация (данные) о параметрах (состоянии) управляемой ТКС или процесса (входная и выходная информация, управляющая (командная) информация, контрольно-измерительная информация, иная критически важная (технологическая) информация); программно-технический комплекс, включающий технические средства (в том числе автоматизированные рабочие места, серверы, телекоммуникационное оборудование, каналы связи, программируемые логические контроллеры, исполнительные устройства), программное обеспечение (в том числе микропрограммное, общесистемное, прикладное), а также средства защиты информации в телекоммуникационных сетях [5].

Защищенность АСУ ТКС достигается путем разработки и реализации в рамках системы защиты автоматизированной системы управления совокупности организационных и технических мер, направленных на блокирование (нейтрализацию) угроз безопасности информации, реализация которых может привести к нарушению штатного режима функционирования системы, управляемой ТКС и (или) процесса, на локализацию и минимизацию последствий от возможной реализации угроз безопасности информации, восстановление штатного режима функционирования автоматизированной системы управления в случае реализации угроз безопасности информации.

При формулировке состава и физической сущности показателей защищенности (ПЗ) АСУ ТКС с учетом потенциальных угроз безопасности информации, должны быть приняты во внимание структурно-функциональные характеристики АСУ ТКС, включающие наличие уровней автоматизированной системы управления, состав автоматизированной системы управления, физические, логические, функциональные и технологические

взаимосвязи в системе, взаимодействие с иными автоматизированными или информационными системами и информационно-телекоммуникационными сетями, режимы функционирования АСУ, а также иные особенности ее построения и функционирования.

Показатели защищенности АСУ ТКС в полной мере определяются качеством проектирования и построения подсистемы, призванной осуществлять защиту АСУ ТКС. При этом в состав ПЗ АСУ ТКС должны быть включены показатели, физически характеризующие и численно аттестующие:

– типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и типы объектов доступа, являющихся объектами защиты в АСУ ТКС (автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, программируемые логические контроллеры, исполнительные устройства, иные объекты доступа);

– методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа к объектам (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в АСУ ТКС;

– меры защиты информации, подлежащие реализации в рамках подсистемы защиты АСУ ТКС;

– параметры программирования и настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей АСУ ТКС;

– виды и типы средств защиты информации, обеспечивающие реализацию технических мер ее защиты;

– структура подсистемы защиты АСУ ТКС, включая состав (количество) и места размещения ее элементов;

– средства защиты информации с учетом их стоимости, совместимости с программным обеспечением и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности автоматизированной системы управления;

– меры защиты информации при информационном взаимодействии с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями [6].

Подсистема защиты АСУ ТКС является основой обеспечения защищенности соответствующей автоматизированной системы, поэтому поиск и разработка адекватных методов, позволяющих сформулировать требования к показателям качества подсистемы защиты и к ПЗ АСУ ТКС, с учетом эволюции в средствах защиты и телекоммуникациях, является, по-прежнему, актуальной задачей [7].

Актуальность этой задачи также объективно связана с тем, что существующие методы обоснования требований к ПЗ АСУ ТКС, как правило, используют математические методы аддитивной свертки и методы параметрической и структурной декомпозиции. Данные методы имеют ряд преимуществ, но не позволяют адаптивно, в динамике совершенствовать систему требований к ПЗ АСУ ТКС в случае изменения требований системы управления к защищенности системы связи, что, в конечном итоге, приводит к необходимости разработки новой системы таких требований.

Таким образом, на наш взгляд, своевременной и важной является задача разработки методического аппарата, обеспечивающего определение требуемой номенклатуры и объема требований к ПЗ АСУ ТКС, а также учитывающего особенности эксплуатации подсистемы защиты АСУ ТКС и разработки ее элементов.

Учитывая, что задача оптимизации номенклатуры и объема системы ПЗ АСУ ТКС и процесса автоматизированного управления защитой информации, является задачей сокращения размерности множества данных с помощью выявления определенного числа основных факторов, размерностей, кластеров и т.д., которые могут объяснить изменчивость результативности защиты АСУ, ее решение может и должно строиться на основе математических методов редукции с учетом наличия корреляционных связей между показателями защищенностями (параметрами).

Другими словами, в основу формулировки задачи положено доказательство истинности или ложности научной гипотезы – существует ли возможность построения на имеющемся множестве показателей защищенности (параметров) сколько-нибудь разумной и полезной системы их отношений с состоянием защищенности АСУ ТКС и процесса автоматизированного управления защитой информации. При этом известно, что построение таких отношений возможно на основе формулировки соответствующих моделей, которые ориентированы на традиционные задачи классификации.

Классификация, в нашем случае, является своеобразной «сверткой» исходных информационных признаков защищенности АСУ ТКС, поскольку число идентифицируемых классов всегда меньше, чем уникальных объектов. Иными словами, в результате получаем небольшое по размеру, наглядное и рациональное представление данных (признаков) в пространстве существенно меньшей размерности, чем исходное. Именно поэтому математические методы редукции пространства признаков (требований) являются одним из наиболее эффективных средств решения задач классификации и ранжирования показателей защищенности (параметров защищенности) АСУ ТКС.

Примером одного из современных подходов к решению задач классификации и ранжирования является подход, в основе которого реализуются механизмы ранжирования по информативной значимости. Ранжирование требований к ПЗ АСУ ТКС по информативной значимости позволяет снять неопределенность наблюдаемого

(моделируемого, описываемого) состояния защищенности системы управления, которая количественно характеризуется энтропией этого состояния [8].

Если предположить, что вектор требований $\vec{W}_{<m>}$ полностью определяет сущность (облик состояния) защищенности АСУ ТКС, то, используя описанное в работах [9, 10] свойство, заключающиеся в том, что энтропия совокупности независимых величин равна сумме энтропии этих величин, справедливо записать:

$$H_{\Sigma} = \sum_{m=1}^{M} H_m(W), \tag{1}$$

где H_{Σ} – энтропия состояния защищенности АСУ ТКС, $H_m(W)$ – безусловная энтропия *m*-го требования к ПЗ АСУ ТКС, *m* = 1, … , *M* – число требований к ПЗ АСУ ТКС.

Тогда количество информации о состоянии защищенности АСУ ТКС (информативность) $I_m(W_m, \Sigma)$, которую несет *m*-ое требование к ПЗ, можно записать:

$$I_m(W_m, \Sigma) = H_{\Sigma} - H_m(\Sigma / W_m), \tag{2}$$

где $H_m(\Sigma / W_m)$ – условная энтропия состояния защищенности АСУ ТКС после задания требования W_m.

Основной аспект определения информативной значимости требований к ПЗ АСУ ТКС – формулировка и задание требований к защищенности следует начинать с требования W_m, которое обладает максимальным количеством информативности (несет максимальное количество информации) $I_m^{\max}$, при этом энтропия по *m*-му требованию определяется в соответствии с выражением [10]:

$$H_m(W) = -\int_{-\infty}^{+\infty} f(W_m) \log_2 f(W_m)\, dW_m, \tag{3}$$

где $f(W_m)$ – функция распределения по *m*-му требованию. Так как функция распределения $f(W)$ почти всегда определяется как многоугольник вероятностей, выражение (3) может быть представлено в виде [9, 10]:

$$H_m(W) = -\sum_{1}^{n} p_i \log_2 p_i, \tag{4}$$

где p_i – вероятность совпадения требования W_m с *i*-м интервалом диапазона его значений.

Второй, не менее важный аспект определения информативной значимости требований к ПЗ АСУ ТКС – требования можно выбирать по критерию минимума величины энтропии. При этом, поскольку распределение $f(W_m)$ почти всегда подчинено нормальному закону, энтропия отдельного требования, согласно (3), равна [10]:

$$H_m(W) = -\frac{1}{\sqrt{2\pi D_{W_m}}} \int_{-\infty}^{+\infty} \left[\exp\left(\frac{W_m^2}{2D_{W_m}} \right) \right] \left(-\frac{1}{2} \log_2 2\pi D_{W_m} - \frac{W_m^2}{2D_{W_m}} \log_2 2\pi D_{W_m} \right) dW_m, \tag{5}$$

где D_{W_m} – дисперсия *m*-го требования к показателям защищенности АСУ телекоммуникационными сетями.

Физический смысл выражения (5) состоит в упорядочении требований к ПЗ АСУ ТКС по степени информативности, причем это упорядочение осуществляется по величине дисперсии распределения требований.

Очевидно, что меньше дисперсия требований D_{W_m}, тем плотнее распределение и тем больше вероятность того, что требования принадлежат к одному классу, характеризующему определенное состояния защищенности АСУ ТКС. Чем больше дисперсия требований D_{W_m}, тем менее коррелированными являются задаваемые требования к ПЗ АСУ ТКС с результативностью управления защищенностью систем такого класса.

Этот метод может быть использован при вероятностном прогнозировании результативности защиты информации в АСУ ТКС, когда идентифицируются и оцениваются значения дисперсий подпроцессов прогнозируемого процесса автоматизированного управления защитой информации.

Полученное в результате упорядочения требований к ПЗ АСУ ТКС и их выбора по степени информативности суммарное количество информации $I_M(z_M, \Sigma)$, которое содержит совокупность задаваемых требований к ПЗ (W_1, W_2, … , W_m , … , W_M), может быть представлено в виде [10]:

$$I_M(z_M, \Sigma) = I_{z_1} + I_{z_2} \ldots + I_{z_m} \ldots + I_{z_M}, \tag{6}$$

где I_{z_m} – количество информации (информативность) *m*-го требования к показателям защищенности АСУ телекоммуникационными сетями.

В результате упорядочения требований и их выбора по степени информативности, с учетом влияния требований к ПЗ АСУ ТКС на результативность автоматизированного управления защитой информации, может быть получена матрица относительной информативной значимости требований к показателям защищенности АСУ телекоммуникационными сетями.

После определения относительной информативной значимости каждого требования к показателям защищенности АСУ телекоммуникационными сетями, осуществляется реорганизация модели зависимостей. При этом относительно требования с наибольшим значением *I*, матрица делится на две части таким образом, что столбцы, в которых отмечена зависимость свойств от данного требования, переносятся в левую часть, другие в правую. В дальнейшем рассчитывается относительная информативность применительно к сформированной матрице.

При этом относительная информативность каждого требования к показателям защищенности АСУ телекоммуникационными сетями на втором шаге определяется как сумма относительной информативности левой и правой части матрицы зависимостей. Проведение итерационных вычислений позволяет провести ранжирование требований относительно их информативной значимости. Расчеты показывают, что уже на седьмом шаге итераций значения относительной информативности требований к ПЗ АСУ ТКС становятся неразличимыми между собой.

Заключение. Таким образом, рассмотрен комплекс современных требований к защищенности автоматизированных систем управления телекоммуникационными сетями. Проведен анализ общих требований к показателям защищенности, выполнение которых призвано обеспечить своевременное и устойчивое управление защитой информации, циркулирующей в системах контроля и мониторинга телекоммуникационных сетей в современных условиях.

Показано, что на основе оценок относительной информативности требований к безопасности информации могут быть сформированы требования к показателям защищенности АСУ ТКС, причем с учетом их адаптации при изменении внешних условий функционирования и разработки системы.

Тем самым может быть решена задача определения объема и номенклатуры требований к показателям защищенности АСУ ТКС. Эта задача может и должна быть сформулирована и решена, как задача многокритериального ранжирования по информативности исходной совокупности требований, описывающих защищенность АСУ при ограничениях на ресурсы, необходимые на реализацию и вероятность достижения требуемой результативности процесса обеспечения защищенности автоматизированного управления современными сетями связи.

Помимо этого, результаты решения данной задачи, по мнению авторов, позволят повысить адекватность и достоверность описания тех существенных свойств подсистем защиты информации, которые, в целом, и определяют их качество.

СПИСОК ЛИТЕРАТУРЫ

1. Межгосударственный стандарт ГОСТ 34.003-90 Автоматизированные системы. Термины и определения. – М.: Стандартинформ, 1992. –14 с.
2. Межгосударственный стандарт ГОСТ 24.104-85 Единая система стандартов автоматизированных систем управления. Автоматизированные системы управления. Общие требования. – М.: Стандартинформ, 1985. – 23 с.
3. Ермолаева В.В., Калашников Д.А. Автоматизированные системы управления // Молодой ученый. №11. 2016. С. 166-168.
4. Паращук И.Б., Башкирцев А.С., Ногин С.Б. Динамическая оптимизация параметров контроля в интересах управления связью между различными информационно-аналитическими и вычислительными системами // Естественные и технические науки. №4 (94), 2016. С. 24-28.
5. Приказ ФСТЭК России от 14 марта 2014 года №31. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. (с изменениями на 9 августа 2018 года). – М.: ФСТЭК. 2014. – 28 с.
6. Башкирцев А.С., Митрофанов Е.А., Паращук И.Б. Автоматизированные системы управления телекоммуникационными сетями: обзор и анализ современных требований // Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020) «. Санкт-Петербург, 28-30 октября 2020 г.: Материалы конференции. Часть 1. \ СПОИСУ. – СПб.: 2020. – 393 с., С. 63-65.
7. Башкирцев А.С., Митрофанов Е.А., Паращук И.Б. Анализ требований к автоматизированным системам управления телекоммуникационными сетями. // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 8. – СПб.: СПОИСУ, 2020. – 474 с. С. 91-95.
8. Корлякова М.О., Твердохлеб Н.О. Анализ подходов к определению информативности признаков // Научная сессия МИФИ-2006. Т.3 Интеллектуальные системы и технологии, – М.: МИФИ, 2006. С. 146-147.
9. Федоров В.К., Сергеев Н.П., Кондрашин А.А. Контроль и испытание в проектировании и производстве радиоэлектронных средств. – М.: Техносфера, 2005. – 563 с.
10. Гаскаров Д.В., Голинкевич Т.А., Мозгалевский А.В. Прогнозирование технического состояния и надежности аппаратуры. – М.: Советское радио, 1974. – 224 с.

УДК 004.75

ДЕТЕКТИРОВАНИЕ АНОМАЛЬНОГО ПОВЕДЕНИЯ УСТРОЙСТВ УМНОГО ДОМА С ПРИМЕНЕНИЕМ ПАТТЕРНОВ ПОВЕДЕНИЯ

Богданов Павел Юрьевич
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, Санкт-Петербург, 190000, Россия
e-mail: 45bogdanov@gmail.com

Аннотация. В статье приведен подход к детектированию аномального поведения сенсорного устройства. Суть подхода заключается в подготовке эталонного шаблона – паттерна поведения сенсорного устройства. Роль паттернов могут выполнять плотности распределения различных характеристик исходящего от сенсорного устройства трафика:

длина передаваемых пакетов данных, время задержки передачи пакетов данных и другие. На вычислительном устройстве остается сравнить реальное поведение сенсорного устройства с паттерном.

Ключевые слова: интернет вещей; сенсорное устройство; атака; детектирование атаки; паттерн поведения.

DETECTING ANOMALOUS BEHAVIOR OF SMART HOUSE DEVICES USING BEHAVIOR PATTERNS

Bogdanov Pavel
Saint Petersburg State University of Aerospace Instrumentation
67 Bolshaya Morskaya St, St. Petersburg, 190000, Russia
e-mail: 45bogdanov@gmail.com

Abstract. The paper describes an approach to detecting anomalous behavior of a sensor device. The essence of the approach is to prepare a reference template - a pattern for the behavior of a sensor device. The role of patterns can be played by the distribution densities of various characteristics of the traffic outgoing from the sensor device: the length of the transmitted data packets, the delay time of the data packet transmission, and others. On the computing device, it remains to compare the real behavior of the sensor device with the pattern.

Keywords: internet of things; touch device; attack; attack detection; pattern of behavior.

Введение. Решения безопасности инфокоммуникационных сетей реализуются средствами систем обнаружения атак (СОА). Для сетей интернета вещей (IoT), сложно организовать защиту, аналогичную для компьютерных инфраструктурных сетей из-за ограничений по энергопотреблению [1].

СОА для интернета вещей можно реализовать для мощных компьютеров или даже серверов на границе среды IoT, и она действует как первая линия защиты для всех устройств в среде IoT. Однако развертывание консолидированной СОА, которая работает в любой среде IoT, является сложной задачей, поскольку эти разнородные интеллектуальные объекты имеют разные характеристики, и трафик, генерируемый этими устройствами, отличается (т. е. трафик законных устройств IoT в данной среде IoT может отличаться от трафика, генерируемого законными устройствами Интернета вещей в другой среде Интернета вещей) [2].

С учетом этих проблем, предлагается следующее решение для системы типа умный дом, состоящей из гетерогенных IoT-устройств.

Постановка задачи. В процессе функционирования для каждого устройства интернета вещей возникает последовательность событий, которые характеризуются значениями наборов метрик [3]. В дискретные моменты времени регистрируются значения метрик IoT-устройств, которые можно рассматривать как временные ряды.

Пусть процесс передачи данных от сенсорного устройства за раунд представляет собой случайную векторную функцию

$$X(t)=f(M(t),h(t)),\ t_0\le t\le t_k, \tag{1}$$

где $X(t)$ – наблюдаемая последовательность данных;

$M(t)$ – метрика объема передаваемых данных;

$h(t)$ – шумовая составляющая.

Определим множество состояний $S=\{s_0, s_1, \ldots, s_n\}$, в одном из которых в дискретный момент времени t_i может находится устройство. Метрика фиксируются в дискретные моменты времени $t_i,\ i=\overline{0,k}$ временного ряда $x_i=X(t_i)$, так что $M_i=M(t_i)$.

Известно множество $P=\{p_0, p_1, \ldots, p_n\}$ паттернов поведения Iot-устройств в каждом из состояний, в которых пребывает устройство во время раунда сенсорной сети.

Паттерн поведения может быть разным: загрузка процессора и/или памяти устройства, число отправляемых пакетов, размеры пакетов, плотность распределения вероятностей временных задержек передачи/приема пакетов в каждом из $s_j,\ j=\overline{0,n}$ состояний.

В качестве показателя, указывающего на аномальное (нестандартное) поведение устройства берется расстояние $d(p,p')$ между паттерном и реальным поведением. Таким образом при детектировании аномального поведения сенсорного устройства в системе умного дома необходимо создать базу данных паттернов $p_0, p_1, \ldots, p_n$ поведения для каждого IoT-устройства и найти алгоритм A: $P \to S$, отражающий множество P во множество S.

Разбивая множество S на два подмножества нештатных $S1$ и штатных $S2$ состояний соответственно, решающее правило $\dot{R}\Leftrightarrow d(p,p')$ для алгоритма A и ставит в соответствие наблюдению $X(t)$ одного из множеств $S1$ или $S2$

$$\dot{R}=\begin{cases} S1, \text{ при } d \ge d_{\text{доп}} \\ S2, \text{ при } d < d_{\text{доп}} \end{cases}, \tag{2}$$

где $d_{\text{доп}}$ – пороговое значение.

На рис.1 приведен снимок состояния порта 100, на который совершалась Dos-атака утилитой hping3: на протяжении 4 с лишним минут генерировалось более 1 миллиона пакетов со стандартным размером 120 байт (общий объем 150 Мбайт)

```
hping3 -V -c 1000000 -d 120 -S -w 64 -p 100 --flood 192.168.100.3
```

Как видно из рис.1 Dos-атака произошла на второй минуте, продолжалась около 2-х минут, сгенерировано более 1,5 миллионов пакетов, из которых 1 миллион – это пакеты, несущие Dos-атаку.

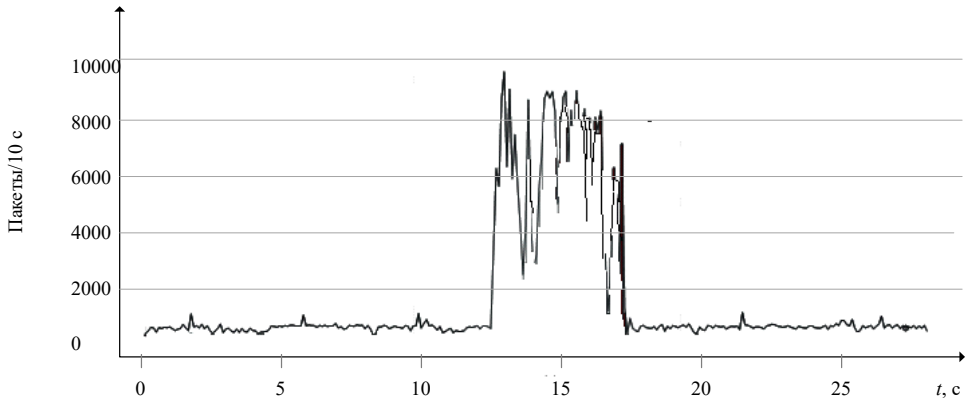


Рис.1. Снимок состояния порта 100.

Таким образом в роли паттерна поведения любого узла сенсорной сети могут выступать, как нагрузочные характеристики, так и статистические характеристики временного ряда, отображающего функционирование устройства [4, 5].

Очевидно, что статистические характеристики плотности распределения вероятностей временных задержек могут являться паттерном поведения сенсорного устройства. Во-первых, данная характеристика показывает реальную нагрузку сенсорного устройства во времени, и во-вторых, само распределение уже является паттерном поведения. Решающим правилом для алгоритма в таком случае является проверка статистической гипотезы о функции распределения вероятностей временных задержек, пороговое значение $d_{доп}$ является статистическим критерием, например хи-квадрат, 3σ или другой.

Данное предложение по построению паттерна возникло в результате анализа трафика умных устройств. Например, для умной розетки Xiaomi ряд экспериментов по передаче данных с розетки на смартфон (состояние s_1) и со смартфона на розетку (состояние s_2) по каналу Bluetooth позволили аппроксимировать функции распределения временных интервалов. Состояния s_1 и s_2 соответствуют активному режиму работы розетки. В активном режиме розетка в случайные моменты времени принимает запросы на включение/отключение, после чего переходит в фоновый режим. В фоновом режиме розетка не получают запросов. Таким образом, розетка может находится в трех состояниях:

- состояние s_0 – соответствует фоновому режиму.
- состояние s_1 – соответствует активному режиму, розетка отправляет данные.
- состояние s_2 – соответствует активному режиму, розетка принимает данные.
- сенсорные устройства начинают передачу данных только по запросу головного узла. Время отдельного опроса – временной интервал, который разделен на блоки – окна. Размер окон определяется количеством слотов, на которые они делятся. Размер слота – фиксированная величина для каждого сенсорного устройства. Так как слот – это тоже временной интервал, его размер определяется скоростью передачи данных от СУ до узла, т. е. его определяет оборудование, используемое в системе [6].

В начале процесса узел посылает сигналы «опроса» всем СУ, которые находятся в зоне его покрытия. В этих сигналах содержится время начала доступа и продолжительность, то есть количество слотов. СУ, приняв эти сигналы, случайным образом выбирают слот, в котором будут передавать свои данные.

В процессе доступа в слоте возможно возникновение трех состояний:

- пусто – в том случае, когда ни одно из СУ не выбрала текущий слот для передачи данных;
- успех – когда только одно СУ передает данные в текущем слоте;
- конфликт (коллизия) – когда более одного СУ начинают передавать данные в текущем слоте.

Опрос СУ, находящихся в зоне покрытия головного узла, заканчивается, когда в окне появляются только слоты с успешной передачей и пустые слоты.

На рис. 1 приведен временной ряд числа отправляемых пакетов розеткой Xiaomi. На его основе построена плотность распределения вероятностей временных задержек отправки пакетов розеткой Xiaomi (рис. 2).

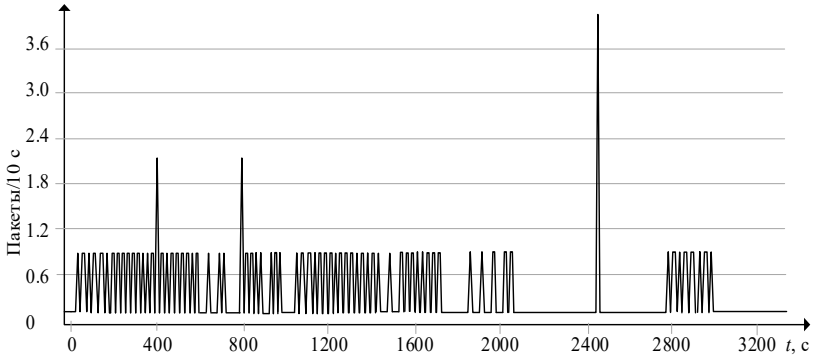


Рис. 1. Временной ряд отправляемых пакетов данных от розетки.

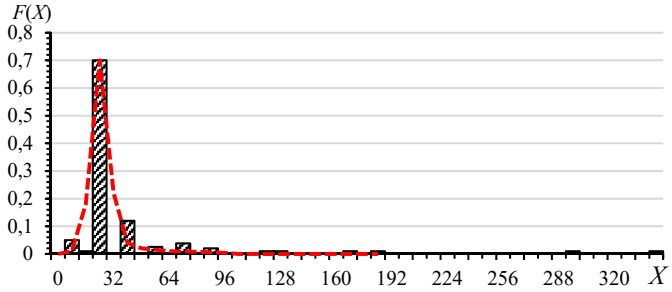


Рис. 2. Плотность распределения вероятностей временных задержек отправляемых пакетов данных от розетки.

Плотность распределения вероятностей временных задержек отправляемых от розетки пакетов данных аппроксимируется функцией логистического распределения с параметрами $\alpha = 8{,}4$; $\beta = 21$.

$$F(x,\alpha,\beta) = \frac{x^{\beta}}{\alpha^{\beta} + x^{\beta}}, \tag{3}$$

На рис. 3 приведен временной ряд числа принимаемых розеткой Xiaomi пакетов. На его основе построена плотность распределения вероятностей временных задержек, принимаемых розеткой Xiaomi пакетов (рис. 4).

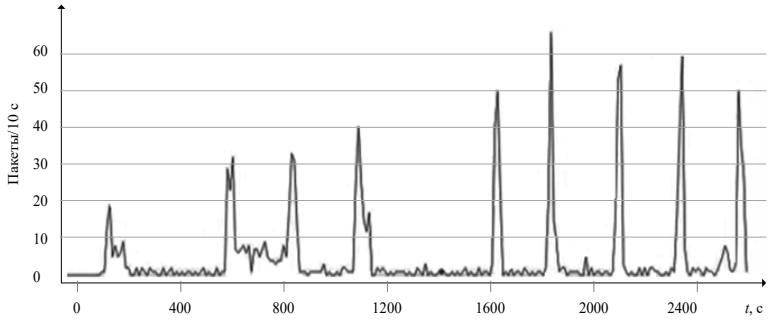


Рис. 3. Временной ряд пакетов данных, получаемых розеткой.

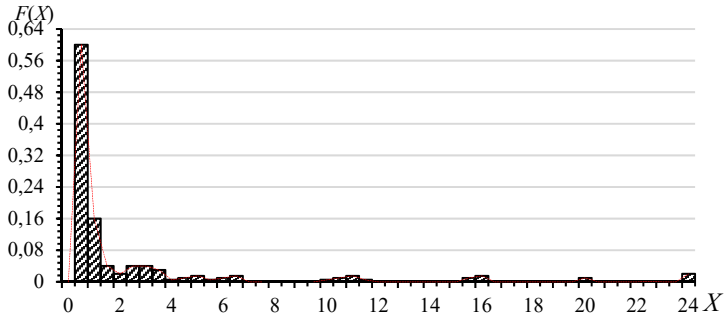


Рис. 4. Плотность распределения вероятностей временных задержек получаемых розеткой пакетов данных.

Плотность распределения вероятностей временных задержек принимаемых розеткой пакетов аппроксимируется функцией логнормального распределения с параметрами σ=2,8704; μ=-6,7315

$$F(x,\mu,\sigma)=\Phi\left(\frac{\ln x-\mu}{\sigma}\right). \quad (4)$$

Диаграмма, демонстрирующая процесс детектирования аномального поведения при взаимодействии «СУ– Сервер» и «Сервер – СУ» приведена на рис. 3.

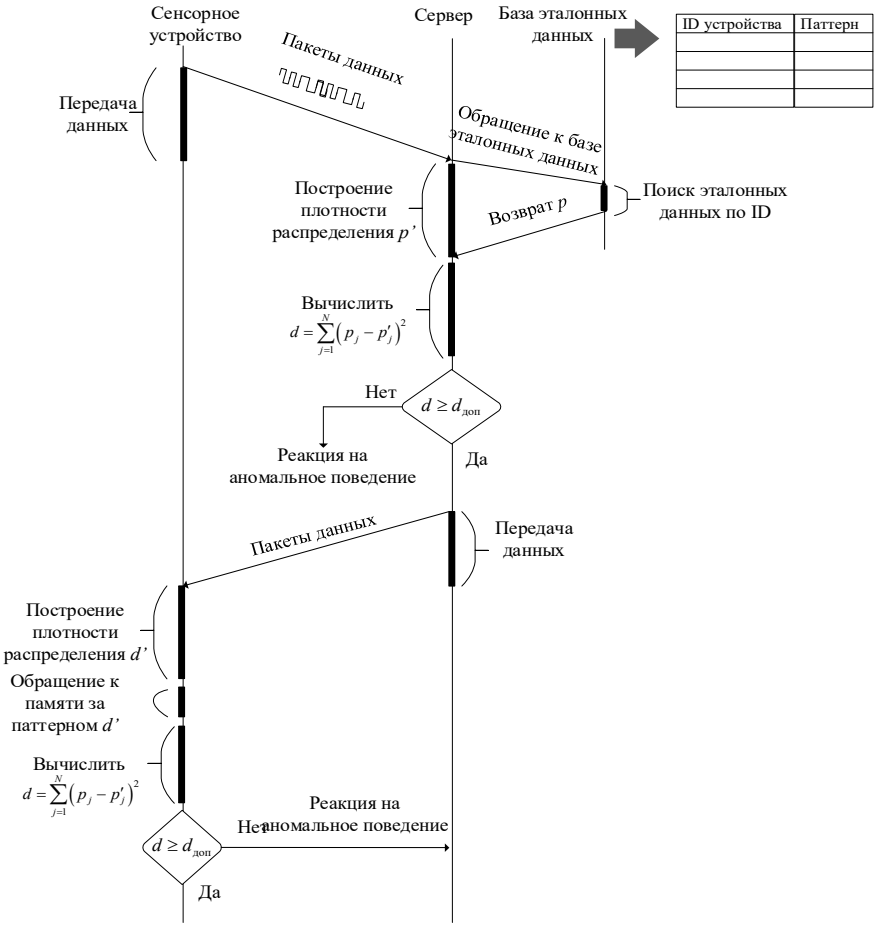


Рис. 3. Диаграмма процесс детектирования аномального поведения при взаимодействии «СУ– Сервер» и «Сервер – СУ».

Заключение. Обнаружение сетевой атаки реализуется средствами СОА. При этом средствами СОА могут анализироваться метрики, характеризующие нагрузку на узлы сети, загруженность оперативной памяти, скорость работы и т.д.

Предложенная методика процесса детектирования аномального поведения сенсорного устройства апробирован на стенде и показала высокие результаты – 99,9% обнаруженных аномалий в поведении сенсорных устройств.

СПИСОК ЛИТЕРАТУРЫ

1. Татарникова Т.М. Механизмы обеспечения безопасности сетей интернета вещей. В сборнике: Интеллектуальные и информационные технологии в формировании цифрового общества. сборник научных статей международной научной конференции. Санкт-Петербургский государственный экономический университет. 2017. С. 108-114.
2. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаужение вторжений в компьютерные сети. Сетевые аномалии. – М.: Горячая линия - Телеком, 2013. 220 с.
3. Jyothsna V., Prasad V.V.R. A Review of Anomaly Based Intrusion Detection Systems // International Journal of Computer Applications. 2011. Vol. 28, no. 7. P. 26–35
4. Wattenberg F.S., Perez J.I.A, Higuera P.C., Fernandez M.M., Dimitradis I.A. Anomaly detection of network traffic based on statistical inference and a-stable modeling // IEEE Transaction on Dependable and Secure Computing. 2011. Vol. 8, no. 4. P. 494-509.
5. Татарникова Т.М. Статистические методы исследования сетевого трафика // Информационно-управляющие системы. 2018. № 5 (96). С. 35-43.
6. Татарникова Т.М., Вольский А.В. Оценка вероятностно-временных характеристик сетевых узлов с дифференциацией трафика //Информационно-управляющие системы. 2018. № 3 (94). С. 54-60.

УДК 004.056.5

ПРЕИМУЩЕСТВА КЕРАМИЧЕСКИХ ДИСПЕРСНО-НАПОЛНЕННЫХ И ПОРИСТЫХ КОМПОЗИЦИОННЫХ МАТЕРИАЛОВ ДЛЯ СНИЖЕНИЯ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ

Гаршин Анатолий Петрович[1], Супрун Александр Федорович[1], Туманов Николай Игоревич[2]
[1] Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
[2] Управление ФСТЭК России по Северо-Западному Федеральному округу
Исаакиевская площадь, 11, Санкт-Петербург, 190000, Россия
e-mails: apgarshin@gmail.com, afs54@inbox.ru, tumanovn@gmail.com

Аннотация. Проведено обоснование эффективности применения керамоматричных композиционных материалов (КМК) для защиты структур обработки информации от несанкционированного съема по каналу побочного электромагнитного излучения. Рассмотрены основные электромагнитные свойства керамических композиционных материалов. Показано, что применение дисперсно-наполненных и пористых КМК для экранирования и поглощения электромагнитного излучения (ЭМИ) имеет большие перспективы.

Ключевые слова: керамические материалы; информация; экраны; поглощение; композит.

THE ADVANTAGES OF CERAMIC PARTICULATE-FILLED AND POROUS COMPOSITE MATERIALS TO REDUCE SIDE ELECTROMAGNETIC RADIATION

Garshin Anatoly[1], Suprun Alexander[1], Tumanov Nikolai[2]
[1] Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
[2] Management of the FSTEC of Russia for the Northwestern to Federal District
11 Isaakievskaya Square, St. Petersburg, 190000, Russia
e-mails: apgarshin@gmail.com, afs54@inbox.ru, tumanovn@gmail.com

Abstract. The substantiation of the effectiveness of the use of ceramic-matrix composite materials (CMC) to protect the structures of information processing from unauthorized removal through the channel of side electromagnetic radiation. The basic electromagnetic properties of ceramic composite materials are considered. It is shown that the use of dispersion-filled and porous CMCS for shielding and absorption of electromagnetic radiation (EMR) has great prospects.

Keywords: ceramic materials; information; screens; absorption; composite.

Введение. Информация, обрабатываемая техническими средствами (ТС), продолжает представлять значительную ценность для структур, занимающихся несанкционированным съемом информации. Как известно, при обработке информации в ТС возникает побочное электромагнитное излучение и наводки (ПЭМИН).

Канал ПЭМИН является единственным способом для злоумышленника получить конфиденциальные данные, не проникая в помещение, или контактируя с людьми и при этом быть незамеченным. Такой канал может эксплуатироваться длительное время. Единственным недостатком такого способа является то, что злоумышленнику нужно ждать, когда пользователь обратится к нужной ему информации, и только тогда из полученных ПЭМИН можно выделить необходимую информацию. Часто бывает, что вся обрабатываемая информация представляет интерес.

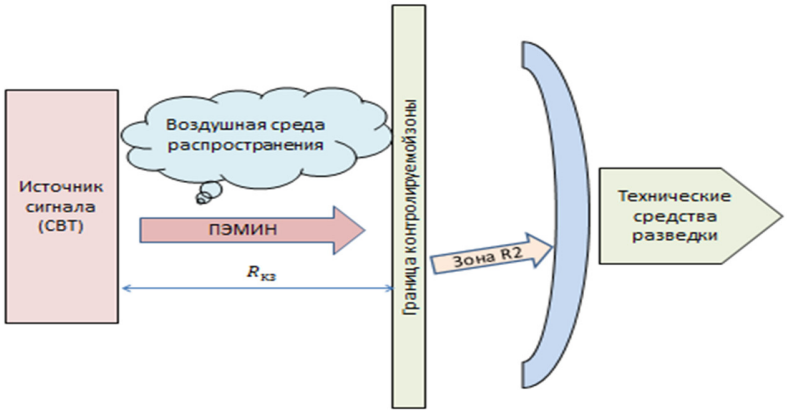


Рис. 1. Схема расположения ТСР ПЭМИН за пределами опасной зоны.

Схема возможного расположения технических средств разведки за пределами опасной зоны представлена на рис. 1.

Ожидание обращения к нужным данным может продолжаться долго. Это привело к созданию вредоносных программ, способных вмешиваться в работу процессорного блока и заставлять его обрабатывать необходимые данные без существенного изменения характеристик системного блока. Более того, если вредоносная программа способна осуществлять нужную модуляцию последовательности сигналов обмена с монитором (другими периферийными устройствами), то можно увеличить дальность распространения ПЭМИН в разы из-за изменения спектра ПЭМИН. Данная технология получила название Soft TEMPEST [4].

Технология реализации метода состоит в том, что в «компьютер-жертву» любым из доступных методов злоумышленником интегрируется специальная программа. Задачей программы является поиск необходимой информации (необязательно на жестком диске) и в результате обращения к различным аппаратным средствам компьютера формируются побочные излучения, которые будут промодулированы информативными битами. Перехватывая эти излучения и выделяя информативную составляющую, злоумышленник получает желанную информацию.

Особенностью технологии Soft Tempest является использование для передачи данных канала ПЭМИН, что значительно затрудняет обнаружение самого факта несанкционированной передачи по сравнению с традиционной компьютерной стеганографией. Действительно, если для предотвращения несанкционированной передачи данных по локальной сети или сети Интернет существуют аппаратные и программные средства (FireWall, Proxy server и т.п.), то средств для обнаружения скрытой передачи данных по ПЭМИН нет, а обнаружить такое излучение в общем широкополосном спектре (более 1000 МГц) паразитных излучений ПК без знания параметров полезного сигнала весьма проблематично.

Для закрытия каналов ПЭМИН используют следующие методы: 1. Установка зашумляющих активных генераторов широкополосных помех; 2. Экранирование помещений (в том числе полная экранизация); 3. Устройство поглощающих элементов на всех конструкциях помещения [7].

У первого способа есть несомненные преимущества, но есть и недостатки. Самый существенный недостаток — это то, что персонал подвергается дополнительному воздействию СВЧ за счет устройства зашумления. Другой недостаток заключается в том, что наличие маскирующего излучения демаскирует процесс обработки конфиденциальных данных, вызывая повышенный интерес злоумышленников. При определенных условиях метод может давать сбои и не обеспечивать гарантированную защиту компьютерной информации.

Второй способ заключается в создании помещений, где СВЧ энергия много раз переотражается от стен, потолка, пола и постепенно теряет мощность. Недостаток метода состоит в том, что персонал фактически работает внутри «микроволновой печи» и второй существенный недостаток – это сложность и дороговизна.

Устройство поглощающих покрытий на конструкциях помещения является сложным, очень дорогим и для многих помещений не подходит.

Наиболее перспективным и эффективным способом, обеспечивающим значительное снижение мощности ПЭМИН, является метод устройства поглощающих экранов. Использование поглощающих экранов дает возможность значительно снизить мощность ПЭМИН и защитить человека от вредного воздействия электромагнитного излучения (ЭМИ).

Для построения экранирующих конструкций предлагается использовать материалы, сочетающие в себе разнообразные технические характеристики и способные эффективно выполнять в конструкциях сразу несколько полезных функций, в том числе и эстетических. Композиционные материалы (КМ) могут соответствовать заданным требованиям. КМ на основе керамических матриц (керамоматричные композиты – КМК), армированные различными типами дисперсных и волокнистых наполнителей. В качестве матриц для КМК используются керамические материалы на основе оксидов, карбидов, нитридов, боридов и других керамик. Эти композиты характеризуются уникальным комплексом физико-механических, электромагнитных, теплофизических, триботехнических свойств и способны функционировать в сложных условиях. Разработка КМК с регулируемыми электрофизическими свойствами, использующих токопроводящие и магнитные наполнители, значительно расширяет области применения керамических композитов и позволяет рассматривать их как перспективные материалы нового поколения для многофункциональных систем защиты от электромагнитного излучения (ЭМИ). На основе КМК можно создавать радиоэкранирующие и радиопоглощающие покрытия и конструкции, обеспечивающие выполнение функций несущей конструкции, тепловой и эрозионной защиты.

Радиоэкранирующие и радиопоглощающие свойства КМК в определенном диапазоне частот определяются электрофизическими и магнитными свойствами их компонентов, типом и концентрацией диэлектрических и электропроводящих компонентов (матрица и наполнители), микро- и макроструктурой композита, геометрическими параметрами покрытий и конструкций, однородностью распределения наполнителей в объеме матрицы, технологией изготовления КМК и др.

Современные КМК, создаваемые для защиты от ЭМИ, можно разделить на несколько групп.

Дисперсно-наполненные КМК с наполнителями на основе нано- и микроразмерных частиц.

КМК и керамические материалы с пористой структурой.

КМК, армированные волокнистыми наполнителями.

КМК с гибридным армированием на основе волокон и дисперсных функциональных наполнителей.

КМК слоистой и градиентной структуры.

Экранирующие дисперсно-наполненные композиционные материалы на основе керамических матриц.

Важнейшими характеристиками керамики с точки зрения создания на их основе экранирующих и поглощающих ЭМИ материалов являются показатели их диэлектрических и магнитных свойств (электропроводность, диэлектрическая и магнитная проницаемость и др.). Очень большое количество монолитных керамик на базе оксидов, нитридов, боридов, стеклокерамик, ситаллов являются радиопрозрачными материалами, имея очень малые диэлектрические потери, не отражают радиоволны. К ним в первую очередь относятся керамика SiO_2, Si_3N_4, MgO, системы AlN-BN, AlN-SiO_2-Al_2O_3, Si_3N_4 с различными оксидными спекающими добавками, ситаллы систем MgO-Al_2O_3-SiO_2, Na_2O-Al_2O_3-SiO_2 и др. [1]. Ряд керамик являются средами, абсорбирующими ЭМИ, среди которых выделяется SiC керамика, которая является диэлектрическим поглотителем излучения благодаря своей собственной электрической дипольной поляризации. При этом снижение мощности отраженного сигнала ЭМИ лежит в пределах -(5–12) дБ для диапазона частот излучения 8–12,4 ГГц [2].

Для повышения характеристик экранирования и поглощения ЭМИ керамики модифицируют различными типами электропроводящих или магнитных наполнителей на основе нано- и микроразмерных частиц. К электропроводящим модификаторам относят технический углерод, графит, сажу, углеродные наноструктры (однослойные и многослойные углеродные нанотрубки (ОУНТ и МУНТ), фуллерены, графены, углеродные нановолокна, луковичные структуры) и др., а к магнитным – добавки в виде частиц металлов и металлических сплавов (например, Fe, Co, Ni, сплавы систем Fe–Ni и др.) или их металлических оксидов и др.

Дисперсно-наполненные КМК с наполнителями на основе микроразмерных частиц. В работе [3] керамические образцы на основе порошков каолина и Al_2O_3 с добавкой в них 40-70% по весу порошков графита (фракция < 63 мкм) были получены методом спекания при температуре 900^0C. Проведенные исследования показали, что данные композиции могут быть использованы в качестве электромагнитных экранов. Эффективность экранирования для диапазона частот 1-10 МГц составила 60-70 дБ, для 20-300 МГц – 25-60 дБ, для 1-10 ГГц – 30-40 дБ.

С точки зрения практической возможности получения КМК, модифицированных различными дисперсными и волокнистыми наполнителями, особый интерес представляют методы, основанные на технологии PIP (Polymer Infiltration and Pyrolysis), когда керамическая матрица получается в результате высокотемпературного пиролиза органометаллических полимеров. Получение КМК на основе PIP процессов рассматривается как перспективный путь повышения эффективности электромагнитных экранов. К настоящему времени разработаны предкерамические полимеры, позволяющие получать различные виды кремнийсодержащей керамики [5]: поликарбосилан (матрица SiC), полиметилвинилсилазан (SiCN), полисилоксан (SiOC), полиборосилозан (SiBCN) и др. При этом получаемая керамическая матрица может самостоятельно выступать в качестве абсорбирующего ЭМИ компонента. Кроме того, технология PIP предполагает получение конечного керамического материала в зависимости от количества циклов «пропитка-отверждение-пиролиз» с пористостью от 10 до 40%, наличие которой также способствует внутреннему рассеиванию ЭМИ.

Керамика AlN-SiBCN, полученная спеканием порошка AlN, смешанного с размолотой керамикой SiBCN (продукт отвержения и пиролиза полиборосилозана – PIP процесс), существенно снижает мощность сигналов отражения и достигает показателя -38,88 дБ при частоте излучения 8,5 ГГц (массовая доля SiBCN 40% и толщина образца 2 мм) [6]. При этом следует отметить, что коэффициент отражения ЭМИ данной КМК имеет узкие пиковые интервалы эффективности (шириной не более 1 ГГц) и существенное различие показателя снижения отражающей способности в диапазоне от -5 до -38 дБ, который очень чувствителен как к исходным характеристикам AlN-SiBCN керамики (концентрации SiBCN, толщине экрана), так и частоте излучения.

Другими компонентами поглощающих ЭМИ керамических экранов могут выступать различного рода магнитные частицы (порошки) на базе металлов Fe, Ni, Co и их оксидов. Эти частицы могут вводиться в керамическую основу через смешивание, путем пропитки керамического каркаса суспензиями на их основе или нанесения магнитных материалов на поверхность керамических или модифицирующих частиц и др. В работе [2] на поверхность порошков SiC наносилось покрытие NiO и далее образцы прессовались. Снижение отражающей составляющей такой керамики достигало -40 дБ, причем для 85% диапазона частот 8-12,4 ГГц уровень снижения этой составляющей был менее -20 дБ.

В работе [8] УНТ (от 0 до 4,5 мас.%) диспергировались и вводились в кремний содержащий полимер полиметилвинилсилазан с последующим отверждением и пиролизом последнего с образованием пористой SiCN матрицы. Проведенные исследования показали, что с увеличением содержания УНТ в исследованном процентном диапазоне снижается отражательная составляющая экранирования ЭМИ в диапазоне частот 8-12,4 ГГц. При этом максимальные показатели снижения составили -26,1 дБ при толщине образца 2 мм (4,5 мас.% УНТ). Однако наиболее широкий диапазон частот экранирования со снижением менее -10 дБ (8,7-12,4 ГГц) отмечался для образцов толщиной 2,2 мм (рис. 2).

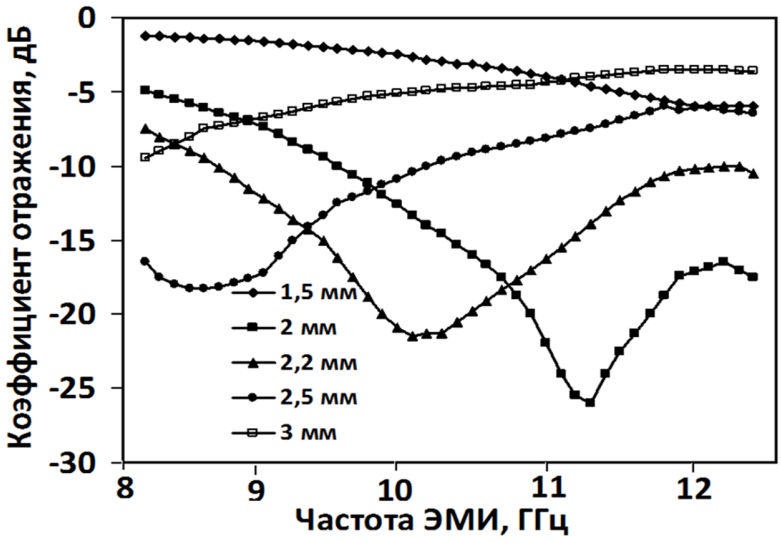


Рис. 2. Зависимости изменения показателя снижения отражательной составляющей эффективности экранирования ЭМИ для композита.

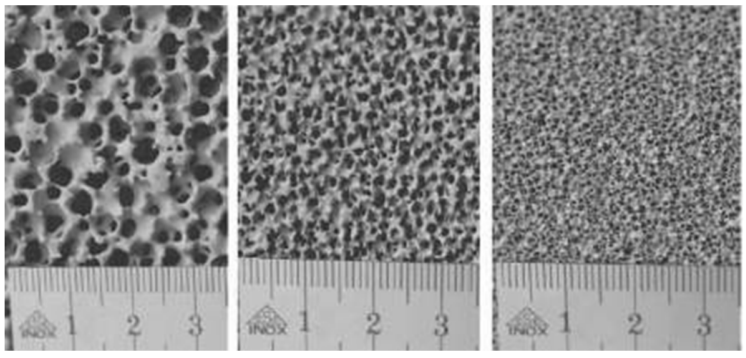
УНТ (4,5 мас.%)-SiCN от толщины образца

Пористые структуры на основе керамических материалов. Перспективными керамическими структурами для экранирования ЭМИ являются пористые (ячеистые, вспененные) композиты, которые разрабатываются для создания легковесных материалов и конструкций, обладающих как свойствами поглощения электромагнитного излучения, так и приемлемыми механическими или химическими свойствами и способностью функционировать при высоких температурах. Возможные механизмы потерь в таких пористых материалах – поглощение, рассеяние ЭМИ, а также образование вихревых токов. При этом следует отметить, что при использовании токонепроводящей керамики потерь за счет вихревых токов не существует.

В работе [9] пористая SiC керамика с изменяемыми толщинами образцов была получена путем силицирования парами кремния углеродного пористого каркаса. При этом для полученной керамики был достигнут показатель ослабления отраженной составляющей ЭМИ -60 дБ. Этот высокий коэффициент отражения, по-видимому, объясняется комплексным воздействием как рассеивания ЭМИ в пористой структуре SiC и его электрической дипольной поляризацией, так и поглощением излучения остаточным углеродом, не прореагировавшим с парами кремния.

Образование поглощающих ЭМИ химических компонентов и соединений возможно на этапе проведения высокотемпературной операции пиролиза различных предкерамических полимеров. Так, например, пористая керамика SiCN, полученная через пиролиз полисилозана, состояла из четырех основных компонентов SiC, Si_3N_4, SiO_2 и свободного углерода, и имела очень высокие показатель по коэффициенту отражения – -53 дБ [10].

Пористая керамика, как правило, выступает в качестве материала покрытия. Поэтому в работе [11] исследовалась эффективность применения вспененной SiC-керамики различной пористости в качестве лицевого слоя на металлическом электромагнитном экране. Для повышения электропроводности SiC-керамика была допирована бором. Образцы изготавливались из серийной пористой керамики марки CERASIC-B (Toshiba Ceramics Co). На рис. 3 приведены различные варианты вспененной SiC структуры, отличающихся размером и плотностью поровых ячеек в керамике.



а *б* *в*

Рис. 3. Различные варианты вспененной SiC структуры для экранирования ЭМИ.

Отмечается, что для всех исследованных пористых структур до частот излучения 40 ГГц доминирующим является только механизм поглощения. Однако при частотах 40-110 ГГц для крупноячеистых SiC образцов идет постепенное нарастание рассеивающего эффекта, который, тем не менее, при частоте 110 ГГц не превышает величины 25% от поглощающей составляющей. С ростом частоты излучения общая эффективность экранирования такого рода электромагнитных экранов растет. При этом определено, что наиболее эффективными являются металлические экраны, покрытые крупноячеистой SiC керамикой (рис. 3, *а*), которые имеют общую эффективность экранирования в пределах 60-70 дБ при толщине керамического слоя 28 мм.

Эффект межфазной поляризации и переотражения волн способствует снижению отражающей и росту поглощающей составляющих ЭМИ. Для этого создают керамические системы с большим количеством межфазных границ. В работе [12] были получены электромагнитные экраны на основе пористых матов из оксида иттрия, связанных SiC матрицей, осажденной в поровом каркасе матов газофазным методом CVI. В результате при осаждении в пористый каркас 86,9 % масс. SiC (пористость 84,8%) общая эффективность экранирования такого материала выросла с 0.069 до 16.2 дБ, а при 97,9 % масс. SiC (пористость 32,3%) до 20,3 дБ в диапазоне от 8,2 ГГц до 12,4 ГГц. Повышение эффективности экранирования обуславливается наличием межфазных границ в пенокерамике и, как следствие, межфазной поляризацией и переотражением электромагнитных волн.

В работе [13] в качестве высокотемпературного электромагнитного экрана предложена композиция, состоящая из пористой спеченной Si_3N_4-керамики, поровое пространство которой покрывают слоем SiC методом газофазного осаждения CVI. В результате образцы из такой керамики толщиной 2,5 мм и 3 об.% осажденного SiC имели снижение отражающей составляющей ЭМИ до -27,1 дБ при частоте излучения 9,8 ГГц и в широком интервале частот (2,2 ГГц) ослабление отражательной составляющей ЭМИ менее -10 дБ (рис. 4).

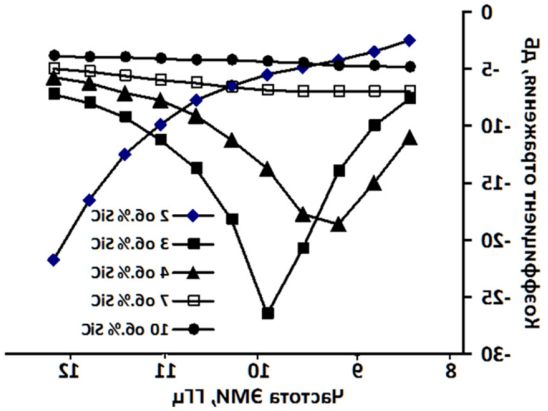


Рис. 4. Зависимости изменения отражающей составляющей ЭМИ Si_3N_4–SiC керамики от объемной доли осажденного SiC.

В другой работе [14] на керамике Si_3N_4–SiC, полученной тем же способом, создавали защитную антиокислительную SiO_2 пленку на осажденной поверхности SiC слоя. В результате образцы из такой керамики толщиной 3,8 мм имели снижение отражающей составляющей ЭМИ менее -30 дБ за счет 99,9% поглощения электромагнитного излучения в диапазоне частот 8,3-12,4 ГГц. В таком материале часть энергии преобразовывается в ток утечки в полупроводниковых структурах SiC, часть ее ослабляется поляризационным поведением (рис. 5, *а*). Кроме того, за счет пористой структуры Si_3N_4–SiC/SiO_2 и большого количества межфазных контактов, остаточное ЭМИ может быть многократно переотражено и поглощено в межфазных зонах (рис. 5, *б*).[14]. В работе [15] показано, что с повышением температуры хорошие экранирующие свойства для данной керамики растут от -38,6 дБ при 25^0C до -51,9 дБ при 500^0C (при 600^0C – -35,9 дБ), при этом возможно уменьшение толщины экрана. В работе это объясняется тем, что с увеличением температуры до 600^0C повышается комплексная диэлектрическая проницаемость всего композита.

Введение в матричный керамический состав или осаждение на поверхности пор токопроводящих или магнитных добавок существенно усиливают эффективность экранирования ЭМИ. В работе [16] восстановленный оксид графена (ВОГ) диспергировался и вводился в кремнийсодержащий полимер полиметилвинилсилазан по технологии аналогичной работе [8] с образованием пористого ВОГ/SiCN-композита. Содержание ВОГ варьировалось от 0 до 12 мас.%. Отмечалось, что с увеличением содержания ВОГ в диапазоне частот 8-12,4 ГГц SE_T и SE_A растут, а SE_R практически не меняется, достигая значений 42,2 дБ, 35,2 дБ и 9 дБ соответственно.

В работе [17] слоистая композиция пироуглерод/Si_3N_4 последовательно осаждалась методом CVI на поверхности пор керамики Si_3N_4. Общая эффективность экранирования полученной керамики толщиной 2,8 мм с 11,7 об.% пироуглерода составила 43,3 дБ в диапазоне частот 8,2-12,4 ГГц. Эффект экранирования был обусловлен переотражением ЭМИ в порах полученной керамики, наличием в ее составе абсорбирующего излучение углерода и большого количества межфазных контактов.

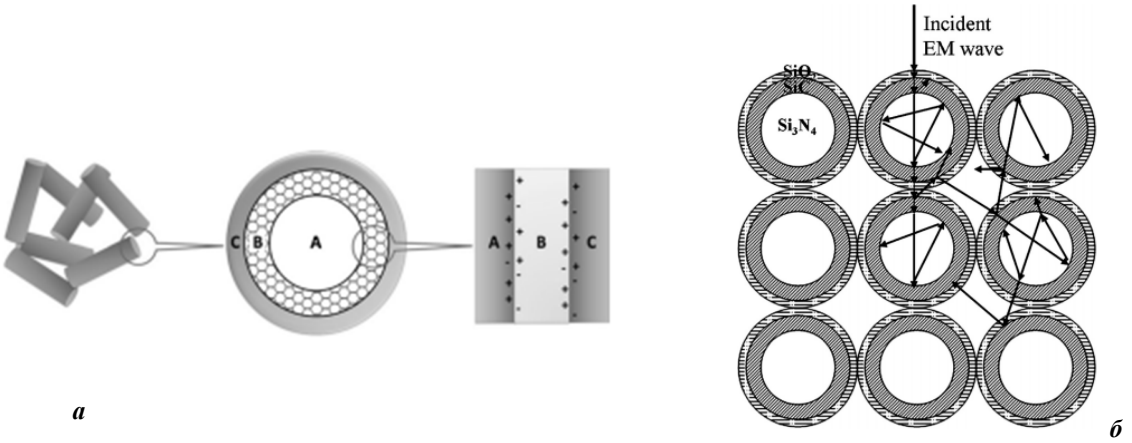


Рис. 5. Модель поведения Si_3N_4–SiC/SiO_2 –керамики: *а* – схема образования межфазной поляризации; *б* – схема переотражения ЭМИ.

Таким образом, проведенный анализ показывает, что применение современных дисперсно-наполненных и пористых КМК для экранирования ПЭМИН имеет большие перспективы, особенно при использовании в структурах с большим количеством автоматизированных рабочих мест.

Заключение. Эффективность экранирования зависит от типа керамической матрицы, формы самой конструкции, типа и вида дисперсных наполнителей, их размеров и концентрации, общей пористости и размера пор, микро- и макроструктуры композита, технологии изготовления КМК и др.

Варьирование данными параметрами дает возможность создавать КМК с заданными электромагнитными характеристиками и требуемыми показателями экранирования и поглощения ЭМИ. Именно это свойство определяет основное преимущество керамических дисперсно-наполненных и пористых композиционных материалов, используемых в целях снижения ПЭМИН.

СПИСОК ЛИТЕРАТУРЫ

1. Ивахненко Ю.А. Высокотемпературные радиопрозрачные керамические композиционные материалы для обтекателей антенн и других изделий авиационной техники (обзор) / Ю.А. Ивахненко, Н.М. Варрик, В.Г. Максимов // Электронный научный журнал «Труды ВИАМ», 2016. - №5. – С.36-43.
2. Yang H.J. NiO Hierarchical Nanorings on SiC: Enhancing Relaxation to Tune Microwave Absorption at Elevated Temperature / H.J. Yang, W.Q. Cao, D.Q. Zhang et al. // ACS Appl. Mater. Interfaces, 2015. – Vol.7. – P.7073–7077.
3. Bara A. Electromagnetic shielding properties of carbon based composites / A. Bara, A.M. Bondar, I. Iordache et al. // Revue Roumaine des Sciences Techniques - Serie Électrotechnique et Énergétique, 2008. – Vol.53. – P. 13-20.
4. Киреева Н.В., Семенов А.В. УТЕЧКА ИНФОРМАЦИИ ПО КАНАЛАМ ПЭМИ И СПОСОБЫ ИХ ЗАЩИТЫ // Международный журнал прикладных и фундаментальных исследований. – 2016. – № 8-4. – С. 499-504; URL: https://applied-research.ru/ru/article/view?id=10110 (дата обращения: 10.06.2019)
5. Гаршин А.П. Современные технологии получения волокнисто-армированных композиционных материалов с керамической огнеупорной матрицей (Обзор) /А.П. Гаршин, В.И. Кулик В. И., С.А. Матвеев, А.С. Нилов // Новые огнеупоры, 2017. – №4. – С. 20-35.
6. Garshin A.P. The state-of-art technologies for the fiber-reinforced composition materials with the ceramic refractory matrix (Review) / A.P. Garshin, V.I. Kulik, S.A. Matveev, A.S. Nilov // Refractories and Industrial Ceramics, 2017. ― Vol.58. - №2. ― P. 148-161.
7. He Y. Dielectric and microwave absorption properties of AlN-SiBCN lossy ceramics / Y. He, X. Li, J. Zhang et al. // Journal of Applied Ceramic Technology, 2018. – Vol.15. – P. 522–530.
8. Хорев, А.А. Техническая защита информации, учебное пособие для студентов ВУЗов, - М.: «НПЦ Аналитика», 2008 г.
9. Liu X. Role of single-source-precursor structure on microstructure and electromagnetic properties of CNTs-SiCN nanocomposites / X. Liu, Zh. Yu, L. Chen et al. // Journal of American Ceramic Society, 2017. – Vol.100. – P. 4649–4660.
10. Liu C. Porous Silicon Carbide derived from apple fruit with high electromagnetic absorption performance / C. Liu, D. Yu, D.W. Kirk, Y Xu // Journal of Materials Chemistry C, 2016. – Vol.4. – P. 5349–5356.
11. Li Q. Dielectric and microwave absorption properties of polymer derived SiCN ceramics annealed in N_2 atmosphere / Q. Li, X. Yin, W. Duan et al. // Journal of the European Ceramic Society, 2014. – Vol.34. – P. 589–598.
12. Zivkovic I. Characterization of open cell SiC form material / I. Zivkovic, A. Murk // Progress In Electromagnetics Research B, 2012. - Vol.38. - P. 225-239.
13. Yin X. Dielectric, electromagnetic absorption and interference shielding properties of porous yttria-stabilized zirconia/silicon carbide composites / X. Yin, Y. Xue, L. Zhang, L. Cheng // Ceramics International, 2012. - Vol.38. - Iss.3. – P. 2421-2427.
14. Zheng G. Complex Permittivity and Microwave Absorbing Property of Si_3N_4–SiC Composite Ceramic / G. Zheng, X. Yin , J. Wang et al. // Journal of Materials Science and Technology, 2012. - Vol.28. – Iss.8. – P. 745–750.
15. Zheng G. Improved electromagnetic absorbing properties of Si_3N_4–SiC/SiO_2 composite ceramics with multi-shell microstructure / G. Zheng, X. Yin, S. Liu et al. // Journal of the European Ceramic Society, 2013. – Vol.33. – Iss.11. – p. 2173–2180.
16. Li M. High-temperature dielectric and microwave absorption properties of Si_3N_4–SiC/SiO_2 composite ceramics / M. Li, X. Yin, G. Zheng et al. // Journal of material science, 2015. – Vol.50. – P.1478–1487.
17. Liu X. Single-source-precursor synthesis and electromagnetic properties of novel RGO–SiCN ceramic nanocomposites / X. Liu, Zh. Yu, R. Ishikawa et al. // Journal of Materials Chemistry C, 2017. - Vol5. – P. 7950-7960.
18. Li X. Synthesis and Electromagnetic Shielding Property of Pyrolytic Carbon-Silicon Nitride Ceramics with Dense Silicon Nitride Coating / X. Li, L. Zhang, X. Yin // Journal of American Ceramic Society, 2012. – Vol.95. - Iss.3. – P. 1038-1041.

УДК 004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВЕБ-ПРИЛОЖЕНИЙ

Коростень Александра Олеговна, Аксенов Сергей Сергеевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: aleksa22-1@mail.ru

Аннотация. Обеспечение безопасности сайта. Виды уязвимостей веб-приложений. Правила обеспечения безопасности веб-приложения. Аутентификация, способы защиты сайта от посторонних пользователей сайта.

Ключевые слова: сайт; веб-приложение; безопасность; данные; угроза; уязвимости; атаки**.**

INFORMATION SECURITY OF WEB APPLICATIONS

Gantsatsuk Valentin, Zinovieva Nadegda, Mikhailichenko Nikolay, Smirnova Daria
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: aleksa22-1@mail.ru

Abstract. Ensuring the security of the site. Types of web application vulnerabilities. Web application security rules. Authentication, ways to protect the site from unauthorized users of the site.

Keywords: website; web application; security; data; threat; vulnerabilities; attacks.

Введение. Web-приложения являются одними из наиболее небезопасных систем на сегодняшний день. Чем больше критически важных и конфиденциальных данных хранит программное обеспечение, тем важнее становится проведение проверки его безопасности. Многолетний опыт различных компаний показывает, что обеспечение безопасности веб-приложений должно начинаться еще на ранних стадиях процесса проектирования и разработки приложений. При разработке веб-приложений необходимо выполнить следующие задачи: избежать уязвимости в приложениях еще на ранних стадиях разработки; сделать так, чтобы разработчики приложений создавали качественные и безопасные конструкции; если имеются приложения, разработанные не внутри компании, необходимо требовать от поставщиков приложений экспертное заключение с целью обеспечения безопасности. Рассмотрим самые популярные виды уязвимостей, их разновидности и способы защиты от них.

На просторах Интернета можно найти веб-приложения, написанные на различных языках программирования; при этом для каждого языка характерен свой набор наиболее значимых уязвимостей. Что касается классических видов уязвимостей так это: SQL injection; PHP include; XSS.

Атаки и уязвимости. CSRF (англ. Cross Site Request Forgery — «Подделка межсайтовых запросов», также известен как XSRF) — вид атак на посетителей веб-сайтов, использующий недостатки протокола HTTP. Если жертва заходит на сайт, созданный злоумышленником, от её лица тайно отправляется запрос на другой сервер (например, на сервер платёжной системы), осуществляющий некую вредоносную операцию (например, перевод денег на счёт злоумышленника). Это атака, при которой злоумышленник пытается вынудить браузер жертвы создать запрос к целевому серверу, втайне от самой жертвы.

Данная атака в чем-то похожа на классическую XSS, в которой злоумышленнику необходимо было вынудить жертву перейти по некоторой ссылке на уязвимую страницу. Здесь же необходимо вынудить пользователя перейти на специально подготовленную злоумышленником страницу, на которую был добавлен некоторый код. При выполнении данного кода браузер жертвы совершает некий запрос к другому серверу (допустим под видом загрузки изображения), и тем самым выполняет некие, нужные злоумышленнику действия.

Опасность CSRF в том, что данное поведение браузеров и всего HTTP протокола является нормальным. К примеру, ведь нормально то, что сайт может на своих страницах содержать картинки с другого сайта. А браузеру неизвестно заранее что именно пытаются заставить его загрузить, действительно картинку, или под видом данной загрузки будет выполнено какое-то действие на целевом сайте.

XSS (англ. Cross Site Scripting — «межсайтовый скриптинг») — тип атаки на уязвимые интерактивные информационные системы в вебе, внедрение выполняемых на клиентском компьютере вредоносных скриптов в выдаваемую системой страницу. Специфика подобных атак заключается в том, что для атаки на сервер в качестве средства атаки используется авторизованный на этом сервере клиент. К сожалению, межсайтовые скриптовые атаки происходят, в основном, потому что разработчики не в состоянии обеспечить безопасный код.

К счастью, провести XSS-атаку можно так же легко, как и защититься от нее. Прежде всего, нужно думать о том, что вы пишите. Первое правило, которое нужно знать в любой веб-среде (будь то разработка, постановка задач, или производство) никогда не доверять данным, поступающим от пользователя или от любых других сторонних источников. Каждый бит данных должны быть проверен на входе. Это золотое правило предупреждения XSS.

В целях реализации радикальных мер безопасности, которые предотвращают XSS-атаки, мы должны помнить о проверке данных, санитарной обработки данных, и экранирование.

Проверка данных — это процесс обеспечения того, чтобы ваше приложение работает с правильными данными. Если ваш PHP скрипт ожидает целое число, для ввода данных пользователем, то любой другой тип данных будут отклонен, и пользователь получит сообщение об этом. Каждая часть пользовательских данных должна быть проверена при получении.

Санитарная обработка данных сосредоточена на манипулировании данными, чтобы убедиться, что они безопасны. Происходит удаление нежелательных битов данных и их приведение к правильной форме. Например, если на входе вы ожидаете простую текстовую строку, вы можете удалить любую HTML разметку из него.

Для того, чтобы защитить целостность отображения выходных данных, вы должны экранировать их. Это предотвратит попытку браузера непреднамеренно исказить смысл специальных последовательностей символов, которые могут быть найдены им.

Использование стандартной функции secureInnerData, позволяет защитить от атак типа SQL injection и XSS. Чаще всего их проводят, используя GET или POST запросы, которые не фильтруются на стороне сервера. Используя данную функцию в качестве фильтра входящих данных, вы сможете частично обезопасить себя

Аутентификация. Если какие-то области веб-сайта должны быть доступны только некоторым клиентам или зарегистрированным пользователям, для подобного разграничения доступа потребуется метод проверки подлинности пользователей.

Существует несколько способов аутентификации пользователей: базовая аутентификация, дайджест-аутентификация и HTTPS.

При использовании базовой аутентификации имя пользователя и пароль включаются в состав веб-запроса. Даже если контент с ограниченным доступом не слишком важен, этот метод лучше не использовать, так как пользователь может применять один и тот же пароль на нескольких веб-сайтах. Старайтесь защищать пользователей от подобных ошибок, используя более безопасные методы аутентификации.

Дайджест-аутентификация, поддерживаемая всеми популярными серверами и браузерами, позволяет надежно шифровать имя пользователя и пароль в запросе. Она помогает обеспечить безопасность имен и паролей, что производит соответствующее впечатление на пользователей и снижает вероятность успешной атаки на сервер.

Протокол HTTPS позволяет шифровать все данные, передаваемые между браузером и сервером, а не только имена пользователей и пароли. Протокол HTTPS (основанный на системе безопасности SSL) следует использовать в случае, если пользователи должны вводить важные личные данные -- адрес, номер кредитной карты или банковские сведения.

При выборе системы аутентификации рекомендуется использовать самый безопасный вариант из имеющихся в наличии. Другие варианты отпугнут клиентов, заботящихся о защите своих данных, и могут привести к возникновению излишнего риска для пользователей.

Заключение. Для того чтобы знать, как обезопасить собственный ресурс необходимо мыслить, как бы со стороны атакующего и при этом знать основные требования для успешного проведения атаки: возможность вынудить жертву перейти на страницу с дополнительным кодом. Или возможность модификации злоумышленником часто посещаемых жертвой; отсутствие защиты от CSRF на целевом сайте; пользователь в момент атаки должен быть авторизован для действия, которое мы хотим выполнить от его имени.

И на основе этих требований необходимо попытаться построить защиту.

СПИСОК ЛИТЕРАТУРЫ

1. Авраменко В.С., Бобрешов-Шишов Д.И., Беденков В.Н., Маликов А.В. Определение актуальных угроз безопасности информации в инфокоммуникационных системах на основе аппарата нечеткой логики // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017). VI Международная научно-техническая и научно-методическая конференция. Т.3. – СПб.: СПБГУТ, 2017. С.13-18.
2. Паращук И.Б. Саенко И.Б. Перспективные направления развития отечественных информационных технологий: материалы VI межрегиональной научно-практической конференции. Севастополь, 22-26 сентября 2020 г. / Севастопольский государственный университет, науч. ред. Б.В. Соколов. – Севастополь: СевГУ, Том2, 2020. – 179 с., С. 243-249.
3. Козлов Д. Д., Петухов А. А. «Методы обнаружения уязвимостей в web- приложениях» / Программные системы и инструменты: тематический сборник ф-та ВМиК МГУ им. Ломоносова N 7. П/р Л.Н. Королева. М: Издательский отдел ВМиК МГУ. Изд-во МАКС Пресс, 2006 г.
4. Издательство БХВ-Петербург, Тактика защиты и нападения на Web-приложения – 2005. – 432с

УДК 004.75

ОПРЕДЕЛЕНИЕ ЕМКОСТИ БУФЕРА ПРИ ОБСЛУЖИВАНИИ САМОПОДОБНОГО ТРАФИКА, МОДЕЛИРУЕМОГО РАСПРЕДЕЛЕНИЕМ ВЕЙБУЛЛА

Кутузов Олег Иванович, Татарникова Татьяна Михайловна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mail: tm-tatarn@yandex.ru

Аннотация. Предлагается решение по оценке емкости буфера сетевых узлов при обслуживании самоподобного трафика, моделируемого распределением Вейбулла. Показано, что одним из эффективных способов решения задачи оценки буферной емкости сетевого узла, обслуживающего самоподобный трафик является метод

экстремальных порядковых статистик. Результаты экспериментов по применению метода экстремальных порядковых статистик для оценки хвоста известных теоретических распределений показывают высокую точность аппроксимации.

Ключевые слова: самоподобный сетевой трафик; распределение Вейбулла; буферная емкость; теория экстремальных порядковых статистик; вероятность потери.

DETERMINING BUFFER CAPACITY WHEN SERVING SELF-SIMILAR TRAFFIC SIMULATED BY A WEIBULL DISTRIBUTION

Kutuzov Oleg, Tatarnikova Tatiana
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mail: tm-tatarn@yandex.ru

Abstract. A solution is proposed for estimating the buffer capacity of network nodes when servicing self-similar traffic modeled by the Weibull distribution. It is shown that one of the effective ways to solve the problem of estimating the buffer capacity of a network node serving self-similar traffic is the method of extreme order statistics. The results of experiments on the application of the method of extreme order statistics to estimate the tail of known theoretical distributions show a high accuracy of the approximation.

Keywords: self-similar network traffic; Weibull distribution; buffer capacity; theory of extreme order statistics; probability of loss.

Введение. Буферные накопители сетевых узлов являются важнейшим ресурсом управления сетевым трафиком. Исследования последних полтора десятка лет доказывают, что сетевой трафик по своей природе является самоподобным (self–similar) или фрактальным (fractal) [1, 2].

Самоподобность трафика оказывает существенное влияние на качество связи. Исследования в основном концентрируются вокруг статистических характеристик очередей, поскольку буферизация является основной обеспечивающей ресурсами стратегией. Оказывается, что традиционный анализ очередей, в основе которого лежит предположение о пуассоновском потоке, не может точно предсказать производительность системы в условиях самоподобного трафика. Практическое следствие фрактальной структуры трафика показывает, что буферы сетевых узлов должны иметь значительно больший объем, чем это предписывалось результатами традиционного анализа и моделирования процессов обработки очередей [3, 4].

Адекватное описание самоподобного трафика определяется распределениями вероятностей с тяжелыми хвостами. Одним из таких распределений, отражающим пачечный характер сетевого трафика является распределение Вейбулла [5].

Распределение Вейбулла W относится к классу экспоненциальных распределений, но «хвост» у распределения Вейбулла тяжелее «хвоста» экспоненциального распределения.

«Тяжелый хвост» у распределения Вейбулла означает, что этом распределении значительные (большие) значения случайной величины встречаются с большей вероятностью (чаще), чем, те же значения в классическом экспоненциальном распределении.

В настоящее время не существует общих аналитических результатов исследования очередей при самоподобном трафике и влияния самоподобности на качество его обслуживания [6].

Ограниченные возможности применения точных и приближенных аналитических методов приводят к необходимости имитационного моделирования. При этом имитационное моделирование сопряжено с рядом специфических вычислительных проблем, обусловленных стохастическим характером отклика имитационных моделей и необходимостью корректной обработки этого отклика [7].

Одним из эффективных способов решения задачи оценки емкости буферного накопителя сетевого узла при вейбулловском трафике является статистика экстремальных значений. Это экстраполяционный метод, основанный на знании асимптотического поведения распределения вероятностей. «Хвост» распределения вероятностей значений случайной величины аппроксимируется зависимостью, параметры которой оцениваются по результатам непосредственного моделирования методом Монте-Карло. При надлежащем выборе структуры формулы экстраполяции можно существенно ускорить проведение вычислительного эксперимента [8].

Постановка задачи. Для задач проектирования сетевых устройств одними из наиболее подходящих математических моделей являются системы с очередями (системы массового обслуживания – СМО).

В общем случае узел инфокоммуникационной рассматриваем как СМО класса G|G|1|m при стационарном режиме функционирования. Это класс одноканальных СМО с рекуррентным потоком заявок, определяемым произвольной функцией распределения длительности интервалов между ними (интервалов поступления), с рекуррентным временем обслуживания, определяемым произвольной функцией распределения, с числом мест в очереди (размером буфера) $m \leq \infty$. Рассматриваем стационарный режим функционирования такой СМО.

Основную задачу проектирования буферов как систем класса G|G|1|m поставим в виде нахождения зависимости

$$P = \varphi(m) \quad (1)$$

вероятности потери заявки P от размера буфера m (m = 0, 1, 2, …). Это позволит для любой наперед заданной допустимой вероятности потерь P^* определять соответствующий наименьший допустимый размер буфера m по формуле (2), следуемой из (1):

$$\lfloor m \rfloor = \varphi^{-1}(P^*), \quad (2)$$

где φ^{-1} – функция, обратная функции φ,

$\lfloor x \rfloor$ – ближайшее целое не меньшее x.

Полагая, что функция φ монотонно убывающая, можно утверждать, что φ^{-1} существует.

Следовательно, решив основную задачу (1), для любой максимально допустимой вероятности потерь P^* можно по формуле (2) определять наименьший размер буфера m, обеспечивающий требуемый уровень качества сетевого сервиса.

Используемые методы. Процесс поступления и обслуживания заявок в СМО с ограниченной очередью можно рассматривать, как регенерирующий процесс занятости и освобождения системы.

В течение интервала занятости заявки поступают и покидают систему. Точка регенерации – это момент поступления заявки на свободное обслуживающее устройство. Интервал занятости буфера – это длина периода от момента, когда в него поступила первая заявка до момента, когда его покинула последняя заявка.

В силу стационарности СМО анализ происходящих событий в одном промежутке занятости эквивалентен для всех промежутков.

При решении так поставленной задачи будем опираться на метод экстремальных значений (Extreme Value Theory, EVT). Метод EVT был разработан для анализа непрерывных случайных величин [9].

Очередь в буфере – дискретная случайная величина. Для описания функции вероятностей значений «хвостов» дискретных случайных получено расширение (1) в виде

$$P(m) = R\frac{a_n}{n\bar{K}}\exp\left(-\frac{m-b_n+1}{a_n}\right), \quad (3)$$

a_n и b_n – коэффициенты, вычисляемые по выборочным данным;

$\bar{K}$ – среднее число заявок, поступающих на вход СМО за период регенерации;

n – число значений в последовательностях, на которые разбивается выборочная последовательность, составленная из максимальных значений очереди на интервалах регенерации;

$R = exp(\Delta x/a_n)$. Константа R зависит от значения интервала $2\Delta x = h_i - h_{i-1}$ между значениями h_i, h_{i+1} дискретной величины x.

Зададимся значением P^* и разрешим (3) относительно переменной m. Получаем выражение для оценки значения емкости буфера m, обеспечивающего значение вероятности потерь $P^*(m)$, в виде.

$$m = a_n \ln\left[\frac{a_n R}{n\bar{K}P^*}\right] + b_n - 1, \quad (4)$$

Чтобы использовать выражение (4) для определения требуемого значения емкости буфера конечной емкости, необходимо вычислить по выборочным данным коэффициенты $\bar{K}$, a_n и b_n;

Методика расчета вероятности потерь в конечном буфере. Изложим основные шаги методики сбора и обработки выборочных данных при построении модели для оценивания потерь в буфере конечной емкости методом экстремальных статистик (EVT) [10].

Итак, в процессе сбора и обработки данных необходимо:

1. Выделить интервалы регенерации из общей выборки значений очереди, подсчитать число интервалов и оценить их среднюю длину $\bar{K}$ ($\bar{K}$ – среднее число заявок, поступивших в систему на интервале регенерации). При поступлении каждой заявки фиксируется значение очереди в системе).

2. По всем интервалам выделить максимальные выборочные значения, которые образуют последовательность независимых значений случайной величины - длины возможной очереди в КБ – для последующей обработки методом EVT.

3. Образовать порядковую последовательность из независимых значений длин очереди и оценить вероятности этих значений.

4. Разделить полученную в п.2 последовательность на M подпоследовательностей, содержащих по n выборочных значений (n можно принимать равным 50 значениям).

5. Образовать последовательность из максимальных значений x_i, i=1, ..., M подпоследовательностей.

6. Образовать порядковую последовательность из максимальных значений (п.5), оценить вероятность каждого значения в ней и построить в виде гистограммы оценку $\hat{H}_n(x)$ функции распределения максимального значения выборочной последовательности (п.2):

$$\hat{H}_n(x) = \frac{\sum_{i=1}^{j} h_i}{M+1};\ i = \overline{1,N}, \tag{5}$$

где h_i есть количество повторов i-го выборочного значения;

N – число шагов гистограммы.

7. Образовать последовательности значений для каждого x_i и

$$u_i = -\ln\left(-\ln\left(\hat{H}_n(x_i)\right)\right),\ i = \overline{1,N}. \tag{6}$$

8. Оценить значение a_n как статистику по формуле

$$\hat{a}_n = \frac{\sum_{i=1}^{N} x_i u_i - N\bar{x}\bar{u}}{\sum_{i=1}^{N} u_i^2 - N\bar{u}^2}, \tag{7}$$

где $\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i,\ \bar{u} = \frac{1}{N}\sum_{i=1}^{N} u_i,$

N – число шагов гистограммы.

9. Исходя из допустимой вероятности потерь, определить необходимую емкость m буфера из выражения

$$P^*(m) = \frac{e^{\Delta x}}{a_n} \cdot \frac{a_n}{n\bar{K}} \cdot e^{-\frac{N-b_n+1}{a_n}}, \tag{8}$$

где $2\Delta x = h_i - h_{i-1}$ – длительность интервала между значениями h_i, h_{i-1} дискретной величины;

$\bar{K}$ – среднее число поступлений за отдельный период регенерации;

значение b_n определяется по выражению $\hat{b}_n = \bar{x} - \hat{a}_n\bar{u}.$

Результаты эксперимента. Точность аппроксимации методом EVT была оценена путем сравнения результатов, полученных методом EVT с рассчитанными по соответствующим теоретическим распределениям.

В таблице 1 приведены результаты моделирования «хвоста» распределения Вейбулла: W(c,b) с функцией распределения $F(x) = 1 - e^{-(x/b)^c}$, $x > 0$ с параметрами c=0.5; b=4;

Таблица 1

Результаты моделирования «хвоста» распределения Вейбулла

x	200	400	600	800	1000	1200	1600	2000
W	8,49E-4	4,5E-5	4,8E-6	7,2E-7	1,36E-7	3,0E-8	2,06E-9	1,9E-10
EVT	9,1E-4	5,5E-5	6,1E-6	9,2E-7	1,7E-7	3,64E-8	2,27E-9	1,9E-10

В таблице 2 приведены результаты моделирования «хвоста» экспоненциального распределения E: $F(x) = 1 - e^{-(x/m)}$ с параметром m=3.37.

Таблица 2

Результаты моделирования «хвоста» экспоненциального распределения

x	25	35	45	50	55	60	65	70
E	6,1E-4	3,08E-5	1,58E-6	3,6E-7	8,16E-8	1,89E-8	4,2E-9	9,52E-10
EVT	5,6E-4	2,8E-5	1,44E-6	3,24E-7	7,3E-8	1,64E-8	3,7E-9	8,33E-10

Результаты экспериментального исследования применения метода EVT для оценки хвоста известных теоретических распределений показывают достаточно высокую точность аппроксимации – для одних и тех же значений хвоста значения вероятностей одного порядка малости.

Следовательно, можно утверждать, что функция, построенная методом EVT и аппроксимирующая хвост распределения, эквивалентна теоретической функции.

Кроме того, сопоставление значений «хвостов» Вейбулла- и экспоненциального распределений при вероятностях одного порядка малости показывает, насколько «хвост» Вейбулла тяжелее экспоненциального.

Модель соответствовала СМО четырем типам: M/W/1, W/W/1, W/M/1 и M/M/1 с коэффициентами загрузки ρ =0.5; 0.7; 0.9 для каждого типа СМО. Имитация проведена для задаваемых значений вероятности потерь $P^*(m)$: 10^{-4}, 10^{-6}, 10^{-8}, 10^{-10}.

В таблице 3 приведены результаты моделирования по найденным значениям емкости буфера m.

Таблица 3

Результаты моделирования

Тип СМО	$P^*(m)$	m		
		ρ=0.5	ρ=0.7	ρ=0.9
M/W/1	10^{-4}	42	66	180
	10^{-6}	69	113	300
	10^{-8}	94	154	430
	10^{-10}	122	203	576
W/M/1	10^{-4}	53	81	198
	10^{-6}	81	128	343
	10^{-8}	121	179	482
	10^{-10}	150	227	603
W/W/1	10^{-4}	83	128	311
	10^{-6}	128	217	546
	10^{-8}	184	279	780
	10^{-10}	242	366	1026
M/M/1	10^{-4}	12	21	60
	10^{-6}	18	32	103
	10^{-8}	23	49	147
	10^{-10}	32	61	187

Таким образом, применение аналитико-статистического метода и выражения (4) в случае мультисерверного трафика позволяет рассчитать значения емкости буфера, исходя из допустимого значения вероятности потерь $P^*(m) \le 10^{-9}$.

Заключение. Фрактальные модели с трудом поддаются аналитическому моделированию. Представленный метод расчета емкости буфера в условиях самоподобного трафика, описываемого распределением Вейбулла, относительно прост и эффективен. Хотя в данной статье не приведены результаты об ускорении получении результатов, авторы в [8] демонстрируют метод EVT для оценки малых и очень малых значений вероятностей случайных величин позволяет сократить время имитации в 4-5 декад по сравнению с классическим методом Монте-Карло.

СПИСОК ЛИТЕРАТУРЫ

1. Bernabei F., Ferretti R., Listanti M., Zingrillo G. A methodology for buffer design in ATM switches // J. European transactions on telecommunications and related technologia. 1991. Vol. 2, no. 4. P. 367-379.
2. 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. P. 1–3. DOI: 10.1109/MWENT.2018.8337306
3. Шелухин О.И. Мультифракталы. Инфокоммуникационные приложения. – М.: Горячая линия – Телеком, 2011. 576 с.
4. Tanenbaum A., Wetherall D. Computer Networks. 5th ed. – Prentice Hall, 2010. 960 p.
5. Arfeen M.A., Pawlikowski K., McNickle N., Willig A. The role of the Weibull Distribution in Internet traffic modeling // 25th International Teletraffic Congress (ITC), Shanghai, 2013. P. 1–8. DOI: 10. 1109/ITC.2013.6662948.
6. Self-Similar Network Traffic and Performance Evaluation. Ed. by K. Park and W. Willinger New York: Wiley, 2000. 576 p.
7. Крэйн М., Лемуан О. Введение в регенеративный метод анализа моделей. – М.: Наука, 1982. 104 с.
8. Ramirez-Cobo R., Lillo R.E., Wiper M. P. Bayesian analysis of a gueeuing system with a long-tailed arrival process // Communication in Statistics. 2008. Vol. 37. P. 697–712.
9. Королев В.Ю., Соколов И.А. Об условиях сходимости распределений экстремальных порядковых статистик к распределению Вейбулла//Информатика и ее применение. 2014. №3(8). С. 3-11.
10. Галамбош Я. Асимптотическая теория экстремальных порядковых статистик. – М.: Наука, 1984. 303 с.
11. Zadorozhnyi, V.N. Simulation modeling of fractal queues, in Dynamics of Systems, Mechanisms and Machines (Dynamics), 2014. P. 1-4. DOI: 10.1109 / Dynamics.2014.7005703.
12. Tatarnikova T., Kutuzov O. Evalution and comparison of classical and fractal queuing systems // In 15th International Symposium on Problems of Redundancy in Information and Control Systems, REDUNDANCY 2016. P. 155-157. DOI: 10.1109 / RED.2016.7779352.

УДК 004.056.5

ОБЩИЕ ЗАДАЧИ И СОДЕРЖАНИЕ ЭТАПОВ РАЗРАБОТКИ МЕТОДИКИ АНАЛИЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Михайличенко Николай Валерьевич, Паращук Игорь Борисович, Михайличенко Антон Валерьевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: 23esn2008@rambler.ru, shchuk@rambler.ru, katjuha777@inbox.ru

Аннотация. Проведен анализ научно-практических подходов к совершенствованию методологии и инструментария анализа информационной безопасности современных мобильных центров обработки данных. Осуществлены формулировка задач и детальное описание этапов разработки методики многокритериального анализа

информационной безопасности мобильных дата-центров в различных условиях обстановки, с учетом различных аспектов неопределенности исходных данных, которые могут быть формализованы в рамках математики нейро-нечетких сетей и гранулярных вычислений.

Ключевые слова: анализ; информационная безопасность; мобильный центр обработки данных; защищенность; показатель; этап; нейро-нечеткая сеть; гранулярные вычисления.

GENERAL TASKS AND CONTENT OF THE DEVELOPMENT STAGES OF THE METHODOLOGY FOR ANALYZING THE INFORMATION SECURITY OF MOBILE DATA CENTERS

Mikhailichenko Nikolay, Parashchuk Igor, Mikhailichenko Anton
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: 23esn2008@rambler.ru, shchuk@rambler.ru, katjuha777@inbox.ru

Abstract. The analysis of scientific and practical approaches to improving the methodology and tools for analyzing information security of modern mobile data centers is carried out. The tasks are formulated and the stages of development of the methodology for multi-criteria analysis of the information security of mobile data centers are described in detail in various conditions, taking into account various aspects of the uncertainty of the source data, which can be formalized in the framework of the mathematics of neuro-fuzzy networks and granular computing.

Keywords: analysis; information security; mobile data center; security; indicator; stage; neuro-fuzzy network; granular computing.

Введение. Эволюция современного информационного общества невозможна без значимых, либо, иногда, революционных шагов в рамках развития IT-инфраструктуры этого общества. Это касается как всех секторов экономики, сферы здравоохранения, так и оборонной сферы и сферы обеспечения безопасности. Очевидно, что для реализации своевременного и эффективного управления всеми сферами жизни страны и общества необходимо использовать новейшую IT-инфраструктуру, и эти вопросы уже успешно решаются в России. Ключевым элементом построения IT-инфраструктуры практически любого масштаба являются центры обработки данных (ЦОД), иногда называемые дата-центрами [1]. В большинстве случаев под ЦОД понимается специализированное помещение, стационарное сооружение или мобильное помещение для размещения (хостинга) серверного и сетевого оборудования. С помощью этого оборудования к ЦОД подключаются абоненты по каналам специализированных сетей или глобальной сети Интернет.

Вместе с тем, особое внимание специалистов в последние годы сосредоточено на поиске новых технических и программных решений по хранению и обработке больших массивов данных. Это связано с тем, что в течение жизненного цикла современного ЦОД, по некоторым данным, сменяется от трех до пяти поколений серверного и сетевого оборудования, а объем данных удваивается каждые восемнадцать месяцев [2]. В этих условиях все более очевидна необходимость разработки гибких и масштабируемых систем хранения данных. Эффективным решением данных проблем могут стать мобильные ЦОД (МЦОД) [3].

Важными преимуществами МЦОД, к которым также относят контейнерные и модульные дата-центры, являются удобство их транспортировки и возможность работы в любой местности. Мобильный ЦОД – одномодульный дата-центр, который размещен либо в специальном боксе (кунге – кузове универсальном нормального габарита) на транспортной базе (грузовой автомобиль, судно, самолет), либо в специализированном транспортном контейнере (может перевозиться железнодорожным или водным транспортом). Он, как и его стационарный аналог, оснащен комплексом информационной, телекоммуникационной и инженерной инфраструктуры, подключен к каналам связи и предназначен для хранения и обработки информации, а также для оказания широкого диапазона иных услуг, которые может предоставить хранилище данных.

При этом контейнерный ЦОД – самый распространенный тип МЦОД с готовой инфраструктурой для размещения серверов, систем хранения данных и другого IT-оборудования. Это либо одиночный контейнер или набор контейнеров со всеми компонентами ЦОД: серверными стойками, коммуникациями, системами электропитания и охлаждения.

Типовой МЦОД обычно смонтирован на базе большегрузного автомобиля с размещенным внутри комплексом информационной, телекоммуникационной и инженерной инфраструктуры. Классический МЦОД представляет собой небольшой автономный и готовый к эксплуатации автомобильный модуль, который внутри оборудован серверными стойками, структурированной кабельной системой, системами бесперебойного и гарантированного электропитания, системами вентиляции и кондиционирования, средствами противопожарной защиты и средствами контроля управления доступа, мониторинга и управления инфраструктурой [4].

Мобильные ЦОД предназначены для: оперативного развертывания IT-инфраструктуры в труднодоступных и, зачастую, отдаленных местах; для «приближения к клиенту» – размещения IT-инфраструктуры рядом с потребителями; для реализации возможности частого перемещения (перевозки) и установки в различных местах; для

быстрого развертывания инфраструктуры или увеличения ее мощности (масштабирование), а также для выполнения функций резервного ЦОД [5].

Применение МЦОД позволить снизить количество функциональных узлов (аппаратных, серверных, кроссовых), унифицировать оборудование, рационально использовать существующие и вновь вводимые новые вычислительные ресурсы и ресурсы хранения, реализовать программную виртуализацию серверов, а также придать дополнительный, расширенный функционал существующим средствам обработки и хранения данных, что, в конечном итоге, создает предпосылки для оптимизации расходов на создание и поддержание информационной инфраструктуры в любой точке местности. Вместе с тем, необходимо признать, что пока не существует единого подхода в вопросах управления МЦОД и в вопросах анализа и обеспечения их информационной безопасности.

Более того, лишь недавно начали появляться документы (стандарты), регламентирующие процессы проектирования и эксплуатации различных ЦОД, включая вопросы обеспечения их информационной безопасности [1]. Все это делает, безусловно, актуальной проблему выработки системного подхода в вопросах оценивания и обеспечения информационной безопасности МЦОД, а также задачу разработки моделей и методов повышения защищенности элементов таких систем (аппаратных, программных, иных) и, в целом, защищенности систем такого класса [6].

Решение предложенной проблемы на основе новых моделей и методов, позволит унифицировать механизмы оценивания и обеспечения информационной безопасности МЦОД и упростить внесение изменений в его инфраструктуру безопасности, будет способствовать повышению защищенности МЦОД, а также тиражируемости и масштабируемости структурных решений, нацеленных на повышение информационной безопасности систем такого класса.

По-прежнему, важно получить ответ на вопрос – как в условиях постоянного роста цены ресурсов, затрачиваемых на защиту, получать максимальную отдачу от эксплуатации системы информационной безопасности МЦОД. При этом возникают сопутствующие задачи, которые необходимо решать при управлении информационной безопасностью мобильных ЦОД: как добиться существенного увеличения основных показателей защищенности; каким образом при минимизации затрат учесть возможный рост уровня и количества угроз безопасности, предусмотреть восстановление полной работоспособности МЦОД после компьютерных атак. Решение этих основных и сопутствующих задач возможно в рамках и по результатам процесса анализа информационной безопасности МЦОД.

При этом, как фундаментальный этап, важным является решение задачи создания достоверных и оперативных алгоритмов анализа информационной безопасности, которые позволят максимально точно, в оговоренные сроки и полноценно оценить защищенность МЦОД с учетом динамики изменения условий их применения, динамики угроз, а также с учетом неопределенности исходных данных, необходимых для принятия решения по управлению информационной безопасностью МЦОД.

Таким образом несмотря на то, что существуют общемировые подходы к классификации (категоризации) уровней защищенности дата-центров, единой методики оценивания информационной безопасности МЦОД не существует, поэтому направление исследований, на котором предполагается сосредоточиться при создании методики, создании достоверных и оперативных частных алгоритмов многокритериального оценивания информационной безопасности МЦОД, нам видится состоящим из нескольких последовательных этапов:

Первый этап: формулировка системы показателей информационной безопасности МЦОД, а также синтез вероятностно-временной модели процесса смены состояний защищенности мобильного дата-центра, которая будет учитывать неопределенный характер изменения значений показателей информационной безопасности на основе применения математического аппарата условных вероятностей, нейронных сетей и методов гранулированных (гранулярных) вычислений [7].

Второй этап: разработка обобщенного и частных алгоритмов анализа информационной безопасности МЦОД в условиях неопределенности.

Описание программных средств формирования и расчета информационной безопасности МЦОД в условиях неопределенности, а также рекомендации по использованию программно-алгоритмических средств при управлении защищенностью МЦОД, могут составлять содержание третьего этапа.

И наконец, в рамках четвертого этапа возможно проведение проверки конструктивности разработанной методики и алгоритмов анализа информационной безопасности МЦОД в условиях неопределенности. Проверка конструктивности позволит разработать научно-технические предложения по совершенствованию системы обеспечения информационной безопасности сложных мобильных информационных объектов такого класса.

Объективно существующая неопределенность исходных данных, важных для анализа информационной безопасности МЦОД, обуславливает необходимость привлечения для задач анализа защищенности новых методов и средств, например, таких, как часто применяемые в рамках интеллектуальной обработки данных нейро-нечеткие сети (ННС) и алгоритмы гранулярных вычислений (ГВ).

В ряду современных методов интеллектуальной обработки информации известны подходы [8], ориентированные на учет нечетко заданных исходных данных, когда в рамках оценки информационной безопасности сложных информационных систем, подобных МЦОД, ряд характеристик защищенности этих систем моделируется и оценивается на основе параметрически заданных данных, традиционными методами, а оценка нечетко заданных (идентифицируемых) параметров информационной безопасности систем такого класса осуществляется путем

последовательных преобразований с использованием ННС, нейро-нечетких вычислительных методов и алгоритмов, позволяющих реализовать возможность их относительно параметрического анализа.

При этом ННС, объединяющие в себе нейронные сети и нечеткую логику, консолидируют лучшие свойства обоих подходов (нейросетевого и нечеткого), и, в то же время, почти свободны от их проблем. С одной стороны, такие структуры включают вычислительную мощность и способность к обучению нейронных сетей, а с другой стороны интеллектуальные возможности нейронных сетей усиливаются свойственными «человеческому» способу мышления нечеткими правилами принятия решений.

В ННС вывод осуществляется на основе аппарата нечеткой логики, а параметры функций принадлежности нечетких множеств настраиваются при помощи алгоритмов обучения нейронной сети [8]. Вместе с тем, ННС не способны решать задачи идентификации и оценки большого количества (массивов) параметров защищенности в интересах интеллектуального информационного анализа информационной безопасности неочевидно структурированных динамических систем с изменяющейся в процессе функционирования структурой. Именно к таким системам относятся сложные управляемые МЦОД. Данные, которые используются в нейро-нечетких алгоритмах анализа информационной безопасности (в частности, значения функций принадлежности нечетких множеств), носят нечеткий, но формализованный, не зашумленный, упорядоченный характер.

Физический смысл этого объективного факта заключается в том, что нечеткие данные и знания могут быть описаны (наблюдаемы) как точные, формализованные и однозначные лингвистические переменные и функции принадлежности, а могут иметь большую размерность (избыточность) и быть неточными, зашумленными, неупорядоченными и неформализованными. Могут быть сформированы массивы данных, характеризующие степень принадлежности или не принадлежности конкретного параметра информационной безопасности к некому конкретному множеству. Причем, ввиду большого объема параметров защищенности, ошибок наблюдения (идентификации), неупорядоченности и слабой формализованности, формируемые данные могут иметь некоторый «разброс» значений. При этом сложно, а зачастую невозможно определить точные границы разрозненных множеств (массивов) данных. Иными словами, эти данные не только нечеткие, но и неточны, зашумлены.

В этих случаях используют современные математические подходы из области интеллектуального анализа данных, нацеленные на слияние массивов нечетко заданных неточных, зашумленных исходных данных в группы (информационные «гранулы») по принципу семантического и функционального сходства и на математически корректную обработку этих данных в интересах анализа информационной безопасности.

Таким образом, для решения задач анализа информационной безопасности МЦОД и формирования точных, формализованных и однозначных значений (на основе нечетких знаний) исходных данных для оценки защищенности, могут использоваться методы и алгоритмы ГВ, иногда называемые fuzzy-granular computing – нечетко-гранулярные вычисления [9].

В рамках подобных задач также иногда говорят о «неточных множествах», как о широко известных в настоящее время подходах к гранулированию информации [9, 10].

Под гранулой понимается группа информационных объектов (данных), объединяемых неразличимостью, сходством, близостью, т.е. отношениями, обладающими, по крайней мере, свойствами симметричности и рефлексивности. Термин «гранула» означает динамическую целостную информационную структуру, организованную для достижения некоторой цели, а гранулярные вычисления (методы математической обработки и преобразования информационных гранул) применяются наряду с методами обработки нечеткой информации в ННС [9, 10].

Известен метод представления информационных гранул, индуцированный нечеткостью, который является наиболее часто применяемым, при этом нечеткая гранула (в общем случае нечеткое множество) может быть представлена как произведение независимых скалярных экспоненциальных функций [10]. При этом гранула рассматривается, в частности, как тензорное произведение векторов, представляющих собой элементы множества упорядоченных пар информационных объектов (данных). Причем нечеткое множество как информационная гранула – объект, элементы которого (α-уровни) связаны иерархической структурой, свойства которой определяются матрицей семантического и функционального сходства [9, 10].

Гранулярное представление нечетких множеств для задач анализа информационной безопасности МЦОД в условиях неопределенности позволяет операции нейро-нечетких вычислений осуществлять в соответствии с алгоритмами гранулярных (нечетко-гранулярных) вычислений [9, 10]. Алгоритмы ГВ в задачах интеллектуальной обработки данных при анализе информационной безопасности МЦОД включают два этапа:

Этап информационного гранулирования – слияние больших массивов нечетко заданных неточных, зашумленных исходных данных о значениях параметров информационной безопасности МЦОД в информационные гранулы по принципу функционального сходства.

Здесь неточно заданные, зашумленные нечеткие множества (исходные данные), характеризующие, значения параметров информационной безопасности МЦОД, группируются в гранулы (множества) по принципу сходства функций принадлежности – минимального численного расстояния между значениями большого количества функций принадлежности, которые описывают конкретный нечетко заданный параметр информационной безопасности мобильного центра обработки данных. Иными словами, определятся, к какому нечеткому множеству данное нечеткое число (исходные данные) математически (функционально) «тяготеет».

Этап гранулярных вычислений – математическая обработка информационных гранул с целью преобразования, характеризующих их неточных, зашумленных, неупорядоченных и неформализованных нечетких исходных данных большой размерности (избыточных данных) к виду, пригодному для осуществления достоверного параметрического анализа информационной безопасности МЦОД.

Этот этап включает две операции [9, 10]: первая – операция гранулярного суммирования над векторами (гранулами) и вычисление функции следа гранулярной суммы. Вторая – операция минимизации функции следа гранулярной суммы, как итог реализации преобразования нечетких переменных – показателей информационной безопасности, заданных неточно (зашумленных) в точную численную форму.

Результат расчетов в рамках данного метода оценивания защищенности численно характеризует уточненное (точное, не зашумленное) значение конкретного элемента исходного нечеткого множества, содержащего информацию о количественном значении соответствующего конкретного параметра информационной безопасности МЦОД.

Заключение. Таким образом, рассмотрен новый подход к совершенствованию методологии и инструментария анализа информационной безопасности современных мобильных ЦОД. Сформулированы частные задачи и проведено детальное описание этапов разработки методики многокритериального анализа информационной безопасности мобильных ЦОД в различных условиях обстановки, с учетом различных аспектов неопределенности исходных данных, которые могут быть учтены в рамках математики ННС и гранулированных (гранулярных) вычислений.

Рассмотренные основы ННС и вычислительный алгоритм гранулярных вычислений позволяют повысить достоверность анализа информационной безопасности МЦОД за счет уточнения (реконструкции, верификации) неточных, зашумленных нечетких исходных данных большой размерности. Данные методы интеллектуального анализа данных позволяют устранить нечеткость, зашумление, неупорядоченность и неформализованность при формировании исходных данных для анализа информационной безопасности МЦОД.

Это, в свою очередь, позволяет повысить объективность задания этих исходных данных, а в конечном итоге, получить выигрыш в достоверности и оперативности анализа информационной безопасности, что призвано способствовать повышению эффективности процесса информационной поддержки принятия решений по обеспечению защищенности мобильных ЦОД в условиях различного вида угроз и негативных воздействий.

СПИСОК ЛИТЕРАТУРЫ

1. Национальный стандарт Российской Федерации ГОСТ Р 58811 - 2020. Центры обработки данных. Инженерная инфраструктура. Стадии создания. – М.: Стандартинформ, 2020. – 17 с.
2. Мобильный модульный центр обработки данных. [Электронный ресурс] // ПитерЭнергоМаш. URL: http://piterenergomash.ru/index.php/katalog-produktsii/kontejnernye-resheniya/kontejnernye-tsod (дата обращения 30.04.2021).
3. Паращук И.Б., Михайличенко Н.В. Особенности построения и анализа качества дата-центров как базовых элементов IT-инфраструктуры // Перспективные направления развития отечественных информационных технологий: материалы IV Межрегиональной научно-практической конференции. – Севастополь: Севастопольский государственный университет, 2018. – 352 с., С. 28-29.
4. Google Unveils Its Container Data Center. Data Center Knowledge. [Электронный ресурс] // Google (Alphabet). URL: https://www.datacenterknowledge.com/archives/2009/04 /01/google-unveils-its-container-data-center/ (дата обращения 30.04.2021).
5. Мобильные центры обработки данных. [Электронный ресурс] // Инженерно-техническая компания «ИЛТОР». URL: https://iltor.ru/projects/data-centry/ (дата обращения 30.04.2021).
6. Авраменко В.С., Бобрешов-Шишов Д.И., Беденков В.Н., Маликов А.В. Определение актуальных угроз безопасности информации в инфокоммуникационных системах на основе аппарата нечеткой логики // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017). VI Международная научно-техническая и научно-методическая конференция. Т.3. – СПб.: СПБГУТ, 2017. С.13-18.
7. Бутакова М.А., Климанская Е.В., Чернов А.В. Формальные структуры и представления для гранулярных вычислений. // Современные наукоемкие технологии. 2018. №5. С. 36-40.
8. Андриевская Н.В., Резников А.С., Черанев А.А. Особенности применения нейро-нечетких моделей для задач синтеза систем автоматического управления. // Фундаментальные исследования. Технические науки. № 11. 2014. С. 1445-1449.
9. Минаев Ю.Н., Филимонова О.Ю., Минаева Ю.И. Гранулярный компьютинг в системе нечетких множеств на уровне тензорных гранул // Проблемы информатизации и управления. 2012. №4(40). С. 51-61.
10. Бутакова М.А., Гуда А.Н., Иванченко О.В., Карпенко Е.В. Элементы теории гранулярных вычислений с нечеткими приближенными информационными гранулами. // Вестник Ростовского государственного университета путей сообщения. 2015. № 4(60). С. 27-33.

УДК 621.391.28

СПОСОБЫ ОБЕСПЕЧЕНИЯ СКВОЗНОГО КАЧЕСТВА УСЛУГ B2C В СЕТИ LTE

Мошак Николай Николаевич, Щербак Владимир Игоревич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: nnmoshak49@mail.ru, ius@sut.ru

Аннотация. Анализируются проблемы и способы обеспечения качества услуг B2C в сети LTE в режиме установленного соединения E2E на основе преобразования параметров DiffServ в параметры QCI и наоборот.

Ключевые слова: параметры QoS LTE; услуги B2C LTE; соединение E2E LTE; технология DiffServ; код дифференцированных услуг DSCP.

METHODS OF PROVIDING END-TO-END QUALITY OF B2C SERVICES IN LTE NETWORK

Moshak Nikolay, Shcherbak Vladimir
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: nnmoshak49@mail.ru, ius@sut.ru

Abstract. Problems and methods of ensuring the quality of B2C services in the LTE network in the established connection mode are analyzed E2E based on conversion of DiffServ parameters to QCI parameters and vice versa.

Keywords: QoS LTE parameters; services B2C LTE; E2E LTE connection; DiffServ technology; the code of the differentiated services DSCP.

Введение. При передаче трафика различной природы от/в оконечное устройство сети LTE существует проблема взаимно однозначного преобразования значения параметров класса сервиса обработки IP-потоков в технологии Diffserv в значения идентификатора качества обслуживания на участке радиодоступа сети LTE и/или во внешнем пакетном шлюзе P-GW при взаимодействии с внешними сетями на технологии Diffserv. В статье рассматриваются проблемы и способы обеспечения качества услуг B2C в сети LTE в режиме установленного соединения E2E на основе преобразования параметров Diffserv в параметры QCI и наоборот.

Сеть LTE или развитая пакетная система EPS (Evolved Packet System) состоит из сети радиодоступа RAN (Radio Access Network) и ядра сети EPC (Evolved Packet Core). Для передачи сервисного информационного потока конкретной услуги B2C в сети LTE организуют составной сквозной E2E (end-to-end) виртуальный канал (bearer) соответствующего класса обслуживания QoS между двумя оконечными точками: либо между двумя оконечными устройствами UE (Urser Equetvitment), либо, например, между UE и каким-либо интернет-сервером. Соответственно этому, возникают понятия части сквозного канала, представленные на рис.1: радиоканал (radio bearer) между UE и eNB, S1- bearer между eNB и S-GW, канал радиодоступа E-RAB (E-UTRAN Radio Access Bearer) между UE и S-GW, S1-S5/S8- bearer между S-GW и P-GW, EPS-канал (EPS-bearer) выделенной пакетной системы EPS между UE и P-GW, внешний канал (external bearer) – между P-GW и внешней IP-сетью и др. Канал E-RAB является частью канала EPS-bearer [1]. Таким образом, канал EPS (EPS- bearer) — это маршрут, который пользовательский трафик (IP-потоки) использует между UE и P-GW.

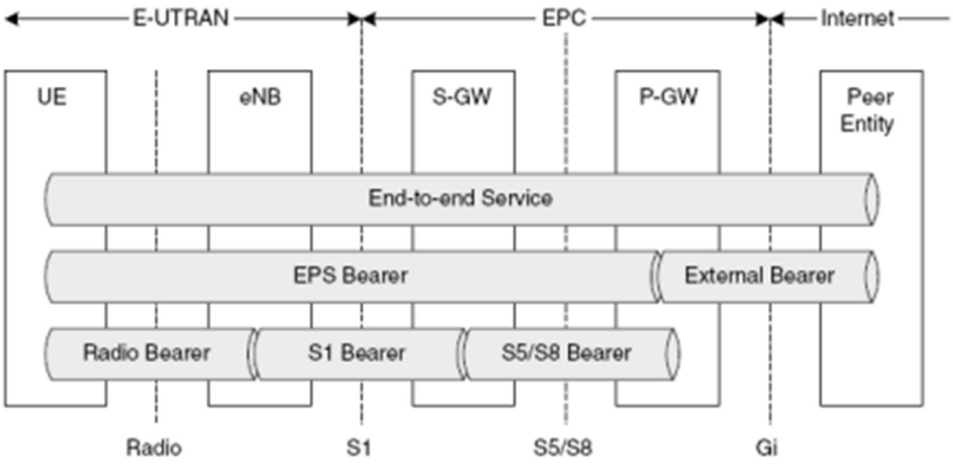


Рис.1. Архитектура сквозного канала в сети LTE.

Аналогично понятию сквозного канала вводится понятие сквозной услуги B2C в сети LTE — сервис E2E (end-to-end service) как последовательность действий между двумя оконечными пользователями и, соответственно, частей услуг — по их отношению к определённых сетевым составляющим: в локальном канале «оконечное оборудование—пользовательский терминал» (Terminal Equipment / Mobile Terminal local Bearer Service), в канале сети LTE (LTE Bearer Service), во внешнем канале (External Bearer Service). Таким образом, возникает многоуровневое взаимодействие при передаче услуги в различных сетевых узлах и на различных уровнях. В сетевой структуре LTE существует два разных уровня IP-сетей (рис.2).

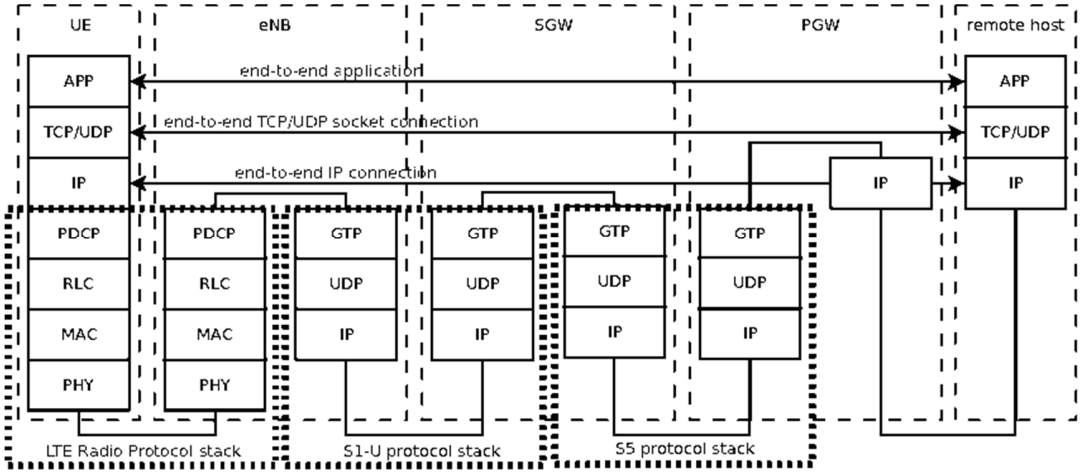


Рис. 2. Стек протоколов, используемый в пользовательской плоскости.

Первый — это сквозной уровень, который обеспечивает сквозное E2E соединение для пользователей. Этот уровень включает в себя UE, PGW и удаленный хост (включая возможные интернет-маршрутизаторы и хосты между ними), но не включает eNB и SGW. При этом LTE EPC может поддерживать протоколы типа IPv4 и IPv6. Второй уровень IP-сетей — это внутренняя сеть EPC. Она включает в себя все узлы eNB, узлы SGW и узлы PGW. Эта сеть реализована как набор двухточечных линий связи, которые соединяют каждый eNB с его соответствующим узлом SGW и двухточечной линии связи, которые соединяют каждый узел SGW с его соответствующим узлом PGW. Таким образом, каждый SGW имеет набор двухточечных устройств, каждое из которых обеспечивает возможность подключения к другому eNB. При передаче данных по сети пользовательские потоки должны пройти несколько интерфейсов (LTE-Uu, S1, S5/S8) прежде, чем они попадут во внешнюю сеть или на абонентский терминал. Сквозной E2E IP-канал туннелируется по внутренней IP-сети EPC с использованием двух туннелей на интерфейсах S1 и S5/S8. На интерфейсах S1 и S5/S8 каждый поток определяется идентификатором GTP (GPRS Tunneling Protocol туннеля [2]. GTP — это коммуникационный протокол, используемый LTE для доставки IP-пакетов внутри EPC. Как указано 3GPP, сквозная E2E IP-связь туннелируется по локальной сети EPC IP с использованием GTP / UDP / IP. Идентификатор конечной точки туннеля TEID (Tunneling End Identificater) генерируется каждым узлом во время начальной процедуры присоединения. Вновь сгенерированный TEID включается в тело каждого отправляемого сообщения и доставляется на одноранговый узел. Одноранговый узел воспринимает конечную точку GTP на основе полученного TEID. Пакеты, относящиеся к одному и тому же EPS потоку, всегда обрабатываются одинаковым образом. Схема реализации сквозного E2E канала EPS представлена на рис.3 [3].

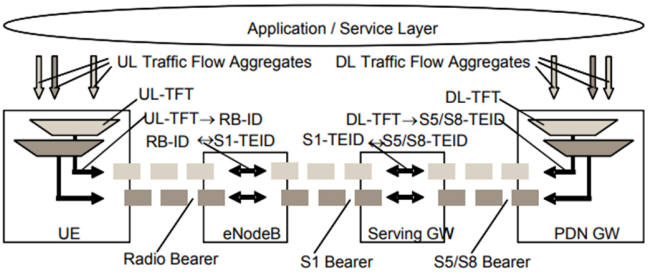


Рис.3. Схема реализация сквозного EPS-канала.

Рассмотрим кратко алгоритмы обработки пакетов в нисходящей и восходящей линии [4]. Алгоритм обработки пакетов в нисходящей линии следующий. При получении пакета из внешнего канала (external bearer) узел PGW: 1) фильтрует потоки IP через шаблоны SDF в различные SDF; 2) выполняет управление скоростью MBR для каждого SDF; 3) классифицирует пакет с использованием шаблонов потока трафика (TFT), чтобы определить, к какому каналу EPS он принадлежит (EBI). Каналы EPS имеют однозначное соответствие каналам S5, поэтому эта операция возвращает идентификатор конечной точки туннеля GTP-U (TEID), которому принадлежит пакет; 4) применяет QoS к каждому однонаправленному каналу EPS (управление скоростью MBR DL для каналов GBR и управление скоростью передачи DL APN-AMBR для каналов non-GBR); 5) добавляет соответствующий заголовок протокола GTP-U к пакету; 6) определяет узел SGW, на который он должен направить трафик для конкретного UE, путем просмотра IP-адреса назначения (который является адресом UE) и отправляет пакет через сокета UDP на двухточечный туннель S5, адресованный соответствующему SGW, где он принимается и доставляется локально

(в качестве адреса назначения самого внешнего заголовка IP соответствует IP-адресу SGW). Узел SGW выполняет следующие операции: 1) определяет узел eNB, к которому подключено UE, путем просмотра TEID S5; 2) отображает S5 TEID, чтобы получить S1 TEID. Каналы EPS имеют однозначное отображение на туннели S1-U, поэтому эта операция возвращает идентификатор конечной точки туннеля S1 GTP-U (TEID), которому принадлежит пакет; 3) добавляет новый заголовок протокола GTP-U к пакету; 4) отправляет пакет через сокет UDP в двухточечный туннель S1-U, адресованный узлу eNB, к которому подключено UE. Далее сквозной IP-пакет с вновь добавленными заголовками IP, UDP и GTP отправляется по одному из туннелей S1 на узле eNB, где он принимается и доставляется локально (так как адрес назначения самого внешнего заголовка IP совпадает с IP-адрес ом узла eNB). Узел eNB выполняет следующие операции: 1) удаляет заголовок GTP и извлекает содержащийся в нем TEID S1; 2) используя взаимно-однозначное сопоставление между однонаправленными туннелями S1-U и однонаправленными радиоканалами (что является требованием 3GPP), определяет идентификатор однонаправленного канала (BID), которому принадлежит пакет; 3) пересылает пакет в узел eNB. В этот момент самым верхним заголовком пакета является сквозной IP-заголовок, поскольку заголовки IP / UDP / GTP стека протоколов S1 уже удалены. После получения пакета eNB будет извлекать BID и на его основе будет определять экземпляр радиоканала (и соответствующие экземпляры протоколов PDCP и RLC), которые затем используются для пересылки пакета в UE через радиоинтерфейс LTE; 4) осуществляет контроль скорости передачи DL UE- AMBR.

UE, получив пакет, доставляет его локально в стек протоколов IP. Далее пакет доставляется в приложение UE, которое является конечной точкой связи нисходящей линии связи.

Алгоритм обработки пакетов в восходящей линии следующий. IP-пакеты восходящей линии связи генерируются приложением внутри UE и направляются локальным стеком TCP / IP в сетевой драйвер UE, который выполняет следующие операции: 1) классифицирует пакет с использованием фильтров TFT и определяет радиоканал, которому принадлежит пакет (и соответствующий RBID); 2) идентифицирует соответствующий экземпляр протокола PDCP, который является точкой входа в стек протокола радиосвязи LTE для этого пакета; 3) отправляет пакет в eNB через стек протокола радиосвязи LTE; 4) применяет политики QoS к каждому каналу EPS (с использованием UL MBR для каналов GBR и с использованием UL APN-AMBR для каналов non-GBR). Узел eNB принимает пакет через сетевое устройство, определяет BID пакета (т.к. для каждого однонаправленного радиоканала существует один экземпляр протокола PDCP и RLC) и отправляет пакет в EPC-приложение eNB. Затем EPC-приложение выполняет следующие операции: 1) получает BID из пакета; 2) определяет соответствующий экземпляр EPS-канала и TEID туннеля GTP-U путем использования взаимно-однозначного отображения между однонаправленными туннелями S1-U и радиоканалами; 3) добавляет заголовок GTP-U к пакету, включая TEID, определенный ранее; 4) применяет политики QoS к каждому каналу EPS (с использованием UL MBR для каналов GBR и с использованием UL APN-AMBR для каналов non-GBR); 5) отправляет пакет на узел SGW через сокет UDP, подключенный к сетевому устройству S1-U. На этом этапе пакет содержит заголовки IP, UDP и GTP S1-U в дополнение к первоначальному сквозному заголовку IP. Когда пакет принимается сетевым устройством SGW, он доставляется локально (так как адрес назначения самого верхнего IP-заголовка совпадает с адресом сетевого устройства «точка-точка»). Процесс локальной доставки переадресует пакет в EPC-приложение узла SGW через соответствующий сокет UDP, которое выполняет следующие операции:1) удаляет заголовок GTP и получает TEID S1-U; 2) отображает TEID S1-U для получения TEID S5, к которому принадлежит пакет; 3) определяет PGW, которому он должен отправить пакет из отображения TEID; 4) добавляет новый заголовок протокола GTP-U к пакету; 5) отправляет пакет через сокет UDP в сетевое устройство двухточечного туннеля S5, адресованного соответствующему PGW. На данный момент пакет содержит заголовки S5 IP, UDP и GTP в дополнение к исходному сквозному заголовку IP.

Когда пакет принят соответствующим двухточечным сетевым устройством S5 узла PGW он доставляется локально (так как адрес назначения самого верхнего IP-заголовка совпадает с адресом двухточечного сетевого устройства):

1) осуществляет контроль скорости передачи APN-AMBR всех IP-потоков каналов non-GBR;

2) производит фильтрацию пакетов IP (шаблоны SDF);

3) осуществляет контроль скорости MBR выполняется для каждого SDF (параметр UL MBR);

4) процесс локальной доставки переадресует пакет в EPC-приложение узла PGW через соответствующий сокет UDP;

5) EPC-приложение узла PGW удаляет заголовок GTP и пересылает пакет в сетевое устройство.

В этот момент самый верхний заголовок пакета является сквозным IP-заголовком. Следовательно, если адрес назначения в этом заголовке является удаленным хостом (например, в Интернете), пакет отправляется в Интернет.

Концепция качества сервиса QoS, используемая в сетях LTE, основана на классе, где каждому типу каналаносителя назначается один идентификатор класса качества обслуживания QCI (Quality Chanel Indicator) сетью. Идентификатор QCI – это механизм, используемый в сетях LTE для гарантии того, что трафику канала- носителя назначается соответствующее качество обслуживания QoS. Различному трафику каналаносителя требуется разное QoS и, следовательно, разные значения QCI. Значения QCI стандартизированы в стандарте 3GPP TS 23.203 «Policy and charging control architecture» [5] и связаны с конкретными характеристики QoS, такими

как (см. таблицу): приоритет планирования, тип ресурса (GBR и non-GBR), бюджет задержки пакета и коэффициент потери пакетов PERL (Packet Error Loss Rate).

В [5] перечислено 26 QCI, представляющих два типа канала-носителя (GBR, non-GBR), 21 значение риоритета, 9 значений бюджета задержки и 7 значений допустимости потерь. Задержка передачи пользовательских данных определяется как период времени между моментом, когда пакет данных доступен на IP уровне на UE/eNB, и моментом, когда этот же пакет доступен на IP уровне на eNB/UE. Характеристики каждого значения QCI используется оператором для предварительной конфигурации параметров, специфичных для узлов сети, чтобы гарантировать, что приложения/услуги, которые используются в сети LTE, отображаются на заданный индикатор QCI и получают одинаковый уровень QoS в мультивендорных средах, а также в сценариях роуминга.

Индикатор QCI используется в сети доступа на узлах eNB для контроля приоритета пакетов, доставляемых по радиоканалам. Кроме того, характеристики QCI также отображаются на параметры соответствующих узлов ядра базовой сети EPC (Evolved Packet Core) и параметры транзитных маршрутизаторов внешней мобильной IP-сети на технологии DiffServ [RFC 2475] оператора связи. Это реализуется с помощью предварительно сконфигурированного отображения индикатора QCI в определенные значения кода дифференцированных услуг DSCP (DiffServ Code Point). В качестве кодов DSCP используются шесть первых битов поля DS (Differentiated Service) заголовка пакета IPv6. Весь сетевой трафик внутри домена DiffServ получает определенный режим обслуживания PHB (Per-Hop Behavior) в зависимости от указанного в байте DS класса трафика, называемый «Режимом на переходе» из группы режимов PHB, поддерживаемых в пределах домена. Документ [RFC 2475] определяет PHB как комбинацию функций маршрутизации, классификации, обработки очередей и методов сброса пакетов на каждом шаге передачи пакета от узла к узлу внутри домена DiffServ. Режим PHB можно рассматривать как совокупность параметров, в соответствии с которыми маршрутизатор устанавливает порядок направления пакетов на интерфейс вывода. Это могут быть отдельные очереди с заданными приоритетами, определенные параметры для установления длины очереди или алгоритмы удаления пакетов из обращения в зависимости от их приоритета и веса.

Группа режимов — это набор одинаковых или различных режимов PHB, каждый из которых может быть реализован на УК одновременно с другими при обслуживании очередей. Пакеты «окрашенные» одинаковым кодом DSCP получат одинаковый класс сервиса в сеансе связи во всех транзитных маршрутизаторах домена выбранного маршрута посредством предоставления соответствующей услуги PHB для всего агрегированного потока. В технологии DiffServ реализованы два типа классов услуг PHB: немедленная переадресация пакетов (Expedited Forwarding, EF) и гарантированная доставка пакетов (Assured Forwarding, AF).

Услуга EF PHB в DiffServ, предоставляет пользователю гарантии по полосе пропускания и сквозной сетевой задержке для пакетов, проходящих через зарезервированный путь. Она аналогична услуге «гарантированной доставки» (Guaranteed Service), IntServ. При этом требования по вероятности потери пакета, значениям задержки и джиттера, необходимой полосе пропускания и т. д. гарантируются только в рамках домена DiffServ, на маршрутизаторах которого предоставляется услуга EF. Услуга AF PHB позволяет реализовать четыре класса QoS с тремя уровнями приоритета пакета для каждого из них.

Пакеты, принадлежащие различным классам обслуживания, маршрутизируются на каждом маршрутизаторе домена DiffServ отдельно друг от друга с выделением требуемых ресурсов. Услуга AF PHB может быть реализована с помощью нескольких типов механизмов управления очередями, например, Premium Queue для предоставления услуги Premium Service – «виртуальная арендованная линия», а услуга AF PHB - с помощью таких механизмов как, например, очереди в соответствии с классами CBQ (Class-Based Queuing) и RED (Random Early Detection).

Значение кода DSCP устанавливается в соответствии с заранее оговоренным уровнем сервиса в соответствии с характеристиками индикатора QCI и предоставляемым пользователю при поступлении от него потока пакетов на обслуживание. Например, для услуги немедленной переадресации EF рекомендуемое значение DSCP=101110. Стандартным значением DSCP по умолчанию является 000000.

В [6] определяется эквивалентное отображение идентификатора QCI в значение кода DSCP. В таблице 1 приведены рекомендации по маркировке QCI от 3GPP до [RFC4594] DSCP.

Таблица 1

Рекомендации по маркировке QCI от 3GPP до [RFC4594] DSCP

CI	Тип ресурса	Уровень приоритета	Примеры услуг	Рекомендуемый DSCP (PHB)
1	GBR	2	Разговорный голос	44 (BA)
2	GBR	4	Разговорное видео (прямая трансляция)	35 (нет данных)
3	GBR	3	Игры в реальном времени, сообщения V2X, распределение электроэнергии (среднее напряжение) Автоматизация процессов (мониторинг)	19 (нет данных)
4	GBR	5	Видео без разговора (буферизованная потоковая передача)	37 (нет данных)

65	GBR	0,7	Голосовая связь для критически важных пользователей (например, MCPTT).	42 (нет данных)
66	GBR	2	Нажимайте и говорите голосом на уровне пользователя, не являющегося критически важным.	43 (нет данных)
67	GBR	1.5	Самолет пользователя Mission Critical Video	33 (нет данных)
75	GBR	2,5	Сообщения V2X	17 (нет данных)
82	GBR	1.9	Дискретная автоматизация (небольшие пакеты)	27 (нет данных)
83	GBR	2.2	Дискретная автоматизация (большие пакеты)	29 (нет данных)
84	GBR	2,4	Интеллектуальные транспортные системы	31 (нет данных)
85	GBR	2.1	Распределение электроэнергии - высокое напряжение	25 (нет данных)
5	Не-GBR	1	Сигнализация IMS	40 (CS5)
6	Не-GBR	6	Видео (буферизованная потоковая передача) на основе TCP (например, www, электронная почта, чат, ftp, совместное использование файлов p2p, прогрессивное видео)	10 (AF11)
7	Не-GBR	7	Голос, видео (прямая трансляция), интерактивные игры	38 (AF43)
8	Не-GBR	8	Видео (буферизованная потоковая передача) на основе TCP (например, www, электронная почта, чат, ftp, совместное использование файлов p2p, прогрессивное видео)	12 (AF12)
9	Не-GBR	9	То же, что и 8	14 (AF13)
69	Не-GBR	0,5	Критически важная сигнализация, чувствительная к задержке (например, сигнализация MC-PTT, сигнализация MC Video)	41 (нет данных)
70	Не-GBR	5.5	Критически важные данные (например, примеры услуг такие же, как QCI 6/8/9)	20 (AF22)
79	Не-GBR	6.5	Сообщения V2X	21 (нет данных)
80	Не-GBR	6,8	Приложения eMMB с низкой задержкой (на основе TCP / UDP); дополненная реальность	32 (CS4)

В зависимости от значения QCI сеть LTE предоставляет определенные механизмы для обеспечения качества обслуживания QoS [7]. Однако на практике узлам ядра EPC LTE и транзитным маршрутизаторам внешних операторов сложно одновременно обрабатывать и пересылать пакеты на основе характеристик QCI и требования сквозного QoS могут не соблюдаться, особенно внутри зашифрованного туннеля. Кроме того, например, маршрутизаторы Cisco или Juniper при обслуживании пакетов только решают вопрос очередности их отправки с помощью механизмов планирования (WFQ, DWRR, SPQ и др.) исходя из приоритета пакетов без учета задержки, уровня ошибок и потерь. Это требует ручной настройки параметров QoS на узлах ядра сети и узлах внешних операторов. При этом, если в любом месте сквозного соединения E2E LTE на транзитных маршрутизаторах имеются неправильные настройки, то сервисы B2C, не будут должным образом предоставлены сетью для пользователя с требуемым качеством вплоть до полной их деградации. В этом случае UE не может применить сквозную маркировку Diffserv. Стандарты 3GPP не определяют и не рекомендуют какое-либо конкретное сопоставление между каждым QCI и Diffserv и оставляют выбор этого сопоставления оператору границы пограничного домена. Однако 3GPP определяет, что «для магистрали на основе IP должны использоваться дифференцированные услуги, определенные IETF» ([TS 23.107] v15 6.4.7) [5]. В справочном Руководстве по межсетевому соединению IP Backbone [IR.34] Ассоциации GSM (GSMA) представлены технические рекомендации поставщикам услуг по сопоставлению 1-9 индикаторов QCI и Diffserv. Однако эти два плана неоднозначно трактуют согласование трафика Diffserv как в услугах, так и в указанных для них кодовых точках.

Кроме того, новые индикаторы QCI могут потребовать новых классов трафика и маркировки Diffserv. В этом случае можно, например, группировать несколько QCI в иерархические группы, которые затем могут быть преобразованы в ансамбли, согласованные с логикой Diffserv. Этот подход, в свою очередь, позволяет включать новые QCI по мере развития модели 3GPP [6].

Необходимо отметить, что в IPv6 также имеются дополнительные механизмы для «окраски» пакета в сеансе связи, что можно использовать для более тонкой настройки взаимно однозначного преобразования параметров Diffserv в параметры QCI и наоборот. Например, новая версия протокола IPv6 помимо расширения адресного пространства до 128 битовых адресов, позволяет ввести также масштабируемость групповых (multicast) адресов и

определить новый тип адреса anycast (кому-нибудь) для передачи пакетов любому узлу из группы. Кроме того, IPv6 расширяет набор опций заголовка, в число которых входят: Hop-by-Hop, Routing (Type 1), Fragment, Destination Option, Authentication, Encapsulation Payload. Кроме того, 4-битовое поле «приоритет» в IPv6 заголовке позволяет отправителю идентифицировать относительный приоритет доставки пакетов (таблица 2).

Таблица 2

Значения кодов поля «приоритет» в заголовке IPv6

Код приоритета	Назначение
0	Нехарактеризованный трафик
1	Заполняющий трафик (например, сетевые новости)
2	Несущественный информационный трафик (например, электронная почта)
3	Резерв
4	Существенный трафик (напр., FTP, HTTP, NFS)
5	Резерв
6	Интерактивный трафик (напр. telnet, x)
7	Управляющий трафик Интернет (например, маршрутные протоколы, snmp)
8-15	Мультимедийная информация

Значения приоритетов делятся на два диапазона. Коды от 0 до 7 используются для задания приоритета трафика, для которого отправитель осуществляет контроль перегрузки (например, снижает поток TCP в ответ на сигнал перегрузки). Значения с 8 до 15 используются для определения приоритета трафика, для которого не производится снижения потока в ответ на сигнал перегрузки, например, в случае пакетов «реального времени», посылаемых с постоянной частотой.

Для «окраски» пакета в сеансе связи может быть использовано и поле заголовка IPv6 «метка потока». Поле «метка потока» позволяет выделять и особым образом обрабатывать отдельные потоки данных без необходимости анализировать содержимое пакетов. Поле «метка потока» в заголовке пакета IPv6 может использоваться отправителем для указания на специальную обработку пакета в маршрутизаторе с целью обеспечения требуемого QoS или сервиса реального времени «real-time».

«Окраска» потока, пакеты которого требуют соответствующей обработки в маршрутизаторе, может также осуществлена посредством протокола управления или в заголовках пакетов, например, в опции «hop-by-hop».

Выводы. Стандарты 3GPP не определяют и не рекомендуют какое-либо конкретное сопоставление между каждым QCI и Diffserv по настройках параметров QoS сквозного канала связи E2E при конвергенции сетей LTE и фиксированных IP-сетей и оставляют выбор этого сопоставления оператору границы пограничного домена. Однако при этом необходимо учитывать рекомендации документов [TS 23.107] v15 6.4.7 и [IR.34].

Для более тонкой настройки взаимно однозначного преобразования параметров Diffserv в параметры QCI и наоборот можно использовать дополнительные механизмы для «окраски» пакета IPv6 в сеансе связи (поле 4-битовое поле заголовка IPv6 «приоритет», «метка потока»)

Более тонкая настройка взаимно однозначного преобразования параметров Diffserv в параметры QCI и наоборот может также осуществлена посредством настройки параметров протокола управления или в заголовках пакетов, например, в опции «hop-by-hop» для соответствующей обработки в маршрутизаторе.

СПИСОК ЛИТЕРАТУРЫ

1. Гельгор А.Л. Технология LTE мобильной передачи данных: учеб. пособие / Гельгор А.Л., Попов Е.А. — СПб.: Изд-во Политехн. ун-та, 2011. — 204 с.
2. Мошак Н.Н., Харитонов Г.Д. ОРГАНИЗАЦИЯ ТРАНСПОРТНЫХ ТУННЕЛЕЙ В ЯДРЕ СЕТИ LTE. Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 9 / СПОИСУ. – СПб., 2020. – 304 с. ISBN 978-5-907223-89-9, с. 268-270 http://spoisu.ru/news/165-ri-2020-finish
3. Тихвинский В.О., Терентьев С.В., Высочин В.П. Сети мобильной связи LTE/LTEAdvanced: технологии 4G, приложения и архитектура. – М.: Издательский дом Медиа Паблишер, 2014. – 384 с.
4. До М., Якименко С.И. QoS в LTE (часть 2). [Электронный ресурс] Режим доступа: http://masters.donntu.org/2018/fkita/yakymenko/library/article11.
5. 3GPP TS 23.203 version 15.4.0 Release 15 [Электронный ресурс] Режим доступа: https://www.etsi.org/deliver/etsi_ts/.
6. Diffserv to QCI Mapping-01 - IETF Tools [Электронный ресурс] Режим доступа: https://tools.ietf.org › draft-he...
7. Мошак Н.Н., Харитонов Г.Д. МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ QOS В СЕТИ LTE. Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября Р32 2020 г.: Материалы конференции. Часть 2. \ СПОИСУ. – СПб, 2020. – 335 с. ISBN 978-5-907223-86-8, с. 296-297. http://www.spoisu.ru/conf/ri2020/materials.

УДК 025.2.004; 621.311.23: 629.12

ИНТЕРВАЛЬНЫЙ АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ БИБЛИОТЕК

Паращук Игорь Борисович, Крюкова Елена Сергеевна
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: shchuk@rambler.ru, e.kkrukovaa69@yandex.ru

Аннотация. Рассматриваются вопросы анализа сущности и содержания этапов метода интервального анализа информационной безопасности современных электронных библиотек. Анализируются показатели информационной безопасности, последовательность реализации стадий их интервального анализа, функции и задачи этих стадий. Исследование проводилось с целью систематизации и выявления особенностей определения интервальных (нижней и верхней) оценок информационной безопасности электронных библиотек на основе методов теории интервальных средних в интересах достоверного анализа и повышения качества управления структурой, параметрами и режимами работы систем информационной безопасности для сложных управляемых объектов такого класса.

Ключевые слова: электронная библиотека; информационная безопасность; показатель; состояние; качество; анализ; контроль; оценка; интервальные средние.

INTERVAL ANALYSIS OF INFORMATION SECURITY OF ELECTRONIC LIBRARIES

Parashchuk Igor, Kryukova Elena
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: shchuk@rambler.ru, e.kkrukovaa69@yandex.ru

Abstract. The article deals with the analysis of the essence and content of the stages of the method of interval analysis of information security of modern electronic libraries. The information security indicators, the sequence of implementation of the stages of their interval analysis, the functions and tasks of these stages are analyzed. The study was conducted to systematize and identify the features of determining interval (lower and upper) estimates of information security of electronic libraries based on the methods of the theory of interval averages in the interests of reliable analysis and improving the quality of management of the structure, parameters and modes of operation of information security systems for complex managed objects of this class.

Keywords: electronic library; information security; indicator; status; quality; analysis; control; evaluation; interval averages.

Введение. Современные электронные библиотеки (ЭБ) считаются важным элементом сложных управляемых информационных систем, они занимают все более существенное место в Едином информационном пространстве России [1-3]. Общепринятые подходы, составляющие основу методологии анализа состояния информационной безопасности таких ЭБ, анализа качества защиты информации в ЭБ и эффективности функционирования подсистем защиты информации в рамках ЭБ, обычно ориентированы на использование обобщенных (комплексных) показателей информационной безопасности (ИБ) и связаны с интегрированием (по пороговым значениям параметров и показателей ИБ) совместных плотностей распределения вероятностей, описывающих эти показатели информационной безопасности [4].

Не секрет, что такие текущие совместные плотности распределения вероятностей имеют размерность $K\times M\times T$, где K – число показателей информационной безопасности ПИБ системы (например, ЭБ), M – число состояний этих ПИБ ЭБ, а T – число временных отсчетов анализа ПИБ ЭБ. Этот факт обуславливает необходимость использования при оценивании обобщенных (комплексных) ПИБ ЭБ процедуры непосредственного K-кратного интегрирования совместной плотности распределения вероятностей размерности $K\times M\times T$, что приводит к высокой математической и вычислительной сложности решения задач такого класса. При этом осуществляется точечный, текущий анализ ИБ, что не всегда эффективно с точки зрения управления ИБ ЭБ на интервалах времени. Это обуславливает актуальность формулировки и решения задачи построения методики интервального анализа ИБ современных ЭБ, оценки защищенности ЭБ на любом (t+Δt)-ом временном интервале ее функционирования [5].

При этом показатели ИБ ЭБ могут быть сгруппированы в систему ПИБ (СПИБ), которая, в отличие от традиционных, содержит показатели в виде текущих отклонений параметров ИБ ЭБ от требований к ним.

Так, текущий векторный ПИБ, который характеризует такие наиболее важные свойства системы защиты ЭБ, как доступность, целостность, конфиденциальность информации, хранимой, обрабатываемой и передаваемой в ЭБ, ресурсопотребление на реализацию процесса обеспечения безопасности информации в ЭБ и имеет вид:

$$\Delta\vec{Y}_{\text{ф}}(t+\Delta t)=[\Delta\bar{t}_{\text{дост}}^{\,\text{усл}\,/\,\text{угр}}(t+\Delta t);\ \Delta K_{\text{п дост}}(t+\Delta t);\ \Delta K_{\text{иск}}(t+\Delta t);\ \Delta K_{\text{конф инф}}(t+\Delta t);\ \Delta\vec{З}_{\text{ф}}(t+\Delta t)]^{\text{т}},\qquad(1)$$

где доступность характеризует $\Delta\bar{t}_{\text{дост}}^{\,\text{усл}\,/\,\text{угр}}(t+\Delta t)$ – отклонения времени доступа легальных (авторизированных) пользователей к защищаемому информационному ресурсу на (t+Δt)-ом интервале функционирования ЭБ; целостность (достоверность и неискаженность информации, несмотря на наличие угроз и уязвимостей) характеризуют $\Delta K_{\text{п дост}}(t+\Delta t)$ – отклонения коэффициента потери достоверности информации и $\Delta K_{\text{иск}}(t+\Delta t)$ – отклонения коэффициента искажений информации на (t+Δt)-ом интервале функционирования ЭБ; конфиденциальность (способность ЭБ сохранять информацию в тайне от субъектов, не имеющих полномочий на доступ к ней) характеризует $\Delta K_{\text{конф инф}}(t+\Delta t)$ – отклонения коэффициента конфиденциальности хранимой, обрабатываемой и передаваемой информации на (t+Δt)-ом интервале функционирования ЭБ.

Помимо этого, выражение (1) содержит отклонения вектора затрат ресурсов $\Delta\vec{З}_{ф}(t+\Delta t)$ на построение подсистемы ИБ ЭБ и реализацию процесса функционирования этой подсистемы на (t+Δt)-ом интервале функционирования электронной библиотеки.

Вектор (1) представляет собой формализованную запись глобальной СПИБ, характеризующей общую задачу, стоящую перед подсистемой ИБ ЭБ. Система показателей ИБ ЭБ может включать глобальную СПИБ и локальные СПИБ процесса обеспечения ИБ ЭБ, процесса управления обеспечением ИБ ЭБ, комплекса средств обеспечения ИБ и подсистемы управления.

Ведущей среди локальных систем показателей информационной безопасности ЭБ выступает локальная СПИБ процесса обеспечения ИБ, компоненты которой во многом аналогичны компонентам глобальной СПИБ ЭБ и содержат векторы частных показателей доступности легальных (авторизированных) пользователей ЭБ к защищаемому информационному ресурсу, непрерывности процесса обеспечения ИБ ЭБ, целостности информации при реализации этого процесса, конфиденциальности информации и вектор показателей затрат ресурсов на реализацию процесса обеспечения ИБ ЭБ на (t+Δt)-ом интервале ее функционирования

$$\Delta\vec{Y}_{оиб}(t+\Delta t)=[\Delta\vec{Y}_{дост}(t+\Delta t);\Delta\vec{Y}_{непр}(t+\Delta t);\Delta\vec{Y}_{цел}(t+\Delta t);\Delta\vec{Y}_{конф}(t+\Delta t);\Delta\vec{З}_{оиб}(t+\Delta t)]^{т}. \quad (2)$$

Функции управления процессом обеспечения ИБ делают возможным собственно процесс защиты информации в ЭБ, поэтому локальная СПИБ управления процессом обеспечения ИБ имеет более низкий уровень иерархии по сравнению с локальной СПИБ данного процесса и включает: отклонения длительности цикла управления параметрами процесса обеспечения ИБ при нарушении нормальных условий функционирования ЭБ (t+Δt)-ом интервале; отклонения вектора приращений значений показателей процесса обеспечения ИБ (определяющего точность управления этим процессом) на (t+Δt)-ом интервале функционирования электронной библиотеки, обусловленных ошибками в контуре управления; отклонения времени доступности потенциального нарушителя к сигналам и командам управления процессом обеспечения ИБ на (t+Δt)-ом интервале функционирования ЭБ и отклонения вектора затрат ресурсов управления на (t+Δt)-ом интервале функционирования ЭБ и реализации процесса обеспечения ее ИБ

$$\Delta\vec{Y}_{у}(t+\Delta t)=[\Delta T_{цу}(t+\Delta t);\Delta\vec{Y}^{у}_{оиб}(t+\Delta t);\Delta\bar{t}_{ду}(t+\Delta t);\Delta\vec{З}_{у}(t+\Delta t)]^{т}. \quad (3)$$

Материальной основой процесса обеспечения ИБ электронной библиотеки и управления этом процессом являются два ключевых элемента подсистемы ИБ ЭБ: комплекс средств обеспечения ИБ и подсистема управления, иерархия которых определяется иерархией осуществляемых ими процессов и иерархией управления.

Компонентами локальной СПИБ комплекса средств обеспечения ИБ ЭБ являются векторы отклонений от требуемых значений показателей производительности, устойчивости, разведзащищенности, достоверности функционирования, масштабируемости, совместимости, мультисервисности, безопасности и ресурсопотребления данного комплекса на (t+Δt)-ом интервале функционирования электронной библиотеки:

$$\begin{aligned}\Delta\vec{Y}_{ксоиб}(t+\Delta t)=[&\Delta\vec{Y}_{пр\ ксоиб}(t+\Delta t);\Delta\vec{Y}_{уст\ ксоиб}(t+\Delta t);\Delta\vec{Y}_{рз\ ксоиб}(t+\Delta t);\Delta\vec{Y}_{достов\ ксоиб}(t+\Delta t);\\ &\Delta\vec{Y}_{масшт\ ксоиб}(t+\Delta t);\Delta\vec{Y}_{совмест\ ксоиб}(t+\Delta t);\Delta\vec{Y}_{м/серв\ ксоиб}(t+\Delta t);\Delta\vec{Y}_{безоп\ ксоиб}(t+\Delta t);\Delta\vec{З}_{ксоиб}(t+\Delta t)]^{т}.\end{aligned} \quad (4)$$

Заключительной, но, не менее важной, в иерархии систем показателей ИБ является СПИБ подсистемы управления комплексом средств обеспечения ИБ ЭБ, имеющая вид

$$\Delta\vec{Y}_{пу}(t+\Delta t)=[\Delta V^{уср}_{тех\ пу}(t+\Delta t);\Delta T_{цу\ пу}(t+\Delta t);\Delta\vec{Y}^{у}_{пу}(t+\Delta t);\Delta\bar{t}_{бсф\ пу}(t+\Delta t);\Delta\bar{t}_{ду\ пу}(t+\Delta t);\Delta\vec{З}_{пу}(t+\Delta t)]^{т} \quad (5)$$

и включающая отклонения от требуемых значений показателей технической производительности подсистемы управления, оперативности (своевременности, длительности цикла) управления, достоверности, устойчивости, непрерывности и скрытности управления комплексом средств обеспечения ИБ, а также затраты ресурсов на реализацию подсистемы управления на (t+Δt)-ом интервале функционирования электронной библиотеки.

Таким образом, предложенная СПИБ ЭБ, развитая на случай динамического интервального анализа информационной безопасности систем такого класса, обладая полнотой и безизбыточностью, вместе с тем, позволяет расширить диапазон исследуемых характеристик защищенности современных электронных библиотек. Такой подход справедлив для сложных динамичных и инерционных систем с жестким замкнутым контуром управления, у которых имеется достаточный ресурс для поддержания показателей ИБ в области требуемых значений.

С учетом этого, предлагаемые и исследуемые подходы к интервальному анализу ИБ, рассмотренные нами ПИБ ЭБ (1)–(5) и параметры процесса смены их состояний на определенном (t+Δt)-ом временном интервале, имеют очевидные преимущества.

Предлагаемая совокупность методов оптимального анализа частных ПИБ ЭБ на определенном временном интервале, основанная на методах теории интервальных средних и методах теории фильтрации, позволяет, в отличие от общепринятых комплексных методов, значительно сократить размерность задачи анализа, предполагая наличие двухэтапной процедуры:

Первый этап – применение модели процесса смены состояний ПИБ ЭБ в виде непрерывных цепей Маркова в форме разностных стохастических уравнений, что позволяет свести размерность задачи к $K\times M\times\tau$, где τ – временные интервалы оценивания ПИБ ЭБ [6].

Второй этап – замена процедуры непосредственного K-кратного интегрирования совместной плотности распределения вероятностей размерности $K\times M\times\tau$ процедурами сбора данных наблюдения (или моделирования) и вычисления оценочных значений нижнего и верхнего средних уровней ИБ (частных ПИБ) элементов ЭБ и ИБ ЭБ в целом на интервале времени $(\tau+\Delta\tau)$ с использованием методов теории интервальных средних.

Таким образом, предлагаемый метод интервального анализа частных ПИБ ЭБ на определенном временном интервале, основанный на постулатах теории интервальных средних и алгоритмах оптимальной фильтрации (экстраполяции), позволяет осуществить переход к текущей пошаговой фильтрации ПИБ ЭБ и к получению оценочных значений нижнего и верхнего средних уровней ИБ (частных ПИБ) ЭБ на интервале времени $(\tau+\Delta\tau)$ с использованием методов теории интервальных средних.

При этом временной интервал оценивания $(\tau+\Delta\tau)$ включает конечное множество T непрерывных отсчетов наблюдения (моделирования): $(\tau+\Delta\tau)=\{(t_1+\Delta t)+(t_2+\Delta t)+\ldots+(t_T+\Delta t)\}$.

Взаимосвязь перечисленных этапов и влияющих факторов представлена на рис. 1.

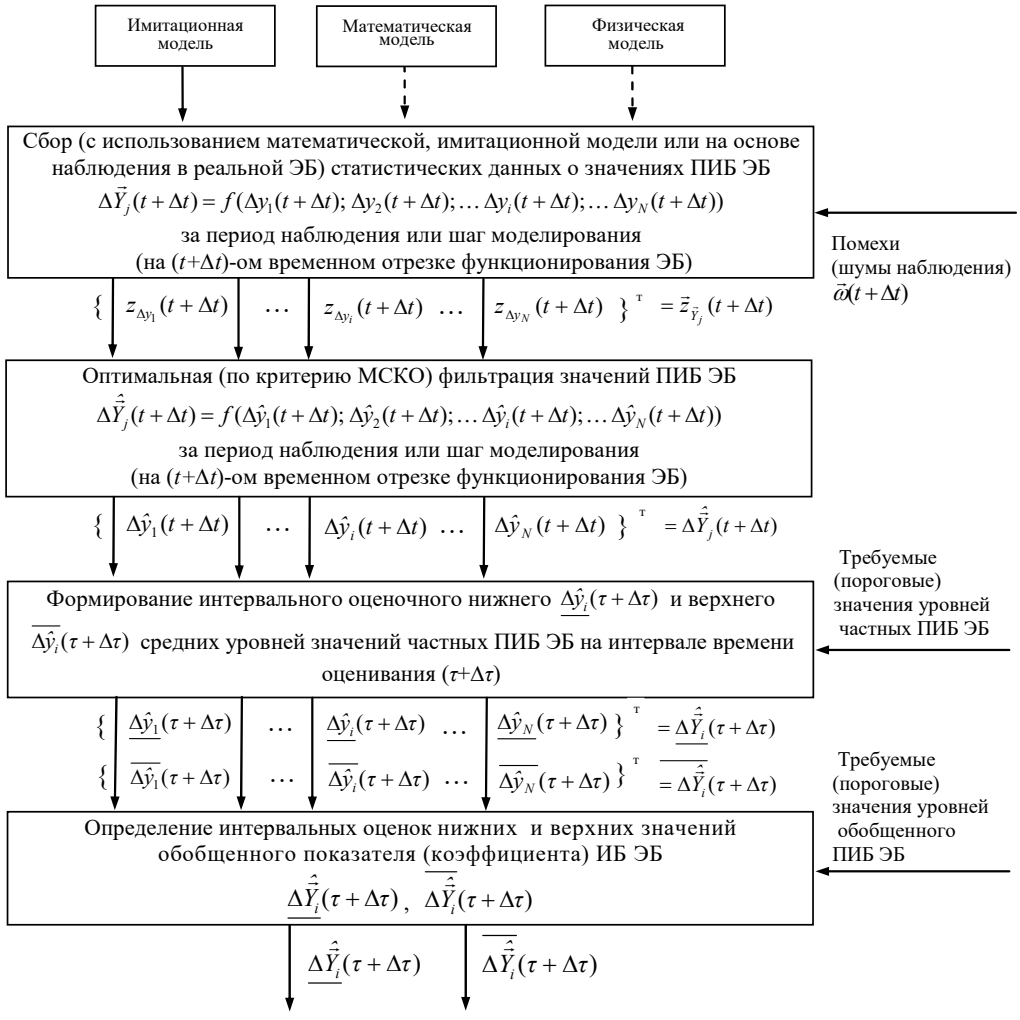


Рис. 1. Этапы метода интервального анализа информационной безопасности электронных библиотек.

Как видно из рис. 1, ключевыми стадиями интервального анализа частных показателей ИБ ЭБ являются:

Стадия сбора (с использованием математической, имитационной модели или на основе наблюдения в реальной ЭБ) статистических данных о значениях ПИБ ЭБ за период наблюдения или шаг моделирования (на $(t+\Delta t)$-ом временном отрезке функционирования ЭБ),

$$\Delta\vec{Y}_j(t+\Delta t)=f(\Delta y_1(t+\Delta t);\Delta y_2(t+\Delta t);\ldots\Delta y_i(t+\Delta t);\ldots\Delta y_N(t+\Delta t)),\qquad(6)$$

где $\Delta y_1(t+\Delta t); \Delta y_2(t+\Delta t); \ldots \Delta y_i(t+\Delta t); \ldots \Delta y_N(t+\Delta t)$ – частные ПИБ ЭБ, рассмотренные нами в рамках выражений (1)–(5).

Стадия оптимальной по критерию минимального среднего квадрата ошибки (МСКО) фильтрации значений показателей ИБ электронных библиотек за период наблюдения или шаг моделирования (на (t+Δt)-ом временном отрезке функционирования ЭБ), которую можно представить в виде выражения

$$\Delta\hat{\tilde{Y}}_j(t+\Delta t) = f(\Delta\hat{y}_1(t+\Delta t); \Delta\hat{y}_2(t+\Delta t); \ldots \Delta\hat{y}_i(t+\Delta t); \ldots \Delta\hat{y}_N(t+\Delta t)). \quad (7)$$

Стадия формирования интервального оценочного нижнего $\underline{\Delta\hat{y}_i}(\tau+\Delta\tau)$ и верхнего $\overline{\Delta\hat{y}_i}(\tau+\Delta\tau)$ средних уровней значений каждого из ПИБ ЭБ на интервале времени оценивания (τ+$\Delta\tau$) на основе оценочных значений этих ПИБ за все непрерывные отсчеты (периоды) наблюдения или шаги моделирования (t+Δt), составляющие в сумме содержание шага оценивания (τ+$\Delta\tau$).

Стадия определения интервальных оценок нижних $\underline{\Delta\hat{\tilde{Y}}_i}(\tau+\Delta\tau)$ и верхних $\overline{\Delta\hat{\tilde{Y}}_i}(\tau+\Delta\tau)$ значений обобщенного показателя (коэффициента) ИБ ЭБ с учетом результатов интервальных оценок (идентификации) ее частных показателей информационной безопасности.

Таким образом, в рамках рассмотренных стадий интервального анализа показателей ИБ ЭБ (см. рис. 1), на основе статистического анализа измеряемых (наблюдаемых, моделируемых) параметров ИБ и с использованием методов теории интервальных средних находят нижний и верхний средние уровни ИБ элементов ЭБ и ИБ ЭБ в целом на интервале времени (τ+$\Delta\tau$). Рассчитывается точное нижнее $\underline{\Delta\hat{y}_i}(\tau+\Delta\tau)$ и верхнее $\overline{\Delta\hat{y}_i}(\tau+\Delta\tau)$ значения среднего уровня частных ПИБ ЭБ, наблюдаемых на интервале времени оценивания (τ+$\Delta\tau$), путем решения задачи линейного программирования на основе средних значений идентифицированных параметров ИБ системы [5, 7].

Особого внимания, на наш взгляд, заслуживает заключительная стадия – определение интервальных оценок обобщенного показателя (коэффициента) ИБ ЭБ с учетом результатов интервального анализа (идентификации) параметров ИБ системы. При этом для систем с мультипликативным обобщенным показателем (коэффициентом) ИБ, используется соотношение, характеризующее функцию взаимосвязи обобщенных показателей (коэффициентов) ИБ ЭБ с частными j-ми (j=1, … , J) показателями ИБ ЭБ:

$$\underline{\Delta\hat{\tilde{Y}}}(\tau+\Delta\tau) = \prod_j^J \underline{\Delta\hat{\tilde{Y}}_j}(\tau+\Delta\tau); \quad (8)$$

$$\overline{\Delta\hat{\tilde{Y}}}(\tau+\Delta\tau) = \min_{j=1,\ldots,J} \overline{\Delta\hat{\tilde{Y}}_j}(\tau+\Delta\tau). \quad (9)$$

Заключение. Таким образом, в соответствии с предложенным методологическим подходом могут быть получены интервальные частные (нижняя и верхняя) оценки ИБ и обобщенная оценка ИБ ЭБ на основе методов теории интервальных средних. Полученные интервальные результаты анализа ИБ, оценочные значения параметров ИБ системы за интервал времени, позволят повысить достоверность оценивания защищенности ЭБ, что, в конечном итоге, сыграет свою важную роль в повышении качества управления информационной безопасностью, управления структурой, параметрами и режимами работы подсистем защиты информации для современных электронных библиотек.

СПИСОК ЛИТЕРАТУРЫ

1. Зуйкина К.Л., Соколова Д.В., Скалабан А.В. Электронные библиотеки в России. Текущий статус и перспективы развития. – М.: Ваш формат, 2017. 120 с.
2. Антопольский А.Б., Маркарова Т.С., Крюкова О.П., Харламов А.А. Электронные библиотеки в образовании / Под редакцией О.П. Крюковой, А.А. Харламова. – М.: 2009. 94 с.
3. Национальный стандарт Российской Федерации ГОСТ Р 7.0.96 - 2016. Электронные библиотеки. Основные виды. Структура. Технология формирования. – М.: Стандартинформ, 2016. 13 с.
4. Авраменко В.С., Тарасов А.В. Прогнозирование защищенности информации в автоматизированных системах специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019): сборник научных статей VIII Международной научно-технической и научно-практической конференции. Т. 4., – СПб.: ГУТ им. А.А. Бонч-Бруевича. 2019. С. 19-24.
5. Гуров С.В., Уткин Л.В. Надежность систем при неполной информации. – СПб.: Любавич, 1999. 160 с.
6. Крюкова Е.С. Модель функционирования электронной библиотеки для анализа ее качества и информационной безопасности // Вопросы оборонной техники. Научно-технический журнал. Технические средства противодействия терроризму. Серия 16. Выпуск № 9-10 (147-148), 2020. С. 16-22.
7. Крюкова Е.С., Малофеев В.А., Паращук И.Б. Анализ современных подходов к оценке качества систем хранения данных и электронных библиотек // Новые информационные технологии и системы: сборник научных статей XVI Международной научно-технической конференции (г. Пенза, 27–29 ноября 2019 г.). – Пенза: Изд-во ПГУ, 2019. С. 177-180.

УДК 004.056.5

ОЦЕНКА ПОТЕНЦИАЛА И ОБЗОР ОСОБЕННОСТЕЙ ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ТЕЛЕКОММУНИКАЦИЙ ОТ СЕТЕВЫХ АТАК

Паращук Игорь Борисович, Малофеев Валерий Александрович, Морозов Иван Васильевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: shchuk@rambler.ru, valeron12.1366@gmail.com, moroz_i.v@mail.ru

Аннотация. Проведены сравнительная оценка потенциала и анализ особенностей современных программных средств защиты (обнаружения и противодействия) телекоммуникаций от сетевых атак. Полученные в ходе исследования данные могут помочь при оценивании эвентуальной эффективности применения тех или иных средств обнаружения вредоносных воздействий с учетом достоинств и недостатков рассмотренных программных средств. Результаты анализа позволят повысить обоснованность принятия решений при выборе систем обнаружения атак в интересах обеспечения защиты данных в телекоммуникационной сети или системе.

Ключевые слова: защита; обнаружение; сетевая атака; программное средство; телекоммуникационная сеть; система; воздействие; блокирование; угроза; ресурс.

EVALUATION OF THE POTENTIAL AND REVIEW OF THE FEATURES OF SOFTWARE TOOLS FOR PROTECTING TELECOMMUNICATIONS FROM NETWORK ATTACKS

Parashchuk Igor, Malofeev Valery, Morozov Ivan
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: shchuk@rambler.ru, valeron12.1366@gmail.com, moroz_i.v@mail.ru

Abstract. A comparative assessment of the potential and analysis of the features of modern software protection (detection and counteraction) of telecommunications against network attacks is carried out. The data obtained in the course of the study can help in evaluating the eventual effectiveness of the use of various means of detecting malicious influences, taking into account the advantages and disadvantages of the considered software tools. The results of the analysis will increase the validity of decision-making when choosing attack detection systems in the interests of ensuring data protection in a telecommunications network or system.

Keywords: protection; detection; network attack; software; telecommunications network; system; impact; blocking; threat; resource.

Введение. Защита и обеспечение безопасности телекоммуникационных сетей и систем была и остается приоритетной задачей для специалистов. Их задача заключается в наиболее эффективной нейтрализации угроз, которые могут нарушить конфиденциальность, целостность и доступность данных, циркулирующих, обрабатываемых и хранящихся в рамках телекоммуникационных сетей и систем.

Угрозы безопасности данных, циркулирующих в телекоммуникационных сетях и системах – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, используемой сетью (системой), а также условиями обработки и хранения данных.

Одной из самых опасных угроз являются сетевые атаки – злоумышленные действия (мероприятия, процедуры), целью которого является захват контроля над удаленной локальной телекоммуникационной сетью или системой. Помимо этого, сетевые атаки нацелены на отказ в обслуживании либо дестабилизацию сети, а также получение личных идентификационных данных пользователей, являющихся абонентами (пользователями) этой удаленной локальной телекоммуникационной сети или системы.

Иными словами, сетевая атака – информационное разрушающее воздействие на распределенную IT-инфраструктуру, телекоммуникационную сеть или систему, осуществляемое программно по каналам связи. Это направленные действия на удаленные сервера для создания затруднений в работе или для утери данных. Важнейшим этапом противодействия сетевым атакам является этап их выявления и классификации, предназначенный для выяснения (идентификации) их происхождения, характера воздействия и степени опасности.

При этом принято различать сетевые атаки на телекоммуникационные сети или системы: атаки типа mailbombing, переполнение буфера, атаки с использованием специализированных вредоносных программ (вирусов, снифферов, троянских коней, почтовых червей и т.д.), сетевая разведка, IP-спуфинг, man-in-the-middle, атаки типа «инъекция» (PHP-инъекция, SQL-инъекция, межсайтовый скриптинг или XSS-атака, XPath-инъекция), атака типа «отказ в обслуживании» (DoS- и DDoS- атаки), а также «фишинг»-атаки.

Сниффер-атаки – анализаторы трафика телекоммуникационные сети, программы или устройства для оценки и перехвата своего или чужого сетевого трафика. IP-спуфинг – тип атаки, при которой один человек или программа

(IP-адрес) успешно маскируется под другую программу, путем фальсификации данных и позволяет получить незаконные преимущества.

Сетевая атака man-in-the-middle или атака »человек посередине» – вид атаки, при которой злоумышленник перехватывает и подменяет сообщения, которыми обмениваются пользователи телекоммуникационные сети, причем ни один из пользователей не догадывается о присутствии нарушителя в канале [1, 2].

При этом, в рамках комплексной защиты информации, циркулирующей в телекоммуникационные сети, от актуальных угроз, наиболее вредоносными принято считать сетевые атаки типа «захват» (системы, данных, управления, информации), типа «срыв» (нарушение, деградация, отрицание, уничтожение) и типа «манипуляция» (внешней информацией, датчиками, беспроводными сенсорами и подмена системной информации) [3, 4].

Существует несколько ключевых направлений обеспечения безопасности телекоммуникаций от сетевых атак. Это реализация устойчивости к сетевым атакам, аутентификация данных, контроль доступа, а также реализация приватности пользователя телекоммуникационные сети.

Защита от сетевых атак должна выполняться следующими методами: псевдослучайная смена сетевых адресов; блокирование соединения; блокирование хоста сети; блокировка трафика от сетевого хоста (целиком, или на основе некоторых критериев); снижение интенсивности трафика телекоммуникационные сети; внесение изменений в трафик (например, удаление атакующих последовательностей); передача данных другим системам, а также комбинацией вышеперечисленных методов.

Базовым инструментом обнаружения сетевых атак являются программы и программные комплексы, способные выявлять (идентифицировать) и блокировать воздействия такого типа. Причем обнаружение атак – динамический процесс определения и реагирования на любую подозрительную деятельность, направленную на сетевые или вычислительные ресурсы телекоммуникаций.

Результативность данного процесса зависит от методов анализа входной сетевой информации. Например, методы обнаружения хакерских атак используют результаты анализа контролируемых пространств (сетевой трафик или журналы регистраций). Этот метод основан на статистике и на наборе правил экспертных систем. В дополнение к этим подходам, зачастую используются нейронные сети, позволяющие анализировать информацию и оценить, насколько согласуются полученные данные с характеристиками атак, которые нейронная сеть может распознавать.

Проведем сравнительный анализ потенциала и обзор особенностей современных программных средств защиты телекоммуникаций от сетевых атак. Рассмотрим популярные и зарегистрированные в реестре ФСТЭК России программные комплексы и системы обнаружения атак, такие как:

- система обнаружения атак «ФОРПОСТ»;
- система обнаружения вторжений Dallas Lock;
- система ViPNet HIDS;
- система Security Capsule SIEM;
- система Kaspersky Anti Targeted Attack;
- система обнаружения вторжений «Кречет».

Система обнаружения сетевых атак «ФОРПОСТ» предназначена для автоматического выявления воздействий на контролируемую телекоммуникационную сеть или систему, которые могут быть классифицированы как сетевые атаки или вторжения, а также для блокировки развития выявленных сетевых атак. Достоинствами этой системы является ее способность обнаруживать и предотвращать развитие сетевых атак, направленных на сервера телематических служб (WEB, FTP, электронная почта, СУБД пр.) и рабочие станции, размещенные в контролируемых сегментах телекоммуникационной сети; анализ сетевого трафика со второго по седьмой уровень сетевой модели стека сетевых протоколов OSI/ISO; обработка сетевого трафик на скоростях до 10 Гбит/с; контроль целостности собственных ресурсов системы обнаружения атак и ресурсов защищаемой телекоммуникационные сети; ведение журнала системных сообщений и генерация отчетов на основе содержимого журнала; оповещение об обнаруженных атаках и новых сообщениях в системных журналах путем вывода соответствующего сообщения на консоль администратора системы обнаружения атак, записи сообщения в специальный журнал, путем отправки сообщений по электронной почте; возможность удаленного управления сетевым оборудованием телекоммуникационные сети по защищенному с использованием отечественных средств криптографической защиты информации каналу.

Кроме того, система дает возможность интеграции с внешними системами путем передачи сообщений о зафиксированных сетевых атаках из журнала системы обнаружения атак по протоколу syslog (стандарт отправки и регистрации сообщений о происходящих в системе событиях (то есть создания событийных журналов), использующийся в телекоммуникационных сетях, работающих по протоколу IP.).

Этот продукт обладает подсистемой собственной безопасности, которая позволяет шифровать передаваемую между компонентами информацию с использованием отечественных средства комплексной защиты информации, осуществлять контроль целостности собственных ресурсов и ресурсов защищаемой телекоммуникационной сети или системы [5].

Система обнаружения вторжений Dallas Lock предназначена для противодействия сетевым атакам различной степени сложности.

Эта система способна реализовывать целый ряд функций: эвристический и сигнатурный анализ попыток нарушения безопасности; гибкие настройки реагирования на попытки нарушения безопасности (уведомления, блокировки IP-адреса злоумышленника и т.д.); механизмы обнаружения вторжений на основе анализа служебной информации протоколов сетевого уровня телекоммуникационной сети; выявление аномалий в действиях пользователя телекоммуникационной сети; мандатный и дискреционный контроль доступа к объектам файловой системы и устройствам телекоммуникационной сети; механизм делегирования полномочий.

Кроме того, эта система способна реализовывать проверку целостности системы защиты информации, программно-аппаратной среды и реестра телекоммуникационной сети; локальное администрирование авторизованными пользователями телекоммуникационной сети; межсетевое экранирование; анализ журналов операционных систем рабочих мест пользователей телекоммуникационной сети; разграничение доступа к файловой системе, реестру и устройствам телекоммуникационной сети; преобразование информации в файлах-контейнерах; преобразование сменных накопителей для защиты от несанкционированного доступа в обход системы защиты информации; прозрачное преобразование жестких дисков; контроль подключаемых устройств; контроль целостности и др. [6].

Также в состав Dallas Lock входит безопасная среда Dallas Lock («песочница»). Она представляет собой среду для безопасного исполнения приложений защиты информации в телекоммуникационной сети. Пользователь может запустить любое программное обеспечение и протестировать его в изолированной, защищенной среде. Ресурсы операционной системы рабочих мест пользователей телекоммуникационной сети при этом будут в безопасности. «Песочница» является эмулятором среды функционирования программного обеспечения (ПО) рабочих мест пользователей телекоммуникационной сети, что позволяет: запускать и выполнять работу ПО в изолированной, защищенной среде без внесения изменений в окружение операционной системы; осуществлять проверку ПО рабочих мест пользователей телекоммуникационной сети на опасные действия с целью определения степени доверия к такому программному обеспечению [6].

Программно-аппаратный комплекс ViPNet HIDS предназначен для обнаружения вторжений в телекоммуникационные сети или системе. Это реализуется на основе динамического анализа сетевого трафика стека протоколов TCP/IP на серверах (хостах) защищаемой телекоммуникационной сети.

Преимущество данной системы заключается в особых возможностях: хостовые системы, в отличие от сетевых, собирают информацию и выявляют признаки вторжений непосредственно на серверах (хостах) защищаемой телекоммуникационной сети.

Эти системы следят не только за сетевыми атаками, но и за событиями, происходящими в операционных системах сетевых устройств и рабочих мест пользователей телекоммуникационной сети. Расположение ViPNet HIDS на защищаемых узлах телекоммуникационной сети позволяет с большой точностью и достоверностью определить пользователя, процессы и выполняемые действия, которые приводят к вторжениям (атакам). Такая система не требует большой вычислительной мощности и дополнительной функциональности сетевых устройств телекоммуникационной сети [7].

Система Security Capsule SIEM предназначена для мониторинга и управления событиями безопасности телекоммуникационных сетей или систем. Она позволяет: обрабатывать события информационной безопасности; управлять событиями безопасности информации телекоммуникационных сетей; контролировать состояние информационной безопасности телекоммуникационных сетей; управлять информацией об угрозах безопасности информации; оценивать эффективность применяемых средств защиты телекоммуникационных сетей, систем защиты информации; оценивать полноту и корректность настроек средств и механизмов защиты, включая механизмы защиты, встроенные в операционные системы, системы управления базами данных, коммуникационное оборудование, прикладное программное обеспечение телекоммуникационных сетей; оценивать соответствие состояния информационной безопасности телекоммуникационных сетей требованиям регуляторов.

Помимо этого, система Security Capsule SIEM позволяет управлять инцидентами информационной безопасности, использовать данные о событиях при разборе инцидентов, контролировать и управлять учетными записями пользователей телекоммуникационных сетей, реализовать ролевой метод доступа и разграничение доступа пользователей телекоммуникационных сетей к объектам доступа, определять состав и содержание информации о событиях безопасности от различных источников, осуществлять просмотр и анализ результатов регистрации и реагировать на них (регистрационные журналы с регламентированным доступом), редактировать регистрационные формы, а также восстанавливать работоспособность в полном объеме после сбоев и отказов программных и программно-аппаратных частей [8].

Система Kaspersky Anti Targeted Attack позволяет своевременно обнаруживать многоступенчатые действия злоумышленников в телекоммуникационной сет и противодействовать им на всех этапах за счет: специализированной платформы для противодействия комплексным угрозам на уровне сети; минимизации последствий от целевых атак путем оперативного выявления направленных действий злоумышленников; наглядной визуализации и прозрачности корпоративной инфраструктуры; автоматизации процесса сбора и хранения информации и цифровых улик. Эта системе имеет сформированный и отлаженный процесс анализа инцидентов с помощью передовых технологий на базе машинного обучения. В ней сокращено количество задач по ручному

обнаружению угроз. Она может: сопоставлять данные, получаемых в режиме реального времени, с ретроспективными данными и вердиктами от механизмов детектирования; сводить все полученные данные в единый инцидент информационной безопасности для оперативного расследования и реагирования; автоматизировать задачи по расследованию инцидентов и, как следствие, оптимизировать расходование ресурсов служб информационной безопасности телекоммуникационных сетей.

Преимущества платформы Kaspersky Anti Targeted Attack: сокращение рисков информационной безопасности телекоммуникационных сетей; повышение продуктивности и качества работы сотрудников по защите телекоммуникационных сетей и соответствующих департаментов; оптимизация трудозатрат высококвалифицированных кадров; сокращение количества рутинных ручных операций; увеличение количества обрабатываемых инцидентов без дополнительных трудозатрат; сбор, хранение и предоставление информации об инцидентах безопасности в рамках требований внутреннего и внешнего регулирования.

Иными словами, она обладает средствами наглядной визуализации, опирается на прозрачность инфраструктуры телекоммуникационных сетей или систем. Эта система позволяет автоматизировать процессы сбора и хранения информации и «цифровых улик». Система способна готовить данные для оперативного расследования и реагирования, автоматизировать задачи расследования инцидентов и, как следствие, позволяет оптимально расходовать ресурсы служб безопасности телекоммуникаций [9].

Система обнаружения вторжений «Кречет» – программный инструмент, реализующий в телекоммуникационной сети или системе функции автоматизированного обнаружения и блокирования действий, нацеленных на несанкционированный доступ к данным, негативных воздействий на информацию в целях ее добычи, модификации (изменения) и блокирования доступа к ней. Данное программное средство встраивается в существующую сетевую инфраструктуру и анализирует копию сетевого трафика, проходящего через пограничное устройство телекоммуникационной сети. На основе системы обнаружения вторжений «Кречет» может быть построена система обнаружения, регистрации и классифицирования сетевых атак на телекоммуникационные сети или системы. Система обнаружения вторжений «Кречет» выпускается в виде ПО для установки на сетевых устройствах телекоммуникационных сетей, а также может поставляться совместно с аппаратной платформой, подходящей под требования защищаемой телекоммуникационной сети.

Данная система обнаружения вторжений, подключаясь в соответствующий порт пограничного сетевого устройства телекоммуникационной сети, анализирует копию сетевого трафика, проходящего через это пограничное устройство. Кроме того, существует возможность подключения система обнаружения вторжений «Кречет» к нескольким пограничным сетевым устройствам одновременно, при многочисленном выходе защищаемой телекоммуникационной сети в сторонние сети.

Система обнаружения вторжений «Кречет» способна выявить как «плохой» трафик и использование эксплоитов (выявление Shellcode), так и распознать сканирование системы и атаки на службы (такие как Telnet, FTP, DNC и другие), выявить атаки, связанные с web-серверами и атаки на базы данных, различные Backdoors, web-фильтры и вирусы [10].

Заключение. Таким образом, проведены сравнительная оценка потенциала и обзор особенностей современных программных средств защиты телекоммуникаций от сетевых атак. Полученные в ходе исследования данные могут дать реальную возможность осуществить анализ потенциальной эффективности применения тех или иных средств обнаружения вредоносных воздействий с учетом достоинств и недостатков рассмотренных программных средств.

Помимо этого, результаты анализа, по мнению авторов, позволят повысить обоснованность принятия решений при выборе систем обнаружения атак в интересах обеспечения защиты данных в телекоммуникационной сети или системе.

СПИСОК ЛИТЕРАТУРЫ

1. Бокова О.И. Оптимальное управление безопасностью территориальных сегментов информационно-телекоммуникационных систем: монография / О.И. Бокова. – Воронеж: Воронежский институт МВД России, 2006. 153 с.
2. Miller D., Harris S., Harper A., VanDyke S. Security Information and Event Management (SIEM) Implementation. – London: McGraw-Hill. 2010. 464 p.
3. Паращук И.Б., Чернявский А.В., Шестаков Е.О. Эффективность комплексной защиты информации в системах хранения данных и электронных библиотеках: модели и методы оценивания. // Информационная безопасность регионов России (ИБРР-2019) XI-я Санкт-Петербургская Межрегиональная конференция, Материалы конференции, – СПб.: СПОИСУ, 2019. С. 248-250.
4. Авраменко В.С., Бобрешов-Шишов Д.И., Беденков В.Н., Маликов А.В. Определение актуальных угроз безопасности информации в инфокоммуникационных системах на основе аппарата нечеткой логики // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017). VI Международная научно-техническая и научно-методическая конференция. Т.3. – СПб.: СПБГУТ, 2017. С.13-18.
5. Система обнаружения атак «Форпост» версия 3.0. [Электронный ресурс] // Акционерное общество «Российские наукоемкие технологии» (АО «РНТ»). URL: https://www.rnt.ru/ru/production/detail.php?ID=689 (дата обращения 27.04.2021).
6. Обнаружение и предотвращение вторжений. [Электронный ресурс] // ООО «Конфидент». URL: https://dallaslock.ru/resheniya/obnaruzhenie-i-predotvraschenie-vtorzhenii/ (дата обращения 26.04.2021).
7. ViPNet IDS. [Электронный ресурс] // Компания «ИнфоТеКС». URL: https://infotecs.ru/product/setevye-komponenty/vipnet-ids/ (дата обращения 26.04.2021).
8. Система мониторинга и корреляции событий информационной безопасности Security Capsule SIEM. [Электронный ресурс] // Инновационные технологии в бизнесе. URL: https://www.itb.spb.ru/products/Security_Capsule_SIEM/ (дата обращения 27.04.2021).
9. Kaspersky Anti Targeted Attack. Комплексная защита от сложных угроз и целевых атак. [Электронный ресурс] // ОАО «Лаборатория Касперского». URL: https://www.kaspersky.ru/enterprise-security/anti-targeted-attack-platform (дата обращения 27.04.2021).
10. Система обнаружения вторжений «Кречет». [Электронный ресурс] // НПП «Гамма». URL: https://nppgamma.ru/catalog/setevaya_bezopasnost/krechet/ (дата обращения 27.04.2021).

УДК 004.7

ИССЛЕДОВАНИЕ ТИПОВ ФРЕЙМОВ, ПРИМЕНЯЕМЫХ ДЛЯ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ

Петров Владислав Андреевич, Ковцур Максим Михайлович, Кистуга Антон Юрьевич, Штеренберг Станислав Игоревич

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
[2] ООО «Фаст Лайн»
Профессора Попова ул., 37В, Санкт-Петербург, 197136, Россия
e-mails: vladpetrovvv@gmail.com, maxkovzur@mail.ru, anton.kistruga@gmail.com, shterenberg.stanislaw@yandex.ru

Аннотация. В современном обществе, где развитие технологий продвигается ежесекундно, требуется системы, способные обеспечивать контроль за каждой сферой жизни. Количество беспроводных устройств неуклонно растет, равно как и количество задач, для которых они предназначены. Развитие технологий позволило осуществить прорыв в области компьютерных микропроцессоров, уменьшении и повышении эффективности аккумуляторных батарей и т.д. Что в свою очередь привело к задаче позиционирования узлов в беспроводных сетях стандарта IEEE 802.11. В статье будут рассмотрены способы позиционирования на основе данных, получаемых на сетевом интерфейсе беспроводного устройства с дальнейшей обработкой их при помощи анализатора сетевого трафика — Wireshark.

Ключевые слова: беспроводные сети; IEEE 802.11; Wireshark; RSSI; Wi-Fi.

INVESTIGATION FRAME TYPES USED TO DETERMINE LOCATION

Petrov Vladislav, Kovtsur Maxim, Kistruga Anton, Shterenberg Stanislav

[1] The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
[2] LLC «Fast Lane»
37B Professor Popov St, St. Petersburg, 197136, Russia
e-mails: vladpetrovvv@gmail.com, maxkovzur@mail.ru, anton.kistruga@gmail.com, shterenberg.stanislaw@yandex.ru

Abstract. In modern society, where the development of technology advances every second, systems are required that can ensure control over every area of life. The number of wireless devices is growing steadily, as well as the number of tasks for which they are designed. The development of technology has made it possible to make a breakthrough in the field of computer microprocessors, reduce and increase the efficiency of batteries, etc. This, in turn, led to the task of positioning nodes in wireless networks of the IEEE 802.11 standard. The article will discuss positioning methods based on data received on the network interface of a wireless device with their further processing using a network traffic analyzer - Wireshark.

Keywords: wireless networks; IEEE 802.11; Wireshark; RSSI; Wi-Fi.

Введение. В беспроводных сетях, при передаче данных, используется множество видов служебной информации. Она позволяет устройствам более качественно взаимодействовать друг с другом, решая проблему отладки, мониторинга основных показателей, загруженности сети и т.д. Для устройств, работающих в стандарте IEEE 802.11 — Received Signal Strength (RSS) является одним из методов, позволяющим измерить расстояние от устройства до базовой станции или другого узла в сети.

Метод RSS использует RSSI (англ. Received Signal Strength Indicator) — индикатор уровня принимаемого сигнала, т. е. полная мощность принимаемого устройством сигнала. Суть метода заключается в измерении уровня приходящего радиосигнала, на основе которого может быть определена величина затухания сигнала в радиоканале (путевые потери), являющаяся функцией расстояния между передающей и принимающей антеннами. Эта функция задается заранее на основе опытных экспериментов и задается, в зависимости от параметров антенн приемника и передатчика, мощности усилителя и т.д. Измеряется по логарифмической шкале в дБм (децибел относительно 1 милливатта).

Структурная схема метода позиционирования представлена на рис. 1. Этот метод является наиболее доступным, т.к. практически все беспроводные приемопередатчики измеряют уровень входного сигнала и возвращают параметр RSSI [1].

Таким образом, в статье будут рассмотрены методы, на основе которых можно осуществить позиционирование устройств в беспроводной сети посредством принимаемого уровня RSSI.

Уровень RSSI выделяется на сетевой карте принимающего устройства и служит качественной мерой принимаемых пакетов. Например, для тестируемой в дальнейшем точки доступа (ТД) допустимая мощность приема на скорости 300 Мбит/с составляет -71 дБм. При худших значениях передаваемые фреймы будут приняты с ошибкой и станут «нечитаемы» для сетевой карты.

Для перехвата и анализа фреймов, передаваемых в эфире по стандарту IEEE 802.11 можно использовать различное ПО. Данный тип программ предназначен для перехвата, хранения и последующего анализа сетевого

трафика, предназначенного для своих или других узлов. Также, анализатор трафика имеет и другое название – сниффер. Анализироваться могут лишь те данные, которые проходят через его сетевую карту.

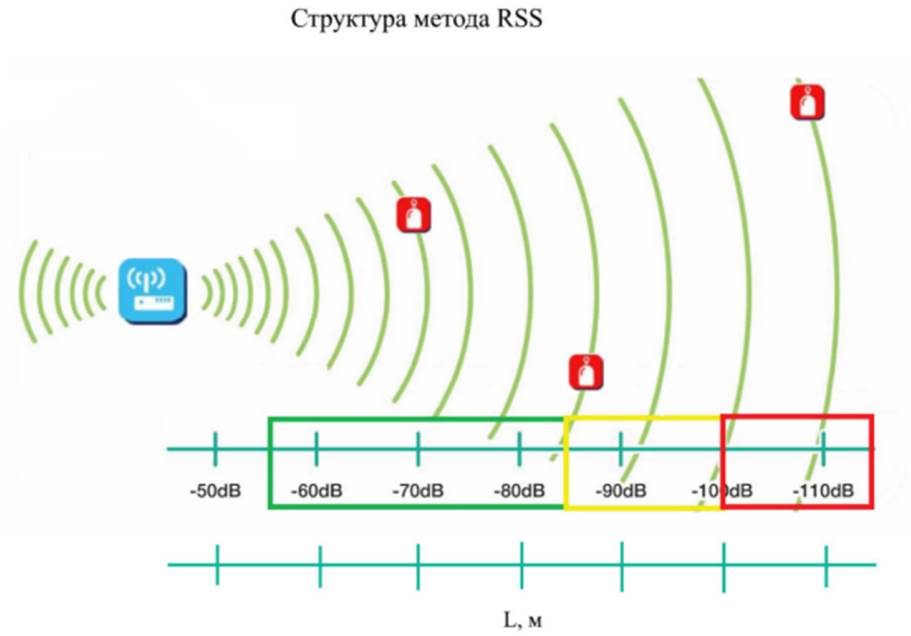


Рис. 1. Структура позиционирования при помощи метода RSS.

Одна из программ, применяемая для анализа сетевого трафика — Wireshark. Данная программа поддерживает разбор большого количества различных сетевых протоколов, а также предоставляет возможность сортировки и фильтрации трафика. В режиме реального времени пользователь данного сниффера имеет возможность просматривать весь проходящий по сети трафик. Таким образом, данная программа может показать частоту следования фреймов, чтобы в дальнейшем сделать вывод о том, в каких случаях (поиск ТД, передача файлов, подключение к ТД, отключение от ТД и т.д.) на фреймах какого тип следует основываться для определения местоположения [2]. Пример структуры Radiotap фрейма в программе Wireshark представлен на рис. 2.

```
> Frame 5: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface wlan0, id 0
v Radiotap Header v0, Length 26
    Header revision: 0
    Header pad: 0
    Header length: 26
  > Present flags
    MAC timestamp: 2508536723
  > Flags: 0x00
    Data Rate: 24,0 Mb/s
    Channel frequency: 2462 [BG 11]
  > Channel flags: 0x00c0, Orthogonal Frequency-Division Multiplexing (OFDM), 2 GHz spectrum
    Antenna signal: -66 dBm
    Antenna: 0
  > RX flags: 0x0000
v 802.11 radio information
    PHY type: 802.11g (ERP) (6)
    Short preamble: False
    Proprietary mode: None (0)
    Data rate: 24,0 Mb/s
    Channel: 11
    Frequency: 2462MHz
    Signal strength (dBm): -66 dBm
    TSF timestamp: 2508536723
  > [Duration: 32µs]
v IEEE 802.11 Null function (No data), Flags: ...P...T
    Type/Subtype: Null function (No data) (0x0024)
  > Frame Control Field: 0x4811
    .000 0001 0101 1000 = Duration: 344 microseconds
    Receiver address: Tp-LinkT_05:28:f6 (a4:2b:b0:05:28:f6)
    Transmitter address: e6:ec:8a:33:4b:c2 (e6:ec:8a:33:4b:c2)
    Destination address: Tp-LinkT_05:28:f6 (a4:2b:b0:05:28:f6)
    Source address: e6:ec:8a:33:4b:c2 (e6:ec:8a:33:4b:c2)
    BSS Id: Tp-LinkT_05:28:f6 (a4:2b:b0:05:28:f6)
    STA address: e6:ec:8a:33:4b:c2 (e6:ec:8a:33:4b:c2)
    .... .... .... 0000 = Fragment number: 0
    0101 0111 0011 .... = Sequence number: 1395
```

Рис. 2. Экран программы Wireshark с отображенным Radiotap случайного фрейма.

На рис. 2 видно, что для передаваемой мощности отведен специальный параметр — Antenna signal, выражаемый в дБм.

Данные собирались в офисной сети, в качестве ТД выступает Omada EAP110, имеющая всенаправленные антенны MIMO 2*2 с коэффициентом усиления 4 дБи и ЭИИМ <= 19 дБм, работающая в стандарте 2,4 ГГц, в 11 канале.

В качестве принимающего устройства используется мобильный телефон POCO F1, с антенной MIMO 2 * 2 и мощностью передатчика находящимся в нелицензируемом диапазоне (ЭИИМ ≤ 20 дБм). Схема эксперимента приведена на рис. 3.

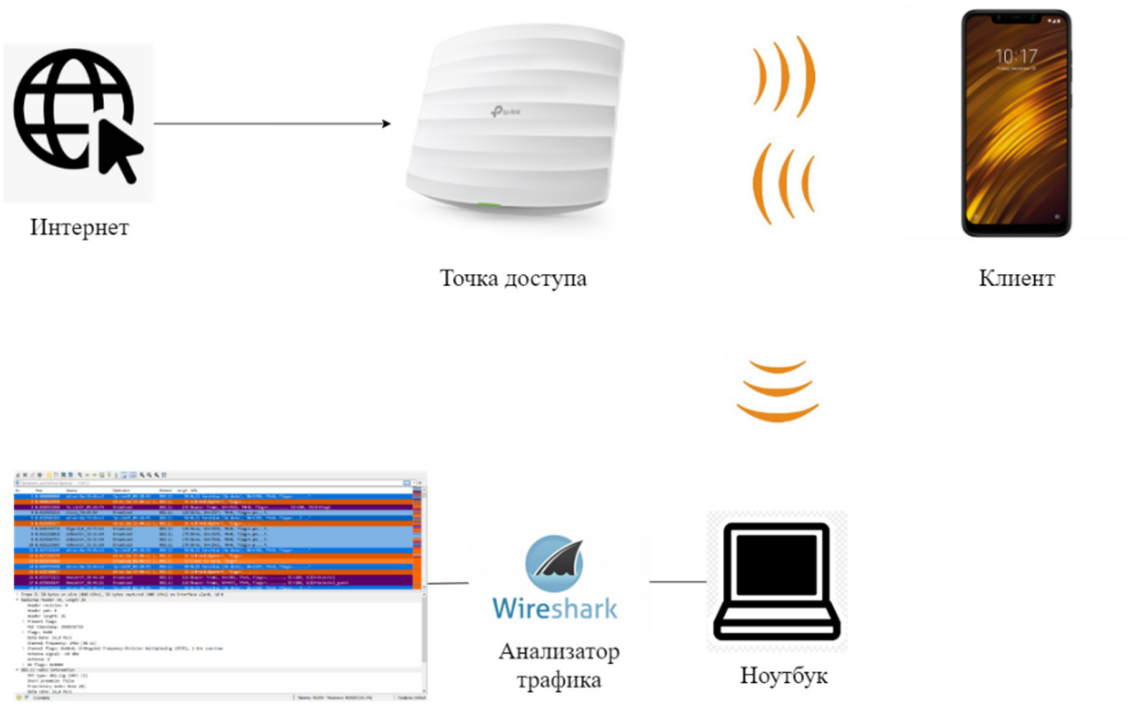


Рис. 3. Схема эксперимента.

Для работы сети IEEE 802.11 используется несколько типов беспроводных фреймов: management, control, data. Стоит сразу отметить, что основываться на типе фреймов, использующих технологию MIMO, не стоит, так как это будет вносить значительные ошибки в точность и объективность позиционирования. В процессе исследования вычислялась частота следования каждого типа кадров. Для очевидности, в программе Wireshark они выделены разным цветов относящимся к соответствующим группам. На рис. 4 показаны отношения цвета к типу фреймов.

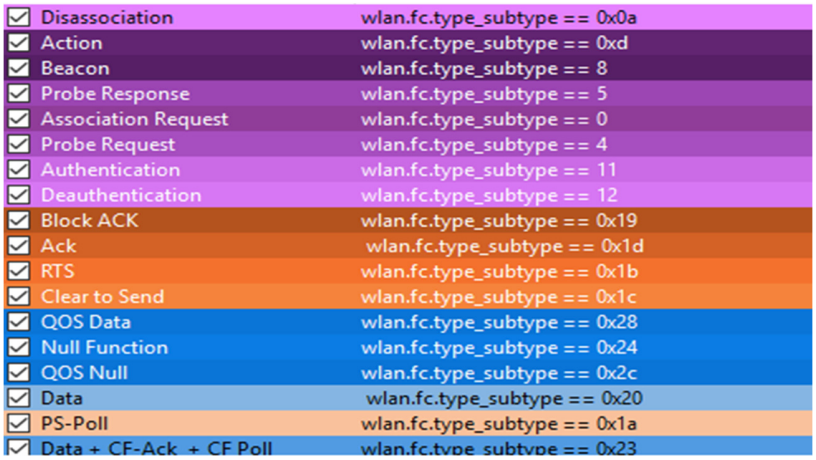


Рис. 4. Типы фреймов и их цветовая маркировка.

Для получения замеров требуется компьютер с сетевой картой, которая способна переключаться в режим мониторинга. Перехват трафика производится для всех устройств участвующих в исследовании, с последующей фильтрацией и подсчетом числа фреймов разных типов. На рис. 5 показан пример перехваченного фрейма в программе Wireshark [3-4]. Замеры проходили в несколько этапов, в различных условиях:

000-100 с. мониторинг ТД Wi-Fi на телефоне выключен;
100-200 с. режим сканирования сетей;
200-300 с. подключение и отключения от сети несколько раз подряд;
300-500 с. телефон подключен к ТД и не передает данных;
500-700 с. телефон подключен к ТД и на нем запущено потоковое видео в разрешении 2К.

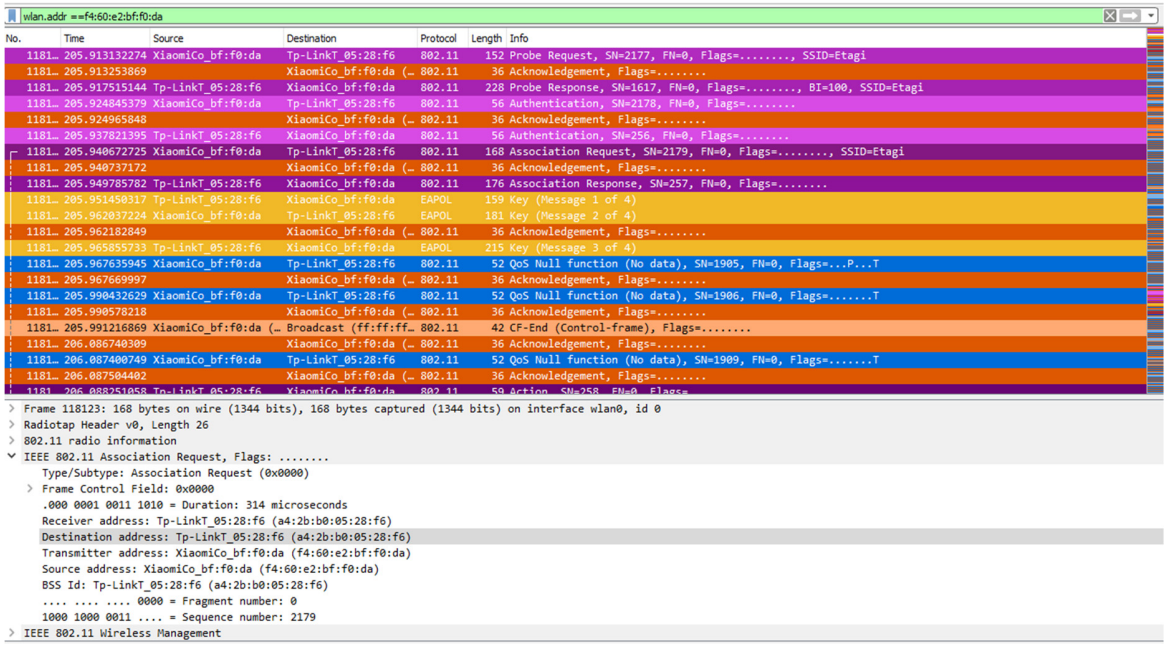


Рис. 5. Пример перехваченных пакетов.

Полученные графики, в которых замеряется частота следования фреймов каждого типа, представлены на следующих рисунках.

На рис. 6 показана частота появления management фреймов, в процессе всего снятия дампа. На графике в промежутке 100 - 200 с. отсутствует передача фреймов, это связано с тем, что у клиента в памяти нет каких-либо сетей, к которым он ранее подключался, а кроме того, политики безопасности на нем настроены таким образом, чтобы не выполнять активного сканирования беспроводной сети. Данная политика настроена по умолчанию для данного устройства. Видно, что частота появления низкая, и данные передаются преимущественно в процессе соединения с точкой доступа.

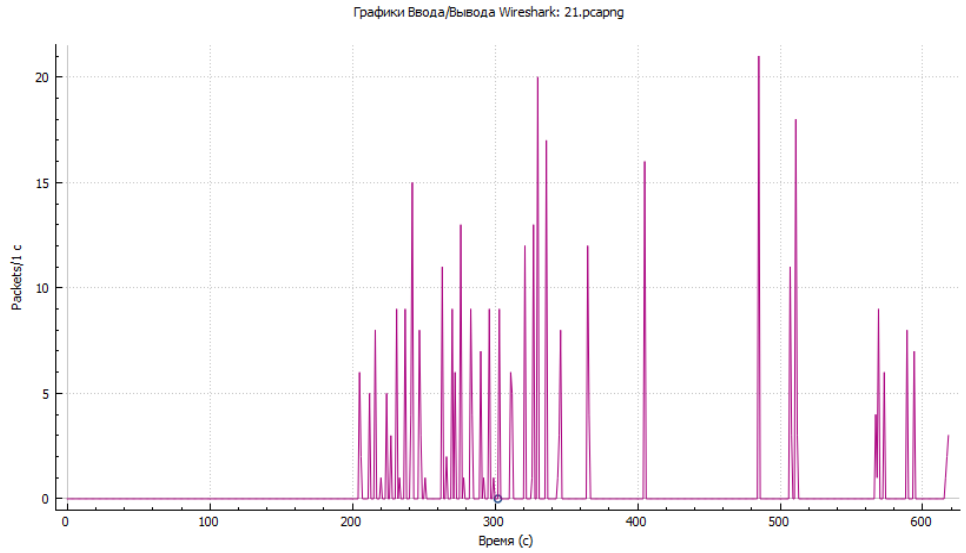


Рис. 6. Частота следования management фреймов.

Исходя из выше приведенных графиков, можно сделать вывод, что радиометрика в данном тип фреймов подходит для определения дальности устройства с высокой частотой и точностью только в моментах подключения устройств к ТД [5].

На рис. 7 представлена частота появления control фреймов.

Можно заметить, что частота следования фреймов данного типа относительно стабильна в моменты подключения к ТД и в моменты передачи данных. Когда пользователь подключен, но не передает данные, следование фреймов данного типа практически прекращается. Из этого можно сделать вывод что данный тип не подходит для постоянного использования в качестве основного источника. Он может быть использован в моменты подключения и активной передачи данных.

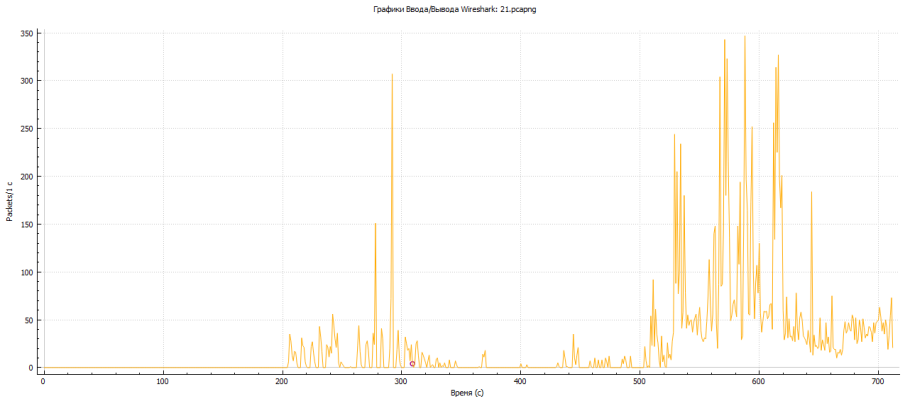


Рис. 7. Частота следования control фреймов.

На рис. 8 представлена частота появления data фреймов.

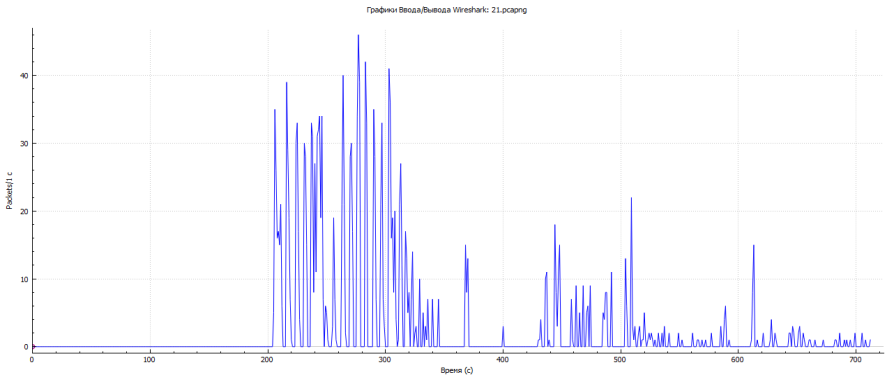


Рис. 8. Частота следования data фреймов.

На графике видно, что часто фреймы передаются в момент подключения в точке доступа, когда все сервисы активно обновляют свои данные. Также, в момент передачи тяжелого трафика частота фреймов относительно постоянна и стабильна. Данный тип фреймов передается с использованием технологии MIMO, что для позиционирования может вносить значительные ошибки в точность и объективность позиционирования.

Заключение. На основе выполненного исследования видно, что для станции с модулем Wi-Fi находящимся в неактивном состоянии не получается определить дальность. Из графика на рис. 6, следует что устройства с отключенным активным сканированием сети не видны окружающим устройствам. На этапе подключения станции к сети можно успешно выполнять определение дальности станций по Management, Control и Data фреймам, причем Control и Data фреймов количественно больше, чем Management, но для Data фреймов следует исключить фреймы, использующие технологию MIMO, т.к. она влияет на уровень мощности получаемого сигнала, что в свою очередь требует дальнейшего исследования. Для подключенных станций, но не выполняющих активную передачу данных особый интерес представляют Control и Data фреймы. Во время активной передачи данных следует подавляющее количество Control фреймов.

Требуется дальнейшее исследование, т.к. необходимо расширить набор станций, участвующих в тестировании. Кроме того, в данном исследовании выборка фреймов производилась достаточно грубо, что не может в полной мере раскрыть набор подходящих для дальнометрии фреймов. В частности, некоторые Control фреймы не имеют MAC-адреса источника, что не позволяет без дополнительной аналитики определить станцию, на которой был

сгенерирован данный фрейм. Помимо этого, при передаче фреймов индивидуальной (одноадресной) рассылки используется технология MIMO, которая в зависимости от текущего режима работы может влиять на мощность принимаемого сигнала, что в свою очередь может серьезно исказить точность определения дальности.

СПИСОК ЛИТЕРАТУРЫ

1. Построение доверенной вычислительной среды // Красов А.В., Гельфанд А.М., Коржик В.И., Котенко И.В., Петрив Р.Б., Сахаров Д.В., Ушаков И.А., Шариков П.И., Юркин Д.В. Санкт-Петербург, 2019.
2. Маркин Ю. В., Санаров А. С. Обзор современных инструментов анализа сетевого трафика. [Электронный ресурс]. - URL: http://www.ispras.ru/preprints/docs/prep_27_2014.pdf, (Дата обращения 25.06.2021).
3. Wireshark. [Электронный ресурс]. - URL: http://www.wireshark.org/, (Дата обращения 25.06.2021).
4. Исследование методов дальнометрии в беспроводных сетях // Петров В.А., Ковцур М.М., Киструга А.Ю. // REDS: Телекоммуникационные устройства и системы – 2021 – Т. 11 – № 4 – С. 42-49.
5. Ковалев, Д. Механизмы аутентификации и управления ключами стандарта IEEE 802.11-2012 / Ковалев Д., Ковцур М. // Первая миля. 2014. № 3 (42). С. 72-77.

УДК 004.451.87

РАЗРАБОТКА МЕХАНИЗМА ЗАЩИТЫ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ОТ LKM ROOTKIT

Фёдорова Ольга Вячеславовна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mail: olagfedorova666@gmail.com

Аннотация. В ходе выполнения выпускной квалификационной работы были разработаны методы обнаружения LKM RootKit в системе Linux, благодаря чему можно вовремя заметить нахождение вредоносного ПО.

Ключевые слова: ядро Linux; Модуль ядра системы Linux; RootKit; права суперпользователя; системные вызовы; аппаратные прерывания; механизм защиты; виртуальный лабораторный стенд.

DEVELOPMENT OF A MECHANISM FOR PROTECTING A SPECIAL-PURPOSE SYSTEM FROM LKM ROOTKIT

Fedorova Olga
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mail: olagfedorova666@gmail.com

Abstract. During the completion of the final qualification work, methods for detecting LKM RootKit in the Linux system were developed, thanks to which it is possible to notice the presence of malware in time.

Keywords: Linux kernel; Linux kernel module; RootKit; superuser rights; system calls; hardware interrupts; protection mechanism; virtual laboratory stand.

Введение. Руткиты – тип программного обеспечения, который специализируется на сокрытии сущностей в компьютерных системах, обеспечивая непрерывный контроль или доступ к ним, его – особенно трудно обнаружить по сравнению с другими видами программного обеспечения. Существуют различные инструменты для детектирования руткитов, использующие широкий спектр методов и механизмов обнаружения. Однако эффективность таких инструментов не вполне доказана, особенно в современных академических исследованиях и в контексте операционной системы Linux.

Описание метода обнаружения 1. Первый метод, предлагаемый для обнаружения руткита в системе описан на рис. 1. Он реализует и описывает все возможные способы обнаружения руткита без работы в нулевом кольце защиты. Такой способ реализуем без установки дополнительных средств разработки. Основная идея заключается в сравнение списка загруженных модулей и модулей, разрешенных в ядре. Не все руткиты тщательно скрывают свое присутствие в системе и найдя различия между этими списками можно определить злонамеренно загруженный модуль. Команды необходимые исследования системы это: modprobe –c – список всех модулей и cat /proc/modules – список всех загруженных модулей. Если данный способ н дал результатов, а часто модули удаляют эту информацию маскируя свое присутствие. Есть еще одна возможность определить присутствие руткита из области пользователя.

Руткит может перехватывать системные вызовы и даже функции самого ядра, которые за этими вызовами стоят: например, Reptile перехватывают функции файловой подсистемы ядра VFS. Руткиты проверяют, было ли среди прочитанного что-то, что необходимо скрыть от глаз пользователя или администратора, и при необходимости модифицируют буфер со считанными данными.

И когда ничего не подозревающий (или подозревающий) пользователь попытается просмотреть содержимое модифицированного руткитом файла, увидит он только список вполне легитимных модулей или команд. Именно это

становится проблемой при попытке обнаружить руткит, работая за зараженной машиной. Поэтому важно понимать, что при заражении руткитами уровня ядра не стоит верить никакой информации, получаемой от ядра.

Предположим, в нашей системе установлен Reptile. Открываем в любом текстовом редакторе /etc/modules и видим, что он будто бы чист, но мы-то знаем — там есть скрытое содержимое. Если пересохранить файл не внося изменений, то скрытая информация будет удалена и после перезагрузки ОС вредоносный LKM будет неактивен. Автор руткита сам предлагал такой способ предотвращения его загрузки. Описанный эффект наблюдается потому, что сохраняется ровно то, что открыто в редакторе, то есть часть файла, свободная от данных руткита.

Если неизвестно, в какой именно файл автозагрузки прописался руткит, то придется перебирать все задействованные файлы. Но описанный ниже модуль позволяет не только пересохранить подозрительный файл, но и выводит информацию о том, что именно за файл был подвержен изменениям. Нужно найти модифицированный файл автозагрузки, поместить вместо него свободную от данных руткита копию, но при этом как-то оставить эти данные, чтобы было проще найти вредоносный LKM.

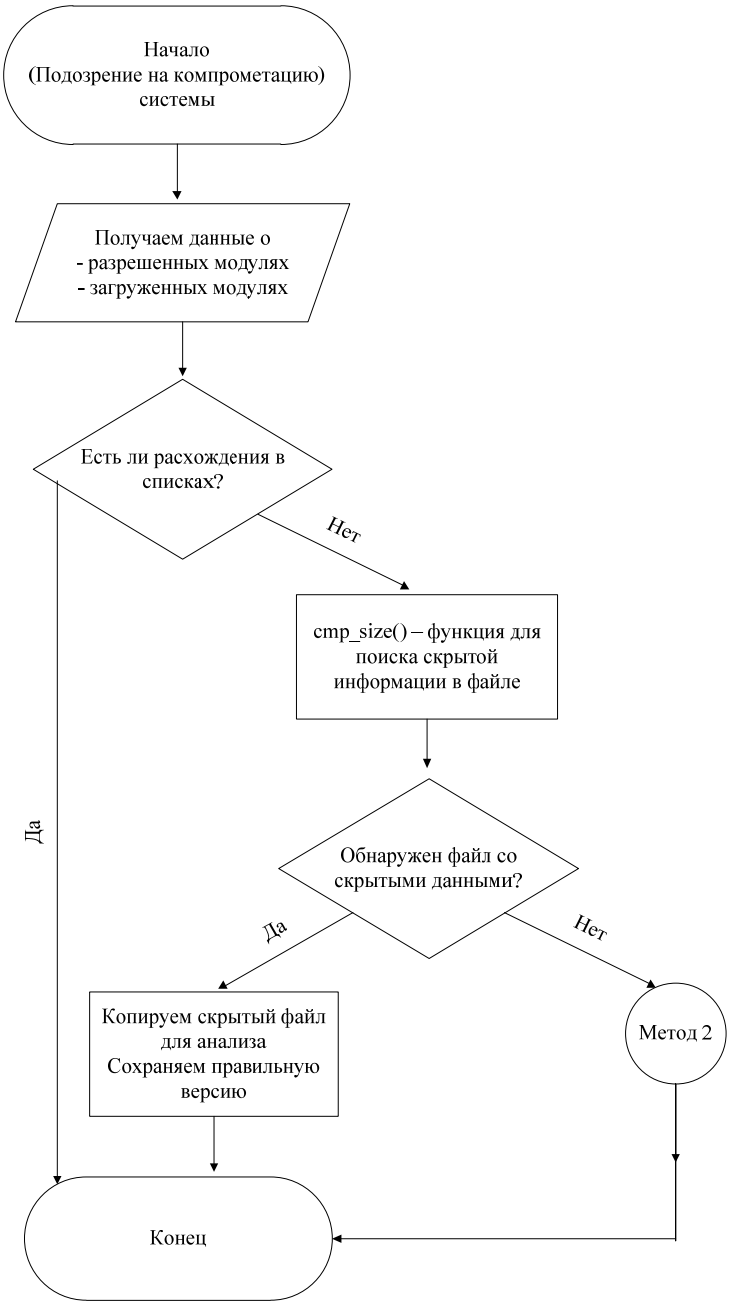


Рис. 1. Алгоритм обнаружения руткита по методу 1.

Таким образом, детектирования LKM-руткита сводится к двум вопросам:

– как найти файл со спрятанным содержимым, если неизвестно, каким образом руткит закрепился в системе;

– как сохранить этот файл так, чтобы это содержимое не оказалось удалено, а сохранилось для дальнейшего анализа.

Основной принцип: лишнее содержимое — значит, лишние данные на диске. Это позволит автоматизировать поиск и восстановление модифицированного файла автозагрузки. Необходим лишь список этих файлов, чтобы программа знала, где именно искать подвох. Далее для каждого такого файла программа сравнивает количество байтов, прочитанных с помощью fread() (за которой стоит системный вызов read(), а за ним, в свою очередь, перехваченная функция ядра vfs_read()), с размером файла, полученным из структуры, описывающей файл в файловой системе (i-node). Так как данная структура недоступна из пространства юзера, необходимо воспользоваться системным вызовом fstat() [2].

Основная часть этой проверки заключена в функции cmp_size (), она описана в приложение А. При подозрении на руткит выводится соответствующее сообщение с информацией о том, на какое количество байтов отличается фактическое содержимое от прочитанного. get_fsize () получает размер проверяемого файла из его дескриптора.

Описание метода обнаружения 2. Некоторые руткиты скрывают себя более тщательно и для их обнаружения недостаточно простого анализа файлов. Более сложным и более эффективным методом является динамическое отслеживание регистра CR0, контролирующего возможность записи в память ядра. При попытке изменения нужного бита регистра мы определим наличие руткита в системе и сменим регистр обратно. Рассматриваемый дальше модуль может быть выполнен только тогда, когда текущий уровень привилегий равен 0.

Параллельно с отслеживанием регистра CR0, предполагается выполнять контроль адресов функций таблицы системных вызовов. Решение о необходимости отслеживать данные адреса сделано на основе анализа двух руткитов, описанных выше. Функции подменяются для возможности скрыть файлы руткита. При загрузке системы мы делаем слепок таблице и регулярно сравниваем текущие адреса с зафиксированными.

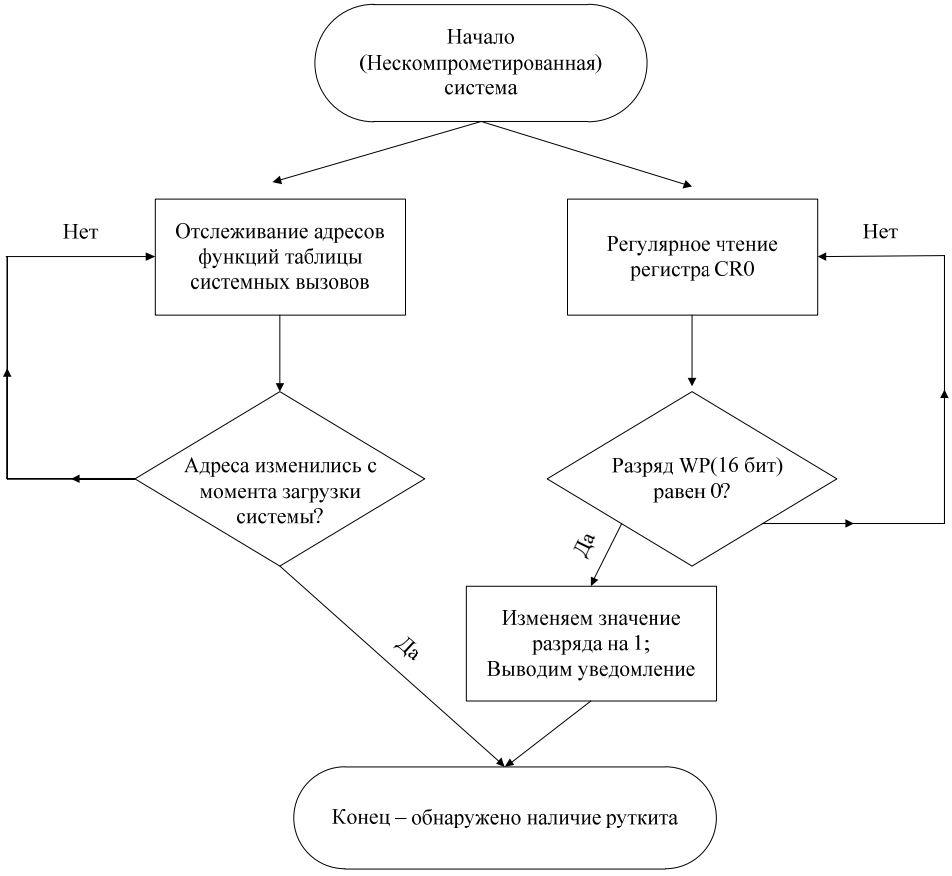


Рис. 2. Алгоритм обнаружения руткита по методу 2.

Итоговая схема анализа системы для обнаружения более сложных руткитов описаны на рис. 2. Два процесса, контролирующих систему выполняются параллельно.

Пример обнаружения руткитов. При практической реализации были запущены 2 программы. Первая программа обнаруживает несоответствие размера файла ее содержимому. Перед запуском сканирования в системе был загружен руткит Reptile. В результате удалось обнаружить уязвимый файл.

```
olga@debian:~/nitara-l3$ sudo ./nitara-l3
***WARN*** Something performs file tampering of /etc/modules : read 256 bytes instead of 286.
  So, d'ya want me to try to read the hidden stuff? [Y/n] y
Mmaped() successfully. File:
# /etc/modules: kernel modules to load at boot time.
#
# This file contains the names of kernel modules that should be loaded
# at boot time, one per line. Lines beginning with "#" are ignored.
# Parameters can be specified after the module name.

lp
rtc
#<reptile>
reptile
#</reptile>

Done.
  Maybe then clear the file from the hidden things? [Y/n] y
Reading file... fread() returned 256
Writing to /etc/modules... fwrite() returned 256
The vulnerable /etc/modules now renamed as /etc/modules.old. The safe copy is placed instead
/etc/rc.local looks fine to the userland
***ERR*** Couldn't open /etc/inittab: No such file or directory
***ERR*** Couldn't open /etc/rc.d/rc.sysinit: No such file or directory
/etc/init.d/rc looks fine to the userland
************************
1 vulnerable startup files found
************************
olga@debian:~/nitara-l3$ ls -l /etc/modules*
-rw-r--r-- 1 root root 256 Oct  1 03:19 /etc/modules
-rw-r--r-- 1 root root 286 Oct  1 02:21 /etc/modules.old
olga@debian:~/nitara-l3$
```

Рис. 3. Пример обнаружения руткита.

Пример работы программы отображен на рис. 3. По мимо обнаружения файла программа так же сохраняет файл, чтобы удалить строки, вставленные руткитом. Выводя информацию об этом действие на экран.

Для 2 метода была реализована программа, дающая возможность просматривать регистр CR0. Результат работы выводится в сообщения отладки. Значения, полученные с интервалом запуска в 1 минуту, можно наблюдать на рис. 4.

```
[ 4253.837331] hello: module license 'unspecified' taints kernel.
[ 4253.837335] Disabling lock debugging due to kernel taint
[ 4253.837472] cr0 = 0x80050033
[ 4253.837474] cr2 = 0x4F9DA6F8
[ 4253.837475] cr3 = 0x1783E000
[ 5270.963271] cr0 = 0x8005003B
[ 5270.963275] cr2 = 0x30C60418
[ 5270.963277] cr3 = 0x12F68000
```

Рис. 4. Модуль, демонстрирующий возможность отслеживания регистров.

Заключение. Были разработаны 2 метода определения наличия руткита в системе. Представлены блок-схемы, наглядно демонстрирующие логику анализа. На основе схем можно реализовывать программный код, автоматизирующий процесс обнаружение. В результате стало понятно, что руткиты очень разнообразны и для надежной защиты системы необходимо использовать комбинацию различных методов.

СПИСОК ЛИТЕРАТУРЫ

1. Долгих Д. Учимся писать модуль ядра (Netfilter) или Прозрачный прокси для HTTPS: [Электронный ресурс] URL: https://habr.com/ru/post/138328/
2. Кирилова К.С., Цветков А.Ю. Анализ существующих методов реализации rootkit [Текст] В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). сборник научных статей VIII Международной научно-технической и научно-методической конференция: в 4 т.. 2019. С. 492-497.
3. Кирилова К.С., Цветков А.Ю., Волкогонов В.Н. Проблема обезвреживания руткитов уровня ядра в системах специального назначения [Текст] I-methods. 2020. Т. 12. № 3. С. 1-9.
4. Матвейчиков И.В. Простая маскировка модуля ядра Linux с применением DKOM [Электронный ресурс] URL: https://habr.com/ru/post/205274/
5. Фёдорова О.В., Цветков А.Ю. // Инновации. Наука. Образование. 2021. №31. С. 118-124.
6. Цилюрик О. Практикум: модули ядра Linux. Конспект с примерами и упражнения с задачами: [Электронный ресурс], URL: https://losst.ru/wp-content/uploads/2016/08/BOOK_PRACTIS_245.pdf
7. Щербакова Т. Фишинговые письма — самый распространенный способ взлома почты: [Электронный ресурс] URL: https://www.kaspersky.ru/blog/email-account-stealing/23433/
8. Alavoor Vasudevan The Linux Kernel HOWTO: [Электронный ресурс] URL: http://www.faqs.org/docs/Linux-HOWTO/Kernel-HOWTO.html

9. Andreas Bunten UNIX and Linux based Rootkits. Techniques and Countermeasures: [Электронный ресурс] // DFN-CERT Services GmbH, 2004. URL:http://repository.root-me.org/Virologie/EN%20-20UNIX%20and%20Linux%20based%20Rootkits%20Techniques%20and%20Countermeasures%20-%20Andreas%20Bunten.pdf
10. Кирилова, К.С. Анализ существующих методов реализации rootkit / К.С. Кирилова, А.Ю. Цветков // Актуальные проблемы инфотелекоммуникаций в науке и образование. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2019. С. 492-497.
11. Таргонская, А.И. Разработка защищенного веб-интерфейса для управления устройствами в сети / А.И. Таргонская, А.Ю. Цветков // Актуальные проблемы инфотелекоммуникаций в науке и образование. VIII Международная научно-техническая и научно- методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2019. С. 734-739.
12. Темченко, В.И. Проектирование модели информационной безопасности в операционной системе / В.И. Темченко, А.Ю. Цветков // Актуальные проблемы инфотелекоммуникаций в науке и образование. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2019. С. 740-745.
13. Цветков, А.Ю. Исследование существующих механизмов защиты операционных систем семейства Linux / А.Ю. Цветков // Актуальные проблемы инфотелекоммуникаций в науке и образование. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 657-662.
14. Цветков А.Ю. Обеспечение безопасности в клиент-серверном Java приложении для учета и автоматической проверки лабораторных работ / А.Ю. Цветков, М.Е. Шалаева, М.А. Юрченко // Актуальные проблемы инфотелекоммуникаций в науке и образование. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2019. С. 756-761.
15. Багомедова А.Р., Ушаков И.А., Цветков А.Ю. Разработка методов проверки соответствия серверов виртуализации требованиям безопасности согласно стандарту ГОСТ Р 56938-2016 // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): сборник статей VII Международной научно-технической и научно-методической конференции. 2018. С. 58-63.

УДК 004.7: 621.39

ПРОТОКОЛ МАРШРУТИЗАЦИИ ДЛЯ ГЕТЕРОГЕННЫХ БЕСПРОВОДНЫХ ЯЧЕИСТЫХ СЕТЕЙ

Хазиев Нугаян Нурутдинович, Григорьев Артем Александрович, Зятинин Александр Александрович, Коростень Александра Олеговна
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: grigorev.artem-x@yandex.ru

Аннотация. Внедрение гетерогенных беспроводных сетчатых технологий дает возможность повысить пропускную способность сети, расширить охват и повысить качество обслуживания (QoS). Каждое беспроводное устройство использует различные стандарты, форматы данных, протоколы и технологии доступа. Однако разнообразие и сложность таких технологий создают проблемы для традиционных систем контроля и управления. В данной статье предлагается гетерогенная архитектура столичной сети, которая сочетает в себе беспроводную ячеистую сеть IEEE 802.11 (WMN) с сетью LTE. Кроме того, предлагается новый гетерогенный протокол маршрутизации и алгоритм маршрутизации, основанный на усилительном обучении, называемый когнитивной гетерогенной маршрутизацией, для выбора соответствующей технологии передачи данных на основе параметров каждой сети. Предлагаемая гетерогенная сеть преодолевает проблемы отправки пакетов по длинным путям, островным узлам и помехам в WMNs и увеличивает общую пропускную способность комбинированной сети за счет использования нелицензионных частотных полос вместо покупки большего количества лицензионных частотных полос для LTE. Результаты моделирования показывают, что предлагаемая сеть достигает увеличения пропускной способности до 200% по сравнению с сетями только Wi-Fi или сетями только LTE.

Ключевые слова: интернет-трафик; гетерогенная сеть; гетерогенные узлы; пропускная способность; метрика; интероперабельность.

PROTOCOL ROUTING ALGORITHM IN PACKET MOBILE DATA NETWORKS

Haziev Nugayan, Grigorev Artem, Zatinin Aleksandr, Korosten Aleksandra
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: grigorev.artem-x@yandex.ru

Abstract. The introduction of heterogeneous wireless mesh technologies provides the opportunity to increase network capacity, expand coverage and improve quality of service (QoS). Each wireless device uses different standards, data formats, protocols, and access technologies. However, the variety and complexity of such technologies creates problems for traditional monitoring and control systems. This article proposes a heterogeneous metropolitan network architecture that combines an IEEE 802.11 wireless mesh network (WMN) with an LTE network. In addition, a new heterogeneous routing protocol and a learning-based routing algorithm called cognitive heterogeneous routing are proposed to select the appropriate transmission technology based on the parameters of each network. The proposed heterogeneous network overcomes the problems of sending packets over long paths, island nodes and interference in WMNs and increases the overall capacity of the combined network by using unlicensed frequency bands instead of buying more licensed frequency bands for LTE. Simulation results show that the proposed network achieves a throughput increase of up to 200% compared to Wi-Fi-only or LTE-only networks.

Keywords: internet traffic; heterogeneous network; heterogeneous nodes; bandwidth; metric; interoperability.

Введение. Интернет-трафик, как ожидается, увеличится в три-пять раз в течение следующих трех лет из-за роста числа подключенных мобильных устройств. Количество подключенных устройств и машинно-машинной связи, как ожидается, увеличится в 2 раза. Прогнозируется, что в течение следующего десятилетия для поддержки этого роста интернет-трафика потребуется более развитая интернет-инфраструктура. Беспроводные сети [1] следующего поколения должны решать несколько задач, включая затраты на покрытие районов с высокой плотностью населения, многолюдных мероприятий, больших площадей или на временные изменения где будут востребованы, например, крупные спортивные мероприятия. Оценка стоимости зависит от количества необходимых базовых станций и стоимости аренды полос частот. Интероперабельность - это еще одна проблема, поскольку многие устройства используют различные операционные системы, протоколы и технологии доступа. Надежность сети также является важным вопросом, который необходимо решить, чтобы гарантировать, что системы способны функционировать без сбоев в сложных и изменяющихся условиях. Интернет-взаимодействие различных беспроводных технологий, в частности LTE и беспроводных локальных вычислительных сетей, является одной из ключевых возможностей для развития беспроводных сетей следующего поколения. LTE - это эволюция стандарта третьего поколения, который обеспечивает широкий охват и пиковую скорость передачи данных.

Однако в сетях LTE используются лицензированные полосы частот [2], и поэтому для обеспечения большей пропускной способности вводятся дополнительные затраты либо на покупку большего количества полос частот (которые могут быть доступны не во всех регионах), либо на инвестиции в более высокую плотность базовых станций. Еще одной перспективной беспроводной архитектурой для следующего поколения беспроводных сетей являются беспроводные ячеистые сети (WMNs). WMN - это парадигма, разработанная для обеспечения широкого покрытия сети без использования централизованной инфраструктуры. Таким образом, WMNs - это реальный выбор для обеспечения магистральной сети для крупномасштабных сетей. В таких сетях для обеспечения интернет-соединения с ячеистой сетью используются шлюзы (беспроводные узлы с высокоскоростным проводным подключением к внешнему интернету). Эта архитектура обеспечивает экономичное повсеместное беспроводное подключение к интернету [3] на больших площадях через многопоточную передачу к шлюзу и наоборот. Обширное моделирование при различных сценариях и требованиях к сетям позволяет получить прирост пропускной способности до 200% в предлагаемой гетерогенной сети по сравнению с сетями только LTE и Wi – Fi.

Существуют два типа протоколов маршрутизации в WMNs. Первый тип состоит из реактивных протоколов маршрутизации, в которых маршрут создается по требованию путем заполнения сети маршрутными запросами. Выбор маршрута поддерживается только для узлов, передающих трафик в определенный пункт назначения. Примерами такого типа маршрутизации являются ad hoc on-demand distance vectors и dynamic source routing. Реактивная маршрутизация вызывает некоторую задержку из-за того, что маршрут создается только тогда, когда есть данные, готовые к отправке. Второй тип протокола маршрутизации состоит из проактивных или табличных протоколов маршрутизации. Они поддерживают таблицу всего назначения в сети, периодически распространяя обновление таблицы маршрутизации на все узлы. Примерами такого типа протокола маршрутизации являются целевой секвенированный вектор расстояния и оптимизированная маршрутизация состояния канала связи.

Наиболее широко используемые метрики в протоколах маршрутизации WMN выбирают кратчайший путь к шлюзу на основе количества переходов, то есть количества узлов между источником и пунктом назначения.

Также особенностью этой статьи является создание алгоритма маршрутизации, который называется CHR, который определяет требования к выбору передающего устройства на узлах, имеющих как LTE, так и Wi-Fi устройства. Обучение с подкреплением используется для того, чтобы извлечь уроки из предыдущих действий и оптимизировать производительность сети.

Гетерогенная сеть (HetMeshNet) [3] рассматривает сосуществование нескольких беспроводных технологий, а также проводной сети. Он использует следующие типы узлов: гетерогенные узлы (HetNode)—узлы с поддержкой Wi-Fi и LTE; узлы mesh шлюзов—узлы с Wi-Fi и проводным соединением; базовые станции LTE—также известные как развитый NodeB (eNodeB или eNB); узлы Internet gateway—узлы, которые соединяют все сети с интернетом с помощью высокоскоростной проводной сети; и клиентские узлы-используемые конечными пользователями или датчиками. HetMeshNet. Он включает в себя несколько типов сетевых компонентов. Во-первых, сеть LTE состоит из множества ячеек, распределенных в регионе. Базовая станция LTE расположена в каждой ячейке. Во-вторых, в сети развернуто несколько Гетнодов, каждый из которых может быть использован в различных технологиях. Гетерогенные узлы (HetNodes) оснащены сетевыми интерфейсными картами Wi-Fi и LTE. Узлы mesh gateway - это узлы третьего типа, которые соединяют WMN с интернет-шлюзом. Интернет-шлюз действует как сервер; он обеспечивает подключение к интернету как LTE, так и WMN сети. Наконец, клиентскими узлами могут быть люди, использующие мобильный телефон, ноутбук или любое другое устройство, подключенное к интернету (например, датчик, отправляющий данные в интернет).

Рассмотрим протокол маршрутизации гетерогенного WMN. Предлагаемый новый протокол маршрутизации использует метрики двух сетей для динамического переключения между технологиями передачи. Предлагаемый протокол состоит из двух основных компонентов: гетерогенных таблиц маршрутизации и алгоритма маршрутизации.

В гетерогенных таблицах маршрутизации каждый тип узла использует различные технологии передачи, и каждая технология передачи использует другой сетевой адрес. Для маршрутизации пакетов между этими различными сетями каждый тип узлов поддерживает таблицу маршрутизации для пересылки пакетов данных из разных сетей так же, как если

бы они поступали из одной и той же сети. Во-первых, узел интернет-шлюза нуждается в таблице маршрутизации для пересылки пакетов данных в интернет и из интернета для сетей WMN и LTE. Во-вторых, каждый гетерогенный узел поддерживает таблицу маршрутов к другим гетерогенным узлам сети, а также список доступных сетчатых шлюзов и сетчатый шлюз по умолчанию для пересылки гетерогенных узловых данных. Для создания этой таблицы используется протокол маршрутизации OLSR, используемый для определения таблицы маршрутов для ячеистой сети Wi-Fi и использует счетчик ретрансляций в качестве метрики. Затем добавляется расширение инструментов для поддержки использования сетки шлюза в WMN. Расширенный OLSR использует две метрики для выбора mesh-шлюза: количество переходов к mesh-шлюзу и количество подключенных к нему узлов. Для достижения этой цели управляющее сообщение передается соседним узлам от каждого шлюза для объявления его нагрузки с точки зрения количества узлов, связанных с ним. Каждый узел выбирает шлюз [4] с кратчайшим путем, и если более чем один шлюз имеет одинаковое количество переходов, то узел выбирает шлюз с меньшей нагрузкой. Использование кратчайшего пути для выбора маршрута к шлюзу с помощью OLSR позволит избежать возникновения проблемы колебания маршрута, поскольку узел использует только кратчайший путь к шлюзу без переключения к неоптимальным маршрутам.

Гетерогенная WMN оценивается с помощью симулятора NS-3, который является широко используемым инструментом для оценки и валидации беспроводных сетей. Для оценки и валидации предлагаемой сети используются два типа сценариев. Первый сценарий состоит из топологий сетки, в которых гетноды распределены в сетке. Второй сценарий состоит из случайных топологий, в которых все узлы случайным образом распределены в области 1000 м×1000 м. В обоих сценариях есть пять шлюзов, распределенных в сети, и LTE eNB выделяется в центре. Для анализа производительности предлагаемой сети применяются различные нагрузки на сеть, использующую 19 и 30 узлов, передающих одновременно информацию как в одноуровневой сети, так и осуществляет передачу информации на базовые станции.

HetMeshNet сравнивается с сетями LTE, использующие различное количество блоков радиоресурсов (RBs), а также сетями Wi-Fi. Для оценки предлагаемой системы используются два типа сценариев: один для тестирования линии связи с шлюзами и один для тестирования одноранговой сети. В сценариях связи с шлюзами линии связи узлы (за исключением узлов mesh gateway) генерируют трафик протокола пользовательских дейтаграмм (UDP) с одинаковой скоростью, и единственным назначением является интернет. Это имитирует «восходящий» трафик от клиентских терминалов к интернету. В моделировании используются сеточная и случайная топологии, и к сети прикладываются две различные нагрузки, используя 19 и 30 узлов, одновременно передающих данные в интернет. Второй сценарий используется для того, чтобы показать, как алгоритм адаптируется к изменению величины нагрузки во время моделирования. Результаты моделирования для сценариев «восходящей» линии связи указывают на значительное улучшение пропускной способности системы для предлагаемой гетерогенной системы по сравнению с базовыми сетями.

В данной статье представлен новый подход к построению гетерогенной сетевой архитектуры, в которой беспроводные устройства [4] LTE и Wi-Fi используются для получения преимуществ в пропускной способности каждой технологии передачи. Кроме того, был разработан новый протокол маршрутизации для гетерогенных WMNs, который динамически выбирает технологию передачи для увеличения общей пропускной способности сети и повышения средней пропускной способности. Кроме того, для нужд протокола маршрутизации был предложен новый алгоритм маршрутизации, который оценивает стоимость передачи трафика через каждую сеть. Предлагаемый алгоритм рассматривает нагрузку трафика на сеть LTE в качестве метрики для оценки стоимости передачи по LTE и использует скорость передачи в качестве метрики для ячеистой сети Wi-Fi. Результаты моделирования показывают, что предлагаемая сеть обеспечивает до 200% большую пропускную способность по сравнению с сетями только Wi-Fi и сетями только LTE. Гетерогенная сетевая архитектура управляет различными беспроводными устройствами как частью единой виртуальной сети. Сеть LTE используется для того, чтобы избежать перегруженных узлов Wi-Fi и пути высокой интерференции в WMN, в то время как WMN разгружает нагрузку сети LTE, снижает стоимость использования большего количества лицензированных частотных диапазонов и вперед, когда пропускная способность LTE ухудшается. Эта работа обеспечивает основу для будущих исследований развития гетерогенных ячеистых сетей Wi-Fi/LTE и использования других беспроводных технологий в составе гетерогенных сетей.

Заключение. Предлагаемый протокол маршрутизации потенциально может быть расширен для поддержки других беспроводных технологий за счет использования их параметров в алгоритме обучения. Предлагаемая архитектура обеспечивает простой способ расширения покрытия и пропускной способности мобильной сети и может внести свой вклад в инфраструктуру пятого поколения. Кроме того, гетерогенные сети могут использоваться для подключения сетей интернета вещей и использоваться для обеспечения инфраструктуры умных домов и умных городов.

СПИСОК ЛИТЕРАТУРЫ

1. Чуднов А. М., Кирик Д. И., Курашев З. В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений. // Радиотехнические и телекоммуникационные системы. 2017, №2, с.41-49.
2. Чуднов А. М., Курашев З. В. Принципы формирования маршрутных таблиц на основе оптимизации распределения потоков в сети передачи данных. // Наукоемкие технологии в космических исследованиях Земли. 2017. Т.9, № 6, с. 46–51.
3. Маркин В. Г., Рыжкова А. Г. Протоколы маршрутизации в мобильных самоорганизующихся сетях. // Теория и техника радиосвязи, 2013, №4, с.48-56. Siachalou S. Efficient QoS routing.// The International Journal of Computer and Telecommunications Networking. 2003. vol. 43. iss. 3. p. 351-367.
4. Toh C. K. Wireless Atm and Ad-Hoc Networks: Protocols and Architectures.// Kluwer Academic Publisherb Group. 1997. – 313 p.

УДК 004.7: 621.39

ПРОТОКОЛ МАРШРУТИЗАЦИИ С УЧЕТОМ СЕТЕВОГО КОДИРОВАНИЯ В БЕСПРОВОДНЫХ ЯЧЕИСТЫХ СЕТЯХ

Хазиев Нугаян Нурутдинович, Зятинин Александр Александрович, Азоркин Владимир Викторович, Аксенов Сергей Сергеевич

Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: zyatinin@rambler.ru

Аннотация. Механизмы кодирования такие как COPE, могут эффективно повысить пропускную способность в беспроводных ячеистых сетях (WMN). В то время как гибридный mesh-сетевой протокол (HWMP) подходит для WMN, его расширение с помощью COPE не дает каких-либо дополнительных преимуществ, в частности, HWMP не может устанавливать пути с большим количеством возможностей кодирования. В результате чего преимущества сетевого кодирования не могут быть использованы в достаточной степени. В этой статье предлагаются улучшения HWMP с помощью нового сетевого протокола маршрутизации (CAHWMP) для WMN. В протоколе CAHWMP полагался критерий кодирования, основанный на распределении информационных потоков данных, позволяющего разработать динамический алгоритм кодирования во время построения множества маршрутов. CAHWMP впоследствии устанавливает пути, используя метрику маршрутизации с учетом возможных методов кодирования, который может сбалансировать потребление ресурсов канала и выигрыш за счет совместного использования ресурсов, вводимых сетевым кодированием. Результаты моделирования показывают, что CAHWMP может устанавливать маршруты с большим количеством кодов возможности, в результате повышается производительность сети и ее пропускная способность.

Ключевые слова: протокол маршрутизации; сетевое кодирование; беспроводные ячеистые сети; сетевой протокол; информационный поток; сбалансирование потребление ресурсов; пропускная способность сети.

NETWORK CODING ROUTING PROTOCOL IN WIRELESS MESH NETWORKS

Haziev Nugayan, Zatinin Aleksandr, Azorkin Vladimir, Aksenov Sergey

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: zyatinin@rambler.ru

Abstract. Encoding mechanisms such as COPE can effectively improve throughput in wireless mesh networks (WMNs). While Hybrid Mesh Network Protocol (HWMP) is suitable for WMN, its extension with COPE does not provide any additional benefits, in particular, HWMP cannot establish paths with many encoding possibilities. As a result, the advantages of network coding cannot be sufficiently exploited. This article suggests improvements to HWMP with the new Network Routing Protocol (CAHWMP) for WMN. In the CAHWMP protocol, we propose an encoding criterion based on the distribution of information data streams, which allows developing a dynamic encoding algorithm during the construction of multiple routes. CAHWMP subsequently establishes the paths using routing metrics considering possible encoding techniques that can balance the consumption of channel resources and the sharing gains introduced by network encoding. Simulation results show that CAHWMP can establish routes with more capability codes, resulting in improved network performance and network throughput.

Keywords: routing protocol; network encoding; wireless mesh networks; network protocol; information flow; balancing resource consumption; network bandwidth.

Введение. Беспроводная ячеистая сеть (WMN) - это многозвенная сеть с широким радиусом покрытия, большой пропускной способностью, высокой скоростью доступа и низкой стоимостью развертывания [1]. Это новая схема для решения проблем, связанных с критериями радиуса покрытия. Разработка протоколов маршрутизации является одной из ключевых проблем в WMN. Протокол управления гибридной беспроводной ячеистой сетью (HWMP) является протоколом маршрутизации по умолчанию для WMN в IEEE 802.11s стандарте. В отличие от традиционных протоколов проактивной и реактивной маршрутизации, HWMP представляет собой гибридный протокол маршрутизации WMN, который расширяет и сочетает в себе реактивную маршрутизацию с проактивной древовидной структурой. HWMP в полной мере использует преимущества двух типов протоколов маршрутизации, что приводит не только к сокращению срока задержки при построении маршрутов, но также приходится меньше накладных расходов на управление. Более того, HWMP использует пространственно-временную метрику, которая может лучше отражать качество связи, чем метрика количества переходов. Это делает HWMP более подходящим для WMN с различными топологиями и качествами каналов по сравнению с протоколами маршрутизации, такими как Ad hoc On-Demand Distance Vector (AODV) или Destination-Sequenced Distance Vector (DSDV). Исследования по сетевому кодированию в WMN все еще находятся на стадии исследования. COPE изучает реализацию сетевого кодирования в протоколах беспроводной сети. COPE - это механизм, который применяет сетевое кодирование в реальных беспроводных одноадресных сетях связи. COPE основан на принципе

оппортунизма. Он интегрирует сетевое кодирование в стек протоколов и позволяет беспрепятственно работать с протоколами высокого уровня. COPE значительно увеличивает пропускную способность беспроводных сетей. COPE предоставляет хорошую схему для применения сетевого кодирования с одноадресной передачей в WMN. Следовательно, COPE является активной областью исследований. Механизм COPE может быть улучшен путем кодирования узла с большим количеством входных потоков. Узлы с большим количеством выходных портов, чем входных, могут передавать пакеты данных без кодирования. Это может уменьшить накладные расходы на избыточное кодирование. Протокол распределенной маршрутизации с учетом кодирования (DCAR) использует метрику маршрутизации с учетом кодирования для достижения эффективного механизма маршрутизации, это помогает найти потенциальные возможности кодирования.

DCAR может привести к не оптимальным маршрутам, поскольку его метрика маршрутизации не точна. Представлено восприятие кодирования, и разработан уникальный процесс сопоставления для сравнения реальной беспроводной сети с виртуальной.

Протокол маршрутизации HLCR представлен для обнаружения возможности кодирования и эффективного балансирования сетевой нагрузки. Также выведена теоретическая формула вычисления пропускной способности с сетевым кодированием в любой топологии беспроводной сети и в любом режиме одновременной одноадресной передачи. Она обеспечивает оптимальный путь для пакетов данных до узла назначения на основе максимальной пропускной способности сети. Каждый узел в сети может балансировать трафик данных и избежать беспроводных помех с возможностью кодирования.

Рассмотрим протокол сетевого кодирования OASIS. Он не только наследует две особенности оппортунистического восприятия и оппортунистического кодирования от COPE, но также вводит оппортунистическое распространение информации. Узел кодирует как можно больше пакетов и увеличивает объем пакетов данных для соседних узлов, чтобы повысить вероятность кодирования в будущем. Результаты моделирования показывают, что OASIS может повысить пропускную способность сети примерно в 1,4 раза по сравнению с традиционной одноадресной передачей и примерно в 1,2 раза больше по сравнению с COPE. Протоколы маршрутизации с поддержкой кодирования имеют некоторые недостатки, а именно доставка в реальном времени по каналам происходит с потерями. Протокол маршрутизации с учетом кодирования в реальном (CARTR) разработан для решения этой проблемы. Он распределяет закодированные и некодированные пакеты данных по каналу по приоритету. Эксперименты показывают, что CARTR увеличивает пропускную способность примерно на 20%. Стратегия развертывания с учетом кодирования создает возможность для сетевого кодирования на агрегированных узлах ретрансляторах. Стратегия развертывания [2] может эффективно избежать многоканальных сбоев в сети. Обнаруженные данные конечных узлов передаются после кодирования промежуточными узлами, что снижает избыточность пакетов Существующие исследования протоколов и алгоритмов маршрутизации с учетом сетевого кодирования рассматривают увеличение возможностей кодирования или максимизацию пропускной способности сети, однако исследование обнаружения возможности кодирования и выбор пути, основанный на выигрыше от кодирования, ограничен.

Основная идея добавления осведомленности о сетевом кодировании в протоколы маршрутизации заключается в активном обнаружении возможностей кодирования в процессе обнаружения маршрутизации и использовании метрик маршрутизации с учетом сетевого кодирования для установления путей с большим количеством структур кодирования. Это позволяет создать больше возможностей для кодирования и улучшает использование COPE. Если потоки данных следуют по путям в соответствии с какой-либо одной структурой кодирования, тогда существует возможность для кодирования, и можно использовать механизм COPE.

Чтобы гарантировать, что каждый узел следующего перехода декодирует закодированный пакет данных и получает желаемый пакет, необходимо определять критерий кодирования с помощью COPE в узле. Критерий кодирования основан на пакетах данных; однако передача данных не начинается до установления пути. В результате этот критерий не подходит для оценки кодирования при обнаружении пути. Следовательно, чтобы гарантировать, что узел следующего перехода на пути каждого пакета данных сохранил все другие пакеты для кодирования, этот узел должен быть узлом предыдущего перехода или его соседом на путях этих пакетов данных. В протоколе CAHWMP необходимая информация для критерия кодирования о потоках данных при передаче и соответствующих парах переходов в узле может быть получена путем поиска в таблица маршрутизации, поддерживаемая узлом. CAHWMP - сетевой протокол маршрутизации с учетом кодирования для беспроводных ячеистых сетей, основанный на HWMP. В установление пути протокола CAHWMP включены три процесса: обнаружение пути, ответ пути и обслуживание пути. Таблица маршрутизации состоит из ряда записей маршрутизации к различным узлам назначения. В каждой записи маршрута для однозначной идентификации пути используются адрес назначения, порядковый номер пункта назначения и идентификатор PREQ ID пункта назначения.

В стандарте IEEE 802.11s определена метрика канала по умолчанию [3] Ca, основанная на пространстве-времени, которая используется для расчета ресурсов канала, потребляемых при передаче данных. По сравнению с метрикой количества переходов, обычно используемой в мобильной сети. В механизме сетевого кодирования, если несколько пакетов закодированы в определенном узле, то закодированный пакет достигает всех пунктов назначения за одну передачу. Связь между потреблением ресурсов канала при передаче одного закодированного пакета и каждым исходным пакетом данных, который должен быть закодирован в канале следующего перехода, может быть описана теоремой 1.

Теорема1. Если существует n исходных пакетов данных, которые могут быть закодированы в узле, предполагается, что объем потребления ресурсов в канале следующего перехода каждого пакета индивидуально равен Ca1, Ca2 …. Can. Ресурс канала, который потребляется закодированным пакетом, является максимальным по всем каналам, max {Ca1, Ca2 …. Can}. Другими словами, каждый кодируемый пакет может совместно использовать максимальное количество ресурсов линии связи для передачи.

В беспроводной ячеистой сети, узел называется Mesh Point (MP). Когда исходному MP необходимо отправить данные в целевой MP, он сначала проверяет свою таблицу маршрутизации, чтобы увидеть, есть ли доступный маршрут к месту назначения. Если маршрута нет, исходный MP должен начать процесс обнаружения пути к целевому MP. Сначала он передает пакет запроса пути PREQ. В PREQ протокола CAHWMP добавляются два поля: «Добавить» и MP-адрес предыдущего перехода. В поле «Добавить» хранится набор ADD, который представляет собой результат выполнения алгоритма обнаружения возможности кодирования. Перед широковещательной передачей все поля Hop Count, Metric и Add инициализируются равными 0, а MAC-адрес исходного MP записывается в поле Last Hop Address в алгоритме обнаружения возможности кодирования, если промежуточный MP принимает пакет PREQ.

В CAHWMP сказано, что после того, как MP-получатель получит несколько пакетов PREQ за короткое время задержки T, тогда он выберет пакет с минимальным NCCA в поле Metric для генерации пакета ответа пути. Если порядковый номер в PREQ равен порядковому номеру MP назначения плюс 1, то MP назначения должен добавить 1 к своему порядковому номеру перед генерацией пакета PREP. В противном случае он не меняет свой порядковый номер. После этого MP-адресат вставляет свой порядковый номер в соответствующее поле PREP и устанавливает оба поля Hop Count и Metric на 0. После этого пакет PREP одноадресно передается MP предыдущего перехода по обратному пути, пока не достигнет MP-источника.

Альтернативный путь – это необязательный способ обслуживания маршрута в протоколе HWMP, но протокол CAHWMP не включает этот механизм [4]. Поскольку пакет PREQ отправляется периодически для установления альтернативных путей от исходного MP к целевому MP с использованием того же процесса и сохраняется в таблице маршрутов, то это вызывает увеличение потребления полосы пропускания и ресурсов. Когда MP на активном пути не может передать пакет данных после конечного времени повторной передачи, то тогда это означает, что канал от этого MP к его следующему переходу отключен. Это приводит к отправке сообщения об ошибке пути PERR для поддержки пути. Целевой MP этого пути называется недоступным целевым MP. Пакет PERR записывает номер, MAC-адрес и порядковый номер недоступных целевых MP.

Программное обеспечение для моделирования сети. NS2, используется для моделирования производительности протокола CAHWMP. Он сравнивается с протоколами HWMP и COPE-HWMP. Здесь COPE-HWMP означает использование протокола HWMP вместе с COPE. При моделировании используется случайная топология сети. Для моделирования аналогового WMN выбираются 36 стационарных узлов, случайным образом распределенных на площади 1000x1000 м. Эффективное расстояние передачи между узлами составляет 300 м. Время моделирования установлено 200 с. Уровень MAC настроен на использование стандарта IEEE 802.11b, а емкость канала составляет 2 Мбит. Вероятность потери пакетов между любыми двумя узлами устанавливается случайным образом. Потоки данных с постоянной скоростью передачи (CBR) устанавливаются в сетевой передаче, размер пакета которых составляет 512 байт. Исходный MP генерирует 20 пакетов CBR в секунду. Путем моделирования исследуются производительность пропускной способности сети, средняя сквозная задержка и скорость доставки пакетов в ячеистой сети с различным количеством потоков данных. Количество потоков данных увеличивается с интервалом от 2 до 28. Результаты моделирования берутся в среднем из 30 экспериментов.

Заключение. Сравнивая два протокола CAHWMP и COPE-HWMP видно, что первый оказывается лучше. Это связано с тем, что протокол CAHWMP имеет больше возможностей кодирования и использует маршруты для более эффективной доставки пакетов, что может еще больше снизить перегрузку и количество потерянных пакетов. Сравнивая среднюю скорость доставки пакетов в трех случаях, значение CAHWMP на 8,7% выше, чем у HWMP, и на 4,3% выше, чем у COPE-HWMP. Из моделирования видно, что протокол CAHWMP имеет лучшую сетевую производительность, чем два других протокола.

В этой статье был рассмотрен протокол маршрутизации с учетом сетевого кодирования CAHWMP, основанный на HWMP, и представлена метрика маршрутизации с учетом кодирования NCCA, которая улучшает пространственно-временную метрику канала CaHWMP.

СПИСОК ЛИТЕРАТУРЫ

1. Чуднов А. М., Кирик Д. И., Курашев З. В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений.// Радиотехнические и телекоммуникационные системы. 2017, № 2, с.41-49.
2. Чуднов А. М., Курашев З. В. Принципы формирования маршрутных таблиц на основе оптимизации распределения потоков в сети передачи данных.// Наукоемкие технологии в космических исследованиях Земли. 2017. Т.9, № 6, с. 46–51.
3. Маркин В. Г., Рыжкова А. Г. Протоколы маршрутизации в мобильных самоорганизующихся сетях.// Теория и техника радиосвязи, 2013, № 4, с.48-56. Siachalou S. Efficient QoS routing.// The International Journal of Computer and Telecommunications Networking. 2003. vol. 43. iss. 3. p. 351-367.
4. Toh C. K. Wireless Atm and Ad-Hoc Networks: Protocols and Architectures.// Kluwer Academic Publisherb Group. 1997. – 313 p.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ WEB-САЙТОВ

Бариков Леонид Николаевич
Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП)
Большая Морская ул., 67, Санкт-Петербург, 190000, Россия
e-mail: lnbarikov@gmail.com

Аннотация. Рассматриваются вопросы обеспечения информационной безопасности функционирования web-сайтов, решаемые в процессе их разработки, на примере создания Internet-магазинов.

Ключевые слова: информационная безопасность web-ресурсов; открытое программное обеспечение; DDOS-атака; SQL-инъекция; криптографические методы; спам.

ENSURING INFORMATION SECURITY FOR WEB SITES

Barikov Leonid
Saint Petersburg State University of Aerospace Instrumentation (SUAI)
67 Bolshaya Morskaya St, St. Petersburg, 190000, Russia
e-mail: lnbarikov@gmail.com

Abstract. The information security issues of websites, which are solved in the process of their development, are considered, using the example of creating Internet stores.

Keywords: information security of web resources; open software; DDOS attack; SQL-injection; cryptographic methods; spam.

Введение. В настоящее время большое количество организаций, занятых в сфере торговли во всем мире, столкнулись с необходимостью перевести продажи частично или полностью из обычного формата в формат Internet-магазина. Этому способствовали введённые из-за пандемии ограничения на торговлю и желание потребителей проводить покупки без посещения физических торговых площадок. Согласно отчётам исследовательских агентств, за 2020-й год количество on-line заказов в Internet-магазинах в РФ увеличилось на 78% [1]. Согласно оценкам Digital Commerce 360 [2] и данным министерства торговли США, в 2020-м году потребители потратили $861,12 миллиардов on-line, что на 44,0% больше по сравнению с предыдущим годом. Такой рост торговли в Internet обеспечивается разработкой и реализацией Internet-магазинов, осуществляющих полный цикл обслуживания покупателей. Эти разработки должны учитывать решение вопросов информационной безопасности, которые возникают при on-line взаимодействии покупателей и магазинов.

Internet-магазин как торговая система представляет собой совокупность клиентской и серверной части web-сайта. Клиентская часть в свою очередь разделена на разделы, используемые покупателями, и разделы для администратора Internet-магазина. Клиентская часть представляет собой интерфейс, который используется для взаимодействия человека с web-сайтом.

Серверная часть отвечает за хранение, обработку и передачу информации между базой данных, клиентской частью и сторонними сервисами, такими как платёжные шлюзы, сервисы логистики и т.д. Кроме того, серверная часть осуществляет автоматическую обработку заказов, отправку информационных сообщений.

В комплексе эти системы и составляют Internet-магазин, осуществляющий полный цикл обслуживания покупателя в автоматическом или полуавтоматическом режиме.

Существующие методы решения задачи разработки Internet-магазина можно разделить на три категории.

К первой категории относятся различные системы управления сайтом и готовые (обладающие базовым функционалом) решения для электронной коммерции. Примерами решений из первой категории могут служить: WordPress, Joomla, 1С Битрикс. Такие решения поставляются в виде законченного программного обеспечения и инструкции по установке. Сама установка происходит в автоматическом или полуавтоматическом режиме. Базовые возможности доступны сразу, дополнительный функционал поставляется в виде расширений и шаблонов оформления. Несомненным достоинством является быстрота и простота, с которой можно получить готовый Internet-

магазин. К недостаткам в случае с бесплатными и условно-бесплатными системами можно отнести то, что не все расширения разработаны качественно. Основными вопросами являются возможные проблемы с безопасностью [3], скоростью работы и дальнейшей поддержкой конкретного расширения. Если происходит обновление версии основного программного обеспечения системы управления сайтом, то зачастую необходимо провести обновление кода расширения или темы. В случае, когда автор расширения больше его не поддерживает, пользователь вынужден либо отказаться от обновления основной части системы управления, либо вносить изменения в код расширения самостоятельно.

В случае использования готовых коммерческих систем пользователь получает схожее решение, однако в большинстве случаев основные расширения поддерживаются разработчиком платформы. Лицензия на подобное программное обеспечение может включать в себя платную техническую поддержку и другие платные услуги. Некоторые из коммерческих платформ поставляются с готовой, «из коробки», возможностью интеграции с другими программными продуктами от данного производителя. Коммерческие системы привязывают бизнес к одному конкретному поставщику программного обеспечения. Лицензия может ограничивать, какие модификации можно внести в код приложения. Кроме того, технические возможности для подобных модификаций могут быть ограничены.

Во вторую категорию будут отнесены коммерческие, бесплатные или условно-бесплатные платформы, позволяющие пользователю создать Internet-магазин, используя программное обеспечение, поставляемое в формате услуги (SaaS). Примерами могут служить платформы Square, Shopify, Wix. Некоторые решения из первой категории так же иногда предоставляются в виде SaaS.

Общая модель работы – подписка, при которой подписчикам предоставляется готовое программное обеспечение, полностью обслуживаемое провайдером. Достоинством является то, что пользователь получает полностью готовое решение, не требующее затрат на размещение, обслуживание, поддержку. С помощью графического интерфейса пользователь может провести настройку внешнего вида и информации, отображаемой на сайте.

Основным минусом является полная зависимость от провайдера, предоставляющего услугу. Создание резервных копий может быть затруднено по причине того, что код приложения принадлежит провайдеру услуги, а доступ к экспорту данных ограничен условиями лицензии или форматом экспорта. В случае отказа в обслуживании, ухода провайдера с рынка или каких-либо ещё причин, бизнес, использующий подобное решение, столкнётся с отсутствием возможности быстро восстановить работоспособность.

Возможность модификаций, настройки и адаптации подобных решений под нужды конкретного бизнеса ограничена предоставляемой платформой.

Третья категория — это решения, основанные на открытом программном обеспечении – фреймворках и библиотеках. Эти решения лишены многих недостатков, присущих решениям из первой и второй категории. Среди достоинств можно отметить бесплатность, открытость и максимальную свободу при реализации функционала Internet-магазина или любого другого сайта.

Кроме того, именно эти решения предоставляют разработчику наиболее актуальные инструменты для решения возникающих задач. Многие из открытых библиотек и фреймворков задают направление, по которому идет web-разработка. В качестве примера можно привести JavaScript фреймворки React и Vue.js.

К недостаткам можно отнести необходимость написания программного кода. Поэтому для реализации необходимого web-сайту функционала требуется больше времени, чем при использовании готовых систем. Кроме того, на разработчике лежит ответственность за обновление и поддержку кода сайта.

Для сайтов, состоящих из клиентской и серверной части характерно использование следующих технологий: языка разметки, языка описания внешнего вида документа, базы данных, языка программирования с возможность исполнения на клиентской части и серверного языка программирования.

Для разметки предлагается использовать язык гипертекстовой разметки HTML, который поддерживается всеми браузерами. Для разделения описания логической структуры web-страницы и описания внешнего вида предлагается применять язык CSS. В качестве языка программирования для клиентской части приложения рекомендуется выбирать язык JavaScript, так как именно он поддерживается браузерами в качестве сценарного языка. В качестве языка программирования для серверной части обычно выбирают язык PHP. Его отличительными особенностями являются простота, скорость разработки и большое количество популярных открытых фреймворков и библиотек. В качестве механизма связи между серверной частью web-сайта и базой данных предлагается использовать язык SQL. В качестве СУБД можно выбрать, например, свободную систему управления базами данных MySQL.

При разработке клиентской части web-сайта необходимо определить средства и инструменты, которые будут использоваться при работе с DOM.

Объектная Модель Документа (DOM) – это программный интерфейс (API) для HTML и XML документов. DOM позволяет управлять документом (web-страницей) используя объектно-ориентированное представление этого документа. Благодаря этому, возможно изменять документ, используя язык JavaScript.

Для управления документом можно воспользоваться как «чистым» JavaScript, так и библиотекой (например, jQuery) или фреймворком.

При разработке Internet-магазина требуется реализовать множество интерактивных элементов. Использование «чистого» JavaScript требует больших временных затрат и скорее подходит при реализации на странице базовых сценариев: вывести уведомление или спрятать элемент.

При выборе библиотеки или фреймворка стоит ориентироваться на то, какие решения наиболее востребованы на рынке web-разработки и популярны у разработчиков в текущий момент. Популярные ранее инструменты, такие как библиотека jQuery, в настоящий момент используются реже. Чаще всего эти инструменты необходимы, когда на сайте используется решение, основанное на этой библиотеке.

Для работы с клиентской частью приложения и создания интерактивных элементов предлагается выбирать JavaScript-фреймворк Vue.js. Фреймворк представляют собой программный продукт, который является «каркасом» программы. Он объединяет различные, связанные между собой и сконфигурированные для совместной работы, библиотеки и вспомогательные программы. Использование подобного «каркаса» облегчает и ускоряет разработку программного обеспечения. Фреймворк не является готовой системой управления сайтом.

Все популярные серверные web-фреймворки основаны на реализации шаблона проектирования MVC (Model-View-Controller или же модель-отображение-контроллер). Изначально MVC был разработан для приложений для настольных компьютеров, но позже распространился и стал очень популярен при web-разработке. MVC может быть применён практически ко всем используемым в web языкам программирования.

Использование шаблона проектирования MVC позволяет осуществлять быструю разработку современных web-приложений. При использовании MVC web-приложение делится на три основных компонента: контроллер, представление и модель.

Контроллер обрабатывает входящие запросы. Он также направляет трафик туда, куда он должен идти, определяет, какое представление должно быть загружено, взаимодействует с соответствующими моделями и возвращает ответ на входящий запрос.

Представление — это шаблон пользовательского интерфейса. Кнопки, формы и другая информация, видимая пользователю в Internet, являются частью представления. Контроллер вызывает представление после взаимодействия с соответствующей моделью, которая собирает информацию, необходимую для отображения в конкретном представлении.

Модель отвечает за запросы к базе данных и обработку данных. Модель загружает или записывает данные и возвращает результат в контроллер. Модель не имеет прямой связи с web-сервером или представлением.

Для реализации серверной части web-сайта необходимо выбрать такой инструмент, который:

- позволит реализовать паттерн MVC;
- будет соответствовать принципам открытого программного обеспечения;
- будет иметь большое сообщество разработчиков;
- будет иметь хорошую документацию.

Техническая реализация Internet-магазина должна быть рассчитана на то, что к клиентской и серверной части может одновременно поступать большое количество запросов.

Всем этим характеристикам отвечает несколько вариантов фреймворков для языка программирования PHP. На сегодняшний день наиболее широко используемым и зарекомендовавшим себя решением является фреймворк Laravel [4].

В работе Internet-магазина очень важно обеспечить быструю коммуникацию с пользователем посредством электронной почты. Несмотря на массовое появление мессенджеров и других способов связи, электронная почта остаётся важным инструментом в Internet-торговле. Через электронную почту осуществляется отправка рассылок, рекламных материалов, подтверждение информации о заказах и доставка пользователю важной информации.

Электронная почта используется не только бизнесом и индивидуальными пользователями, но и как инструмент для рассылки спама, вредоносных сообщений. Подобное негативное использование привело к тому, что все популярные сервисы электронной почты используют различные методы выявления легитимных сообщений от доверенных отправителей. Маркерами хорошего сообщения служат репутация IP-адреса, число успешных доставок сообщений, контент сообщения, число жалоб на спам со стороны пользователя.

С учётом указанных факторов при использовании собственных серверов Internet-магазина достаточно сложно обеспечить надёжную доставку сообщений электронной почты.

Основными угрозами, которые могут помешать нормальному функционированию web-сайта, являются:

- атака «отказ в обслуживании» или же DDOS-атака. При этой атаке на сервер отправляется огромное количество запросов, что вызывает перегрузку;
- хранение паролей пользователей в открытом виде. Если злоумышленники получат доступ к базе данных сервера, то пароли пользователей будут скомпрометированы;
- межсайтовая подделка запроса (CSRF). При этой атаке от имени пользователя может быть тайно отправлен запрос на сервер Internet-магазина;

– межсайтовый скриптинг (XSS). При этой атаке на страницу может быть внедрён вредоносный скрипт, который будет исполняться после того, как страница будет открыта в браузере;

– SQL-инъекция. При этой атаке в пользовательские данные, которые ожидает сервер, внедряется произвольный SQL код, который позволяет выполнять любые действия с базой данных.

Для противодействий атакам типа «отказ в обслуживании» сервер, на котором работает Internet-магазин, может использовать защитные сервера компании Cloudflare. Это позволит отфильтровать паразитный трафик и избежать перегрузки сервера.

Пароли пользователей предлагается хранить в базе данных с использованием bcrypt. Это адаптивная криптографическая хеш-функция формирования ключа, используемая для защищенного хранения паролей. Таким образом, никто кроме пользователя не имеет доступа к данным об используемом пароле.

Для противодействия атакам типа CSRF при получении от пользователя запросов, требующих отправки данных методом POST, предлагается проводить верификацию специального токена, который будет генерироваться в скрытом поле формы. Таким образом, сторонние лица не могут узнать или подделать этот токен и отправить данные без разрешения пользователя.

Для противодействия атаке типа XSS предлагается осуществлять фильтрацию и экранирование вывода данных, полученных от пользователя.

Для противодействия атакам типа SQL-инъекция предлагается использовать ORM Eloquent, которая, в свою очередь, использует механизм подготовленных запросов. Подготовленные запросы исключают возможность ошибок интерпретации, на которых основаны SQL-атаки. При получении данных от пользователя для сортировки по отдельным столбцам проводится сверка полученных данных со списком безопасных для работы столбцов. Для обеспечения безопасной передачи данных все соединения с сервером необходимо выполнять через безопасное соединение по протоколу HTTPS.

Владельцы Internet-магазинов часто сталкиваются с таким явлением как сбор данных о товарах и ценах конкурентами. Для этого используются автоматические программы, которые создают повышенную нагрузку на инфраструктуру Internet-магазина. Для решения этой задачи инфраструктурным решением является использование системы доставки контента, системы фильтрации трафика и использование реверсивного прокси-сервера с кешированием.

В предлагаемой схеме запрос изначально поступает к провайдеру, который обеспечивает доставку контента и защиту от атак. Каждый запрос анализируется специальным алгоритмом и в случае, если не выявляется подозрительной активности, то запрос передаётся на сервер Internet-магазина. Такой подход позволяет остановить работу автоматических программ сбора данных или какого-то другого программного обеспечения, направленного на прерывание работы Internet-магазина.

При реализации такого подхода дополнительным буфером между пользователем и сервером Internet-магазина предлагается использовать реверсивный прокси-сервер. В задачи этого сервера будет входить установка зашифрованного соединения с пользователем и проксирование запросов к серверной части Internet-магазина. На рис.1 показан процесс работы такой схемы.

Рис.1. Схема взаимодействия сервера Internet-магазина, системы доставки контента и реверсивного прокси-сервера.

В процессе реализации предлагается использовать бесплатный HTTP прокси-сервер Nginx. Этот сервер хорошо зарекомендовал себя при использовании в высоконагруженных web-приложениях.

В качестве сети доставки контента предлагается использовать сеть Cloudflare. Cloudflare предоставляет бесплатный тарифный план и обеспечивает все необходимые для выполнения данной работы функциональные возможности.

Заключение. Меры, описанные в статье, позволят повысить информационную безопасность разрабатываемого web-ресурса. Это, прежде всего, криптографические методы, интеграция с защитными сервисами и экранирование входных данных.

СПИСОК ЛИТЕРАТУРЫ

1. Data Insight Интернет-торговля в России 2020 [Электронный ресурс] URL: https://datainsight.ru/DI_eCommerce2020 (дата обращения: 20.06.2021).
2. Digital Commerce 360 Retail News [Электронный ресурс] URL: https://www.digitalcommerce360.com/article/us-ecommerce-sales/ (дата обращения: 20.06.2021).
3. Active Attack on Recently Patched Duplicator Plugin Vulnerability Affects Over 1 million Sites [Электронный ресурс] URL: https://www.wordfence.com/blog/2020/02/active-attack-on-recently-patched-duplicator-plugin-vulnerability-affects-over-1-million-sites/ (дата обращения: 20.06.2021).
4. Фреймворк Laravel. Официальная документация [Электронный ресурс] URL: https://laravel.com/docs/master (дата обращения: 25.06.2021).

УДК 004

СОЗДАНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ПРИНЯТИЯ УПРАВЛЕНЧЕСКОГО РЕШЕНИЯ ДЛЯ ПРОТИВОДЕЙСТВИЕ ВОЗНИКАЮЩИХ УГРОЗ В СИСТЕМЕ

Бурлов Вячеслав Георгиевич[1], Грачев Михаил Иванович[2], Капицын Сергей Юрьевич[3], Абрамов Валерий Михайлович[4]

[1] Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
[2] Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
[3] Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
[4] Российский государственный гидрометеорологический университет
Воронежская ул., 79, Санкт-Петербург, 192007, Россия
e-mails: burlovvg@mail.ru, mig2500@mail.ru, wolf.76@bk.ru, val.abramov@mail.ru

Аннотация. Рассматриваются процесс создания математической модели управленческого решения лица, принимающего решение в системе управления, как процесс противодействия возникающим угрозам возникших в системе и направленных против этой системы управления.

Ключевые слова: математическая модель; противодействие, управление; угроза, информационные системы и технологии; безопасность системы.

CREATION OF A MATHEMATICAL MODEL OF MANAGERIAL DECISION-MAKING FOR COUNTERING EMERGING THREATS IN THE SYSTEM

Burlov Vyacheslav[1], Grachev Mikhail[2], Kapitsyn Sergey[3], Abramov Valery[4]

[1] Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
[2] St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
[3] Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
[4] Russian State Hydrometeorological University
79 Voronezhskya St, St. Petersburg, 192007, Russia
e-mails: burlovvg@mail.ru, mig2500@mail.ru, wolf.76@bk.ru, val.abramov@mail.ru

Abstract. The process of creating a mathematical model of a managerial decision of a decision-maker in a management system is considered as a process of countering emerging threats that have arisen in the system and are directed against this management system.

Keywords: mathematical model; counteraction, management; threat, information systems and technologies; system security.

Введение. Формирование информационного пространства Российского в российском обществе проходит во всех сферах жизнедеятельности человека, коснулось это и образовательную систему. Повсеместное внедрение достижений науки и техники привело к распространению и внедрению в жизнедеятельность человека и общества «умных устройств». Тем не менее, и число угроз и атак на устройства и услуги системы «умный устройств» также увеличивается. Кибер атаки на безопасность системы управления не являются чем-то новым для этой системы, но, поскольку умные устройства будут тесно связаны с нашей жизнью и обществом, становится необходимым серьезно относиться к обеспечению безопасности пользователя и всю систему управления.

Следовательно, существует практическая необходимость в защите этих устройств, что в результате привело к необходимости всестороннего понимания угроз и атак на инфраструктуру системы «умных устройств».

Внедрение современных информационных технологий приведет к необходимости проводить обучение, подготовку и переподготовку персонала, задействованного на новых комплексах, так как противодействие возникающим угрозам будет складываться из степени подготовленности, как персонала, так и аппаратно-программной части распознать угрозу, вырабатывать решение и принимать решение по дальнейшей логике действий по противодействию возникшей угрозы.

Проведя анализ вышесказанного, можно сделать вывод, что лицо, отвечающее за противодействие возникающим угрозам, должно располагать адекватной моделью управленческого решения по противодействию возникающим угрозам.

Возрастающие требования к функционалу и наполнению систем безопасности сделали необходимостью в определении создания такой комплексной системы обеспечения общественной безопасности и правопорядка, которая в своей повседневной деятельности основывалась бы на современных подходах к анализу, прогнозированию и возможному предупреждению правонарушений и происшествий.

Проведение операций даже на известной местности требует от лица, принимающего решение (ЛПР) самих решений, так как основой системы управления является решение. ЛПР принимает решение на основе модели. Решение ЛПР должно, как содержать модель процесса, который он формирует (управляет), так и являться системой. Поэтому для осуществления деятельности адекватной сложившейся обстановке необходимо располагать адекватной математической моделью решения человека.

Без математической модели решения сложно гарантировать достижения цели управления.

Для формирования условий, гарантирующих достижения цели деятельности, используется естественно - научный подход (ЕНП). ЕНП определяется интеграцией свойств Мышления человека, окружающего Мира и Познания. Который реализуется научно-педагогической школой «Системная интеграция процессов государственного управления».

Трехкомпонентность отражается в трёх принципах:

Первый принцип трехкомпонентности основывается на условии существования, причинно-следственных связях и технологиях;

Второй принцип основывается на законе сохранения целостности объекта (ЗСЦО). ЗСЦО определяется как устойчивая, объективно повторяющаяся связь свойств объекта и действия при фиксированном предназначении;

Третий принцип представлен методами: декомпозиция, абстрагирование, агрегирование.

Принцип трёхкомпонентности познания состоит в том, что человек, осознанно или нет, осуществляет выработку решения в трёх уровнях представления обстановки.

Существует всего два подхода к разработке системы (модели). Это разработка на основе анализа и на основе синтеза. Подход на основе анализа обладает существенным недостатком - он не позволяет формировать процессы с наперёд заданными свойствами, что особенно важно. На рис.1 схематично представлена схема этапов синтеза модели управленческого решения.

Под управленческим решением мы будем понимать такие условия, обеспечивающие субъектом условия по реализации предназначения объекта, которым он управляет, в соответствующей обстановке в интересах достижения цели управления.

Обстановка — это такая совокупность факторов и условий, в которых осуществляется деятельность ЛПР.

Под управленческим решением мы будем понимать такие условия, обеспечивающие субъектом условия по реализации предназначения объекта, которым он управляет, в соответствующей обстановке в интересах достижения цели управления.

Обстановка — это такая совокупность факторов и условий, в которых осуществляется деятельность ЛПР.

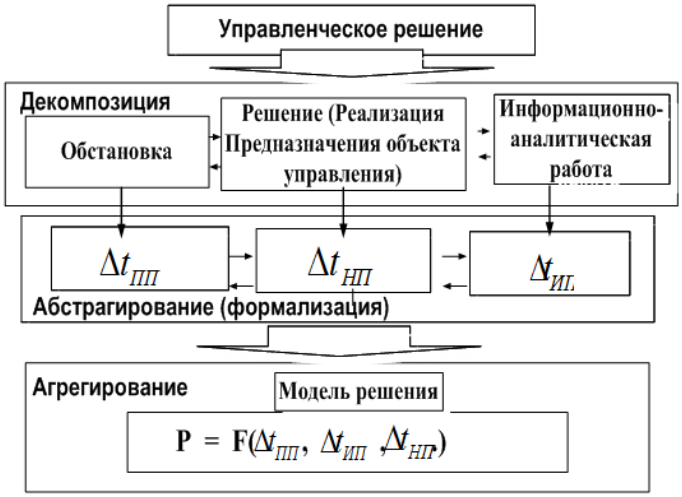


Рис.1. Структурная схема синтеза математическоймодели управленческого решения.

где: $\Delta t_{ПП}$ – проявление проблемы перед человеком;

$\Delta t_{НН}$ – нейтрализация (устранение) проблемы человеком; $\Delta t_{ИП}$ – идентификация (распознание) проблемы человеком.

Применив методы декомпозиции, абстрагирования и агрегирования мы преобразовали понятие «управленческое решение» в агрегат – математическую модель управленческого решения следующего вида:

$$P = F(\Delta t_{ПП}, \Delta t_{ИП}, \Delta t_{НП}) \quad (1)$$

В этом соотношении связаны три параметра.

Заключение. Таким образом мы установили зависимость характеристик проявления проблемы ($\Delta t_{ПП}$), идентификации проблемы ($\Delta t_{ИП}$) и её нейтрализации ($\Delta t_{НП}$), возникшей при управлении. Применение модели управленческого решения позволяют продолжить работу в области совершенствования информационного управляющих систем и позволяет своевременно противодействовать возникающим в системе угрозам, а также противодействовать им с необходимым уровнем заданной эффективности принятия управленческого решения.

Предлагаемый математический аппарат позволяет построить математическую модель управленческого решения и на основе этого увязать три важнейших процесса в организации обеспечения безопасности. За счет этой математической модели обеспечивается безопасность. Использование подхода к моделированию на основе синтеза позволяет строить такую систему, как система управления процессом обеспечения безопасной деятельности человека и общества в условиях возникновения угроз из требуемого уровня показателя эффективности. Соответственно, система, построенная на подобных началах, будет лишена основного недостатка – несоответствие результатов управления ожиданиям ЛПР. Подобных подход позволяет оценить любое принимаемое решение с позиции временных и ресурсных затрат, а также установить четкую, научно обоснованную связь принимаемого решения с результатами действия.

СПИСОК ЛИТЕРАТУРЫ

1. Бурлов, В. Г. Геоинформационные системы и вопросы управления в особых условиях / В. Г. Бурлов, С. А. Горелов, М. И. Грачев // Информационные технологии и системы: управление, экономика, транспорт, право. – 2017. – № 3(21). – С. 68-70.
2. Бурлов, В. Г. Модель управления транспортными системами, учитывающей возможности инноваций / В. Г. Бурлов, М. И. Грачев // Технико-технологические проблемы сервиса. – 2017. – № 4(42). – С. 34-38.
3. Бурлов В.Г., Грачев М.И. Разработка математической модели управленческого решения руководителя высшего учебного заведения, учитывающей возможности Web-технологий//Региональная информатика и информационная безопасность. Сборник трудов. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2016. С. 212-216.
4. Бурлов В.Г., Грачев М.И., Примакин А.И. Внедрение информационных технологий в процесс обучения как необходимость. В сборнике: Региональная информатика «РИ-2018» материалы конференции. 2018. С. 360-361.
5. Бурлов В.Г., Грачев М.И. Разработка математической модели управленческого решения руководителя высшего учебного заведения, учитывающей возможности Web-технологий//Региональная информатика и информационная безопасность. Сборник трудов. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2016. С. 212-216.
6. Бурлов В.Г., Грачев М.И. Модель управленческого решения как перспективное направление в обеспечении информационной безопасности. В сборнике: Информационная безопасность: вчера, сегодня, завтра. Сборник статей по материалам III Международной научно-практической конференции. Москва, 2020. С. 153-157.
7. Burlov V.G., Grachev M.I. Model of transport systems management, taking into account the possibilities of innovation. Technical and technological problems of service. 2017, vol. 42. no. 4, pp. 34-38. (In Russian) DOI: 10.1016/j.trpro.2017.01.023
8. Имитационная модель управления образовательной организацией высшего образования / М. И. Грачев, В. Г. Бурлов, О. Е. Чудаков, А. И.

Примакин // XXI век: итоги прошлого и проблемы настоящего плюс. – 2021. – Т. 10. – № 1(53). – С. 57-62. – DOI 10.46548/21vek-2021-1053-0010.
9. Бурлов, В. Г. Оценивание эффективности принятия управленческих решений в социально-экономических системах на примере учебного заведения высшего образования / В. Г. Бурлов, М. И. Грачев // T-Comm: Телекоммуникации и транспорт. – 2020. – Т. 14. – № 2. – С. 32-38. – DOI 10.36724/2072-8735-2020-14-2-32-38.
10. Модель управления в социальных и экономических системах с учетом воздействия на информационные процессы в обществе / В. Г. Бурлов, М. И. Грачев, М. Н. Васильев, С. Ю. Капицын // T-Comm: Телекоммуникации и транспорт. – 2020. – Т. 14. – № 5. – С. 46-55. – DOI 10.36724/2072-8735-2020-14-5-46-55.
11. Бурлов, В. Г. Аналитическо-динамическая модель управленческого решения в социально-экономических системах на примере руководителя учебного заведения высшего образования / В. Г. Бурлов, М. И. Грачев // T-Comm: Телекоммуникации и транспорт. – 2019. – Т. 13. – № 10. – С. 27-34. – DOI 10.24411/2072-8735-2018-10314.
12. Беженцев, А. А. Внедрение новых информационных технологий в образовательный процесс на основе использования учебных полигонов мониторинговый центр и ситуационный центр / А. А. Беженцев, В. Г. Бурлов, М. И. Грачев // T-Comm: Телекоммуникации и транспорт. – 2020. – Т. 14. – № 7. – С. 36-41. – DOI 10.36724/2072-8735-2020-14-7-36-41.

УДК 004.032.24

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ АДАПТИВНЫХ СИСТЕМ УПРАВЛЕНИЯ НА ОСНОВЕ СИТУАЦИОННОГО ЦЕНТРА

Власенко Александра Владимировна, Величко Александра Александровна
Кубанский государственный технологический университет
Московская ул., 2, Краснодар, 350072, Россия
e-mails: alex_vlasenko@list.ru, aleksandravelichko@mail.ru

Аннотация. Статья посвящена комплексному исследованию адаптивных систем управления. Рассматривается создание моделей и технологий, обеспечивающих показатели защищенности системы ситуационного центра. Методы, рассмотренные в статье, характеризуют иерархичность системы с точки зрения математической формулировки.

Ключевые слова: система; безопасность; управление решениями; модель; мониторинг; иерархия.

TECHNOLOGIES FOR ENSURING INTEGRATED SECURITY OF ADAPTIVE CONTROL SYSTEMS BASED ON THE SITUATIONAL CENTER

Vlasenko Alexandra, Velichko Alexandra
Kuban State Technological University
2 Moskovskaya St, Krasnodar, 350072, Russia
e-mails: alex_vlasenko@list.ru, aleksandravelichko@mail.ru

Abstract. The article is devoted to a comprehensive study of adaptive control systems. The article considers the creation of models and technologies that provide indicators of the security of the situation center system. The methods discussed in the article characterize the hierarchy of the system from the point of view of mathematical formulation.

Keywords: system; security; decision management; model; monitoring; hierarchy.

Введение. В эпоху высоких скоростей, технологии обеспечения комплексной безопасности адаптивных систем управления постоянно развиваются, вследствие этого управление можно сделать более эффективным и результативным — за счет повышения скорости и глубины анализа текущей ситуации, возможности прогнозирования ее дальнейшего развития, ускорения поиска ресурсов для решения проблем и достижения поставленных целей, контроля исполнения управленческих поручений, оперативности получения обратной связи о результатах управленческих воздействий [1].

Неадаптивные методы управления предусматривают наличие достаточного объёма априорных сведений о внутренних и внешних условиях работы на предварительной стадии. Чем полнее априорная информация о характеристиках, тем выше качество неадаптивного управления [2]. Инструментом при этом управлении становится интеллектуальный ситуационный центр.

Существующие методы оценки защищенности не способны отразить реальные показатели защищенности систем, однако, от данных недееспособных моделей до сих пор не отказываются, предполагая расширить возможности до необходимых критериев путем добавления недостающей функциональности или исправления серьезных ошибок без должной переработки системы, что затрудняет дальнейшее развитие.

В рамках данной задачи перспективным направлением исследований является создание моделей и технологий, обеспечивающих формирование и расширение сетецентрической информационной инфраструктуры системы распределенных СЦ для задач цифровой трансформации управления и обеспечения региональной безопасности.

Главной задачей сетецентрической системы СЦ является информационная поддержка управления – формирование ситуационной осведомленности и выработка рекомендаций для согласованного принятия управленческих решений на всех уровнях управления. Эта задача пока еще остается открытой как у нас, так и за рубежом, не имеет окончательного решения и, поэтому, требует детальной научной и экспериментальной проработки [3].

Применение технологии мультиагентных систем позволяет создавать адекватную среду информационно-аналитической поддержки процесса разработки стратегии адаптивных систем управления, учитывающую распределенность динамичность и структурную сложность образующих его подсистем с субъектами деятельности.

При анализе иерархической структуры для системы с большим количеством элементов, возникает задача выделения уровней, группировки элементов по уровням и установлением связей. Данная задача решается при выполнении ограничений, связанных с принадлежностью элементов к заданным группам (кластерам) [5].

Зарубежный и отечественный опыт обеспечения комплексной безопасности свидетельствует о том, что для борьбы с потенциально возможными и реально возникающими угрозами необходима строгая и узконаправленная организация процесса противодействия

Для реализации нормального информационного потока в адаптивной системе необходимо использовать комплексный мониторинг системы, включающий в себя такие ключевые принципы как:

– всесторонний мониторинг всех ресурсов, задействованных в обеспечении принятия управленческих решений;
– консолидация информации о критичных событиях в едином центре обработки;
– предотвращение мониторинга всех ресурсов и показателей;
– накопление исторической информации мониторинга с целью дальнейшего анализа и принятия решений.

Анализируя существующие подходы реализации иерархических структур для применения в рамках ситуационного центра, определены 3 наиболее перспективных в соответствии с источниками [6-12].

Рассмотрим подробнее каждый из них.

Структурный подход. Структурный метод подразумевает под собой разбиение процесса на структурные операции, представленные в виде типовых таблиц (далее ТЭФ) с добавлением к ним дополнительных единиц функционирования, отражающих индивидуальные особенности моделируемой системы.

Для него характерно: углубленное внимание к описанию актуального состояния объектов; выяснение внутренне присущих им вневременных свойств; интерес не к изолированным фактам, а к отношениям между ними. В отношении структурного анализа необходимо обратить внимание на то, что в его основу положено выделение абстрактных элементов и применение математизации. Например, трехуровневую систему возможно описать при помощи следующих уравнений:

$$\mu = \{\, \mu_1 = \frac{N}{N(N-1)};\ \mu_2 = \frac{M}{N(N-1)k(k-1)};\ \mu_3 = \frac{M}{N(N-1)k(k-1)r(n+m)(r(n+m)-1)} \} \quad (1)$$

где μ - количество функций на определенном уровне иерархий;

k –количество элементов системы;

n –количество уровней;

n+m- количество выходов информацией;

r-количество входов системы.

К плюсам структурного метода стоит отнести возможность ориентирования его на выявление и описание самой структуры объектов, смещение акцента от элементов системы к взаимосвязям и отношениям между ними. Минусами этого метода являются сложность представления иерархической структуры и большие временные затраты.

2. Метод аналитических иерархических процессов. Применяется для решения задач ранжирования конечного множества сложных объектов, прямое попарное сравнение которых невозможно.

Этот метод более общая форма метода анализа иерархий, используемого в условиях мультикритериальности. МАИ структурирует решение проблемы в иерархию с целью определения критерия выбора и альтернативы, в то время как МАС структурирует его в качестве аналитической сети, и затем используют систему парных сравнении для измерения веса компонентов структуры, и, наконец, ранжирует альтернативы в решении.

Компоненты вектора иерархических процессов:

$$\omega_i = \sqrt[n]{\prod_{j=1}^{n} \frac{\omega_i}{\omega_j}} \quad (2)$$

где $\omega_{i,J}$ - оценка элементов иерархии (веса критериев).

К плюсам данного метода можно отнести: выделение разновероятностных альтернатив системы, для выбора лучшего варианта. К минусам относится проблема невозможности распределения всех существующих альтернатив без СППР.

3. Методы теории когнитивного, ситуационного и имитационного моделирования отображают особенности принятия решений в динамической сложной (иерархической) среде. Рассматриваются модели следующего характера:

– качественные модели системной динамики, такие как графические диаграммы прямых и обратных причинно-следственных связей и глобальных слияний одних параметров на другие во времени.
– количественные модели. К ним принято относить потоковые дискретно-событийные, агентные модели.

– потоковые модели представляются в виде диаграмм и имеют четкое математическое описание, и соответственно позволяют проводить количественный анализ.

– дискретно-событийные модели предполагают отказ от рассмотрения непрерывного изменения системы, происходящего в определенный момент времени, когда наблюдается изменение состояния системы.

– агентные модели предложены для использования децентрализованных систем, динамика функционирования которых определяется индивидуальной активностью членов (агентов) группы, а не глобальными правилами и законами. Здесь агент, некая сущность, обладающая активностью, автономным поведением, может принимать решения в соответствии с некоторым набором правил, взаимодействовать с окружением, а также самостоятельно изменяться.

– ситуационные модели, основанные на идеях теории искусственного интеллекта: представление знаний об объекте управления им на уровне логико-лингвистических моделей, использование обучения и обобщения в качестве основных процедур при построении процедур управления по текущим ситуациям, с использованием дедуктивных систем для построения многошаговых решений.

Плюсами методов когнитивного, ситуационного и имитационного моделирования можно назвать возможность применения для различных областей, наглядное рассмотрение структур, адаптивность, высокая степень проработки структуры. К минусам большая трудозатратность и объемность моделей структуры.

Авторами проведен сравнительный анализ методов построения иерархических структур для комплексной системы безопасности по критериальным показателям, представленным в таблице 1.

Таблица 1

Сравнительный анализ методов

№ п/п	Используемый метод	Масштабируемость	Адаптируемость к различным задачам	Надежность	Возможность сохранения информации для дальнейшего исследования
1	Структурный	+	-	+	+-
2	Аналитических и иерархических процессов	+	+-	+	+
3	Теория когнитивного, ситуационного и имитационного моделирования	+	+	+	+

Проведенный анализ позволяет определить, что наилучшими для создания адаптивной иерархической структуры комплексной системы безопасности подходят технологии теории когнитивного, ситуационного и имитационного моделирования, обеспечивающие масштабность действий и адаптивность моделей к изменяющимся условиям.

Заключение. Описанные выше авторами статьи возможные технологии создания комплексной системы безопасности в составе ситуационного центра позволяет сделать следующие выводы.

Комплексная система обеспечения безопасности представляет собой сложную иерархическую систему в составе интеллектуального ситуационного центра, которая обеспечивает организацию обеспечения безопасности как объекта управления, так и ситуационного центра, в частности.

Предложенные методы и подходы построения иерархической структуры системы комплексной безопасности системного анализа могут с успехом применять для построения КСОБ в рамках СЦ.

Наиболее эффективными для построения КСОБ представляются технологии моделирования, позволяющие построить максимально адаптивную структуру системы для решения различных задач и возможности реагирования на инциденты.

Исследование выполнено при финансовой поддержке РФФИ и администрации Краснодарского края в рамках научного проекта № 20–47–235003 «Разработка теоретических основ и алгоритмов функционирования адаптивных иерархических систем управления с использованием методов искусственного интеллекта на основе ситуационных центров.

СПИСОК ЛИТЕРАТУРЫ

1. Ситуационный центр как инструмент управления [Электронный ресурс]/Антон Трунович 28.02.2020 - https://vc.ru/services/109504-situacionnyy-centr-kak-instrument-upravleniya (Дата обращения 16.08.2021)
2. Калдыбаев Р.С. АДАПТИВНЫЕ (САМОНАСТРАИВАЮЩИЕСЯ) СИСТЕМЫ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ // Международный студенческий научный вестник. – 2020. – № 6. [Электронный ресурс] URL: https://eduherald.ru/ru/article/view?id=20320 (Дата обращения: 20.08.2021).
3. Oleynik A., Fridman A., Masloboev A. Informational and analytical support of the network of intelligent situational centers in Russian Arctic // CEUR Workshop Proceedings. 2018. vol. 2109. pp. 57-64.

4. Вопросы построения ИСО для крупных промышленных объектов// Системы безопасности. 2008. №3. С. 89-95 Обзор алгоритмов кластеризации данных (Дата обращения 19.09.2021)
5. Дубровская Л.И., Князев Г. Б. Компьютерная обработка естественно-научных данных методами многомерной прикладной статистики: Учебное пособие. - Томск: ТМЛ-Пресс, 2011,- 120 с.
6. Михайлова С.В. «Инструментарий оценки эффективности функционирования комплексной системы обеспечения безопасности корпоративной компьютерной сети»/ автореф. канд.техн.наук: спец. 05.13.13/ 2003
7. Семенова В.А. «Модель и метод формирования комплексной системы банковской безопасности» автореф. канд.техн.наук: спец.05.13.19 /2008
8. Дунина В.С. «Моделирование интеллектуальных систем управления защитой информации в инфокоммуникационных системах ОВД». автореф. канд.техн.наук: спец.05.13.18 /2012
9. Горелова Галина Викторовна Когнитивный подход к имитационному моделированию сложных систем // Известия ЮФУ. Технические науки. 2013. №3 (140). URL: https://cyberleninka.ru/article/n/kognitivnyy-podhod-k-imitatsionnomu-modelirovaniyu-slozhnyh-sistem (дата обращения: 19.09.2021).
10. Ахлюстина С.Б. «Математическое моделирование оценки защищенности объектов с эргатическими интегрированными системами безопасности». автореф. канд.техн.наук: спец.05.13.18 /2020
11. Демидова Н.Е. «Математические модели и методы анализа иерархий в системах обеспечения информационной безопасности» автореф. канд.техн.наук: спец.05.13.01 /2004
12. Израилова К.Е. «Метод алгоритмизации машинного кода для поиска уязвимостей в телекоммуникационных устройствах». автореф. канд.техн.наук: спец.05.13.19 /2017.

УДК 004.451:004.056

ПРИМЕНЕНИЕ ТРЕБОВАНИЙ БЕЗОПАСНЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ДИСТАНЦИОННОГО ИЗУЧЕНИЯ ДИСЦИПЛИНЫ «ОПЕРАЦИОННЫЕ СИСТЕМЫ»

Егоров Сергей Сергеевич, Широков Владимир Владимирович, Щиголева Марина Андреевна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: ssegorov@mail.ru, vvshirokov@mail.ru, vvcehanovsky@mail.ru

Аннотация. В работе рассматривается опыт преподавания дисциплины «Операционные системы» с использованием требований безопасных информационных технологий учащимся бакалавриата по направлению «Информационные системы и технологии» и специалитета по направлению «Компьютерная безопасность». Учтены требования к необходимым умениям и формируемым необходимым знаниям обучаемых при создании перспективных современных средств разработки программных продуктов. Отмечены слабые стороны дистанционного формата обучения и предложены способы активизации процесса изучения дисциплины.

Ключевые слова: безопасность информационных технологий; требования к безопасности программного продукта; дистанционный формат обучения; операционная система.

APPLICATION OF THE REQUIREMENTS OF SECURE INFORMATION TECHNOLOGIES FOR REMOTE STUDY OF THE DISCIPLINE «OPERATING SYSTEMS»

Egorov Sergey, Shirokov Vladimir, Schigoleva Marina
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: ssegorov@mail.ru, vvshirokov@mail.ru, vvcehanovsky@mail.ru

Abstract. The paper considers the experience of teaching the discipline «Operating Systems»using the requirements of secure information technologies to students of the bachelor's degree in the direction of» Information Systems and Technologies «and the specialty in the direction of «Computer Security». The requirements for the necessary skills and the necessary knowledge formed by the trainees are taken into account when creating promising modern software development tools. The weaknesses of the distance learning format are noted and ways to activate the process of studying the discipline are proposed.

Keywords: information technology security; software product security requirements; distance learning format; operating system.

Для реализации дистанционного обучения дисциплины «Операционные системы» методические материалы дисциплины [1, 2] были проанализированы на соблюдение требований к безопасности программного продукта, разрабатываемого обучаемыми в качестве отчетных заданий по изученному курсу. Учебный курс дисциплины содержит лекционный материал с конспектом лекций по предусмотренному набору тем и комплекс практических заданий по всем темам лекций. В соответствии с профессиональным стандартом программиста, которому должны по роду профессиональной деятельности соответствовать выпускники направления «Информационные системы и технологии» и квалификации программиста по специальности «Компьютерная безопасность», необходимо обеспечить выполнение профессиональных трудовых функций, поддержанных необходимыми знаниями, умениями и навыками по разработке и проектированию программного продукта.

Учет необходимых требований при создании перспективных современных программных продуктов и средств разработки программных продуктов является необходимой составляющей обеспечения безопасности информационных технологий, применяемых на всех этапах профессиональной деятельности программиста от проектирования и создания до практического применения программных средств реализации информационных компьютерных технологий. Обучаемым необходимо получить навык реализации существующих требований к программному обеспечению, программным компонентам и средствам их взаимодействия - сервисного и коммуникационного.

По требованиям безопасных информационных технологий необходимо: оценить возможность реализации требований к программному обеспечению; проводить анализ возможностей и дополнительной трудоемкости реализации требований; проводить анализ исполнения требований; вырабатывать варианты реализации требований. На основании необходимости реализации этих требований, методологии и технологии обучения безопасным информационным технологиям должны включать эти знания в существующую программно-техническую архитектуру, программное обеспечение и технологии программирования, комплексы современных перспективных средств разработки программно-технических продуктов.

Дистанционный формат обучения подразумевает изначально более плотную сшивку набора тем в общую тематику дисциплины; компиляцию теоретического и практического материалы по каждой теме; совокупность оценочных средств освоения как лекционного материала, так и результатов выполнения практических заданий. Специфика дистанционного формата и опыт его реализации позволили выстроить стратегию обучения в виде логической последовательности лекционного материала по темам изучения с сопровождением каждой темы материалом практических занятий.

Дисциплина курса включает:

– Конспект лекций, по числу разделов дисциплины. Разделы поддерживаются файлами в формате docx по числу разделов дисциплины и дополнены видеолекциями в формате mp4 (от трех до пяти файлов mp4 на один раздел). Каждый файл создан путем сохранения озвученной презентации (pptx) через меню «Демонстрация экрана» среды Zoom. Каждый раздел в среде Moodle представлен ресурсом «Тема».

– Практические занятия. Представлены методические указания к выполнению практических работ в формате файла docx, и видеоуроки для каждой работы. Лекции и практические занятия поддерживаются единой технологией представления материала и его визуализации. Каждая практическая работа представлена ресурсом «Задание» среды Moodle.

Практические задания охватывают все разделы курса. На каждый раздел приходится от одного до пяти заданий [3, 4]. Все задания выстроены в логической последовательности, определяемой материалом курса. Обучаемым запрещено нарушать эту последовательность: нельзя посылать на проверку некоторую работу, не сдав работу предыдущего шага технологии. Ограничения диктуются не только очередностью, но и необходимостью согласования с преподавателем вариантов задания следующего шага технологии обучения. Перечисленные ограничения необходимы для введения упорядоченности приема работ при большом потоке заданий, а также как элемент актуализации контакта с обучающимся на каждом шаге технологии обучения.

Для выполнения заданий необходимо прочитать лекционный материал раздела, просмотреть видеолекции, просмотреть видеоуроки и, согласно методическим указаниям, реализовать программу, использующую программный интерфейс (API) операционной системы, относящийся к изучаемому разделу. Результаты работы показали большой интерес учащихся к практической части курса. Однако, как правило, по собственной инициативе они ограничивались изучением методических указаний для реализации работ. Выдача дополнительных заданий, связанных с лекциями, видеолекциями и видеоуроками, позволяет стимулировать работу с этими методическими материалами. Выдача персональных дополнительных заданий также активизирует самостоятельную работу, хотя и является трудоемкой при большом потоке учащихся. Для облегчения этого процесса было бы целесообразно усовершенствовать систему сортировки, группировки и фильтрации обработки выполненных заданий.

Важную положительную роль играет синхронизация работы среды Moodle с корпоративной почтой. Такая синхронизация позволяет выстраивать очередь проверяемых работ в хронологическом порядке их посылки учащимися, что важно при большом потоке.

Для оценки результатов освоения учащимися материала курса кроме ресурса «Задание» в среде Moodle предусмотрено использование еще ресурсов «Тест» и «Опрос». В них реализован принцип «вопрос-ответ», причем вопросы могут выбираться из банка вопросов, а ответы могут быть, как бинарные, так и множественные. Поскольку правильные ответы заранее известны преподавателю, то здесь было бы целесообразно реализовать функцию автоматического формирования оценок, а на ее основе и такой ресурс как «Зачет/Экзамен».

СПИСОК ЛИТЕРАТУРЫ

1. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. — СПб.: Питер, 2015. — 1120 с.: ил. — (Серия «Классика computer science»).
2. Система электронного обучения и тестирования Moodle: обзор возможностей. URL: https://www.ispring.ru/elearning-insights/moodle.
3. [Электронный ресурс] URL: http://manpages.org/namespaces/7 (Дата обращения: 12.10.2021).
4. [Электронный ресурс] URL: http://manpages.org/acl/5 (Дата обращения: 12.10.2021).

УДК 681.1.003

СТАТИСТИЧЕСКАЯ УСТОЙЧИВОСТЬ РЕЗУЛЬТАТОВ РЕТРОСПЕКТИВНЫХ ИССЛЕДОВАНИЙ НА ОСНОВЕ ГЕОХРОНОЛОГИЧЕСКОГО ТРЕКИНГА

Ивакин Ян Альбертович, Потапычев Сергей Николаевич
[1] АО «Концерн «Океанприбор»
Чкаловский пр., 46, Санкт-Петербург, 198226, Россия
[2] Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: potapychev@mail.ru, yan_a_ivakin@mail.ru

Аннотация. Геохронологический трекинг получил широкое признание как соответствующий научно-методический инструментарий и эффективная информационная технология ретроспективных исследований в интересах обоснования и рационализации маршрутных сетей транспорта, логистики перевозок, анализа фактов миграции населения и перемещений отдельных исторических личностей и пр. На базе геохронотрекинга разработана процедура статистической проверки исследовательских гипотез об устойчивых тенденциях в развитии различных пространственно-временных процессов. Надежность и достоверность принятия той или иной гипотезы в рамках ретроспективного исследования определяется представительностью (репрезентативностью) объема исходных данных о географических перемещениях, рассматриваемых как выборка из генеральной совокупности. Статистическая значимость (устойчивость) результатов ретроспективного исследования на основе геохронологического трекинга зависит от достаточности учтенных исходных данных о перемещениях исследуемых объектов. Анализу указанной зависимости и выработке алгоритма оценки указанной устойчивости (значимости) посвящен данный доклад.

Ключевые слова: географические информационные системы; ГИС-технологии для ретроспективных исследований; геохронологический трек и трекинг; изоморфизм графов; рациональный алгоритм; междисциплинарные исследования на базе ГИС; статистическая устойчивость выводов.

STATISTICAL ROBUSTNESS SUPPORT OF RETROSPECTIVE RESEARCH BASED ON GEOCHRONOLOGICAL TRACKING

Ivakin Yan, Potapychev Sergey
[1] JSC «Concern «Oceanpribor»
46 Chkalovsky Av, St. Petersburg, 198226, Russia
[2] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: potapychev@mail.ru, yan_a_ivakin@mail.ru

Abstract. Geochronological tracking has been accorded wide recognition as an appropriate scientific and methodological toolkit and an effective information technology for retrospective research in the interests of substantiating and rationalizing transport route networks, transportation logistics, analyzing the facts of population migration and movements of individual historical figures. A procedure based on geochronological tracking for statistical verification of research hypotheses has been developed about robust trends in the development of various spatio-temporal processes. The reliability and validity of accepting a particular hypothesis within the framework of a retrospective study is determined by the representativeness of the initial dataset on geographic movements, considered as a sample from the general population. The statistical significance (robustness) of the results of a retrospective study based on geochronological tracking depends on the sufficiency of the considered initial data on the movements of the objects under study. This article is devoted to the analysis of this dependence and the development of an algorithm for assessing the specified robustness (or significance).

Keywords: Geographic information systems; GIS-technologies for historic research; geochronological track and tracking; graphs isomorphism; optimal algorithm; refinement of algorithm; GIS-based interdisciplinary research; statistical inference robustness.

Ретроспективный статистически-значимый анализ перемещений в географическом пространстве есть база для принятия решений по организации различных пространственно-временных систем. Геохронологический трекинг получил широкое признание как соответствующий научно-методический инструментарий и эффективная информационная технология ретроспективных исследований в интересах обоснования и рационализации маршрутных сетей транспорта, логистики перевозок, анализа фактов миграции населения и перемещений отдельных исторических личностей и пр. Основные принципы, процедуры и алгоритмы геохронологического трекинга описаны в [1-3]. Его математическая сущность сводится к поиску и оценке статистической значимости изоморфизма соответствующих графов: итоговый граф геохронотрекинга представляется как граф-базис в структуре которого выявляется подграф изоморфный заданному, т.е. устанавливается наличие взаимно однозначного отображения одного графа на подграф другого, при котором сохраняется отношение инцидентности [2]. Граф, на изоморфность к

которому в составе базового графа геохронологического трекинга определяется подграф, топологически описывает ту или иную определенную гипотезу исследования об устойчивой особенности в перемещениях исторических личностей, объектов или других сущностей в географическом пространстве. Далее определяется степень устойчивости в признании гипотезы исследования о выявляемой особенности в перемещениях с использованием статистического аппарата доверительной вероятности и доверительных интервалов [3].

Вместе с тем, надежность и достоверность принятия той или иной гипотезы в рамках ретроспективного исследования определяется представительностью (репрезентативностью) объема исходных данных о географических перемещениях, рассматриваемых как выборка из генеральной совокупности. Статистическая значимость (устойчивость) результатов ретроспективного исследования на основе геохронологического трекинга зависит от достаточности учтенных исходных данных о перемещениях исследуемых объектов. Иными словами, для принятия исследовательских гипотез ретроспективного исследования на базе геохронотрекинга с заданной доверительной вероятностью должно быть обеспечено необходимое и достаточное (релевантное) число учтенных единичных геопространственных перемещений, рассматриваемых как единичные статистические испытания. Обоснованная выработка математико-статистического аппарата и методики увязывания доверительной вероятности принятия гипотез исследований на базе геохронотрекинга с исходным числом учитываемых перемещений составляет существо обеспечения статистической устойчивости (значимости) выводов указанных исследований.

Разработка и обоснование математико-статистического аппарата и методики определения необходимого и достаточного (релевантного) числа разовых испытаний в ходе ретроспективных исследований на базе геохронотрекинга для обеспечения требуемого уровня доверия к итоговым результатам осуществлено путем последовательной реализации следующих логических шагов:

Теоретическая разработка и адаптация к условиям исследования математико-статистических основ определения необходимых и достаточных объемов выборки из генеральной совокупности данных о единичных перемещениях в географическом пространстве для обеспечения заданного значения доверительной вероятности получаемых выводов проводимого ретроспективного исследования;

Интерпретация выделенного математико-статистического аппарата, как аппарата обеспечения требуемого уровня надежности получаемых выводов проводимого ретроспективного исследования, применительно к подходам и моделям геохронотрекинга;

Конкретизация и описательное представление алгоритма расчета релевантного числа учитываемых перемещений объектов- единичных испытаний в ходе ретроспективных исследований методом геохронотрекинга для обеспечения приемлемого уровня рисков при принятии итоговых решений.

Детализация существа указанных шагов позволяет раскрыть существо методики определения необходимого и достаточного числа разовых испытаний в ходе ретроспективных исследований на основе геохронотрекинга для обеспечения требуемого уровня доверия к результатам и выводам исследования, в целом.

В рамках постановки ретроспективных исследований на базе геохронотрекинга в работах [4, 5] в качестве генеральной совокупности данных рассматривается теоретическое число выборочных значений учитываемых перемещений рассматриваемых объектов, обеспечивающее доверительную вероятность принятия решений о выводе частного исследования равным 1. Очевидно, что размер генеральной совокупности, при данной постановке, теоретически не ограничен, однако на практике объем данных положенных в основу геохронотрека всегда конечен и ограничен. Тогда, частная задача определения релевантного (т.е. необходимого и достаточного) объема выборки из генеральной совокупности данных о перемещениях в географическом пространстве за заданный промежуток времени для обеспечения заданного уровня доверия к выводам исследования сводится к математическому увязыванию значения доверительной вероятности правильного вывода в оценке исследуемого параметра с таким числом единичных испытаний, которое обеспечивает оценку требуемого доверительного интервала в разбросе искомого параметра. В своей информационно-логической сущности данная задача детально рассмотрена и теоретически решена в работах, посвященных информационным технологиям компьютерного моделирования, трудах по теории вероятности и прикладной статистике. Например, в таких как [6-10]. Существо теоретического решения данной задачи заключается в построении (оценке) доверительного интервала для исследуемого параметра, обусловленного заранее заданной доверительной вероятностью, как некоторого двумерного функционала, определяемого разницей между теоретическим значением искомого параметра и выборочным значением накопленной статистики его оценок.

В работах [7, 8, 10] решение указанной частной математической задачи сведено к построению конкретизированных эллипсов рассеивания выборочных значений исследуемых параметров применительно к назначаемым величинам доверительной вероятности. Очевидно, что в условиях гехронологического трекинга, т.е. в условиях дискретного прироста объема значений данных по итогам разовых испытаний, а также объективной ограниченности генеральной совокупности в силу конечности учитываемых данных о географических перемещениях анализируемых объектов, сводная теоретическая картина решения указанной частной математической задачи может быть преобразована к дискретному варианту представления. В частности, соотношение числа r выбросов в экспериментально получаемых значениях параметра вне обоснованного эллипса среднеквадратического отклонения

к общему числу единичных испытаний (наблюдений) эксперимента N в рамках эксперимента позволяет формализовать решение указанной частной задачи (для дискретного варианта) в виде, показанном на рис. 1.

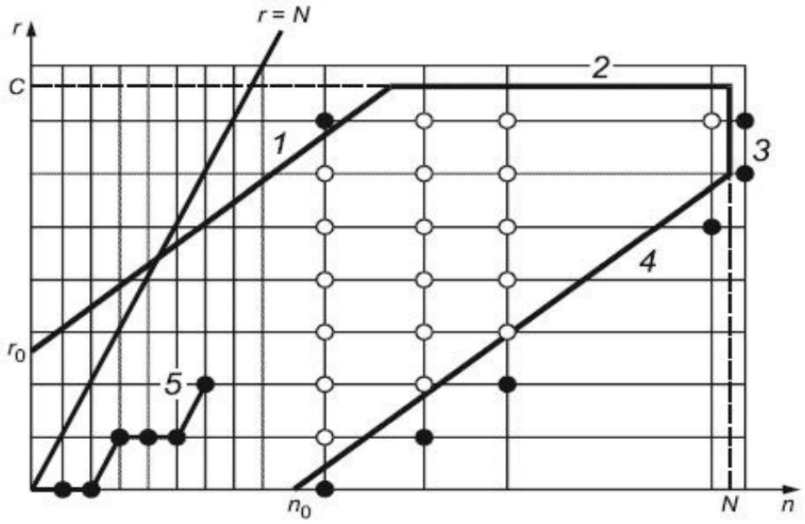


Рис. 1. Интерпретация наблюдаемых выборочных значений исследуемого параметра при накоплении его статистики в ходе геохронотрекинга.

Так, на рис. 1 фигура, ограниченная линиями 1-2-3-4, является дискретной интерпретацией эллипса среднеквадратического отклонения, определяемого доверительным интервалом и интервалом допуска, соответствующих задаваемой доверительной вероятности правильного принятия решения в ретроспективном исследовании на базе геохронотрекинга. Соответственно, линии 1 и 2 обозначают границы зоны, за которыми регистрируемые экспериментальные значения параметра нельзя считать соответствующими теоретическому значению. Линии 3 и 4 обозначают границы зоны избыточного числа единичных испытаний при обоснованном принятии решения с заданной доверительной вероятностью, что принимаемые значения параметра геохронотрека следует считать соответствующими теоретическому значению. Линия 5 обозначает дискретный процесс накопительного учета выбросов в экспериментально получаемых значениях исследуемого параметра вне обоснованного эллипса среднеквадратического отклонения при геохронотрекинге в зависимости от текущего суммарного числа одиночных испытаний (наблюдений) в ходе исследования. При этом, очевидно, что линия дискретного учета выбросов 5 в экспериментально получаемых значениях исследуемого параметра не может попадать в область, расположенную на рис. 1 выше границы

$$r = N. \quad (1)$$

Приведенная на рис. 1 интерпретация решения логико-математической задачи определения релевантного (т.е. необходимого и достаточного) объема выборки из генеральной совокупности данных многократных испытаний - перемещений для обеспечения заданного уровня доверия к выводам ретроспективного исследования позволяет рассматривать указанный объем выборки как ключевой показатель обеспечения требуемой надежности выводов проводимого исследования. То есть, релевантным является такое не избыточное число единичных испытаний (учитываемых перемещений в географическом пространстве), которое обеспечивает заданную, в виде доверительной вероятности, надежность результатов проведения ретроспективных исследований. Именно такое понимание задачи определения релевантного объема выборки из генеральной совокупности данных геохронотрекинга для обеспечения заданного уровня доверия к выводам исследования позволило интерпретировать её в рамках подходов к определению надежности статистических выводов в рамках эксперимента на базе ГИС.

Результаты (Results). В общенаучном смысле, надежность выводов исследования – это свойство такого объекта инфосферы, как вновь полученное знание, устойчиво и неизменно вырабатывать функционально пригодные и достоверные результаты при заданных начальных данных и входных условиях [11]. Применительно к условиям проведения ретроспективных исследований на базе геохронотрекинга показателем с количественной мерой для оценки указанной надежности выступает доверительная вероятность истинности результатов частного испытания, исследования. При этом доверительная вероятность истинности результатов задается априорно и обеспечивается в ходе проведения ретроспективных исследований путем проведения релевантного (прежде всего, достаточного) числа элементарных испытаний.

Вышеописанный вариант рассмотрения статистической сущности проводимого исследования позволил интерпретировать её в рамках стандартизированного аппарата обеспечения и расчета показателей надежности в технике [12]. Указанный аппарат разработан, апробирован и рекомендован к применению в рамках действующей

национальной системы нормативно-технического регулирования. Он применим к предметной области ретроспективных исследования на базе геохронотрекинга в ГИС.

Интерпретация математико-статистического аппарата, обеспечения требуемого уровня доверительной вероятности к получаемым выводам проводимого исследования на базе геохронотрекинга сводится к определению основных входных и выходных переменных указанного аппарата в категориях проводимого в ГИС анализа перемещений исследуемых сущностей (объектов), а также заданию общих граничных условий его применения. В частности, объемы испытаний N (общее число одиночных учитываемых перемещений в составе трека (наблюдений)) установленные в разработанной методике, основаны на предположении, что единичные испытания являются статистически независимыми и значение доверительной вероятности истинности получаемых выводов является постоянным.

По результатам полного объема испытаний N по каждой из исследуемых характеристик геохронотрека принимается одно из следующих альтернативных исследовательских решений:

– наблюдаемое (регистрируемое) и осредненное по N единичным актам испытаний значение численного параметра (качественного проявления) геохронотрека принимается истинным с доверительной вероятностью P (т.е. принятие значения как истинного, с определенным уровнем доверия);

– наблюдаемое (регистрируемое) и осредненное по N единичным актам испытаний значение численного параметра (качественного проявления) геохронотрека не принимается истинным (т.е. отклонение значения как истинного, с определенным уровнем доверия).

В рамках геохронотрекинга альтернатива Б. означает необходимость либо снижения априорного уровня требуемой доверительной вероятности правильного принятия исследовательского решения, либо дальнейшего наращивания общего числа N одиночных испытаний (учитываемых перемещений)) для подтверждения надежности принимаемых исследовательских решений. В отдельных случаях – изменения постановки организации ретроспективного исследования.

Применительно к методике определения необходимого и достаточного (релевантного) числа разовых испытаний в ходе ретроспективных исследований на базе геохронотрекинга для обеспечения требуемого уровня доверия к итоговым результатам приняты следующие обозначения входных и выходных величин, переменных используемого научно-методического аппарата:

P - апостериорная, т.е. накопленная в треке доверительная вероятность истинности частного результата ретроспективного исследования, значения численного параметра (качественного проявления) той или иной дуги трека;

P_α - априорный уровень вероятности доверительного принятия значения численного параметра (качественного проявления) той или иной дуги трека;

P_β - априорный уровень вероятности доверительного отклонения (несоответствия, непризнания истинности) значения численного параметра той или иной дуги трека;

Q - апостериорное значение вероятности риска некорректного принятия частного результата ретроспективного исследования, значения численного параметра (качественного проявления) дуги геохронотрека;

Q_α - априорное значение вероятности-дополнения до единицы уровня вероятности доверительного принятия значения численного параметра (качественного проявления) той или иной дуги трека, то есть

$$Q_\alpha = 1 - P_\alpha ; \quad (2)$$

Q_β - априорное значение вероятности дополнений до единицы уровня вероятности доверительного отклонения (несоответствия, непризнания истинности) значения численного параметра той или иной дуги трека, то есть

$$Q_\beta = 1 - P_\beta ; \quad (3)$$

Наличие заданных параметров ретроспективного исследования (2) и (3) на базе геохронотрекинга согласно [13] определяет т.н. разрешающий коэффициент D, равный отношению значений дополнений до единицы уровня вероятности доверительного принятия наблюдаемого значения в исследовании к уровню вероятности отклонения:

$$D = Q_\beta / Q_\alpha = (1 - P_\beta) / (1 - P_\alpha) ; \quad (4)$$

N - общее (суммарное) число единичных испытаний (объем учитываемых перемещений объектов или артефактов в составе геохронотрека);

n - учитываемое, апостериорное число фактов корректной реализации единичных испытаний (т.е. учитываемых перемещений объектов, артефактов и пр.) и успешного принятия наблюдаемого значения, результата каждого единичного испытания;

r - учитываемое, апостериорное число фактов отклонения, в силу различных причин, наблюдаемого значения, результата каждого единичного испытания т.е. из числа учитываемых перемещений объектов, артефактов и пр.;

При этом, очевидно, что в каждый конкретный момент учета данных в составе геохронотрека верно соотношение

$$N = n + r ; \quad (5)$$

C - предельное (максимально допустимое, пороговое) суммарное учитываемое число фактов отклонений, в силу различных причин, результата каждого единичного перемещения, учитываемого в процессе ретроспективного исследования;

α - априорное (директивно заданное, исходное для ретроспективного исследования) значение риска некорректного принятия наблюдаемого значения, результата геохронотрекинга;

α_1 - апостериорное (фиксируемое в ходе исследования) значение риска некорректного принятия результата геохронотрекинга;

β - априорное (директивно заданное, исходное для ретроспективного исследования) значение риска некорректного отклонения при необходимости принятия наблюдаемого значения;

β_1- апостериорное (фиксируемое в ходе эксперимента) значение риска некорректного отклонения при необходимости принятия результата геохронотрекинга;

P_3 - заданная в нормативных (априорная для всей гаммы исследований) документах требуемая доверительная вероятность обеспечения надежности результатов ретроспективного исследования на базе геохронотрекинга.

Исходными априорными данными для определения релевантного объема испытаний N (т.е. объема учитываемых перемещений объектов или артефактов в составе геохронотрека) с целью подтверждения вероятностных показателей надежности выводов ретроспективного исследования, их составляющих параметров являются:

– значения априорных уровней вероятности доверительных принятия P_α и отклонения P_β наблюдаемых значений численного параметра (качественного проявления) той или иной дуги геохронотрека, которые определяют собой разрешающий коэффициент *D*.

– априорные значения рисков некорректного принятия значений, результатов ретроспективного исследования α и некорректного отклонения при необходимости принятия значения или качественных результатов указанного исследования β.

В общем случае методика определения необходимого и достаточного (релевантного) числа разовых испытаний (учитываемых перемещений объектов или артефактов) в ходе ретроспективных исследований на базе геохронотрекинга для обеспечения требуемого уровня доверия к итоговым результатам включает три основных (обобщенных) этапа:

– подготовка исходных данных для расчета необходимого и достаточного числа единичных испытаний в ходе геохронотрекинга ретроспективного исследования;

– расчет и оценка доверительного интервала для принятия наблюдаемого значения, результата каждого единичного испытания (перемещения) при назначенных (априорных) значениях риска (или доверительной вероятности);

– принятие итогового исследовательского решения по релевантному числу (объему) единичных испытаний.

Последовательное описание каждого из указанных этапов позволяет раскрыть содержание предлагаемой методики в целом.

I). Подготовка и подбор исходных данных для определения объема испытаний необходимо осуществлять в следующей последовательности:

на основании анализа ранее полученного опыта экспериментирования с аппаратом геохронологического трекинга, а также исходя из объективной ограниченности ресурсов ретроспективных исследований априорно устанавливаются значения вероятности доверительного принятия P_α и доверительного отклонения (несоответствия, непризнания истинности) P_β наблюдаемого значения параметров анализируемого или синтезируемого геохронотрека;

априорно устанавливаются значения рисков некорректного принятия значения, результата ретроспективного исследования α и некорректного отклонения при необходимости принятия значения β. Значения указанных уровней P_α и P_β изначально устанавливаются, исходя из предельных возможностей накопления пространственно-временной информации о перемещениях объектов, учитываемых в процессе геохронотрекинга. Рекомендуется P_α и P_β устанавливать таким образом, чтобы значение P_3 находилось в интервале $\left[(P_\beta + P_\alpha)/2, P_\alpha\right]$ ближе к априорному уровню P_α вероятности доверительного принятия наблюдаемого значения параметра (качественного проявления) геохронотрека. Уровни допускается устанавливать двумя равнозначными способами: (P_α и P_β) или (P_α и *D*). При втором способе значение разрешающего коэффициента *D* рекомендуется выбирать из ряда: 1,5; 1,75; 2,0; 3,0.

значения рисков α и β устанавливаются следующим образом: Значение риска некорректного отклонения при необходимости принятия наблюдаемого значения β устанавливается субъективно, применительно к особенностям реализуемой архитектуры геохронотрека, в соответствии с принятыми нормативами или стандартами предметной области будущего применения результатов ретроспективного исследования. Традиционно значение риска некорректного принятия наблюдаемого значения, результата испытания α априорно устанавливают по субъективному усмотрению, равным значению β или больше него. В настоящей методике, на основании принципа равной вероятности несмещенных статистических ошибок, принято

$$\alpha = \beta \tag{6}$$

На основании (6) далее приняты (приведены ниже в таблицах 1 и 2) значения рисков α и β равными. Значения рисков в соответствии с [14] рекомендуется выбирать из ряда: 0,05; 0,1; 0,2; 0,3.

Согласно [14] не рекомендуется устанавливать исходные данные, сочетающие большие значения разрешающего коэффициента D с малыми значениями рисков α и β. Такие исходные данные следует изменять путем уменьшения значения разрешающего коэффициента D и увеличения значений рисков α и β. Соответственно, рекомендуемые соотношения исходных данных для определения объема испытаний (т.е. объема учитываемых перемещений объектов или артефактов в составе геохронотрека) приведены в таблице 1.

II). Расчет и оценка доверительного интервала для принятия значений, результатов каждого единичного перемещения при назначенных (априорных) значениях риска (или доверительной вероятности) необходимо осуществлять в следующей последовательности:

В силу несмещенного характера оценки P_α относительно значения P_3, в качестве точечной оценки для апостериорной доверительной вероятности истинности частного результата ретроспективного исследования, значения параметра (качественного проявления) геохронотрека принимается частота P, определяемая как

$$P = n / N; \tag{7}$$

Таблица 1

Рекомендуемые соотношения исходных данных для анализа геохронотрека

№ п/п	D	P_α	$\alpha = \beta$
	1,50-1,75	0,9995	0,05
		0,9990	0,10
		0,9950	0,20
	1,75-2,00	От 0,99 до 0,90 с шагом 0,01	0,10
			0,20
			0,30
	2,00-2,50	0,8500	0,20
			0,30
	3,00	0,8000	0,20

Объем единичных испытаний (т.е. объем учитываемых перемещений объектов или артефактов в составе геохронотрека) N для подтверждения выводов ретроспективного исследования является параметром, определяющим размер доверительного интервала I для вероятности P, т.е. задача расчета N достаточного для подтверждения априорно требуемой надежности оценки истинности частного результата ретроспективного исследования, значения численного параметра (качественного проявления) геохронотрека сводится к типовой математической задаче построения доверительного интервала и оценки надежности некоторой вероятности по частоте события, наблюдаемого в процессе итеративного ретроспективного исследования. Детализированное математическое решение данной задачи приведено в [6, 12, 14].

В общем виде, при N испытаниях доверительный интервал I, в который с доверительной вероятностью 1- α (при $\alpha = \beta$) попадет несмещенная оценка истинности частного результата ретроспективного исследования, значения параметра (качественного проявления) геохронологического трека определяется из сводного соотношения:

$$I = \frac{P + \frac{D}{2N} \pm D\sqrt{P\frac{1-P}{N} + \frac{D^2}{4N^2}}}{1 + \frac{D^2}{N}} \tag{8}$$

Указанные соотношения (7) и (8) позволили в рамках данной частной методики алгоритмически связать общее (суммарное) число единичных перемещений объектов (общий объем единичных испытаний) N и предельное (максимально допустимое, пороговое) суммарное учитываемое число фактов отклонения, в силу различных причин, анализируемого значения, результата каждого единичного испытания-перемещения, наблюдаемых в процессе геохронотрекинга C с исходными данными, описанными в таблице 1. Принимая значение уровня вероятности P_α доверительного принятия наблюдаемого значения параметра (качественного проявления) геохронотрека за априорно соответствующее целям подтверждения уровня требуемой доверительной вероятности обеспечения надежности результатов в комплексном ретроспективного исследовании P_3, заданного для всей гаммы исследований, определены соотношения выше указанных значений испытаний для подтверждения искомых характеристик геохронотрекинга. Некоторые результаты этого определения приведены в таблице 2.

III). Принятие исследовательского решения по релевантному числу (объему) единичных испытаний - учитываемых перемещений объектов (артефактов) в геохронотреке, осуществляется путем выполнения следующих логических шагов:

На основании трактовки существа дуг геохронотрека и накопительного характера учета единичных перемещений производится определение и предметная интерпретация исходных данных для определения релевантного объема учитываемых перемещений. При этом рекомендуется придерживаться соотношений исходных данных, представленных в таблице 1.

По выбранным параметрам исходных данных осуществляется вход в таблицу 2 настоящей методики, из которой становится возможным определить общее (суммарное) число единичных испытаний (объем учитываемых перемещений объектов (артефактов) в геохронотреке) N и предельное (максимально допустимое, пороговое) суммарное учитываемое число фактов отклонения, в силу различных причин, результата каждого единичного испытания, наблюдаемых в процессе ретроспективных исследований C, недостижение которого в процессе реализации всего объема единичных испытаний означает факт принятия альтернативы А.) (наблюдаемое и осредненное по N единичным актам испытаний-перемещений значение параметра (качественного проявления) геохронотрека принимается истинным с доверительной вероятностью P); а достижение или превышение текущего значения C над табулированным значением означает факт принятия альтернативного исследовательского решения Б.) (наблюдаемое и осредненное по N единичным актам испытаний-перемещений значение параметра (качественного проявления) геохронотрека не принимается истинным).

Для многоэтапных ретроспективных исследований оценка уровня доверия к апостериорным значениям параметров геохронотреков проводится применительно для каждого этапа такого исследования. Далее сводная оцененная доверительная вероятность к результатам многоэтапного ретроспективного исследования, соотносимая с априорной для всей гаммы исследований, т.е. требуемой, доверительной вероятностью обеспечения надежности результатов в серии однотипных этапов-испытаний комплексного исследования P_3, рассчитывается согласно формулам условной и полной вероятностей. Существо задачи указанного расчета детально раскрыто в работах [15, 16].

Таблица 2

Значения объема учитываемых перемещений объектов (артефактов) в геохронотреке с обеспечиваемой доверительной вероятностью результатов ретроспективных исследований

P_α	D	$\alpha=\beta=5\%$		$\alpha=\beta=10\%$		$\alpha=\beta=20\%$		$\alpha=\beta=30\%$	
		N	c	N	c	N	c	N	c
0,9	1,5	474	58	288	35	134	16	53	6
	1,75	227	30	138	18	64	8	27	3
	2	135	19	86	12	39	5	18	2
	3	41	7	23	4	14	2	8	1
0,85	1,5	294	54	181	33	79	14	35	6
	1,75	141	28	87	17	42	8	18	3
	2	85	18	53	11	21	4	12	2
	3	26	7	16	4	9	2	5	1
0,8	1,5	204	50	127	31	55	13	26	6
	1,75	98	26	61	16	28	7	13	3
	2	60	17	36	10	19	5	9	2
	3	17	6	9	3	4	1	4	1

Решение задачи достижения необходимой статистической значимости (устойчивости) результатов ретроспективного исследования на основе геохронологического трекинга заключается в обеспечении достаточности учтенных исходных данных о перемещениях исследуемых объектов при построении соответствующего геохронотрека. При решении указанной задачи введена понятная и традиционная мера указанной значимости (устойчивости) результатов ретроспективного исследования в виде доверительной вероятности. Для различных градаций указанной вероятности и уровня риска в её принятии определен объем (релевантное количество) учитываемых перемещений объектов или артефактов в составе геохронотрека, рассматриваемый как суммарное число единичных испытаний, которое должно быть обеспечено при синтезе соответствующего указанного трека. При непревышении выявленного соотношения указанного объема и числа фактов отклонений тех или иных единичных перемещений, гипотеза ретроспективного исследования принимается с искомой доверительной вероятностью.

Граничные условия для полученного решения задачи достижения статистической устойчивости результатов ретроспективного исследования на основе геохронологического трекинга определены как границы применимости приложений теории вероятности и математической статистики.

Дальнейшие направления совершенствования методики определения необходимого и достаточного (релевантного) числа разовых испытаний в ходе ретроспективных исследований на основе геохронотрекинга для обеспечения требуемого уровня доверия к результатам и выводам исследования связаны с её алгоритмизацией и автоматизацией, интеграцией в состав современных геоинформационных систем, ориентированных на прикладные исследования и решение пространственно-временных, аналитических задач в смежных областях [18-22].

Таким образом, приведенный вариант методики решения задачи достижения статистической устойчивости результатов ретроспективного исследования на основе геохронологического трекинга позволяет обеспечить и значительно расширить применимость научно-методического аппарата геохронологического трекинга на новые классы приложений. В свою очередь, данный факт позволяет расширить применимость математического аппарата проверки гипотез ретроспективных исследований на основе геохронологического трекинга для различных предметных областей и новых объектов изучения, добиться более эффективной его интеграции в соответствующие программные приложения для геоинформационных систем.

Разработка математико-статистического аппарата и методики определения необходимого и достаточного (релевантного) числа разовых испытаний в ходе ретроспективных исследований на базе геохронотрекинга позволит развить соответствующий научно-методический инструментарий и вытекающие из него информационные технологии ретроспективных и исторических геопространственных исследований в интересах инженерии, логистики, а также гуманитарных наук. Также очевидна перспективность работ по развитию прикладной алгоритмики геохронотрекинга, как такового. К указанным работам следует отнести внедрение и интеграцию соответствующих информационных технологий искусственной интеллектуальности, интеграции и слияния информации, виртуализации и пр. в соответствующие геоинформационные приложения.

Работа выполнена при поддержке РФФИ (проект №19-07-00006).

СПИСОК ЛИТЕРАТУРЫ

1. Ивакин Я. А. Рациональный алгоритм проверки гипотез ретроспективных исследований использования водного транспорта на базе геохронологического трекинга/ Я. А. Ивакин, С. Н. Потапычев, Р. Я. Ивакин // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. — 2019. — Т. 11. — No 3. — С.448–460. DOI: 10.21821/2309-5180-2019-11-3-448-460.
2. Потапычев, С.Н. Геохронологический трекинг – специализированный ГИС-инструментарий исторического исследования [Текст] // Ивакин Я.А., Потапычев С.Н. – Журнал «Историческая информатика. Информационные технологии и математические методы в исторических исследованиях и образовании», № 1-2 -2016; с. 3-11.
3. Ивакин Я. А. Информационная технология геохронологического трекинга для проверки гипотез ретроспективных исследований использования водного транспорта / Я. А. Ивакин, С. В. Потапычев //Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. — 2018. — Т. 10. — № 2. — С. 452–461. DOI: 10.21821/2309-5180-2018-10-2-452-461.
4. Ивакин Р.Я., Ивакин Я.А., Потапычев С.Н. Оптимизированный алгоритм статистической проверки гипотез ретроспективных исследований на основе геохронологического трекинга// Труды учебных заведений связи. 2020. Т. 6. No1. С. 86–93. DOI:10.31854/1813-324X-2020-6-1-86-93
5. Ивакин Я. А., Потапычев С. Н. Информационная технология исследований особенностей применения изделий гидроакустической техники на основе геохронологического трекинга // Информационные технологии и телекоммуникации. 2020. Том 8. No 2. С. 109–119. DOI 10.31854/2307-1303-2020-8-2-109-119.
6. M.Codescu, G.Horsinka, O.Kutz, T.Mossakowski, R.Rau DO-ROAM: Activity-Oriented Searh and Transport Navigation with OpenStreetMap / GeoSpatial Semantics // Proceedings of the 6th International Conference, GeoS 2015. — 2015. —Pp. 88-108.
7. Sigma Knowledge Engineering Environment [Электронный ресурс] - электронные данные, – режим доступа URL: http://sigmakee.sourceforge.net. Дата доступа: январь 2020г.
8. Советов, Б. Я. Моделирование систем / Б. Я. Советов, С. А. Яковлев. — 7-е изд. — Москва: Издательство Юрайт, 2019. — 343 с.
9. Юсупов Р.М., Заболотский В.П. Концептуальные и научно-методологические основы информатизации. - СПб.: Наука, 2009. - 541 с.
10. Советов, Б. Я. Информационные технологии / Б. Я. Советов, В.В.Цехановский. — 6-е изд., перераб. — Москва: Издательство Юрайт, 2016. — 263 с.
11. Шмид А.В. Революция в области философии и технологиях принятия корпоративных решений [Электронный ресурс] URL: http://4cio.activetextbook.com/active_textbooks/34#page642
12. Хлебенских, Л. В. Автоматизация производства в современном мире / Л. В. Хлебенских, М. А. Зубкова, Т. Ю. Саукова. — Текст: непосредственный // Молодой ученый. — 2017. — № 16 (150). — С. 308-311. — URL: https://moluch.ru/archive/150/42390/
13. Steve McConnel. Code Complete: A Practical Handdook of Software Construction – NewYork, MicrosoftPress, 2004. – 889p.
14. Фаулер, Мартин, Бек, Кент, Брант, Джон, Опдайк, Уильям, Робертс, Дон. Рефакторинг: улучшение проекта. — Спб: «Диалектика», 2019. — 448 с. — ISBN 978-5-9909445-1-0.
15. Макконнелл С. Совершенный код. Мастер-класс / Пер. с англ. — М.: Издательство «Русская редакция», 2010 — 896 стр.: ил.
16. Steve McConnel. Software Estimation: Demystifying the Black Art (Developer Best Practices) – NewYork, MicrosoftPress, 2006. – 610p.
17. ГОСТ Р 27.403-2009. Планы испытаний для контроля вероятности безотказной работы [Электронный ресурс] - http://docs.cntd.ru/document/1200078695 ; Дата публикации – 15.02.2021г.
18. Шатохин А.В. Информационно-сопроводительная сеть – новый подход к эксплуатации гидроакустического вооружения // Национальная оборона. – 2020. -№ 1(82). – с. 62 – 67.
19. Коротков А. В., Кристальный Б. В., Курносов И. Н. Государственная политика Российской Федерации в области развития информационного общества. — М.: ООО «Трейн», 2007. ISBN 978-5-903652-01-3. — 472 с.
20. Потапычев С.Н., Ивакин Я.А. Использование геопространственных данных для интеллектуальной поддержки принятия диспетчерских решений // Вестник СПбГУТиД. Серия 1. Естественные и технические науки. – 2018.- №2 – С.24-32.
21. Шатохин А.В., Ивакин Я.А., Нештенко В.С. Координирование услуг предприятий морского приборостроения в интересах системы эксплуатации гидроакустического вооружения ВМФ // Морской сборник – 2020, - №11 – с. 12-54
22. Шатохин А.В., Ивакин Я.А. Современный подход к участию предприятий морского приборостроения в поддержании технической готовности гидроакустического вооружения ВМФ // Морская радиоэлектроника – 2020, - № 4 (21) – с. 56 -67.

УДК 004.056.5

КРИТЕРИИ ОЦЕНКИ ДОСТУПНОСТИ ИНФОРМАЦИОННЫХ, ТЕЛЕКОММУНИКАЦИОННЫХ И ДРУГИХ КРИТИЧЕСКИ ВАЖНЫХ РЕСУРСОВ В ИНТЕРЕСАХ АНАЛИЗА ИХ ЗАЩИЩЕННОСТИ

Котенко Игорь Витальевич, Саенко Игорь Борисович, Паращук Игорь Борисович
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: ivkote@comsec.spb.ru, ibsaen@comsec.spb.ru, shchuk@rambler.ru

Аннотация. Рассмотрены состав и физическая сущность множества показателей доступности авторизированных пользователей и администраторов сложной управляемой критически важной инфраструктуры к защищаемым информационным, телекоммуникационным и другим ресурсам. Элементы этого множества характеризуют одну из граней безопасности – пространство параметров защищенности инфраструктур такого класса с точки зрения доступности ресурсов. Предложены частные критерии оценивания временной и топологической доступности. Обобщенный вероятностный критерий оценивания доступности авторизированных пользователей и администраторов сложной управляемой критически важной инфраструктуры к защищаемым информационным, телекоммуникационным и другим ресурсам предложено формулировать в виде совместной условной вероятности выполнения требований по временной и топологической доступности.

Ключевые слова: критически важный ресурс; инфраструктура; показатель; доступность; критерий; анализ; защищенность.

CRITERIA FOR ASSESSING THE AVAILABILITY OF INFORMATION, TELECOMMUNICATIONS AND OTHER CRITICAL RESOURCES FOR THE ANALYSIS OF THEIR SECURITY

Kotenko Igor, Saenko Igor, Parashchuk Igor
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: ivkote@comsec.spb.ru, ibsaen@comsec.spb.ru, shchuk@rambler.ru

Abstract. The composition and physical nature of a set of indicators of the availability of authorized users and administrators of a complex managed critical infrastructure to protected information, telecommunications and other resources are considered. The elements of this set characterize one of the security facets – the space of security parameters of infrastructures of this class in terms of resource availability. Particular criteria for evaluating temporal and topological availability are proposed. The generalized probabilistic criterion for assessing the availability of authorized users and administrators of complex managed critical infrastructure to protected information, telecommunications and other resources is proposed to be formulated in the form of a joint conditional probability of meeting the requirements for temporary and topological availability.

Keywords: critical resource; infrastructure; indicator; availability; criterion; analysis; security.

Введение. В современных условиях все больший интерес у аналитиков и практиков вызывает проблема мониторинга и аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности в интересах оценки состояния, поддержки принятия решений и расследования компьютерных инцидентов в критически важных инфраструктурах [1].

В частности, много современных работ посвящены вопросам разработки научно-методического обеспечения для построения и функционирования систем аналитической обработки больших массивов гетерогенных данных в интересах оценки состояния, поддержки принятия решений и расследования инцидентов для обеспечения кибербезопасности критически важных инфраструктур. Эти работы, в большинстве своем, нацелены на повышение эффективности ключевых информационных процессов, подлежащих реализации на прикладном уровне функционирования современных и перспективных систем мониторинга и управления безопасностью различных критически важных инфраструктур, в том числе в энергетике, в управлении транспортом, в нефтегазовой отрасли, в автоматизированном промышленном производстве, в системах управления городским хозяйством, в науке, в различных отраслях обеспечения обороноспособности, правопорядка и в Российской Федерации в целом.

Современные и перспективные критически важные инфраструктуры используют для своего построения, как правило, ресурсы глобальных компьютерных сетей общего пользования, что обуславливает широкий диапазон потенциальных угроз их кибербезопасности. Одной из ключевых задач при этом выступает задача разработки моделей, методов, алгоритмов и программных средств оперативной оценки защищенности информационных, телекоммуникационных и других критически важных ресурсов на основе аналитической обработки больших массивов гетерогенных данных.

Понятие информационных, телекоммуникационных и других критически важных ресурсов, в общем случае, может включать в себя любой класс средств, доступ к которым может нанести ущерб кибербезопасности критически важных инфраструктур. Рассматривая современную ситуацию, к таковым классам средств могут относиться дата-

центры, узлы телекоммуникационных сети, серверы, а также исполняемые файлы, Web-сайты или их отдельные страницы, электронные почтовые сообщения и т.д.

Поэтому вопросы оперативной оценки защищенности информационных, телекоммуникационных и других критически важных ресурсов продолжают оставаться актуальными. Эти вопросы могут быть решены, например, на основе использования моделей и методов параллельных вычислений [2, 3].

Иногда могут быть использованы методы нейросетевого моделирования, нечеткой классификации и кластеризации, нечеткой оптимизации и нечеткого логического вывода [4, 5].

Вместе с тем, важнейшим вопросом остается обеспечение защищенности при доступе пользователей к ресурсам системы [6, 7]. Главным, основополагающим этапом при разработке научно-методического инструментария для оперативной оценки защищенности информационных, телекоммуникационных и других критически важных ресурсов, важной стадией аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности, является этап формулировки показателей и критериев оценки защищенности.

При этом под защищенностью следует понимать поддержание на заданном уровне тех параметров предоставляемых для критической инфраструктуры ресурсов, которые характеризуют установленный безопасный статус их хранения, обработки и использования. Это свойство системы (инфраструктуры) обеспечивать состояние безопасности своих критически важных ресурсов с учетом внутренних или внешних угроз. Это свойство, характеризующее:

– доступность авторизованных пользователей и администраторов системы к защищаемым критически важным ресурсам (временная доступность – своевременность и топологическая доступность) – как гарантию того, что авторизованные пользователи и администраторы всегда получат доступ к этим критически важным ресурсам;

– целостность критически важных ресурсов (их достоверность) – как гарантию их сохранности (сохранения их правильных объемов и значений), которая обеспечивается запретом для неавторизованных пользователей и администраторов системы каким-либо образом изменять, модифицировать, разрушать, создавать критически важные ресурсы;

– конфиденциальность критически важных ресурсов – как гарантию того, что данные ресурсы будут доступны только тем пользователям и администраторам системы, которым этот доступ разрешен. Именно такие пользователи и администраторы критически важных инфраструктур называются авторизованными.

Процесс оценивания (анализа) защищенности критически важных ресурсов – процесс принятия решения о состоянии (уровне) защищенности этих ресурсов, процедура получения качественных и количественных оценок состояния (уровня) защищенности либо оценочных значений показателей защищенности.

При этом показателем защищенности (единичным) называют числовую (шкалированную) величину, характеризующую степень соответствия конкретного аспекта (отдельной стороны, грани) свойства защищенности предъявляемым к данному аспекту требованиям. Показатель защищенности есть функционал от параметров, характеризующих данное свойство, и вводимый для снижения размерности пространства параметров безопасности в интересах удобства сравнения нескольких систем, критических ресурсов этих систем (объектов, процессов) с точки зрения их защищенности от внутренних или внешних угроз.

Показателем защищенности (векторным) будем называть вектор, компоненты которого суть показатели защищенности отдельных объектов (процессов), составляющих критически важные ресурсы и представляющих собой частные, единичные показатели их защищенности.

Критерий – руководящее правило (условие или совокупность условий), мерило оценки (суждения о) защищенности критически важных ресурсов.

В рамках аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности необходимо определить состав векторов показателей защищенности и критерии оценки защищенности критически важных ресурсов, сформулировать их физическую сущность и определить способы их измерений и вычислений.

Например, в составе комплексного векторного показателя защищенности критически важных ресурсов важную роль играет вектор показателей доступности $\vec{Q}_{\text{дост}}(\tau)$ авторизованных пользователей и администраторов системы к этим защищаемым ресурсам, а входящие в него показатели защищенности (с точки зрения доступности ресурсов) призваны количественно описывать способность: предоставлять пользователям и администраторам системы услуги безопасного доступа к защищаемым информационным, телекоммуникационным и другим критически важным ресурсам тогда, когда это им необходимо; в необходимом пользователям и администраторам системы месте; и в течение требуемого времени (продолжительность предоставления доступа к критически важным ресурсам) с требуемым качеством (достоверность и целостность предоставляемых критически важных ресурсов). Иными словами, вектор показателей доступности авторизированных пользователей и администраторов системы к защищаемым информационным, телекоммуникационным и другим критически важным ресурсам $\vec{Q}_{\text{дост}}(\tau)$ на τ-ом временном отрезке функционирования системы имеет две составляющие – временную (когда, своевременность) и топологическую (где).

Временная доступность (своевременность) к критически важным ресурсам рассматривается как способность системы обеспечивать доступ авторизированных пользователей и администраторов к этим защищаемым ресурсам и предоставление им требуемого перечня безопасных информационных, телекоммуникационных и других критически важных ресурсов в установленные сроки.

Показатель защищенности (с точки зрения своевременности) доступа авторизированных пользователей и администраторов к защищаемому ресурсу – к требуемому *n*-ому (из перечня возможных $N^{усл}_{реал}(\tau)$) информационному, телекоммуникационному или другому критически важному ресурсу, может быть выражен через время ожидания доступа к *n*-ому ресурсу $t^{n}_{ож}(\tau)$ на *τ*-ом временном отрезке функционирования системы. Аналитическое выражение для определения значения показателя защищенности, характеризующего свойство временной доступности доступа авторизированных пользователей и администраторов к защищаемому ресурсу, имеет вид [8]:

$$t^{n}_{ож}(\tau) = (t^{n}_{прд\ запр}(\tau) + t^{n}_{обр\ запр}(\tau) + t^{n}_{реал\ запр}(\tau)), \quad (1)$$

где $t^{n}_{прд\ запр}(\tau)$ – время, затрачиваемое пользователем и администратором на формирование и передачу запроса на предоставление *n*-ого информационного, телекоммуникационного или другого критически важного ресурса на *τ*-ом временном отрезке функционирования системы, $t^{n}_{обр\ запр}(\tau)$ – время, затрачиваемое на проверку полномочий терминала системы, откуда пришел запрос, на проверку пользователя и администратора (аутентификация, идентификация, полномочия, приоритетность) и на иные обязательные мероприятия по обработке запроса на предоставление *n*-ого информационного, телекоммуникационного или другого критически важного ресурса на *τ*-ом временном отрезке функционирования системы, $t^{n}_{реал\ запр}(\tau)$ – время, затрачиваемое на обеспечение безопасной реализации запроса на предоставление *n*-ого ресурса или на передачу сигнала пользователю и администратору о невозможности предоставления этого вида информационного, телекоммуникационного или другого критически важного ресурса на *τ*-ом временном отрезке функционирования системы.

С учетом многообразия угроз безопасности $U^{усл}_{реал}(\tau)$ для информационного, телекоммуникационного или другого критически важного ресурса из множества ресурсов $N^{усл}_{реал}(\tau)$, своевременность доступа авторизированных пользователей и администраторов можно охарактеризовать средним временем их доступа к защищаемому ресурсу $\bar{t}^{усл/угр}_{дост}(\tau)$, интегральным (по всему перечню ресурсов и соответствующих им угроз) показателем, имеющим вид:

$$\bar{t}^{усл/угр}_{дост}(\tau) = \sum_{n=1}^{N^{усл}_{реал}(\tau)} \sum_{u=1}^{U^{угр}_{реал}(\tau)} \alpha_{ип}\ P_{бп}(\tau)\ t^{n}_{ож}(\tau) + t^{n}_{пред\ рес}(\tau), \quad (2)$$

где $\alpha_{ип}$ – относительная опасность (сложность преодоления) *и*-ой угрозы при предоставлении *n*-ого ресурса на *τ*-ом временном интервале функционирования системы, причем, $\Sigma\, \alpha_{ип}=1$; $P_{бп}(\tau)$ – вероятность безотказного предоставления критически важного ресурса в условиях воздействия угроз на *τ*-ом временном интервале функционирования системы; $t^{n}_{пред\ рес}(\tau)$ – среднее время предоставления *n*-ого ресурса.

Кроме того, временная доступность авторизированных пользователей и администраторов системы может количественно характеризоваться интенсивностью отказов в доступе $\lambda_{отк\ дост}(\tau)$ к информационному, телекоммуникационному или другому критически важному ресурсу, вызванных сбоями (ошибками) при реализации процесса предоставления этих ресурсов, а также средним временем межу отказами в доступе $\bar{t}_{отк\ дост}(\tau)$. Так, например, интенсивность отказов в доступе к защищаемому ресурсу может определяться как отношение количества полученных авторизированными пользователями и администраторами системы отказов в доступе к общему числу запросов на доступ к защищаемому информационному, телекоммуникационному или другому критически важному ресурсу

$$\lambda_{отк\ дост}(\tau) = \frac{N_{отк\ дост}(\tau)}{N_{запр\ дост}(\tau)}. \quad (3)$$

Таким образом, векторный показатель защищенности $\vec{Q}_{врем\ дост}(\tau)$, характеризующий временную доступность авторизированных пользователей и администраторов системы к защищаемому информационному, телекоммуникационному или другому критически важному ресурсу, содержит следующие показатели (параметры) [8]:

$$\vec{Q}_{врем\ дост}(\tau) = (\bar{t}^{усл/угр}_{дост}(\tau); \bar{t}^{усл/угр}_{ож}(\tau); \lambda_{отк\ дост}(\tau); \bar{t}_{отк\ дост}(\tau))^{T}. \quad (4)$$

Помимо обеспечения ресурсами за необходимое время, авторизированным пользователям и администраторам системы должна быть обеспечена топологическая доступность к защищаемому информационному, телекоммуникационному или другому критически важному ресурсу, т.е. доступ к защищенным ресурсам в необходимом пользователю месте. При этом топологическая доступность зависит от множества каналов и средств, задействованных в обеспечении пользователей информационным, телекоммуникационным или иным критически важным ресурсом.

Например, для обеспечения топологической доступности к защищаемому информационному ресурсу, предоставляемому пользователям по каналам и трактам сетей беспроводного абонентского доступа (СБАД), важны: радиус контролируемой зоны; радиус зоны охвата точки доступа СБАД; удаленность пользователя; флуктуации параметров радиосигналов СБАД, вызванные многолучевостью; уровень потерь при распространении сигналов по кабелю и при распространении радиоволн с учетом неровностей земли и препятствий и др.

Для нашего конкретного примера, показатели защищенности, составляющие содержание вектора показателей топологической доступности $\vec{Q}_{\text{топ дост}}(\tau)$, количественно характеризуют способность не препятствовать доступу авторизированных пользователей к защищаемому информационному ресурсу и не затруднять предоставление им требуемого перечня этих ресурсов (услуг) в установленном месте их нахождения и при перемещении пользователя:

$$\vec{Q}_{\text{топ дост}}(\tau) = (R_{\text{з}}(\tau); L_{\text{удал}}(\tau); \eta_{\text{м}}(\tau))^{\text{т}}, \quad (5)$$

где $R_{\text{з}}(\tau)$ – радиус зоны, в пределах которого пользователь СБАД может иметь безопасный доступ к информационному ресурсу с заданным качеством; $L_{\text{удал}}(\tau)$ – удаление пользователя (терминала) от центрального сервера (либо точки беспроводного доступа) СБАД; $\eta_{\text{м}}(\tau)$ – параметр, характеризующий интегральное влияние пересеченности местности на ослабление сигналов в линии связи между терминалом пользователя и точкой беспроводного доступа СБАД. Экспериментальные значения $\eta_{\text{м}}$ лежат в пределах 2…5, где $\eta_{\text{м}}$=2 соответствует распространению радиоволн в свободном пространстве. В условиях города и при низких высотах антенн точек беспроводного доступа СБАД величина $\eta_{\text{м}}$ достигает значения 5.

Таким образом, векторный показатель доступности авторизированных пользователей и администраторов системы к защищаемым информационным, телекоммуникационным и другим критически важным ресурсам $\vec{Q}_{\text{дост}}(\tau)$, характеризующий способность обеспечивать безопасный доступа к этим ресурсам тогда, когда это им необходимо и там, где это необходимо, включает:

$$\vec{Q}_{\text{дост}}(\tau) = (\vec{Q}_{\text{врем дост}}(\tau);\ \vec{Q}_{\text{топ дост}}(\tau)), \quad (6)$$

где $\vec{Q}_{\text{врем дост}}(\tau)$ – вектор показателей временной доступности, характеризующий способность системы не препятствовать доступу ее авторизированных пользователей и администраторов к защищаемым информационным, телекоммуникационным и другим критически важным ресурсам в установленные сроки (своевременность предоставления ресурсов) на τ-ом временном отрезке функционирования системы; $\vec{Q}_{\text{топ дост}}(\tau)$ – вектор показателей топологической доступности, характеризующий способность системы не препятствовать доступу ее авторизированных пользователей и администраторов к защищаемым информационным, телекоммуникационным и другим критически важным ресурсам в установленном месте их нахождения и при их перемещении.

Критерием временной доступности к защищаемым критически важным ресурсам может служить соотношение $\vec{Q}_{\text{врем дост}}(\tau) \geq \vec{Q}^{\text{тр}}_{\text{врем дост}}(\tau)$, где $\vec{Q}_{\text{врем дост}}(\tau)$ – показатель временной доступности на τ-ом временном отрезке функционирования системы, $\vec{Q}^{\text{тр}}_{\text{врем дост}}(\tau)$ – требуемое значение временной доступности (своевременности предоставления ресурсов), характеризующее время, отводимое на реализацию потребности авторизированных пользователей и администраторов в доступе к защищаемым информационным, телекоммуникационным и другим критически важным ресурсам на τ-ом временном отрезке функционирования системы. Критерий оценивания временной доступности может быть задан в вероятностно-временном виде, через вероятность обеспечения своевременного доступа $P_{\text{свр рес}}(\tau)$ пользователей и администраторов к защищаемым критически важным ресурсам

$$P_{\text{свр рес}}(\tau) = P(\vec{Q}_{\text{врем дост}}(\tau) \geq \vec{Q}^{\text{тр}}_{\text{врем дост}}(\tau)) = P(\bar{t}^{\,усл/уг}_{\text{дост}}(\tau) \leq \bar{t}^{\,усл/уг\ \text{тр}}_{\text{дост}}(\tau);\ t^{n}_{\text{ож}}(\tau) \leq t^{n\ \text{тр}}_{\text{ож}}(\tau)). \quad (7)$$

Критерий оценивания топологической доступности к защищаемым критически важным ресурсам также может быть задан в вероятностно-временном виде, как вероятность топологической доступности $P_{\text{тд рес}}(\tau)$ авторизированных пользователей и администраторов к защищаемым информационным, телекоммуникационным и другим критически важным ресурсам на τ-ом временном отрезке функционирования системы:

$$P_{\text{тд рес}}(\tau) = P(\vec{Q}_{\text{топ дост}}(\tau) \geq \vec{Q}^{\text{тр}}_{\text{топ дост}}(\tau)). \quad (8)$$

Вероятность топологической доступности пользователей к защищаемым критически важным ресурсам должна быть больше или равна требуемой $P_{\text{тд рес}}(\tau) \geq P^{\text{тр}}_{\text{тд рес}}(\tau)$, где $P^{\text{тр}}_{\text{тд рес}}(\tau)$ – требуемая вероятность топологической доступности авторизированных пользователей и администраторов к защищаемым информационным, телекоммуникационным и другим критически важным ресурсам на τ-ом временном отрезке функционирования системы.

С учетом того факта, что выполнение требований по временной и топологической доступности авторизированных пользователей и администраторов к защищаемым информационным, телекоммуникационным и другим критически важным ресурсам являются событиями совместными, обобщенный критерий оценивания доступности может быть задан в вероятностно-временном виде, через совместную условную вероятность обеспечения временной и топологической доступности:

$$P_{\text{дост рес}}(\tau) = P(\vec{Q}_{\text{врем дост}}(\tau) \geq \vec{Q}^{\text{тр}}_{\text{врем дост}}(\tau)) \times (\vec{Q}_{\text{топ дост}}(\tau) \geq \vec{Q}^{\text{тр}}_{\text{топ дост}}(\tau)) =$$

$$= P(\vec{Q}_{\text{врем дост}}(\tau) \geq \vec{Q}^{\text{тр}}_{\text{врем дост}}(\tau)) \times P(\vec{Q}_{\text{топ дост}}(\tau) \geq \vec{Q}^{\text{тр}}_{\text{топ дост}}(\tau)) / (\vec{Q}_{\text{врем дост}}(\tau) \geq \vec{Q}^{\text{тр}}_{\text{врем дост}}(\tau)) = \quad (9)$$

$$= P(\vec{Q}_{\text{топ дост}}(\tau) \geq \vec{Q}^{\text{тр}}_{\text{топ дост}}(\tau)) \times P(\vec{Q}_{\text{врем дост}}(\tau) \geq \vec{Q}^{\text{тр}}_{\text{врем дост}}(\tau)) / (\vec{Q}_{\text{топ дост}}(\tau) \geq \vec{Q}^{\text{тр}}_{\text{топ дост}}(\tau)).$$

Вероятность доступности авторизированных пользователей и администраторов к защищаемым информационным, телекоммуникационным и другим критически важным ресурсам должна быть больше или равна требуемой $P_{\text{дост рес}}(\tau) \geq P^{\text{тр}}_{\text{дост рес}}(\tau)$, где $P^{\text{тр}}_{\text{дост рес}}(\tau)$ – требуемая вероятность доступности к защищаемым критически важным ресурсам на τ-ом временном интервале функционирования системы.

Заключение. Таким образом, предложен состав и оговорена физическая сущность множества показателей доступности авторизированных пользователей и администраторов сложной управляемой критически важной инфраструктуры к защищаемым информационным, телекоммуникационным и другим ресурсам. Элементы этого множества характеризуют одну из множества граней безопасности – пространство параметров защищенности инфраструктур такого класса с точки зрения доступности ресурсов.

Рассмотрены частные критерии оценивания временной и топологической доступности. Обобщенный вероятностный критерий оценивания доступности авторизированных пользователей и администраторов сложной управляемой критически важной инфраструктуры к защищаемым информационным, телекоммуникационным и другим ресурсам предложено формулировать в виде совместной условной вероятности выполнения требований по временной и топологической доступности.

Использование предложенных показателей и критериев оценивания создает предпосылки для учета специфических особенностей предоставления ресурсов, а значит, для повышения достоверности комплексного анализа защищенности критически важных инфраструктур в различных условиях обстановки.

Исследования проводятся при поддержке гранта РНФ № 21-71-20078 в СПб ФИЦ РАН (СПИИРАН).

СПИСОК ЛИТЕРАТУРЫ

1. Уилсон Э. Мониторинг и анализ сетей. Методы выявления неисправностей. Пер. с англ. – М.: ЛОРИ, 2002. – 350 с.
2. Саенко И.Б., Кушнеревич А.Г., Котенко И.В. Реализация платформы распределенных параллельных вычислений для сбора и предварительной обработки больших данных мониторинга в киберфизических системах // Международный конгресс по информатике: информационные системы и технологии (CSI ST-2016). Материалы международного научного конгресса. Республика Беларусь, Минск, 24-27 октября 2016 г., С. 641-645.
3. Kotenko I., Fedorchenko A., Saenko I., Kushnerevich A. Parallelization of security event correlation based on accounting of event type links // Proceedings of the 25th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2018). Cambridge, UK, March 21-23, 2018. Los Alamitos, California. IEEE Computer Society. 2018. 462-469 pp.
4. Паращук И.Б., Бобрик И.П. Нечеткие множества в задачах анализа сетей связи. – СПб.: ВУС, 2001. – 80 с.
5. Паращук И.Б., Иванов Ю.Н., Романенко П.Г. Нейросетевые методы в задачах моделирования и анализа эффективности функционирования сетей связи. – СПб.: ВАС, 2010. – 103 с.
6. Авраменко В.С. Адаптивный контроль защищенности информации от несанкционированного доступа // Информация и космос. 2010. № 3. С. 116-119.
7. Михайличенко Н.В. Проблемы и перспективы обеспечения безопасности центров обработки данных // Региональная информатика и информационная безопасность. Выпуск 4. – СПб.: СПОИСУ, 2017. С. 137-138.
8. Паращук И.Б., Крюкова Е.С., Ясинский С.А. Временная и топологическая доступность пользователей к информационному ресурсу электронных библиотек: показатели и критерии оценивания в рамках системных исследований // Труды ЦНИИС. Санкт-Петербургский филиал. Научно-технический сборник статей. Т. 1. № 9. 2020. – 51 с. С. 8-16.

УДК 004.056

ОБЗОР СПОСОБОВ СКРЫТИЯ ИНФОРМАЦИИ В ФАЙЛАХ И ОБЪЕКТАХ ИГРОВЫХ СОХРАНЕНИЙ С УЧЕТОМ СОДЕРЖИМОГО С ПОМОЩЬЮ СТЕГАНОГРАФИИ

Куликов Илья Александрович, Ахрамеева Ксения Андреевна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: wyzzus@gmail.com, oklaba@mail.ru

Аннотация. В статье рассматриваются способы сохранения игровых данных, в которых скрыта информация с помощью стеганографии с учетом содержимого. Приводится обзор использования воспринимаемых человеком форматов данных, бинарных файлов, созданных при помощи бинарной (двоичной) сериализации и реляционных баз данных. Приводятся примеры подготовки и анализа игровых файлов перед началом стегоанализа содержимого файлов. Сравнивается эффективность противодействия определения структуры сохраняемого объекта при использовании форматов, воспринимаемых человеком и форматов, требующих предварительного приведения к виду, удобному для восприятия человеком.

Ключевые слова: стеганография; стеганография с учетом содержимого; компьютерные игры; бинарная сериализация.

OVERVIEW OF WAYS TO HIDE INFORMATION IN FILES AND OBJECTS OF GAME SAVINGS USING CONTENT AWARE STEGANOGRAPHY

Kulikov Ilya, Akhrameeva Ksenia
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: wyzzus@gmail.com, oklaba@mail.ru

Abstract. This article discusses ways to save game data that hide information using content-aware steganography. Provides an overview of the use of human-readable data formats, binary files created using binary (binary) serialization and relational databases. Examples of preparation and analysis of game files before the start of steganalysis of the file contents are given. The article compares the effectiveness of counteracting the determination of the structure of the stored object when using formats perceived by a person and formats that require preliminary reduction to a form that is convenient for human perception.

Keywords: steganography; content-aware steganography; computer games; binary serialization.

Введение. Файл игрового сохранения – это файл, в котором хранится информация об объекте, представляющим состояние игры и игровых данных во время сохранения игры. В нем могут содержаться данные об игровом прогрессе игрока, его позиции на игровой сцене, номер игровой сцены, на которой он находился в момент сохранения, в целом информация об объектах, которую разработчики игры посчитали необходимой для хранения в файле для воспроизведения того же состояния, когда игрок загрузит этот файл, чтобы продолжить игру.

При этом стеганография [1] с учетом содержимого (когда скрытое послание внедряется в семантический смысл игрового контента) [2] отлично подходит для внедрение скрытого сообщения в сохраняемые игровые данные, чтобы передать этот файл знающим лицам для извлечения скрытого сообщения, и чтобы посторонние не заметили скрытого сообщения. Примером такого использования может служить игра в жанре градостроительного симулятора, где информация о символе из скрытого сообщения кодируется первой координатой построенного на карте дома. Предполагается, что игрок, который решит внедрить скрытое сообщение в игровой файл, введет в игре текст скрытого сообщения, а игра выставит дома на игровой сцене в соответствие с введенным сообщением. Игроку лишь остается дополнить игровую сцену домами, чтобы сцена не выглядела подозрительно (если это потребуется), сохранить ее в файл и передать этот файл через внутреннюю систему обмена игры (торговая площадка, игровая библиотека и другие системы обмена пользовательским контентом). Для сохранения игровой сцены и последующего обмена применяются разные методы и форматы файлов и игровых объектов.

Воспринимаемые человеком форматы. Существует достаточное количество текстовых форматов обмена данными, которые легко читаются человеком. Среди них можно выделить такие популярные форматы, как JSON (JavaScript Object Notation), XML (eXtensible Markup Language), YAML (Yet Another Markup Language). Эти три формата отличаются синтаксисом, но в целом они преследуют одну и ту же цель – представить исходный объект простейшими типами: числами, строками, логическими переменными, массивами.

Как было сказано ранее, файл представляет состояние игры в момент сохранения. При этом состояние описано объектом, и этот объект можно перевести в один из описанных выше форматов данных. Вне зависимости от формата данных при анализе файла человеком понять структуру объекта сохранения будет не очень сложно, после можно приступить к стегоанализу на основе полученной структуры.

Бинарная сериализация. Бинарную сериализацию или двоичную сериализацию можно представить как процесс сохранения состояния объекта в среде хранения [3]. Во время этого процесса поля объекта, преобразуются в поток байтов, который затем записывается в поток данных. И этот поток данных можно записать в файл, который затем можно передать знающим лицам для извлечения скрытой информации.

Но, в отличие от JSON или XML, если открыть бинарный файл через текстовый редактор, то вместо четкой структуры с данными можно увидеть лишь последовательность байтов (рис. 1).

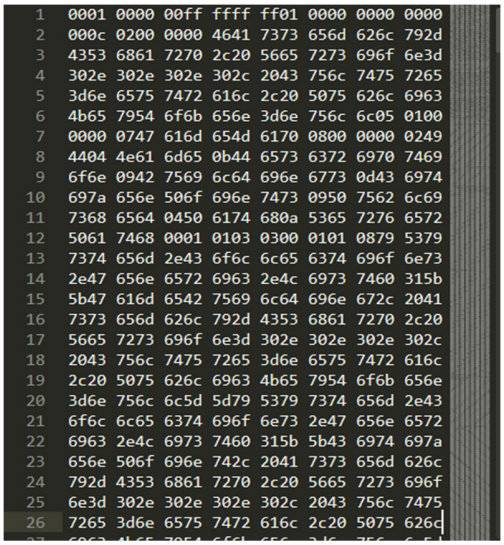


Рис. 1. Содержимое бинарного файла при открытии текстовым редактором Sublime Text 3.

Для того, чтобы понять структуру объекта, сохраненного в этом файле, потребуется провести анализ файла методом обратной разработки (reverse engineering). Подобные процедуры для неизвестных структур проводятся вручную специальными инструментами, типа Hex-редактора Synalyze It! (рис. 2).

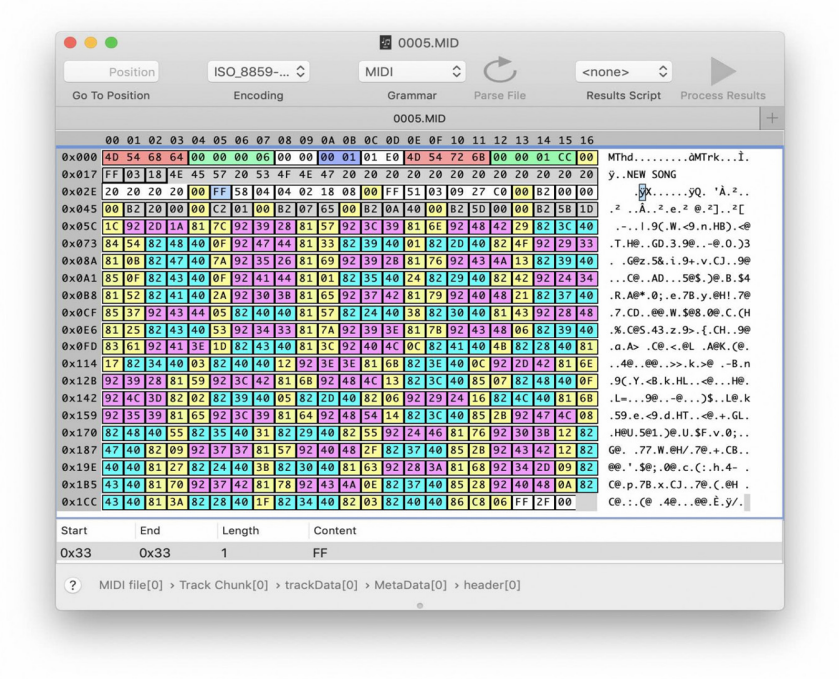


Рис. 2. Содержимое бинарного файла при открытии Hex-редактором Synalyze It.

Атакующему для начала потребуется составить грамматику файла [4]. Грамматика в данном случае — это иерархическая описательная структура, позволяющая представить двоичные данные в понятном человеку виде. При составлении грамматики потребуется проанализировать несколько файлов сохранений, а не только исходный, что значительно увеличивает время анализа. При этом сложность возрастает пропорционально сложности исходного сохраняемого в файле объекта сохранения: чем сложнее и комплекснее объект, тем больше блоков будет содержать бинарный файл и тем сложнее получится иерархия блоков этого файла.

Следует заметить, что процесс декомпозиции сложный, но не является невозможным. При определении структуры исходного объекта атакующий сможет так же приступить к стегоанализу.

Реляционная база данных. Многие игры, в которых используется сетевое взаимодействие, могут для хранения пользовательских публикаций использовать не хранилище файлов, а реляционные базы данных. При таком подходе для объекта в базе данных создаются таблицы, которые представляют основные поля объекта сохранения с помощью простейших типов данных. Это исключает из процесса обмена файл сохранения, и данные сохранения игроки могут получать по программному интерфейсу приложения с игрового сервера по протоколу HTTP или HTTPS. В таком случае атакующему придется для начала записать трафик с сервера до начала игры или искать данные об объекте в оперативной памяти при запущенной игре. В первом случае решить проблему можно при использовании HTTPS – атакующий не сможет расшифровать содержимое пакетов без сертификата. Во втором случае процесс поиска данных об объекте будет не менее трудоемким, чем анализ бинарного файла. Но это также не является невыполнимой задачей, поэтому атакующий, после определения структуры, все равно может приступить к стегоанализу.

Заключение. При сохранении данных компьютерной игры и скрытии в них сообщения методом стеганографии с учетом содержимого целесообразно использовать сохранение в файл в бинарном формате или сохранять данные напрямую в базу данных на сервере. В первом случае атакующий будет вынужден заниматься анализом структуры бинарного файла, а во втором – анализом трафика или анализом оперативной памяти. При этом форматы, воспринимаемые человеком, рекомендуется не использовать, поскольку игрок получает возможность модифицировать файл сохранения для получения преимуществ, а атакующий, определив структуру файла, – начать стегоанализ его содержимого.

СПИСОК ЛИТЕРАТУРЫ

1. Коржик В.И., Небаева К.А., Герлинг Е.Ю., Догиль П.С., Федянин И.А. Под общей редакцией профессора В.И. Коржика. Цифровая стеганография и цифровые водяные знаки // Санкт-Петербург, Том Часть 1 Цифровая стеганография, 2016
2. Chance Gibbs, Narasimha Shashidhar. StegoRogue: Steganography in Two-Dimensional Video Game Maps // Sematic Schoolar [Электронный ресурс]. URL: https://www.semanticscholar.org/paper/StegoRogue%3A-Steganography-in-Two-Dimensional-Video-Gibbs-Shashidhar/c2b2c98fb2141231fff76c21ffb32bc4f479fe93 (Дата обращения: 28.06.2021).
3. Бинарная сериализация. BinaryFormatter // METANIT.COM Сайт о программировании [Электронный ресурс]. URL: https://metanit.com/sharp/tutorial/6.2.php (Дата обращения: 28.06.2021).
4. Котов Б. Реверс-инжиниринг бинарного формата на примере файлов Korg SNG // Хабр [Электронный ресурс]. URL: https://habr.com/ru/post/442740/ (Дата обращения: 28.06.2021).

УДК 004.93'1

ЗАЩИЩЕННОЕ ИСПОЛНЕНИЕ НЕЙРОСЕТЕВЫХ АЛГОРИТМОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: АКТУАЛЬНОСТЬ ПРОБЛЕМЫ И ПЕРСПЕКТИВНЫЕ РЕШЕНИЯ

Ложников Павел Сергеевич, Сулавко Алексей Евгеньевич
Омский Государственный Технический Университет
Мира пр., 11, Омск, 644050, Россия
e-mails: lozhnikov@mail.ru, sulavich@mail.ru

Аннотация. Алгоритмы и приложения искусственного интеллекта становятся объектом потенциальных компьютерных атак. Рассматриваются атаки, которые гипотетически могут быть реализованы на искусственный интеллект в виде манипуляций с моделями, обучающими и входными данными, направленные на извлечение модели, обучающих данных и знаний. Предлагается использовать сети корреляционных нейронов, которые защищают от атак без применения гомоморфного шифрования решающих правил, позволяют реализовать быстрое автоматическое обучение искусственного интеллекта на малых выборках.

Ключевые слова: искусственный интеллект; машинное обучение; нейронные сети; нейросетевые алгоритмы; атаки на искусственный интеллект; архитектурная безопасность искусственного интеллекта.

NEURAL NETWORK ALGORITHMS OF ARTIFICIAL INTELLIGENCE IN A PROTECTED VERSION: RELEVANCE OF THE PROBLEM AND PROMISING SOLUTIONS

Lozhnikov Pavel, Sulavko Alexey
Omsk State Technical University
11 Mira Av, Omsk, 644050, Russia
e-mails: lozhnikov@mail.ru, sulavich@mail.ru

Abstract. Artificial intelligence algorithms and applications are becoming the target of potential computer attacks. Attacks are considered that can hypothetically be implemented on artificial intelligence in the form of manipulations with models, training and input data, aimed at extracting a model, training data and knowledge. It is proposed to use networks of correlation neurons that protect against attacks without the use of homomorphic encryption of decision rules, and make it possible to implement fast automatic training of artificial intelligence on small samples.

Keywords: artificial intelligence; machine learning; neural networks; neural network algorithms; attacks on artificial intelligence; architectural security of artificial intelligence.

В настоящее время технологии искусственного интеллекта (ИИ) и приложения на его основе становятся существенным интеллектуальным активом компаний, другими словами – нематериальным ресурсом, обладающим свойством уникальности и исключительности, способным приносить значительные экономические выгоды.

Специалисты аналитической компании IDC прогнозируют рост мирового рынка искусственного интеллекта ежегодно на 16-17%, включающего в себя программное обеспечение, оборудование и сервисы. Уже к концу 2021 он составит 327 млрд долларов. А к концу 2024 года рынок преодолеет отметку в 500 млрд долларов [1]. Выводы экспертов института экономических исследований McKinsey Global Institute ещё смелее: к 2030 году доля доходов в сфере ИИ будет ежегодно увеличивать мировой ВВП на 1,2% [2]. В настоящее время ИИ используется уже практически во всех отраслях экономики, включая транспорт, энергетику, здравоохранение, образование, оборону, финансы и производство.

Любое несанкционированное вмешательство в работу искусственного интеллекта может повлечь за собой последствия – материальный ущерб, нарушение информационной безопасности, угрозу жизни, здоровья граждан, технологический сбой или даже катастрофу. Все зависит от назначения конкретной реализации ИИ и возможностей, которыми данный экземпляр обладает. Под «защищенным исполнением» ИИ понимается невозможность совершения следующих действий любым неавторизованным лицом или субъектом доступа (процессом, пользователем, злоумышленником):

- анализа операций, совершаемых ИИ (алгоритма работы ИИ, суть преобразований);
- управления ИИ (с помощью изменения алгоритма работы, подмены данных ИИ и т.д.);
- извлечения знаний ИИ.

Поэтому в ответственных приложениях искусственный интеллект должен выполняться в защищенном исполнении.

Учитывая то, что ИИ в перспективе будет все больше и больше приносить прибыли компаниям, он становится объектом потенциальных компьютерных атак. Традиционный подход к построению интерфейса взаимодействия с ИИ в системах управления основан на том, что на вход ИИ поступает информация в пакетном режиме или режиме реального времени. Она анализируется по некоторому алгоритму, после чего на выходе ИИ возникают управляющие воздействия. Каждое «воздействие» — это код определенной команды, который представляет собой один или несколько бит информации. Печальным фактом является то, что при такой концепции построения ИИ злоумышленники гипотетически могут провести следующие виды атак:

1. Манипуляции с моделями. Частным случаем являются атаки «на решающий бит» (атаки «одного бита»). Существует, по крайней мере, две ситуации, касающиеся такого рода атак. Первая связана с редактированием программного кода ИИ (точнее его скомпилированной и обученной версии). Если на выходе ИИ возникают короткие команды, то злоумышленник может инвертировать логику программы, изменив решающее правило. Например, если на выходе нейронной сети располагается функция SoftMax, то достаточно поменять два ее выхода местами, чтобы заменить одно управляющее воздействие на другое (см. рис.1).

Вторая ситуация возникает, если хакер напрямую подключится к объекту управления или к каналу передачи данных с возможностью изменять сигналы на выходе ИИ. В этом случае он сможет имитировать определенные управляющие воздействия и изменять одну команду на другую. При этом ему не потребуется вникать в суть работы алгоритма анализа данных, достаточно лишь выявить ассоциации кода команды и связанного с ней действия. Для коротких управляющих команд выявить эти ассоциации несложно (см. рис.1). Одним из направлений по противодействию данной угрозе является разработка технологий «цифровых двойников» объектов управления [3]. «Цифровой двойник» должен прогнозировать результат выполнения последовательности команд, прежде чем запускать их на реальном объекте управления. Однако разработка подобных решений — сложный, ресурсоемкий процесс, успех которого зависит от предметной области [4] (разработать подобную технологию далеко не всегда возможно).

2. Манипуляции с обучающими данными. Целью таких манипуляций может быть создание вредоносного экземпляра ИИ, который будет выполнять функции, заложенные злоумышленником. Подмену экземпляра ИИ можно зафиксировать при сравнении контрольных сумм параметров и знаний ИИ.

Отметим, что если обучающая выборка фрагментирована и распределена между множеством владельцев данных, каждый из которых заинтересован в обеспечении конфиденциальности этих данных при обучении, то на практике реализуется концепция федеративного обучения (заключение модели ИИ в защищенную среду и ее обучение без перемещения обучающей выборки куда-либо). Однако при федеративном обучении возрастают риски, связанные с низким качеством или вредоносным характером обучающих данных (никто из участников процесса обучения не имеет доступа к обучающим данным других участников и не может проконтролировать корректность и репрезентативность выборки).

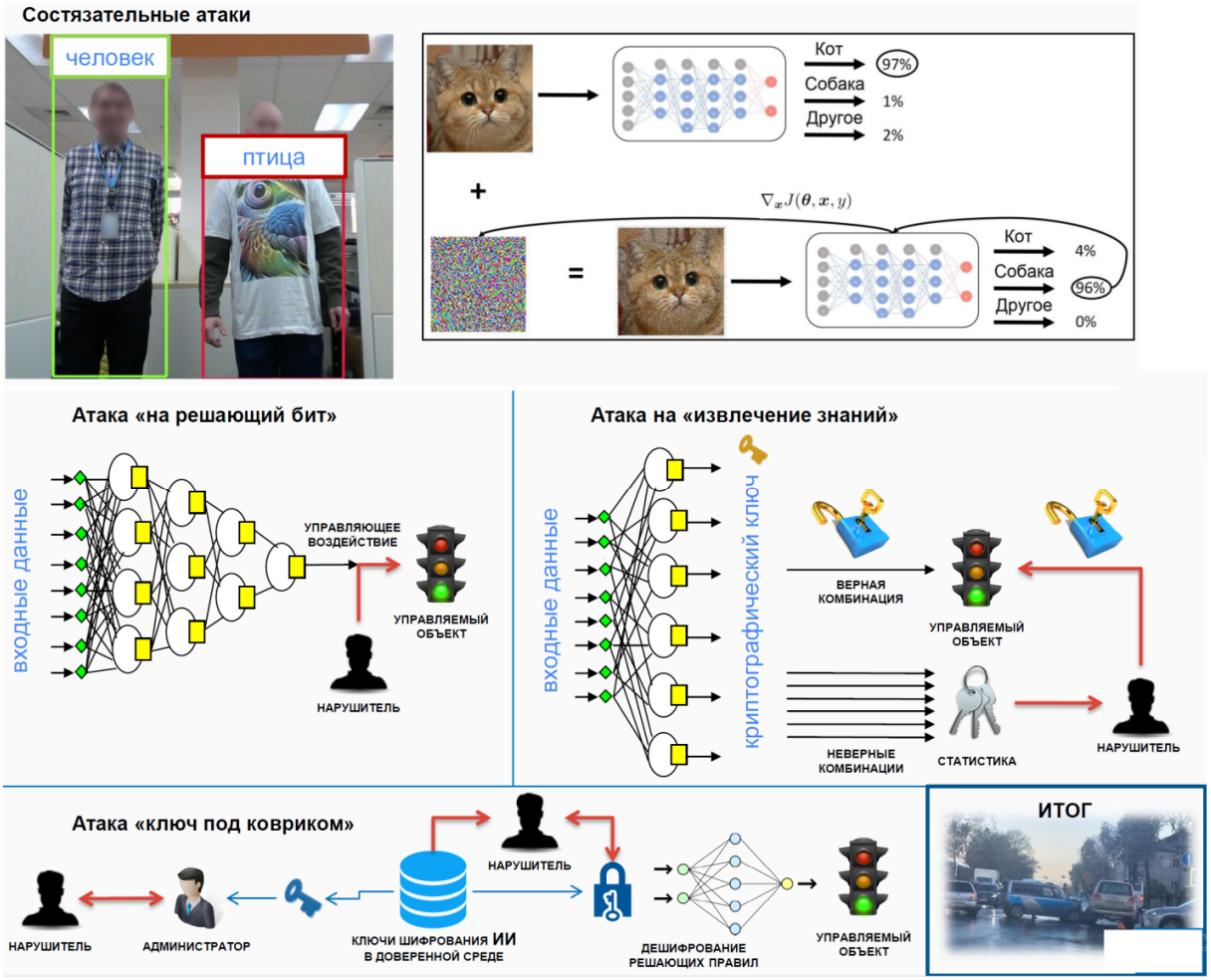


Рис.1. Некоторые атаки на нейросетевой искусственный интеллект.

3. Манипуляции с входными данными. К данной категории можно отнести «состязательные» атаки (спуфинг), при которых хакер подает на вход ИИ фальсифицированные или перехваченные данные с целью получения на выходе ИИ желаемых управляющих воздействий. Обычно для защиты от такого рода атак обучающую выборку пытаются расширить с учетом всех возможных вариаций входных данных, что не всегда возможно на практике.

4. Извлечение модели и/или обучающих данных (атаки «ключ под ковриком»). В памяти ИИ могут храниться конфиденциальные или персональные данные. Чтобы защитить эти данные от угрозы нарушения конфиденциальности, параметры решающих правил (например, таблицы весовых коэффициентов и связей нейронов) принято шифровать на некотором криптографическом ключе [5]. Ключ (или ключи) шифрования параметров решающих правил ИИ должны где-то храниться. Чтобы ИИ «заработал», требуется сначала дешифровать его «память». Таким образом, когда алгоритм анализа входных данных выполняется приложением, параметры решающих правил остаются незащищенными. В теории гомоморфное шифрование может быть использовано для защиты ИИ, но на практике до этого еще далеко, так как имеются нерешенные проблемы с низкой производительностью и с накоплением ошибок при шифровании даже небольших объемов данных [6]. Начиная с некоторого размера гомоморфные шифртексты перестают однозначно расшифровываться. Чем больше длина зашифрованного текста, тем больше вероятность, что, верно, дешифровать гомоморфное решение не удастся. На сегодняшний день для гомоморфного шифрования создан стандарт ISO/IEC 18033-6:2019, но этот стандарт не касается шифрования параметров нейросетевых решающих правил. Для защиты обученного ИИ и нейронных сетей с помощью гомоморфного шифрования следует разработать отдельные стандарты или рекомендации, которых на данный момент не предложено. Если не использовать гомоморфное шифрование, то ключи должны где-то храниться (в базе данных, в коде ИИ и т.д.), что создает ряд внешних и внутренних угроз. Хакер может похитить ключ, используя уязвимости в защите или вступив в сговор администратором. Человек всегда является «узким местом» в системе безопасности, поэтому эти вопросы нельзя закрыть полностью. Хуже всего, если все знания ИИ шифруются

на одном ключе (нет разделения знаний на независимо зашифрованные фрагменты). Создание инфраструктуры для безопасного хранения криптографических ключей – сложная задача, требующая значительных финансовых затрат.

5. Гибридные атаки. Эта категория атак может также быть связана с определенными манипулятивными воздействиями. Примером является атака «извлечения знаний» из нейронной сети с множеством выходов. Под этим термином подразумевается частичное или полное восстановление обучающей выборки путем манипуляций с входными данными и наблюдения статистики входов/выходов нейронной сети во время ее работы, либо путем непосредственного анализа параметров обученной нейронной сети в незашифрованном виде (таблиц связей и весовых коэффициентов нейронов). Конфиденциальная информация и персональные данные, находящиеся в памяти нейронной сети, не должны быть извлечены злоумышленником, даже если ее параметры хранятся в незашифрованном виде. Отметим, что реализация такой концепции как федеративное обучение не дает защиты от атаки «извлечения знаний», так как эта атака направлена на параметры уже обученного ИИ, при условии, что процесс обучения мог уже проходить в защищенной среде. Отметим, что подобная атака может осуществляться в отношении не только нейросетевых реализаций ИИ.

Чтобы указанные угрозы можно было устранить (или снизить до минимально возможного уровня) ИИ должен работать, как преобразователь входных воздействий (поступающей информации) в длинный криптографический ключ или пароль, который можно ассоциировать с определенным управляющим воздействием. Таким образом, вместо коротких кодовых команд на выходе ИИ, нужно использовать длинные криптографические ключи. Каждый ключ должен быть ассоциирован с отдельным действием, и только объект управления должен «знать», что нужно делать с поступившим от ИИ ключом (последовательность управляющих команд может быть зашифрована на данном ключе). Другими словами, ИИ должен проходить процедуру аутентификации. Для авторизации необходимо использовать неотчуждаемый от ИИ ключ или пароль, который должен храниться безопасно в защищенной памяти (ключ должен «помнить» только ИИ). Под этим имеется в виду, что нейросетевой ИИ необходимо научить продуцировать на своих выходах криптографические ключи (сгенерированные заранее по всем правилам и нормам), когда на его входы поступает образ, принадлежащий определенному классу (задача классификации образов).

Параметры обученного ИИ необходимо хранить в специальном виде, защищенном от извлечения «знаний» даже при отсутствии стороннего шифрования (конечно, шифрование можно применять для усиления защиты). Для этого нужно перейти от весовых коэффициентов классических нейронов к параметрам корреляционных нейронов Байеса-Минковского [7]. Корреляционные нейроны – это новый класс нейронов, анализирующих корреляционные связи между признаками вместо значений признаков в задачах классификации образов [8]. Анализ собственных (внутренних) корреляционных связей образов и принятие классификационных решений происходит без необходимости хранения информации о корреляционных связях или значениях признаков, характерных для образов, принадлежащих к тому или иному классу. Другими словами, эталонная информация о классах образов не компрометируется при хранении. Корреляционные нейроны обучаются с учителем в автоматическом режиме.

Инвертировать решения нейросетевого преобразователя, о котором идет речь, затруднительно. Для этого требуется перенастроить больше половины его нейронов. Проблема хакера будет заключаться в том, что операция инверсии каждого нейрона должна быть согласована с инверсией остальных нейронов. Для правильной настройки преобразователя нужно заново полностью обучить его с использованием той же выборки.

Нейросетевой преобразователь образа в криптографический ключ можно использовать совместно с любыми другими интеллектуальными технологиями анализа данных, в том числе, глубокой нейронной сетью. Например, автокодировщик или сиамские сети, можно использовать для извлечения признаков, а нейросетевой преобразователь образов в код — для продуцирования решения в виде длинного криптографического ключа. Таким образом, нейросетевой преобразователь может как бы заменить функцию SoftMax на выходе нейронной сети. При этом нейросетевой преобразователь будет обучаться отдельно от глубокой сети.

Чтобы атаки «на решающий бит» было затруднительно реализовать, необходимо, чтобы нейросетевой ИИ мог быстро обучаться в полностью автоматическом режиме. Тогда новую таблицу криптографических ключей можно генерировать периодически (например, раз в день или раз в 10 минут), заново обучая нейросетевой преобразователь в доверенной среде, после чего он может быть помещен в потенциально враждебную среду, где будет функционировать до следующего обучения. После каждого обучения предыдущая версия утратит работоспособность, поэтому хакеру придется взламывать преобразователь снова и снова его перенастраивать, чтобы получить требующийся для злоумышленных действий эффект.

На кафедре комплексной защиты информации Омского государственного технического университета под руководством Сулавко А.Е. разработаны модели корреляционных нейронов и алгоритмы их обучения, проведено аналитико-синтетическое исследование научных работ, а также международных и национальных стандартов, касающихся проблем безопасности искусственного интеллекта и методов их решения, включая гомоморфное шифрование, федеративное обучение и др. [8]. В отчете о НИР приводится обоснование необходимости защиты ИИ от ряда угроз и разработки третьего национального стандарта «Искусственный интеллект в защищенном исполнении» [9], а также предлагается план-проспект проекта данного стандарта, который затрагивает только задачи классификации.

Первый национальный стандарт ГОСТ Р 52633.5 по автоматическому обучению сетей нейронов с накоплением данных в линейном пространстве разработан в Пензенском научно-исследовательском электротехническом институте под руководством доктора технических наук Иванова Александра Ивановича, как и остальные стандарты серии ГОСТ Р 52633. Эти стандарты пока не имеют аналогов в мире. Стандарт ГОСТ Р 52633.5 ориентирован только на физически защищенную доверенную вычислительную среду. Защита параметров обученных нейросетевых преобразователей биометрия-код с помощью криптографических методов [10] приводит к необходимости использования коротких ключей и паролей при биометрической аутентификации. Проект второго национального стандарта позволяет повысить длину ключа аутентификации (примерно в 4 раза) за счет перехода к использованию квадратичных нейронов с многоуровневыми квантователями.

Третий национальный стандарт [10] на базе автоматически обучаемых сетей корреляционных нейронов должен решить все проблемы с длиной ключа.

Сети корреляционных нейронов дают преимущества:

– защиту от множества угроз информационной безопасности без применения гомоморфного шифрования решающих правил;

– быстрое автоматическое обучение ИИ на малых выборках.

Конечно, атаки на «извлечение знаний» из защищенного ИИ будут появляться (как и в случае с атаками на алгоритм ГОСТ Р52633.5), но они будут гораздо менее эффективны, к тому же защиту ИИ дополнительно можно усилить криптографией. Криптографическая защита корреляционных нейронов Байеса-Минковского может быть основана на классических методах без применения гомоморфного шифрования [10]. Перспективным является использование трех видов нейронов (линейных, квадратичных и корреляционных) для синтеза единой гибридной сети, которая будет обладать наивысшим уровнем защищенности от перечисленных угроз и давать более низкий процент ошибочных решений.

СПИСОК ЛИТЕРАТУРЫ

1. IDC прогнозирует ускорение роста мирового рынка искусственного интеллекта. URL: https://www.ixbt.com/news/2021/02/26/idc-prognoziruet-uskorenie-rosta-mirovogo-rynka-iskusstvennogo-intellekta.html (дата обращения: 30.08.2021).
2. Искусственный интеллект уже зарабатывает миллиарды. URL: https://www.dp.ru/a/2021/03/14/Iskusstvennij_intellekt_u (дата обращения: 30.08.2021).
3. Гарбук С.В., Правиков Д.И., Полянский А.В., Самарин И.В. Обеспечение информационной безопасности АСУ ТП с использованием метода предиктивной защиты//Вопросы кибербезопасности. 2019, №2(30). С.63-71. DOI: 10.21681/2311-3456-2019-3-63-71
4. Дмитриевский А.Н. Анализ рисков при использовании технологий искусственного интеллекта в нефтегазодобывающем комплексе / А. Н. Дмитриевский, Н. А. Еремин, П. С. Ложников [и др.] // Автоматизация, телемеханизация и связь в нефтяной промышленности. – 2021. – № 7(576). – С. 17-27. – DOI 10.33285/0132-2222-2021-7(576)-17-27.
5. Lozhnikov, P. S. Generation of a biometrically activated digital signature based on hybrid neural network algorithms / P. S. Lozhnikov, A. E. Sulavko // Journal of Physics: Conference Series, Omsk, 27–28 февраля 2018 года. – Omsk: Institute of Physics Publishing, 2018. – P. 012047. – DOI 10.1088/1742-6596/1050/1/012047.
6. А. О. Жиров, О. В. Жирова, С. Ф. Кренделев. Безопасные облачные вычисления с помощью гомоморфной криптографии // Безопасность информационных технологий. – 2013. - №1. – С. 6-12
7. Sulavko A.E. Bayes-Minkowski measure and building on its basis immune machine learning algorithms for biometric facial identification // Journal of Physics: Conference Series. - Vol. 1546. - IV International Scientific and Technical Conference «Mechanical Science and Technology Update» (MSTU-2020) 17-19 March, 2020, Omsk, Russian Federation. - doi:10.1088/1742-6596/1546/1/012103
8. Защищенный режим исполнения искусственного интеллекта на базе автоматически обучаемых сетей автокорреляционных нейронов: отчет о НИР. ОмГТУ. Рук. Сулавко А.Е. – Омск. – 101 С. – Исполн.: Ложников П.С., Самотуга А.Е., Магазев А.А., Данилова О.Т. URL:
9. https://www.researchgate.net/publication/351904440_ZASISENNYJ_REZIM_ISPOLNENIA_ISKUSSTVENNOGO_INTELLEKTA_NA_BAZE_AVTOMATICESKI_OBUCAEMYH_SETEJ_AVTOKORRELACIONNYH_NEJRONOV (дата обращения: 30.08.2021)
10. Иванов А.И., Сулавко А.Е. Проект третьего национального стандарта россии по быстрому автоматическому обучению больших сетей корреляционных нейронов на малых обучающих выборках биометрических данных // Вопросы кибербезопасности. - 2021. - №3. - С. 84-93. DOI:10.21681/2311-3456-2021-3-84-93
11. Техническая спецификация «Системы обработки информации. Защита криптографическая. Техническая спецификация. Защита нейросетевых биометрических контейнеров с использованием криптографических алгоритмов»: документ принят на заседании ТК 26 19.11.2020 / разраб. Акционерным обществом «Пензенский научно-исследовательский электротехнический институт» (ФГУП «ПНИЭИ»).

УДК 004.4

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ПОСТРОЕНИИ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

Михайлов Николай Семёнович
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., д. 67, лит. А, Санкт-Петербург, Россия
e-mail:nmikhailov.ru@gmail.com

Аннотация. Рассмотрены вопросы разработки методологии и средств поддержки процесса проектирования и практической реализации единого информационного пространства (КИС) промышленного предприятия. Предлагаемая методология позволяет топ-менеджменту, аналитикам, разработчикам и ИТ-специалистам оперативно реагировать на изменяющиеся организационно-технические условия производства и влияние внешней среды,

уточнять и согласовывать требования к элементам системы управления предприятием, постоянно совершенствовать и модернизировать. СНГ в процессе работы предприятия.

Ключевые слова: единое информационное пространство; бизнес-процесс; производственное предприятие.

SAFETY OF INFORMATION TECHNOLOGIES IN THE CONSTRUCTION OF A UNIFIED INFORMATION SPACE OF AN INDUSTRIAL ENTERPRISE

Mikhailov Nikolay
Saint Petersburg State University of Aerospace Instrumentation
Bolshaya Morskaya st., 67, lit. A, Saint Petersburg, Russia
e-mail:nmikhailov.ru@gmail.com

Abstract. The issues of development of methodology and means of support of the design process and practical implementation of a unified information space (CIS) of an industrial enterprise are considered. The proposed methodology allows top management, analysts, developers and IT specialists to quickly respond to changing organizational and technical conditions of production and the impact of the external environment, to clarify and agree on the requirements for the elements of the enterprise management system, to constantly improve and modernize. CIS in the process of the enterprise.

Keywords: unified information space; business process; manufacturing enterprise.

Необходимость успешного функционирования и развития промышленного предприятия в условиях жесткой конкурентной среды диктует свои требования к эффективности бизнес-процессов предприятия. Решение задачи повышения эффективности управления предприятием связано с необходимостью обеспечения информационной поддержки основных и вспомогательных процессов.

Любые значимые изменения на предприятии внедряются с помощью стратегии развития предприятия. В общем случае выделяют четыре уровня стратегий развития предприятия: корпоративная стратегия, бизнес-стратегия, функциональная стратегия и операционная стратегия (таблица 1)

Таблица 1

Классификация стратегий

Типы стратегии	**Ответственность**	
	Диверсифицированная компания	***Однопрофильная компания***
Корпоративная стратегия	Корпоративный менеджмент	-
Бизнес стратегия	Руководители подразделений	Высшее руководство
Функциональная стратегия	Руководители функциональных единиц в рамках подразделений	Руководители функциональных единиц в рамках подразделений
Операционная стратегия	Руководители предприятий и линейный менеджмент	Руководители предприятий и линейный менеджмент

Корпоративная или портфельная стратегия описывает общий управленческий план, который готовит высший менеджмент для диверсифицированной компании.

Бизнес-стратегия или конкурентная стратегия описывает меры и подходы, которые необходимы для оптимального функционирования подразделений. В однопрофильной компании бизнес-стратегия совпадает с корпоративной. Лучшие бизнес-стратегии описывают средства достижения уникальной компетенции в сфере в сфере ключевых направлений деятельности предприятия.

Функциональная стратегия описывает конкретный план деятельности функциональной единицы. Примерами функциональных стратегий предприятия могут служить стратегия развития информационных технологий и стратегия цифровой трансформации предприятия.

Операционная стратегия определяет принципы управления элементами организационной структуры (корпорациями, предприятиями, структурными подразделениями) в ежедневной деятельности по реализации стратегически важных направлений и инициатив.

В настоящее время широко используются как различные модели управления предприятием, так и подходы к проектированию информационной архитектуры и организации бизнес-процессов предприятия. В результате анализа результатов исследований [1-3], сделан вывод, что для обеспечения согласованного управления данными и информационным пространством предприятия необходимо построение единого информационного пространства (ЕИП) предприятия.

На решение задачи построения ЕИП промышленных предприятий направлена комплексная стратегия повышения эффективности бизнес-процессов, отражающих этапы жизненного цикла изделия и непосредственно влияющих на конкурентоспособность и качество продукции, за счет интеграции и преемственности информации, порождаемой на всех этапах жизненного цикла, т.е. сквозной информационной поддержки процессов на протяжении жизненного цикла изделия [4].

В данной работе под ЕИП промышленного предприятия понимается совокупность баз и банков данных, технологий их ведения и использования, информационно-телекоммуникационных систем и сетей, функционирующих на основе единых принципов и по общим правилам, обеспечивающим защищенное информационное взаимодействие всех участников, а также удовлетворение их информационных потребностей в соответствии с иерархией обязанностей и уровнем доступа к данным. Концептуальная модель ЕИП представлена на рис. 1.

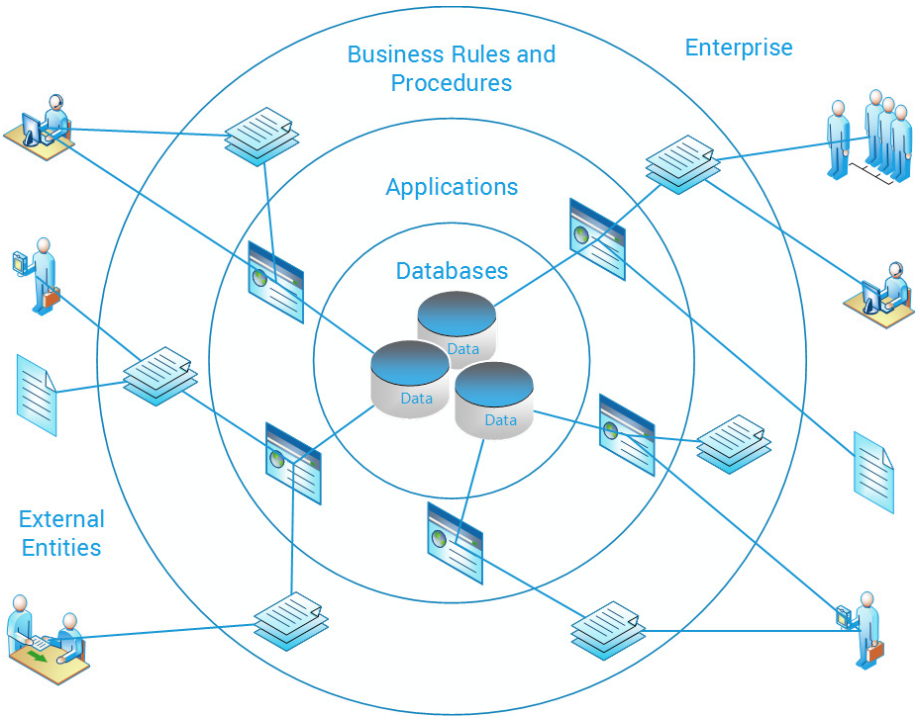


Рис. 1. Концептуальная модель ЕИП

Отличительной особенностью ЕИП промышленного предприятия является наличие интегрированной информационной системы, включающей следующие элементы:

1) телекоммуникационную среду, коммуникационное программное обеспечение (ПО), средства организации совместной работы Groupware;

2) информационные системы, информационные ресурсы и механизмы представления информации на их основе:

ERP-системы;

ПО управления электронным документооборотом;

ПО информационной поддержки предметной области;

ПО оперативного анализа информации и поддержки принятия решений;

ПО управления проектами: встроенные инструментальные средства и другие продукты, такие как CAD/CAE/CAM/PDM-системы;

ПО управления персоналом;

системы управления производством MES;

системы компьютерного менеджмента качества продукции промышленного предприятия на всех этапах ЖЦИ;

системы электронного сопровождения продукции промышленного предприятия в эксплуатации;

CRM-системы взаимоотношения с клиентами;

3) организационную инфраструктуру, обеспечивающую функционирование ЕИП промышленного предприятия;

4) систему подготовки и переподготовки специалистов и пользователей ЕИП промышленного предприятия.

Проектируемое ЕИП промышленного предприятия должно обеспечивать скорость перестройки бизнеса, цифровую трансформацию или внедрение изменений. Для этого необходимо учитывать множество связанных параметров из различных стратегических и программных документов. Процесс построения ЕИП промышленного предприятия сопряжен с необходимостью учитывать большое количество требований, содержащихся в многочисленных концептуальных, программных, проектных и регламентирующих документах. Представляется целесообразным структурировать указанные требования путем разделения их на три уровня:

1. Стратегический уровень (уровень бизнес-требований), включающий требования верхнего уровня к развитию промышленного предприятия, которые содержатся в стратегии развития предприятия (корпоративная стратегии, бизнес-стратегия, стратегия инновационного развития).

2. Функциональный уровень, учитывающий требования, выделенные из бизнес-уровня, и включающий различные функциональные стратегии, такие как стратегия развития информационных технологий, стратегия цифровой трансформации и т.п.

3. Уровень приложений, объединяющий требования прикладного уровня, определяемые техническими заданиями, техническими условиями, отраслевыми стандартами, лучшими практиками.

Для того, чтобы все участники процесса построения ЕИП промышленного предприятия могли системно взаимодействовать и учитывать требования разных уровней, предлагается формировать и использовать матрицу требований к ЕИП промышленного предприятия, представленную в табличной форме (таблица 2). В столбцах матрицы размещается информация, соответствующая трем уровням ЕИП:

1. Бизнес-уровень (стратегический уровень);
2. Функциональный уровень;
3. Уровень приложений.

В строках матрицы требования разделены по группам элементов ЕИП в соответствии с общепринятой методологией проектирования информационных систем промышленного предприятия [5]:

1. Взаимоотношения с контрагентами;
2. Корпоративное управление;
3. Управление данными об изделии;
4. Управление производством;
5. Управление инфраструктурой и оборудованием.

СПИСОК ЛИТЕРАТУРЫ

1. Марков Н.Г. Инструментальные средства для создания единого информационного пространства промышленных компаний // Информационное общество, вып.3, 2014. с.53-62.
2. Методология IDEF3 // Справочные материалы по информационным технологиям URL: http://itteach.ru/bpwin/metodologiya-idef3 (Дата обращения: 01.06.2020 г.).
3. URL: https://analytics.infozone.pro/methodology-design-software/ (Дата обращения: 01.06.2021 г.).
4. URL: https://studme.org/132133/informatika/integratsiya_informatsionnyh_sistem_edinom_informatsionnom_prostranstve_proizvodstvennoy_kompanii (Дата обращения: 01.06.2021 г.).
5. Mikhailov N. S. Approach to Construction of Common Information Space of Manufacturing Enterprise / Mikhailov N. S., Mikhailova A. S., Kasatkin V. V. // 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), 2020, pp. 385-390.

УДК 004.4

ПОДХОД К КЛАСТЕРИЗАЦИИ ТЕКСТОВОЙ ИНФОРМАЦИИ С ПОМОЩЬЮ ТЕЗАУРУСА

Михайлова Анна Сергеевна
Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
1-я Красноармейская ул., 1, Санкт-Петербург, Россия
e-mail: anna.mikhais@gmail.com

Аннотация. В статье рассматривается способ кластеризации текста с помощью коэффициента встречаемости ключевых слов тезауруса.

Ключевые слова: тезаурус; семантический анализ; семантическая сеть; кластеризация

APPROACH TO CLUSTERING TEXT INFORMATION USING THESAURUS

Mikhailova Anna Sergeevna
Baltic State Technical University «VOENMEKH» D.F. Ustinova
1 1st Krasnoarmeyskaya str., St. Petersburg, Russia
e-mail: anna.mikhais@gmail.com

Abstract. The article discusses a method for clustering text using the frequency of occurrence of keywords of the thesaurus.

Keywords: thesaurus; semantic analysis; semantic web; clustering.

Текст (от лат. textus – ткань, объединение, сочетание) - это произвольная человеческая мысль, письменно выраженная упорядоченной цепочкой языковых знаков.

Текстовая информация представляет из себя последовательность символов (в основном печатных знаков, принадлежащих тому или иному набору символов).

В текстовом файле текст может храниться как в неформатированном, так и форматированном или размеченном виде (например, Rich Text Format, HTML), где к каждому символу может быть применено форматирование (шрифт, начертание, размер и т. п.).

В DOS и Windows для файлов с неформатированным текстом обычно используется расширение .txt. Тем не менее, текстовыми могут являться файлы с любым другим расширением или без оного. Например, исходные коды программ обычно хранятся в файлах с расширениями, соответствующими языку программирования, на котором написаны программы (bas, .pas, .c).

Форматированный тест (текст с разметкой) обычно хранится в файлах с расширением, соответствующим формату или языку разметки — .rtf, .htm, .html и другие.

Семантический анализ текстовой информации дает возможность сопоставить этой информации предельно допустимое количество слов, которые могут кратко определить смысл содержания. Данные слова называют <терминами>, <метками>, <ключевыми словами>, <словами – определениями>. В информационной архитектуре – это <метаданные>.

В связи с тем, что ручной метод структурирования информации является достаточно трудоемким использование автоматизированного установления семантических связей между словами (терминами) значительно упрощает структуризацию текста, при этом связанные определенным отношением термины образуют тематические блоки. Таким образом, частично структурированный текст преобразуется в тезаурус.

Применение тезаурусов является классическим методом в задачах информационного поиска [1].

Тезаурусом является: словарь, в котором максимально полно представлены все слова языка с исчерпывающим перечнем примеров их употребления в текстах; – идеологический словарь, в котором показаны семантические отношения (родовидовые, синонимические и др.) между лексическими единицами. Моделью тезауруса служит семантическая сеть.

Для установления связей между словами и устойчивыми словосочетаниями текстовой информации используется корреляционный анализ. Вычисление коэффициентов корреляции для каждой пары слов производится по формуле [2]:

$$r = \frac{\sum (x_{1,i} - \bar{x}_1) \cdot (x_{2,i} - \bar{x}_2)}{\sqrt{\sum (x_{1,i} - \bar{x}_1)} \cdot \sqrt{\sum (x_{2,i} - \bar{x}_2)}}$$

где $\bar{x}_1 = \frac{\sum x_{1,i}}{n}$, $\bar{x}_2 = \frac{\sum x_{2,i}}{n}$ – средние значения для каждого параметра массива из точек.

Коэффициент корреляции r отображает степень статистической зависимости между двумя числовыми переменными (в данном случае между словами), $r \in [-1; 1]$.

При r = 1 корреляция считается положительной, при r = −1 корреляция считается отрицательной. При r=0 слова независимы друг от друга.

В Таблице 1 представлены виды корреляции в соответствии со значением коэффициента корреляции

Таблице 1

Таблица 1: виды корреляции в соответствии со значением r

Значение	**Интерпретация**
до 0,2	Очень слабая корреляция
до 0,5	Слабая корреляция
до 0,7	Средняя корреляция
до 0,9	Высокая корреляция
свыше 0,9	Очень высокая корреляция

После подсчета всех коэффициентов корреляции строится график, ранжируются связи терминов по заданному значению коэффициента корреляции, и удаляется информационный шум. Из оставшихся значимых пар слов формируется семантическая сеть.

Добавление в семантическую сеть определений терминов преобразует её в тезаурус текстовой информации.

Связи между элементами в тезаурусе отображаются в виде семантической сети (ориентированного графа), в котором все слова и устойчивые словосочетания связаны определенной связью, имеют иерархию и вес. Исходными данными для формирования тезауруса являются тексты.

Разработанный алгоритм построения тезауруса выглядит следующим образом:

1. Первоначальная обработка текста и выделение множества слов.
2. Удаление из полученного множества слов имен числительных, местоимений, союзов, предлогов, частиц и междометий.
3. Морфологический анализ каждого элемента из множества слов.
4. Вычисление коэффициентов корреляции для всех пар слов.
5. Ранжирование связей по заданному значению коэффициента корреляции и выделение устойчивых словосочетаний. В итоге сформированы массивы терминов и связей.
6. На основе полученных данных формируется семантическая сеть.
7. Сформированные массивы терминов и связей дополняются определениями терминов, и семантическая сеть преобразуется в тезаурус [2].

По результатам построения тезауруса производится кластеризация текста по коэффициенту встречаемости ключевых слов с помощью градиентных и квазиньютоновских методов минимизации, в Rn, при этом вместо поиска минимума функции осуществляется поиск максимума [3].

СПИСОК ЛИТЕРАТУРЫ

1. Башмаков А. И., Башмаков И. А. Интеллектуальные информационные технологии: учебное пособие. М.: Изд-во МГТУ им. Н.Э. Баумана, 2005. 304 с.
2. Метод построения тезауруса при семантическом анализе текста / А.С. Михайлова // Информационная безопасность регионов России (ИБРР-2019). XI Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2019 г.: Материалы конференции. \ СПОИСУ. – СПб, 2019. – С.188-189.
3. Полак Э. Численные методы оптимизации. Единый подход. (1971) Перевод с английского Ф.И. Ерешко. Под редакцией И.А. Вателя. С предисловием Н.Н. Моисеева. Москва: Издательство «Мир». 1974.

УДК 004.056.5

АНАЛИЗ ЗАЩИЩЕННОСТИ СИСТЕМ ИНДУСТРИАЛЬНОГО ИНТЕРНЕТА ВЕЩЕЙ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ ВХОДНОЙ ИНФОРМАЦИИ БЕЗОПАСНОСТИ

Федорченко Елена Владимировна, Паращук Игорь Борисович
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: doynikova@comsec.spb.ru, shchuk@rambler.ru

Аннотация. Проведен обзор особенностей, уровней и характера неопределенности, влияющей на анализ защищенности систем индустриального Интернета вещей в различных условиях функционирования. Сформулированы общие подходы к оценке показателей защищенности систем такого класса в условиях нестохастической неопределенности, а именно, неоднозначности (нечеткости) и недостаточности (неполноты и противоречивости) исходных данных – входной информации безопасности. Использование данных подходов создает предпосылки для повышения достоверности и оперативности анализа защищенности систем индустриального Интернета вещей в различных условиях обстановки.

Ключевые слова: неопределенность; анализ; защищенность; индустриальный Интернет вещей; показатель; нечеткость; противоречивость.

ANALYSIS OF THE SECURITY PROTECTION OF INDUSTRIAL INTERNET OF THINGS SYSTEMS IN THE CONDITIONS OF UNCERTAINTY OF SECURITY INPUT INFORMATION

Fedorchenko Elena, Parashchuk Igor
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: doynikova@comsec.spb.ru, shchuk@rambler.ru

Abstract. A review of the features, levels and nature of uncertainty affecting the analysis of the security of industrial Internet of Things systems in various operating conditions is carried out. General approaches to assessing the security indicators of systems of this class in the conditions of non – stochastic uncertainty, namely, ambiguity (fuzziness) and insufficiency (incompleteness and inconsistency) of the initial data-the security input information, are formulated. The use of

these approaches creates prerequisites for improving the reliability and efficiency of the analysis of the security of industrial Internet of Things systems in various conditions.

Keywords: uncertainty; analysis; security; industrial Internet of things; indicator; fuzziness; inconsistency.

Введение. Важным направлением развития мировой информационно-телекоммуникационной инфраструктуры являются системы индустриального Интернета вещей (ИИВ). Системы ИИВ представляют собой комплексные программно-аппаратные промышленные системы, обеспечивающие эффективное взаимодействие объектов (машин, устройств, механизмов), компьютеров и человека. Они обеспечивают интеллектуальные производственные процессы с использованием новейших методов анализа данных для получения новых качественных результатов индустриальных операций [1].

Системы ИИВ позволяют связывать и интегрировать подсистемы промышленного управления с корпоративными подсистемами, бизнес-процессами и бизнес-аналитикой. При этом системы ИИВ являются большими и сложными индустриальными объектами, содержат множество сенсоров, датчиков и исполнительных механизмов.

Многогранность, разнообразие и сложность разнородных взаимодействующих компонентов ИИВ обуславливает объективное существование проблем защиты объектов такого класса, проблем разработки методов и средств анализа их защищенности [2, 3].

Подобные проблемы решаются путем научных исследований и практических разработок в рамках частных подзадач:

- формирования множества объектов и метрик анализа защищенности ИИВ;
- анализа журналов событий объектов ИИВ и существующих средств мониторинга защищенности ИИВ;
- идентификации источников и значений параметров входной информации безопасности;
- синтеза множества иерархически взаимосвязанных метрик безопасности (показателей защищенности), позволяющих оценивать защищенность ИИВ;
- анализа онтологий метрик безопасности ИИВ в интересах оценки защищенности системы.

Эти подзадачи могут быть решены на основе применения методов классификации, теоретического и системного анализа, статистического и семантического анализа, логического вывода и методов интеллектуального анализа данных.

Вместе с тем, важной задачей продолжает оставаться разработка методов и средств достоверного и оперативного анализа защищенности систем ИИВ. Тем более, что значения параметров входной информации безопасности не всегда могут быть заданы четко и однозначно.

К информации безопасности, являющейся исходными данными для анализа защищенности систем ИИВ, относят входную информацию об объектах коммуникации, об уязвимостях, об инцидентах (событиях) безопасности, контрмерах (защитных мерах), конфигурациях, политиках безопасности и т.д. При этом, с точки зрения онтологии метрик безопасности, группа концептов (Security Information) объединяет именно информацию безопасности и включает концепты: product («продукт»), configuration («конфигурация»), weakness («слабое место»), attack («атака»), attacker («атакующий»), vulnerability («уязвимость»), countermeasure («контрмера»), exploit («эксплойт») [3].

Известно, что в классической постановке анализ защищенности систем ИИВ осуществляется в условиях детерминированности, вероятности и неопределенности значений параметров подобной входной информации безопасности. При этом детерминированные условия, характеризуемые строгим соответствием каждому параметру входной информации безопасности вполне определенного однозначного значения, реально встречаются крайне редко, особенно для систем ИИВ, функционирующих в условиях возможных кибератак.

Вероятностные условия более реальны, они характеризуются тем, что каждому параметру входной информации безопасности соответствует вполне определенное распределение вероятностей его состояния на множестве возможных состояний.

В неопределенных условиях, наиболее характерных для среды функционирования и управления системами ИИВ, характеристики их защищенности также могут иметь случайный характер, но в отличие от вероятностных условий, закон их распределения неизвестен. Кроме того, причины неопределенности значений параметров входной информации безопасности могут быть и не связаны со стохастичностью поведения защищаемого объекта [4].

Причины неопределенности информации безопасности при анализе защищенности систем ИИВ связаны с опытом администраторов безопасности, с нечеткостью и неполнотой знаний о значениях наблюдаемых параметров защищенности, с нестабильностью условий функционирования и управления системами ИИВ, с нестабильностью (изменчивостью) параметров самого процесса анализа защищенности. Изменение параметров процесса анализа защищенности объясняется рядом факторов:

1. Изменяются исходные данные (значения параметров входной информации безопасности), на основе которых осуществляется анализ защищенности систем ИИВ;
2. Изменяются внешние условия и текущие требования (критерии) по защищенности систем ИИВ (причина

– среда, нарушитель, задачи контроля и управления);

3. Изменяются методы и средства анализа защищенности систем ИИВ.

Можно сформулировать два класса нестабильности условий анализа защищенности систем ИИВ. Первый – условия анализа защищенности изменяются закономерно (например, в зависимости от шага функционирования систем ИИВ), т.е. детерминированный случай. Второй – условия анализа защищенности изменяются случайно, тогда речь идет о вероятностных и неопределенных условиях эксплуатации систем ИИВ.

Характер неопределенностей принято описывать четырьмя уровнями априорной неопределенности:

– полного задания распределений вероятностей случайных процессов по всей области их значений;

– параметрической априорной неопределенности (известен вид распределения, неизвестны параметры распределения);

– непараметрической априорной неопределенности (неизвестен даже вид распределения вероятностей случайных процессов);

– нечеткой (размытой) априорной неопределенности (неизвестны четкие границы множества состояний и вида распределения вероятностей значений его элементов).

Специалистам в области оценки информационной безопасности сложных систем различного назначения очевидна актуальность задачи разработки алгоритмов анализа защищенности систем ИИВ, учитывающих неопределенность исходных данных (значений параметров входной информации безопасности), неопределенность параметров текущего состояния защищенности систем такого класса, вызванные различного вида воздействиями и другие виды неопределенности.

При анализе защищенности систем ИИВ источником неопределенности исходных данных (значений параметров входной информации безопасности) различного вида могут выступать сами администраторы безопасности. Это происходит:

– когда системы ИИВ функционирует в нестационарных режимах, в условиях воздействия дестабилизирующих факторов, возникающих вследствие природных катастроф, осмысленной деятельности антагонистической системы (например, нарушителей);

– когда ограничения на ресурсы контроля и отсутствие статистических данных о параметрах входной информации безопасности вынуждают администратора безопасности использовать неопределенную, например, нечеткую (лингвистическую) форму описания входной информации безопасности;

– когда присутствует неопределенность (нечеткость) целей контроля и управления защищенностью систем индустриального Интернета вещей.

В рамках анализа защищенности систем ИИВ неопределенность может быть связана с вероятностной, неполной, недостоверной и т.п. информацией безопасности, т.е., информацией о поведении системы ИИВ, о механизме перехода параметров защищенности такой системы из состояния в состояние. Исследование подходов к анализу защищенности систем ИИВ, исследование видов и характера неопределенности, имеющей место при таком анализе показывают, что на современном этапе недостаточно развиты алгоритмы анализа в условиях нестохастической неопределенности, а именно, неоднозначности (нечеткости) и недостаточности (неполноты и противоречивости) исходной информации (входной информации безопасности) для анализа защищенности систем индустриального Интернета вещей.

Выход из этой ситуации нам видится в использовании «нечетких» и «противоречивых» оценок защищенности. При этом «нечеткие» оценки защищенности принимают значения в рамках множества лингвистических переменных, описывающих уровни (значения) показателей защищенности: плохая – удовлетворительная – хорошая – отличная защищенность. Степень соответствия тому или иному значению лингвистических переменных (показателей защищенности) определяется в рамках методов теории нечетких множеств на основе функций принадлежности и нечетких отношений [5-7].

Приведенные оценки защищенности называют «нечеткими». Очевидно, что за каждой из них скрыты количественные характеристики защищенности систем ИИВ в конкретной ситуации. Иными словами, можно говорить как о качественных характеристиках количественной меры защищенности, так и о количественных характеристиках качественной меры защищенности систем ИИВ.

Рассмотрением таких качественных решений занимается теория нечетких множеств. Основная идея «нечеткого» анализа заключается в том, что вместо определенных понятий, выражающих классы (множества) оценок защищенности с жестко заданными границами, вводятся понятия (например, плохая – удовлетворительная – хорошая – отличная защищенность), объемы которых расплывчаты в следующем смысле: имеются оценки показателей защищенности, которые попадают под данное понятие и являются элементами «жесткой» части его объема; оценки показателей защищенности, которые полностью не попадают под понятие, и результаты анализа, которые подпадают под понятие с определенной степенью.

Если полную принадлежность уровня (значения) показателя защищенности соответствующему множеству (объему расплывчатого лингвистического понятия типа плохая – удовлетворительная – хорошая – отличная защищенность) оценить единицей, а полную непринадлежность – нулем, то промежуточные степени

принадлежности будут оцениваться числами, лежащими между 0 и 1. Степень принадлежности оценочного значения (уровня) показателя защищенности y нечеткому подмножеству $\widetilde{A}$ возможных значений защищенности, называют характеристической функцией принадлежности $\mu_{\widetilde{A}}(y)$ [5, 7].

Помимо этого, «нечеткий» подход к решению задачи многокритериального анализа защищенности и выбора защитных мер заключается в выражении общей цели функционирования подсистемы безопасности системы ИИВ в виде иерархии подцелей. Здесь на нижнем уровне иерархии находятся частные цели, связываемые с элементарными критериями, которые позволяют оценить объекты из заданного множества. При этом для анализа защищенности и выбора защитных мер осуществляется операция свертки над нечеткими множествами, объединяющими частные цели. В итоге получим нечеткое множество метрик защищенности и защитных мер, которое, при использовании принципа обобщения, обеспечит итоговые нечеткие оценки защищенности.

Вторым ключевым аспектом нестохастической неопределенности является недостаточность (неполнота, противоречивость) исходных данных, которая может быть решена на базе «противоречивых» оценок защищенности. Для решения таких задач нашли свое успешное применение методы теории искусственных нейронных сетей [8].

Действительно, существующие методы анализа защищенности систем с нечетко заданными исходными данными (входной информацией безопасности) ориентированы, в основном, на математические марковские модели смены четких и нечетких состояний, четко и нечетко заданные пороговые значения (границы) состояний случайных процессов, протекающих в системах ИИВ, что в значительной степени позволяет решать задачи анализа защищенности в рамках лингвистической и физической неопределенности исходных данных о параметрах информационной безопасности систем такого класса.

В то же время на основе данных методов сложно произвести анализ защищенности систем ИИВ в условиях неполноты и противоречивости исходных данных и недостоверно заданных параметрах, характеризующих защищенность индустриального Интернета вещей в различных условиях функционирования. Очевидно, это связано с тем, что в процессе сбора информации для реализации процедур моделирования и фильтрации (экстраполяции) на определенном этапе может сложиться следующая ситуация:

– собрана еще не вся возможная (неполнота) или не вся необходимая (недостаточность) входная информация безопасности;

– для значений некоторых параметров защищенности систем ИИВ определены не точные их описания, а лишь множества, которым эти описания принадлежат (недоопределенность);

– ряд элементов задачи анализа защищенности систем ИИВ, временно описанный по аналогии с уже решавшимися задачами, имеет лишь «замещающее» описание (неадекватность) [7].

С точки зрения анализа защищенности систем ИИВ в процессе их функционирования это означает, что исходные данные для моделирования, фильтрации и экстраполяции (результаты наблюдений, измерений и диагностики параметров защищенности ИИВ, элементы стохастических матриц, пороговые значения (границы) состояний параметров защищенности) могут быть недостоверными. Что, в свою очередь, затрудняет применение известных моделей и алгоритмов для многокритериального анализа защищенности систем ИИВ в условиях неопределенности.

В таких ситуациях традиционно используют различные методы обработки экспертной исходной информации, а в нашем конкретном случае, когда характер информации не связан с лингвистической и физической неопределенностью, одним из действенных и математически корректных подходов к обработке неполной и противоречивой экспертной информации является использование нейросетевых алгоритмов идентификации исходных данных (входной информации безопасности).

Такие алгоритмы предназначены для того, чтобы использовать данные, знания, объективные и субъективные модели для анализа и решения слабоструктурированных и неструктурированных задач. Слабоструктурированными считаются задачи, которые содержат как количественные, так и качественные переменные, причем качественные аспекты проблемы имеют тенденцию доминировать. Неструктурированные задачи имеют лишь качественное описание. В свою очередь, в отличие от задач, решаемых методами теории нечетких множеств, в слабоструктурированных и неструктурированных задачах, характеризуемых наличием недостоверной и противоречивой информации, невозможно сформулировать лингвистические переменные и определить функции принадлежности. Именно поэтому задачи подобного класса решаются с использованием нейросетевых алгоритмов обработки экспертной информации.

В основу этих методов положена экспертная система, предназначенная для снижения уровня неполноты и противоречивости исходных данных при формировании управленческих воздействий, для прогнозирования оптимальных управлений по имеющимся априорным данным. Такой подход использует, так называемые, экстраполирующие нейронные сети, являющиеся разновидностью известных моделей ассоциативной памяти. Предлагаемый подход расширяет возможности существующих искусственных нейронных сетей, используемых в интересах поддержки принятия решений по контролю за системами ИИВ, позволяя принимать обоснованные решения по анализу защищенности.

Заключение. Таким образом, проведен анализ особенностей, уровней и характера неопределенности,

влияющей на анализ защищенности систем индустриального Интернета вещей в различных условиях функционирования. Предпринята попытка сформулировать общие подходы к оценке показателей защищенности систем такого класса в условиях нестохастической неопределенности, а именно, неоднозначности (нечеткости) и недостаточности (неполноты и противоречивости) исходных данных – входной информации безопасности для анализа.

Использование данных подходов создает предпосылки для повышения не только обоснованности, достоверности, но и для повышения оперативности анализа защищенности систем индустриального Интернета вещей в различных условиях обстановки. Показано, что существует ряд конкретных практических задач, где методы теории нечетких множеств и методы искусственных нейронных сетей позволяют устранить либо корректно учесть неопределенность в вопросах принятия решений при анализе защищенности и при выборе защитных мер противодействия в рамках обеспечения безопасности систем индустриального Интернета вещей.

Исследования проводятся при финансовой поддержке РФФИ (проект 19-07-01246) в СПб ФИЦ РАН (СПИИРАН).

СПИСОК ЛИТЕРАТУРЫ

1. Страшун Ю.П. Технические средства автоматизации и управления на основе IIoT/IoT. Учебное пособие. М.: Лань, 2020. – 76 с.
2. European Union Agency for Cybersecurity (ENISA). Good practices for Security of Internet of Things in the context of Smart Manufacturing. 2018. – P. 11.
3. Дойникова Е.В. Классификация и анализ целей кибератак в системах Индустриального Интернета вещей. // Информационная безопасность регионов России (ИБРР-2019). XI Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2019 г.: Материалы конференции. / СПОИСУ. СПб.: 2019. 596 с., С. 116-117.
4. Бушуев С.Н., Осадчий А.И., Фролов В.М. Теоретические основы создания информационно-технических систем. – СПб.: ВАС, 1998. – 404 с.
5. Паращук И.Б., Бобрик И.П. Нечеткие множества в задачах анализа сетей связи. – СПб.: ВУС, 2001. – 80 с.
6. Kotenko I., Parashchuk I. Decomposition and Formulation of System of Features of Harmful Information Based on Fuzzy Relationships // 2019 International Russian Automation Conference (RusAutoCon), Sochi, Russia, / IEEE Xplore Digital Library: Browse Conferences (2019). Vol. 8867588, 2019. pp. 1-5.
7. Авраменко В.С., Бобрешов-Шишов Д.И., Беденков В.Н., Маликов А.В. Определение актуальных угроз безопасности информации в инфокоммуникационных системах на основе аппарата нечеткой логики // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017). VI Международная научно-техническая и научно-методическая конференция. Т.3. – СПб.: СПБГУТ, 2017. С.13-18.
8. Паращук И.Б., Иванов Ю.Н., Романенко П.Г. Нейросетевые методы в задачах моделирования и анализа эффективности функционирования сетей связи. / Учебно-методическое пособие. – СПб.: ВАС, 2010. – 103 с.

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИЕ И ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 004.056.5

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ СИЛОВЫХ ВЕДОМСТВ РОССИИ ПОСРЕДСТВОМ ПРИМЕНЕНИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

Бобонец Сергей Алексеевич[1], Примакин Алексей Иванович[2]

[1] Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии Российской Федерации (СПВИ войск национальной гвардии)

[2] Санкт-Петербургский университет Министерства внутренних дел Российской Федерации

Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия

e-mails: sbobon@mail.ru, primakin@mail.ru

Аннотация. Рассматривается вопрос защиты информационных ресурсов, обеспечивающих деятельность силовых ведомств России, посредством применения криптографических алгоритмов.

Ключевые слова: шифрование; криптография; алгоритм; информационные технологии; компьютерные технологии.

ENSURING PROTECTION OF INFORMATION RESOURCES OF POWER DEPARTMENTS OF RUSSIA BY USING CRYPTOGRAPHIC ALGORITHMS

Bobonets Sergey[1], Primakin Alexey[2]

[1] St. Petersburg Military Order of Zhukov Institute of the National Guard Troops of the Russian Federation (SPVI National Guard Troops)

[2] St. Petersburg University of the Russian Interior Ministry

1 Pilot Pilyutov St, St. Petersburg, 198206, Russia

e-mails: sbobon@mail.ru, primakin@mail.ru

Abstract. The issue of protecting information resources that ensure the activities of law enforcement agencies of Russia through the use of cryptographic algorithms is being considered.

Keywords: encryption; cryptography; algorithm; information technology; computer technology.

Введение. Информация в последние годы обретает все большую важность и является универсальным орудием для достижения целей во всех областях жизнедеятельности общества: политических, экономических и военных. Благодаря широкому внедрению информационных технологий во все сферы деятельности общества и особенно в государственное и военное управление, которые являются критически важными и потенциально опасными объектами, остро встал вопрос защиты информационных ресурсов, обеспечивающих деятельность силовых ведомств России [1].

В рамках данной статьи вопросы защиты информационных ресурсов силовых ведомств России будут рассмотрены применительно к защите жестких (виртуальных) дисков информационных систем соответствующих структур. Актуальность и практический аспект выбранного направления заключается в том, что в настоящее время хорошо защищена только передаваемая информация, а хранящаяся на накопителях находится под угрозой, поскольку до сих пор большинство компьютеров работает на операционной системе (ОС) Windows, которая не обеспечивает должного уровня защиты данных. Возникает необходимость шифрования жесткого (виртуального) диска вычислительной машины.

Шифрование диска – технология защиты информации, переводящая данные на диске в нечитаемый код, который нелегальный пользователь не сможет легко расшифровать. Для шифрования диска используется специальное программное или аппаратное обеспечение, которое шифрует каждый бит хранилища. На рынке есть множество реализаций полного шифрования диска, они могут очень сильно различаться по возможностям и защищённости.

На данный момент существует несколько подходов (методов) к шифрованию жестких дисков:

1. Прозрачное шифрование (Transparent encryption), также называемое шифрованием в реальном времени (real-time encryption) или шифрованием на лету (on-the-fly encryption) – это метод, использующий какое-нибудь программное обеспечение для шифрования диска [2].

2. Шифрование на уровне файловой системы (filesystem-level encryption – FLE) – процесс шифрования каждого файла в хранилище. Доступ к зашифрованным данным можно получить только после успешной аутентификации. Некоторые операционные системы имеют собственные приложения для FLE, при этом доступно и множество реализаций от сторонних разработчиков. FLE прозрачно, это значит, что каждый, кто имеет доступ к файловой системе, может просматривать названия и метаданные зашифрованных файлов, которыми может воспользоваться злоумышленник.

3. Шифрование диска и Trusted Platform Module. Trusted Platform Module (TPM) – это безопасный криптопроцессор, встроенный в материнскую плату, который может быть использован для аутентификации аппаратных устройств. Так же он может хранить большие двоичные данные, например, секретные ключи и связывать их с конфигурацией целевой системы, в результате чего они будут зашифрованы, и расшифровать их можно будет только на выбранном устройстве. Есть как FDE, использующие TPM, например, BitLocker, так и те, которые не поддерживают работу с ним, например, TrueCrypt [3].

4. Полное шифрование и главная загрузочная запись. При установке программно-реализованного FDE на загрузочный диск операционной системы, которая использует главную загрузочную запись (англ. master boot record, MBR), FDE должен перенаправлять MBR на специальную предзагрузочную среду (англ. pre-boot environment, PBE), для осуществления предзагрузочной аутентификации (англ. Pre-Boot Authentication, PBA). Только после прохождения PBA будет расшифрован загрузочный сектор операционной системы. Некоторые реализации предоставляют возможность PBA по сети. Однако изменение процесса загрузки может привести к проблемам. Например, это может помешать осуществлению мультизагрузки или привести к конфликту с программами, которые обычно сохраняют свои данные в дисковое пространство, где, после установки FDE, будет расположена PBE. Так же это может помешать пробуждению по сигналу из локальной сети, так как перед загрузкой требуется PBA [3].

Самих программ, которые бы позволяли шифровать данные на жестких дисках, достаточно много, как для ОС Windows, так и для ОС Linux.

Так, BitLocker – технология шифрования жестких дисков, используемая в ОС семейства Windows. Однако, случается, что встроенной в операционную систему защиты либо недостаточно, либо она не соответствует необходимым требованьям. В этом случае приходиться прибегать к сторонним программам, предназначенным для шифрования накопителя информации. На рынке представлено огромное количество программного обеспечения, предназначенного для создания виртуальных зашифрованных жестких дисков. Наиболее удачными на наш взгляд являются: Folder Lock, PGP Desktop, VeraCrypt, GostCrypt, CyberSafe Top Secret, CryptoExpert 8 [4].

В контексте рассматриваемого вопроса необходимо отметить, что силовые структуры России, как и все остальные органы власти, работающие с государственной тайной и персональными данными, переходят на отечественную операционную систему Astra Linux Special Edition. Это единственная программная платформа, сертифицированная одновременно в системах ФСТЭК России, ФСБ, Минобороны РФ. Она позволяет обрабатывать информацию ограниченного доступа, содержащую государственную тайну, сведения с грифом не выше «совершенно секретно» в автоматизированных средствах всех министерств, ведомств и других учреждений Российской Федерации. Система включена в единый реестр российских программ для электронно-вычислительных машин и баз данных Минкомсвязи России, принята на снабжение Вооружённых Сил Российской Федерации, Войск национальной гвардии Российской Федерации и активно внедряется другими органами государственного управления, ведомствами и учреждениями [5].

По этой причине наиболее актуально и востребовано для силовых структур России искать систему безопасности именно для Astra Linux Special Edition. В Astra Linux за основу взята операционная система Debian, состоящая из свободного программного обеспечения с открытым кодом. Почти во всех ОС Linux есть встроенная система шифрования LUKS (Linux Unified Key Setup) – спецификация формата шифрования дисков, изначально нацеленная на использование в ОС на основе ядра Linux. В данной спецификации поддерживаются такие алгоритмы шифрования как AES, Serpent, Twofish и CAST. Данных алгоритмов вполне достаточно для защиты обрабатываемой информации, тем более что LUKS может использовать несколько алгоритмов одновременно [6].

Помимо встроенной спецификации для шифрования дисков в Linux можно установить стороннее программное обеспечение, выполняющие эти задачи. Примерами наиболее часто используемых утилит, которые имеют возможность создавать зашифрованные виртуальные жесткие диски являются: Tomb, VeraCrypt, GostCrypt, dm-crypt, ECryptfs, 7-ZIP, GPG.

Tomb (англ. гробница) – это утилита, которая задает «гробницы», которые по сути своей являются виртуальными зашифрованными жесткими дисками. Доступ к «гробнице» можно получить с помощью пароля или файла-ключа, который может храниться отдельно. Наиболее безопасным вариантом хранения этого файла-ключа является его хранение на USB накопителе. Контейнер, создаваемый Tomb, можно скрыть в файловой системе, а также передавать его по сети. Tomb нуждается в нескольких программах, таких как zsh, gnupg, cryptsetup и pinentry-curses,

которые должны быть установлены в системе для корректной работы. Данная утилита так же требует отключение файла подкачки, связано это с угрозой безопасности, которую создает файл подкачки [7].

VeraCrypt и GostCrypt для ОС Linux почти ничем не отличается от версии для ОС Windows.

Dm-crypt – стандартная подсистема шифрования дисков Linux-ядра версии 2.6, которая опирается на подсистему Device Mapper (dm), способную отображать дисковые устройства друг на друга, и криптографическое API (Crypto API), так же предоставляемое ядром и предназначенное для выполнения различных криптографических функций. Работает в паре с LUKS, поэтому может использовать все алгоритмы шифрования, которые использует LUKS [8].

ECryptfs – это POSIX-совместимая (Portable Operating System Interface – набор стандартов, описывающих интерфейсы между операционной системой и прикладной программой (системный API)) криптографическая «стековая» файловая система для Linux, в отличии dm-crypt не является подсистемой полного дискового шифрования на уровне ядра, но может создать зашифрованные каталоги поверх основной файловой системы. Поддерживает такие шифры, как: AES, BlowFish, 3Des, TwoFish, Cast [9].

7-ZIP – свободный файловый архиватор с высокой степенью сжатия данных [10]. Программа бесплатная и имеет открытый исходный код, большая часть которого свободно распространяется на условиях лицензии GNU LGPL. Может создавать зашифрованные хранилища (архивы) формата 7z и ZIP. Используется алгоритм шифрования AES-256. В качестве ключа используется пароль. Взломать защиту можно только методом перебора. Минусами можно считать то, что забытый пароль – потерянная информация, а также то, что работать можно только с распакованным файлом.

GPG (GNU Privacy Guard) – свободная программа для шифрования информации, выпущена под свободной лицензией GNU General Public License [11]. Поддерживает блочные алгоритмы шифрования, такие как AES, CAST5, 3DES, Twofish, Blowfish, Camellia, а также IDEA с помощью плагина. Работа с GPG осуществляется с помощью командной строки, что может отпугнуть неопытных пользователей.

В настоящее время частные предприятия, работающие с информацией, могут использовать почти любое лицензионное программное обеспечение, а выбор программы для защиты информации у таких компаний зависит от соотношения цены и качества программного обеспечения. Силовые структуры России, в свою очередь, должны использовать только российские алгоритмы шифрования, которые лицензированы и рекомендованы ФСБ России, а именно, описанные в ГОСТ 34.12-2018 – блочные шифры «Магма» и «Кузнечик» [12].

В ГОСТ 34.12-2018 приведено описание двух базовых блочных шифров с длинами блоков n=128 бит и n=64 бит, длинами ключей k=256 бит. Шифр «Магма» был разработан КГБ СССР и изначально носил название «ГОСТ 28147-89». Основан данный шифр на сети Фейстеля, имеет 256 битный ключ, блоки размером 64 бита и 32 раунда [13].

«Кузнечик» симметричный алгоритм блочного шифрования с размером блока 128 бит и длиной ключа 256 бит, в свою очередь, основан на подстановочно-перестановочной сети (SP-сети) В отличие от сети Фейстеля, при использовании SP-сети преобразуется весь входной блок. Такая структура иногда также называется AES-like (похожей на AES), однако, в отличие от последнего у «Кузнечика» есть ряд своих преимуществ – линейное преобразование может быть реализовано с помощью регистра сдвига; ключевая развертка реализована с помощью сети Фейстеля, в которой в качестве функции используется раундовое преобразование исходного алгоритма [14].

У Linux, как было описано выше, есть своя система защиты – Luks, функционал которой позволяет создавать зашифрованные контейнеры. Ядро Linux возможно модифицировать с помощью фреймворка DKMS (Dynamic Kernel Module Support), т.е. существует возможность внедрения в Luks алгоритма «Кузнечик», что позволит использовать все возможности Luks совместно с отечественным шифром.

По адресу https://github.com/kuzcrypt/kuznyechik-kernel47 в общем доступе и с лицензией свободного распространения лежит код для модифицирования ядра Linux и внедрения в него отечественных блочных шифров «Магма» и «Кузнечик» [15].

Для ОС Linux есть алгоритмы шифрования GotsCrypt и VeraCrypt, которые можно применять в паре с Luks. Сам же Luks имеет утилиты для создания зашифрованных виртуальных жестких дисков Tomb и ECryptfs. Учитывая, что в Luks есть возможность полнодискового шифрования, появляется возможность зашифровать один из дисков, а на зашифрованном носителе создать еще зашифрованный контейнер с помощью Luks (GotsCrypt или VeraCrypt). Выбирая между GotsCrypt и VeraCrypt, стоит отметить, что утилита VeraCrypt полностью переведена на русский язык, имеет больше алгоритмов шифрования и хеширования, а также более современный интерфейс [16].

Заключение. Таким образом, с переходом силовых структур России на ОС Astra Linux, осуществление модификации ядра данной ОС с помощью фреймворка DKMS и внедрение в систему шифрования Luks отечественных блочных шифров «Магма» и «Кузнечик» можно рассматривать, как перспективное направление в области обеспечения эффективной защиты информационных ресурсов соответствующих силовых ведомств.

СПИСОК ЛИТЕРАТУРЫ

1. Стратегия и контрстратегия гибридной войны // Военная мысль. 2018. № 10 [Электронный ресурс]. URL: https://vm.ric.mil.ru/Stati/item/138034/ (Дата обращения: 12.08.2021).
2. Коротин А.М. О способах реализации прозрачного шифрования файлов на базе сертифицированного скзи для операционной системы Linux // Безопасность информационных технологий. – 2012. – № 2012 – 2. – С. 62-66.

3. K. Scarfone, M. Souppaya, M. Sexton. Guide to Storage Encryption Technologies for End User Devices. – Special Publication 800-111. – National Institute of Standards and Technology, 2007. – 40 c.
4. CryptoExpert 8 - Secure Offline Storage for Windows 10. URL: [Электронный ресурс]. https://www.cryptoexpert.com/ (Дата обращения: 12.08.2021).
5. Об импортозамещение программного обеспечения в Российской Федерации. [Электронный ресурс]. URL: https://digital.gov.ru/uploaded/files/ob-importozameschenii-programmnogo-obespecheniya-v-rossijskoj-federatsii.pdf (Дата обращения: 12.08.2021).
6. Шутки в сторону: обзор ПО для российских военных и силовых структур. [Электронный ресурс]. URL:https://servernews.ru/968470 (Дата обращения: 12.08.2021).
7. Tomb – шифрование файлов и личный инструмент резервного копирования для Linux. [Электронный ресурс]. URL: https://itsecforu.ru/2018/10/01/tomb (Дата обращения: 12.08.2021).
8. Шифрование дисков в Linux. [Электронный ресурс]. URL: https://losst.ru/shifrovanie-diskov-v-linux (дата обращения: 12.08.2021).
9. Как зашифровать каталоги с помощью eCryptfs на Linux. [Электронный ресурс]. URL: https://itsecforu.ru/2020/06/06/ (Дата обращения: 12.08.2021).
10. 7-Zip. [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/7-Zip (Дата обращения: 12.08.2021).
11. Используем GPG для шифрования сообщений и файлов. [Электронный ресурс]. URL: https://habr.com/ru/post/358182/(Дата обращения: 14.02.2021).
12. ГОСТ Р 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры. [Электронный ресурс]. URL: https://files.stroyinf.ru/Data2/1/4293732/4293732907.pdf (Дата обращения: 12.08.2021).
13. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200007350 (Дата обращения: 12.08.2021).
14. Криптографический алгоритм «Кузнечик»: просто о сложном. [Электронный ресурс]. URL: https://habr.com/ru/post/459004/ (Дата обращения: 12.08.2021).
15. 15. Kuznyechik and Magma Linux Kernel Modules. [Электронный ресурс]. URL: https://github.com/kuzcrypt/kuznyechik-kernel (дата обращения: 12.08.2021).
16. 16. VeraCrypt – практические руководства по использованию программы, инструкции VeraCrypt, зашифровать диск VeraCrypt, зашифровать системный диск в Windows и Linux. [Электронный ресурс]. URL: https://veracrypt.ru/ (дата обращения: 12.08.2021).

УДК 004.05

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ МЕТОДОМ АДАПТИВНОГО ИНФОРМАЦИОННОГО РЕЗЕРВИРОВАНИЯ УСТРОЙСТВ ПАМЯТИ

Бородавко Александр Владимирович[1], Бобонец Сергей Алексеевич[1], Примакин Алексей Иванович[2]
[1]Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии Российской Федерации
Летчика Пилютова, ул., 1, Санкт-Петербург, 198206, Россия
[2]Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова, ул., 1, Санкт-Петербург, 198206, Россия
e-mail: univermvd@rambler.ru, a.primakin@mail.ru

Аннотация. Для обеспечения безопасности автоматизированных систем, функционирующих в условиях воздействия дестабилизирующих факторов, в качестве реализации технологических мер защиты рассмотрены методы информационного резервирования устройств памяти, как наиболее уязвимых компонентов к деструктивным воздействиям. По критерию сокращения аппаратурных затрат предложен наиболее эффективный метод адаптивного информационного резервирования устройств оперативной памяти.

Ключевые слова: безопасность автоматизированных систем; надежность; информационное резервирование; корректирующие коды; оперативное запоминающее устройство с автономным контролем.

ENSURING THE SECURITY OF AUTOMATED SYSTEMS ADAPTIVE INFORMATION RESERVATION METHOD MEMORY DEVICES

Borodavko Alexander, Bobonets Sergey, Primakin Alexey
Saint Petersburg Military Order of Zhukov Institute of the National Guard of the Russian Federation
Pilyutov's pilot, 1 St., Saint Petersburg, 198206, Russia
Saint Petersburg University of the Ministry of Internal Affairs of the Russian Federation
Pilyutov's pilot, 1 St., Saint Petersburg, 198206, Russia
e-mail: univermvd@rambler.ru, a.primakin@mail.ru

Abstract. To ensure the safety of automated systems operating under the influence of destabilizing factors, the methods of information backup of memory devices as the most vulnerable to destructive effects of components are considered as the implementation of technological protection measures. According to the criterion of reducing hardware costs, the most effective method of adaptive information redundancy of RAM devices is proposed.

Keywords: security of automated systems; reliability; information redundancy; correction codes; RAM with autonomous control.

Введение. Резервирование является одним из эффективных методов повышения надежности и безопасности автоматизированных систем (АС) различного назначения, функционирующих в условиях воздействия

дестабилизирующих факторов. Наиболее уязвимыми компонентами АС в отношении как естественных, так и искусственных источников угроз безопасности (отказов и сбоев элементов, вызванных ионизирующими изучениями, электромагнитными воздействиями и т.п.) являются устройства памяти. Это обусловлено плотностью компоновки и регулярностью структур запоминающих элементов устройств памяти, подверженных дестабилизирующим воздействиям. Особую актуальность приобретают задачи обеспечения безопасности информации в устройствах памяти специализированных АС, функционирующих в агрессивных средах в условиях воздействия активных помех. При этом классические методы резервирования для повышения надежности и безопасности АС не всегда эффективны с позиций изменения параметров среды эксплуатации и учета всех деструктивных воздействий.

В свою очередь, блочно-модульное построение и специфика организации доступа к информации, позволили широко применять на практике методы информационного резервирования устройств памяти, в основу которых положены корректирующие коды с избыточностью [1, 2].

Однако, для обеспечения безопасности АС, функционирующих в условиях воздействия помех и дестабилизирующих факторов, традиционные методы информационного резервирования устройств памяти из-за больших аппаратурных затрат и временных ограничений на обнаружение и исправление ошибок большой кратности не всегда приемлемы. В этой связи, в современных АС для обеспечения безопасности информации в устройствах памяти целесообразно использовать методы адаптивного информационного резервирования, основанные на реализации кодов с изменяемой корректирующей способностью, с учетом складывающейся обстановки по интенсивностям отказов и сбоев элементов устройств. При таком информационном резервировании реализуется так называемый альтернативный ряд кодов, схожих по своей структуре, но с разной корректирующей способностью. Эффективность данного метода обусловлена особенностями блочных структур выборки информации в современных устройствах памяти различного уровня. В оперативных запоминающих устройствах имеется возможность контролировать не только информационные слова, но и целые страницы памяти, предварительно считываемые из накопителей блоков памяти запоминающих устройств по старшим разрядам адресов.

К примеру, в запоминающем устройстве с автономным контролем, построенном на многоразрядных накопителях динамического типа [1], страница памяти имеет вид (рис. 1):

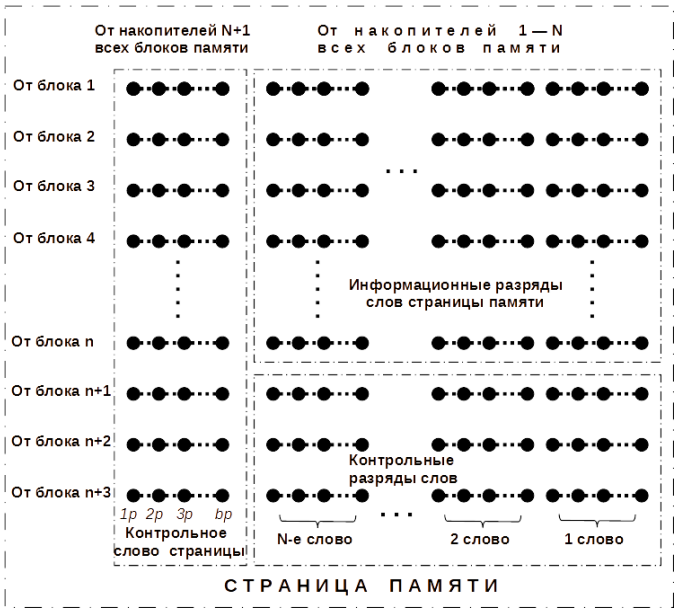


Рис. 1. Структура страницы памяти

В данном оперативном запоминающем устройстве, за счет использования принципа прямоугольного помехоустойчивого кодирования на основе блочного контроля по модулю 2 строк страницы памяти, а также информационных слов (столбцов страницы памяти) по GF(2)-подкоду кода Рида-Соломона, имеется возможность обнаружения тройных и коррекции одиночных и двойных модульных ошибок, равных разрядности блоков памяти. Это значительно повышает надежность оперативной памяти. Однако, как видно из рис. 1, существенно снижается информационная емкость памяти из-за большой избыточности корректирующего кода.

С учетом того, что запоминающие устройства с помехоустойчивым кодированием обладают способностью постепенного накопления корректируемых отказов элементов памяти, целесообразно применять на практике методы адаптивного информационного резервирования. В качестве примера, рассмотрим альтернативный ряд, состоящий из двух кодов: 1 уровень – блочный контроль по модулю 2 строк и столбцов страницы памяти; 2 уровень – контроль строк страницы по модулю 2 и столбцов страницы по GF(2)-подкоду Рида-Соломона. Для обеспечения постоянства

длины информационных слов осуществляется перенос их контрольных разрядов в соответствующие пакеты разрядов старших столбцов страницы памяти (от i-того информационного слова в пакеты разрядов, соответствующие i-тому блоку памяти) рис.2.

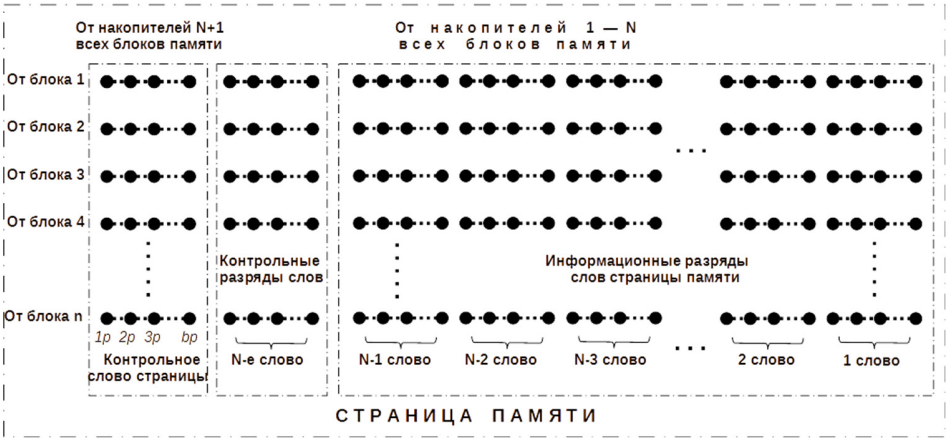


Рис.2. Структура страницы памяти для кода 1 уровня

Для кода 2 уровня, на который производится переход в случае обнаружения корректируемой одиночной модульной ошибки, обусловленной отказом элемента памяти, структура страницы показана на рис. 3.

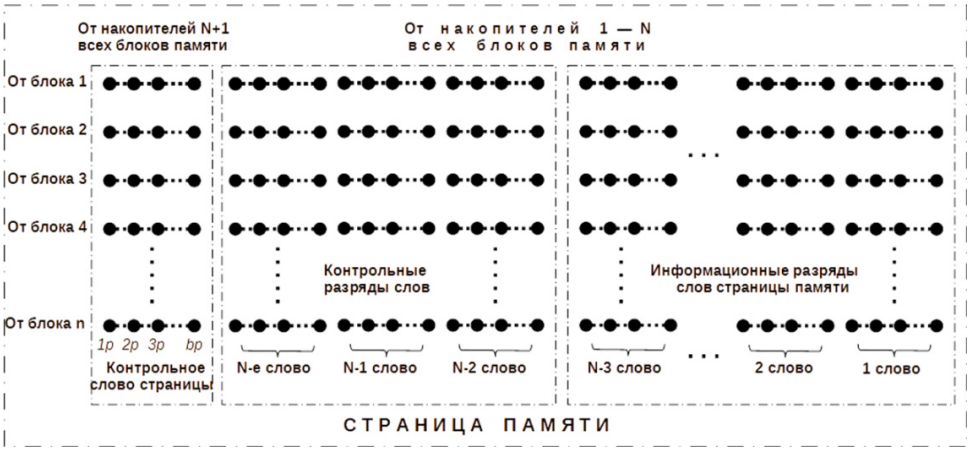


Рис. 3. Структура страницы памяти для кода 2 уровня

Для кода 2 уровня контрольные разряды информационных слов формируются в соответствии с проверочной матрицей GF(2)-подкода кода Рида-Соломона:

$$\mathbf{H} = \begin{pmatrix} \mathbf{I} & \mathbf{I} & \mathbf{I} & \dots & \mathbf{I} & \dots & \mathbf{I} & \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{I} & \mathbf{h}^{1} & \mathbf{h}^{2} & \dots & \mathbf{h}^{j/2} & \dots & \mathbf{h}^{\beta-1} & \mathbf{0} & \mathbf{I} & \mathbf{0} \\ \mathbf{I} & \mathbf{h}^{2} & \mathbf{h}^{4} & \dots & \mathbf{h}^{j} & \dots & \mathbf{h}^{\beta-2} & \mathbf{0} & \mathbf{0} & \mathbf{I} \end{pmatrix} \quad (1)$$

где b – разрядность блока памяти запоминающего устройства; I – единичная подматрица размерности bxb; 0 – нулевая подматрица размерности bxb; h^{β} – подматрица размерности bxb, определяемая выражением:

$$h^{\beta} = [\alpha^{\beta+b-1}\ \alpha^{\beta+b-2} \dots \alpha^{\beta+b-b}], \quad (2)$$

где $\alpha^{\beta+B-1}$ – столбец, соответствующий остатку от деления $x^{\beta+b-1}$ на порождающий многочлен G(x) степени b; β – показатель степени матрицы, $1 \le \beta \le 2^{b}-1$.

Максимально возможное количество разрядов в информационном слове ограничено разрядностью блоков памяти запоминающего устройства и определяется выражением:

$$K \le b(2^{b}-1) \quad (3)$$

При этом общее число блоков памяти в данном оперативном запоминающем устройстве $n \le 2^{b}-1$, что на 3 блока меньше чем в устройстве без адаптации при значительно большей эффективно используемой информационной емкости оперативной памяти. Это видно из представленных выше структур страниц памяти, так

как лишь незначительное их число в оперативной памяти со временем будет кодироваться более мощным корректирующим кодом в зависимости от складывающихся условий эксплуатации.

Похожие подходы к реализации адаптивного информационного резервирования также возможны с учетом блочного характера выборки информации в устройствах внешней памяти (системах на магнитных дисках, твердотельных накопителях). В устройствах внешней памяти на магнитных дисках, начиная с систем уровня RAID 2 и выше широко применяется код Хэмминга и контроль на четность [2]. Технология же твердотельных накопителей (SSD на микросхемах NAND), вообще не может гарантировать отсутствие ошибок. Поэтому разработчики микросхем NAND для коррекции ошибок в накопителях заранее предусматривают выделение резервных областей для записи контрольных разрядов (кодов коррекции ошибок – ECC). К примеру, компания Samsung предлагает блочный модифицированный код для коррекции одиночных ошибок в странице памяти емкостью 256 байт с хранением в резервной области 22 разрядов ECC [3].

Заключение. Предложенный метод адаптивного информационного резервирования, учитывая особенности структуры и функционирования устройств оперативной памяти с постепенным накоплением в течение времени корректируемых ошибок, позволяет значительно повысить их надежность с малыми аппаратурными затратами. Целесообразно применение адаптивного информационного резервирования в устройствах не только внутренней, но и внешней памяти, что дает возможность за счет коррекции ошибок большой кратности повысить эффективность и информационную безопасность автоматизированных систем, функционирующих в условиях воздействия дестабилизирующих факторов.

СПИСОК ЛИТЕРАТУРЫ

1. Бородавко А.В., Корженевский С.В., Уханов М.В. Запоминающее устройство с автономным контролем // Авторское свидетельство №1785040, 30.12.1992 г.
2. Совершенствуя системы хранения данных. – Режим доступа: https://www.ixbt.com/storage/raids.html (дата обращения 15.06.2021).
3. NAND Flash ECC Algorithm // Memory Division Samsung Electronics Co., LTD. – Режим доступа: https://www.elnec.com/sw/samsung_ecc_algorithm_for_256b.pdf (дата обращения 15.06.2021).

УДК 32.019.5

СТРУКТУРИРОВАНИЕ И ОСОБЕННОСТИ СОВРЕМЕННОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

Борщенко Виктор Владимирович
Северо-Западный институт управления РАНХиГС
Средний пр., В.О., 57/43, Санкт-Петербург, 199178, Россия
e-mail: boss-victor@yandex.ru

Аннотация. Статья посвящена уточнению понятия информационного пространства в современном мире. Рассмотрены ключевые понятия в социально-экономическом направлении, а также этапы формирования и уровни защищённости информационного пространства.

Ключевые слова: информационное пространство; степени защищённости; информационное общество; элементы политической структуры; информационные технологии.

STRUCTURING AND FEATURES OF THE MODERN INFORMATION SPACE

Borshenko Viktor
The North-West Institute of Management of RANEPA
57/43 Sredny Av, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: boss-victor@yandex.ru

Abstract. The article is devoted to clarifying the concept of information space in the modern world. The key concepts in the socio-economic direction, as well as the stages of formation and levels of security of the information space are considered.

Keywords: information space; degrees of security; information society; elements of the political structure; information technologies.

Понятие информации в начале XXI в. стало ключевым для большинства социальных наук и ключевым ресурсом современной экономики. Под информацией в техническом смысле понимается совокупность любых сигналов и символов, посредством которых осуществляется передача образов реального (материального) мира от источника к реципиенту. В социальных науках под информацией стали понимать не только сведения, но и образы и смыслы, то есть факторы, определяющие не реальный, а символический, виртуальный мир.

Формирование информационного общества обеспечило стремительное увеличение ее производительности. Информация, информационные технологии и системы превращаются в системообразующий элемент почти всех сфер деятельности человека. Вместе с тем с использованием информации связан огромный спектр проблем. Такое понятие

как «информационное пространство» нельзя назвать неоднозначным. Ряд авторов считает, что информационное пространство функционирует на основе общих принципов, и его главной функцией является обеспечение процессов коммуникации между различными участниками информационного пространства. В информационное пространство они включают совокупность технических устройств, сетей и систем накопления и хранения данных, а также технологии и программные продукты.

В состав информационного пространства также следует включать информационные объекты, представляющие собой сформированные по определенным правилам данные, трактуемые информационной системой как единое целое и их потоки [2].

В информационном пространстве взаимодействие элементов политической структуры осуществляется посредством обмена информацией.

Качество такого взаимодействия определяется свойствами информационного пространства:

- Высокая динамика пространственного развития и семантического наполнения.
- Высокая степень структурированности информационного пространства.
- Постоянное повышение уровня защищенности информационного пространства.
- Универсальность информационного пространства.
- Высокая потенциальная доступность; информационное неравенство.
- Высокая технологичность информационного пространства.
- Рассмотрим каждое из них более подробно.

Высокая динамика пространственного развития связана с постоянным совершенствованием информационно-телекоммуникационных систем и инфраструктуры в целом, повышением эффективности методов распространения информации, учитывающих тенденции информационных потребностей формируемого общества знаний, а также с лавинообразным нарастанием массы различной информации в современном обществе, получившее название «информационного взрыва».

Структурирование информационного пространства. Все связи и элементы современного информационного пространства, особенно в рамках сети интернет, должны быть представлены в формализованном виде, а процессы преобразования информации описаны на принятых к использованию языках программирования. При использовании способов структурирования информационного пространства создается возможность передачи информации пользователю в форме документов и, соответственно, манипулирования данными в ходе этого процесса с помощью различных программных и технических средств.

Сетевая структура электронной части информационного пространства способна формировать новые сегменты пользователей. Интернет дает возможность каждому пользователю сформировать собственное подпространство, где фактически он сочетает индивидуальные и групповые множества различных подпространств, событий, ситуаций, идентичности [9]. Часто используется собственный язык и распространение сугубо индивидуальных ментальных и познавательных моделей. Это создает объективные предпосылки для оказания мощного влияния на мировоззрение и поведение пользователей.

Язык манипуляции данными, первоначально созданный для обеспечения эффективных команд манипуляции сетевой системой базы данных, позволяет заинтересованным лицам выполнять над этой базой операции в целях формирования искаженной информации [10]. Это происходит в связи с тем, что электронные тексты способны быстро меняться по содержанию и по способу их представления. Так, на страницах интернет-сайтов происходит постоянное обновление контента (новостей и рекламы), появляются новые комментарии и оценки, меняется оформление, анимационные эффекты и многое другое. Это позволяет оперативно редактировать контент путем внесения самых разнообразных правок, а также изменять их структуру и комментировать каждый фрагмент текста отдельно («фрейминг»), появляется возможность организации диалога или дискуссии соответствующей направленности.

Так, например, компрометация, как один из видов информационных манипуляций, может реализоваться посредством несанкционированных изменений в контенте, что влечёт опасность принятия ошибочных решений. Недостоверная или модифицированная информация может скомпрометировать политическую организацию, даже если она была размещена непреднамеренно, но остается на ресурсе в дальнейшем. При этом смысл статей популярных сайтов может существенно влиять на общественное мнение [5].

Другим примером являются так называемые «сайты-клоны». Их целью является ввести пользователей в заблуждение. Сайт-клон является практически полной копией реального сайта организации. Меняется только контент. Сайт наполняется текстами, включающими нецензурную лексику, медийные материалы экстремистского или иного оскорбительного содержания.

Таким образом, структурирование современного информационного пространства позволяет с одной стороны, создавать и получать данные в строго формализованном виде, контролируя тем самым свое коммуникационное поле, а с другой стороны, такая формализация понижает критичность восприятия к получаемой информации и повышает уязвимость получателей информации к манипуляционному воздействию.

Повышение уровня защищенности современного информационного пространства. Вопросам его защиты уделяется особое внимание во всех государствах. В России существует специальный орган власти, функцией

которого является защита информационного пространства и противодействие наиболее серьезным информационно-политическим и, в более общем виде, информационным угрозам, которые часто именуются также «кибер-угрозами». Федеральная служба по техническому и экспортному контролю реализует политику России в данной сфере, а также координирует все взаимоотношения между ведомствами и контролирует все процессы в рамках обеспечения государственной безопасности информационных системах [3].

В информационном пространстве существует немало уязвимых мест для несанкционированного доступа к информационным ресурсам [7]. К числу основных каналов утечки информации относятся: акустические, электроакустические, оптико-электронные, параметрические, визуально-оптические, электромагнитные, компьютерные, материально-вещественные каналы утечки информации, переработка открытой информации для выявления закрытых сведений, человеческий фактор. С практической точки зрения деятельность по обеспечению информационно-политической безопасности может быть представлена как осуществление комплекса мероприятий, включающего:

- меры правового характера;
- организационные воздействия (совершенствование структуры и процесса функционирования соответствующих органов и учреждений);
- повышение эффективности работы правоохранительных, разведывательных и оперативно-розыскных структур;
- совершенствование контрразведывательных мероприятий;
- внедрение научных, технических, информационных, аналитических, кадровых, экономических (всех необходимых) мер для снижения интенсивности информационных угроз и их ликвидации.

К сожалению, реализация этих мероприятий не демонстрирует высокую степень эффективности вследствие высокой динамики развития информационных технологий.

Универсальность информационного пространства заключается в том, что в нем активно взаимодействуют в процессе коммуникации акторы, преследующие различные цели. Взаимодействие происходит по различным каналам:

- служб по связям с общественностью;
- СМИ различной формы собственности;
- общественных организаций;
- объединений политической направленности, действующих в национальных интересах;
- иных СМИ;
- профессиональных групп;
- отдельных граждан.

Это создает исключительно широкие возможности для воздействий не только конструктивного, но и деструктивного характера, формирует уникальные возможности для манипулирования, в том числе и политического, как коллективами людей, так и отдельными людьми [8]. Особое значение приобретают неинституционализированные каналы взаимодействия, а также новые формы коммуникационных технологий, например, социальные сети или сервисы мгновенного обмена сообщениями (мессенджеры) [4].

Высокая потенциальная доступность, с одной стороны, и информационное неравенство, с другой стороны. Информация считается доступной, когда, имеющие законное право доступа к ней граждане, могут беспрепятственно пользоваться этим правом. Не только получать информацию, но выполнять ряд других действий могут пользователи, с полномасштабным правом доступа. Доступность информации в электронной части информационного пространства обеспечивается, во-первых, соответствующих наличием аппаратно-программных средств и технологий, во-вторых, охватом регионов электронным информационным полем.

Подобная доступность имеет для России особое значение. Многие государственные и муниципальные услуги не могут предоставляться вследствие удаленности населенных пунктов от административных центров и учреждений и именно новые информационные технологии способны преодолевать преграды пространства и сокращать время передачи информации. Но в то же время создаются проблемы осуществления коммуникации между индивидуумами, регионами, гражданами и органами власти, так как на место прямого взаимодействия приходит опосредованное.

При этом следует учитывать, что интернет обладает не только неограниченными возможностями, но и создает благодатную почву для распространения различного рода ложной, вредной, разрушающей и деформирующей общественное сознание информации. При этом ее чрезвычайно сложно не только опровергать или верифицировать, но и просто объяснить ее подлинное значение молодому поколению, или исключить возможности доступа граждан к источникам подобного рода. Информация необходима для адаптации человека к быстро меняющемуся миру, что требует определенной культуры от каждого индивидуума, позволяющей отсеивать недостоверные, вредоносные, ложные источники и осмысливать проверенные. Новые возможности требуют большей ответственности в сфере получения, осмысления и оценки информации, так как это влияет на весь окружающий человека мир. В современной информационной среде мышление становится менее критическим, происходит унификация и стандартизации всех операций по обработке и восприятию информации [1].

Таким образом, разные потребители информации оказываются в неравных условиях – те, кто способен самостоятельно проанализировать полученные данные и отсеять очевидно ложные или опасные, оказываются в преимущественном положении по сравнению с теми, кто в силу технических характеристик или личностных качеств вынуждены доверять полученным сведениям. При этом в силу определенных психологических особенностей, описанных в работах по массовому сознанию, общественность, как правило, чаще поддается манипуляционному воздействию, если оно приобретает вид истерии [6].

Высокая технологичность информационного пространства обеспечивает высокую доступность к его информационным ресурсам, но создает риски использования отдельных элементов технологической и технической структуры информатизации для несанкционированных действий с информацией.

В целом, современное информационное пространство позволяет не только постоянно совершенствовать синергетическое взаимодействие миллионов участников (среди которых немалое число участников информационного процесса, которые распространяют намеренно ложную или искаженную информацию, исходя из заданным им целям), но и позволяет легко придавать частному формат всеобщего и в кратчайшие сроки превращать события, имеющие локальное значение, в события глобального масштаба. Под синергетическим взаимодействием в данном случае понимается переход от одного равновесного состояния в другое на более высоком организационном уровне. В экономике синергетический эффект рассматривается как фактор повышения рентабельности и увеличения прибыли за счет более эффективной организации производственной структуры и коммуникационных технологий. В отношении политических процессов синергия подразумевает неконтролируемое усиление политического эффекта принимаемых управленческих решений. Так, например, считается, что к разрушению СССР привел, в том числе, синергетический эффект: в сложившейся (в те годы нестабильной) федеративной системе за счет интенсивных преобразований во всех ее элементах, в ряде случаев происходило полное разрушение прежних механизмов и стали накапливаться многочисленные флуктуации от нормальных федеративных начал государственности.

СПИСОК ЛИТЕРАТУРЫ

1. Баранов Н.А. Технология постправды в эпоху демократии // Материалы XVI Санкт-Петербургской международной конференции «Региональная информатика (РИ-2018)», 2018. – С.186–188.
2. Борщенко, В.В. Особенности современного информационного пространства как среды формирования информационно-политических угроз. // Социально-гуманитарные знания. 2018. – № 4. – С. 216.
3. Дармокрик, В.Ф. Политическая безопасность в современной России: специальность 23.00.02 «Политические институты, процессы и технологии»: автореферат диссертации на соискание ученой степени кандидата политических наук; ФГОУ ВПО «Поволжская академия государственной службы имени ПА Столыпина». – Саратов, 2007.
4. Бутусов, А.В. Социальные сети как инструмент политического противоборства и информационных войн // Вестник Тамбовского университета. Серия: Общественные науки. №13. – 2018. – С. 71–75.
5. Кортунов, С.В. Мировая военно-политическая ситуация. Год 2025 // Международная жизнь. – 2010. – № 4. – С. 98–106.
6. Костюк, А.В. Подходы к информационно-психологической безопасности личности // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 3 / СПОИСУ, Санкт-Петербург. – 2017. – С. 52–54.
7. Кравченко, С.А., Подберезкин А.И. Диагностика доверия к безопасности России в условиях нового знания о рисках и уязвимостях // Гуманитарий Юга России, 2017. – Т. 23. – №1. – С. 27–41.
8. Middlestead, R.W. Digital Communications with Emphasis on Data Modems: Theory, Analysis, Design, Simulation, Testing, and Applications. Hoboken: John Wiley & Sons, Incorporated, 2017. – 328 p.
9. Wang, J., Kissel, Z. Introduction to Network Security: Theory and Practice – M.: Wiley, 2015. – 418 p.
10. Wang, Y., Zhong, G., Kun, L., Wang, L., Kai, H., Guo, F., Liu, C., Dong, X. The Performance Survey of in Memory Database // 2015 IEEE 21st International Conference on Parallel and Distributed Systems (ICPADS), 2015. – p. 815–820.

УДК 070.15

МОДЕЛИРОВАНИЕ ОБРАЗА ВАКЦИНАЦИИ ЯЗЫКОВЫМИ СРЕДСТВАМИ В ПРОПАГАНДИСТСКОМ ДИСКУРСЕ

Глущенко Олеся Анатольевна
Северо-Западный институт управления РАНХиГС
Средний пр., В.О., 57/43, Санкт-Петербург, 199178, Россия
e-mail: oag.kam@mail.ru

Аннотация. В статье систематизированы основные лингвистические средства, которые используются для выражения концепта вакцинации ее сторонниками и противниками в пространстве социальной сети ВКонтакте (https://vk.com/stopcoronavirusrf).

Ключевые слова: дискурс; концепт; пропаганда; семантика; вакцинация.

MODELING THE IMAGE OF VACCINATION BY LANGUAGE MEANS IN PROPAGANDA DISCOURSE

Glushchenko Olesya
The North-West Institute of Management of RANEPA
57/43 Sredny Av, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: oag.kam@mail.ru

Abstract. The article systematizes the main linguistic means that are used to express the concept of vaccination by its supporters and opponents in the space of the social network VKontakte (https://vk.com/stopcoronavirusrf).

Keywords: discourse; concept; propaganda; semantics; vaccination.

Введение. Массовая вакцинация против коронавируса стартовала в России с наступлением 2021 года и сразу же стала тем событием, в орбиту которого оказался вовлечен практически каждый дееспособный гражданин. Круг лиц, подлежащих вакцинации, все время расширяется за счет включения разных возрастных групп граждан. И сегодня вакцинация остается в центре внимания как активный информационный повод, по отношению к которому российское общество расколото и на фоне которого публично оцениваются достижения и провалы государственной социальной политики [1, 238-239]. Изучать дискурс вакцинации необходимо как для задач управления общественным мнением, так и для прогнозирования эмоций и настроения социальных групп. «Освещение этой эпидемии в средствах массовой информации позволяет выявить ценности, с одной стороны, определяющие картину мира наших современников, с другой – показывающие столкновения разных точек зрения» [2, 25].

Социальные сети предоставляют богатейший материал для контент-анализа проблемы вакцинации и моделирования концепта вакцинации в разговорной речи. В центре изучения социальная сеть ВКонтакте «СтопКоронавирус.РФ» (https://vk.com/stopcoronavirusrf), отражающая фрагмент пропагандистского дискурса вакцинации. При создании большей части комментариев к постам отправителями сообщения движут порыв и стремление быстро обозначить свою позицию в связи с актуальным информационным поводом, на страницах социальной сети противники и сторонника вакцинации ведут непрерывный спор, упорно доказывают свою правоту. Неслучайно дискурс пандемии исследователи сближают с политическим, властным дискурсом [3, 379]. Материалом исследования стали высказывания с ключевыми словами «вакцинация», «вакцина», «вакцинироваться», «прививка» и «прививаться» (общим объемом порядка 3500 предложений), извлеченные методом сплошной выборки из текстов комментариев к постам о вакцинировании и постам со статистикой по коронавирусу. Объект исследования – языковая репрезентация образа вакцинации в пропагандистском дискурсе определенной социальной сети. Предмет исследования – система языковых средств и их функциональная нагрузка в создании образа вакцинации.

Представления о вакцинации на языковом уровне реализуются в отдельных номинациях и словосочетаниях, в сфере сочетаемости в синтаксических конструкциях (в том числе в стилистических фигурах) и в тексте в целом.

1. Так, на лексико-семантическом уровне в качестве базовых предметных наименований выступают слова вакцинация, вакцина и прививка. Основными процессуальными обозначениями вакцинирования мы считаем глаголы вакцинироваться и колоть (с учетом производных вакцинироваться, ревакцинироваться, колоться, уколоться и др.). Иные номинации используются в двух случаях: 1) собственно синонимическая и контекстуально-синонимическая замена словами и словосочетаниями (в том числе с образным значением) с дополнительной стилистической коннотацией (вакса, химия, гадость, эта дрянь и др.); 2) видовые обозначения разновидностей вакцин: эпиваккорона, эпивака, ковивак, гамковидвак, спутник, спутник-лайт, спутник V и др.:

Так и от ковидлы умирают только с тяжелыми сопутствующими заболеваниями. Получается, что колоться – лишний риск (комментарий 27.08.2021) [Орфография и пунктуация примеров отредактированы];

Колоть химию каждые 6 месяцев – это издевательство над организмом (комментарий 08.08.2021);

Я колоться этой или какой-то другой бодягой колоться не собираюсь (комментарий 30.08.2021);

… подскажите, через какое время можно делать прививку от гриппа и пневмококка после вакцинации Спутником и СпутникЛайт? (комментарий 30.08.2021);

А вот с валидированными исследованиями безопасности и эффективности у всех российских вакцин беда. Только по Спутнику V на сегодня есть валидированные данные РКИ, но и то лишь на 18 тысячах добровольцах. По всем другим российским вакцинам, данные РКИ отсутствуют в принципе 😡 (комментарий 30.08.2021);

Алексей, не, россияне выбирают Спутник V, а вот «россияне», у которых мозг повернут на запад, нет, ждут пфайзер (комментарий 29.08.2021).

Особый интерес вызывает блок образных номинаций, где основой для переноса становятся функционал вакцины – противостоять болезни, защищать (защита от вируса, залог победы, спасительная вакцина и т.п.):

Вакцинация – это залог победы над COVID-19. □ Уважаемый Стопкороновирус, а почему Вы не озвучиваете (офф. каналы уже оповестили), что в Израиле началась 4-я 😊😂□ волна коронавируса (заболевают 10 тыс. чел.), и это несмотря на коЛЛективный иммунитет в Израиле!!!! (комментарий 25.08.2021);

Юлия, у вас, может быть, и свободны, а у нас, в Челябинске, ковидники открывают заново. Но сути это не меняет, низкая вакцинация = высокая летальность (комментарий 31.08.2021).

2. Анализ сочетаемости базовых предметных наименований показывает, что частотностью в контекстах и с субъектным (слова вакцина, прививка, вакцинирование в позиции субъекта действия), и с объектным (перечисленные слова в синтаксической позиции объекта действия) представлением вакцины обладают глаголы нескольких тематических групп: 1) названия действий в рамках медицинской процедуры (ставить, колоть(ся), делать, прививаться и др.); 2) названия насильственных действий (заставлять, принуждать, навязывать и др.); 3) названия

речевых действий (ругать, хаять, поносить, хвалить, восторгаться, критиковать, говорить, рассуждать и др.); 4) названия экономических и юридических действий, отношений и процессов (продавать, продвигать, гарантировать и др.); 5) названия исследовательских и производственных действий и процессов (изучить, исследовать, узнать, штамповать и др.); 7) названия бытийных состояний, обозначение существования (быть, существовать, иметься); 8) названия процессов применения без конкретизации сферы (использовать, применять и др.):

Делайте прививку и не бойтесь никаких цифр, в мире есть более опасные факторы риска...вы наверняка же не считаете погибших в ДТП, а странно, там риск смерти выше (комментарий 31.08.2021);

Желаем легкого течения болезни и скорейшего выздоровления. Жаль, что ни одна вакцина не может гарантировать 100% защиты (комментарий 09.08.2021);

Кто ж тебя так запугал, вирус достаточно не изучен, как и вакцина, и ты эту ахинею сейчас несешь с таким «авторитетным» умным видом, не стыдно нести эту пургу? (комментарий 08.08.2021);

За столько лет не могут лекарство от рака создать, а вакцины штампуют только в путь! (комментарий 30.08.2021).

Наблюдения за атрибутивной сочетаемостью базовых наименований показывает частотность характеристик принадлежности (отечественный, российский, наш, западный и т.п.), общих и аспектных оценок (хороший – плохой, качественный, недоработанный, проверенный и т.д.), порядка следования и количества (первая, вторая, единственная, разовая и др.) и степени обязательности (добровольный, принудительный, обязательный, поголовный, тотальный, всеобщий, добровольно-принудительный и т.д.):

Ответственность вместе с ними разделяет и наше государство, допустившее множество фатальных просчетов и не проводящее политику принудительной вакцинации (комментарий 27.08.2021);

Если вакцина является экспериментальной, то это называется испытательный этап. И каждый сам для себя решает быть подопытным объектом или нет (комментарий 28.08.2021);

Раньше делали прививки на долгие годы, а эти разовые прививки переняли у китайцев, как разовые носки (комментарий 25.08.2021).

Обобщение семантической основы сочетаемости показывает, что контекстуальные партнеры для нейтральных базовых наименований вакцины во многих случаях имеют смысловые коннотации, что создает эмоционально насыщенный контекст, а при экспрессивных наименованиях вакцины в этом случае степень экспрессивного накала высказывания возрастает:

Пробежался по другим гнилым комментам: практически все авторы громят российскую вакцину где-то из-за бугра, бодро подтявкивая друг другу☺ (комментарий 11.08.2021);

СтопКоронавирус.РФ, я в курсе, что за любое медицинское вмешательство надо подписывать свое согласие, а кто отвечает за побочки? Врачи шлюпают прививки даже кому их нельзя делать, как это тогда объяснить? И кто будет отвечать за это? (комментарий 30.08.2021).

Отметим, что исследование эмоционального пространства именно разговорных текстов в этой сфере позволяет выявить основные, так сказать, узлы конфликтности и прогнозировать вектор развития гражданской дискуссии. Кроме того, языковой материал определенным образом коррелирует с данными социальных опросов и отражает латентные аспекты обсуждаемой проблемы (делать или не делать отечественную прививку против ковида).

3. На уровне текста образ вакцины и вакцинации сопряжен с совершенно полярными представлениями: жизнь и спасение – смерть; уверенность и безопасность – страх; победа – провал и позор; панацея, суперсредство защиты от болезни – эксперимент, средство сомнительного качества. Вакцина и сам процесс вакцинации наделяются такими оценочными характеристиками в общественном сознании, которые позволяют разделять общество на своих и чужих, правильных и ошибающихся, лидеров и ведомых. По наблюдениям лингвистов, пандемия в качестве экстралингвистического фактора активизировала концептуальную метафору именно войны как своеобразный ответ человека на агрессивную внешнюю среду [4, 32].

В ряде контекстов пересекаются понятия вакцинирования и политической лояльности, с одной стороны, отвержения вакцинирования и идейный протест – с другой:

Привился в марте. Никаких побочных эффектов после прививки не было. Вакцинация против коронавируса – единственный способ защититься от этого ненасытного вируса убийцы!!! (комментарий 25.08.2021);

Мы вакцинировались, родственники тоже. Среди наших знакомых вакцинированных ВСЕ НОРМАЛЬНО. В вашем мире вакцинированные болеют и мрут (комментарий 25.08.2021);

…так вы уже трясетесь от страха, как сумасшедшие. Уже готовы колоть детей. Вам не так много осталось, вы прожили большую часть своей жизни. И плевать вы хотели на последствия, которые могут возникнуть у здоровых людей или детей (комментарий 09.08.2021);

Смертность стоит на одном месте. Такое ощущение, что людей хотят напугать, чтоб прививаться стали. Igor, для Вас – новая страшилка! (комментарий 07.08.2021);

… учитель, боящийся прививок, это нонсенс...учителя не должны приносить детям дремучесть, а если они антиваксеры, им не место в школе...да, знаю, с учителями проблема, но и это не учителя (комментарий 09.08.2021);

Сколько умерло от прививки??!!! Почему не включаете в статистику??!! Люди должны знать правду! (комментарий 09.08.2021);

Никита, тебе, самому не стыдно? Почему я должна быть испытуемой? Причем добровольно? Вакцину делают до ... А не во время такой эпидемии... (комментарий 02.-8.2021);

… а вам какое дело до «всех» других? Вам вкололи уже? Защитился сам – значит, бессмертен и спокоен (комментарий 08.08.2021).

Другими словами, активно распространяемый противниками вакцинации негативный опыт вакцинирования (часто вымышленный или основанный на слухах) с описанием серьезных побочных проявлений не только объясняется желанием поделиться информацией и предостеречь или напугать получателей информации, но и отражает общую неудовлетворенность российской действительностью, усиливающиеся протестные настроения на фоне единого события – вакцинации. В текстах антипрививочного посыла отвержение отечественных вакцин мотивируется недоверием к их качеству. Именование негативных эмоций в связи с вакцинацией соседствует в контексте с представлениями о медицинском и даже политическом произволе, принуждении к экспериментам на грани с насилием. За счет этого концепт вакцинации пересекается с концептом насилия, и на уровне языковой картины мира формируется образ принудительной вакцинации как проявления полицейского государства:

… не понимаю, почему вы боитесь здоровых людей, которые не хотят быть подопытными кроликами. Мы не антипрививочники. Прививки делали и себе и детям. Но сейчас не хотим участвовать в тестировании малоизученных вакцин. Почитайте инструкцию к вакцинам. Там много чего неизвестно и не проводилось. Не бойтесь, вы же привиты и теперь бессмертные. Но это не точно. Как и все связанное с вакцинацией (комментарий 10.08.2021);

… это я вам сочувствую, столько стараний зря пропадает, одни и те же персонажи агитируют и требуют всех насильно вакцинировать. Смеха у вас только не наблюдается. Сплошная агрессия (комментарий 10.08.2021);

То есть, оправдываясь сейчас, вы себя реально ПРИЗНАЛИ ВАКСАНУТОЙ :) А говорите, что в очереди за прививкой от глупости не были бы первой :) Или это прививка так на вас подействовала? Побочка такая, да?? (комментарий 06.08.2021);

Алана, да кого интересуют твои медотводы? Сказано колоться!! Мыши кололись, плакали, но продолжали жрать кактус... (комментарий 06.08.2021);

… идет подготовка нового мирового порядка, изучают вакцины на нас. Подбирают более действенную жидкость для не понятно пока чего. Потом узнаем. Скорее всего, эта «вакцина» – фундамент чего-то более страшного и бесчеловечного по отношению к нам (комментарий 30.08.2021).

На большинство развернутых положительных отзывов-комментариев о вакцинировании в течение первого часа поступает ряд отрицательных комментариев антипрививочной направленности, в которых активированы такие концепты, как безумие, угроза, обман и иные, что искусственно подпитывает антипрививочные настроения. Противники вакцинирования применяют самый широкой спектр характеристик крайних эмоционально-психологических состояний человека по сравнению с теми, кто поддерживает вакцинацию.

Заключение. Тема вакцинации в 2021 году по своей популярности не может быть ограничена исключительно медицинским дискурсом – она действительно стала политической. Следовательно, изучение всех аспектов этой темы значимо для прогнозирования социально-массовой дискуссии и управления общественным мнением и настроением.

СПИСОК ЛИТЕРАТУРЫ

1. Глущенко О.А. Организация агитационного дискурса вакцинации (на примере сообщества ВКонтакте «СтопКоронавирус.РФ») / Язык и речь в Интернете: личность, общество, коммуникация, культура: сборник статей V Международной научно-практической конференции. Москва, РУДН, 22-23 апреля 2021 г.: в 2 т. / под общ. ред. А.В. Должиковой, В.В. Барабаша. – М.: РУДН, 2021. 502 с. С 236-242.
2. Карасик В.И. Эпидемия в зеркале медийного дискурса: факты, оценки, позиции // Политическая лингвистика. – 2020. – № 2(80). – С. 25-34.
3. Новикова О.Н., Калугина Ю.В. COVID-19 в контексте современного состояния исследования дискурса о пандемии // Вестник Башкирского университета. – 2020. – № 2(Т.25) – С. 376-381.
4. Темиргазина З.Ф., Лучик М. Семиотика «пандемического» дискурса: «новояз» эпохи карантина // Филологические науки. – 2020. – № 6(1). – С. 30-38.

УДК 004.056.53

ЗАРОЖДЕНИЕ И РАЗВИТИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В РОССИИ

Егоров Константин Николаевич
Военный институт (военно-морской политехнический) ВУНЦ ВМФ «Военно-морская академия»
Кадетский бульвар, 1, Пушкин, Санкт-Петербург, 196601, Россия
e-mail: ekn.2017@yandex.ru

Аннотация. В статье рассмотрены основные моменты зарождения и развития системы защиты информации и государственных интересов в России в период с конца XV века по настоящее время.

Ключевые слова: защита информации; защита государственных интересов; информационная безопасность; нормативно-правовые акты.

GENERATION AND DEVELOPMENT OF INFORMATION PROTECTION SYSTEMS IN RUSSIA

Egorov Konstantin
Military Institute (Naval Polytechnic) Military Educational and Scientific Center of the Navy «Naval Academy»
1 Kadetsky Blvd, Pushkin, St. Petersburg, 196601, Russia
e-mail: ekn.2017@ yandex.ru

Abstract. Reviewed highlights of the origin and development of the system of information protection and public interest in Russia in the period since the end of the 15th century to the present.

Keywords: data protection; the protection of public interest; information security; regulatory legal acts.

Введение. Защита информации обеспечивается в любом государстве и в своем развитии проходит множество этапов в зависимости от потребностей государства, возможностей, методов и средств ее добывания, правового режима в государстве и реальных усилий его по обеспечению защиты информации. Информация, проникая во все сферы деятельности государства, приобретает конкретные политические, материальные и стоимостные выражения. На этом фоне в настоящее время все более актуальный характер приобретает задача обеспечения информационной безопасности России, как неотъемлемого элемента ее национальной безопасности, а защита информации превращается в одну из приоритетных государственных задач. Зарождение и развитие системы защиты информации в России проходило на протяжении многих веков.

В древних летописях нет упоминания о профессионалах, занимающихся определенными специфическими видами защиты информации или безопасности государства, специальных органах системы обеспечения безопасности государства, таких как разведка, контрразведка, специализированные органы внутренней и внешней политики государства. Для этого не хватало двух очень важных составных частей: развитой государственности и развитых внешнеполитических связей.

Политический аппарат централизованного государства в полной мере сложился только во второй половине XVI в. В конце XV в. был принят первый судебник централизованного государства – Судебник 1497 г.

В 1480 г. после окончания ига Золотой Орды над русскими княжествами (противостояние на реке Угре Московского и монголо-татарского войск) Иван III (1440–1505 гг.) принял титул «государя всея Руси», объединив под своим владением практически все земли, некогда управлявшиеся его отдаленными предками – киевскими князьями. В этот период защиту государственных интересов осуществлял государь с думой.

Во главе государства начиная с 1547 г. стоял царь. Изменение титула было важной политической реформой, целью которой было укрепление власти монарха. В конце XVI века сложился порядок утверждения и избрания царя на Земском соборе. Царь был главой государства, но правил он не единолично, а вместе с Боярской думой и Земскими соборами.

Система приказов – это система органов центрального отраслевого управления. Число приказов значительно увеличилось, выросли штаты, более четко определились компетенция, порядок делопроизводства. Продолжали действовать Посольский, Разрядный, Ямской приказы.

В сфере обеспечения внешнеполитической безопасности государства, а также разведывательной деятельности, наиболее важную роль играл Посольский приказ, который был в России первой самостоятельной государственной структурой, ведавшей всеми вопросами международных отношений и разведывательной деятельностью с 1549 г. При этом в этот период не делалось различий между дипломатической и разведывательной службой. В сравнении с предыдущим периодом функции по хранению дипломатических, секретных и других важных документов в этот период перешли непосредственно Посольскому приказу.

Царь Алексей Михайлович в 1654 г. создает при себе особую канцелярию – Приказ тайных дел. Этот приказ осуществлял наиболее важные дела в области безопасности государства в таких областях, как дипломатическая, военная, полицейская, финансовая и другие.

В регулярную практику секретной переписки были введены шифры.

Приказом тайных дел управлял дьяк, в распоряжении которого были подьячие.

Царь Алексей Михайлович, а также дьяк в «государевом имени» большинство приказаний отдавали в устной форме. Если приказ (указ) отдавался письменно, то его имел право читать только тот, кому он был непосредственно адресован. Прочитав секретное распоряжение, адресат тут же должен был вернуть его посланцу. А если посланец по каким-либо причинам не мог вручить его адресату, то должен был вернуть царю или своему высшему должностному лицу в нераспечатанном виде.

Подьячие Приказа тайных дел и посольские дьяки, ведавшие поддержанием связи с царскими представителями в зарубежных странах, осуществляли зашифрованную переписку. Ключ к расшифровке этих посланий не записывался, его заучивали наизусть. Существовали различные варианты секретного письма, и, как предписывалось по правилам конспирации, никто из подьячих не должен был знать все варианты тайнописи.

При царе, позднее императоре Петре I вышло Уложение о наказаниях уголовных и исправительных, от 15 августа 1845 года.

Это Уложение очерчивает такие нормативно-уголовные моменты, как государственная измена, защита государственной тайны, работа персонала с документами, содержащими государственную и коммерческую тайны, нарушение Уставов фабричной и заводской промышленности, тайное делопроизводство в коллегиях и канцеляриях.

По уложению 1845 г. государственной изменой признается:

1. Предательство государства, государя или правительства.

2. Поддержка подданными Российской Империи иностранных держав во время войны, а также передача им государственной тайны.

3. Пособничество во время войны неприятелю в военных или других действиях против отечества или союзников России:

- через явное участие в таких действиях;
- советом;
- открытием тайны;
- сообщение иных каких-либо сведений;
- воспрепятствование успехам Российского оружия или союзников России;
- сообщение противнику сведений о расположении и движении войск, состоянии армии, средствах нападения или обороны;
- помощь неприятельским лазутчикам.

За государственную измену уголовные нормативные акты предусматривали лишения всех прав на состояние (конфискация родового и «благоприобретенного» имущества) и смертную казнь.

Однако за разглашение государственной тайны (планы Российских крепостей, иных укрепленных мест, гаваней, портов арсеналов; опубликование этих планов без дозволения правительства) иностранным, хотя и не враждебным с Россией, государствам наказание было менее строгим – лишение всех прав состояния, телесные наказания и ссылка на поселение в отдаленные места Сибири.

Работа персонала с документами определялась Уложением 1845 г. статьями 447-455. Согласно этим статьям:

1. Чиновник при выходе из присутствия оставил вверенные ему дела и бумаги незапертыми (1-й и 2-й раз – выговоры, более или менее строгие, в 3-й раз – вычет от 1 до 6 месяцев из времени службы).

2. Утрата отправленных из присутственного места документов через частных людей или оставленных незапертыми дел и бумаг (вычет от 1 до 6 месяцев из времени службы, отрешение от должности). Утрата чиновником бумаг, вверенных ему по службе, если не было злого умысла, а только небрежность или неосторожность (выговор с внесением в послужной список, вычет от 3 месяцев до 1 года из времени службы, удаление от должности).

3. Разглашение дел, производимых в судебных и правительственных местах и за сообщение без дозволения какого-либо из актов или других принадлежащих к делам бумаг лицам посторонним, вопреки порядку для производства дел и хранения деловых бумаг установленному, виновный, если при том не было никакого иного преступления или злоупотребления, подвергается (1-й раз – замечание, выговор; 2-й раз – строгий выговор или вычет из времени службы от 3 месяцев до 1 года, 3-й раз – отрешение от должности).

4. Если от разглашения дел и сообщения бумаг произошли или долженствовали произойти какие-либо вредные последствия, то (1-й раз – строгий выговор с внесением в послужной список; 2-й раз вычет от 3 месяцев до 1 года из времени службы, удаление от должности).

5. Недозволенное (хотя и без корыстных или иных личных видов или побуждений) сообщение мнения судей или судебных актов, или других принадлежащих к делам бумаг лицам, прикосновенным к делу, непосредственно или через других, виновный в том чиновник подвергается строгому выговору с внесением или без внесения оного в послужной список, удалению от должности.

6. Злонамеренное открытие обвиняемому в преступлении судебных о нем актов или иных бумаг, и за сообщение ему сведений, могущих служить к сокрытию истины или к избежанию заслуженного им наказания – исключение из службы, наказание за укрывательство преступления.

7. Разглашение дел, подлежащих тайне, и недозволенное сообщение кому-либо бумаг, отмеченных надписью секретно, виновный подвергается, смотря по важности дела и произошедшем или долженствовавшим произойти от того последствиям, более или менее вредным – отрешение от должности, исключение из службы, заключение в смирительном доме от 6 месяцев до 1 года.

8. Открытие должностным лицом постороннему принадлежащего правительству или частному человеку секрета для производства каких-либо изделий, работ, машин, медицинских или иных составов. Виновный подвергается сверх вознаграждения за причиненные им убытки, отрешению от должности и заключению в тюрьме от 6 месяцев до 1 года.

9. Открытие с намерением государственной тайны иностранным правительствам – наказание за государственную измену. Обнаружение государственных тайн без намерения, а по неосторожности: исключается из службы; по важности дела и тайн – заключение в крепости от 6 месяцев до 1 года».

Во второй половине XIX в. в целом сохранились основные составляющие понятия «безопасность государства», заложенные во второй половине XVIII – начале XIX в.

Сложившаяся после 2017 года обстановка потребовала создания и совершенствования системы мер противодействия иностранным разведкам. Противоборство с техническими разведками зарубежных стран стало задачей государственной важности и одной из составных частей в общей системе мер по сохранению государственной и служебной тайны.

Рассмотрим историческое развитие системы информационной безопасности, начиная с 20-х годов и заканчивая современным состоянием.

В мае 1921 года Постановлением Малого Совнаркома от 5 мая 1921 года создан специальный отдел под руководством Г.И. Бокия, в октябре этого же года Декретом СНК утвержден перечень сведений, составляющих тайну и не подлежащих распространению. Сведения делились на военные и экономические.

В августе 1922 года Секретариат ЦК РКП(б) принял постановление «О порядке хранения и движения секретных документов», ноябрь - принято постановление «О порядке хранения секретных постановлений ЦК РКП (б)».

В 1926 году Совет народных комиссаров СССР утвердил «Перечень сведений, являющихся по своему содержанию специально охраняемой государственной тайной» (первый открытый перечень). Сведения делились на 3 группы: Сведения военного характера; Сведения экономического характера; Сведения иного рода.

В 1928 году приняты раздельные «Инструкция по секретному делопроизводству» и »Инструкция по шифровальному делопроизводству».

В 1929 году принята «Инструкция местным органам ОГПУ по наблюдению за состоянием секретного и мобилизационного делопроизводства учреждений и организаций».

В конце 1920-х годов проведена унификация состава секретных органов и установлена стандартная номенклатура должностей секретных аппаратов учреждений и организаций. В центральных аппаратах созданы секретные отделы, в остальных наркоматах - секретные части, а в главках, управлениях и отделах секретные части и секретные отделения соответственно.

Приказом НКО СССР № 024 1937 года утверждено «Положение о центральной военной цензуре РУ».

В 1939 году принимается Постановление СНК СССР № 884-145с «О реорганизации фельдъегерской связи НКВД СССР», в сентябре приказом НКО СССР введено «Наставление по секретному делопроизводству в РККА».

Период с 1941 по 1945 год требует отдельного рассмотрения, следует сказать, что и в это тяжелое для страны время уделялось большое внимание сохранению военной и государственной тайн.

В июне 1947 года выходит Постановление Совета Министров СССР «Об установлении перечня сведений, составляющих государственную тайну, разглашение которых карается по закону», в этом же месяце принят Указ Президиума Верховного Совета СССР «Об ответственности за разглашение государственной тайны и за утрату документов, содержащих государственную тайну».

Постановлением Совета Министров СССР от 01.03.48 утверждены «Перечень главнейших сведений, составляющих государственную тайну» и «Инструкция по обеспечению сохранности государственной тайны в учреждениях и на предприятиях СССР». В Инструкции 1948 года установлены три степени секретности (- С; - СС; - СС ОВ), порядок определения степени секретности сведений, проведена унификация названий секретных органов.

С начала 50-х годов начала складываться общегосударственная система противодействия иностранным техническим разведкам.

Это было связано с тем, что усилился интерес и устремленность иностранных разведок к военным и научно-техническим достижениям нашей страны. Это период становления и развития атомной промышленности, освоения новых видов вооружения, успехов в области ракетостроения и освоения космоса.

В 1953 году постановлением СМ СССР утверждена «Инструкция о порядке производства фотографических и кинематографических съемок и зарисовок на территории СССР иностранными туристами
и иностранцами», которая ограничивала и регламентировала эту деятельность.

Указом Президиума ВС СССР от 13 марта 1954 года был образован Комитет государственной безопасности (КГБ) при Совете Министров СССР.

В 1958 году Постановление ЦК КПСС «О мерах по сохранению государственной тайны».

Дальнейшая реорганизация органов, обеспечивающих сохранность государственной тайны в 80-е гг. связана с демократизацией общественной жизни в стране.

Основное значение в данный период имело постановление ЦК КПСС и СМ СССР от 1 октября 1970 г. «О мерах по усилению режима секретности». В соответствии с ним планировалось создание в стране системы комплексного противодействия иностранной технической разведке. В его развитие было принято постановление ЦК КПСС и СМ СССР «О мерах противодействия иностранным техническим разведкам» от 15 ноября 1976 г.

В ноябре 1976 г. выходит постановление ЦК КПСС и СМ СССР «О мерах по дальнейшему совершенствованию системы сохранения государственных секретов».

Указ Президиума ВС СССР от 77 января 1984 г. «О внесении изменений и дополнений в некоторые законодательные акты СССР об уголовной ответственности и уголовном судопроизводстве». Устанавливалась уголовная ответственность за передачу или собирание с целью передачи иностранным организациям или их представителям экономических, научно-технических или иных сведений, составляющих служебную тайну («секретно»), лицом, которому эти сведения были доверены по службе или стали известны иным путем.

В 1990 году Главным управлением по охране государственных тайн в печати при Совете Министров СССР утверждены «Методические рекомендации по охране сведений, подлежащих защите от разглашения в печати и других средствах массовой информации».

В апреле 1994 года Совместным Решением Государственной технической комиссии при Президенте РФ и Федерального агентства правительственной связи и информации при Президенте РФ утверждено «Положение о государственном лицензировании деятельности в области защиты информации».

Постановлением Правительства РФ в ноябре 1994 года утверждено «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

В апреле 1995 года выходит Постановлением Правительства РФ утверждено «Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»; в июне - Постановлением Правительства РФ утверждено «Положение о сертификации средств защиты информации»; в сентябре - Постановлением Правительства РФ утверждены «Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности»; в ноябре - Указом Президента РФ от 30 ноября 1995 года № 1203 утвержден «Перечень сведений, отнесенных к государственной тайне»

В начале 1996 года утверждено «Положение о Межведомственной комиссии по защите государственной тайны».

9 сентября 2000 года была принята Доктрина об информационной безопасности Российской Федерации.

Федеральный закон Российской Федерации № 149-ФЗ «Об информации, информационных технологиях и о защите информации» был принят 27 июля 2006 года.

Указом Президента РФ от 05.12.2016 года № 646 была принята Доктрина информационной безопасности РФ.

В настоящее время в России действуют более 140 нормативно-правовых акта различного уровня, регулирующих деятельность, как самого государства, так и его граждан в области защиты информации.

СПИСОК ЛИТЕРАТУРЫ

1. Бабаш А.В., Баранова Е.К., Ларин Д.А., Информационная безопасность. История защиты информации в России: Учебно-практическое пособие. – М.: Изд. центр ЕАОИ, 2012.
2. Григорьев С.М. Возникновение и история развития проблемы защиты информации. «Евразийский Научный Журнал» №4 2016.
3. Перечень основных действующих документов в области технической защиты информации. Режим доступа: http://www.Pandia.ru (Дата обращения: 29.06.2021).

УДК 004.056.5

ПРОБЛЕМЫ И МЕТОДЫ ЗАЩИТЫ ДАННЫХ В ОБЛАЧНЫХ СИСТЕМАХ ПРИ РАБОТЕ С ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

Игнатов Данил Юрьевич, Родин Владимир Николаевич
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: da.ignatoff@gmail.com, vl.rodin@mail.ru

Аннотация. В статье рассматриваются вопросы безопасности информации при использовании в организации облачных технологий работы с электронными документами, в частности, выявляются основные проблемы защиты данных в облачных системах хранения. Приведены основные методы защиты данных в облачных системах хранения, а также разработаны рекомендации пользователям облачных сервисов для обеспечения конфиденциальности, целостности и доступности их данных.

Ключевые слова: безопасность информационных технологий; облачные сервисы хранения данных; система электронного документооборота; электронный документ.

PROBLEMS AND METHODS OF DATA PROTECTION IN CLOUD SYSTEMS FOR WORKING WITH ELECTRONIC DOCUMENTS

Ignatov Danil, Rodin Vladimir
St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: da.ignatoff@gmail.com, vl.rodin@mail.ru

Abstract. The article discusses the issues of information security when using cloud technologies for working with electronic documents in the organization; in particular, the main problems of data protection in cloud storage systems are identified. The main methods of data protection in cloud storage systems are presented, as well as recommendations for users of cloud services to ensure the confidentiality, integrity and availability of their data are developed.

Keywords: information technology security; cloud data storage services; electronic document management system; electronic document.

В настоящее время методы работы с электронными документами приобретают все большую актуальность из-за внедрения компьютерных технологий в документооборот организации. В связи с переходом на электронный документооборот возникли два очень важных вопроса, касающиеся аспектов хранения и обработки электронных документов – это поиск оптимальной технологии, предоставляющей разнообразный функционал по работе с документами, а также выбор надежного, защищенного носителя информации, обеспечивающего её долговременное хранение.

Облачные системы работы с документами являются гибкими и масштабируемыми, обладают большим пулом вычислительных ресурсов. Из-за расширенного функционала облака злоумышленники могут использовать его не по назначению. Это вызывает различные проблемы с безопасностью облачных вычислений.

Защита данных в облачной системе электронного документооборота – это актуальная проблема для государственных и муниципальных учреждений России.

В современной России наблюдается процесс активного внедрения в систему государственного управления информационно-коммуникационных технологий, на базе которых образуется новая форма взаимодействия государства с бизнесом, гражданами, общественными объединениями и негосударственными некоммерческими организациями [1].

Динамично развиваются веб-сайты федеральных, региональных и муниципальных органов власти, объединенные в единый правительственный интернет-портал. Внедряются системы «Электронное муниципальное управление», «Электронное государственное управление регионом» и т.д.

В связи с активной «цифровизацией» государственных структур в будущем возможно повсеместное использование облачных систем электронного документооборота.

Таким образом, эффективность государственного управления может напрямую зависеть от информационных технологий, которые используются государственными предприятиями для работы с документами. Следовательно, защиту данных в современных информационных технологиях документооборота можно рассматривать как фактор политического риска в нашей стране.

Чем больше ИТ-специалистами разрабатываются более сложные и хитрые методы защиты информации, тем быстрее возникают новые виды атак, которые обходят современные средства защиты и ставят под угрозу всю безопасность компании.

Для российских организаций вопрос защиты электронных документов – один из краеугольных, особенно с учетом Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [2]. Безопасность – это «ахиллесова пята» облачных решений.

Проблемы безопасности, связанные с облачными вычислениями, делятся на две широкие категории: проблемы безопасности, с которыми сталкиваются поставщики облачных услуг, и проблемы безопасности, с которыми сталкиваются их клиенты. Однако ответственность распределяется. Поставщик должен обеспечить безопасность своей инфраструктуры и защиту данных приложений своих клиентов, в то время как пользователь должен принять меры для укрепления своего приложения, использования надежных паролей и мер аутентификации. Рассмотрим подробно основные проблемы защиты данных в облачных системах работы с электронными документами.

Данные в руках разработчика. Основной особенностью, подвергающейся постоянной критике является то, что при использовании виртуального программного обеспечения данные автоматически попадают в руки разработчика этого программного обеспечения. В последнее время относительно облачных сервисов стал популярен лозунг «это не облако, а просто чей-то компьютер». Большинство компаний, которые отказались от использования облака, сделали это из-за страха утечки своих данных [3]. То есть данные могут подвергаться риску неправильного обращения со стороны поставщика. Лучшая стратегия заключается в том, чтобы зависеть от шифрования файлов и более надежных паролей, а не от самих поставщиков облачных услуг. У большинства приличных компаний облачных хранилищ должны быть гарантированные протоколы по защите данных. Также в некоторых облачных системах появились очень надежные способы защиты информации, например, способ под названием «принцип нулевого разглашения», основанный на постоянном шифровании. Суть этой защиты сводится к тому, что только у организации есть ключ доступа к данным. То есть даже сам поставщик облачной услуги не будет иметь права доступа к системе.

Кибератака (DDoS-атаки, спуфинг, фишинг и др.). Кибератаки в наше время – одна из важных проблем, к которой облачная система крайне уязвима. Часто встречающимися, но в тоже время характерными угрозами для облачной технологии, являются DDoS-атаки, перехват личных данных для доступа к облаку через его API, несанкционированный захват данных, отправляемых и получаемых из облака, а также взлом целостной среды. Для

минимизации рисков и профилактики подобных угроз поставщики облачных услуг используют продвинутые средства безопасности. Но помимо современных решений требуется понимание сущности и природы такого вида атак [4].

Небезопасный интерфейс. Интерфейс облачной системы – важная составляющая программного обеспечения облака, с которой постоянно взаимодействует пользователь. От того, насколько хорошо проработаны механизмы интерфейса облачной системы, зависит безопасность данных. Для защищенной работы с программой поставщик должен уделить внимание механизму контролю доступа к системе, идентификации и аутентификации пользователя.

Потеря или утечка данных. Документы, хранящиеся в облаке, могут быть утеряны и без кибератак. Случайное удаление данных поставщиком облачных услуг или физическая катастрофа, например, пожар или землетрясение, могут привести к необратимой потере данных клиента. При этом вина может лежать не только на плечах провайдера. Если клиент зашифровывал свои данные перед загрузкой в облако и потерял свой ключ шифрования, то информация может быть безвозвратно утеряна.

Правительственное вторжение. Политическая ситуация в России последние несколько лет нестабильна. Блокировка правительством иностранных Интернет-ресурсов возможна в любое время и нет никаких гарантий, что этого не произойдет. Точный прогноз такого события составить невозможно. Вполне может возникнуть неожиданная ситуация, когда правительство заблокирует какой-либо иностранный сервис для русских пользователей, а ведь некоторые отечественные облачные системы электронного документооборота используют иностранные облачные платформы для хранения данных своих клиентов. Кроме того, данные своего клиента может предоставить сам провайдер вследствие государственного давления на него.

Технология общего пользования. Принцип работы в облачной среде – это общий пул ресурсов, т.е. провайдер предоставляет универсальную виртуальную инфраструктуру для множества пользователей. Неправильная конфигурация может привести к компрометации всего облака. Следовательно, если на одном из уровней возникает ошибка, это влияет на всю систему.

Кража учетных записей. Взлом учетной записи в облаке – это процесс, при котором злоумышленник похищает или захватывает учетную запись отдельного лица или организации. Это распространенная тактика в схемах кражи личных данных, когда злоумышленник использует украденную информацию учетной записи для осуществления злонамеренной или несанкционированной деятельности. Как только информация для входа в систему или другая конфиденциальная информация получена, злонамеренный пользователь может легко проникнуть в систему, поскольку сама система доступна из любого места.

При захвате учетной записи в облаке злоумышленник обычно использует взломанную электронную почту или другие учетные данные, чтобы выдать себя за владельца учетной записи. В основном, такие проблемы являются результатом неправильного обращения с механизмами защиты, например, при использовании слабых паролей управление ключами шифрования происходит ненадлежащим образом и др.

Злоупотребление облачными сервисами. Пользоваться облачными услугами могут нелегитимные организации. Их цель – использовать облачные системы для своих злонамеренных действий – рассылка спама, DDoS-атаки, запуск вредоносных программ и др. Провайдером необходимо распознавать подобных пользователей – изучать трафик, производить мониторинг облачной системы и т.д.

Злоумышленники среди сотрудников поставщика. Даже если сам провайдер услуг не имеет намерения вредить своему клиенту, под его управлением может работать сотрудник, который обрабатывает информацию пользователей. Такой сотрудник может в корыстных целях тайно использовать данные клиента.

Халатность сотрудников поставщика. Ошибки сотрудников остаются одной из самых больших проблем безопасности для всех систем, и эта угроза особенно опасна для облачных решений. Сотрудники могут подключаться к облачным решениям со своих мобильных телефонов, домашних планшетов и домашних ПК, что потенциально делает систему уязвимой для внешних угроз.

Отсутствие необходимых мероприятий по защите со стороны пользователя. Клиент облачных систем также должен принимать участие в обеспечении безопасности свои данных. Если офис и персональные компьютеры организации не защищены от проникновения посторонних лиц, то вина за утечку информации будет лежать на клиенте. К обязательным мероприятиям относятся обучение сотрудников безопасной работе с системой, мониторинг ошибок системы, тестирование на проникновение угроз и т.д.

Таким образом, облачные вычисления сталкиваются со многими проблемами безопасности как на стороне поставщика услуг, так и на стороне клиента. Основными проблемами являются нахождение данных в руках разработчика, кибератаки, небезопасный интерфейс, потеря или утечка данных, правительственные вторжения, принцип технологии общего пользования, кража учетных записей, злоупотребление облачными сервисами, злоумышленники среди сотрудников поставщика, халатность сотрудников поставщика, отсутствие необходимых мероприятий по защите со стороны пользователя.

Полноценная защита данных и полное соответствие требованиям ФЗ № 152 «О персональных данных», а также иным руководящим документам – задача не из легких и не из дешевых. Размещение базы данных организации с ее секретной документацией в облаке – шаг достаточно рискованный, требующий всестороннего анализа таких рисков и создания надежной системы защиты.

Безопасность облачных вычислений относится к широкому набору политик, технологий, приложений и элементов управления, используемых для защиты виртуальных IP, баз данных, приложений, услуг и инфраструктуры облачных вычислений.

Защита облачных систем – это часть компьютерной безопасности, сетевой безопасности и, в более широком смысле, информационной безопасности. Защита данных является одним из наиболее важных аспектов в проблеме безопасности облачных систем работы с документами. Чтобы повысить безопасность облачных сред, предприятиям необходимо использовать современные технологии и передовые методы для защиты своих данных.

Облачная система безопасности эффективна только при наличии правильных методов защиты. Архитектура облачной системы электронного документооборота должна распознавать проблемы, возникающие при управлении безопасностью [3]. Управление безопасностью решает эти проблемы с помощью средств управления безопасностью. Эти элементы управления введены в действие, чтобы защитить любые слабые места в системе и уменьшить эффект кибератак.

Облачные сервисы имеют высокую безопасность при должном ее обеспечении, однако при халатном отношении эффект может быть полностью противоположным. Решением является соответствие облака требованиям нормативных документов и стандартов в области обеспечения информационной безопасности.

В российском законодательстве пока нет стандартов, описывающих принцип построения защиты информации в облачных технологиях. Вследствие этого поставщики облачных услуг вынуждены сами выбирать способы защиты информации из огромного количества готовых решений, представленных на рынке. Но все средства защиты должны учитывать особенности облачной технологии [5].

Рассмотрим основные виды угроз информации в облачных системах работы с документами:

1. Традиционные атаки на программное обеспечение. Связаны с уязвимостью применяемых сетевых протоколов, операционных систем, модульных компонентов и т.д. Для защиты от таких атак применяют антивирусные программы, межсетевой экран (файервол), систему предотвращения вторжений (Intrusion Prevention System) и др.

2. Функциональные атака на элементы облака. Такие атаки связаны с многослойностью облака. Основным средством обороны от подобных кибератак выступает защита самого слабого места системы.

Для защиты от функциональных атак для каждого слоя облака нужно использовать специальные средства защиты: для прокси – защиту от DDoS-атак, для веб-сервера – контроль целостности страниц, для сервера приложений – экран уровня приложений, для слоя СУБД – защиту от SQL-инъекций, для системы хранения – резервное копирование и разграничение доступа.

3. Атаки на клиента. Этот тип атак очень распространен в веб-пространстве. Такие атаки также характерны для облачных систем, поскольку пользователи обычно получают доступ к облаку через веб-браузер. К этим видам атак относятся межсайтовый скриптинг, кража паролей, перехват веб-сессий, атака посредника и др.

В качестве защиты здесь традиционно используется аутентификация пользователя, в том числе эффективная двухфакторная аутентификация, шифрованное соединение с взаимной аутентификацией [6].

4. Атаки на средства виртуализации. К ним относятся атаки на гипервизор, на виртуальные машины при взаимодействии между узлами облака, а также атаки на системы управления облаком.

Такие угрозы в настоящее время крайне редки, сведения о подобных реальных атаках отсутствуют. Однако их стоит иметь в виду, поскольку они могут появиться в будущем в связи с популярностью виртуализации облаков [7].

5. Комплексные угрозы облачных сервисов. Причины такой угрозы – неправильный контроль инфраструктуры. Нет никаких гарантий, что все ресурсы облака посчитаны и в нем нет неподконтрольных виртуальных машин, не запущено лишних бизнес-процессов и не нарушена взаимная конфигурация слоев и элементов облака. Этот тип угроз связан с управляемостью облаком как единой информационной системой и поиском злоупотреблений или других нарушений в работе облака, которые могут привести к излишним расходам на поддержание работоспособности информационной системы.

Этот тип угроз более сложный и для него нельзя назвать универсальный способ защиты – методы безопасности в таком случае разрабатываются персонально для каждого облака.

Итак, проанализировав различные источники, посвященные безопасности данных в облачных технологиях работы с электронными документами, можно выделить следующие эффективные методы защиты данных в облачных технологиях работы с электронными документами:

1. Шифрование данных. Шифрование – один из самых эффективных методов защиты информации. Провайдер должен шифровать данные пользователя со стороны сервера, который находится в центре обработки данных. Существует несколько методов шифрования данных при использовании облачного хранилища. Шифрование на стороне сервера – шифрование, которое происходит после того, как система получает как данные, но до того, как данные записываются на диск и сохраняются, а также шифрование на стороне клиента – шифрование, которое происходит перед отправкой данных в облачное хранилище. Такие данные поступают в облачное хранилище уже в зашифрованном виде, но также подвергаются шифрованию на стороне сервера.

Важным остается вопрос о ключах шифрования. Хранить их на сервере облака не разумно, т.к. любой, у кого есть доступ к этому серверу, мог бы получить доступ к ключу, а значит и к зашифрованной информации. Физический

ввод ключа заменяется запросом, который облачный сервер отправляет внешнему источнику – серверу управления ключами

Важной составляющей для реализации такой защиты является раздельная эксплуатация облачного сервера и сервера управления ключами: если оба размещены у одного и того же провайдера облачных сервисов, то вся информация снова оказывается собранной в одном месте. Хорошей альтернативой является установка сервера управления ключами в локальном центре обработки данных или в качестве внешней услуги у другого сервис-провайдера [5].

2. Защита данных при передаче. Для безопасной обработки данных обязательным условием является их шифруемая передача. В целях защиты данных в публичном облаке используется туннель виртуальной частной сети, связывающий клиента и сервер для получения публичных облачных услуг. Туннель виртуальной частной сети способствует безопасным соединениям и позволяет использовать единое имя и пароль для доступа к разным облачным ресурсам. В качестве средства передачи данных в публичных облаках VPN – соединение использует общедоступные ресурсы, такие как Интернет. Процесс основан на режимах доступа с шифрованием при помощи двух ключей на базе протокола SSL.

3. Аутентификация. Аутентификация – это защита паролем. Например, используют токены. Токен – это электронный ключ, используемый для обеспечения информационной защиты, а также для идентификации пользователя. В системе аутентификации используют концепцию одноразовых паролей. Такие пароли могут использоваться только для одного сеанса аутентификации и могут быть ограничены определённым промежутком времени.

Основное отличие облачной инфраструктуры заключается в большой масштабируемости и более широкой географической распределенности. На первый план выходит использование для получения одноразовых паролей мобильных гаджетов. В самом простом случае одноразовый пароль будет сгенерирован специальным сервером аутентификации и выслан в SMS на мобильный телефон пользователя после ввода правильного статического пароля на странице доступа к облачному сервису.

Для прозрачного взаимодействия провайдера с системой идентификации при авторизации также рекомендуется использовать протокол LDAP и аутентификацию SAML.

4. Изоляция пользователей. Использование индивидуальной виртуальной машины и виртуальной сети. Виртуальные сети должны быть развернуты с применением таких технологий, как VPN, VLAN и VPLS.

Часто провайдеры изолируют данные пользователей друг от друга за счет изменения кода в единой программной среде. Этот подход имеет риски, связанные с опасностью найти дыру в нестандартном коде, позволяющем получить доступ к данным. В случае возможной ошибки в коде пользователь может получить доступ к информации другого пользователя.

Говоря о защите данных в облачных системах работы с документами, нельзя не упомянуть про сам центр обработки данных. Под центром обработки данных подразумевается совокупность серверов, размещенных на одной площади с целью повышения эффективности и защищенности.

Подсистема обеспечения безопасности центров обработки данных должна включать в себя следующие элементы: охранное видеонаблюдение; охранно-пожарная сигнализация; система контроля и управления доступом; система резервного копирования и восстановления данных; система защиты информации в центре обработки данных.

Помимо технологий защиты информации с точки зрения провайдера также важны методы предупреждения проблем со стороны клиента.

1. Провести анализ облачного рынка. Важно понять, какие облачные системы хранения существуют на предприятиях, кто их использует и каким образом. Доверять свои данные можно только надежным и проверенным компаниям, зарекомендовавшим себя на рыке. Чтобы не ошибиться в выборе, нужно учесть такие немаловажный факторы, как репутацию облачного сервиса, срок его работы, отзывы клиентов, а также его популярность.

2. Определить, как поставщик облачного хранилища решает вопросы конфиденциальности и безопасности. Условия соглашений об обслуживании – хорошая отправная точка для определения общих мер защиты, предлагаемых облачным провайдером. Но этого недостаточно для обеспечения безопасного хранения файлов. Поставщики облачных услуг часто обновляют условия обслуживания и пользовательские соглашения. Из-за этого можно легко пропустить незначительные изменения, которые могут оказать существенное влияние на конфиденциальность и безопасность.

Большинство соглашений не охватывают детали того, как поставщик облачного хранилища реализует безопасность, какие конкретные методы защиты он использует, и что происходит в случае поломки или нарушения. В результате важно точно определить политику и процедуры, что будет способствовать дальнейшим переговорам с провайдером.

3. Знать, какие средства защиты должны применяться. Шифрование в облачной среде является фундаментальным требованием. Важно знать, как поставщик облачного хранилища использует шифрование, в том числе при передаче данных между центрами обработки данных, серверами и устройствами хранения, а также кто контролирует ключи шифрования, как они применяются к конкретному набору данных.

Организация, использующая облачного провайдера, должна знать, у кого есть доступ к системам, какие существуют другие средства защиты – от DDoS-атак до системных ошибок в приложениях.

4. Использовать многофакторную аутентификацию на всех устройствах и системах. Широкое использование многофакторной аутентификации во много раз снижает риск получения доступа к системе или приложению для выпуска вредоносных программ или похищения ценной информации. Многофакторная аутентификация может помочь в защите конфиденциальных данных от хакеров, недовольных сотрудников и других инсайдеров, которые могут преднамеренно или непреднамеренно подвергать данные риску.

5. Проводить аудит и тестирование на проникновение угроз. Независимо от того, сотрудничает ли компания со сторонней фирмой по безопасности или полагается на внутренний персонал своей организации, эксперты считают, что необходимо провести тестирование на проникновение угроз, чтобы определить, правильно ли разработаны меры по облачной безопасности системы.

Организация должна регулярно проводить аудит возможностей облачной безопасности системы. Аудит должен включать анализ возможностей поставщиков, методы защиты должны соответствовать условиям безопасности.

Также для обеспечения безопасности следует проверять свои журналы доступа, чтобы быть уверенным, что только авторизованные сотрудники имеют доступ к конфиденциальным данным и приложениям в облаке.

6. Обеспечить физическую защиту своих данных. Физическая защита данных предполагает минимизирование рисков, связанных с проникновением посторонних лиц к компьютерам организации. Кроме контроля входящих и выходящий посетителей стоит закрывать кабинет на ключ и обязательно блокировать компьютер перед уходом.

Таким образом, мы рассмотрели основные методы защиты данных облачной системы работы с электронными документами, а также разработали рекомендации мер безопасности для пользователей таких систем.

В большинстве случаев проблемы с безопасностью не должны мешать организациям использовать облачные сервисы. Благодаря рекомендациям по облачной безопасности можно еще больше снизить риск таких угроз, пользуясь при этом всеми преимуществами облачных вычислений.

Как большие, так и малые организации тратят приличные ресурсы на разработку и усовершенствование систем защиты своих облачных продуктов. Выбирая облачный сервис, необходимо внимательно изучить все его характеристики, особенно это касается вопроса надежности.

В настоящее время методы защиты информации в облачных сервисах нуждаются в новом подходе. Защита должна включать целый комплекс мер, реализуемый с помощью слаженной работы поставщика и пользователя услуг.

Для реализации проекта еще на этапе его проработки нужно подключать профессиональных специалистов по безопасности, с помощью которых будут прорабатываться и предусматриваться соответствующие программно-аппаратные средства защиты, включая надежное шифрование, ограничение доступа к серверному оборудованию надежное протоколирование работы, регламентированный доступ на основе групповых политик и т.д.

Облачные вычисления – современный и перспективный способ работы с электронными документами, который активно развивается как за рубежом, так и в нашей стране. Безопасность облачных систем невозможна без использования профессиональных методов по защите данных – электронной подписи документа, шифрования информации, мониторинга угроз, аутентификации и идентификации пользователя, мониторинга угроз и прочих методов и программ защиты информации. Помимо применения инновационных методов защиты важно учитывать человеческий фактор. Необходимо, чтобы каждый участник процесса понимал свою роль в системе защиты данных, поскольку обеспечение безопасности облачной системы хранения электронных документов – это совместная работа провайдера и пользователя.

СПИСОК ЛИТЕРАТУРЫ

1. Овчинников С.А. Облачные технологии как фактор политического риска электронного государственного управления // Автоматика. Вычислительная техника. 2012. № 4. С. 187.
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (ред. от 2 июля 2021 г.) // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3451.
3. Котяшичев И. А. Защита информации в «Облачных технологиях» как предмет национальной безопасности // Молодой ученый. 2015. № 6. С. 30,35
4. Малков В.В. Защита информации в облаках для предпринимательского сектора // Вестник Московского государственного университета печати. 2015. № 15. С. 88.
5. Хажиева А.С. Принципы защиты информации в облаке // Информационная безопасность. 2016 № 9. С. 10-11.
6. Кодлов П.А. Проблемы безопасности облачных вычислений // Наука, техника и образование. 2016. № 12. С.56.
7. Гладкий М.В. Безопасность приложений на платформах облачных вычислений // Труды БГТУ. 2015. № 9. С 205.

УДК 351/354 (470)

СТРАТЕГИИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ 1997–2021

Казанцев Виктор Прокопьевич[1], Поправко Елена Александровна[2]

[1] Университет «РЕАВИЗ»

Калинина ул., 8/2А, Санкт-Петербург, 198099, Россия

[2] Военная академия материально-технического обеспечения имени генерала армии А.В. Хрулёва

Макарова наб., 8, Санкт-Петербург, 199034, Россия

e-mails: smunspb@rambler.ru, elena_popravko@mail.ru

Аннотация. В статье исследуются изменения о национальной безопасности Российской Федерации, отраженные в Концепции 1997 г. и Стратегиях 2009, 2015, 2021 гг. Авторы анализируют внешние и внутренние факторы, которые привели к изменению самого понятия «национальная безопасность». Исследуются новеллы, внесённые в Стратегию национальной безопасности 2021, а также практические трансформации приоритетов в данной сфере, которые обозначены в данном документе.

Ключевые слова: концепция; стратегия; национальная безопасность; угроза; национальные приоритеты; Российская Федерация.

NATIONAL SECURITY STRATEGIES OF RUSSIA OF 1997–2021

Kazantsev Viktor[1], Popravko Elena[2]
[1] University «REAVIZ»
8/2A Kalinina St, St. Petersburg, 198099, Russia
[2] Army General A.V. Khrulev Military Academy of Logistics
8 Makarova Emb, St. Petersburg, 199034, Russia
e-mails: smunspb@rambler.ru, elena_popravko@mail.ru

Abstract. In the article changes in the national security of the Russian Federation was researched as that reflected at the Concept of 1997 and the Strategies of 2009, 2015, 2021. The authors analyzed the external and internal factors that changed of «national security» definition, the novelties in the National Security Strategy 2021, as well as transformations of priorities in practice of national security, which are represent in this document.

Keywords: conception; strategy; national security; threat; national priorities; Russian Federation.

Введение. В 1991 г. после распада СССР для России начался новый этап развития, характеризующийся необходимостью решения ряда проблем социального, экономического и политического развития. Одной из таких проблем стала потребность в комплексном обеспечении безопасности личности, общества и государства в новых исторических условиях.

Проблема обеспечения национальной безопасности находится в центре внимания общественных и государственных деятелей, ученых, всех граждан России. Многоаспектность этой проблемы сделала ее предметом исследования специалистов многих отраслей научного знания: информатики, права, философии, социологии, политологии, психологии, экономики, экологии, биологии, здравоохранения и др.

Мультидисциплинарность проблемы национальной безопасности обусловлена рядом причин. Во-первых, теми кардинальными изменениями, которые произошли на рубеже XX и XXI вв. в общественно-политической сфере как в России, так и в мире в целом.

Распад СССР и реформирование всей системы общественных отношений в Российской Федерации распространился на все внутренние и внешние отношения страны, вызвав крупномасштабные последствия как положительного, так и отрицательного характера. В 1990-е гг. среди актуальных угроз безопасности личности, обществу и государству были резкий демографический спад, масштабное падение национального промышленного и сельскохозяйственного производства, стремительная экономическая дифференциация и увеличение числа тех, кто живёт за чертой бедности; криминализация общества; рост сепаратизма и национализма, что привело к вооруженному конфликту в Чечне.

Президент Российской Федерации В. В. Путин в 2008 г. так характеризовал этот период: «У нас, по сути, не было единой страны, у нас даже гимна своего не было на постоянной основе. У нас в каждом субъекте Федерации была своя конституция, отличающаяся от Конституции Российской Федерации, у нас не было единой страны. Мы восстановили территориальную целостность и единство нашего государства, мы воссоздали государство. Мы достигли уровня доходов граждан дореформенного периода и превысили его. И это, на самом деле, Самое главное – мы восстановили фундаментальные основы российской экономики на абсолютно новой рыночной базе. Мы уверенно превращаемся в одного из экономических лидеров» [1].

В 2000-е гг. добавляются внешние угрозы, связанные с мировым терроризмом, оранжевыми революциями, в том числе на постсоветском пространстве, формированием внесистемных оппозиций, развязыванием информационных войн. Становится очевидным, что тезис о «конце холодной войны», провозглашенный в 1989–1992 гг. оказался иллюзией.

Второй аспект, влияющий на мультидисциплинарность проблемы национальной безопасности связан с тем, что само понятие «национальная безопасность» находится в постоянной динамике. Оно отражает не только специфические признаки феномена, но и включает в себя то общее, устойчивое, что характерно для всех областей жизнедеятельности человека и общества. Это общее состоит в том, что безопасность как цель, условие и стратегия защиты от опасности нацелена, в конечном счете, на выживание социальной системы, личности, общества и государства.

Термин «национальная безопасность» появился в США. В 1904 г. его впервые употребил Президент США Т. Рузвельт (Th. Roosevelt) в Послании к Конгрессу (Annual State of the Union Address.). После принятия в 1947 г. закона «О национальной безопасности» (National Security Act of 1947) этот термин стал широко использоваться в политической практике не только США, но и его союзников по НАТО. В 1950 г. Г. С. Трумэн (H. S. Truman) впервые представил в

рамках Послания Конгрессу Стратегию национальной безопасности. Основанием для регулярного обновления Стратегий стал принятый в 1986 г. закон Голдуотера–Николса о реформе Министерства обороны (Goldwater–Nichols Defense Department Reorganization Act of 1986), который предусматривал ежегодную публикацию этого документа [6].

На практике США пересматривают Стратегию национальной безопасности каждые 3–5 лет. С 1986 г. он обновлялся 18 раз [см.: 6].

В Российской империи и СССР не было практики регулярного обращения главы государства (или в советский период – ещё и руководителя партии) к законодательным органам, в том числе с формулировкой стратегии национальной безопасности. Главным объектом и субъектом безопасности выступало государство, которое (как субъект национальной безопасности) через систему силовых структур стремилось к поддержанию, прежде всего, внешней и внутренней стабильности политического режима (объект национальной безопасности). Для этого создавались специальные органы: в Российской империи – Внутренняя стража, Отдельный корпус жандармов, в советский период – ВЧК–ОГПУ–НКВД–МГБ–КГБ. К концу существования Российской империи, как и к концу существования СССР, конфликт между обществом и государством выражался в противопоставлении деятельности органов политического сыска интересам общества. Подобный подход особенно проявился в годы перестройки, когда в стране развернулась кампания критики органов государственной безопасности, сопровождавшаяся их дискредитацией.

Одновременно возникает целый ряд общественных организаций и независимых исследовательских центров, специализирующихся на проблемах безопасности. Их состав рекрутировался из специалистов по проблемам военной политики, международных отношений, криминологии, бывших сотрудников правоохранительных органов и военнослужащих. Этот круг неправительственных организаций претендовал на независимую от государства разработку проблемы безопасности. Соответственно веяниям времени в сознании россиян появились новые виды угроз и новые составляющие национальной безопасности: экологическая, информационная, продовольственная и т. д.

В 1997 г. в Российской Федерации впервые была принята Концепция национальной безопасности. В 2000 г., вступив в должность Президента РФ, В. В. Путин утвердил новую редакцию данного документа. В 2009 г. была принята Стратегия национальной безопасности Российской Федерации до 2020 г., но реально документ действовал до 2015 г. В 2015 и 2021 гг. Россия обновила свою Стратегию национальной безопасности (см. таб. 1). Таким образом, практика представления Стратегий национальной безопасности (далее – Стратегия, Стратегии) в России включает 4 документа [см.: 3; 2; 5; 4]: 1997, 2009, 2015 и 2021 гг. (для сравнения: США с 1997 по 2021 г. обновляли аналогичный документ 10 раз [см.: 6]).

Таблица 1

Сравнительный анализ приоритетов в Стратегиях национальной безопасности России 2015 и 2021 гг. [5; 4]

Стратегия 2015	Стратегия 2021
I. Общие положения	I. Общие положения
II. Россия в современном мире	II. Россия в современном мире: тенденции и возможности
III. Национальные интересы Российской Федерации и стратегические национальные приоритеты	III. Национальные интересы Российской Федерации и стратегические национальные приоритеты
IV. Обеспечение национальной безопасности: – Оборона страны; – Государственная и общественная безопасность; – Повышение качества жизни российских граждан; – Экономический рост; – Наука, технологии и образование – Здравоохранение – Культура – Экология живых систем и рациональное природопользование – Стратегическая стабильность и равноправное стратегическое партнерство	IV. Обеспечение национальной безопасности: – Сбережение народа России и развитие человеческого потенциала; – Оборона страны; – Государственная и общественная безопасность; – Информационная безопасность; – Экономическая безопасность; – Научно-технологическое развитие – Экологическая безопасность и рациональное природопользование – Защита традиционных российских духовно-нравственных ценностей, культуры и исторической памяти – Стратегическая стабильность и взаимовыгодное международное сотрудничество
V. Организационные, нормативно-правовые и информационные основы реализации настоящей Стратегии	V. Организационные основы и механизмы реализации настоящей Стратегии
VI. Основные показатели состояния национальной безопасности	–

Обращают внимание в разделе II «Россия в современном мире: тенденции и возможности» изменения формулировок относительно целей взаимодействия страны с внешним миром. Вместо формулировки «равноправное стратегическое партнерство» (как желательный результат международного взаимодействия), которую содержала Стратегия 2015 г., Россия включила в число приоритетов достижение «взаимовыгодного международного сотрудничества» в Стратегии 2021 г. Это, видимо, отражает определенный качественный перелом в российском представлении о своём месте в мире: страна уже не ищет партнеров (хоть каких-нибудь), но очевидно осознает себя одним из лидеров международной политики [сравните: 5; 4].

Особого внимания заслуживает, несомненно, расстановка ключевых составляющих национальной безопасности в разделе IV. В Стратегии 2015 г. на первое место выносились проблемы обороны страны, в 2021 г. на первое место поставлен комплекс социальных и демографических проблем, названный «сбережение народа России и развитие человеческого потенциала» (см. таб. 1).

Есть изменения и в других частях этого раздела. Так, в 2015 г. Стратегия включала подраздел «Культура», который подразумевал, прежде всего, внутриполитические аспекты сохранения традиционных духовно-нравственных ценностей, и уже потом – противодействие внешним угрозам в данной сфере. При этом конкретные источники угроз российским духовно-нравственным ценностям не определялись.

В Стратегии 2021 г. на первое место вынесены именно внешние аспекты «угрозы утраты традиционных духовно-нравственных ориентиров и устойчивых моральных принципов», а также назван конкретный источник угрозы: «США и их союзников, а также со стороны транснациональных корпораций, иностранных некоммерческих неправительственных, религиозных, экстремистских и террористических организаций» [сравните: 5; 4].

Отдельным параграфом в Разделе IV в Стратегии 2021 г. впервые выделена информационная безопасность. В Стратегии 2015 г. проблемы информационной безопасности занимали весьма незначительное место и трактовались исключительно в технологическом аспекте: «Одним из главных направлений обеспечения национальной безопасности в области науки, технологий и образования является повышение уровня технологической безопасности, в том числе в информационной сфере» [5].

В Стратегии 2021 г. этот аспект национальной безопасности не только выделен в отдельное направление, но и раскрыт с точки зрения реальных угроз:

– личности: «снижение до минимально возможного уровня количества утечек информации ограниченного доступа и персональных данных, а также уменьшение количества нарушений установленных российским законодательством требований по защите такой информации и персональных данных», «обеспечение защиты конституционных прав и свобод человека и гражданина при обработке персональных данных, в том числе с использованием информационных технологий»;

– обществу: «обеспечение приоритетного использования в информационной инфраструктуре Российской Федерации российских информационных технологий и оборудования, отвечающих требованиям информационной безопасности», «развитие взаимодействия органов публичной власти, институтов гражданского общества и организаций при осуществлении деятельности в области обеспечения информационной безопасности Российской Федерации», «противодействие использованию информационной инфраструктуры Российской Федерации экстремистскими и террористическими организациями, специальными службами и пропагандистскими структурами иностранных государств для осуществления деструктивного информационного воздействия на граждан и общество»;

– государству и его отдельным институтам: «предотвращение и (или) минимизация ущерба …, связанного с осуществлением иностранными государствами технической разведки»; «укрепление информационной безопасности Вооруженных Сил, других войск, воинских формирований и органов, а также разработчиков и изготовителей вооружения, военной и специальной техники» [4].

Эти формулировки позволяют увидеть, что понимание информационной безопасности в Стратегии 2021 г. включает в себя технологический и содержательный аспект. Технологический связан с надежностью технического обеспечения доступа для россиян к информационным ресурсам и технологиям, с одной стороны, а также с повышением контроля в данной сфере, гарантирующим, что персональная информация, личная, семейная, коммерческая и государственная тайна будут доступны только тем, кто имеет на это право по закону, с другой.

Отдельно раскрываются проблемы содержательной интерпретации информационной безопасности. Этому аспекту уделяется ключевое внимание, что подтверждается и освещением данных вопросов в других разделах Стратегии 2021 г., например, в п.п. 19–20 раздела II «Россия в современном мире: тенденции и возможности»:

«19. Все более актуальной становится проблема морального лидерства и создания привлекательной идейной основы будущего мироустройства. На фоне кризиса западной либеральной модели рядом государств … проводятся информационные кампании, направленные на формирование враждебного образа России. …

20. Недружественные страны пытаются использовать имеющиеся в Российской Федерации социально-экономические проблемы для разрушения ее внутреннего единства, инспирирования и радикализации протестного движения, поддержки маргинальных групп и раскола российского общества. Все более активно применяются непрямые методы, направленные на провоцирование долговременной нестабильности внутри Российской Федерации».

Интересно, что впервые после проведённой в 1991 г. деидеологизации и декоммунизации Россия в Стратегии 2021 г. открыто признала, что информационная безопасность зависит от идеологии («привлекательной идейной основы

будущего мироустройства»), а информационные войны ведутся не только в сфере доступа к технологиям (когда «запрещается деятельность российских средств массовой информации и использование российских информационных ресурсов»), но в сфере содержательных контентов – фактически, в сфере идеологии [4]. Это свидетельствует о том, что внутриполитические тенденции последнего времени, в том числе «тренд» на патриотизм, (который В. В. Путин провозгласил единственно возможной идеологией для демократического и правового государства), стали одной из ключевых причин очередного обновления Стратегии национальной безопасности Российской Федерации и оказали существенное влияние на ее содержание.

Заключение. Проделанный нами анализ динамики представлений о национальной безопасности в России позволяет сделать ряд выводов. Заимствовав традицию создания и публичного представления Стратегий национальной безопасности из практики США, российские Президенты сумели сделать этот документ одним из ключевых в Российской политике. В нем не только декларируются, но действительно находят отражение изменения в представлениях государства (как одного из социальных институтов) и общества в целом о приоритетных направлениях развития, о характере и источниках внутренних и внешних угроз, а также о способах поддержания стабильности российского социума. Динамика приоритетов национальной безопасности, как они формулируются в Концепции 1997 г. и Стратегиях 2009, 2015 и 2021 гг., свидетельствует о том, что документы отражают особенности положения России в мире, в том числе усиление позиций страны в международном политическом пространстве. Впервые в Стратегии 2021 г. особое внимание уделяется вопросу информационной безопасности, ее технологическим и содержательным аспектам, что отражает значимость соответствующих проблем для решения задачи достижения стабильности российского социума. Также в контексте обсуждения путей достижения информационной безопасности фактически признана связь данной проблемы с уровнем идеологического единства общества.

СПИСОК ЛИТЕРАТУРЫ

1. Путин В. В. Я получил подарок от народа и от Господа – работать главой России // Комсомольская правда. 2008. 15 февраля. – Доступно из URL: https://www.kp.ru/daily/24049/102749/ (Дата обращения: 20. 07. 2021).
2. Указ Президента РФ от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года». – Доступно из URL: https://docs.cntd.ru/document/902156214?marker=6540IN (Дата обращения: 20. 07. 2021).
3. Указ Президента РФ от 17 декабря 1997 г. № 1300 «Об утверждении Концепции национальной безопасности Российской Федерации» (в ред. от 10 января 2000 г.). – Доступно из URL: https://docs.cntd.ru/document/901751578 (Дата обращения: 20. 07. 2021).
4. Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации». – Доступно из URL: http://www.consultant.ru/document/cons_doc_LAW_389271/ (Дата обращения: 20. 07. 2021).
5. Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации». – Доступно из URL: http://www.consultant.ru/document/cons_doc_LAW_191669/ (Дата обращения: 20. 07. 2021).
6. National Security Strategy Archive. – Доступно из URL: https://nssarchive.us/ (Дата обращения: 20. 07. 2021).

УДК 004.891.3

ОСОБЕННОСТИ ЛИЧНОСТИ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Корх Ирина Анатольевна
Кубанский государственный технологический университет
Московская ул., 2, Краснодар, 350072, Россия
e-mail: Aia2004@inbox.ru

Аннотация. В работе предлагается использовать определение акцентуации личности для прогнозирования подверженности человека конкретным атакам методами социальной инженерии, что является научной новизной исследования. Практической новизной является использование результатов для повышения уровня доверия к персоналу и информационной безопасности организации путем автоматизации и персонификации проведения всех видов инструктажей на рабочем месте. Представленное решение позволит улучшить качество проведения обучения сотрудников, повысить уровень осведомленности в вопросах информационной безопасности, что полностью соответствует требованиям стандарта ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. Требования.

Ключевые слова: акцентуации личности; информационная безопасность; социальная инженерия; повышение осведомленности; доверие.

PERSONALITY TRAITS IN INFORMATION SECURITY

Korkh Irina
Kuban State Technological University
2 Moskovskaya St, Krasnodar, 350072, Russia
e-mail: Aia2004@inbox.ru

Abstract. The paper proposes to use the definition of personality accentuation to predict a person's susceptibility to specific attacks by social engineering methods, which is the scientific novelty of the study. The practical novelty is the use of the results to increase the level of trust in the personnel and information security of the organization by automating and personalizing all types of briefings at the workplace. The presented solution will improve the quality of employee training,

increase awareness of information security issues, which fully complies with the requirements of GOST R ISO/IEC 27001-2006 Information Technology standard. Methods and means of ensuring security. Information security management system. Requirements.

Keywords: personality accentuations; information security; social engineering; awareness raising; trust.

Введение. Вопросы информационной безопасности не ограничиваются техническими направлениями исследований и обязательно должны учитывать «человеческий фактор» при прогнозировании рисков, а также построении моделей угроз и нарушителя. Обоснованием такой необходимости является признанный многими практическими специалистами тезис: «самая большая угроза и самая действенная атака проводится на человека и с помощью человека». В таких условиях становится очевидной актуальность проблемы доверия к обеспечению информационной безопасности организаций различных форм собственности, с учетом атак социальной инженерии и влияния психологии личности на принятие управленческих решений в сфере безопасности личности, общества и государстве в целом.

В работе предлагается применение методики «7 радикалов» В.В. Пономаренко [1]. Выбор обусловлен необходимостью дальнейшей автоматизации и внедрения в организацию, что не позволило применять в полной мере метод А.Е. Личко и Е. Леонгарда [2, 3]. В психологии, для определения сильных и слабых сторон личности используют совмещенный опросник Леонгарда-Шмишека. Применение его для целей информационной безопасности также затруднено.

Виды атак, проводимых методами социальной инженерии, их характеристики и направления нейтрализации, проанализированы в предыдущих работах автора [4] и других исследователей [5].

На основе вышесказанного предлагается применить методы и технологии социологии, психологии личности и педагогики к информационной безопасности для формирования методики проведения персонифицированного инструктажа.

Использование методики «7 радикалов» в информационной безопасности не является новизной. Она внедрена в некоторые DLP-системы, оснащенные модулями психолингвистики [6]. Однако, в данной работе такой подход без модификации не приемлем, поскольку критериями определения ведущего радикала являются:

– внешность (нельзя использовать для автоматизации анализ жестов, походки, мимики);

– особенности поведения (привычки требуют длительного изучения, что не соответствует целям, поставленным в работе);

– оформление пространства (нет возможности использовать знания, поскольку инструктаж проводится для вновь набираемых сотрудников и нет сведений об их предпочтениях в организации рабочего места).

В качестве модернизации, была произведена корреляция типа радикала с подверженностью этого типа определенным атакам социальной инженерии. На первом этапе испытуемым предлагалось пройти тестирование для определения акцентуации характера. Результат тестирования для десяти случайно выбранных испытуемых приведен на фрагменте таблицы 1. В таблице указана интерпретация результата для ранжирования радикалов. Общее количество образцов 247. Результаты каждого были обработаны аналогично представленным данным.

Таблица 1

Результаты тестирования и таблица ранжирования радикалов по частоте проявления

	Номер вопроса								
	1	2	3	4	5	6	7	8	
1	Гипертимный	Тревожный	Эмотивный	Паранойяльный	Эпилептоидный	Эмотивный	Эмотивный	Эпилептоидный	Пар
2	Шизоидный	Паранойяльный	Эмотивный	Паранойяльный	Эмотивный	Паранойяльный	Паранойяльный	Эпилептоидный	Пар
3	Истероидный	Эмотивный	Паранойяльный	Тревожный	Эпилептоидный	Гипертимный	Эпилептоидный	Паранойяльный	Эпи
4	Паранойяльный	Эмотивный	Эмотивный	Гипертимный	Гипертимный	Паранойяльный	Шизоидный	Тревожный	Пар
5	Паранойяльный	Эмотивный	Шизоидный	Гипертимный	Эпилептоидный	Эмотивный	Шизоидный	Паранойяльный	Пар
6	Эмотивный	Эмотивный	Эмотивный	Гипертимный	Паранойяльный	Эмотивный	Шизоидный	Эпилептоидный	Пар
7	Истероидный	Эмотивный	Эмотивный	Эмотивный	Гипертимный	Эмотивный	Шизоидный	Эпилептоидный	Пар
8	Гипертимный	Эмотивный	Паранойяльный	Паранойяльный	Эпилептоидный	Эмотивный	Паранойяльный	Эпилептоидный	Пар
9	Паранойяльный	Паранойяльный	Эмотивный	Эмотивный	Эмотивный	Эмотивный	Эмотивный	Паранойяльный	Пар
10	Шизоидный	Шизоидный	Паранойяльный	Шизоидный	Эмотивный	Эмотивный	Эмотивный	Эмотивный	Эмо
...									

	Гипертимный	Шизоидный	Истероидный	Паранойяльный	Эмотивный	Эпилептоидный	Тревожный
1	1	0	0	3	6	2	1
2	0	2	0	6	3	2	0
3	1	1	2	2	1	4	2
4	2	2	1	3	3	0	2
5	1	3	1	3	4	1	0
6	1	1	1	3	5	2	0
7	1	2	2	3	4	1	0
8	1	0	0	5	2	4	1
9	0	2	0	4	7	0	0
10	0	3	0	1	7	2	0
...	0	0	0	0	0	0	0

На рис. 1 представлено распределение по частоте появления радикалов в результатах тестирования. Анализ данных показывает, что наибольшее количество сотрудников из исследуемой выборки, имеют радикал Эмотивный и Паранойяльный.

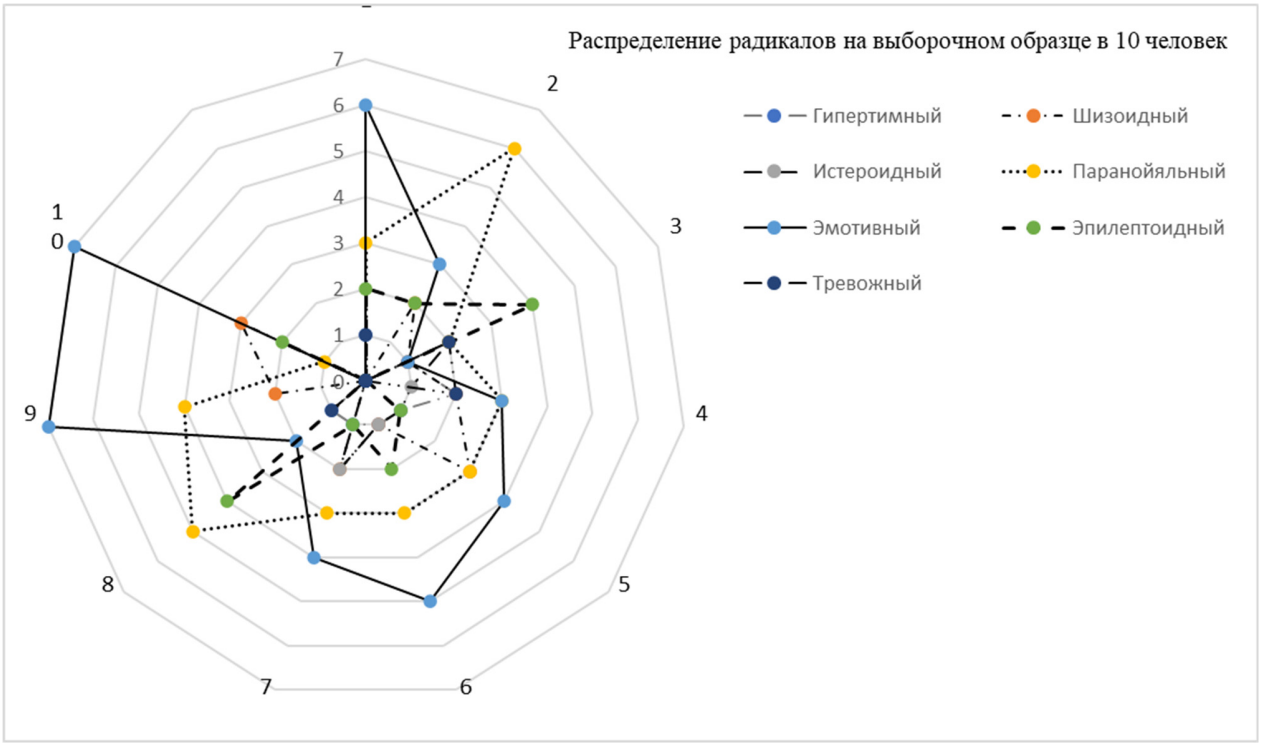


Рис. 1. Ранжированная выборка радикалов.

Заключение. Вторым этапом исследования являлось изучение подверженности каждого типа радикала атакам социальной инженерии. Данная часть исследования продолжается, но уже сейчас можно с уверенностью сказать, что для личностей с эмотивным радикалом наиболее опасным является метод воздействия «дорожное яблоко». Конечным результатом представляется сводная таблица методов и радикалов, которая будет положена в основу автоматизации и персонификации инструктажа по информационной безопасности. Математической основой моделирования выбрана нечеткая и многозначная логика, рассматриваемая в работах [7]. Аппарат алгебры логики представляет интерес для решения, данный задачи, поскольку поведенческие характеристики человека не всегда подчиняются здравому смыслу и для моделирования системы с количеством неизвестных больше четырех классические подходы не дают достоверных результатов.

Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ) №26/2020.

СПИСОК ЛИТЕРАТУРЫ

1. Практическая характерология: методика 7 радикалов / В.В. Пономаренко. – Москва: Издательство АСТ, 2019. -224с. – (Практический тренинг).
2. Овчинников, Б. В. Проблема диагностики акцентуаций личности: опросник акцентуированных радикалов / Б. В. Овчинников, И. В. Тюряпина // Вестник Южно-Уральского государственного университета. Серия: Психология. – 2016. – Т. 9. – № 1. – С. 27-31. – DOI 10.14529/psy160103.
3. Духновский, С. В. Оценка кадровых рисков как фактор профилактики коррупционного поведения государственных гражданских служащих / С. В. Духновский, В. И. Яхонтов // Проблемы противодействия коррупции на государственной и муниципальной службе и пути их решения в современной России : Материалы участников Круглого стола с международным участием, Ростов-на-Дону, 16–17 февраля 2018 года. – Ростов-на-Дону: Южно-Российский институт управления - филиал федерального государственного бюджетного образовательного учреждения высшего профессионального образования Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (ЮРИУФ РАНХиГС), 2018. – С. 366-378.
4. Власенко, А.В. Социотехнические и гуманитарные аспекты доверия к обеспечению информационной безопасности / А.В. Власенко, И.А. Корх // Социотехнические и гуманитарные аспекты информационной безопасности: Материалы II Всероссийской научно-практической конференции. Пятигорск: ПГУ, 2020. – с.45-50.
5. Исследование механизмов социальной инженерии и анализ методов противодействия / В. Ю. Евглевский, М. М. Путято, А. С. Макарян, И. В. Володин // Электронный сетевой политематический журнал «Научные труды КубГТУ». – 2021. – № 2. – С. 57-68.
6. Принцип работы DLP-системы [Электронный ресурс]: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/printsip-raboty-dlp-sistemy/ (Дата обращения 28.08.2021).
7. Л. А. Лютикова, М. А. Шогенов, «Метод обнаружения выбросов в данных на основе многозначной логики предикатов», Известия Кабардино-Балкарского научного центра РАН, 2019, 6, 67–74.

УДК 378.6

ОСОБЕННОСТИ ФОРМИРОВАНИЯ ЭФФЕКТИВНОЙ СИСТЕМЫ ПОДГОТОВКИ КАДРОВ ДЛЯ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ, СПЕЦИАЛИЗИРУЮЩИХСЯ НА ПРЕДОТВРАЩЕНИИ, ВЫЯВЛЕНИИ, РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Примакин Алексей Иванович
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: primakin@mail.ru

Аннотация. Представлен опыт решения базовых задач по основным направлениям деятельности кафедры специальных информационных технологий Санкт-Петербургского университета МВД России, позволяющий повысить эффективность подготовки кадров для ОВД Российской Федерации, специализирующихся на предотвращении, выявлении, раскрытии и расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

Ключевые слова: подготовка специалистов; кибербезопасность; предотвращение преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

FEATURES OF FORMATION OF THE EFFECTIVE SYSTEM OF TRAINING FOR THE LAW ENFORCEMENT AGENCIES OF THE RUSSIAN FEDERATION SPECIALIZING IN PREVENTION, IDENTIFICATION, DISCLOSURE AND INVESTIGATION OF THE CRIMES COMMITTED WITH USE OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Primakin Alexey
St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mail: a.primakin@mail.ru

Abstract. The experience of the solution of basic tasks of the main activities of department of special information technologies of the St. Petersburg university Ministry of Internal Affairs of the Russian Federation allowing to increase efficiency of training for Department of Internal Affairs of the Russian Federation, the crimes specializing in prevention, identification, disclosure and investigation committed with use of information and telecommunication technologies is presented.

Keywords: training of specialists; cybersecurity; Prevention of crimes committed using information and telecommunications technologies.

Введение. Актуальность темы статьи связана, прежде всего, с задачами, которые на расширенном заседании коллегии МВД России (3 марта 2021) поставил Президент В.В. Путин перед органами внутренних дел на ближайшее будущее. Динамика преступлений в сфере информационных технологий за последние шесть лет их число возросло более чем в десять раз. Криминальные деяния, совершенные с использованием IT-технологий, составляют всё большую долю в общей структуре преступности. Сегодня она достигла двадцати пяти процентов. Ежегодный прирост фиксируется за последние несколько лет, что отражает глобальные тенденции, связанные с «уходом в онлайн» многих сфер жизнедеятельности общества [1].

Задача органов внутренних дел – эффективно ответить на этот криминальный вызов, защитить граждан и добросовестный бизнес, который активно осваивает цифровое пространство. Для этого важно своевременно информировать людей о способах защиты от мошенников, повышать профессиональную подготовку и техническое оснащение органов внутренних дел.

Кроме этого, ранее, в Приказе МВД России от 25 ноября 2019 г. № 878 «Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. № 3км 27 Декабря 2019 «О мерах по совершенствованию организации работы по выявлению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-телекоммуникационных технологий» отмечалось, что «Приобретают все большую актуальность вопросы совершенствования кадровой политики и организации подготовки для органов внутренних дел специалистов в сфере информационных технологий» [2].

Санкт-Петербургский университет МВД России в период с 22 по 23 апреля 2021 г. посетили представители ДИТСиЗИ и ГИАЦ МВД России для ознакомления с процессом подготовки специалистов по защите информации. Оценивались: кадровый потенциал кафедры специальных информационных технологий (СИТ), материально-техническое обеспечение, научно-исследовательская и редакционно-издательская работа, уровень подготовки курсантов и слушателей (III и IV курсы), обучающихся по специальности 10.05.05 – «Безопасность информационных технологий в правоохранительной сфере» (БИТ). Рассматривались вопросы организации и совершенствования на

базе Санкт-Петербургского университета МВД России комплексной системы подготовки, переподготовки и повышения квалификации специалистов в сфере информационных технологий, связи и защиты информации (в рамках исполнения подпункта 16.2 решения коллегии МВД России от 5 декабря 2018 г. № 2 км, объявленного приказом МВД России от 18 января 2019 г. № 20, и в соответствии с решением Министра внутренних дел Российской Федерации от 5 июня 2019 г.).

По результатам инспектирования представителями ДИТСиЗИ и ГИАЦ МВД России процесса подготовки специалистов по защите информации кафедрой СИТ разработан план повышения эффективности реализации основной образовательной программы высшего образования по специальности БИТ.

Таким образом, цель статьи – представить опыт решения базовых задач по основным направлениям деятельности кафедры СИТ Санкт-Петербургского университета МВД России, позволяющий повысить эффективность подготовки специалистов для ОВД, специализирующихся на предотвращении, выявлении, раскрытии и расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

1. Учебная и учебно-методическая работа.

Разработаны рабочие программы учебной дисциплины «Основы кибербезопасности» для всех специальностей (направлений подготовки) в Санкт-Петербургском университете МВД России набора 2021 года.

Актуализирована основная профессиональная образовательная программа (ОПОП) по специальности БИТ с учетом усиления практической направленности и формирования у обучающихся компетенций, необходимых для успешного осуществления профессиональной деятельности.

Подготовлен пакет документов, необходимых для проработки вопроса об открытии новой специализации «Компьютерная экспертиза» в рамках специальности БИТ и реализации ее на базе университета с 2022/2023 учебного года (планируемые результаты освоения соответствующей ОПОП в виде универсальных, общепрофессиональных и профессиональных компетенций, соответствующих профессиональной деятельности выпускников; потребность в материально-техническом и кадровом обеспечении; и др.).

Приняты меры по обеспечению заключения договоров между Санкт-Петербургским университетом МВД России и организациями, осуществляющими деятельность по профилю ОПОП по специальности БИТ (организации, осуществляющие образовательную деятельность; специализированные подразделения по противодействию IT-преступлениям; иные федеральные государственные органы и отечественные компании, заинтересованные в противодействии IT-преступлениям) в целях организации практической подготовки обучающихся. В частности, заключено соглашение о сотрудничестве Санкт-Петербургского университета МВД России с ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого» № 223 от 26.05.2021.

Организована практическая подготовка обучающихся по специальности БИТ непосредственно в университете, предусматривающая выполнение ими определенных видов работ, связанных с будущей профессиональной деятельностью. Так, в период с 05 июня по 16 июля 2021 г. в информационном центре Санкт-Петербургского университета МВД России проходили производственную практику по получению профессиональных умений и опыта профессиональной деятельности курсанты, обучающиеся по специальности БИТ. Они закрепили полученные в процессе теоретического обучения знания, накопили новые в области безопасности информационных технологий, а также приобрели практические навыки, профессиональные умения и компетенции, необходимые для решения реальных профессиональных задач.

Переработаны реализуемые кафедрой СИТ образовательные программы повышения квалификации и переподготовки сотрудников подразделений, специализирующихся на предотвращении, выявлении, раскрытии и расследовании IT-преступлений, обеспечена их актуализация с учетом потребностей ОВД, складывающейся оперативной обстановки, изменений нормативно-правового регулирования. В частности, обновлены дополнительные профессиональные программы повышения квалификации сотрудников территориальных органов МВД России «Изучение технологии и противодействие использованию криптовалют в противоправных целях с учетом зарубежного опыта» и повышения квалификации сотрудников ОВД, занимающихся вопросами выявления и расследования преступлений, связанных с использованием криптовалют и других виртуальных активов.

Проработаны с иными организациями (например, ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого»), заинтересованными в противодействии IT-преступлений, возможность привлечения их ведущих экспертов и специалистов к проведению учебных занятий с обучающимися по специальности БИТ и программам повышения квалификации и переподготовки, указанным выше.

Организована разработка учебной и учебно-методической литературы для обеспечения реализации учебных дисциплин «Основы кибербезопасности» и «Актуальные вопросы деятельности подразделений, специализирующихся на предотвращении, выявлении, раскрытии и расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий», осваиваемых сотрудниками в рамках профессиональной (первоначальной) подготовки.

2. Научная, научно-исследовательская и редакционно-издательская работа.

Обеспечена подготовка НИР «Криминалистический полигон исследования информации о преступлениях, совершенных посредством информационно-телекоммуникационных технологий» с учетом перспектив открытия специализации «Компьютерная экспертиза».

Сотрудники кафедры СИТ организовывают и принимают участие в проводимых на базе других организаций, заинтересованных в противодействии IT-преступлений, научно-практических конференциях по направлениям оперативно-служебной деятельности специализированных подразделений, в интересах которых в университете осуществляется подготовка специалистов, в том числе, в рамках существующей на кафедре СИТ научной школы «Исследование проблем информационной безопасности». Привлекаются к этой деятельности и обучающиеся в университете. Так, в апреле 2021 года были сформированы команды курсантов, обучающихся по специальности 10.05.05 – «Безопасность информационных технологий в правоохранительной сфере», которые приняли участие в конкурсе хакатон «Искусственный интеллект на службе полиции».

Осуществляется участие профессорско-преподавательского состава кафедры СИТ в редакционной коллегии и написании научных трудов для опубликования в научно-практическом журнале Санкт-Петербургского университета МВД России «Оперативно-розыскной портал: право и технологии».

3. Работа с кадрами.

Запланирована и проводится переподготовка и повышение квалификации профессорско-преподавательского состава кафедры СИТ в организациях, осуществляющих образовательную деятельность, в том числе, не входящих в систему МВД России, в целях приобретения актуальных знаний и навыков в области информационной и кибербезопасности.

Обеспечено прохождение стажировок профессорско-преподавательского состава кафедры СИТ в Центре информационных технологий, связи и защиты информации ГУ МВД России по Санкт-Петербургу и Ленинградской области, Бюро специальных технических мероприятий ГУ МВД России по Санкт-Петербургу и Ленинградской области, а также в иных организациях, заинтересованных в противодействии IT-преступлениям.

Подготовлено совместно с Санкт-Петербургским суворовским военным училищем МВД России предложение в проект плана мероприятий по перепрофилированию училища в ведомственную общеобразовательную организацию по подготовке несовершеннолетних учащихся к поступлению в образовательные организации высшего образования МВД России на специальности, реализуемые в интересах подразделений, специализирующихся на предотвращении, выявлении, раскрытии и расследовании IT-преступлений.

4. Материально-техническое обеспечение подготовки специалистов.

Данное направление деятельности кафедры СИТ и Санкт-Петербургского университета МВД России в целом, видится наиболее проблемным и сложным, поскольку для формирования учебно-лабораторной базы кафедры требуются значительные финансовые затраты.

В соответствии с требованиями ФГОС ВО (от 19.12.2016 № 1612; п.7.3.1 ФГОС 3+) по специальности: 10.05.05 – «Безопасность информационных технологий в правоохранительной сфере» учебно-лабораторная база кафедры должна включать лаборатории: «Физика (исследования физических процессов)», «Системы и сети передачи данных», «Программно-аппаратные средства обеспечения информационной безопасности» и полигон технической защиты информации.

Дополнительно к этому, в соответствии с требованиями ФГОС ВО (от 26.11.2020 № 1461; п. 4.3.1 ФГОС 3++), необходимы еще лаборатории: «Электротехника, электро-, радиоизмерения», «Информатика и программирование», «Проектирование систем информационной безопасности».

Активно проводится работа по доукомплектованию учебно-лабораторной базы кафедры СИТ.

В рамках этого направления подготовлены предложения по размещению минимально необходимых для реализации ОПОП БИТ лабораторий и полигонов, предусмотренных соответствующими ФГОС ВО, а также их оснащению. Определен перечень лицензионного программного обеспечения, необходимого для обучения в рамках специальности БИТ, и представлены предложения по его приобретению.

С учетом необходимости в значительных финансовых затратах подготовлена обобщенная обоснованная заявка о выделении дополнительного финансирования, необходимого для обеспечения учебного процесса по ОПОП БИТ и программам переподготовки и повышения квалификации сотрудников подразделений, специализирующихся на противодействии IT-преступлениям. Внесены изменения и дополнения в Табель положенности основных средств связи, вычислительной и организационной техники, а также технических средств обучения, криминалистической, специальной техники базовых технических компонентов СДОТ МВД России и полиграфического оборудования, в части включения технических средств обучения.

Предполагаемый поставщик всего учебно-лабораторного оборудования (аппаратно-программных комплексов) вышеперечисленных лабораторий – закрытое акционерное общество «Учебно-методический центр при Санкт-Петербургском Государственном Университете телекоммуникаций им. проф. М.А. Бонч-Бруевича» (ЗАО «УМЦ СПб.ГУТ», г. Санкт-Петербург) является разработчиком и изготовителем учебного лабораторного оборудования, входит во всемирную организацию разработчиков и производителей учебного лабораторного оборудования Worlddidact, имеет прямые заказы от Международного Союза Электросвязи (ITU) на разработку и изготовление учебного лабораторного оборудования.

Заключение. Представленный в статье опыт решения базовых задач по основным направлениям деятельности кафедры специальных информационных технологий Санкт-Петербургского университета МВД России позволит обеспечить повышение эффективности подготовки кадров для ОВД Российской Федерации, специализирующихся на предотвращении, выявлении, раскрытии и расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Расширенное заседание коллегии МВД России 3 марта 2021 года. – Режим доступа: http://www.kremlin.ru/catalog/persons/310/events/65090 (Дата обращения 12.08.2021).
2. Приказ МВД России от 25.11.2019 № 878 «Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. № 3км» – [Электронный ресурс] URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=519451&dst=100001#9QZJrfSUYoOIM33p (Дата обращения 12.08.2021).

УДК 004.056

СОЦИАЛЬНО - ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ СОВРЕМЕННОГО ИНФОРМАЦИОННОГО ОБЩЕСТВА

Пучков Владимир Викторович
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: puchkov-81@bk.ru

Аннотация. В статье рассматривается проблематика построения, развития и дальнейшего существования нашей цивилизации в разрезе построения информационного общества как одного из наиболее предпочтительных путей развития социума. Урсул А.Д. в своей работе [1] дал оценку увеличения знаний в мире. Согласно ей, до начала XXI века общее количество знаний росло достаточно медленно, но уже за первые 50 лет XXI века оно удвоилось, с 1950 по 1970 удвоение происходило каждые 10 лет, с 1970 года каждые 5 лет. Ученый прогнозировал, что с 1990 года удвоение будет происходить каждый год и сейчас мы можем резюмировать, что его прогноз более чем подтвердился. Взрывное увеличение количества и качества информации, а также ее доступность для всех слоев общества приводит к образованию новых социально-психологических вопросов, на которые нам необходимо ответить в кратчайшие сроки.

Ключевые слова: информационное общество; информатизация; «кризис цивилизации»; инфосфера.

SOCIO-PSYCHOLOGICAL ASPECTS OF THE MODERN INFORMATION SOCIETY

Puchkov Vladimir
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: puchkov-81@bk.ru

Abstract. The article deals with the problems of the construction, development and further existence of our civilization in the context of building an information society as one of the most preferred ways of developing society. Ursul A.D. in his work [1] gave an assessment of the increase in knowledge in the world. According to it, until the beginning of the XXI century, the total amount of knowledge grew quite slowly, but already in the first 50 years of the XXI century it doubled, from 1950 to 1970, doubling occurred every 10 years, since 1970 every 5 years. The scientist predicted that since 1990, the doubling will occur every year and now we can summarize that his forecast has more than been confirmed. The explosive increase in the quantity and quality of information, as well as its accessibility to all segments of society, leads to the formation of new socio-psychological questions that we need to answer as soon as possible.

Keywords: information society; informatization; «crisis of civilization»; infosphere.

Введение. Развитие информационной науки и как следствие все большее вхождение в жизнь человека киберфизических систем – всемирный и, наверное, неизбежный этап развития нашей цивилизации. Этот этап включает в себя осознание единой картины мира, открытие и понимание единства информационных законов в природе и индустриальном мире и условия их практического применения.

На данный момент можно резюмировать, что информатизация — это объективная закономерность развития нашей цивилизации, необходимое условие для ее дальнейшего развития. Попытки игнорировать данные закономерности приведут к социальным, экономическим, экологическим и многим другим проблемам, от решения которых будет зависеть не только структура нашего будущего общества, но и дальнейшее существование цивилизации, по крайней мере в том виде, в котором мы привыкли ее видеть и можем представить в будущем.

События конца XX века ясно дали ясно понять, что задачи, которые ставит перед нами история, требуют принципиально нового аналитического аппарата для более полного прогнозирования возможных последствий, которые могут возникнуть при решении данных задач. Данная ситуация имеет название «кризиса цивилизации».

Кризис цивилизации – кризис нашего интеллекта, и он является последствием неспособности человечества решать глобальные проблемы, которые являются следствием его же неконтролируемой деятельности. Нахождение пути выхода из этого кризиса является обязательным условием выживаемости нашей цивилизации. Решение этой проблемы является наиболее важной социальной задачей нашего общества в настоящее время.

Данный кризис вызван предельной сложностью задачи, которую необходимо решить для его преодоления. Эта сложность привела к тому, что усилия одного человека или даже группы людей недостаточны для нахождения положительного результата. Следовательно, для решения этой проблемы необходимо каким-то образом объединить интеллектуальные усилия в единый разум, существенно усилить возможности человеческого мозга, повысить его творческую активность.

Информационное общество и его особенности. В наше время реализуется возможно один из последних для человечества шансов развиться в интеллектуальном плане, научиться мыслить на уровне необходимом для нашего общества уже сейчас. Без этого безусловно сложного, но необходимого требования возможности развития цивилизации находятся под большим вопросом. Соответственно мы можем согласиться со следующим высказыванием: «выживание через интенсификацию интеллекта, интенсификация интеллекта через информатизацию общества» [2].

Естественно вышесказанное не является истиной в последней инстанции для того, чтобы утверждать, что это есть вообще единственный путь к обеспечению выживаемости. Но можно утверждать, что сейчас это единственный способ, который дает реальную возможность поиска выхода из кризиса, он также не только не блокирует, но способствует одновременному поиску других методов решения нашей общей проблемы. Как минимум этот способ позволяет, если не предотвратить, то хотя бы отсрочить время наступления всемирных антропогенных, экологических катастроф.

В разрезе социальной науки можно выделить следующие этапы формирования информационного общества:

- глобализация экономики;
- сопряжение различных технологий;
- обновленные требования к сотрудникам и модели рабочего процесса;
- регулирование информационного законодательства;
- значительная роль государства как регулятора и глобального межгосударственного сотрудничества;

В современном мире понятие «информационное общество» впервые было озвучено в Японии в 1966 году. Тогда сотрудниками группы по техническим и экономическим исследованиям была озвучена работа, в которой говорилось, что информационное общество является социумом, который имеет в достаточном количестве высококачественную информацию и все нужные инструменты для распределения данной информации.

Согласно [3, 4] можно выделить некоторые особенности информационного общества:

- информационная экономика, то есть экономика, при которой производство и потребление информации доминируют над производством материальных ресурсов;
- возрастающие требования к информации членов социума;
- высокая информационная культура;
- неограниченный доступ к информации всех членов общества, сдерживаемый только вопросами безопасности как человека, так и групп населения;

В. И. Вернадский считается отцом-основателем теории информатизации мира. В соответствии с его идеями человечество как единый организм представляет собой силу способную кардинально преобразовывать окружающую его среду, общность, которая имеет возможность влиять на геологическое состояние нашей родной планеты [5].

Данную теорию поддерживали и описывали в своих работах: французский ученый Э. Леруа [6], отечественные философы Н. Н. Моисеев [7], А. И. Ракитов [8]. Можно отметить, что в данных работах отечественных ученых переход биосферы в ноосферу неотделимо от информатизации и образования информационного общества.

Вопросы формирования постиндустриального, и как одного из его проявлений, построение информационного общества интересовали многих ученых XX века. В их работах философия технократии второй половины прошлого века показала нам те удивительные возможности, которые становятся нам доступны в ходе развития. Теория постиндустриализма Д. Белла, «третья волна» цивилизации, описанная в работах Э. Тоффлера, «информационное общество» существование которого обосновывал Й. Масуда, эти возможные пути движения цивилизации, основывались на поистине революционной важности внедрения новых технологий, которые далее получили название информационных. Но наряду с возможностями, которые дает возможность реализовать информационная революция возникает ряд проблем, о которых многие авторы не говорят. Одной из таких «ложек дегтя в бочке меда» является «цифровой разрыв» иначе говоря деление современного мира на страны информационного сообщества и страны, которые не вошли его структуру. К сожалению, Россия относится к странам, которые опаздывают с информатизацией. Наша страна начала активно формировать информационное сообщество на 20 лет позднее США, Японии и других наиболее развитых государств Западной Европы [9].

Социально-психологические проблемы информатизации. В своей основе информатизация является одним из уровней преобразования человеком окружающего его жизненного пространства в антропосферу, итогом этого преобразования будет реализация высокоразвитой ионосферы. Происходящее имеет влияние не только на окружающую нас среду, на общественное пространство, оно затрагивает и человека, в частности.

Рассмотрим социально-психологические аспекты развития информатизации и информационного общества:

– Психологические аспекты. Хотя большинство из нас считает, что технический прогресс имеет решающее значение в развитии общества, однако способность принять и научиться использовать в повседневной жизни те возможности, которые дает нам информатизация дано далеко не всем. При рассмотрении данного аспекта можно выделить несколько проблемных моментов: отсутствие информационной культуры и низкий уровень общей культуры широких слоев населения, консерватизм и отсутствие желания затрачивать усилия на освоение нового. К психологическим вопросам также относим психофизиологическую. Это психологическая и физиологическая совместимость, готовность принятия человеком новой информационной технологии. И соответственно вопрос обеспечения информационно-психологической безопасности личности.

– Социальные аспекты. Их появление является следствием коренного изменения образа жизни общества в связи с информатизацией пространства. Особое место в этой подгруппе занимают вопросы гуманизации инфосферы и вопросы коммуникации [10].

Развиваясь инфосфера обязательно «потянет» за собой усиление коммуникативности между членами общества. Соответственно будет влиять (и уже влияет) на формирование каждого индивида «информационного общества». Несомненно, и не нуждается в доказательствах, то, что люди являются частью окружающего нас мира. Соответственно верным будет как то, что мы влияем на окружающее нас пространство, так и то, что наше окружающая нас природа имеет возможность каким-то образом оказывать на нас влияние. Это обуславливает то, что личность человека формируется при совместной деятельности с другими людьми, деятельности при которой происходит постоянный обмен и усвоение больших объемов информации.

Важная роль в решении вопроса гуманизации инфосферы лежит в самой сути информатизации. Важно понимать, что информация может привести как к положительным, так и к негативным последствиям. И решение проблемы гуманизации лежит в области предотвращения и нейтрализации влияния негативной информации на общество (сайты насилия, самоубийств и многое другое).

Развитие информатизации и решение вопросов, которые возникают вследствие этого развития может происходить разными путями:

1. Первый путь развития является стихийным и самоорганизующимся. Он возможен в тех случаях, когда происходят активные изменения в окружающей жизни и необходима адаптация людей к происходящему. Это ведет к изменениям моральных и нравственных ценностей, что наиболее тяжело происходит у консерваторов. Стихийная регуляция в таком случае даст возможность провести неизбежные изменения достаточно плавно, сгладив острые углы, но сам процесс происходит более длительно и часто с ведет к перерасходу ресурсов.

2. Централизованное управление информатизацией. Фактически осуществление данного процесса нереально. На нашем уровне развития невозможность применения данного процесса обусловлена его невероятной сложностью. Пока данная система рассматривается гипотетически и считается неуправляемым объектом.

3. Направляемая информатизация. В данном случае процесс развивается в условиях заданных параметров и ограничений, которые определяют границы его существования и возможные направления развития. В этом случае сохранив все преимущества саморазвития и самоорганизации есть возможность уменьшить период развития и снизить затраты.

Так называемые страны «первого мира», опережающие остальной мир в развитии, имеют возможность не спешить и идти по первому пути развития. Для них временной фактор не важен – они ПЕРВЫЕ. Страны и регионы, которые отстают в развитии должны выбирать третий путь. Значительное отставание в инфосфере может привести к очень серьезному отставанию в социально-экономическом развитии.

Информатизация в наше время начала приобретать глобальный, массовый характер. В ее основе лежит широкое применение современных технологий и методик. Соответственно ее научный, технический и технологические аспекты несомненны. Но мы должны понимать, что информатизация уже в настоящее время имеет настолько важное значение для развития общества, что ее социальный аспект должен постоянно находиться в поле зрения органов власти. И даже несмотря на важнейшую роль технического, технологического и других аспектов информатизации именно социальному нужно отдать приоритет при решении проблем и определения пути развития информатизации возможности применения ее результатов.

В этом плане одним из главных достижений информатизации будет возможность обеспечения доступа к мировой информационной системе для каждого индивида. Жизнь в индустриальном обществе дает возможность человеку связаться с конечным числом людей, а информационное общество будет гарантировать возможность связи каждого с каждым. Это может привести и уже приводит к серьезному изменению стиля общения между людьми. Произойдет резкий рост интенсивности и видов общения. Эти изменения за короткий промежуток времени будут соответствовать переходу общества на новый уровень развития. Также они будут определяющими при рассмотрении социального вопроса информатизации.

Рассмотренные выше изменения и как следствие глобальное развитие коммуникационных связей социальных отношений членов общества, с одной точки зрения создадут идеальные возможности для развития индивида как личности, а с другой стороны, эти же изменения приведут буквально к революции внутри общества, будут катализатором для перехода его на качественно другую ступень развития. Это обусловлено тем, что наше общество являет собой не просто группу индивидов. Это так же великое множество связей, зависимостей, отношений, в которых члены общества находятся которые так или иначе связывают всех нас, влияют на поступки и наши действия. Соответственно можно сделать логический вывод: любые изменения в обществе будут приводить к каким-либо проблемам. И чем критичнее эти изменения, чем быстрее они будут формироваться, тем большее количество социальных проблем мы будем иметь на выходе. И изменения в плане коммуникации, которые формируют основу нашего нынешнего общества уже сейчас формирует коммуникационную проблему такой глубины, что ее несвоевременное решение грозит нам крупными социальными катастрофами и потрясениями.

В аспекте коммуникации можно выделить следующие составляющие [11]:

- неизбежное появление новых моральных, этических и правовых норм общения;
- ограничение информационной пропускной способности человека;
- «электронного» посредника;
- общение с интеллектуальными и киберфизическими системами (системами искусственного интеллекта).

Проблема новых моральных, этических и правовых норм общения формируется благодаря тому, что информационный мир широко раздвинет пространственные горизонты сфер общения каждого индивида, убрав технические ограничения на возможность связи «каждого с каждым» любой удобный момент времени. Соответственно можно сделать вывод, что информационное воздействие на человека, возникающая при таком уровне общения, возрастет кратно. Но человек достаточно индивидуален и в силу этой особенности не способен, а иногда вполне возможно, что и не захочет быть участником такого интенсивного информационного обмена. Это будет обуславливать необходимость введения новых моральных, правовых, этических норм, которые будут приводить общение в устраивающие всех нас рамки. Но как известно мораль и этика – наиболее консервативны и тяжело поддаются изменениям элементы общественного сознания. И их трансформация будет восприниматься как отдельными индивидами, так и целыми общественными группами достаточно болезненно. Нужно понимать, что введение новых норм однозначно повлечет за собой бурную реакцию противодействия и отрицания. И это отрицание будет тем сильнее, чем меньше мы будем подготовлены к восприятию нового.

Проблема ограниченности информационной пропускной способности человека, будет обусловлена значительным увеличением интенсивности информационных потоков, которые будет необходимо обрабатывать каждому индивиду. На данном этапе каждый из нас имеет возможность нормально воспринимать и оперировать информацией в том случае если скорость ее поступления не превышает 50-70 бит/сек. В случае увеличения трафика неизбежно будет возникать психологический срыв, человек полностью перестает воспринимать информацию. Наличие данного ограничения, связано с психофизиологией человека. И в самом ближайшем будущем данные параметры, вероятно, не удастся существенно увеличить.

В данное время эта проблема имеет значение только для представителей отдельных профессий. Она решается путем строгого отбора, подготовки и организации рабочей деятельности. Однако в ходе построения информационного общества этот аспект будет все более актуален и встанет перед каждым из членов общества. Соответственно решения, которые имеются сейчас не будут удовлетворять требования времени.

Один из важных пунктов: проблема «электронного» посредника. Стремительное развитие информационной и теле коммуникативной среды в ходе информатизации, приводит к неуклонной замене личного, непосредственного общения людей к общению через информационные сети. В данное время нам весьма сложно предугадать последствия такой подмены. В самом предельном случае мы можем прийти к полной замене общения человека с человеком на общение с искусственным интеллектом. Данный вариант очень вероятен, в связи с тем, что для многих людей общение с компьютером дается гораздо легче, чем коммуникация с другими людьми. Это обусловлено тем, что связь человек-компьютер не имеет противоречий, она строго структурирована, тогда как общение в паре человек-человек часто имеет трудности, которые требуют преодоления в том числе эти трудности могут носить и психологический характер. В процессе создания искусственного компьютерного мира человек выстраивает его в соответствии со своим мировоззрением и мироощущением психологическими потребностями и многими другими факторами, которые делают созданный иллюзорный мир более предпочтительным и комфортабельным для жизни, чем реальный. Вполне очевидно, что в случае массовости такого варианта — это будет очаг серьезной социальной проблемы в обществе.

Проблема общения человека с интеллектуальными электронными системами. Данная проблема является одной из важных частей коммуникативной проблемы. Массовое внедрение интеллектуальных систем в жизнь общества в итоге приведет к созданию новой реальности, нового мира – мира интеллектуальных систем. Этот мир будет представлен общением внутренних субъектов (интеллектуальных систем), а также коммуникацией

внутренних субъектов с субъектами иного мира – в данном случае это будет человек. У нас есть понимание, что такое общение должно подчиняться некоторым правилам, моральным и иным нормам, которые нам еще только предстоит выработать. Решение данной проблемы возможно в будущем при развитии информатизации и по мере того, как мир интеллектуальных систем будет обретать свой конечный вид. Особенность этих отношений будет выявляться в зависимости от структуры управления этими системами. На данный момент законов взаимодействия интеллектуальных систем и человека мы не знаем, а сформированы они будут только в процессе моделирования и изучения их работы в различных ситуациях.

В ходе рассмотрения этапов информатизации многие отмечают только ее положительное влияние на процесс развития общества. Можно предположить, что в научном и техническом плане это действительно так. Однако в социальном плане все зависит от того с какой целью будут использованы полученные знания. Мы можем искренне верить в человеческий разум, однако очень маловероятно, что процесс информатизации обязательно будет иметь гуманный характер, а ее плоды в однозначном порядке пойдут на пользу человечеству. Соответственно прогнозирование, своевременное выявление и нейтрализация негативных проблем информатизации необходимо для обеспечения гуманистической направленности тех изменений в социуме, которые неизбежно принесет информатизация.

Последствия информатизации, которые могут привести к антигуманным изменениям в обществе, возможно разделить на прямые и косвенные [11]. Соответственно прямые – есть результат непосредственно информатизации, а косвенные не относятся напрямую к информатизации, но сопутствуют им.

К косвенным последствиям можно отнести:

- перераспределение интеллектуальных функций и требований между человеком и компьютером;
- повышение требований к интеллектуальному уровню членов общества;
- структурные изменения в социуме;
- превалирование алгебраического (двоичного) мышления над образным;
- уменьшение информационной безопасности как человека в частности, так и общественных групп в целом;
- ускорение социальных процессов в связи с возрастанием эффективности обратных связей;

Можно отметить следующие прямые негативные последствия информатизации:

- тотальный контроль над личностью;
- «информационный тоталитаризм»;
- «глобальная информационная цензура»

Заключение. Рассматривая вопрос построения информационного общества проблем и преимуществ, которые получит человечество в ходе этого процесса, можно отметить, что информатизация сама по себе не решит социальные проблемы в обществе. Так же процесс информатизации не сможет обеспечить гуманитарной направленности происходящих изменений. Информатизация развивает обратные связи в обществе. Возможно несколько вариантов развития событий, например, в случае при развитии информатизации в обществе, где бедные беднеют, а богатые богатеют, данное разделение будет происходить особенно ярко и заметно. Антагонизм между двумя слоями общества в этом случае может привести к глобальным социальных катастрофам.

Между тем, наряду с множеством проблем и опасностей, которые может привнести в наше общество информатизация, она остается одним из самых доступных нам путей для преодоления «кризиса цивилизации». В наше время информация уже имеет ценность как некий ресурс необходимый для дальнейшего развития. Однако по сравнению с привычными нам материальными ресурсами, которые ограничены информация имеет тенденцию к постоянному росту и пока не обнаруживает склонности к падению. Человечество как никогда близко подошло к критической черте своего развития. И развитие информатизации в рамках построения «информационного мира» в разрезе обязательной гуманизации данного процесса может дать нашей цивилизации шанс на дальнейшее существование.

СПИСОК ЛИТЕРАТУРЫ

1. Урсул А.Д. Проблема информации и информатизация общества // НТИ. Сер. 2. 1991.- № 6. с. 1-8.
2. Пароджанов В. Д. Кризис цивилизации и нерешенные проблемы информатизации // НТИ. Серия 2. Информатизационные процессы и системы. 1993. №12. С. 1-9.
3. Стратегия перехода Санкт-Петербурга к информационному обществу // Проблемы информатизации. 1999. Вып. 4. С. 50-65.
4. Смолян Г. Л., Черешкин Д. С., Вершинская О. Н., Костюк В. Н. и др. Путь России к информационному обществу (предпосылки, проблемы, индикаторы, особенности). М.: Изд. Института системного анализа РАН, 1997. 64 с.
5. Вернадский В. И. Несколько слов о ноосфере // Успехи современной биологии 1994. №18. Вып. 2. С. 113-120.
6. Le Rou E. Lexidgence idealiste et le fait devolution. Paris, 1927. P 196.
7. Моисеев Н. Н. Человек и ноосфера. М.: Молодая гвардия, 1990. 351 с.
8. Ракитов А. И. Философия компьютерной революции. М.: 1991.
9. Заболотский В. П., Юсупов Р. М., Иванов В. П. Человек в информационном пространстве // Проблемы информатизации. 1996. №4. С. 3 – 7.
10. Заболотский В. П., Юсупов Р. М. Социальный аспект информатизации // Информатика и вычислительная техника. Вып. 1-2. М., 1993. С. 39 – 42.
11. Юсупов Р. М., Заболотский В. П. Концептуальные и научно-методологические основы информатизации. – СПб.: Наука, 2009. – 542 с., 80 ил.

УДК 316.334.3

ПРОТЕСТНЫЙ ДИСКУРС НА СТРАНИЦАХ СОЦИАЛЬНОЙ СЕТИ «ВКОНТАКТЕ»

Сапон Ирина Валерьевна
Сибирский государственный университет телекоммуникаций и информатики
Бориса Богаткова ул., 51, Новосибирск, 630008, Россия
e-mail: irina.sapon@bk.ru

Аннотация. В работе приводятся результаты качественного контент-анализа комментариев участников одного из протестных онлайн-сообществ российской социальной сети «ВКонтакте». Выявляются основные социально-экономические и политические проблемы, декларируемые участниками онлайн-дискуссии как причины существующих протестных настроений. На наш взгляд, решение данных проблем может снизить протестную активность и укрепить доверие между институтами власти и гражданским обществом.

Ключевые слова: интернет; протест; социальные движения; теория относительной депривации; социальные медиа; язык вражды; экономическое неравенство; коррупция; «ВКонтакте».

CONTENT ANALYSIS OF PROTEST SENTIMENTS IN ONLINE DISCUSSIONS

Sapon Irina
The Siberian State University of Telecommunications and Informatics
51 Borisa Bogatkova St, Novosibirsk, 630008, Russia
e-mail: irina.sapon@bk.ru

Abstract. In this paper we present the results of a qualitative content analysis of one of the protest online communities of the Russian social network VKontakte. We Identify the main socio-economic and political problems declared by the participants of the online discussion as the causes of the existing protest moods. In our opinion, solving these problems can reduce protest activity and strengthen trust between government institutions and civil society.

Keywords: internet; protest; social movements; Relative deprivation theory; social media sites; hate speech; economic inequality; corruption; VKontakte.

Введение. Как показали кейсы «Арабской весны», Occupy Wall Street и других крупных протестов, социальные медиа сегодня вносят большой вклад в мобилизацию протестной активности [1]. Они используются для агитации, информирования и координации участников протеста, для поиска единомышленников, эмоционального обмена, формирования общественного мнения и коллективной идентичности.

В организации российской протестной активности 2011-2012 годов социальные медиа также сыграли заметную роль [2, 3]. На страницах LiveJournal, Facebook и «Твиттер» проходила общественная дискуссия, звучали призывы выйти на митинг, публиковались репортажи с мест событий. К недоверию по поводу существующей власти у участников событий добавилось ощущение доверия к информации из дружеских онлайн-сетей, а к чувству гнева и обманутости властью по поводу фальсификации выборов — ощущение групповой солидарности с единомышленниками [2]. Волна российских протестов 2020-2021 годов также была организована с помощью социальных медиа и активно сопровождалась обменом эмоционально-заряженным контентом.

Согласно теории относительной депривации, протестные социальные движения основываются на ощущении экономического, социального или политического ограничения (депривации), на чувстве несправедливости, возникающем при сравнении социальной группой своих жизненных условий с условиями жизни других социальных групп [4].

Анализ дискурса протестных сообществ может показать болевые точки и причины недовольства, которые могут запускать механизм протестной активности. Мы проанализировали комментарии пользователей одной из протестных групп «ВКонтакте» — «Я против Путина. Я против Единой России» (2398 участников). Критерием выбора данного сообщества стало видимое отсутствие связи с каким-либо явным оппозиционным движением, что, на наш взгляд, должно показать более непредвзятую картину. Сначала мы отобрали посты на стене сообщества, имеющие максимальное количество комментариев, а затем проанализировали все комментарии к ним. Всего для анализа было отобрано 1020 комментарив, оставленных участниками в течение всего периода существования данной группы. Качественный контент-анализ проводился вручную с помощью Atlas.ti.

Специфика подобных протестных групп заключается в консолидации возмущения и критики, направленной на смену власти. Поэтому большинство комментариев вполне ожидаемо были наполнены эмоциональной, агрессивной лексикой и содержали обличительную риторику. Мы постарались выделить конструктивные элементы дискуссии и показать социально-экономические проблемы, о которых наиболее часто упоминалось в комментариях участников.

Анализ показал (Табл. 1), что больше всего участников волнует экономическое неравенство (бедность населения, богатство чиновников и олигархов), в котором они винят политическую систему государства (24 цитаты).

Таблица 1

Проблемы, о которых упоминают пользователи

Основные проблемы	***Число цитат***
Экономическое неравенство (бедность населения, богатство чиновников и олигархов)	24
Роль России в украинском конфликте	21
Коррупция и воровство	12
Нечестные выборы	11
Высокие налоги	8
Отсутствие свободы слова	7
Низкие зарплаты	5
Высокие цены	3
Наличие политзаключённых	3

С помощью крайне агрессивной лексики и нецензурных слов многие участники резко высказывались по поводу низкого уровня жизни россиян. Возмущены они были также высокими налогами (8 цит.), низкими зарплатами (5 цит.), высокими ценами (3 цит.). Приведём некоторые цитаты:

«Хлеб и мука у нас дорожают. Продукты тоже. В аптеках лекарств нету, да если и есть, то с космическими ценами. МРОТ, как был, так и есть. На проезд цены выросли...».

«Только что решил пройтись по магазинам у себя возле метро Коломенская, решил прикинуть цены на сахар. «Магнит» — 45 рублей, «Дикси» — 49 рублей, «Пятерочка» — 51 рубль, но я думаю, что ещё не вечер, а где же обещанное повышение пенсий?».

В низком уровне жизни участники нередко обвиняют власть:

«Обобрал страну. Один процент олигархов имеет весь народный капитал».

«Где живут дети российской правящей элиты?»

«А ты в курсе, что так называемые кремлевские патриоты держат деньги в иностранных банках, дети их за границей?».

Также многие участники группы обеспокоены политическими проблемами. Наиболее часто упоминается: роль России в украинском конфликте (21 цитата), коррупция и воровство (12 цит.), нечестные выборы (11 цит.), отсутствие свободы слова (7 цит.), наличие политзаключённых (3 цит.).

«Вы действительно что ли не понимаете, что было бы, останься Крым в составе Украины?».

«Вообще-то Крым — это нестабильный регион... что-то навроде Чечни».

«Для ввода войск на Украину нам необходимо получить на это разрешение от Совета Безопасности ООН. В противном случае это будет означать войну, в которой Россия вторглась на территорию суверенного государства. Массовый геноцид русских на Украине, а та же жителей ДНР и ЛНР не даёт нам юридического права на ввод войск без мандата ООН».

Большая часть комментариев — это не конструктивное обсуждение фактов, а крайне эмоциональные восклицания, направленные на критику действующей партии (29) и государственного лидера (48), что вполне соответствует тематике группы (Табл. 2). Тональность сообщений чаще всего отрицательная.

Таблица 2

Высказывания о власти, о политических лидерах и партиях

Основные темы	***Тональность***	***Число цитат***
Высказывания против Путина (Угрозы, требование уйти в отставку, обвинение в воровстве, обмане, содействии преступной деятельности)	Отрицательная (агрессивная лексика)	48
Высказывания против партии «Единая Россия» (Обвинение партии в причине проблем)	Отрицательная (агрессивная лексика)	29
Жириновский, ЛДПР	разная	13
За Путина	Позитивная (одобрение, поддержка)	12
КПРФ	Разная	12
Навальный	Разная	11
Грудинин	Разная	3

Наиболее часто встречалась форма обращения к президенту на «ты», требование уйти в отставку, обвинения в воровстве, обмане, содействии преступной деятельности. Партия «Единая Россия» также вполне закономерно для дискурса такого типа сообщества представлялась в негативном свете:

«Пенсионеры 10 получают и рады, бегут голосовать за ЕдРос».

«Где берут этих идиотов??? Я до сих пор не могу понять откуда берётся столько людей, любящих ЕР?».

Если тональность сообщений варьировалась, в основном, от крайне отрицательной до нейтральной, и отражала, в целом, схожие мнения и настроения, то мнения комментаторов относительно дальнейших действий расходились.

Таблица 3

Обсуждение вариантов возможных действий и последствий

Основные идеи	***Число цитат***
Мобилизация к восстанию (призыв к свержению власти, уничтожению собственности богатых)	18
Утверждение: «Смена власти ни к чему не приведёт»	7
Утверждение: «Достойной замены нет, выбирать не из кого»	6
Утверждение: «Нужна смена власти»	4
Опасения последствий митингов и смены власти	4
Призыв мирно объединяться и апелляция к прошлому	3

Кто-то объяснял, за кого будет голосовать и почему:

«Поэтому я отдам свой голос за любую партию, кроме ЕР!».

Кто-то открыто призывал всех голосовать:

«Не пойти на выборы — это не выход. Чего вы этим добьётесь? А объявив бойкот, вы тем самым подарите свои бюллетени ЕдРу, а они с удовольствием съединоросят ваш голос».

Однако большинство цитат имело прямые призывы к мобилизации и свержению власти. Такие радикально настроенные пользователи говорили о возмездии и призывали «раскулачить» власть:

«Просто всё забрать, посадить на зарплату обычного рабочего и посмотреть, что будет».

«Россияне, эту власть необходимо уничтожать всеми доступными средствами!».

Проведённый нами подсчёт наиболее часто использованных слов показал, что чаще всего в тексте встречаются слова: «Россия», «Путин», «будет», «была», «людей», «против» (рис. 1).

Рис. 1. Частота встречаемости слов (с минимальной частотой употребления — 25 и составлением списка стоп-слов).

Как видно из рисунка, дискуссии в данной группе в целом строятся вокруг размышлений о прошлом и будущем России, об управлении страной, о власти и народе, о поиске лучшей жизни для большинства.

Заключение. Проблема подобных агрессивно настроенных сообществ может заключаться в том, что они агрегируют, накапливают и тем самым преувеличивают агрессию (известно, что в условиях интернет-среды, люди испытывают эффект растормаживания [5] и ведут себя более агрессивно, кроме того, эмоционально заряженный контент привлекает к себе больше внимания, чем нейтральный [6]). Онлайн-комьюнити становятся неким «информационным пузырём», или «эхо-камерой», огораживающей пользователей от альтернативных взглядов на окружающую действительность и создающей тем самым предпосылку к упрочению предвзятого и однобокого отношения к проблеме [7]. С учётом того, что в социальных сетях сегодня присутствует огромное количество социальных ботов и ботоферм, преследующих свои цели, пользователь может ошибочно полагать, что он попал в группу единомышленников, а его картина мира может искажаться за счёт искусственно созданного в сети общественного мнения.

В ходе работы мы постарались выделить конструктивные элементы дискуссии и очертили круг наиболее заметных социально-экономических проблем, наличие которых запускает волну российских протестов. На наш

взгляд, комплексное решение данных проблем на уровне государства может снизить протестную активность, ликвидировав на корню причины протеста и укрепив доверие между институтами власти и гражданским обществом.

Исследование выполнено при финансовой поддержке РФФИ и ЭИСИ в рамках научного проекта № 21-011-32247 «Российские протестные онлайн-сообщества: характеристики и особенности».

СПИСОК ЛИТЕРАТУРЫ

1. Smidi A., Shahin S. social media and social mobilisation in the Middle East: A survey of research on the Arab Spring // India Quarterly, 2017, Vol. 73, N. 2. P. 196-209.
2. Ваньке А. В., Ксенофонтова И. В., Тартаковская И. Н. Формы протестной интернет-коммуникации в России (на примере движения «За честные выборы») // Пути России. Новый старый порядок-вечное возвращение? 2016. С. 98-129.
3. Платонов К. А., Юдина Д. И. Повестка протестных онлайн-сообществ Санкт-Петербурга во «ВКонтакте» // Мониторинг общественного мнения: Экономические и социальные перемены, 2019, № 5 (153). С. 226-49.
4. Дементьева И. Н. Теоретико-методологические подходы к изучению социального протеста в зарубежной и отечественной науке // Мониторинг общественного мнения: экономические и социальные перемены, 2013, № 4. С. 3-10.
5. Галяшина Е. И., Никишин В. Д. Деструктивное речевое поведение в цифровой среде: факторы, детерминирующие негативное воздействие на мировоззрение пользователя //Lex Russica, 2021, №. 6 (175). С. 79-94.
6. Heiss R., Schmuck D., Matthes J. What drives interaction in political actors' Facebook posts? Profile and content predictors of user engagement and political actors' reactions //Information, Communication & Society, 2019, Vol. 22, N. 10. P. 1497-1513.
7. Фельдман П. Я., Завалишин Н. С. Виртуальные сетевые коммуникации и политическая поляризация общества (на примере Соединенных Штатов Америки) //Коммуникология, 2021, Т. 9, №. 2. С. 98-109.

УДК 510.65; 699.8

РОЛЬ И ЗНАЧЕНИЕ МОДЕЛИ НАРУШИТЕЛЯ В ПРОФИЛАКТИКЕ УГРОЗ БЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Синещук Юрий Иванович
Санкт-Петербургский университет МВД России
Летчика Пилютова, ул., 1, Санкт-Петербург, 198206, Россия
e-mails: sinegal53@mail.ru
+7(911)2138184

Аннотация. Рассматриваются особенности обеспечения информационной безопасности объектов информационной инфраструктуры. Анализируются статистические данные, характеризующие характер и динамику угроз безопасности. Обосновывается роль и значение модели нарушителя в реализации мероприятий защиты информации, формулируются ее содержательные элементы.

Ключевые слова: информационная инфраструктура; угрозы безопасности; информационная безопасность; модель нарушителя.

THE ROLE AND SIGNIFICANCE OF THE INTRUDER MODEL IN PREVENTING THREATS TO THE SECURITY OF INFORMATION INFRASTRUCTURE OBJECTS

Sineshchuk Yury
St. Petersburg University of the Russian Interior Ministry
1, Pilot Pilyutov Street, Russia, 198206, St. Petersburg
e-mails: sinegal53@mail.ru

Abstract. The article considers the features of ensuring information security of information infrastructure objects. Statistical data describing the nature and dynamics of security threats are analyzed. The role and significance of the intruder model in the implementation of information protection measures are substantiated, and its content elements are formulated.

Keywords: information infrastructure; security threats; information security; intruder model.

Введение. В современном информационном обществе информация, уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни. Цифровые преобразования в таком обществе становятся один из главных факторов экономического роста, который обеспечивается не только эффектом от автоматизации существующих процессов, но и с внедрением принципиально новых, прорывных концепций, информационных технологий и цифровых платформ: «Индустрии-4.0» или «Четвёртая промышленная революция» (Industry 4.0 - The Fourth Industrial Revolution), «Общество-5.0» (Society 5.0), роботизация, аналитика больших данных(Big Data – BD), «Интернет вещей» (Internat of Things - IoT), искусственный интеллект(Artificial Intelligence – AI), социотехнические и киберфизические системы(Cyber-Physical System - CPS) и др. [1].

Информационные и коммуникационные технологии становятся неотъемлемой, системообразующей частью современных управленческих систем во всех отраслях экономики, сферах государственного управления, обороны страны, безопасности государства и обеспечения правопорядка. При этом, расширяющиеся возможности общества, риски и угрозы растут пропорционально и экспоненциально. Многофункциональный характер любой современной

технологии способствует тому, что практически одни и те же механические узлы, компьютерные программы и технологические решения могут быть использованы как в военной и гражданской, так и в преступной и террористической деятельности. В этих условиях все чаще совершаются компьютерные атаки на государственные и частные информационные ресурсы, объекты критической информационной инфраструктуры [2].

В общем случае, информационная инфраструктура является (наряду с информационными ресурсами, созданными субъектами информационных отношений, средствами взаимодействия таких субъектов, их информационными системами) частью информационного пространства. Информационная инфраструктура включает в себя: совокупность информационных центров, подсистем, банков данных и знаний, систем связи, центров управления, аппаратно-программных средств и технологий обеспечения сбора, хранения, обработки и передачи информации. Ключевым элементом информационной инфраструктуры, во многом определяющим ее содержание, являются информационные технологии, рассматриваемые как упорядоченная совокупность методов обработки сообщений, включающих поиск, сбор, хранение, передачу и распространение сообщений, а также их предоставление человеку.

Под критической информационной инфраструктурой (далее — КИИ) понимается совокупность объектов критической информационной инфраструктуры в виде: информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления субъектов КИИ; а также сети электросвязи, используемые для организации их взаимодействия. Субъектами КИИ являются компании, работающие в стратегически важных для государства областях.

В настоящее время фиксируются многочисленные попытки осуществления целенаправленных кибератак на объекты информационной инфраструктуры различного иерархического уровня. Создание ГосСОПКА (государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации), а также подписание Федерального Закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» подтверждают актуальность и важность задачи обеспечения безопасности объектов информационной инфраструктуры.

Современные социотехнические и киберфизические системы, как элементы(объекты) информационной инфраструктуры функционируют с участием человека. Следовательно, вопросы безопасности такого рода систем часто сводятся к вопросам человеческих отношений и человеческого поведения.

Нарушителем безопасности называют лицо, которое осуществляет попытку выполнения запрещенных операций, либо по ошибке, либо по незнанию, либо осознанно. Наиболее опасен - злоумышленник, как разновидность нарушителя, который намеренно идет на преступление из корыстных побуждений. В общем случае, нарушитель может быть внешним по отношению к защищаемой системе (посторонние лица) и внутренним -- инсайдер (из числа персонала, пользователь – в широком смысле).

Проводя анализ нарушений информационной безопасности, особое внимание следует уделять не только самому объекту нарушения, но и личности нарушителя, то есть субъекту нарушения. Это поможет разобраться в мотивах преступления и даст возможность избежать повторения подобных ситуаций.

Анализ угроз безопасности, позволяет сделать вывод о неуклонном росте инсайдерских атак, что отражено на рис. 1. [3].

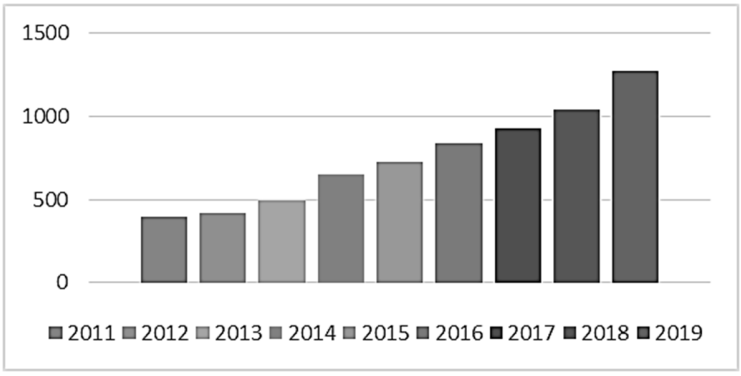


Рис. 1. Общее количество инсайдерских атак

Особую сложность в раскрытии компьютерных преступлений представляют именно пользователи, с одной стороны, - это есть ее необходимый элемент, а с другой стороны, - источник нарушения или преступления. Поэтому целесообразно заблаговременно построить модель нарушителя безопасности, которая характеризует его теоретические и практические знания, навыки, время и место действия и т.п.

Разработка мер защиты объектов информационной инфраструктуры должна включать в себя анализ угроз безопасности и разработку модели угроз, а внедряемые меры защиты не должны оказывать негативного влияния на функционирование самого объекта. При этом анализ угроз предполагает выявление источников угроз, и обязательно

- создание модели нарушителя, а также - анализ уязвимостей используемых систем, определение возможных способов реализации угроз и их последствий. Модель нарушителя представляет собою - некую совокупность сведений о численности, оснащенности, подготовленности, осведомленности и тактике действий нарушителей, их мотивации и преследуемых ими целях, которые используются при выработке требований к системе физической защиты и оценке ее эффективности.

Роль и место модели нарушителя в процессе формирования модели угроз информационной безопасности показаны на рис. 2 [4].

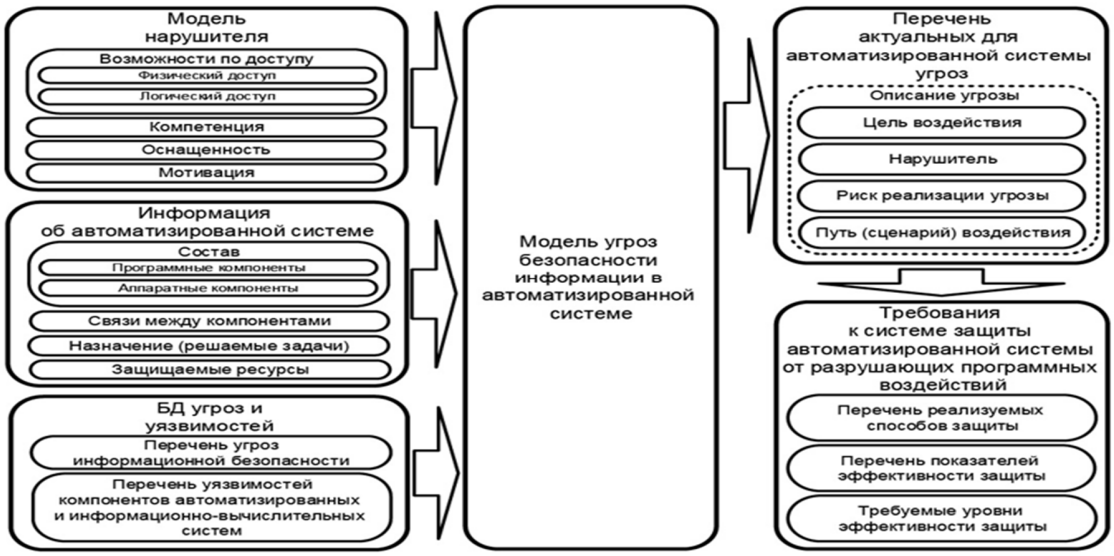


Рис. 2. Роль и место модели нарушителя в процессе формирования модели угроз информационной безопасности

Построение концептуальной модели нарушителя целесообразно начинать с анализа социальных истоков компьютерной преступности. При этом надо учитывать, что между людьми часто возникают конфликты, представленные на рис. 3., которые могут сказаться на состоянии безопасности.

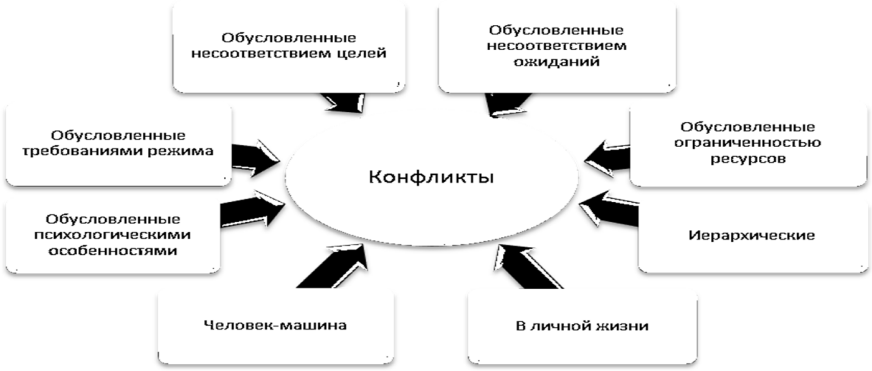


Рис. 3. Основные типы конфликтов в сфере защиты информации.

Анализ сути и содержания социально-психологических конфликтов позволяет выработать конкретные рекомендации, позволяющие воздействовать и даже управлять социально-психологической обстановкой в коллективе, способствуя тем самым повышению уровня защищенности объекта.

Опыт показывает, что частота того или иного вида нарушений обратно пропорциональна наносимому им ущербу: чаще всего встречаются нарушения, вызванные халатностью и безответственностью, - ущерб от них незначителен и легко восполняется. Ущерб от зондирования системы, как правило, больше, но вероятность его реализации - ниже, поскольку требует достаточно высокой квалификации, знания особенностей системы защиты и наличия определенных психологических особенностей. При этом размер ущерба прямо пропорционален положению пользователя-нарушителя в служебной иерархии.

При разработке модели нарушителя необходимо дифференцировать всех пользователей по возможности доступа к системе и по потенциальному ущербу от каждой категории пользователей.

Модель нарушителя позволяет выявить условия, при которых может произойти формировании психологической готовности к противоправным действиям и произвести общую типизацию криминальности

потенциального нарушителя. Каждый тип нарушителя должен быть охарактеризован значениями соответствующих характеристик. При этом, необходимо помнить, что определение конкретных значений характеристик модели нарушителя в значительной степени субъективно и, следовательно, модель нарушителя может быть представлена перечислением нескольких вариантов его облика [5].

В процессе разработке модели нарушителя необходимо определить: категории лиц, к которым может принадлежать нарушитель; мотивы действий нарушителя (его цели); квалификацию нарушителя, его осведомленность о системе защиты и оснащённость; характер возможных действий нарушителя и учитывать следующие факторы: хорошо поставленная работа по подбору кадров и профилактические мероприятия препятствуют формированию коалиций нарушителей, их сговора; принцип «враждебного окружения» предполагает, что любой нарушитель, скрывает свои преступные действия от других сотрудников; деструктивные проявления в функционировании объекта защиты могут быть следствием элементарных ошибок сотрудников (пользователей, администраторов, эксплуатирующего и обслуживающего персонала), а также недостатков принятой технологии обработки информации и т.д.

Выводы. Адекватная реальности модель нарушителя может служить основой прогнозного сценария реализации криминальных поступков по нарушению безопасности объектов информационной инфраструктуры, позволяет проанализировать причины нарушений и дает возможность либо устранить их заблаговременно, либо обоснованно сформулировать требования к разрабатываемой системе защиты и эффективно проводить мероприятия по профилактике и расследованию компьютерных преступлений.

СПИСОК ЛИТЕРАТУРЫ

1. Kateryna Bondar. Challenges and Opportunities of Industry 4.0 – Spanish Experience (англ.) // International Journal of Innovation, Management and Technology. — 2018. — (т. 9, № 5). — p. 202-208.
2. I. Kotenko, I. Saenko, Yu. Sineshchuk, Optimizing Secure Information Interaction in a Distributed Computing System by the Method of Sequential Concessions. Proceedings - 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2020, Vasteras, Sweden Conference Paper, 10p. March 2020.
3. Ушаков, И.А. Обнаружение инсайдеров в корпоративной компьютерной сети на основе технологий обработки больших данных. / И.А. Ушаков // Вестник Санкт- Петербургского государственного университета технологии и дизайна. Серия 1: Есте¬ственные и технические науки. - 2019. - № 4. - С. 38-43.
4. Дроботун Е.Б., Цветков О.В. Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действий нарушителя. «Программные продукты и системы» № 3, 2016 г., стр. 42-50
5. Синещук Ю.И., Синещук М.Ю., Яковлева Н.А. Модель нарушителя, как основа предупреждения и эффективного расследования компьютерных преступлений. Международная НПК Общественная безопасность, законность и правопорядок в III тысячелетии – Ч. 3. – Воронеж: Воронежский институт МВД России, 2013. – 116-121с. ISBN 978-5-88591-119-1.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ

УДК 004.94

ИМИТАЦИОННАЯ МОДЕЛЬ ФОРМИРОВАНИЯ И КОНТРОЛЯ БИЗНЕС-ПРОЦЕССОВ ИНТЕГРАЦИИ ОРГАНИЗАЦИОННЫХ КУЛЬТУР

Абрамова Евгения Александровна
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mail: vectra4444@mail.ru

Аннотация. Организационная культура является важной характеристикой для разработки квалифицированной стратегии интеграции. В условиях объединения компаний из разных стран своевременность, надежность и эффективность интеграции организационных культур является одной из ключевых задач. В статье описана разработанная имитационная модель, позволяющая по результатам проведения экспериментов с достаточно большой точностью прогнозировать количество сотрудников компании, образованной в результате слияния.

Ключевые слова: имитационная модель; надежность интеграции; своевременность интеграции; слияния; поглощения, сценарии объединения.

A SIMULATION MODEL ENSURING THE TIMELINESS, RELIABILITY AND EFFICIENCY OF THE INTEGRATION OF ORGANIZATIONAL CULTURES

Abramova Evgenia
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mail: vectra4444@mail.ru

Abstract. Organizational culture is an important characteristic for developing a qualified integration strategy. In the context of the merger of companies from different countries, the timeliness, reliability and efficiency of the integration of organizational cultures is one of the key tasks. The article describes a developed simulation model that allows, based on the results of experiments, to predict the number of employees of a company formed as a result of the merger with a sufficiently high accuracy.

Keywords: simulation model; reliability of integration; timeliness of integration; mergers; acquisitions, unification scenarios.

Введение. С каждым годом в мире увеличивается количество проводимых сделок слияний и поглощений. Подобные сделки открывают компаниям возможности доступа к новым рынкам, предоставляют возможность использования наиболее современных технологий, способствуют переходу к более перспективным секторам экономики [1-6]. Увеличение объема свободно доступной информации способствует получению новых знаний и проведению значимых исследований, а в сочетании с непрерывно происходящими изменениями экономической среды, подобные факторы создают благоприятные условия для развития внутренних источников экономического роста, позволяющих компаниям активно работать в быстро меняющейся среде [4-7].

Организационная культура компании определяет способы формирования и контроля бизнес-процессов, а также является основой для создания совместной деятельности сотрудников, приобретающей и приобретенной компаний. Процесс формирования организационной культуры должен соответствовать текущим факторам внешней среды и поддерживать эффективное организационное развитие компании [8-10].

Процесс слияния компаний с заранее устоявшимися организационными культурами, как показывает практика, значительно повышает психологическую устойчивость сотрудников к проводимым организационным изменениям.

Основной целью всех сделок слияния и поглощения в конечном итоге является успешная интеграция. Интеграция приводит к созданию новой организационной структуры в процессе объединения компаний. Данная структура, как правило, способна более эффективно и рационально распоряжаться имеющимися ресурсами, оптимизировать трудовые, материальные, информационные и финансовые потоки компаний, участвующих в сделке слияния и поглощения. Статистические данные показывают, что 70% случаев потенциально выгодных транзакций

терпят неудачу из-за некачественной подготовки и проведения интеграции [1]. Таким образом, выбор организационной формы для интеграции компаний в соответствии с заявленными критериями, обеспечивающими своевременность, надежность и эффективность интеграции является важным шагом, который может способствовать объединению ресурсов. Любые бизнес-инструменты должны соответствовать определенному уровню своевременности и надежности, позволяющему исключить факторы потери данных или ошибочных расчетов. Данный аспект особенно важно учесть при построении имитационной модели.

Несомненно, слияния и поглощения предлагают много преимуществ для развития бизнеса. Тем не менее, можно создать некоторую ошибочную иллюзию, что такие транзакции относительно просты, недороги и представляют собой единственный способ значительно расширить бизнес. Однако исследования показывают, что от 60 до 80% компаний, участвующих в сделках слияния и поглощения, не достигают поставленных целей, даже не смотря на наличие потенциально выгодных стратегий. Данный факт объясняется наличием ошибок, допущенных в процессе интеграции предприятия. В первую очередь это неправильно выбранный объект для слияния и поглощения, малоэффективная подготовка к сделке и некорректная финансовая оценка.

Чтобы избежать ошибок, необходимо разработать план процедур слияний и поглощений, и, как уже отмечалось и никогда ранее не формулировалось, вопрос об организационной культуре и персонале новых компаний должен быть сформулирован на этапе выбора объекта для слияний и поглощений [2]. На практике, процесс интеграции организационной культуры является достаточно сложным, поскольку это многофазный процесс, требующий комплексного планирования и точного осуществления. Подробные расчеты и грамотные, и продуманные действия руководящего персонала гарантируют успешную интеграцию. Тем не менее, потенциал конфронтации культурных организаций редко анализируется на ранних этапе сделок слияния и приобретения. В результате культурное противостояние создает серьезную проблему для процедуры слияния. Из этого можно сделать вывод, что в период слияний и поглощений у них наиболее важным является вопрос несовместимости организационной культуры с возникающими организациями. И на этапе планирования сделки, для будущей разработки эффективной стратегии слияния, очень важно знать о возможных результатах интеграции культур.

На сегодняшний день не существует инструмента, позволяющего достоверно диагностировать совместимость организационных культур и воспроизвести за короткий промежуток времени большое количество возможных сценариев объединения компаний для получения результатов интеграции с последующей возможностью выбора наиболее приемлемого варианта среди всех возможных. Используя средства имитационного моделирования, можно за короткий временной промежуток получить большое количество возможных сценариев [3] объединения организационных культур, необходимых для формирования корректной интегрированной культуры. Имитационная модель должна обладать следующими характеристиками: надежность, способность моделировать систему, близкую к реальности; гибкость; возможность изменения параметров модели без изучения сложных зависимостей организационных культур, описываемых в литературе [4].

Таблица 1

Параметризация личностных характеристик сотрудников в разрабатываемой модели

	Возраст	18-25 / 25-40 / 40-50 / 50-60 лет
	Семейное положение	0 – холост / 1 – женат
1.	Наличие высшего образования	0 – отсутствует / 1 - имеется
2.	Общий трудовой стаж	1 год - 40 лет
3.	Трудовой стаж в данной компании	1 год – 10 лет
	Лояльность к ценностям компании	1-10 (условных очков лояльности)
	Адаптация к новым условиям труда	1 – сложно, 10 – легко
	Удовлетворенность условиям труда	1 – не доволен, 10 - доволен
	Ценность квалификации сотрудника	1 – легко заменимый, 10 - ценный
	Эффективность работы	1 – 10 (очков трудоспособности)

Для проверки качества модели проводятся три эксперимента по объединению компаний разных типов, для этого выборка подразделяется на 3 группы.

В первом эксперименте представлены организации с численностью персонала около 20 000 человек каждая; каждая компания имела ассоциированные компании. В эксперименте учитывалось общее количество сотрудников для каждого предприятия, включая ассоциированные компании и представительства.

Во втором эксперименте поглощающая компания до реорганизации имела 300 человек, объединенная компания - 30 человек.

В третьем эксперименте приняли участие малые предприятия; на момент начала сделки персонал поглощающей компании насчитывал не более 100 человек.

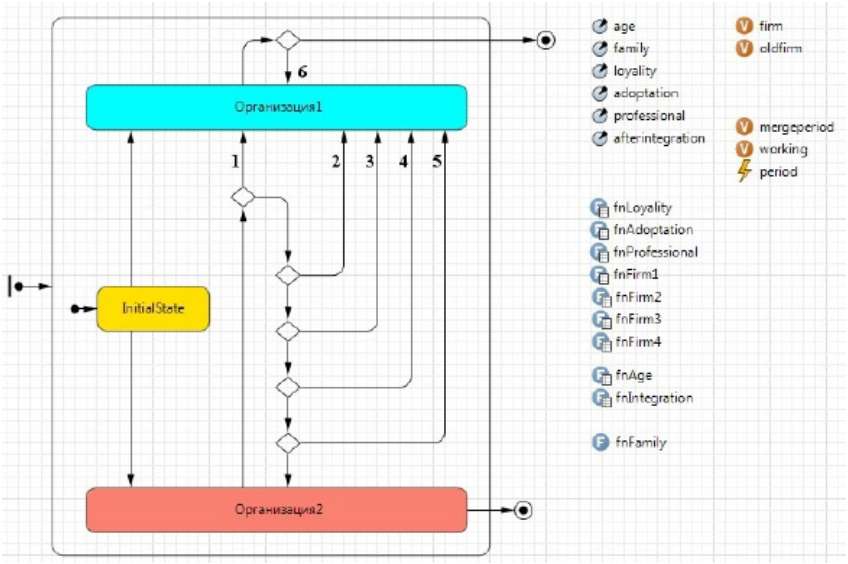


Рис. 1. Схема переходов имитационной модели.

Все группы агентов (people.size()) распределены по возрастным группам и по типам культурных организаций, в зависимости от заданных значений (начальное количество сотрудников, работающих в первой (AgentFirm1) и вторая организация, а также четыре возрастных диапазона (возраст1, возраст2, возраст3, возраст 4).

Следует отметить, что агенты в базовой версии модели определены довольно «жестко», как указано в возрастных рамках; тем не менее, таким же образом можно определить другие параметры агента (лояльность, способность к адаптации, спрос агента на рынке труда и т. д.). Например, с помощью модели можно воссоздать ситуацию, когда большинство сотрудников, работающих в компании, обладают высокой степенью лояльности или спросом на рынке труда.

Описание переходов в разработанной модели представлены на рис. 1., а личностные характеристики сотрудников в таблице 1.

1) Используемые функции — это функции пакета AnyLogic, которые работают с языком Java.

2) Все программные структуры привели общего класса агента-сотрудника, который участвует в процессе слияния двух организаций.

При создании прямого экземпляра класса каждому агенту присваивается уникальный набор параметров, каждый из которых задается нормальным распределением с использованием функции iform ().

Переход 1 работает при условии: randomTrue (fnLoyality (loyalty) / 100) == true, где переменная лояльности задается униформой нормального распределения (1, 10), а функция fnLoyality представлена в виде графика на рис. 1.

Переход 2 работает при условии: randomTrue (fnAdoptation (принятие) / 100) == true, где переменная адаптации задается униформой нормального распределения (1, 10), а функция fnAdoptation представлена в виде графика на рис.1.

Переход 3 работает при условии: randomTrue ((fnFirm4 (get_Main (). Irm1Ty -pe) / 100)) == true, где различные функции fnFirm1, fnFirm2, fnFirm3, fnFirm4 представлены в виде графиков на рис. 1 и независимая переменная rrm1Type, которая определяет тип поглощаемой организации (1, 2, 3 или 4), указывается при проведении экспериментов.

Переход 4 работает при условии: randomTrue (fnAge (age) / 100) == true, переменная age указана при инициализации модели, а функция fnAge представлена в виде графика на рис.6.

Переход 5 работает при условии: randomTrue (fnFamily (family)) == true, семейство переменных определяется случайным образом randomTrue (0.6), а функция fnFamily определяется экспертным образом следующим образом: if (family == true) { return 0.2; } else { return 0.2; }

Переход 6 работает при условии: randomTrue (fnIntegration (afterintegration) / 100) == true, переменная afterintegration задается униформой нормального распределения (9, 10), а функция fnIntegration представлена в виде графика на рис. 1.

На рис. 2-6 представлены результаты имитационного моделирования.

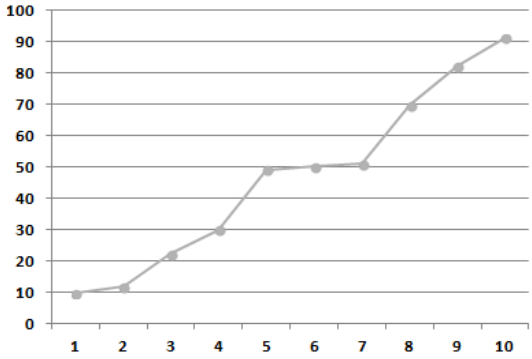


Рис. 2. График - вероятность перехода сотрудника в компанию-покупателя. Ось ординат – вероятность в процентах, ось абсцисс – уровень лояльности.

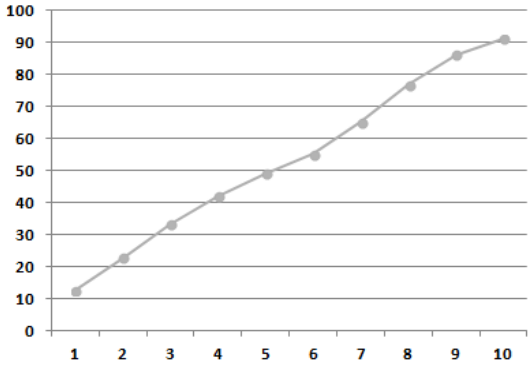


Рис. 3. График - вероятность перехода сотрудника в компанию-покупателя. Ось ординат – вероятность в процентах, ось абсцисс – способность адаптации.

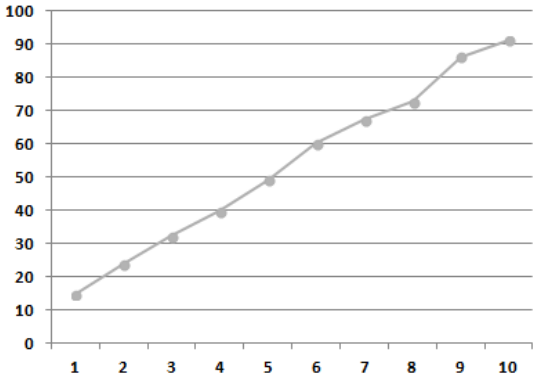


Рис. 4. График – вероятность перехода сотрудника в компанию-покупателя. Ось ординат – вероятность в процентах, ось абсцисс – уровень востребованности.

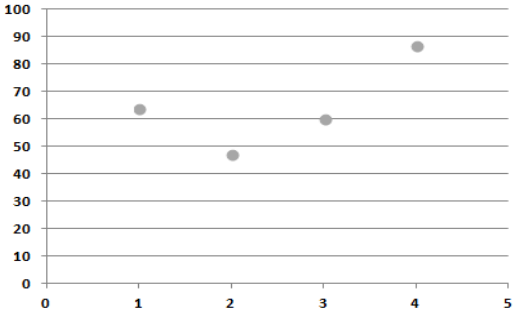


Рис. 5. График – вероятность перехода сотрудника из поглощаемой компании в компанию-покупателя в зависимости от возраста (1 – 18-25 лет; 2 – 25-40 лет; 3 – 40-50 лет, 4 – 50-60 лет). Ось ординат – вероятность в процентах.

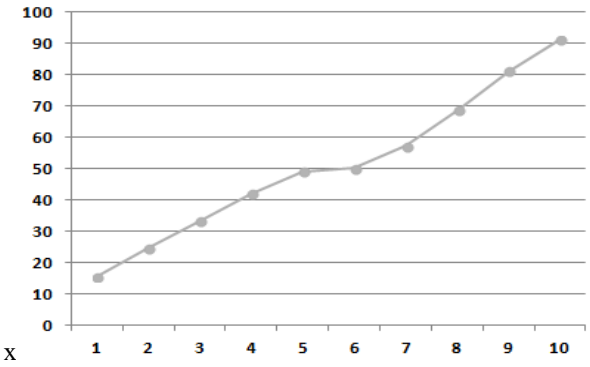


Рис. 6. График – вероятность перехода сотрудника из поглощаемой компании в компанию-покупателя в зависимости от условий труда после интеграции.

Заключение. Разработанная имитационная модель содержит много стохастических величин, поэтому для выявления четких тенденций необходимо проводить большое количество экспериментов с одинаковыми значениями изменяемых экзогенных параметров. По результатам проведения имитационных экспериментов можно с достаточно большой точностью прогнозировать количество сотрудников компании, образованной в результате слияния. Этот фактор успеха является одним из важнейших в сделках слияния и поглощения. В развитии данного направления предполагается оценка влияния на исследуемые процессы инфокоммуникационной составляющей [11-15].

СПИСОК ЛИТЕРАТУРЫ

1. Delong, G., & Deyoung, R. (2007). Learning by observing: Information spillovers in the execution and valuation of commercial bank M&As. // Journal of Finance, 62, p. 181–216.
2. Colombo, G., Conca, V., Buongiorno, M., & Gnan, L. (2007). Integrating cross-border acquisitions: A process-oriented approach. // Long Range Planning 40, p. 202–222
3. Имитационное моделирование: создание терминов // Хабрахабр. [Электронный ресурс]. URL: http://habrahabr.ru/post/246307/
4. Агентное моделирование / Википедия [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Агентное_моделирование
5. Соколов Р.В., Андреевский И.Л. Проектирование и эксплуатация информационных систем. – СПб: СПбГЭУ, 2017. – 382 с
6. Верзун Н.А., Колбанёв М.О., Омельян А.В. Сетевая архитектура цифровой экономики: монография. - СПб.: СПбГЭУ, 2018. - 157 с
7. Мамедов Дж.Ф., Абдуллаев Г.С., Коршунов И.Л., Алиев И.Р. Оценка экономической эффективности на этапах проектирования гибких производственных систем/ Вестник компьютерных и информационных технологий. 2021. Т. 18. № 3 (201). С. 26-32/
8. Емельянов А.А., Коршунов И.Л. Опыт реализации политики информационной безопасности на предприятии малого бизнеса в целях обеспечения информационно-экономической безопасности информационная безопасность регионов России (ИБРР-2015). Материалы конференции. 2015. С. 213-214
9. Коршунов И.Л., Пуха Г.П. от систем компьютерного тестирования - к информационной системе кафедры. В сборнике: Инновационные технологии в сервисе. Сборник материалов IV Международной научно-практической конференции. Под ред. А. Е. Карлика. 2015. С. 310-312
10. Фокин Р.Р., Компьютерные технологии в науке и производстве/_методические указания по выполнению курсовой работы для магистратуры направления 080100.68 (521600) «Экономика» / Санкт-Петербургский государственный университет сервиса и экономики, кафедра «Информационные технологии». Санкт-Петербург, 2009.
11. Богатырев В.А., Богатырев С.В. Резервированное обслуживание в кластерах с уничтожением неактуальных запросов // Вестник компьютерных и информационных технологий - 2017. - № 1(151). - С. 21-28
12. Богатырев В.А. Комбинаторно-вероятностная оценка надежности и отказоустойчивости кластерных систем // Приборы и системы. Управление, контроль, диагностика» - 2006. - № 6
13. Верзун Н.А., Колбанёв М.О., Омельян А.В. Введение в инфоком-муникационные технологии и сети Future Networks. Уч. пособие. СПб.: Изд-воСПбГЭУ. – 2016. – 50 с
14. Bogatyrev S.V., Bogatyrev V.A., Bogatyrev A.V. Redundant maintenance of a non-uniform query stream by a sequence of nodes that are grouped together in groups // Wave Electronics and its Application in Information and Telecommunication Systems (WECONF 2020) - 2020, pp. 9131463
15. Bogatyrev V.A., Bogatyrev S.V., Derkach A.N. Timeliness of the Reserved Maintenance by Duplicated Computers of Heterogeneous Delay-Critical Stream // CEUR Workshop Proceedings - 2019, Vol. 2522, pp. 26-36

УДК 004.4

ОЦЕНКА ЭКОНОМИЧЕСКИХ ПОКАЗАТЕЛЕЙ ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ С ПОМОЩЬЮ ИМИТАЦИОННЫХ МОДЕЛЕЙ

Пуха Геннадий Пантелеевич
Санкт-Петербургский государственный университет сервиса и экономики
наб. канала Грибоедова 30-32, литер А, Санкт-Петербург, 191023, Россия
e-mails: pgp2003@list.ru

Аннотация. На примере производственного процесса базы нефтепродуктов рассматривается возможность применения технологии имитационного моделирования для анализа влияния отклонений не только на производственные, но на экономические показатели функционирования подобных объектов.

Ключевые слова: производственные процессы; экономические показатели; имитационное моделирование; инструментальная среда GPSS Studio.

ASSESSMENT OF ECONOMIC INDICATORS OF PRODUCTION PROCESSES USING SIMULATION MODELS

Puha Gennady
Saint Petersburg State University of Service and Economics
emb. Griboyedov Canal 30-32, letter A, St. Petersburg, 191023, Russia
e-mails: pgp2003@list.ru
+7 (921) 420-64-76

Abstract. On the example of the production process of the base of petroleum products, the possibility of using the technology of simulation modeling to analyze the impact of deviations not only on production, but on the economic indicators of the functioning of such objects is considered.

Keywords: production processes; economic indicators; simulation; instrumental environment GPSS Studio.

Введение. При исследовании производственных объектов процессы их функционирования зачастую представляются с помощью аппарата систем массового обслуживания и реализуются методом имитационного моделирования. Одновременно, любые производственные объекты (ПО) являются и экономическими субъектами и поэтому характеризуется также соответствующими экономическими показателями. Следовательно, в данном случае можно вести речь об исследовании эффективности их функционирования по экономическим показателям [1, 2]. При этом, очевидно, что, решая задачи поиска (синтеза) рациональной структуры или режимов работы системы показатели технологической эффективности потребуется увязать с такими показателями экономической эффективности как расходы, доходы и прибыль [4].

В качестве примера реализации этого направления исследований можно взять, в частности, модель технологического процесса приема, хранения и отпуска нефтепродуктов (НП) на таком ПО как нефтяная база [5]. В такой модели совокупность соответствующих процессу реальных объектов, этапов и производственных операций может быть интерпретирована следующим набором частных объектов (элементов) системы массового обслуживания (рис. 1).

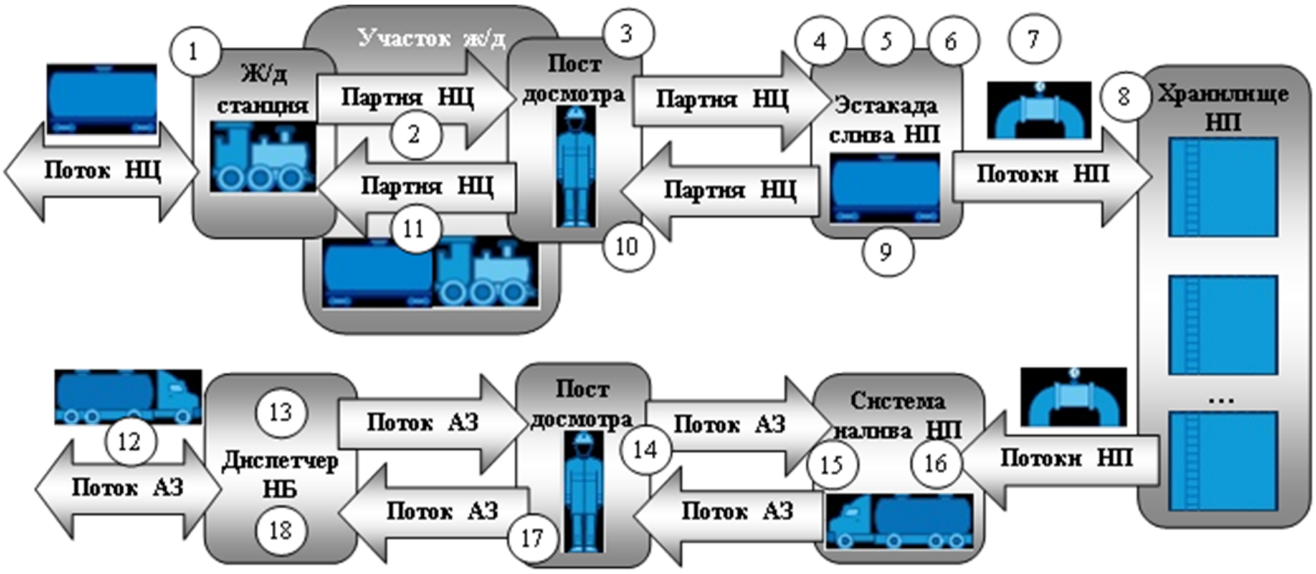


Рис. 1. Условная схема технологического процесса приема и отпуска нефтепродуктов

Железнодорожная станция, где имитируются операции поступления цистерн с НП различного вида с ожидаемой в соответствии с планом поставок с завода интенсивностью.

Железнодорожный участок, отображающий транспортировку этой «поставки» от железнодорожной (ЖД) станции до территории нефтебазы. Пост (бригада) досмотра цистерн – по досмотру каждой цистерны и локомотива на предмет выявления несанкционированных грузов, посторонних лиц и ВВ, а также – наличие товаросопроводительной документации (ТСД).

Сливная эстакада – с соответствующими операциями. Автостоянка – операции, связанные с прибытием автоцистерн (АЦ) для перевозки НП различного вида с ожидаемой в соответствии с планом отпуска потребителям интенсивностью.

Диспетчер НБ – операции по оформлению и выдаче диспетчером нефтебазы разрешения водителю на отпуск НП, а также ТСД для выезда за пределы нефтебазы.

Пост досмотра автоцистерн – операции по досмотру каждого АЦ на предмет выявления нарушений условий безопасности, и их прибытие в рабочую зону системы налива НП, а также - по контролю полноты налива соответствующих НП в АЦ, проведение опломбирования.

Система налива НП – операции, связанные с подключением соответствующих автоматических систем слива (АСН); наполнением АЦ необходимым видом НП с помощью насосов из резервуаров хранения.

Показателем производственной эффективности, данном случае, выступает пропускная способность, по которой может быть оценена, например - степень влияния на эффективность процесса приема и отпуска нефтепродуктов факторов безопасности, проявляющихся, как правило, в виде отклонений тех или иных технологических операций от нормально протекающего процесса и вариантов их устранения. Для полноты анализа целесообразно, на наш взгляд, отдельно учесть также и затраты на выполнение ремонтных работ и формирование суммы ожидаемых штрафных санкций при известной вероятности выявления некачественных поставок НП (см., например, рис. 2).

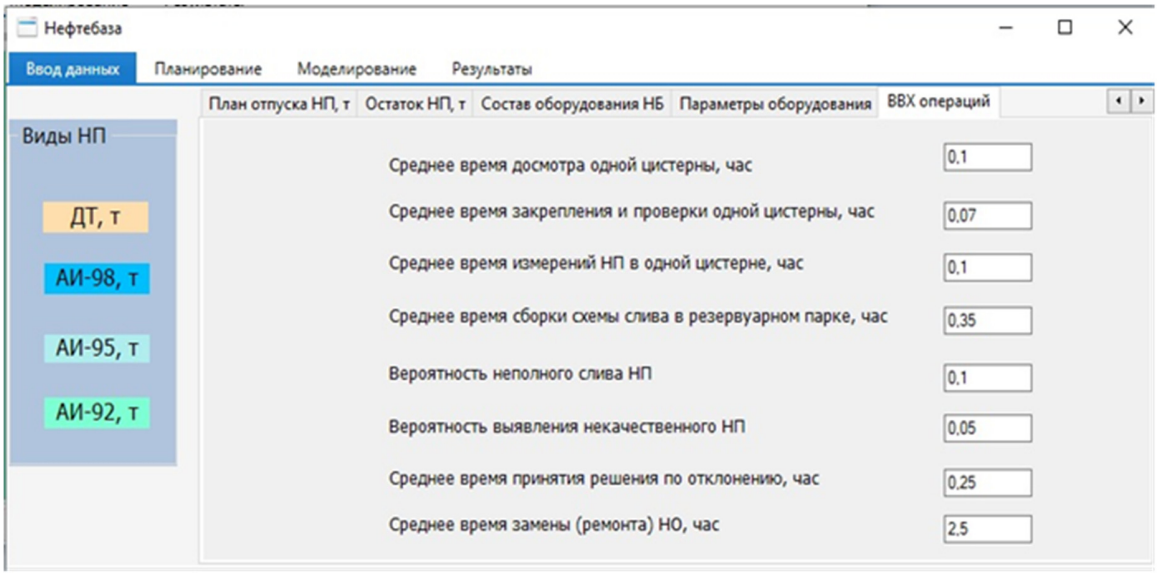


Рис. 2. Исходные данные, характеризующие оборудование нефтебазы (вариант Исходные данные, характеризующие вероятностно-временные характеристики производственных операций и их отклонений (вариант)

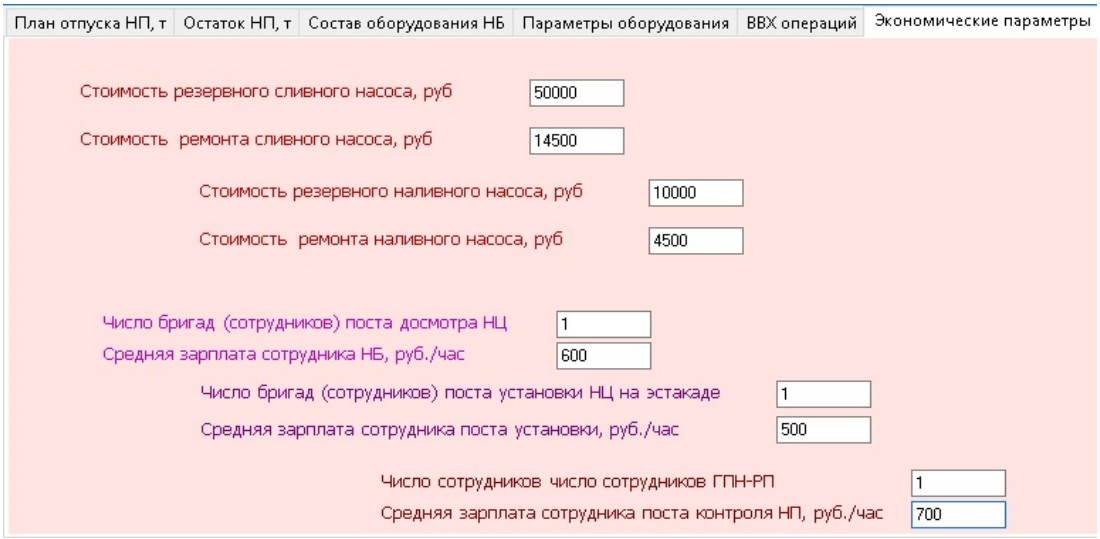


Рис. 3. Исходные данные о штатном составе нефтебазы и нормативах оплаты труда (вариант)

Выход на экономические показатели в качестве исходных данных, несомненно, потребуют использовать не только технологические характеристики процесса, но и рыночные расценки НП, обслуживания (замены) оборудования и нормы труда сотрудников НБ и т.д (см., например, рис. 3).

Определение показателей, связанных с получением НБ доходов, целесообразно реализовать, на наш взгляд, в объекте «система налива НП» исходной модели за счет одновременного подсчета объема отпущенных НП его стоимости. Нахождение же показателей, обеспечивающих оценку расходных средств и штрафных санкций – в объекте «сливная эстакада», одновременного с подсчетом объема НП, принятых на хранение (или «оштрафованных). Расчет затрат на восстановление работоспособности насосного оборудования, есть смысл, реализовать в этих же объектах модели совместно с оценкой времени на ремонтные работы. А расходы на заработную плату, например, в объекте «диспетчер НБ» пропорционально числу сотрудников и времени работы (моделирования). Результаты серии экспериментов на обсуждаемой модели за 90 суток при типовых исходных данных, и предполагаемых стоимостных характеристиках, полученные с помощью средства их анализа среды GPSS Studio (таблица 1), достаточно убедительно свидетельствуют о том, что:

Таблица 1

Результаты серии экспериментов по определению экономических показателей технологического процесса приема и отпуска нефтепродуктов (вариант)

№ п/п	Производительность НН, т/час	Число сотрудников в ГПН	Среднее время прохождения маршрута автоцистерны, часы	Расходы на заработную плату, руб.	Потери на ремонт оборудования, руб.	Общие расходы, руб.	Доходы от реализации НП, руб.	Прибыль, руб.	Сумма штрафов, руб
1	4	1	11,399	4535518	1061000	1359149952	1640640000	275893472	3200000
2	6	1	8,055	4532380,5	843500	1359350016	1533959936	169234112	1800000
3	8	1	6,395	4535404,5	925000	1420525056	1604999936	181197376	3000000
4	10	1	5,379	4525187,5	1111500	1373699968	1537740032	160694256	4200000
5	4	2	10,829	5291960,5	1007000	1383325056	1644600064	257155936	4000000
6	6	2	7,494	5284764,5	1087000	1334024960	1572419968	232029904	2600000
7	8	2	5,813	5290405,5	1188000	1292050048	1370339968	71816368	4400000
8	10	2	4,822	5277385	1049500	1338550016	1293240064	-51635832	3400000
9	4	3	10,659	6046129,5	1081000	1325374976	1589400064	256897872	2000000
10	6	3	7,337	6038430	1016500	1312775040	1567559936	252281264	2600000
11	8	3	5,655	6034614	1013000	1376324992	1333080064	-48014960	3600000
12	10	3	4,655	6041293	1211500	1360300032	1519920000	154552624	3200000

– наибольшее сокращение цикла отпуска НП для автоцистерн из предполагаемого набора значений факторов дает такое их сочетание, когда производительность НН увеличивается в 2,5 раза, а число диспетчеров - с 1 до 3;

– однако достаточно существенные изменения этого показателя в этом случае отмечаются уже и при одном диспетчере.

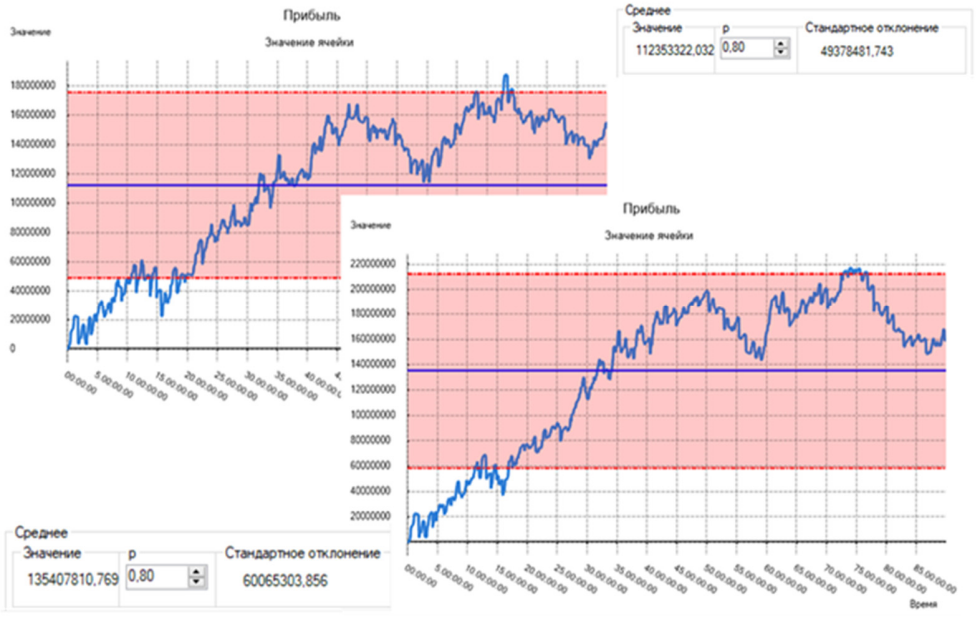


Рис. 4. Динамика показателя прибыли для сочетания факторов № 12 и № 4

И, наконец, сравнение динамики показателя прибыли (рис. 4) уже окончательно убеждают, что при выборе факторов (или средств) повышения эффективности исследуемого процесса следует отдать предпочтение их второму их сочетанию, так как в этом случае среднее значение прибыли может быть получено на 14-15% выше.

Анализ же результатов моделирования влияния этих факторов на затраты, связанные с выходом из строя, например, наливного насосного оборудования показывает, что со снижением его надежности:

во-первых затраты на ремонт будут расти достаточно интенсивно и независимо от его организации (рис.5.а), однако:

во-вторых, с точки зрения эффективности процесса отпуска НП, обеспечивающего получение большего дохода, предпочтение, все же, следует отдать варианту установок оборудования с ненагруженным резервом (рис 5.б).

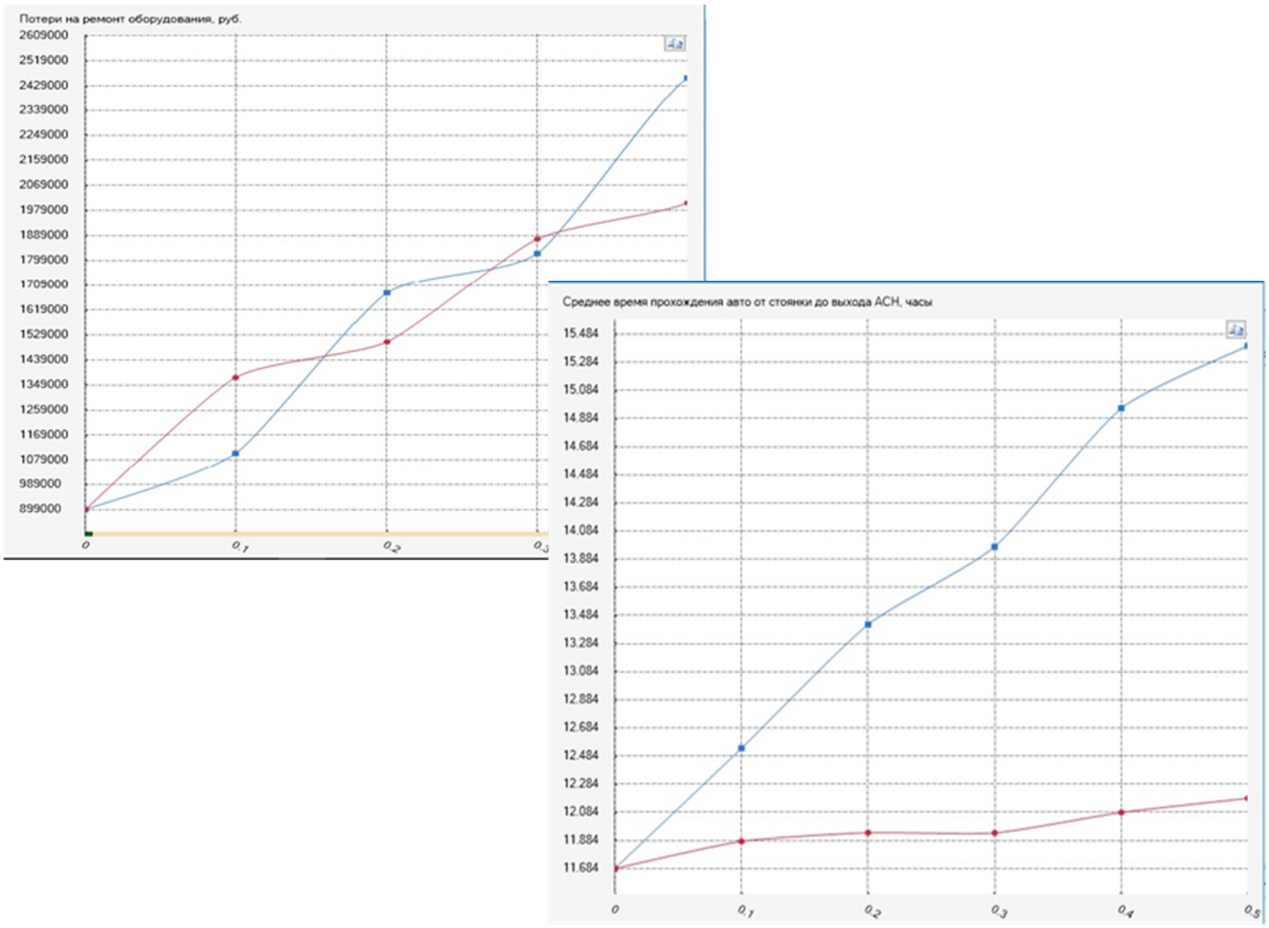


Рис. 5. Динамика затрат на ремонт наливного насосного оборудования (а) и показателя прибыли (б) для сочетания факторов № 12 и № 4

Заключение. Таким образом, данный пример, по нашему мнению, достаточно наглядно демонстрирует возможности применения технологии имитационного моделирования для решения задач, связанных с исследованием деятельности производственных объектов не только с учетом целевых, но и экономических показателей.

СПИСОК ЛИТЕРАТУРЫ

1. Пуха Г.П. Моделирование систем: учебное пособие / Г.П. Пуха. – СПб: Изд-во СПбГЭУ, 2020. – 261 с.
2. Маряшина Д.Н. Использование имитационного моделирования при планировании поставок сырья и организации производства НПЗ /Д.Н. Маряшина, С.А. Марков, В.В. Девятков // Автоматизация телемеханизация и связь, в нефтяной промышленности. – 2019. - № 8(553). – с. 25-30.
3. Пуха Г.П. Разработка систем поддержки решений с использованием среды моделирования GPSS STUDIO / В сборнике: Информационные системы и технологии в экономической деятельности. Сборник статей. Санкт-Петербург, 2020. С. 14-26.
4. Пуха Г.П., Котомин М.А. Моделирование процесса производственной деятельности с использованием метода имитационного моделирования // Актуальные проблемы защиты и безопасности: Труды XXIII Всероссийской научно-практической конференции РАРАН (1–4 апреля 2020 г.). Том 2. Издание ФГБУ «Российской академии ракетных и артиллерийских наук». Москва – 2020. С. 188-196.

УДК 004

ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ ЭЛЕКТРОННЫХ ТОРГОВЫХ ПЛОЩАДОК

Шилков Владимир Ильич, Аденин Семен Михайлович
Уральский федеральный университет имени первого Президента России Б.Н. Ельцина
Мира ул., 19, Екатеринбург, 620002, Россия
e-mails: shilkov-urfu@yandex.ru; semen.dustov@urfu.me

Аннотация. В статье обсуждаются вопросы обеспечения информационно-экономической безопасности электронных торговых площадок. Приведены сведения, подтверждающие актуальность и значимость проблем информационной безопасности в сфере электронной торговли. Предлагается формулировка информационно-экономическая безопасность электронных торговых площадок. Приводятся примеры возникновения экономических и организационно-технологических рисков в системах электронной торговли. Обсуждаются экономические последствия снижения уровней информационной безопасности. Предлагаются мероприятия по повышению информационно-экономической безопасности площадок электронной торговли.

Ключевые слова: цифровизация; искусственный интеллект; электронная торговая площадка (ЭТП); киберугрозы; информационно-экономическая безопасность.

INFORMATION AND ECONOMIC SECURITY OF ELECTRONIC TRADING PLATFORMS

Shilkov Vladimir, Adenin Semyon
Ural Federal University named after the first President of Russia B.N. Yeltsin
19 Mira St, Yekaterinburg, 620002, Russia
e-mails: shilkov-urfu@yandex.ru; semen.dustov@urfu.me

Abstract. The article discusses the issues of ensuring the information and economic security of electronic trading platforms. The information confirming the relevance and significance of the problems of information security in the field of electronic commerce is presented. The formulation of information and economic security of electronic trading platforms is proposed. Examples of the emergence of economic, organizational and technological risks in e-commerce systems are given. The economic consequences of reducing the levels of information security are discussed. Measures are proposed to improve the information and economic security of e-commerce platforms.

Keywords: digitalization; artificial intelligence; electronic trading platform; cyber threats; information and economic security.

Введение. Цифровая трансформация экономики, осуществляемая на основе внедрения инновационных сквозных информационно-коммуникационных технологий (ИКТ) и искусственного интеллекта делает возможным повышение качества управления во многих сферах социально-экономической жизни. Неотъемлемой частью современных концепций трансформации и информатизации экономики стало появление новых моделей рынка, к которым может быть отнесена, например, электронная торговля, в настоящее время, ставшая реалией современных рыночных отношений. Если первые электронные сервисы в сфере торговли в РФ стали возникать более 20 лет назад и были предназначены, главным образом, для сравнения цен, то в настоящее время растущие ожидания потребителя в отношении более выгодных условий получения высококачественных товаров и появившиеся сервисные технологические возможности привели к стремительному развитию сектора электронной торговли.

Электронная торговля и электронная коммерция — это специфические формы торговли, появившиеся только с развитием информационно-коммуникационных технологий (ИКТ) и использующие различные интернет-сервисы, сделавшие возможными не только «розничную куплю-продажу», но и осуществление крупных торговых сделок с помощью сети Интернет. Общий рост масштабов продаж в системе электронной торговли может быть обусловлен как ростом рынков формата «Business-to-Business» (B2B), так и увеличением объемов электронной коммерции формата «Business-to-consumer» (B2C).

Следует отметить, что под получившими распространение терминами электронная коммерция и электронная торговля, подразумеваются сложные динамические системы, представленные большим количеством организационно-технологических звеньев и информационных связей, которые не являются окончательно устоявшимися и по мнению авторов данной статьи, нуждаются в дальнейшем, более подробном обсуждении.

Вместе с тем, несмотря на то, что ИКТ позволяют не только эффективно управлять производственно-технологическими процессами и решать многие задачи в сферах управления финансами, сервисного обслуживания населения и торговли, их применение часто приводит к появлению целого ряда организационных, экономических и технологических проблем и новых угроз, связанных в том числе, с информационной безопасностью не только отдельных предприятий, но и целых отраслей народного хозяйства.

Так, например, внедрение торговых онлайн-платформ и информационно-технологических инноваций в процессы купли-продажи приводит к появлению угроз утечек данных об участниках торговых операций с последующим возникновением рисков значительных экономических потерь.

Актуальность и необходимость решения этих проблем в сфере электронной торговли обусловлена многими особенностями, к которым, в частности могут быть отнесены не только масштаб возможных экономических потерь, распределенный «телекоммуникационный» характер и скорость возникновения киберугроз, но и то обстоятельство, что киберпространство в сфере электронной торговли представляет собой сложную динамичную, быстро изменяющуюся среду, для обеспечения безопасности которой, необходимы согласованные действия всех заинтересованных участников.

Сфера современной электронной торговли обусловила появление многих перспективных видов экономической деятельности. К современным тенденциям, формирующимся на рынке онлайн-торговли, можно отнести: замену посредников и пунктов офлайн-торговли на программно-цифровые платформы и электронные онлайн-площадки; создание систем прямой поставки товаров от производителя к покупателю для минимизации дистрибьюторской наценки и затрат на промежуточную складскую логистику.

Информационно-экономические функции, востребованные в ходе электронных торговых бизнес-процессов, реализуются на основе компьютерные сетей и организационно-технологических элементов, поддерживающих функционирование комплекса программно-аппаратных средств. В [1] отмечено, что к стандартным онлайн-функциям типового интернет-магазина, востребованным в ходе торговой сделки, могут быть отнесены функции приема, обработки заказов и информирования покупателей. В ряде случаев для организации электронного сетевого обмена данными может использоваться, например, электронная почта.

Согласно [2] в системах электронной торговли могут быть передаваемы различные типы данных, представленные: в формате видео и аудио; web-сайты и web-контент; в виде документов; в виде отдельных файлов с данными; файлов с исполняемыми программами; в виде презентаций и электронных таблиц.

В качестве основных функций, присущих сфере электронной торговли, можно выделить: электронный маркетинг, подразумевающий поиск объектов и субъектов экономической деятельности, таргетинг и рекламу предлагаемых товаров и услуг; подготовка, хранение и доставка товаров для реализации напрямую связанные с осуществлением купли-продажи товаров; менеджмент цепочек поставок и запасов; получение данных с помощью автоматизированных систем; организация обмена информацией в электронном виде; денежные операции в электронной форме, представленные переводом средств и обработкой транзакций онлайн; анализ эффективности проведенной торговой деятельности; разработка краткосрочных и долгосрочных прогнозов колебаний спроса на различные группы товаров. Успешная реализация этих функций возможна лишь при условии обеспечения достаточного уровня информационной безопасности.

В связи с данным обстоятельством, согласно [3, 4], из-за необходимости осуществления достаточно высокого уровня информационной безопасности, информационные и финансовые транзакции относятся к дорогостоящим операциям.

Организационная структура интернет-магазина может быть построена по типовому принципу и содержать традиционные информационно-функциональные подразделения «фронт, мидл и бэк-офисы», однако для повышения эффективности торговли и увеличения прибыли могут быть реализованы инструменты и сервисы клиентского анализа. В базе данных интернет-магазина может хранится информация о заказах, товарах, постоянных покупателях. С помощью прямого доступа или файлового обмена информацией обеспечивается актуализация базы данных корпоративной информационной системы, в ходе которой могут быть обновлены, например, данные о товарных остатках [1].

Если под интернет-магазином, ориентированным на самостоятельное получение прибыли и, посредством которого клиенты совершают покупки, можно понимать сайт, торгующий товарами в розницу посредством сети Интернет, то под термином электронная торговая площадка (ЭТП) часто понимают интернет-ресурс, обеспечивающий организаторам площадки получение дохода, как правило, за счет комиссии от проведенных сделок. Условно можно считать, что электронная торговая площадка является рабочим местом, где не только заключаются сделки купли-продажи между предприятиями, но и могут быть организованы различные конкурсы и аукционы различных типов.

Вместе с тем в период резкого увеличения объемов продаж электронная торговля столкнулась с целым рядом серьезных проблем, к которым можно отнести, например, логистические задержки, увеличение рисков отмены заказов, необоснованное повышения цен. Усилились проблемы безопасности торговых операций и возросли риски интернет-мошенничества.

В настоящее время к числу лидеров электронной торговли в России, чаще других относят: «Ozon», «Ситилинк», «Wildberries» и «М.Видео». Можно считать, что эти компании уделяют должное внимание вопросам информационной безопасности, так как в последнее десятилетие не допускали кражу данных своих клиентов и поэтому обладают определенными конкурентными преимуществами в торговой деятельности.

Вместе с тем, согласно [5] мировая электронная коммерция в результате мошеннических действий, использующих уязвимости IT - технологий в 2020 год потеряла около 17,5 миллиардов US долларов. В соответствии

с прогнозами, разработанными на основании анализа динамики трендов потерь за предыдущие периоды, ожидается, что в 2021 году потери мировой электронной торговли от мошеннических действий составят уже 20 миллиардов US долларов, что соответствует 18% росту и свидетельствует об отсутствии должного внимания к вопросам информационной безопасности электронной торговли.

В соответствии с [6], на долю сайтов, связанных с электронной коммерцией и банковским сектором экономики, приходится почти половина всех негативных воздействий в виде сетевых атак, взломов, краж данных

В [7] отмечено, что в связи с уязвимостью сервера ElasticSearch в 2020 году произошла утечка клиентской базы интернет-магазина Decathlon и сведения более чем о 123 млн клиентов оказались в открытом доступе. В частности, злоумышленникам стали известны не только журналы ошибок программных интерфейсов (API), пароли клиентов и незашифрованные электронные письма, но и исчерпывающая личная информация о сотрудниках, включающая сведения о датах рождения и условиях рабочих контрактов.

Своеобразным переломным моментом, благоприятно сказавшимся на финансовых показателях отрасли электронной коммерции, стала пандемия COVID-19, так как по оценкам экспертов объем российского рынка онлайн-коммерции вырос в 1,5 раза, что было обусловлено, введением карантинных мер и повсеместным переходом на дистанционный режим. В свою очередь, повышение доходности торговых операций привело к увеличению количества злоумышленников, желающих обогатиться преступным способом.

Согласно [8] одна из крупнейших мировых площадок электронной коммерции, Alibaba сообщила, что в результате многомесячной кибератаки были похищены 1,1 млрд записей с именами, телефонными номерами и другими персональными данными. По сообщению компании злоумышленником оказался сотрудник компании-консультанта, который с помощью специального программного обеспечения осуществлял несанкционированное сканирование служебной информации.

При поиске необходимого товара, неосторожные покупатели часто оставляют собственные персональные данные на различных интернет-платформах, посредством принятия предложенных условий хранения и обработки персональных данных.

В [9] отмечено, что при утечке клиентских персональных данных различного рода в руки третьих лиц существуют проблемы установления вины конкретного лица, ответственного за дальнейшее незаконное распространение персональной информации клиента. Полученные персональные данные могут быть использованы для формирования навязчивой и нежелательной таргетированной рекламной рассылки «о выгодных предложениях».

В качестве основных опасений пользователей систем электронной торговли, можно назвать возможное отсутствие средств эффективной защиты и гарантий сохранности и конфиденциальности персональных данных и возможности вторжения злоумышленников в личное пространство пользователя.

Так, например, в [10], к негативным факторам применения информационных технологий отнесены опасения пользователей сети интернет относительно качества и степени защиты их личной информации при совершении финансовых операций. Согласно [11], недостаточный уровень безопасности при проведениях торговых сделок на рынке онлайн торговли может повлечь к повышенным издержкам на безопасность со стороны покупателя, что является невыгодным для него предложением и может привести к уходу с рынка электронной торговли. По этой причине при недостаточной защищенности информационной среды электронных площадок продавцам данных площадок приходится дополнительно нести затраты на обеспечение достойного уровня информационной безопасности для обеспечения защиты потенциальных покупателей.

В качестве негативных последствий для бизнеса можно назвать репутационные потери, расходы на ликвидацию последствий взлома, а также штрафы. Стоит отметить, что онлайн-торговля неразрывно связана с хранением и обработкой данных различного рода и чем большим объемом данных обладает компания, тем большим интересом является её взлом, среди самой интересной для взломщиков информации можно выделить платежные данные и данные об их владельцах.

Несмотря на то, что в последние годы наблюдается тенденция увеличения кибератак именно на отрасль электронной розничной торговли, в соответствии с [12], с точки зрения экономической целесообразности для злоумышленника наиболее притягательным объектом для посягательств на защищаемую информацию, являются юридические лица, осуществляющие, как правило, большие обороты денежных средств. По этой причине, как правило, злоумышленники пытаются преодолеть системы защиты, в тех случаях, когда стоимость защищенной информации превышает или хотя бы соизмерима с затратами на осуществление «взломов» систем информационной безопасности.

В связи с тем, что главной целью участников любой торговой операции может быть получение выгоды в не только в виде прибыли или недопущения ущерба, но и в других формах и видах, целесообразно связывать термины информационная и экономическая безопасность. Удобство совершения покупок в любое время, снижение затрат времени для выбора товаров, возможность сравнения цен различных онлайн-продавцов являются факторами, привлекающими людей пользоваться средствами электронной торговли.

В свою очередь, организаторы электронных площадок получают комиссионные выплаты, а продавцы на электронных площадках получают возможность популяризировать бренд, улучшить репутацию компании и увеличить прибыль.

В связи с вышеперечисленными обстоятельствами одной из главных и важнейших задач цифровой экономики в сфере электронной торговли следует считать задачу обеспечения информационно-экономической безопасности электронной торговой площадки и электронной торговли. В определенном смысле можно считать, что электронная торговая площадка — это то место, в котором происходит процесс электронной торговли.

Предлагаем трактовать термин информационно-экономическая безопасность электронной торговли как сложное системное понятие, представленное совокупностью решений организационно-технического характера, реализованных на основе комплекса современных информационно-коммуникационных возможностей для обеспечения нормального осуществления процессов торговой деятельности и при условии достижения требуемых значений показателей экономической целесообразности торговой операции. В соответствии с предлагаемой формулировкой можно определить информационно-экономическую безопасность как некоторое стабильное состояние, при котором не причиняется ущерб информационной и экономической составляющей торговой операции.

Вместе с тем, следует принимать во внимание относительный характер стабильности, обусловленный динамическими процессами, происходящими во внутренней и внешней информационно-экономической среде. Информационным угрозам со стороны третьих лиц могут быть подвержены различные организационно-технологические компоненты комплекса электронной торговли доступные через сеть интернет, количество пользователей которого в России, достигло к настоящему времени, почти 100 млн человек и из которых 90 % пользуется им практически ежедневно.

К компонентам комплекса электронной торговли могут быть отнесены, например: браузеры; процессинговые и биллинговые комплексы; программные интерфейсы приложений (API), представленные в мобильных и стационарных формах и осуществляющие взаимодействие между филиалами компании и сервисами партнеров, а также приложения, предназначенные для корпоративных целей. Несанкционированное проникновение злоумышленников в системы электронной торговли может привести к: разрушению информации; искажению информации (модификации или замене информации, содержащейся на веб-страницах ЭТП); блокированию информации (нарушение работоспособности и доступности интернет-ресурсов, например, в результате DDoS-атак); утечке информации (краже персональных данных и несанкционированное скачивание информации с веб-страниц сайтов другой конфиденциальной информации.

По мнению автора работы [13], «с помощью сети Интернет осуществляется более тридцати видов мошеннических действий», а к препятствиям, возникающим на пути развития электронной коммерции в России, следует отнести, в частности, мошеннические сделки, осуществляемые с помощью реквизитов карточек, похищенных у клиентов фиктивными интернет-магазинами. В [14] отмечено, что к угрозам в сфере электронной коммерции относятся: различные виды вирусных атак; отказы в обслуживании; внешние риски преднамеренного вмешательства в процессы нормального функционирования компьютерных сетей; риски утечек инсайдерской информации; риски финансового мошенничества; взломы технических средств защиты информации, перехват, несанкционированное чтение или повреждение данных; несанкционированная идентификация пользователей систем электронной торговли. В соответствии со сведениями, приведенными в [15], 26% сетевых атак направлены: на браузеры клиентов web-приложений; 18% на систему аутентификации пользователей и 22% связаны с отказом в обслуживании сервисов web-приложений. К основными направлениям киберпреступлений в российском сегменте электронной торговли также часто относят фишинг и парсинг с использованием ботов.

В работе [16] отмечено, что безопасность корпоративных информационных систем зависит на 30% от применяемых технических решений, на 40% от проводимых организационных мероприятий и на 30% зависит от морально-нравственного и общекультурного уровня пользователей. Это означает, что не только программно-аппаратные средства, но также и сознательность, и компетентность персонала являются важными факторами информационной безопасности электронной торговли.

Повысить уровень информационной защищенности онлайн-торговли можно с помощью специальных ложных приманок, заставив злоумышленника пойти по «ложному следу», на котором он будет вынужден потратить свои ресурсы на преодоление препятствий на пути к «фальшивому сервису». В свою очередь, администраторы системы безопасности, выиграв время смогут не только изучить злоумышленника, но и своевременно отреагировать на его действия [17]. С помощью технологий, обеспечивающих физический разрыв между доверенными и ненадежными сетями, можно повысить уровень безопасности, создав изолированные пути для перемещения файлов между внешним сервером и внутренней сетью [18].

Убедить потенциальных участников электронных торговых операций в наличии гарантированного уровня информационно-экономической безопасности, можно внедрив системы кибер-страхования, ориентированного на защиту любых компаний, бизнес которых прямым или косвенным образом связан с обработкой и хранением данных, от информационных рисков [19]. В [20] отмечено, что у России существует огромный потенциал для развития рынка услуг кибер-страхования и в будущем кибер-страхование будет одним из основных средств защиты от кибер-угроз и обеспечения необходимого уровня информационно-экономической безопасности.

Внедрение средств искусственного интеллекта, основанного на использовании поведенческой биометрии, позволит осуществлять интеллектуальный анализ трафика и фильтрацию сети, что позволит защитить электронную

торговлю от распределенных DDoS атак и минимизировать риски, связанные с мошенническими действиями, основанными на ранее украденных данных [18].

Заключение. Таким образом, по результатам проведенного исследования можно сделать выводы и сформулировать ряд рекомендаций:

– электронная торговля стала реалией современных социально-экономических отношений, в связи с чем необходима дальнейшая разработка теоретических и прикладных моделей рынков электронной торговли;

– несмотря на то, что повсеместное внедрение систем электронной торговли, приводит к появлению целого ряда положительных социально-экономических эффектов, возникают дополнительные риски и киберугрозы для информационно-экономической безопасности всех участников торговых операций;

– концепция информационно-экономической безопасности электронной торговли также не является окончательно сложившейся и нуждается в дальнейшем исследовании методами системного анализа;

– уровень информационной безопасности систем электронной торговли может быть повышен с помощью тестирования и оценки опасности возникновения специфических угроз со стороны новых: информационно-коммуникационных технологий, процессов преобразования информации и организационных процедур;

– для снижения уровня киберугроз в системах электронной торговли необходимо уделять внимание цифровой гигиене и информационной культуре всех участников операций на электронных торговых площадках;

– необходимо организовать обучение всех участников торговых операций (покупателей, продавцов и организаторов электронных торговых площадок) и обеспечить проведение мероприятий по усилению контроля над действиями пользователей и персонала;

– меры повышения информационной безопасности не должны вносить дополнительные трудности в осуществление торговых бизнес-процессов, так как увеличение затрат на поддержание безопасности может привести не только к удорожанию размещенных товаров, но и к риску потери клиентов;

– снижение рисков несанкционированного доступа к базам данных, оборудованию и каналам связи возможно за счет внедрения криптографических методов защиты информации, осуществляемых в числе комплекса других организационно-технических мероприятий.

СПИСОК ЛИТЕРАТУРЫ

1. Проблемы построения информационных систем электронной торговли. Моисеенко Н.А., Тасуева Х. З.-А. // Аллея науки. 2017. Т. 4. № 16. С. 929-932.
2. Транзакции электронной торговли через одноранговый канал обмена информацией. Бокатт Э.Д. Патент на изобретение RU 2439704 C2, 10.01.2012. Заявка № 2008152104/08 от 21.02.2007.
3. Защита систем Интернет-торговли. Халиуллина Э.И. // NovaInfo. 2016. №47-3. С. 12-15
4. Understanding use of consumer protection tools among Internet gambling customers: Utility of the Theory of Planned Behavior and Theory of Reasoned Action. Procter L., Angus D.J., Gainsbury S.M. // Addictive Behaviors. 2019. Vol. 99. P. 106-125
5. Juniper Research //Online payment fraud: emerging threats, segment analysis & market forecasts 2021-2025. 2021 // URL: https://www.juniperresearch.com/researchstore/fintech-payments/online-payment-fraud-research-report (Дата обращения: 25.06.2021)
6. PositiveTechnologies // Сборник исследований по практике безопасности. 2015. // URL: http://www.ptsecurity.ru/download/PT_Positive_Research_2015_RU_web.pdf (Дата обращения: 27.06.2021)
7. CBR Staff Writer // Decathlon Leaks 123 million Records via Insecure Elasticsearch Server. 2020 // URL: https://techmonitor.ai/technology/cybersecurity/decathlon-leaks (Дата обращения: 23.06.2021)
8. The Wall Street Journal // Alibaba Falls Victim to Chinese Web Crawler in Large Data Leak 2021. // URL: https://www.wsj.com/articles/alibaba-falls-victim-to-chinese-web-crawler-in-large-data-leak-11623774850 (Дата обращения: 25.06.2021)
9. Ответственность за нарушение правил обработки и хранения персональных данных при осуществлении электронной торговли. Расторгуева А.С. // Актуальные проблемы правоведения. 2018. № 1 (57). С. 20-21.
10. Основные направления обеспечения качества электронной торговли. И. М. Сафарова, А. С. Акимкина, А. И. Дерябина // Экономика и управление: новые вызовы и перспективы. – 2010. – № 1. – С. 312-316.
11. Безопасность рынка электронной торговли с точки зрения трансакционных издержек. Валько Д.В. // Национальные интересы: приоритеты и безопасность. 2012. Т. 8. № 12 (153). С. 59-64.
12. Интернет-агентство «Мибок» // Электронная коммерция: правовое регулирование и налогообложение. 2011 // URL: https://www.mibok.ru/about/press/elektronnaya-kommertsiya-pravovoe-regulirovanie-i-nalogooblozhenie/ (Дата обращения: 20.06.2021)
13. Методы защиты информации при организации торговли в сети интернет. Федоров А. А. // Инновации. Наука. Образование. – 2020. – № 23. – С. 335-346.
14. Информационная безопасность экономических систем: учебно-методическое пособие. Ясенев В. Н. Нижний Новгород: «Нижегородский госуниверситет им. Н.И. Лобачевского», 2006. С. 373
15. Технологии защиты интернет-технологий и web-приложений. В. С. Оладько, С. Ю. Микова, М. А. Нестеренко // Международный научный журнал. – 2015. – № 8. – С. 81-85.
16. Вопросы информационной безопасности в сфере электронной торговли. Милованович Н. Г. // Сибирский торгово-экономический журнал. – 2016. – № 1(22). – С. 217-218.
17. Разработка и тестирование программных модулей для оценки производительности OPENMP и OPENCL технологий. Нурутдинова И.Р., Хафизова А.Ш., Кормильцев Н.В., Уваров А. Д., Перухин М. Ю. // Вестник Технологического университета. Казань: Издательство »Казанский национальный исследовательский технологический университет», 2018. Т.21. №4. С. 202-205
18. Анализ целесообразности использования методов обеспечения информационной безопасности электронной коммерции в цифровой экономике. А. Д. Уваров, Н. В. Кормильцев // XXIV Туполевские чтения: Материалы Международной молодёжной научной конференции. В 6-ти томах, Казань. 2019. – С. 557-562.
19. Кибер-страхование: как обеспечить информационную безопасность бизнесу. Иванов И.К. // Большой портал для малого бизнеса – 2016, №16, С. 13-24
20. Страхование информационных рисков (киберстрахование). Т. А. Волкова, О. Н. Суслякова // Инновационная экономика: перспективы развития и совершенствования. – 2018. – Т. 1. – № 7(33). – С. 117-122.

УДК 004.056

КИБЕРРИСКИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ В СОВРЕМЕННЫХ РЕАЛИЯХ

Юмашева Елена Сергеевна
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mail: elena_umasheva@mail.ru

Аннотация. В данной статье рассмотрены причины роста киберпреступлений в финансовой сфере, а также выявлены некоторые способы улучшения стратегий защиты.

Ключевые слова: киберугрозы; атаки; информационная безопасность.

CYBER RISKS OF FINANCIAL ORGANIZATIONS IN MODERN REALITIES

Yumasheva Elena
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mail: elena_umasheva@mail.ru

Abstract. This article discusses the reasons for the rise in cybercrime in the financial sector, and also identifies some ways to improve protection strategies.

Keywords: cyber threats; attacks; information security.

Киберриски представляют растущую угрозу для финансовых учреждений. Масштабная кибератака потенциально может оказать значительное влияние на способность компании выполнять свои обязательства в полном объеме и своевременно. Финансовая индустрия является ключевой целью киберпреступников, потому что банки и другие финансовые учреждения хранят конфиденциальные персональные данные и обладают ценной информацией о финансовых операциях.

На слушаньях в конгрессе руководители шести крупнейших иностранных банков назвали наибольшие угрозы для их компаний и более широкой финансовой системы. И одним из наиболее популярных ответов был «кибербезопасность».

Растущая цифровизация в банковской системе и ускорение организации работы на дому в ответ на пандемию еще больше познакомили отрасль с киберпреступной деятельностью, значительно увеличив онлайн-коммуникацию.

Кибератаки могут нанести ущерб кредитным рейтингам в результате репутационного ущерба, а также денежных потерь. Например, в феврале 2016 года хакеры нацелились на центральный банк Бангладеш и использовали уязвимость SWIFT (единый международный стандарт, система, в которой банки по всему миру обмениваются информацией и данными о платежах [1]). Несмотря на то, что большинство транзакций были заблокированы, 101 миллион долларов все же исчезли. Это ограбление стало тревожным сигналом для всего финансового мира, что системные киберриски в финансовой сфере серьезно недооценены.

Сегодня оценка того, что крупная кибератака представляет угрозу финансовой стабильности, является аксиоматической - не вопрос, *если*, а *когда*.

Схема атаки. Выбор цели обусловлен технической подготовкой, имеющимися инструментами и знаниями о внутренних процессах банка. Каждая из атак безусловно имеет свои особенности, в частности действия различаются на этапе вывода денежных средств, но присутствуют также и общие черты.

Рис. 1. Основные этапы атаки.

Этап 1. Разведка и подготовка.

Задача – собрать как можно больше информации о банке, которая позволит преодолеть системы защиты, и провести предварительную организационную работу, учитывая специфику атакуемого банка. Так как сканирование внешних ресурсов может быть выявлено системами защиты, а, следовательно, привлечет не нужное внимание, злоумышленники прибегают к пассивным методам получения информации (поиск доменных имен и адресов), привлечение недобросовестных сотрудников.

По итогу работы первого этапа получаем:

– сведения о системах на сетевом периметре и используемом ПО;
– сведения о сотрудниках;
– сведения о партнерах и контрагентах;
– сведения о бизнес-процессах.

Подготовительные действия:

– разработка или адаптация вирусных ПО для используемых версий ПО и ОС;
– подготовка фишинговых писем;
– организация инфраструктуры;
– подготовка инфраструктуры для отмывания денег;
– тестирование инфраструктуры и вирусного ПО.

Этап 2. Проникновение во внутреннюю сеть

Фишинговая рассылка – является наиболее эффективным и распространенным методом проникновения в инфраструктуру. Другим вариантом распространения вредоносного По является взлом сторонних компаний, которые относятся к информационной безопасности не так серьезно, но сотрудники целевого банка часто посещают их ресурсы или сайты.

Этап 3. Развитие атаки и закрепление в сети

После получения локального доступа к сети банка, злоумышленникам необходимо получить права локального администратора. Это представляется возможным из-за:

– наличия устаревших версий ПО и отсутствия актуальных обновлений;
– множественные ошибки конфигурации;
– использование словарных паролей привилегированными пользователями;
– отсутствия двухфакторной идентификации [2].

На сегодняшний день две тенденции усугубляют киберриски. Во-первых, глобальная финансовая система переживает беспрецедентную цифровую трансформацию, которая ускоряется пандемией COVID-19. Банки конкурируют с технологическими компаниями; технологические компании конкурируют с банками. Между тем, пандемия повысила спрос на онлайн-финансовые услуги и сделала работу на дому нормой. Центральные банки по всему миру рассматривают возможность отбросить свой вес от цифровых валют и модернизации платежных систем. В это время трансформации, когда инцидент может легко подорвать доверие и сорвать инновации, кибербезопасность важна как никогда.

Во-вторых, злоумышленники используют эту цифровую трансформацию и представляют растущую угрозу для глобальной финансовой системы, финансовой стабильности и уверенности в целостности системы. Пандемия даже поставила новые цели для хакеров. По данным Банка международных расчетов, финансовый сектор испытывает вторую по величине долю кибератак, связанных с COVID-19, уступая только сектору здравоохранения.

В будущем следует ожидать более опасных нападений и последующих потрясений. Наиболее тревожными являются инциденты, которые разрушают целостность финансовых данных, таких как записи, алгоритмы и транзакции; в настоящее время доступно мало технических решений для таких атак, которые могут подорвать доверие в более широком смысле. Злоумышленники – это только все более смелые преступники, такие как группа Carbanak, которая нацелилась на финансовые учреждения, чтобы украсть более 1 миллиарда долларов в течение 2013-18 годов, но и штатные государственные команды, спонсируемые государством нападавших. Например, Северная Корея украла около 2 миллиардов долларов по крайней мере из 38 стран за последние пять лет.

Хотя кибератаки в странах с высоким уровнем дохода, как правило, попадают в заголовки газет, меньше внимания уделяется растущему числу атак на более мягкие цели в странах с низким и средним уровнем дохода. Тем не менее, именно в тех странах стремление к большей финансовой доступности было наиболее выражено, что привело многих к переходу на цифровые финансовые услуги, такие как мобильные платежные системы. Несмотря на то, что они продвигают финансовую доступность, цифровые финансовые услуги также предлагают целевую среду для хакеров. Например, взлом крупнейших сетей мобильных денег Уганды, MTN и Airtel в октябре 2020 года, привел к крупному четырехдневному сбою в проведении сервисных транзакций.

Несмотря на растущую зависимость глобальной финансовой системы от цифровой инфраструктуры, неясно, кто несет ответственность за защиту системы от кибератак. Отчасти это связано с тем, что окружающая среда меняется очень быстро. Без целенаправленных действий глобальная финансовая система станет только более уязвимой по мере того, как инновации, конкуренция и пандемия еще больше подпитывают цифровую революцию. Хотя многие субъекты угрозы сосредоточены на зарабатывании денег, количество разрушительных атак растет; кроме того, хакеры, также узнают о сетях и операциях финансовой системы, что позволяет им совершать более разрушительные атаки в будущем (или продавать такие знания и возможности другим). Эта быстрая эволюция ландшафта рисков обременительно реагирует на зрелую и хорошо регулируемой в остальном систему.

Улучшение защиты глобальной финансовой системы является в первую очередь организационной задачей. Усилия по ужесточению обороны и регулированию важны, но недостаточны для того, чтобы предотвратить растущие риски. В отличие от многих отраслей, сообщество финансовых услуг не испытывают недостатка в ресурсах или возможности внедрения технических решений. Основным вопросом является проблема коллективных действий: как

лучше всего организовать защиту системы между правительствами, финансовыми органами и промышленностью и как эффективно и результативно использовать эти ресурсы.

Фрагментация между заинтересованными сторонами и инициативами частично обусловлена уникальными аспектами и эволюционирующим характером киберрисков. Сообщество финансового надзора фокусируется на устойчивости, дипломатах - на нормах поведения государства, органах национальной безопасности - на попытке сдерживать вредоносную деятельность, а руководители отрасли - на конкретных фирмах, а не отраслевых рисках. По мере того, как границы между фирмами, предоставляющими финансовые услуги, и технологическими компаниями становятся все более нечеткими, линии ответственности за безопасность также становятся все более размытыми.

Для достижения более эффективной защиты глобальной финансовой системы от киберугроз Фонд Карнеги за международный мир опубликовал в ноябре 2020 года доклад под названием «Международная стратегия лучшей защиты глобальной финансовой системы от киберугроз». Разработанный в сотрудничестве со Всемирным экономическим форумом, в докладе рекомендуются конкретные действия по сокращению фрагментации путем содействия более тесному сотрудничеству как на международном уровне, так и между государственными учреждениями, финансовыми фирмами и технологическими компаниями.

Стратегия основана на четырех принципах:

Во-первых, требуется большая ясность в отношении ролей и обязанностей. Лишь немного стран построила эффективные внутренние отношения между своими финансовыми органами, правоохранительными органами, дипломатами, другими соответствующими государственными субъектами и промышленностью. Существующая фрагментация препятствует международному сотрудничеству и ослабляет коллективную устойчивость, восстановление и возможности реагирования международной системы.

Во-вторых, международное сотрудничество необходимо и срочно. С учетом масштабов угрозы и глобально взаимозависимого характера системы, отдельные правительства, финансовые фирмы и технологические компании не могут эффективно защититься от киберугроз, если они работают в одиночку.

В-третьих, сокращение фрагментации высвободит потенциал для решения этой проблемы. В настоящее время осуществляется много инициатив по лучшей защите финансовых учреждений, но они остаются изолированными. Некоторые из этих усилий дублируют друг друга, увеличивая операционные издержки. Некоторые из этих инициатив достаточно зрелы, чтобы ими можно было бы обмениваться, лучше координировать и дальнейшую интернационализацию.

В-четвертых, защита международной финансовой системы может быть моделью для других секторов. Финансовая система является одной из немногих областей, в которых страны явно заинтересованы в сотрудничестве, даже когда геополитическая напряженность высока. Сосредоточение внимания на финансовом секторе является отправной точкой и может проложить путь к лучшей защите других секторов в будущем.

Правительства могут поддержать эти усилия, создав подразделения для оказания помощи в оценке угроз и координации ответных мер. Сбор разведывательных данных должен включать в себя акцент на угрозах финансовой системе, и правительства должны обмениваться такой разведданной информацией с союзниками и странами-единомышленниками.

СПИСОК ЛИТЕРАТУРЫ

1. Дарья Черкудинова. Что такое SWIFT и почему российские банки хотят The Village разбирается, чем российской финансовой системе грозят новые санкции, в частности отключения SWIFT [Электронный ресурс] – Режим доступа URL: https://www.the-village.ru/city/situation/174921-chto-takoe-svift
2. Векторы хакерских атак на банки [Электронный ресурс] – Режим доступа URL: https://www.ptsecurity.com/ru-ru/research/analytics/banks-attacks-2018/

УДК 742.012

АНАЛОГИИ ПРЕДСТАВЛЕНИЯ ДАННЫХ. ПЛАНОВАЯ ЭКОНОМИКА

Ярошевич Людмила Ивановна
Санкт-Петербургский государственный институт кино и телевидения
Правды ул., 13, Санкт-Петербург, 191119, Россия
e-mail: Ludmila-arttech@rambler.ru

Аннотация. Единая система обратной информационной связи. Иерархическая система представления данных в виде плана. План как проекция рационального логического мышления. Естественные законы восприятия. Фазовая терминология представления данных. Формирование правильных словосочетаний в вербальной диаграмме «Экономика».

Ключевые слова: информационная обратная связь; статус термина экономика; план; диаграмма; фазовое восприятие; фазовое моделирование; фазовая терминология.

UNIFIED DATA PRESENTATION SYSTEM. PLANNED ECONOMY

Yaroshevich Ludmila
The St. Petersburg State institute of film and television
13, Pravda str., St. Petersburg, 191119, Russia
e-mail: Ludmila-arttech@rambler.ru

Abstract. Unified information feedback system. Hierarchical system presenting data as a plan. Plan as projection of rational logical thinking. Laws of perception. Phase terminology of data representation. Formation correct phrases verbal diagram «Economy».

Keywords: information feedback; status of term economy, plan, diagram; phase perception; phase modeling; phase terminology.

«Экономика» является названием целой области, подведомственных ей, составляющих наименований [1]. Термин «Экономика» «возглавляет» всю систему организации и управлении хозяйством страны. Это – титул, предполагающий особый лингвистический статус. Под термином «Экономика» следует понимать вербальное соподчинение составляющих ее частей в иерархической зависимости [2], Данное устройство напоминает о понятии субординация, в системе строгого служебного подчинения подотчетных структур.

Рассмотрим две вербальные величины: Область и Отрасль, первую из них, нужно понимать как автономную (самостоятельную) структуру, а вторую, Отрасль, как подчиненную первой. Подтверждением служит устаревшее понимание слова Отрасль = Отпрыск (потомок) [3]. Кроме того, Область – более широкомасштабное понятие. Поэтому, «Экономику» мы называем областью народного хозяйства, которая управляет и решает важные вопросы, а управляет она отраслями народного хозяйства, такими как: промышленное производство, сельское хозяйство, лесное хозяйство, рыбное хозяйство, транспорт, …

К слову сказать, создается впечатление, что слова область и отрасль изначально созданы для вербальных фазовых диаграмм представления данных.

Путь развития экономики, это – правильно выбранное направление, точно выбранный курс - план, который ничуть не менее важен, чем курс движения авиа и морских судов, при котором отклонение от заданного направления движения является нарушением правил безопасности и, в целом, нарушением рабочего цикла. Из сферы образования возьмем в пример, «Курс лекций», где Курс, как Навигатор, ведет в определенном направлении к достижению цели образовательного процесса.

Также и в экономике, составляется план развития, который ориентирован на решение программных задач. План, как продукт человеческой мысли имеет векторную направленность умственных рассуждений. В плане должен быть соблюден полный цикл намечаемых процессов. В нем, в обязательном порядке, должно быть наличие введения, определенной последовательности выполнения намеченных работ и достижение конечного результата. В этом смысле, система организации задач экономики эквивалентна фазовой диаграмме. Где план – не просто слова, это – проект фазовой реализации рационального логического замысла.

В наши дни недостаточно осознается значение термина План. Нельзя недооценивать тексты, написанные человеком для человека. План является результатом обработки информации человеком, на основе анализа ситуации, накопленных знаний и опыта, представляется кратко, в последовательном изложении. План, как ведущая структурная направляющая сила, «ведет исполнителя за руку», соблюдая определенную последовательность, указывает на цели, задачи, содержание, объемы, сроки, методы выполнения намеченных проектов. Как и всякое другое изображение, план имеет внутреннюю композиционную структуру, которая способствует его прочтению и освоению. Цель плана – управление и связь. Стремление некоторых современных авторов выкинуть понятие план из экономических текстов не правомерно и нарушает намеченный ход развития.

В текстах даже условные обозначения не случайны. Т.е. мы получаем не только нужную информацию, но вместе с тем, знаки препинания регулируют наше дыхание при прочтении. Текст подготовлен для передачи информации с помощью грамматических правил и условных обозначений.

Терминология в экономике представляет собой содержание составляющих ее частей. Где каждый термин занят в конкретной фазе соответствующего процесса единого цикла.

В разговорной речи и печатных работах появились следующие фразы: «цифровая экономика», «рыночная экономика», «цифровой художник». Грамотно ли звучат эти фразы? Чтобы понять, попробуем провести аналогии, например: «нотная музыка», «кирпичное градостроительство», «базарная экономика», «линейный художник». Выглядит «не очень»! Этот путь ведет к хаосу. Цифра и число – понятия разные. Очевидно, лучше сказать: информационные технологии в экономике, в музыке, в проектировании, художник анимации и компьютерной графики.

Главное в экономике - и не цифра и не рынок, главное это – план, который вносит структурный порядок в реализацию намеченных целей с помощью различных технологий.

Теперь о рынке: рынок относится к сфере отраслевого производства и потребления. Нельзя это понятие соединять с заглавной областью народного хозяйства. Фраза «рыночная экономика» - не корректна! Всякое понятие должно находиться на своем месте в целостной системе «Государственная плановая экономика».

Понятия «Экономика» и рынок лежат на разных информационных уровнях. Они, безусловно, связаны между собой способом соподчинения. Поэтому, рынок должен выполнять свои функции, находясь в подчинении у государственной власти. При этом рынок – далеко не главная и не единственная подчиненная структура. Доля каждой отрасли важна и нет нужды вырывать рынок из единой связки всех отраслей, вместе, представляющих народное хозяйство. Рынок, существующий вне сбалансированных отношений государственной экономической системы, становится случайным и, больше похож на базар. Хорошо продуманная экономика может быть только плановой.

План экономического развития это – научно обоснованный документ, который является гарантом рационального управления экономикой страны. Он имеет естественное происхождение, это продукт деятельности человеческого мозга в обратной связи.

Без мозгов, нет будущего у финансового рынка. Как ни странно, о них (о мозгах) никто и не вспоминает, предлагая новый национальный проект, так называемой «цифровой экономики», и даже не Экономики, а «экономической деятельности». Смущает ли кого-нибудь, что итогом глобального финансового рынка может стать чье-нибудь банкротство? Если бы это было кому-то не выгодно, никто бы этим не занимался. Это – новая компьютерная игра, в которой, прокладывается путь: от финансовой несамостоятельности к финансовой несостоятельности. О реализации проекта на просторах интернета пишут так: «Это довольно сложный и многогранный процесс, который должен учесть интересы всех игроков рынка, при этом сформулировать правовые правила игры».

Интересно отметить, что правила это и есть план. Рассмотрим однокоренные слова в их взаимосвязи: от правил наши «гости» идут к правам, далее к управлению,… «Праведники», эдакие! Глобальному финансовому рынку мы интересны пока у нас есть деньги и сырьевые ресурсы. Рыночные отношения выстраивают рыночные игроки, у которых часто мнения не совпадают. Договариваться умеют далеко не все. Чаще развязываются войны.

Где наша государственная плановая экономика?

Технологии это – методы, методики и способы. Есть такое понятие – техницизм, что означает увлечение технической стороной дела в ущерб его сущности. Можно так увлечься, что Экономика, без плана, предусматривающего контроль, и вовсе исчезнет. Останется только глобальный финансовый рынок, не в нашей стране, и мы с протянутой рукой.

Сравним терминологию «Государственная плановая экономика» или «цифровая экономика» или «цифровизация экономической деятельности», … Какая из этих записей, по-вашему, выглядит разумно и достойно?» В двух последних «новообразованиях» нарушен логический порядок представления данных, а именно – пострадала структура, т.е. взаиморасположение и связь составных частей, взятых из разных фаз общего цикла передачи информации. В языковой практике, когда мы говорим о главных и второстепенных членах предложения, мы подразумеваем их иерархическую зависимость. Информационные технологии, применяемые в экономике или образовании, не должны стоять выше рангом самой экономики или образования. Главное сохранить рациональное мышление в управлении экономикой и образованием.

«Этот мир придуман не нами…», и мы до сих пор изучаем его композиционные составляющие части, структурные связи, словосочетания и слова. В каждой фазовой диаграмме «речь идет о строгой и общей зависимости» происходящих процессов, биологи пишут, что животные, птицы и насекомые живут по уникальному плану. И каждая стадия в их развитии жизненно важна. Пробел или ошибка в цикле делает его репродуктивную функцию невозможной.

Специалисты пишут о недостатках плановой системы. Мол, что-то было не так, но и на солнце, как известно, есть пятна. Да и в любой другой системе хозяйственных отношений будут и достоинства, и недостатки.

План это – порядок. А теперь посмотрим на антонимы к слову план, любопытно, но антонимов к слову план не нашлось, хотя нет, это вероятно – хаос. А синонимов к слову план предостаточно: намерение, перспектива, проект, программа, мероприятие, диаграмма, расписание, комбинация, тактика, действие, маневр, и т.д. Кто сказал, что план нам не нужен? План является уникальной структурой организации информации не только в экономике, но и во всех других представлениях данных: в литературе, в живописи, в кинопроизводстве, в структуре учебников, мыслительных процессах, … План, как заранее намеченная система деятельности, сопровождает человека повсюду. Не успев проснуться, человек начинает планировать свой день, а что было бы без расписания в школе, расписания движения транспорта? Причина обязательного наличия плана во всех структурах изображения данных обусловлена законами аудиовизуального восприятия и передачи информации в обратной связи. С помощью плана (фазовой схемы - диаграммы) мы, биосистемы, передаем информацию в пространстве и во времени. Убрать план из экономики означает не только разрушить ее как систему, но и разрушить все информационные связи. Это – опасность!

Плановая экономика и централизованное государственное управление материальными ресурсами обеспечивают стране стабильность и равномерное поступательное развитие.

Посмотрим на примеры от «специалистов сервиса», так называемой, «рыночной экономики»: «…рыночная экономика опирается на личные интересы, ограничивает роль правительства»; «…гарантирует свободу потребителя,

что выражается в свободе потребительского выбора на рынке товаров и услуг»; «В рыночной экономике ограничено вмешательство государства в хозяйственную деятельность»; «Градуализм» - предполагает проведение реформ медленно, шаг за шагом. Источником рыночных преобразований данная концепция видит государство, которое должно постепенно заменять элементы административно-командной экономики рыночными отношениями». Эти примеры взяты из интернета, работа называется «Факторы формирования российской модели рыночной экономики», Н.В. Ворошиловой, эксперта по предмету «Экономика». Ну и ну…?! Как оказывается, чтобы населению свободно выбрать и купить себе новые трусы и майки, нужно чтобы государство в это не вмешивалось. Круто!!!

Рассматривая названия четырех видов экономических систем, следует заметить, что нет достойной формулировки и организованного представления данных о каждой из них:

1. Традиционная экономика;
2. Командно-административная (плановая, командная, государственная, директивная) экономика;
3. Рыночная экономика;
4. Смешанная экономика.

Если бы любое государство гордилось своей экономикой, то и название ей придумало бы более грамотное и звучное. Как говорится, как корабль назовешь, так он и поплывет.

В современном понимании устройства государственной системы экономического развития план играет самую главную роль в любой экономике и в решении любого вопроса. Он осуществляет и поддерживает общую структуру данных, что позволяет легче соотносить пропорции частей этого плана, облегчает скорость поиска нужного раздела, является руководством для подчиненных структур разного уровня, помогает осуществлять контроль.

План может быть представлен в цифровых, вербальных, картографических, нотных, художественно-графических, знаковых системах [4]. Он может быть придуман (задуман). Им можно поделиться (он поделился своими планами на завтра).

По аналогиям представления данных в виде самостоятельных планов, все экономики мира смогут легче найти точки соприкосновения и взаимовыгодной поддержки.

Все попытки избавиться от государственного плана, внести в него элементы дезорганизации или искажения должны пресекаться по закону.

СПИСОК ЛИТЕРАТУРЫ

1. Ярошевич Л.И. «Моделирование функции внимания при создании безопасных информационных технологий построения изображений». II Межрегиональная конференция: Информационная безопасность регионов России (ИБРР-2001), (Санкт-Петербург, 26-29 ноября 2002 года), с.72-75.
2. Ярошевич Л.И. «Аналогии представления данных. Вербальные диаграммы». Материалы XVII, Санкт- Петербургской международной конференции. Часть 2. «Региональная информатика (РИ-2020)». Санкт – Петербург, 28-30 октября 2020 г. с.224-225.
3. Ожегов С.И. и Шведова Н.Ю. Толковый словарь русского языка Москва, «АЗЪ», 1995 г.
4. Ярошевич Л.И. «Системный подход к теории искусствознания» Материалы юбилейной X Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР - 2017)» Санкт-Петербург, 1-3 ноября 2017 г. с.134-135.

УДК 742.012

ПЛАН КАК ЭКВИВАЛЕНТ ФАЗОВОЙ ДИАГРАММЫ

Ярошевич Людмила Ивановна
Санкт-Петербургский государственный институт кино и телевидения
Правды ул., 13, Санкт-Петербург, 191119, Россия
e-mail: Ludmila-arttech@rambler.ru

Аннотация. Цикл процесса передачи информации в обратной связи предполагает аналогичную фазовую структуру представления данных и соответствующую фазовую терминологию. Определение – план. Варианты применения плана на практике. В процессе смены фаз возникают новые формы и появляются их новые названия.

Ключевые слова: информационная обратная связь; сопроводительная фазовая терминология, план, трансформация фазового состояния.

THE PLAN AS THE EQUIVALENT OF A PHASE DIAGRAM

Yaroshevich Ludmila
The St. Petersburg State institute of film and television
13, Pravda str., St. Petersburg, 191119, Russia
e-mail: Ludmila-arttech@rambler.ru

Abstract. The cycle of the information transmission process in feedback assumes a similar phase structure of data representation and the corresponding phase terminology. Definition plan. Options for applying the plan in practice. In the process of changing phases, new forms appear and theirs new names appear.

Keywords: information feedback; accompanying phase terminology, plan, transformation of the phase state.

Термин ПЛАН связан с кибернетикой гораздо больше, чем с Государственным планом экономического развития СССР, хотя его применение в этом случае было очень уместным и грамотным.

Его можно сравнить с многофункциональным передатчиком информации. Это - термин из системы передачи и хранения информации, это – проекция результатов аналитической работы мозга. Именно план формирует структуру текста, его логически обоснованное, последовательное изложение. Он может рассматриваться как вербальная, нотная, художественно-графическая, … диаграмма, описывающая полный цикл процесса передачи информации, в границах данного изображения. Противникам плана следует сказать, что другого пути моделирования изображений не существует.

Всем изображениям, присущи аналогии структурного построения, что делает их устройства похожими. Например, план, в краткой форме оглавление /содержание в конце или начале книги, показывает читателю последовательный фазовый ряд данных, формирующих полный текст.

«Система аудиовизуального восприятия человека – одна и та же на все случаи получения и передачи информации» [1]. Поэтому можно смело говорить о законах композиции единых для картинной плоскости, градостроительного плана, графики, архитектурного стилевого дизайна, музыки, литературы и т.д. В понятии план должен быть соблюден весь цикл процессов, участвовавших в его создании, начиная от настройки на мыслительный процесс, приложения ума, развитие содержания и выводы. Все ступени этой цепочки важны, поскольку уровни иерархии мозговых процессов в обратной связи проецируются в изображения с эквивалентной структурой.

В качестве примера, рассмотрим взаиморасположение и связь составных частей книги:

Оглавление: указатель частей, связанных по содержанию. На примере оглавления/содержания книги мы видим фазовое формообразование слова план. План раскрывает глубинную перспективу представления данных в пространстве и времени.

Предисловие - напутствие автора, предшествующее тексту.

Введение, его цель - вовлечь, помочь освоиться с текстом, направить внимание читателя.

Прежде, чем начать какое-либо действие, нужно настроиться на него. Настроить музыкальный инструмент, певице нужно распеться, хирургу обдумать план предстоящей операции, писателю собрать материал, приготовить напутствие читателю, экономистам продумать до мелочей с чего начать писать план экономического развития. Это и есть ничто иное как, самое начало любой работы, первая фаза задуманного цикла мероприятий предшествующих самой работе и ее результату. В полном цикле, в обратной связи в изображении этот период подготовки проецируется в отдельную самостоятельную часть, которая называется: введение. Синонимы к слову введение: прелюдия, увертюра к опере, вводная часть, начало, вступление, настройка.

Далее, по плану, идет последовательное изложение текста - главы, в центре должно быть главное содержание. Главное, от слова голова, отсюда главы.

Для фиксации внимания в иерархической последовательности существуют акценты, выстраивающие перспективу представления данных. Они не однородны. Они разные по напряжению. Абзац – отступ, который помогает читателю перейти от одной мысли к другой.

Заключение – последняя, заключительная часть содержит вывод. В басне это завершается моралью.

Синонимы к слову заключение: итог, вывод, финиш, решение, постановление, результат, завершение.

Представленный выше пример выявляет функции плана:

1) управляющую;
2) проектирующую;
3) обеспечивающую внутреннюю структуру, помогающую прочтению текста;
4) соблюдение фазового порядка логически обоснованного изложения;
5) поддерживающую связь с другими формами представления данных.

Разновидности плана:

1) проект;
2) оглавление;
3) список, табель;
4) расписание;
5) чертеж)

Технологические приемы:

1) диаграмма;
2) перспектива;
3) масштаб;
4) выбор знаковой системы;
5) условные обозначения.

Последовательная смена состояний объекта называется процессом. Каждая фаза цикла от 1й до завершающей фазы соответствует уровню мышления на момент ее существования. Соподчинение ступеней развития показывает весь цикл, формирующий понятие план. Все части внутри цикла связаны единством замысла. Это подтверждает, что понятие план – циклическая форма. Короткое слово план проходит свой цикл развития, прежде чем стать формой,

готовой к употреблению. Разновидности понятия план это – его синонимы, что говорит о его широком применении в информационном поле.

Далее рассмотрим пример ПЛАНовой экономики. Сегодня рекламируется и предлагается «рыночная система отношений». Наблюдается тенденция уйти от плановой экономики, от целого и полного к части. Из советского курса математики помним: делимое, делитель, частное.

Т.е. от общего понятия «Экономика» к частному, частичному. От общего «Образование» к частному, частичному, не полному.

Однако, рынок это – сегмент, только часть всех необходимых параметров. Необходимо иметь в виду, что при этом искажается управляющая роль термина «Экономика», в единой системе отраслевых составляющих величин. Нарушается многоуровневый порядок логического соотношения системной структуры.

В результате применения разновидностей плана на практике мы имеем: начертательную геометрию, топографическую карту, плановый бизнес, план текста, рабочий план, таблицы, расписания, разного рода проекты, архитектурные планы, литературу, живопись, математику, историю,.. мы живем по плану.

Цикл процесса передачи информации в обратной связи предполагает аналогичную фазовую структуру представления данных и, соответствующую фазовую терминологию. В последовательном иерархическом представлении данных прослеживается соблюдение законов восприятия и соответствие структуры изображения уровням зрительного поля. В готовом изображении это выражается в понятиях: пространственные уровни, «табель о рангах», 1-й, 2-й, 3-й, … планы, средний план, косвенный план, дальний план…

Посмотрим на варианты определения План, взятые из разных источников:

1. Самое простое определение плана из Википедии гласит: «План – первоначально означало равнину, позже стало использоваться в геометрии, в значении плоскость, а также и проекции отдельного предмета на эту плоскость».

Недостатки:

а) Следует добавить, что помимо «проекции отдельного предмета на плоскость» человечество веками проецирует на плоскость и в пространство свои мысли и замыслы. Например: он спланировал как себя вести завтра. Он долго вынашивал (в голове) план решения этой задачи. Она представила себе эту встречу. Три пишем, два в уме.

б) Кроме отдельного предмета могут быть спроецированы несколько предметов, явления и процессы.

2. «План в экономике, программа деятельности хозяйствующих субъектов, отдельных звеньев системы управления. Различают внутрипроизводственный (внутрифирменный) П., народно - хозяйственный (общегосударственный). П., региональные и отраслевые П.; текущие (до 1года) и перспективные П.» [2].

Недостатки:

Узкоспециализированное понятие, без системы.

3. «1) Чертеж в условных знаках, детально отображающий в масштабе на плоскости небольшой участок местности или сооружение;

2) определенный порядок, последовательность в изложении чего-либо, например, научного или литературного произведения, статьи, речи и др.;

3) намеченная на определенный период работа с указанием ее целей, содержания, объема, методов, последовательности, сроков выполнения, например, учебный, производственный, народно-хозяйственный план; 4) замысел, предусматривающий ход, развитие чего-либо» [3].

Недостатки:

Без системы рассматриваются отдельные готовые формы.

На основании представленных определений План можно сделать вывод, что они недостаточные, их непременно нужно усовершенствовать. Например, так: План это - фазовая диаграмма процессов, его образующих. План это – ПРОЕКЦИЯ, результат проецирования предметов, явлений и процессов в уме, пространстве и на плоскости.

Структуры построения информации могут иметь больший или меньший объем, разные цели, но при этом они сохраняют аналогии построения данных. В основе композиционных решений лежат законы аудиовизуального восприятия, вне зависимости от того пишем ли мы живописное полотно или государственный план экономического развития.

Сочетание слов, описывающих графическую фазовую диаграмму, по сути, также является вербальной фазовой диаграммой. Фазовая терминология сопровождает развитие технологического процесса в течение полного цикла, обозначая содержание каждой стадии и именуя название каждой фазы, например, полный цикл «создания» бабочки: яйцо, личинка, куколка и, наконец, бабочка. И, вероятно, появляется особое название, когда в процессе трансформации возникает новая форма, отличающаяся от предыдущей.

Поэтому план, это не чья-то блажь, а необходимость соблюдения всех стадий построения изображения и процесса. Именно, цикл предварительных фазовых рассуждений, прогнозов, расчетов, написания самого плана доказывает закономерность и законность наступления фазы готовой формы - ПЛАН. Искаженный, частичный план или его отсутствие говорит о сбое в системе передачи информации. Некорректно Государственную плановую экономику называть «рыночной экономикой» или «цифровой». В общей пропорциональной системе «Экономика»,

в определенном соотношении частей, ее составляющих, рынку принадлежит не самая главная роль, а цифра относится к технологиям.

Выводы: Не полный план, а предложение развития только его «рыночного» сегмента грозит опасностью превращения экономики страны в сырьевой придаток.

В понимании информационной безопасности страны ПЛАН это – стратегический объект. Это системное устройство, которое подлежит охране от попыток его расстроить или разрушить. Кроме того, форма представления данных, в виде Государственного плана развития, должна соблюдаться ГОСТом и другими охранными мероприятиями особенно тщательно. Нам следует беречь честь и безопасность России.

СПИСОК ЛИТЕРАТУРЫ

1. Ярошевич Л.И. «Модерн умеренного плана» Материалы юбилейной X Санкт- Петербургской межрегиональной конференции Информационная безопасность регионов России (ИБРР-2017) Санкт-Петербург, 1-3 ноября 2017г. с. 407-408.
2. Прохоров А.М. Председатель научно-редакционного совета издательства «Большая Российская энциклопедия» Новый иллюстрированный энциклопедический словарь, Москва, 1999.
4. Словарь иностранных слов. – 7-е изд., С48 перераб. – М.: Русский язык, 1980. – 624 с.
3. Ожегов С.И. и Н.Ю. Шведова Толковый словарь русского языка. Москва, «АЗЪ», 1995.
4. Ярошевич Л.И. «Сфера нематематизированных диаграмм» XXI Международная научно-методическая конференция: «Современное образование: содержание, технологии, качество». Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. Ульянова (Ленина) 22апреля 2015 года, с. 47-48.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ НА ТРАНСПОРТЕ

УДК 004.738.5

ПРИМЕНЕНИЕ IOT НА ВОДНОМ ТРАНСПОРТЕ

Алексеенков Александр Евгеньевич, Ключникова Дарья Дмитриевна, Ли Изольда Валерьевна
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: kseenkovale@gmail.com, lik0011sofia@mail.ru, liiv@gumrf.ru

Аннотация. В статье рассмотрены основные области применения IoT на водном транспорте в настоящее время. Интернет вещей захватывая все больше аспектов нашей жизни дает серьезные предпосылки к применению средств контроля и мониторинга. Системы IoT позволяют гибко и эффективно решать подобные задачи. Это могут быть порты, суда, навигационное оборудование и многие другие сферы. В настоящее время Интернет вещей активно вводится в использование, являясь важной частью работы отрасли водного транспорта.

Ключевые слова: IoT; интернет вещей; водный транспорт; навигация; умный порт; автономное судно.

APPLICATION OF IOT IN WATER TRANSPORT

Alekseenkov Aleksander, Klyuchnikova Daria, Li Izolda
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: kseenkovale@gmail.com, lik0011sofia@mail.ru, liiv@gumrf.ru

Abstract. The article discusses the current uses of IoT at sea. The Internet of Things taking over our lives increasingly provides serious prerequisites for application of controls and monitoring. Today IoT systems allow to solve such tasks flexibly and efficiently. These can be ports, ships, navigational equipment and many other spheres. At present the Internet of things is being actively introduced into use, being an important part of the work of the waterway transport industry.

Keywords: IoT; internet of things; water transport; navigation; smart port; autonomous ship.

Введение. Человечество создает все больше устройств и технологий для более комфортного управления и взаимодействия. Особое внимание уделено автоматизации процессов. Одним из способов автоматизации стал Интернет вещей (Internet of Things). По своей сути Интернетом вещей являются физические объекты, подключенные к сети и обменивающиеся данными.

IoT применяется в самых различных областях: торговля, производство, перевозки, здравоохранение, энергетика и многое другое. Отрасль водного транспорта не исключение. Область применения IoT здесь очень обширна: от различных систем наблюдения до устройств для сохранения экологии.

Машинная связь (MTC - Machine type communications - это форма передачи данных, включающая одну или несколько сущностей, которые не управляются людьми напрямую) является ключом к морскому интернету вещей из-за необходимости установления между судами и берегом, а также между судами для поддержки выполнения различных видов морских услуг. Интернет вещей также может быть полезен при поисково-спасательных операциях, в навигационных устройствах и в устройствах, отслеживающих перевозки. Рассмотрим подробнее области его применения на водном транспорте.

Навигация.

Навигация в данный момент не может обойтись без IoT. Одним из важнейших аспектов навигации является мониторинг буев и маяков [1]. Система контроля на основе Интернета вещей позволяет быстро и эффективно реагировать в случае возникновения проблем, что обеспечивает как безопасность навигации, так и целостность сигналов.

Буи и их световые сигналы необходимы для безопасного прохождения маршрута водным транспортом. Так наблюдательные устройства, развернутые в настоящее время на береговых линиях Ирландии, включают буи, передающие данные о погоде и волнении, приливах и отливах. Однако, из-за плохой погоды швартовочный трос может оборваться. Не исключается дрейф буя по течению, если оно достаточно сильное. В подобных случаях, дрейфующий буй представляет серьезную опасность, поскольку может произойти столкновение с судном.

Устройство IoT, мониторящее буй, в определенный промежуток времени активируется и выполняет необходимые измерения, после чего отправляет все собранные данные на сервер (если буй плывет по течению, время интервала уменьшается, чтобы отслеживать скорость, курс и позицию с большей частотой).

Устройство IoT может отправить сигнал о падении напряжения аккумулятора, увеличении смещения координат, сигнал об открытом кожухе лампы, а также отсутствии сигнала от буя более четырех часов.

В навигации отдельно стоит отметить системы морской картографии [2]. Данные системы разработаны для обеспечения бесперебойной, согласованной и стандартизированной базы данных, включающей: морской климат, данные о навигации с использованием фотограмметрии, подходы, основанные на зондировании или лазерном сканировании и т.д.

Тем не менее современные методы основаны либо на удаленном мониторинге с применением спутников, не имеющих требуемой точности из-за загрязнений в атмосфере, либо на методах, основанных на разведке. К таким методам относят поисковые суда, включая гидрографические и океанографические суда, которые не могут покрыть обширные пространства океанов и морей из-за физических ограничений и ограниченного количества проведенных исследований.

Умные порты.

В основе модели умного порта лежит технология Интернета вещей [3]. Применение данной технологии в процессе создания логистической платформы позволяет уменьшить затраты на логистику. А внедрение Интернета вещей на уровне функционального планирования и при строительстве порта позволяет повысить эффективность каждого реализуемого в порту процесса.

При прохождении сегментов порта судам часто приходится выстраиваться в линию, соблюдая правила навигации. Это не только увеличивает время прохождения маршрута, но также вызывает частые морские дорожно-транспортные происшествия и приводит к гибели людей и порчи имущества, а также к загрязнению окружающей среды. Моделирование транспортных потоков в портах имеет большое значение для проектирования и преобразования порта. Смоделированное поведение судна можно реализовать не только в разработке, но и на практике.

В системе портов каналы являются важной частью обеспечения навигации. Для упрощения анализа отрезок маршрута разделяют на несколько сегментов. Каждый сегмент маршрута в канале заполнен ячейками одинакового размера. Для изменения скорости судна в зависимости от его положения, различают разные участки маршрута, где устанавливаются определенные модели ячеек. Элементарная ячейка канала постепенно становится больше в направлении от причала, так как скорость корабля уменьшается по мере того, как уменьшается расстояние до причала и увеличивается по мере удаления от него.

При строительстве интеллектуального порта можно реализовать интеллектуальное управление производственными операциями порта, управление складом и логистикой.

IoT используется в интермодальных перевозках: система, основывается на постоянной двунаправленной связи с контейнерами, движущимися внутри транспортной цепочки [4]. Модуль, включенный в систему, обеспечивает открытую среду с расширенными возможностями для контроля расположения и состояния каждого контейнера. Это решение позволяет реализовать множество различных способов управления глобальной цепочкой поставок во время транспортировки.

Другие системные модули используют данные отслеживания. Один из которых используется для оптимизации движения внутри морского терминала, а другие регулируют график движения судов. Использование этих модулей с данными отслеживания, должно привести к уменьшению времени пребывания на терминале и времени обработки контейнеров, а также сокращению затрат и времени простоя при транспортировке.

Умные суда.

Владельцы автономных судов стремятся оцифровать и зафиксировать большинство жизненно важных параметров [5]. Информация, которую важно знать: текущее положение и статус самых важных датчиков, таких как состояние дверного люка, состояние батареи, температуры, давления и т.д. Ключевыми задачами системы являются: сбор данных от датчиков и управление ими, связь в морской среде. Службы обеспечивают такие функции, как уведомления при достижении критических уровней, после чего пользователь может выполнить вмешательство на основании состояния судна.

Интернет вещей также позволяет реализовать систему швартовки с автоматическим размещением у причала в порту [6]. При получении запроса от судна, прибывающего в порт, система автоматически отправляет данные о месте, где он может пришвартоваться, прежде чем достигнет швартовой пристани.

Каждое место стоянки в порту может содержать автоматически управляемые устройства и датчики. Помимо этого, есть умные порты с различными коммуникационными технологиями для обмена данными с другими портами, умными судами и умными городами. Сервисы, созданные в интеллектуальных портах, состоят из автоматического мониторинга и контроля местоположения судов в порту, графика движения судов, грузов, проезда пассажиров и т.д.

Некоторые из крупных портов по всему миру уже предоставляют интерактивные услуги своим клиентам используя новейшие технологии. Примером может служить порт Гамбург в Германии. Одной из интерактивных

услуг для клиентов является возможность найти суда и места их расположения, проверить их состояние в режиме реального времени на сайте порта.

Порт Амстердам запустил несколько приложений. Приложение «I am Port» предлагает информацию о местонахождении судов и маршрутах движения в порту в режиме реального времени. Кроме того, мы можем найти информацию о прибытии и отправлении, размере, осадке и причаливании каждого судна в порту. Они также маркируют суда разными цветами, но цвет означает не тип судна, а скорее его статус.

Стартап We4Sea (https://www.we4sea.com/) разрабатывает приложение для судов, что позволяет сократить расходы на топливо до 20 процентов. Система We4Sea собирает некоторые оперативные данные по судну, как его местоположение, скорость, курс и данные двигателя, и отправляет их на берег для объединения с другими данными, такими как погода, высоты волн, сила ветра. После объединения этих данных, системные алгоритмы и энергетические модели преобразуют их в полезную информацию для оптимизации эксплуатации и комплектации.

Системы мониторинга физического и психоэмоционального состояния экипажа могли бы быть внедрены с применением технологии IoT.

Заключение. Гибкость и модульность вместе с низкими затратами являются основными сильными сторонами Интернета вещей.

Основная цель IoT - повысить комфорт и производительность в области применения. Интернет вещей может способствовать существенному повышению эффективности и качества услуг, безопасности эксплуатации оборудования и безопасности портов за счет повышения доступности и точности соответствующей информации. Морской IoT должен иметь адаптивную структуру, гибкость для внедрения новых приложений, обеспечивать безопасное подключение к существующим информационным системам и обрабатывать огромное количество данных. Стоит отметить, что количество областей применения IoT только увеличивается. Интернет вещей находит применение не только в порту, но и на судах, в навигационном оборудовании и многих других сферах.

IoT эффективен в сборе данных о погодных условиях, состоянии оборудования, местонахождении и т.д. Использование полученной информации помогает в принятии решений, позволяя оценить ситуацию в более полном объеме, а также сводить к минимуму чрезвычайные и травмоопасные ситуации, что особенно актуально в системах, применяемых в промышленных и коммерческих задачах.

Можно предвидеть, что системы морского IoT станет незаменимым помощником в области водного транспорта.

СПИСОК ЛИТЕРАТУРЫ

1. S. D. Pizzo, A. De Martino, G. De Viti, R. L. Testa and G. De Angelis, «IoT for Buoy Monitoring System» 2018 IEEE International Workshop on Metrology for the Sea; Learning to Measure Sea Health Parameters (MetroSea), 2018, pp. 232-236, doi: 10.1109/MetroSea.2018.8657828.
2. M. Al-Khalidi, R. Al-Zaidi, J. Woods, M. Reed and E. Pereira, «Securing Marine Data Networks in an IoT Environment» 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud), 2019, pp. 125-132, doi: 10.1109/FiCloud.2019.00025.
3. L. Jiang, G. Huang, C. Huang and W. Wang, «Data Mining and Optimization of a Port Vessel Behavior Behavioral Model Under the Internet of Things» in IEEE Access, vol. 7, pp. 139970-139983, 2019, doi: 10.1109/ACCESS.2019.2943654.
4. Jesús Muñuzuri, Luis Onieva, Pablo Cortés, José Guadix, «Using IoT data and applications to improve port-based intermodal supply chains» School of Engineering, University of Seville, CM Descubrimientos, s/n, 41092 Seville, Spain Available online 23 January 2019.
5. M. Cankar and S. Stanovnik, «Maritime IoT Solutions in Fog and Cloud» 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion), 2018, pp. 284-289, doi: 10.1109/UCC-Companion.2018.00069.
6. Kamolov, A.; Park, S. An IoT-Based Ship Berthing Method Using a Set of Ultrasonic Sensors. Sensors 2019, 19, 5181. https://doi.org/10.3390/s19235181.

УДК 651.011.56

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АДМИНИСТРАТИВНОГО ПРОИЗВОДСТВА НА ТРАНСПОРТЕ В РАЗУМНЫЙ СРОК

Бурлов Вячеслав Георгиевич, Миронов Алексей Юрьевич, Миронова Анна Юрьевна
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: burlovvg@mail.ru, wakepolarbear@gmail.com, milpandaaaa@gmail.com

Аннотация. С целью обеспечения в разумный срок достоверности и полноты производства по делам об административных правонарушениях на транспорте рассмотрен синтез взаимодействия целевой, защитной и обеспечивающей подсистем управления административной практикой при конфликте сторон. Естественно-научным подходом к принятию управленческих решений на базе закона сохранения целостности объекта синтезирована математическая модель подсистем управления административным производством при дефиците ресурсов. Для модели в виде непрерывной цепи Маркова, конкретизированной уравнениями Колмогорова-Чепмена, предложена структурно-функциональная технология сетевого моделирования взаимодействующих процессов.

Ключевые слова: информационная безопасность; синтез управления; административное производство на транспорте; конфликт сторон; дефицит ресурсов; естественно-научный подход; сетевая модель.

PROVING INFORMATION SECURITY OF ADMINISTRATIVE PRODUCTION ON TRANSPORT IN A REASONABLE TIME

Burlov Vyacheslav, Mironov Aleksey, Mironova Anna
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: burlovvg@mail.ru, wakepolarbear@gmail.com, milpandaaaa@gmail.com

Abstract. In order to ensure, within a reasonable time, the reliability and completeness of production on affairs about administrative offenses on transport, interaction synthesis of the target, protective and supporting subsystems for managing administrative practice is considered when parties conflict. Using a natural-scientific approach to management decision making, based on the law of object integrity preserving, a model of management subsystems of administrative production is synthesized with resources shortage. For a model in the form of a continuous Markov chain, concretized by the Kolmogorov-Chapman equations, a structural-functional technology of interacting processes network modelling is proposed.

Keywords: information security; management synthesis; administrative production on transport; conflict of parties; resource scarcity; natural science approach; network model.

Введение. Латентность до 3/4 административно наказуемых деяний, неисполнение до 1/4 постановлений по делам об административных правонарушениях, неуплата до 2/5 административных штрафов, характеризующие ненадлежащее состояние информационной безопасности производства по делам об административных правонарушениях, требуют моделирования инновационных процессов управления административной практикой на транспорте [1, 2]. Хроническое несоблюдение правил эксплуатации транспортных средств, пожары, умышленное или случайное повреждение опасных грузов и магистральных трубопроводов, ненадлежащее строительство и использование транспортной инфраструктуры, техногенные и экологические катастрофы порождаются нарушениями разумного срока. административного производства на транспорте [3]. Спорадичная и постфактумная реакция правоохранителей на поток правонарушений порочно сохраняет карательно-фискальную суть даже при переходе к риск-ориентированному производству по делам об административных правонарушениях. Пока органы по исполнению административного законодательства ориентированы на взыскание штрафов за оконченные деяния и безразличны к причиненному ущербу. Преодоление разрушения целостности в виде неполноты и недостоверности административной практики особенно актуально в отношении административных правонарушений, по которым признаки и следы укрыты особенностями местности. а правонарушители противодействуют субъектам административной юрисдикции [4]. Своевременная профилактика, превентивное выявление и надлежащее доказывание в разумный срок требуют геоинформационной защиты регламентным снабжением правоохранительных органов географическими координатами объектов на подведомственной территории, содержащих признаки подготовки или совершения правонарушений, для незамедлительного проведения по ним целевых проверок, предупреждения или пресечения вредных последствий, сбора объективных доказательств события и состава. Надлежащая интенсивность административного процесса при оперативном установлении местонахождения нарушителей с целью их обязывания, принуждения или привода к исполнению административного законодательства в разумный срок обеспечивается определением географических координат противодействующих участников производства с помощью геолокации персональных средств мобильной связи и гаджетов выхода в Интернет, противоугонных и аварийных оповещателей на их автомототранспорте. Геоинформатика и геолокация предоставляют действенные механизмы целевого решения «камерной» проблемы административной практики, ставящего под контроль работоспособность технических средств неповторимой фотовидеофиксации правонарушений.

На геоинформационном мониторинге построено картографическое отражение обстановки в десятке геопорталов отечественных ведомств и корпораций, в том числе «Оперативный мониторинг судоходства» в ФГУП «Атомфлот», ЛесЕГАИС в ФГКУ «Рослесинфорг», «Деметра» в Россельзознадзоре, «Каскад», «Бриз» и «КосмоПлан» в МЧС России, «ЭРА-ГЛОНАСС» в АО «ГЛОНАСС». Эксплуатируемые средства геоинформатики и геолокации пассивно отражают состояние проблем и объемы ущерба, но не способствуют их профилактике и предотвращению [5]. На стыке организации административной практики и ее геокоординирования настоящей работой решается важная научная проблема обоснования системообразующих требований к структурным и функциональным характеристикам геоинформационного управления, превентивно обеспечивающего надлежащую эффективность производства по делам об административных правонарушениях на транспорте в разумный срок.

Производство по делам об административных правонарушениях функционирует в условиях текущей обстановки и взаимоотношений круга субъектов административно-юрисдикционного процесса. Поэтому в административной практике конкурируют две стороны административно-процессуального правоотношения: субъект административной юрисдикции (орган по исполнению административного законодательства или уполномоченное им должностное лицо, судья, прокурор) и противодействующие участники производства (правонарушитель, представитель, защитник, свидетель, эксперт, специалист), объединенные умышленно или по неосторожности единым стремлением доведения до цели правонарушения. В общем случае, их взаимодействие рассматривается в виде конфликта с несовпадающими интересами.

Адекватность комплекса мероприятий субъекта административной юрисдикции по обеспечению информационной безопасности административного производства основана на осознании и познании окружающей обстановки и противодействия участников. Принятие управленческих решений для поддержания разумности срока функций административного процесса требует моделировать применение управления производством на протяжении всего жизненного цикла дел об административных правонарушениях. Успешность технологии познания и управления определяется адекватностью моделирования. Мерой адекватности математической модели выступает полнота учета ею закономерностей обеспечения разумного срока на базе закона сохранения целостности производства по делам об административных правонарушениях. Косвенным подтверждением игнорирования этого закона в административной практике является нынешнее отсутствие технологий структурно-функционального синтеза превентивного управления административным производством [6].

Исходя из нацеленности на обеспечение разумного срока в условиях динамичной обстановки и ситуации в конфликте, жизненный цикл системы управления административным производством итерационно повторяет такие этапы, как уточнение облика системы, оптимизация ее подсистем, эксплуатация и непосредственное применение подсистем в ее составе. Под обликом системы понимают ее ключевые характеристики и отношения между подсистемами, определяющие возможности системы и механизмы их реализации

Формализация закона сохранения целостности путем аккумулирования потенциальной эффективности системы управления по пространственно-временным состояниям указала облик разрешения конфликта. Согласно рис. 1 сторона конфликта противодействует путем выполнения трех базовых функций. Попытки их дополнения порождают подобные по содержанию и назначению функции, которые следует учитывать в базовых. Для реализации базовых функций каждая сторона конфликта создает соответствующие подсистемы: целевую, защитную, обеспечивающую [7].

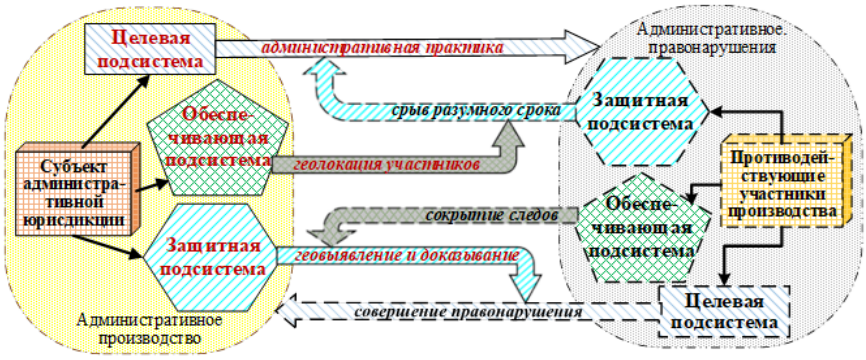


Рис. 1. Взаимодействие трех базовых подсистем в управлении административным производством.

Целевая подсистема предназначена для решения целевых задач на множестве пространственно-временных состояний: у субъекта административной юрисдикции – стадий административной практики, у противодействующих участников производства – этапов совершения административного правонарушения. На стороне субъекта административной юрисдикции она образует штатный стержень административного производства с собственным контрольно-надзорным механизмом и управляется в разумный срок за счет дополнения защитной и обеспечивающей подсистемами.

Параллельно собственному целевому процессу защитная подсистема стороны стремиться препятствовать целевой деятельности противника: субъект административной юрисдикции – превентивно выявить и доказать признаки события и состава латентных правонарушений, противодействующие участники производства – затянуть и сорвать разумный срок процессуальных процедур целевого вида административного производства. Очевидно, что защитная функция превалирует в активности стороны конфликта на стадиях возбуждения и расследования дел об административных правонарушениях. При рассмотрении дел и исполнении наказаний защитный эффект постепенно подавляется противником.

Разнонаправленность целевой и защитной функций каждого противника указывает на диалектическое противоречие реализующих подсистем. Для гармоничного их сосуществования и подавления эффекта противодействия естественно предположить у стороны наличие обеспечивающей подсистемы, снимающей противоречие: для субъекта административной юрисдикции – геолокацией участников производства гарантирующей их присутствие в административном процессе, для противодействующих участников производства – активно скрывающей и уничтожающей следы административного правонарушения и его последствий. Угнетая защитную деятельность противника в отношении собственного целевого процесса, обеспечивающая функция стороны конфликта усиливается от расследования административных дел к стадиям их рассмотрения и исполнения наказаний [8].

Ненадлежащий результат процессуальных процедур на конвейере исполнения управленческих решений в производстве по делам об административных правонарушениях обоснован противоречивыми выводами и ведет

к неоправданному перерасходу ресурсов, сопряженному со срывами разумного срока. Следование формальной аксиоматической концепции, исключающей произвол в рассуждениях, обеспечивает целостный учет закономерностей и существенных связей предметной области, давая адекватный инструмент ее осознанию и познанию в рамках индуктивно-дедуктивных выводов [9]. Базовым постулатом в ней выступает законом сохранения целостности объекта окружающего мира, который используется санкт-петербургской научно-педагогической школой «Системная интеграция процессов государственного управления» и указывает на устойчивую повторяющуюся связь свойств объекта и свойств его действий при фиксированном предназначении [10].

Естественно-научный подход на рис. 2 развертывает процессное осознание принятия управленческого решения в целевой, защитной или обеспечивающей подсистеме управления производством по делам об административных правонарушениях в свете трех свойств на каждом из трех уровней познания [11]. Формирование модели принятия решения подсистемой управления согласно рис. 3 заключается в установлении формальной аналитической зависимости между тремя технологическими компонентами, которые характеризуются невосполнимыми ресурсами времени [12].

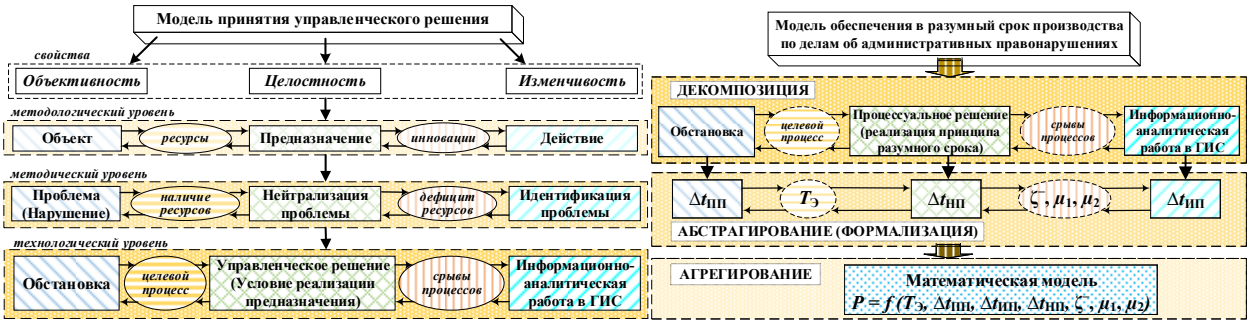


Рис. 2. Естественно-научный подход к осознанию принятия решения. Рис. 2. Познание синтеза математической модели принятия решения.

Используя методы декомпозиции, абстрагирования и агрегирования, процесс принятия управленческого решения формализуется в математический агрегат модели управления: $P=f\,(T_Э, \Delta t_{ПП}, \Delta t_{ИП}, \Delta t_{НП}, \zeta^{-}, \mu_1, \mu_2)$, (1)

где P – вероятность нахождения административного производства в каждом из базовых состояний подсистемы управления: исходном, целевом, идентификации или нейтрализации проблем;

$T_Э=f_{\zeta+}(X_0, X_1, \ldots, X_p)$, $\Delta t_{ПП}=f_{\lambda}(A_0, A_1, \ldots, A_n)$, $\Delta t_{ИП}=f_{v1}(B_0, B_1, \ldots, B_k)$, $\Delta t_{НП}=f_{v2}(C_0, C_1, \ldots, C_m)$ – среднестатистический период Целевого процесса, Появления Проблем, их Идентификации или Нейтрализации соответственно, структурно и функционально объединяющий действия (работы) по переходу через внутренние состояния к его результату;

$\zeta^{-}=f_{\zeta-}(1/T_Э)$, $\mu_1=f_{\mu1}(1/\Delta t_{ИП})$, $\mu_2=f_{\mu2}(1/\Delta t_{НП})$ – средняя частота срыва разумного срока Целевого процесса, Идентификации или Нейтрализации Проблем соответственно, обусловленного дефицитом ресурсов [13].

В качестве организационной системы, производство по делам об административных правонарушениях функционирует при стохастической неопределенности, когда многочисленные объективные и субъективные факторы порождают случайные во времени процессы. Их вероятностные характеристики заранее не известны и неопределенным образом постепенно меняются с течением времени, но выявляемы административной статистикой из промежуточных результатов производственных операций. Среднестатистический период прохождения сквозь процесс дел об административных правонарушениях несет информацию о текущей длительности процесса, через нее информируя будущее управление о динамике прохождения в настоящем и прошлом. То есть, в обобщенном среднем времени процессы административного производства приводятся к случайным марковским с дискретными состояниями и непрерывным временем [14].

Череда дел об административном правонарушении движется процессами административного производства через контрольные точки событий, определенных процессуальными разделами Кодекса РФ об административных правонарушениях. Следовательно, сквозь каждую контрольную точку проходит поток в виде последовательности однородных событий, следующих одно за другим в случайные моменты времени. В связи с отсутствием закономерности для объединения в группы, однородные события следуют в потоке поодиночке. В силу марковского видения ординарных потоков дел, процессы в административном производстве и управлении им близки к пуассоновским [15].

В схеме функционирования целевой, защитной или обеспечивающей подсистемы управления административным производством на рис. 4 Целевой процесс осуществляется за счет штатных ресурсов. При просрочке разумного срока его осуществления административная практика срывается в исходное состояние продлением или прекращением административного процесса. В связи с пуассоновским потоком нарушений лицо, принимающее решение, реализует посредством контрольно-надзорного, геоинформационного или геолокационного механизма за счет резервных ресурсов структурные комбинации функций по их Идентификации и Нейтрализации [8]. В связи с критичным резервом ресурсов при их дефиците процессы выполнения работ над нарушениями разумного срока сопровождаются вероятностными срывами в начальные состояния. Модель целевой, защитной или обеспечивающей

подсистемы управления в виде непрерывной цепи Маркова на рис. 5 характеризуется вероятностями нахождения административного производства в одном из четырех базовых состояний: исходном S_1, целевом S_2, идентификации S_3, нейтрализации S_4. При этом, состояния связаны интенсивностями $\zeta^+=1/T_Э$, $\lambda=1/\Delta t_{ПП}$, $\nu_1=1/\Delta t_{ИП}$, $\nu_2=1/\Delta t_{НП}$ пуассоновских переходов и частотами срывов $\zeta^-=f_{\zeta^-}(\zeta^+)$, $\mu_1=f_{\mu 1}(\nu_1)$, $\mu_2=f_{\mu 2}(\nu_2)$ [16].

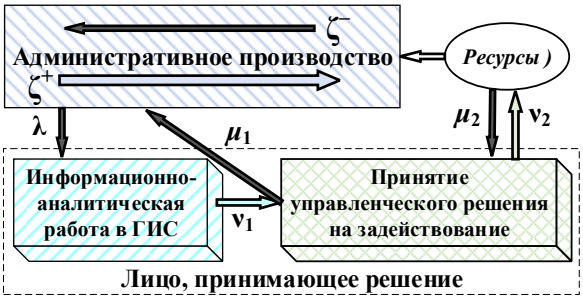


Рис. 4. Схема управления административным производством.

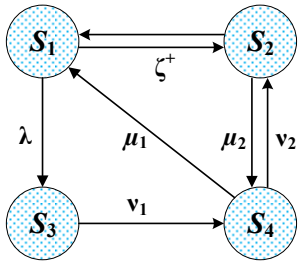


Рис. 5. Граф состояний управления административным производством.

Пуассоновский характер процессов административного производства и управления им позволяет использовать для размеченного графа состояний непрерывной цепи Маркова на рис. 5 систему (2) дифференциальных уравнений Колмогорова-Чепмена при ограничении $P_1(t)+P_2(t)+P_3(t)+P_4(t)=1$:

$$\begin{aligned}
&\frac{dP_1(t)}{dt} = -P_1(t)[\zeta^+ + \lambda] + P_2(t)\zeta^- + P_4(t)\mu_1 \qquad \frac{dP_2(t)}{dt} = P_1(t)\zeta^+ - P_2(t)[\zeta^- + \mu_2] + P_4(t)\nu_2 \\
&\frac{dP_3(t)}{dt} = P_1(t)\lambda - P_3(t)\nu_1 \qquad \frac{dP_4(t)}{dt} = P_2(t)\mu_2 + P_3(t)\nu_1 - P_4(t)[\nu_2 + \mu_1]
\end{aligned} \tag{2}$$

При стремлении с течением времени пуассоновских потоков взаимодействующих процессов к предельному стационарному режиму, дифференциальные уравнения Колмогорова-Чепмена (2) трансформируются в систему линейных однородных алгебраических уравнений, решением которой с помощью метода Крамера являются системообразующие факторы (3) подсистемы управления административным производством [17]:

$$\begin{aligned}
P_1 &= \frac{\zeta^-\nu_1\nu_2 + \nu_1\mu_1(\zeta^- + \mu_2)}{\zeta^-\nu_2(\lambda+\nu_1) + \mu_1(\lambda+\nu_1)(\zeta^- + \mu_2) + \nu_1(\zeta^+ + \lambda)(\nu_2 + \mu_2) + \nu_1(\zeta^+\mu_1 + \zeta^-\lambda)} \\
P_2 &= \frac{\nu_1\nu_2(\zeta^+ + \lambda) + \zeta^+\nu_1\mu_1}{\zeta^-\nu_2(\lambda+\nu_1) + \mu_1(\lambda+\nu_1)(\zeta^- + \mu_2) + \nu_1(\zeta^+ + \lambda)(\nu_2 + \mu_2) + \nu_1(\zeta^+\mu_1 + \zeta^-\lambda)} \\
P_3 &= \frac{\zeta^-\lambda\nu_2 + \lambda\mu_1(\zeta^- + \mu_2)}{\zeta^-\nu_2(\lambda+\nu_1) + \mu_1(\lambda+\nu_1)(\zeta^- + \mu_2) + \nu_1(\zeta^+ + \lambda)(\nu_2 + \mu_2) + \nu_1(\zeta^+\mu_1 + \zeta^-\lambda)} \\
P_4 &= \frac{\nu_1\mu_2(\zeta^+ + \lambda) + \zeta^-\lambda\nu_1}{\zeta^-\nu_2(\lambda+\nu_1) + \mu_1(\lambda+\nu_1)(\zeta^- + \mu_2) + \nu_1(\zeta^+ + \lambda)(\nu_2 + \mu_2) + \nu_1(\zeta^+\mu_1 + \zeta^-\lambda)}
\end{aligned} \tag{3}$$

Исходя из системообразующих факторов (3), в качестве критерия эффективности (4) подсистемы управления целесообразно рассмотреть гарантированную долю P_2^* времени (потока дел об административных правонарушениях в готовности) для реализации в разумный срок функциональности остальных подсистем:

$$\frac{\nu_1\nu_2(\zeta^+ + \lambda) + \zeta^+\nu_1\mu_1}{\zeta^-\nu_2(\lambda+\nu_1) + \mu_1(\lambda+\nu_1)(\zeta^- + \mu_2) + \nu_1(\zeta^+ + \lambda)(\nu_2 + \mu_2) + \nu_1(\zeta^+\mu_1 + \zeta^-\lambda)} \geq P_2^* \tag{4}$$

Технологическая реализация идентификации и нейтрализации нарушений разумного срока строится, в рамках структурно-функционального подхода к структурированию и параметризации системы управления, сетевым моделированием процессов, составляющих целевую, защитную или обеспечивающую цепи Маркова. Определяющим условием поведения управленческих процессов в организационной системе является их неравномерная самоорганизация. Только когда неустойчивое равновесие управленческого процесса грозит потерей функциональной устойчивости, возникает самоорганизующаяся потребность переформирования его структуры в более эффективную. В промежуточный период устойчивого равновесия функциональности управленческий процесс довольствуется параметрической оптимизацией на вызовы обстановки [18].

Исходными данными при оценивании временных параметров сетевой модели служат среднестатистические продолжительности процедур, переводящих процесс из одного события в другое. В условиях стохастической неопределенности математическое ожидание и дисперсия длительности процедур рассчитываются по формулам

аппроксимирующего закона нормального или бета-распределения [19]. Он с точностью до числовых характеристик, достаточной для целей моделирования, аппроксимирует законы распределения продолжительностей всех процедур моделируемого процесса. При достаточно большом количестве процедур, участвующих в процессе, можно утверждать, а при малом – предполагать, что длительность критического пути в сетевой модели подчиняется нормальному закону распределения. Через интегральную функцию Лапласа из математического ожидания и дисперсии критического пути оценивается длительность процесса с детерминированной степенью уверенности в его осуществлении [20].

Следовательно, явно увязав в структуре сетевой модели процесса процедурные переходы и затрачиваемое на них время, сетевое моделирование позволяет по критическому пути каждого из процессов оценить периоды $T_Э$, $\Delta t_{ПП}$ и оптимизировать $\Delta t_{ИП}$, $\Delta t_{НП}$ под условие превентивного управления (4).

Заключение. В обстановке конфликтной активности противодействующих участников производства по делам об административных правонарушениях на транспорте, административная практика в разумный срок субъекта административной юрисдикции гарантированно управляется путем ее сопровождения целевой подсистемой с контрольно-надзорным механизмом, защитной подсистемой на базе геоинформатики и обеспечивающей подсистемой на основе геолокации. Параллельно целевому процессу административной практики органа по исполнению административного законодательства защитная подсистема управления противодействует целевой деятельности правонарушителей ранним выявлением и достоверным доказыванием признаков события и состава латентных правонарушений за счет превентивного геоинформирования. В стремлении нивелировать защитную функцию противодействующих участников производства, обеспечивающая подсистема управления охраняет разумный срок административного процесса принуждением к участию в процессуальных процедурах за счет геолокационного поиска участников. В текущей обстановке, характеризуемой интенсивностями Целевого процесса ζ^+ и Появления Проблем λ, при нормативно установленных уровнях максимально допустимой частоты срыва Целевого процесса ζ^- и минимально достаточной эффективности P_2, критерий эффективности (4) целевой, защитной или обеспечивающей подсистемы управления позволяет контролировать достаточность и оптимизировать интенсивности Информационно-аналитической работы ν_1 и Управленческого решения ν_2 путем рационализации структуры и продолжительностей переходов по их событиям с учетом срывов частотой μ_1 и μ_2, мотивированных дефицитом ресурсов.

СПИСОК ЛИТЕРАТУРЫ

1. Дерюга А.Н., Мотрович И.Д. Причины латентности административных правонарушений // Административное право и процесс. – 2013. – №7. – С. 57-62.
2. Лунеев В.В. Юридическая статистика / В. В. Лунев; Институт государства и права РАН. – М.: Норма: ИНФРА-М, 2017. – 448 с.
3. Цветков В. Я. Анализ применения космического мониторинга / В. Я. Цветков // Перспективы Науки и Образования. – 2015. – № 3 (15). – С. 48-55.
4. Миронов А.Ю. Миронова А.Ю., Сипович Д.Е. Информационная безопасность выявления и доказывания административных правонарушений с применением геоинформационной системы // Региональная информатика и информационная безопасность: Сборник трудов: Выпуск 7. – СПб.: СПОИСУ, 2019. – С.402-407.
5. Лупян Е.А. и др. Создание технологий построения информационных систем дистанционного мониторинга / Институт космических исследований РАН // Современные проблемы дистанционного зондирования Земли из космоса. – 2015. – Т. 12. – № 5. – С. 53-75.
6. Жуков А.О., Бурлов В.Г., Пестун У.А. К вопросу стратегического планирования развития наукоемких предприятий // Стратегическое планирование и развитие предприятий: материалы XVIII Всероссийского симпозиума. – М.: ЦЭМИ РАН, 2017. – С. 935-939.
7. Матвеев А.В., Иванов М.В., Шевченко А.Б. Аналитическая модель системы управления пожарной безопасностью АЭС // Научно-технические ведомости СПбГПУ: информатика, телекоммуникации, управление. – 2010. – № 6. – С.91-95.
8. Миронов, А.Ю. Превентивное управление административным производством в условиях конфликта сторон // Неделя науки ИСИ: сборник материалов Всероссийской конференции, 26–30.04.2021: В 3 ч. – Ч. 3. – СПб.: ПОЛИТЕХ-ПРЕСС, 2021. – С. 234-237.
9. Анохин, П.К. Принципиальные вопросы общей теории функциональных систем. – М.: Директ-Медиа, 2008. – 131 с.
10. Istomin E.P., Abramov V.M., Burlov V.G., Sokolov A.G., Fokicheva A.A. Risk Management Metod in Parametric Geosystems // 18th International Multidisciplinary Scientific Conference on EARTH & GEOSCIENCES. – Albena: SGEM, 2018. – Pp. 377–384.
11. Лепешкин О.М., Лепешкин М.О., Бурлов В.Г. Синтез процесса управления техническими системами на основе теории радикалов // Нейрокомпьютеры и их применение: XIV Всероссийская научная конференция: тезисы докладов. – М.: МГППУ, 2016. – С. 18-В.
12. Andreev A.V., Burlov V.G., Grachev M.I. Information Technologies and Synthesis of the Management Process Model in the Enterprise // 2019 International Science and Technology Conference «EastConf». – Vladivostok: EastConf, 2019. – Pp. 1-5.
13. Бурлов В.Г., Попов Н.Н., Гарсия Эскалона Х.А. Управление процессом применения космической геоинформационной системы в интересах обеспечения экологической безопасности региона // Ученые записки Российского государственного гидрометеорологического университета. – СПб.: РГГМУ, 2018. – № 50. – С. 118-129.
14. Галажинская О.Н. Теория случайных процессов: в 2 ч. Ч. 1 / О.Н. Галажинская, С. П. Моисеева. – Томск: ТГУ, 2015. – 128 с.
15. Лецкий Э.К. Модели информационных процессов на основе дискретных процессов Маркова / Э. К. Лецкий. – М.: МИИТ, 2014. – 25 с.
16. Бурлов В.Г., Миронов А.Ю., Миронова А.Ю. Гарантированное управление производством по делам об административных правонарушениях с использованием геоинформационной системы // Global & Regional Research. – Иркутск: БГУ, 2019. – Т. 1. – № 3. – С. 200-210.
17. Бурлов В.Г., Миронов А.Ю., Миронова А.Ю. Обеспечение гарантированного управления с помощью геоинформационной системы в условиях недостаточных ресурсов административного производства // Региональная информатика и информационная безопасность: Сборник трудов: Выпуск 9. – СПб.: СПОИСУ, 2020. – С. 195-200.
18. Гармаш А.Н. Экономико-математические методы и прикладные модели / А. Н. Гармаш, И. В. Орлова, В. В. Федосеев; под. ред. В. В. Федосеева. – М.: Юрайт, 2019. – 328 с.
19. Заболотский В.П. Математические модели в управлении / В. П. Заболотский, А. А. Оводенко, А. Г. Степанов. – СПб.: ГУАП, 2001. – 196 с.
20. Попов В.С. Новые варианты математического выражения относительных погрешностей измерений и средств измерений / В. С. Попов // Автоматика и телемеханика. – 2002. – №12. – С. 166-173.

УДК 004.056.53

ОСОБЕННОСТИ ПОСТРОЕНИЯ ПОДСИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ТРАНСПОРТЕ

Голоскоков Константин Петрович, 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, korotkovvv@gumrf.ru

Аннотация. В статье рассматривается возможность построения подсистемы информационной безопасности для транспортных информационных систем.

Ключевые слова: подсистема; информационная безопасность; транспортная система; инструментальная среда; технические средства; программное обеспечение.

FEATURES OF BUILDING A SUBSYSTEM OF INFORMATION SECURITY IN TRANSPORT

Goloskokov Konstantin, Korotkov Vitaly
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: goloskokovkp@gumrf.ru, korotkovvv@gumrf.ru

Abstract. The article considers the possibility of building an information security subsystem for transport information systems.

Keywords: subsystem; information security; transport system; tool environment; technical means; software.

Введение. Существует острая необходимость в средствах анализа защищенности для своевременного обнаружения уязвимостей и принятия мер по их ликвидации [1-3].

Сложившаяся ситуация в сфере информационной безопасности предполагает обязательное использование средств анализа защищенности в компаниях, имеющих выход в сети связи общего пользования, осуществляющих обработку персональных данных, а также в иных случаях (соответствие стандартам PCI DSS, ISO 17799, СТО БР ИББС).

Для транспортного бизнеса через сети связи общего пользования осуществляется реализация взаимодействия с клиентской сетью, с контрагентами и контролирующими государственными структурами (налоговая инспекция, пенсионный фонд и др.).

При аудите безопасности, аттестации АИС используются сетевые сканеры уязвимостей, позволяющие проводить инвентаризацию сети и идентификацию уязвимостей. На рынке сканеров представлен широкий спектр устройств. Это и условно бесплатные устройства с открытым кодом до специализированных комплексов аудитора информационной безопасности. Сетевые сканеры служат для анализа защищенности сети путем сканирования и зондирования сетевых ресурсов и выявления их уязвимостей [4-5].

Применение сканеров позволяет решить следующие задачи:

- инвентаризация ресурсов, включающих устройства сети, ОС, службы и ПО;
- идентификация и анализ уязвимостей;
- патчинг (автоматизированная отдельно поставляемая программа необходимая для устранения проблем в ПО или изменения его функционала) новых уязвимостей до выхода официальных исправлений от производителя;
- формирование отчетов, в том числе с описанием проблем и вариантами устранения.

При проведении обследования защищенности ресурсов могут быть использованы различные инструменты выявления проблем безопасности. Большую часть их, как правило, составляют различные сетевые сканеры.

Мониторинг. Инфраструктура современного АТП имеет разнородную, разнообразную, распределенную структуру. Тысячи, и даже десятки тысяч пользователей, десятки и сотни серверов, огромное количество сетевого оборудования, систем безопасности, различных общих, прикладных, специализированных систем требуют круглосуточного управления, мониторинга и контроля состояния, реакции на события.

В таких условиях наиболее важным и критичным для обеспечения безопасности является своевременное обнаружение и реакция на события и инциденты информационной безопасности КИС. В качестве технологической основы возможно, как пример, использовать решение Symantec Security Information Manager (SIM) [6-9].

Symantec SIM– это АПК, позволяющий в режиме реального времени собирать, структурировать по важности и анализировать все события, имеющие значения с точки зрения информационной безопасности в КИС.

Компоненты могут быть установлены как на одном сервера, так и разнесены на разные платформы.

Внедрение АПК позволяет получить следующие преимущества:

- обеспечение контроля состояния КИС в реальном времени;

– снижение затрат на ИТ-штат, за счет централизованного мониторинга и управления событиями;
– уменьшение влияния «человеческого фактора» при обнаружении инцидентов безопасности;
– уменьшение времени реагирования и автоматизация процесса реагирования на инциденты за счет подсказок системы и применения лучших практик;
– получение инструмента для расследования и доказательств инцидентов;
– соответствие требованиям регламентов и стандартов (PCI DSS и др.).

Резервное копирование. Для обеспечения защиты от сбоев, потери информации, а также обеспечения непрерывности и восстановления данных после сбоев и инцидентов используются системы резервного копирования и защиты данных.

Резервирование – это один из необходимых методов обеспечения непрерывности, а в ряде случаев обязательной подсистемой для соответствия стандартам в области информационной безопасности.

В рамках построения систем резервного копирования и защите данных возможно использовать, например, решения ведущих вендоров Symantec (решение Symantec Symantec Backup Exec) и HP (решение HP Data Protector).

Это комплексные решения, позволяющие значительно упростить процедуры резервного копирования, восстановления данных, дедупликации (устранения дублирования данных), управления жизненным циклом резервных копий.

Система резервного копирования и защиты данных позволяет произвести резервное копирование и защиту данных:
– на серверах и рабочих станциях;
– на платформах Windows, Linux, UNIX средах;
– в средах виртуализации Hyper-V, VMWare

Системы антивирусной защиты. С каждым годом растет количество нового вирусного ПО, увеличивается процент вероятности заражения вредоносным кодом. Факт заражения может произойти на конечных рабочих станциях пользователей, серверах, шлюзах или мобильных устройствах, в том числе использующихся удаленно.

Исходя из этого, необходимо осуществлять комплексную защиту всех точек возможного проникновения вредоносного кода в корпоративную сеть АТП.

Данный тип защиты подразумевает применение систем антивирусной защиты, обеспечивающих безопасность всех без исключения устройств внутри и за пределами сети компании.

Необходимо использовать единый центр управления всеми узлами системы антивирусной защиты для удобства администрирования и наглядности процессов, происходящих в области вирусной активности.

Сложившаяся ситуация в сфере информационной безопасности предполагает обязательное использование систем антивирусной защиты (соответствие стандартам PCI DSS, ISO 17799, СТО БР ИББС, выполнение требований по защите персональных данных).

Применение систем антивирусной защиты позволяет решить следующие задачи:
– блокирование проникновения вирусов на АРМ при использовании на них инфицированных файлов с переносимых устройств памяти;
– предотвращение заражения вирусами с помощью ПО из Интернета;
– предотвращение проникновения вирусов при подключении к КИС инфицированных АРМ удаленных или мобильных пользователей;
– предупреждение заражения вирусами с удаленного сервера, обменивающегося данными с корпоративными серверами файл - приложений и БД;
– блокирование распространения почтовых и Интернет-«червей»;
– предупреждение с помощью эвристической защиты заражения новыми и ранее неизвестными угрозами;
– управление доступом к конкретным процессам, файлам и папкам со стороны пользователей и приложений;
– контроль подключения и использования периферийных устройств;
– восстановление работы приложений после вирусных эпидемий и предотвращение вирусных эпидемий.

Системы защиты информации от НСД предназначена для защиты информации, а также для разграничения полномочий пользователей по доступу к файловой системе и другим ресурсам ПК. Разграничения касаются всех пользователей – локальных, сетевых, доменных, терминальных.

Назначение системы:
– идентификация пользователей, как по индивидуальным паролям, так и по аппаратным идентификаторам;
– ограничение доступа пользователей к ПК по дате и времени;
– ранжирование доступа пользователей к массивам данных и ПО с помощью мандатного или дискреционного контроля (управление доступом по спискам);
– контроль целостности параметров компьютера (АПК, файлов и папок при загрузке компьютера или при доступе);

– очистка остаточной информации, освобождаемой памяти, файла подкачки виртуальной памяти, освобождаемого дискового пространства, определенных папок при выходе пользователя из системы – это гарантирует предотвращение восстановления удаленных данных;

– контроль печати на принтерах позволяет протоколировать вывод документов на печать и маркировать эти документы (в качестве маркера может выступать гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация);

– автоматическое ведение различных видов электронных журналов;

– создание замкнутой программной среды для пользователя (режим, в котором пользователь может запускать только программы, определенные администратором);

– функция преобразования в «прозрачном» режиме данных, хранящихся на локальных дисках;

– централизованное администрирование системы защиты, осуществляется с использованием специального модуля — сервера безопасности, установленного на отдельный компьютер.

Система идентификации и аутентификации пользователей обеспечивает аппаратную авторизацию пользователей при доступе к информационным ресурсам на основе электронных ключей или смарт-карт, содержащих личную информацию.

В качестве критерия идентификации пользователя при использовании электронных USB-ключей и смарт-карт eToken могут использоваться:

– цифровые сертификаты стандарта X.509 (PKI);

– пользовательские пароли, коды доступа.

Электронные ключи eToken–персональное средство аутентификации и защищённого хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и ЭЦП.

Назначение электронных ключей:

– модельный ряд eToken представлен USB-ключами, смарт-картами, комбинированными устройствами и автономными генераторами одноразовых паролей;

– аппаратная поддержка работы с цифровыми сертификатами и ЭЦП;

– универсальное устройство: применяется в любых приложениях, использующих технологии смарт-карт или PKI (Public Key Infrastructure);

– встраивание бесконтактных радио-меток (RFID), применяемых для контроля физического доступа сотрудников в помещения.

Криптографическая защита. Одним из способов защиты информации от НСД является криптографическая защита (шифрование). Криптографическая защита может применяться на всех этапах обработки информации.

При построении систем криптографической защиты существуют различные решения. Например, защита информации осуществляется методом «прозрачного шифрования» с помощью стойких алгоритмов шифрования.

Зашифровать можно отдельные жесткие диски сервера, любые дисковые массивы, а также съёмные диски (например, подключаемые к серверу для резервного копирования). При чтении данных с диска происходит их раскодирование, при записи на диск — шифрование.

Находящиеся на диске данные всегда зашифрованы, что делает доступ к ним невозможным для злоумышленника даже в случае кражи или изъятия, как отдельного диска, так и всего сервера.

Основные функции криптозащиты это:

1. Прозрачное шифрование данных, производимое в реальном времени, позволяет работать с документами в обычном режиме;

2. Информация хранится в контейнере в виде зашифрованного файла на диске или внешнем носителе и защищается файл-ключом или электронным ключом;

3. При подключении контейнер отображается в системе как обычный диск. При отключении контейнер перестает отображаться в системе, поэтому установить факт наличия конфиденциальной информации и получить к ней доступ невозможно;

4. В программе существуют режимы экстренного отключения контейнеров и выхода из программы (режим «Опасность»), а также режим экстренного уничтожения доступа к информации для всех пользователей программы (режим «Большая опасность»).

Сетевая защита (системы предотвращения вторжений) обнаруживает вредоносную активность в сети за счет выявления аномалий на уровне протоколов или общего трафика, либо сопоставления событий, описываемых сигнатурами, с состоянием TCP-соединения и предотвращает её.

Назначение сетевой защиты:

– идентифицирует, классифицирует и блокирует вредоносный трафик, в том числе «черви», шпионские и рекламные программы, вирусы, а также предотвращает нарушения работы приложений;

– обеспечивает высокоэффективное интеллектуальное обнаружение угроз и защиту при различных вариантах развертывания;

– использует фильтрацию на основании репутации и глобальные проверки с целью предоставления предприятиям интеллектуальных рекомендаций, позволяющих принимать меры, и уверенного предотвращения угроз;

– поддерживает непрерывность деятельности и помогает предприятиям обеспечивать соответствие требованиям стандартов и нормативов.

Системы фильтрации содержимого (почта, Internet) – комплексное модульное программное решение, предназначенное для защиты корпоративной информации от утечки или несанкционированного распространения, предотвращает утечки конфиденциальной информации за счет оперативного анализа данных и автоматического применения политик безопасности, независимо от того, работают пользователи в корпоративной сети или за её пределами.

Назначение фильтрации содержимого:

– мониторинг и анализ данных, отправляемых за пределы корпоративной сети через почтовые системы, web, системы обмена сообщениями, распечатываемых или копируемых на различные устройства ввода-вывода;

– предотвращение утечки конфиденциальных данных путем блокирования процесса передачи в случае обнаружения нарушения политики безопасности;

– анализ и хранение данных для проведения расследований;

– анализирует содержание, контекст и направление передачи данных, позволяя администраторам управлять тем, кто может пересылать информацию, какую информацию разрешено пересылать, кому она может быть адресована и какими способами осуществляется пересылка;

– проводит мониторинг всех типов данных в сети и на конечных компьютерах, защищая данные от утечек, независимо от их формата и местоположения;

– централизованная система управления и отчетности предоставляет мощные инструменты анализа, выявления и устранения инцидентов, а также генерации отчетов.

Заключение. При формировании требований с условием максимального использования зарубежного научно-технического задела в этой области, необходимо учитывать специфические российские условия.

Так в связи с изменяющимися условиями и постоянными попытками пользователей избежать контроля должна проводиться постоянная адаптация алгоритма контроля.

Это может быть достигнуто при использовании в управляющем блоке РИЦ ИТС специальной ЭС.

Защита от умышленных попыток манипуляции со стороны «хакеров» могут быть предотвращены за счет:

– применения защищённых от НСД специальных АС;

– постоянная модификация АС при обнаружении новых видов мошенничества;

– постоянный мониторинг активности черного рынка (продажа видоизмененных программ и приборов);

– обеспечение высокого уровня контроля за работой АС за счет высокой степени его автоматизации;

– создание специальных контрольных лабораторий для внештатной проверки АС без контакта с сотрудниками контрольных органов;

– создание системы слежения за работой самих контролеров.

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-
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. Власов М.П., Голоскоков К.П., Панова Е.Н.Оценка экономической эффективности нововведений// Экономическое возрождение России. 2011. № 4 (30). С. 25-38.).
4. Брусакова И.А., Власов М.П., Голоскоков К.П. Информационные технологии в научных исследованиях высшей школы// Санкт-Петербург, 2012. 146с.
5. 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.
6. Голоскоков К.П. Технология испытаний и прогнозирования технического состояния электронных средств судовых систем управления//диссертация на соискание ученой степени доктора технических наук / Санкт-Петербургский государственный университет водных коммуникаций. Санкт-Петербург, 2009
7. Голоскоков К.П., Нестеренко Н.К., Чиркова М.Ю. Повышение эффективности деятельности производственного предприятия//Аудит и финансовый анализ. 2014. № 1. С. 331-335.
8. Брусакова И.А., Голоскоков К.П. Математическая модель функциональной надежности автоматизированных систем управления//Вестник ИНЖЭКОНа. Серия: Технические науки. 2010. № 8. С. 48-51.
9. Голоскоков К.П., Железняк М.В. Прогнозирование с применением теории распознавания образов// Вестник ИНЖЭКОНа. Серия: Технические науки. 2011. № 8. С. 114-118.

УДК 004.942

МОДЕЛИРОВАНИЕ РЕАГИРОВАНИЯ СИСТЕМЫ ПОЖАРНОЙ БЕЗОПАСНОСТИ ВОДНОГО ТРАНСПОРТА

Кардакова Мария Владимировна, Цымай Юлия Валериевна, Ныркov Анатолий Павлович, Колесниченко Сергей Викторович

Государственный университет морского и речного флота имени адмирала С.О. Макарова
ул. Двинская, 5/7, Санкт-Петербург, 198035, Россия
e-mails: apnyrkow@mail.ru, serjkop@yandex.com

Аннотация. Пожары и взрывы являются одной из наиболее распространённых причин гибели судов, после затоплений и посадки на мель. Соответственно, улучшение системы пожарной безопасности – это одна из актуальных задач, требующих внимания специалистов разного профиля. В данной статье рассмотрены различные системы пожарной безопасности на судне, проанализирована возможность использования тепловизоров, как пожарных извещателей. Приведены технические характеристики систем, выявлены основные критические зоны функционирования и обслуживания. Выполнены сравнительные расчёты по различным параметрам извещателей системы пожарной безопасности, используемых на судах в настоящее время, и тепловизоров. Рассмотрены критерии срабатывания систем противопожарной безопасности с учетом предлагаемой модернизации. Определены границы рабочих и критических диапазонов параметров срабатывания системы. Сделаны выводы о возможности дальнейшего улучшения системы пожарной безопасности на судне, обоснована возможность использования тепловизоров, как пожарных извещателей.

Ключевые слова: система пожарной безопасности; тепловизор; транспорт; водный транспорт; пожарная безопасность; детекторы дыма; тепловые детекторы; датчики пламени; тепловизионные камеры; судно; имитационное моделирование.

MODELING THE FIRE SAFETY SYSTEM RESPONSE ON WATER TRANSPORT

Kardakova Mariia, Tsymay Yulia, Nyrkov Anatoliy, Kolesnichenko Sergey

Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya street, Saint-Petersburg, 198035, Russia
e-mails: [1]apnyrkow@mail.ru, [2]serjkop@yandex.com

Abstract. Fires and explosions are one of the most common causes of shipwreck, after flooding and stranding. Accordingly, improving the fire safety system is one of the urgent tasks that requires the attention of specialists of various profiles. This article discusses various fire safety systems on the ship, analyzes the possibility of using thermal imagers as fire detectors. The technical characteristics of the systems are given, the main critical areas of operation and maintenance are identified. Comparative calculations have been performed on various parameters of fire safety detectors currently used on ships and thermal imagers. The criteria for the operation of fire safety systems are considered, taking into account the proposed modernization. The boundaries of the operating and critical ranges of the system response parameters are determined. Conclusions are drawn about the possibility of further improvement of the fire safety system on the ship, the possibility of using thermal imagers as fire detectors is justified.

Keywords: fire safety system; thermal imager; transport; water transport; fire safety; smoke detectors; thermal detectors; flame sensors; thermal imaging cameras; vessel; ship; simulation modeling.

Введение. Хотя тенденция происшествий сокращается, так с 2011 число происшествий, приводящих к гибели судов снизилось на 45%, безопасность все равно остается одним из главных критериев. Тем не менее самый большой процент аварий приходится на следующие регионы: Китай, Индокитай, Индонезия, Филиппины, Восточное Средиземноморье, Черное море и регионы Персидского залива. Гибель судов в большей степени происходит из-за: затопления, посадки на мель, пожаров, повреждения машинного оборудования. В большей степени авариям подвержены сухогрузные суда общего назначения и рыболовные суда [1]. Пожарам в большей степени подвержены грузовые суда и танкеры, из-за горючести перевозимых грузов. По данным статистики примерно 47% пожаров возникает во время судоремонта, 35% - при погрузке и выгрузке, а также стоянке, 18% - в пути следования.

Гибелью или полным конструктивным разрушением судна заканчиваются 20% пожаров. Из-за большого количества легко воспламеняющихся материалов и горючих веществ, находящихся в ограниченном пространстве судна, огонь быстро распространяется, а также его сложнее потушить и локализировать. При неудачных попытках предупреждения дальнейшего распространения или полной ликвидации очагов возгорания в течении 15 минут судно спасти не удастся [2]. Исходя из вышесказанного, локализация пожара на ранних стадиях или предотвращение пожара является одной из основных задач. Для задач локализации и выявления пожаров используют извещатели, которые являются частью сложных систем пожарной безопасности. Таким образом модернизация и улучшение извещателей – это актуальная задача для улучшения противопожарных систем.

Основными причинами пожаров являются халатность, нарушение противопожарных норм, самовозгорание грузов и материалов, неисправность электрических цепей и оборудования, разряды атмосферного и статического электричества, столкновение судов, умышленный поджог [3-5].

Тушение пожара важно начать на раннем этапе, с использованием эффективных средств тушения, таким образом удастся не допустить выхода огня за пределы помещения, в котором произошло возгорание. Если пожар не удасться взять под контроль или потушить на ранней стадии, то он может очень быстро распространиться на другие помещения из-за высокой теплопроводности металлических конструкций судна, множества кабелей электропитания, горючести материалов конструкции, наличии узких помещений и труднодоступных мест.

Исходя из вышесказанного локализация и определение пожара вовремя это основной фактор при борьбе с пожаром на судне. Чем быстрее противопожарная сигнализация справляется с этой задачей, тем проще будет потушить пожар. Но также необходимо исключить ложные срабатывания сигнализации. Все эти вопросы достаточно актуальны на сегодняшний день для повышения живучести судна.

Противопожарная система предназначена для локализации очага пожара, тушения его, а также предотвращения распространения огня. Противопожарная система судна состоит из извещателей, оповещателей и системы пожаротушения. На рис. 1 представлена типовая схема пожарной безопасности на водном транспорте с классификацией. На судах в основном используют дымовые, тепловые, комбинированные и ручные извещатели. При срабатывании извещателя сигнал подается на пост управления и на систему оповещения. Оповещение применяется как световое, так и звуковое, так же приходит сообщение о пожаре на пост управления судном. Дальше запускается система пожаротушения - либо автоматически, либо через пост управления.

Рис. 1. Типовая схема пожарной безопасности на водном транспорте

Когда возможен процесс медленного горения с выделением большого количества дыма, используют дымовые извещатели. На судах к таким извещателям относятся устройство для постоянного отбора проб воздуха, устройство для проверки воздуха на загрязнение дымом. Дымовой датчик может сработать при сильной запыленности помещения, от попадания в поток пара или от дыма от сигарет. Потому эти датчики не используются в помещениях, где выделяются струи пара, в местах для курения и в запыленных помещениях.

Тепловые извещатели определяют пожар по признаку выделения тепла. На судах обычно используются пороговые или интегральные тепловые извещатели. Пороговые датчики имеют заданную пороговую температуру, и если температура поднимается выше, то срабатывает сигнал опасности. Интегральные пожарные датчики реагируют на резкое повышение температуры. Такие датчики могут ложно сработать при сильных вибрациях корпуса, или при ударе о корпус извещателя.

Так же на судах используют датчики пламени, в тех помещениях, где может произойти пожар без предварительного дымовыделения. Но такие датчики необходимо использовать на открытых площадках, и нельзя монтировать на вибрирующих конструкциях. Такой датчик может обнаружить пожар на начальной стадии. Пламя определяется по электромагнитному излучению.

Используются и комбинированные датчики, сочетающие несколько способов определения, обычно сочетаются дымовые и тепловые. Такие датчики позволяют более точно определить признаки пожара [6].

Так как в борьбе с пожарами на судне решающим моментом является скорость реакции на пожар, актуальным является предупреждать пожар заранее и контролировать проблемные участки. Такие задачи может решить система с использованием тепловизоров. Тепловизионные камеры можно использовать для контроля помещений, в которых находятся самовоспламеняющиеся предметы или горючие вещества. Так же можно наблюдать за температурой оборудования, устройств или частей конструкции корпуса.

Тепловизионные камеры позволяют наблюдать тепловое (инфракрасное) излучение окружающих объектов и измерять температуру поверхностей. Принцип работы телевизора основан на анализе температуры поверхности

объекта. У любых материалов своя способность отражать и поглощать инфракрасное излучение, таким образом неравномерность нагрева поверхности позволяет сформировать картину распределенных на ней температур. Таким образом тепловизор можно использовать для определения отклонения температуры от заданной.

Тепловизионные камеры не могут использоваться как самостоятельные извещатели, конечно они должны быть использованы как вспомогательная система, регистрирующая температуру заданных поверхностей, и вырабатывающая сигнал на пост управления в случае повышения или отклонения температуры, а также транслирующая изображение камеры на пост управления в любой момент времени. Это поможет предупреждать пожары и реагировать на них в самой начальной стадии, если возгорание подразумевает изменение температуры объекта.

Было проведено моделирование параметров срабатывания систем пожарной безопасности на судне. Модель была построена с помощью комбинированного графа с использованием алгоритма Дейкстры [7, 8]. Одна из веток графа представлена на рис. 2.

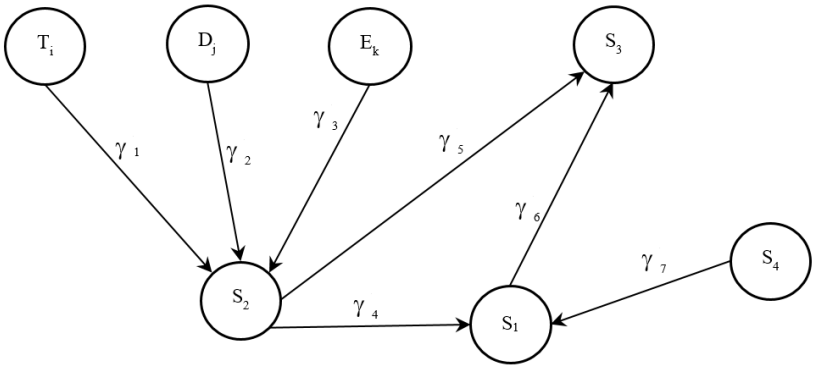


Рис. 2. Модель противопожарной системы

Где S_1 – центральный управляющий блок, S_2 – локальный блок сбора и анализа сигнала, T_i – датчики температуры, D_j – датчики дыма, E_k – датчики пламени, S_3 – блок автоматического оповещения, S_4 – блок ручного оповещения, ($\gamma_1 \ldots \gamma_7$) - весовая функция на множестве ребер графа.

Объекты соединены кабельными трассами. Данная модель позволяет исследовать систему, установленную в одном помещении, с удаленным на некоторое расстояние пультом приема сигналов.

По данным стандартов длина соединения от S_4 до S_1 не более 20 м. Для остальных трасс данные параметры не установлены. Это связано с тем, что стартовый бит сигнала от блока автоматического оповещения начинает передаваться в разы быстрее, чем от блока ручного оповещения. При необходимости можно использовать дополнительные узлы контроля. На рис. 2 представлен только узел S_2, как единственное тестовое пространство. Количество датчиков температуры, дыма и пламени определяется в соответствии с размерами помещения. Если площадь составит не более 37 м^2, то необходимое количество датчиков каждого типа T_i=1, D_j=1, E_k=1. При площади помещения, увеличенной в два раза необходимо T_i=2, D_j=1, E_k=1. Соответственно в математической модели необходимо учесть еще один канал связи, что приведет к повышению нагруженности S_2 на 25%. При увеличении тестируемой площади оптимально использование топологии «звезда», добавляя в математическую модель для каждого помещения состояние, аналогичное S_2 в связке с необходимым набором датчиков.

Модель противопожарной системы математически можно представить следующим образом:

$$G = \begin{cases} S(S_1, S_2, S_3, S_4, T_i, D_j, E_k) \\ N(n_1, \ldots, n_m) \\ \gamma(\gamma_1, \ldots, \gamma_m) \end{cases}, \quad (1)$$

где $S(S_1, S_2, S_3, S_4, T_i, D_j, E_k)$ – множество вершин графа, $N(n_1, \ldots, n_m)$ – множество ребер графа, $\gamma(\gamma_1, \ldots, \gamma_2)$ – весовая функция на множестве ребер графа.

В случае m=7, с учетом пропускной способности C_m каналов связи, можно определить среднюю задержку при передаче сообщения по каналу T_m:

$$T_m = \frac{1}{\mu C_m - \gamma_m}, \quad (2)$$

где $1/\mu$ – средняя длина сообщения.

Для простейшей модели длина сообщения, передаваемого от любого датчика в узел S_2, может соответствовать двухразрядному двоичному коду. На интервале $S_2 – S_1$ – код преобразуется в четырехразрядный. Остальные связи можно отнести к простейшим и присвоить разрядность 2. Такой способ кодирования сообщений позволит локализовать точку возгорания в момент поступления сообщения.

Для учета времени срабатывания противопожарной системы, помимо возможной задержки, необходимо учесть чувствительность датчиков и общее время отклика. Данные параметры обычно рассматриваются как известные константы, т.к. зависят от типа оборудования [9-11].

Недостатком данной модели является невозможность исключить ложные срабатывания, возникающие при уровне влажности 95% и температурах около 40 ^{0}C.

Так как в борьбе с пожарами на судне решающим моментом является скорость реакции на пожар, актуальным является предупреждать пожар заранее и контролировать проблемные участки. Такие задачи может решить система с использованием тепловизоров. Тепловизионные камеры можно использовать для контроля помещений, в которых находятся самовоспламеняющиеся предметы или горючие вещества. Так же можно наблюдать за температурой оборудования, устройств или частей конструкции корпуса. Тепловизионные камеры позволяют наблюдать тепловое (инфракрасное) излучение окружающих объектов и измерять температуру поверхностей. Принцип работы телевизора основан на анализе температуры поверхности объекта. У любых материалов своя способность отражать и поглощать инфракрасное излучение, таким образом неравномерность нагрева поверхности позволяет сформировать картину распределенных на ней температур. Таким образом тепловизор можно использовать для определения отклонения температуры от заданной.

Модель противопожарной системы с тепловизионными камерами показана на рис. 3. Вершина графа S_5 это состояние тепловизора, учитывающее угол поворота в течение определенного времени и объем кадра пересылаемого сообщения. В данном случае для кодирования сообщения недостаточно величины разрядности, предложенной в предыдущем варианте математической модели. Но время передачи данных от тепловизора должно синхронизироваться с временем передачи сигнала от других датчиков. Для этого предполагается использование канала связи с усиленной пропускной способностью.

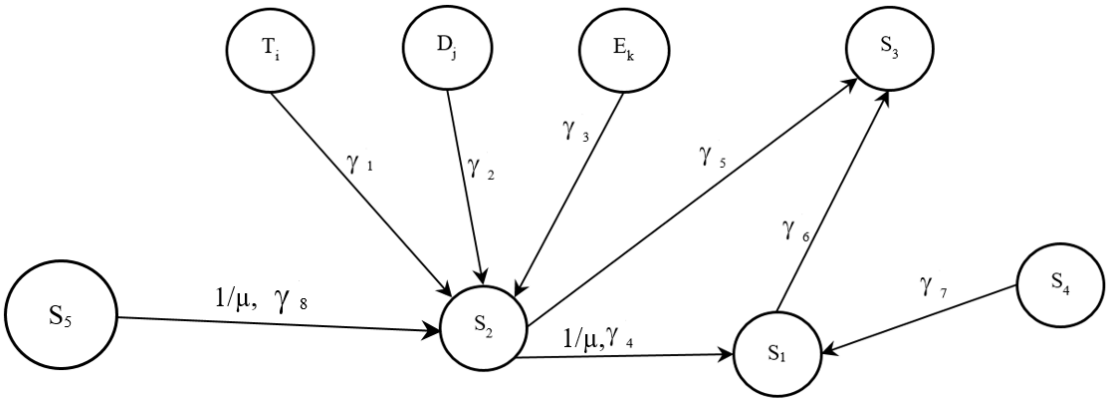


Рис. 3. Модель противопожарной системы с тепловизором

Где S_1 – центральный управляющий блок, S_2 – локальный блок сбора и анализа сигнала, T_i – датчики температуры, D_j – датчики дыма, E_k – датчики пламени, S_3 – блок автоматического оповещения, S_4 – блок ручного оповещения, S_5 – тепловизор, (γ_1 …γ_7) - весовая функция на множестве ребер графа, (1/μ, γ_4), (1/μ, γ_8) - весовая характеристика ребер графа с учетом разрядности передаваемого сообщения.

Исходные данные для моделирования представлены в таблице 1.

Таблица 1

Исходные данные для моделирования противопожарной системы

	Чувствительность	Порог срабатывания	Диапазон температур, t, ^{0}C		Дальность действия, l, м		Время отклика	
			t_{min}	t_{max}	l_{min}	l_{max}	с	%
Тепловизор	0,1 ^{0}C	-	-40	+1200°C	0,1	2100	0,01	0,02
Датчик температуры	1,5 ^{0}C	54 °C 8^{0}C/мин	-40	+90	0	37	10	16,67
Датчик дыма	0,05 дБ/м	0,05 дБ/м	-50	+60	0	74	58	96,67
Датчик пламени	50 лк	54 °C	-40	+75	0,8	25	20	33,33
Кабельная трасса	-	-	-40	+60	0,5	-	-	-

Наружный размер D_H кабельной трассы D_{Hmin} = 11,2 мм, D_{Hmax} = 28,1 мм.

Для сохранения универсальности модели примем допущение о задержке сигнала на каждом ребре графа не более 1% от общего времени передачи, что составит ≈1,67 с, и не менее 20% - для принятия решения об отмене (≈33,3 с).

Результаты реализации временных параметров передачи сигнала о возникновении критической ситуации представлен на рис. 4. По вертикальной шкале определяется условное время от момента определения факта возгорания до включения блока автоматического оповещения. По горизонтальной шкале указаны ключевые моменты срабатывания системы.

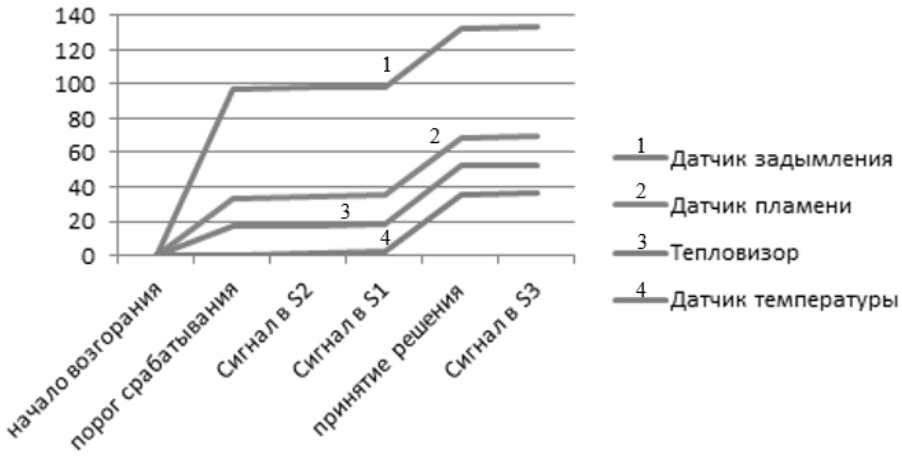


Рис. 4. Результаты реализации временных параметров передачи сигнала о возникновении критической ситуации

Заключение. Сравнительный анализ времени передачи сигнала о возникновении критической ситуации показал, что на этапе первичной обработки сигнала (S_2) система с использованием тепловизора реагирует на 5% быстрее. Соответственно на последующих стадиях функционирования при условии накопительной функции времени срабатывание системы противопожарной безопасности произойдет на 25% быстрее. Таким образом, снижается вероятность ложного срабатывания. В связи с вышесказанным рекомендуется использовать тепловизоры в качестве дополнительного средства контроля.

СПИСОК ЛИТЕРАТУРЫ

1. AGCS «Safety & Shipping Review 2021». Report by Allianz unveils trends and developments in shipping losses and safety during 2021. https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/ AGCS-Safety-Shipping-Review-2021.pdf
2. Sokolov, S.S., Glebov, N.B., Antonova, E.N., Nyrkov, A.P. «The Safety Assessment of Critical Infrastructure Control System» 2018 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies», IT and QM and IS 5 November 2018, pp. 154-157. https://doi.org/10.1109/ITMQIS.2018.8524948
3. Нырков А.А. Особенности возникновения и распространения пожаров на метрополитене // Сб. науч. трудов, посвящ. 190-летию транспортного образования в России. Под редакцией Ю.М.Кулибанова. СПб: СПГУВК, 1999. – С. 270 – 274.
4. Нырков А.А. Автоматизация расчета газовых потоков при пожаре на станциях метрополитена / Нырков А.А., Нырков А.П. // «Информационные управляющие системы и технологии» (ИУСТ–Одесса–2014). Материалы международной научно-практической конференции, 23 – 25 сентября 2014 г. – Одесса. 2014. – С. 77–79.
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» 2019 IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW), St. Petersburg; 2019. pp. 339-343. https://doi.org/10.1109/EIConRus.2019.8657219
6. I.S. Shipunov, A.P. Nyrkov, M.V. Kardakova, Y.F. Katorin and V.V. Vychuzhanin. «Information System for Monitoring and Analyzing the Technical Condition of Autonomous Vehicles» 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg and Moscow, Russia, 2020, pp. 497-500, doi: 10.1109/EIConRus49466.2020.9039181.
7. Dijkstra E. W. A note on two problems in connexion with graphs. Numer. Math. Springer Science+Business Media, 1959. Vol. 1, Iss. 1. P. 269–271. ISSN 0029-599X; 0945-3245. doi:10.1007/BF01386390
8. Нырков А.П., Дмитриева Т.В. Математическая модель резервирующей системы и оптимизация ее работы // Журнал университета водных коммуникаций. – № 2, 2011. – С. 98 – 101.
9. Sokolov, S. Assessment of the Impact of Destabilizing Factors in the Main Engine Shaft of the Adaptive Speed Controller / S. Sokolov, A. Zhilenkov, S. Chernyi, A. Nyrkov // Procedia Computer Science 125 2018. – Pp. 420-426. https://doi.org/10.1016/j.procs.2017.12.055
10. Нырков А.П., Соколов С.С., Белоусов А.С. Мультисервисная сеть транспортной отрасли // «Вестник компьютерных и информационных технологий». – № 4, 2014. – С. 33 – 38. https://doi.org/10.14489/vkit.2014.04.pp.033-038
11. Зубанова А.А., Шипунов И.С., Нырков А.П. «О возможностях применения программируемых логических контроллеров для целей мониторинга состояния судового оборудования» // Материалы конференции «Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября 2020 г.: Материалы конференции. Часть 1. – СПб, СПОИСУ, 2020. – С. 345–348.

УДК 004.056

АНАЛИЗ РИСКОВ ПРИ ПЕРЕДАЧЕ ФУНКЦИЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ НА АУТСОРСИНГ

Кириков Антон Викторович, Ныркoв Анатолий Павлович
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: tony-68@yandex.ru, apnyrkow@mail.ru

Аннотация. Рассмотрены проблемные вопросы, возникающие в случае передачи функций обеспечения информационной безопасности транспортных предприятий внешнему исполнителю.

Ключевые слова: безопасность информации; менеджмент безопасности; аутсорсинг; критическая информационная инфраструктура; транспортные объекты.

RISK ANALYSIS WHEN OUTSOURCING INFORMATION SECURITY FUNCTIONS FOR TRANSPORT INFRASTRUCTURE FACILITIES

Kirikov Anton, Nyrkov Anatoliy
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: tony-68@yandex.ru, apnyrkow@mail.ru

Abstract. The problematic issues that arise in the case of transferring the functions of ensuring information security of transport enterprises to an external contractor are considered.

Keywords: information security; security management; outsourcing; critical information infrastructure; transport facilities.

Введение. Исходя из существующего уровня угроз, современные системы информационной безопасности (ИБ) реализуют принцип «defense-in-depth», или «многоэшелонированной» защиты. Они включают подсистемы сетевой безопасности (часто гетерогенные с позиций используемого оборудования), антивирусные подсистемы, подсистемы строгой аутентификации, резервного копирования, мониторинга и др. Их создание и поддержка требуют приобретения довольно дорогих программно-аппаратных комплексов и привлечения высококвалифицированных специалистов.

В связи со сложностью решаемых при обеспечении ИБ задач, уже сложилась практика передачи данных функций внешним исполнителям. Принципы аутсорсинга информационной безопасности можно найти в стандартах по управлению ИБ, например, в ISO 27001:2013; ISO 13335-3; NIST SP800-35 Guide to Information Technology Security Services или в Cobit 4.0 и 5.0.

Несколько лет назад в публикациях встречались мнения, что «в крупных компаниях, имеющих большой штат ИТ-департамента, проблема подбора высококлассных специалистов не стоит так остро, как в организациях среднего и малого бизнеса» [1]. Вместе с тем, тот же самый автор указывает на то, что «большая инертность крупного бизнеса не позволяет быстро реагировать на новые угрозы и нанимать нужных специалистов» [1].

Здесь необходимо дополнительное развитие указанных выше тезисов. Проблемы с укомплектованием штата подразделений ИБ характерны уже не только для частных, но и для государственных предприятий, в том числе отнесенных законодателем к субъектам критической информационной инфраструктуры. К таковым относятся и предприятия транспорта.

Но и на этом проблемы не заканчиваются. Зачастую руководство даже государственных предприятий откровенно экономит на содержании подразделений ИБ, либо старается не замечать новых угроз, связанных, в частности, с обеспечением безопасности критической информационной инфраструктуры [2, 3], что актуально для предприятий транспорта в том числе [4, 5].

Анализу возможных рисков, возникающих при передаче функций ИБ на аутсорсинг и посвящена данная статья.

«Аутсóрсинг» - передача организацией, на основании договора, определённых видов или функций производственной (предпринимательской) деятельности другой компании, действующей в нужной области [6, 7].

Рассмотрим, что собой представляет рынок аутсорсинга информационной безопасности, и может ли применительно к ИБ это вообще называться аутсорсингом в чистом виде.

Обеспечение ИБ – весьма широкое понятие. Попытаемся проанализировать и составить классификацию его направлений применительно к обеспечению ИБ.

Составление всего списка услуг по обеспечению ИБ позволяет их рассортировать по четырем группам, приведенным в таблице 1.

Таблица 1

Направления аутсорсинга в ИБ, направленные на обеспечение (управление) ИБ на протяжении всего жизненного цикла предприятия (Managed Security Lifecycle)

Направленность на аппаратное и программное обеспечение		Направленность на «человеческий» фактор	
Управление продуктами сетевой безопасности	Управление продуктами прикладной защиты	Предоставление «непродуктовых» услуг	Больше консалтинг, чем продукты
Управление использованием брандмауэров и межсетевых экранов (Managed FW)	Управление использованием антивирусной защитой (Managed AV)	Предоставление защищенной инфраструктуры (ЦОД, SOC, облачные сервисы)	Обеспечение безопасного использования пользователями одинаковых плагинов (Managed Secure IM), IP-технологий (Managed Secure IPT), видеоконференцсвязи (ВКС), Интернет-телевидения (IPTV) и технологий Wi-Fi
Управление использованием VPN – приложений и сервисов (Managed VPN)	Обеспечение безопасности использования приложений *	Управление системой мониторинга событий и управления инцидентами ИБ (Managed SIEM)	Обеспечение безопасного использования мобильных приложений (Managed Mobile Security)
Управление использованием системой обнаружения вторжений (СОВ) - как программной или аппаратной системы сетевой и компьютерной безопасности, обнаруживающей вторжения или нарушения безопасности и автоматически защищающей от них. (Managed IDS)	Обеспечение безопасности использования электронной почты (Managed Secure Email)	Реализация объединенного подхода к защите пользователей оконечных устройств (Managed Secure Endpoint)	Обеспечение безопасного создания веб-проектов, использования Интернет/интранет систем, систем управления информацией (Managed Web)
Управление использованием сканеров безопасности Web – приложений (Managed security scanners)	Обеспечение безопасности использования предоставленного файлового пространства (Managed Secure hosting)	Реагирование на инциденты (использование внешней ГРИИБ)	Обеспечение функционирования защищенных хранилищ (Managed Secure Storage)

*Примечание: управление безопасностью использования приложений включает в себя меры, принимаемые для повышения безопасности приложения, часто путем обнаружения, исправления и предотвращения уязвимостей в безопасности. Для выявления уязвимостей на разных этапах жизненного цикла приложений, таких как проектирование, разработка, развертывание, обновление, обслуживание, используются различные методы.

Проблемные вопросы, возникающие при аутсорсинге, разбитые на группы

1. О цене вопроса:

– чтобы обеспечить своими силами режим работы 24х7, (а не 8х5), предприятию понадобится в 4,2 раза больше людей (плюс оплата сверурочных за работу в выходные);

– как правило, договор с внешним исполнителем заключается в у.е., следовательно, не нужно забывать про колебания валютного курса и, как правило, не в сторону уменьшения, то есть – не в пользу предприятия;

– включено ли обновление ПО в стоимость контракта? Если нет, то цена аутсорсинга может вырасти на 20-70 %. Если договор заключается на длительный срок, то обновление ПО должно быть предусмотрено на этот же срок;

– как оценивается стоимость модернизации аппаратной части и предусмотрено ли это договором?

– как оцениваются затраты, неизбежно возникающие при подготовке к переходу на аутсорсинг? (подготовка каналов связи, резервирования, средств контроля и т.д.).

Итак, сравнивая варианты, возникает вопрос о наличии экономии (табл. 2).

Таблица 2

Сравнение вариантов

Служба ИБ	=	Затраты на ИБ			Без аутсорсинга
Служба ИБ	+	Аутсорсинг ИБ	=	Затраты на ИБ	В чем экономия?

2. О реальной экономии:

– реальная экономия от аутсорсинга может быть достигнута только при соблюдении следующих условий:

– предприятие имеет большой штат дорогостоящих специалистов по ИБ;

– на предприятии достаточно персонала в области ИБ, после передачи части их обязанностей на аутсорсинг «лишний» персонал сократили, перераспределили их или скорректировали их обязанности;

– при отказе от традиционного приобретения средств защиты информации (СЗИ) в пользу лизинга или аренды (такое не всегда возможно, исходя из внутренней политики предприятия или отрасли);

– контракт на аутсорсинг долговременный (более 1 года);

– на предприятии есть силы и средства контроля выполнения аутсорсером своих обязанностей.

3. Проблема выбора аутсорсера с точки зрения ИБ, какие факторы необходимо принять во внимание:

– как организована защита данных и обеспечение приватности;

– как организовано управление уязвимостями;

– как организована объектовая охрана и персонал;

– доступность и производительность;

– как организованы мониторинг событий ИБ и управление инцидентами;

– как будет обеспечена непрерывность производственных процессов (бизнес-процессов) и их восстановление после катастроф;

– как будет производиться ведение журналов регистрации;

– каковы финансовые гарантии от внешнего исполнителя в случае наличия убытков по его вине;

– как обговорена процедура завершения контракта;

– как будет обеспечена сохранность интеллектуальной собственности вашего предприятия внешним исполнителем.

4. Отдельно в обязательном порядке необходимо обсудить вопрос защиты данных:

– как данные вашего предприятия отделены от данных других клиентов?

– как хранятся данные вашего предприятия?

– как обеспечивается конфиденциальность и целостность данных вашего предприятия?

– как осуществляется контроль доступа к вашим данным и их защита от НСД?

– как данные защищаются в случае передачи их от вашего предприятия облачному провайдеру?

– как защищаются данные при передаче от одной площадки облачного провайдера к другой?

– реализованы ли меры по контролю утечек данных?

– может ли третья сторона получить доступ к вашим данным (оператор связи, аутсорсер облачного провайдера, правоохранительные органы) и как это закреплено в договоре?

– все ли данные вашего предприятия удаляются по завершении предоставления сервиса и как это можно проверить?

5. Управление уязвимостями, на что нужно обратить внимание:

– как часто сканируется сеть и приложения?

– попадает ли облачный провайдер под требования стандарта безопасности данных индустрии платёжных карт (PCI DSS) и ежеквартального сканирования со стороны ASV? (Approved Scanning Vendor – поставщик услуг сканирования, имеющий официальный статус от Совета стандартов безопасности (PCI SSC);

– может ли заказчик осуществить внешнее сканирование сети аутсорсера с целью контроля его защищенности и на каких условиях?

– как организован процесс устранения уязвимостей?

6. Управление идентификацией:

– возможна ли интеграция с вашим каталогом учетных записей и каким образом?

– если у аутсорсера собственная база учетных записей, то как она защищается и как осуществляется управление учетными записями?

– поддерживается ли технология единого входа (Single Sign-On, SSO) для обеспечения возможности использования одного идентификатора для доступа ко всем разрешенным ИТ-ресурсам и системам и решения задачи строгой и сквозной аутентификации пользователей, какой стандарт?

– поддерживается ли общероссийская система аутентификации, какой стандарт?

7. Организация объектовой охраны и персонала:

– осуществляется ли контроль доступа на территорию аутсорсера в режиме 24х7?

– у аутсорсера выделенная инфраструктура или разделяемая с другими компаниями?

– производится ли регистрация доступа персонала аутсорсера к данным клиентов?

– есть ли результаты оценки аутсорсера внешним аудитом?

– какова процедура приема на работу и проверки персонала у аутсорсера?

8. Обеспечение доступности ваших данных аутсорсером:

– обеспечиваемый уровень доступности в соглашении об уровне услуг («service-level agreement» (SLA), сколько девяток?

– какие меры обеспечения доступности (резервный оператор связи, защита от DDoS-атак);

– доказательства обеспечения высокой доступности аутсорсера?

– план действий во время простоя;

– пиковые нагрузки и возможность аутсорсера справляться с ними;

– уровень сертификации ЦОД аутсорсера.

9.Обеспечение безопасности приложений:

– исполнение рекомендаций открытого проекта обеспечения безопасности веб-приложений (сообщества OWASP) при разработке приложений;

– процедура тестирования для внешних приложений и исходного кода;

– существуют ли приложения третьих фирм при оказании сервиса;

– используемые меры защиты приложений (Web Application Firewall, Database Firewall, аудит БД).

10. Управление инцидентами:

– каков план реагирования на инциденты (включая метрики оценки эффективности)?

– корреляция политик управления инцидентами вашего предприятия и аутсорсера (особенно, если аутсорсер находится за рубежом и\или в другом часовом поясе)?

– сотрудники фирмы-аутсорсера говорят на вашем родном языке (при оперативном реагировании на инциденты времени искать переводчика не будет)?

11. Обеспечение конфиденциальности вашей информации:

– производится ли обезличивание критичных данных и предоставление к ним доступа только авторизованному персоналу?

– какие данные собираются о заказчике, где хранятся, каким образом и как долго?

– каковы условия передачи данных о клиенте третьим лицам (правоохранительные органы, прокуратура, суд, адвокатские и депутатские запросы)?

– каковы гарантии нераскрытия вашей информации третьим лицам и после этого – третьими лицами?

12. Обеспечение непрерывности производственных процессов (бизнес-процессов):

– есть ли план обеспечения бизнеса и восстановления после катастроф?

– есть ли у предприятия резервный ЦОД, если ЦОД аутсорсера будет выведен из строя?

– проходил ли аутсорсер внешний аудит по непрерывности бизнеса и есть ли у него сертифицированные сотрудники по непрерывности бизнеса?

13. Регистрация событий и инцидентов ИБ:

– каким образом аутсорсер обеспечивает сбор доказательств несанкционированной деятельности?

– как долго аутсорсер хранит логи и возможно ли увеличение этого срока?

– возможно ли организовать хранение логов во внешнем хранилище и каким образом?

14. Ответственность и гарантии:

– какие ваши действия, если инцидент ИБ произошел по вине аутсорсера (и разграничена ли грань между событием и инцидентом, штатной ситуацией в договоре?), какова ответственность аутсорсера каковы и чем обеспечены его гарантии?

– гарантия качества аутсорсера (самым главным в аутсорсинге ИБ представляется ответ на вопрос: что делать, а что нет);

– описано ли качество сервиса в соглашении об уровне услуг («service-level agreement» (SLA), если нет – необходимо потребовать;

– необходимо очень внимательно и критически отнестись к предложенному вам KRI, KPI, PI;

– какова материальная ответственность аутсорсера и готов ли он возмещать ущерб вашему предприятию?

– необходимо помнить о том, что страхование информационных рисков в России не работает!

15.Финансовые гарантии – какая компенсация подразумевается в случае инцидента ИБ или нарушения SLA:

– процент от упущенной выгоды;

– процент от заработка во время простоя;

– процент от стоимости утекшей информации;

– процент от суммы договора на оказание облачных услуг.

16. Вопросы обеспечения интеллектуальной собственности вашего предприятия:

– кому принадлежат права на информацию, переданную аутсорсеру (на резервные копии, на реплицированные данные, на логи, на приложения)?

– есть ли уверенность в том, что контракт с аутсорсером в области ИБ не приводит к потере прав на информацию и иные ресурсы, переданные аутсорсеру?

17. Обеспечение безопасности информации при завершении контракта:

– как прописана процедура завершения контракта (как обеспечивается возврат данных, в каком формате; в какой разумный срок происходит возврат ваших данных; каким образом будут уничтожены все резервные и иные копии ваших данных и каковы гарантии этого)?

– какие дополнительные затраты возможны на завершение контракта?

Вышеуказанные показатели рисков при аутсорсинге ИБ являются глобальными, т.е. общемировыми. Но аутсорсинг ИБ в России имеет еще и дополнительные особенности:

1) сложность заключается в том, что Россия – страна с очень большой территорией. Если у вашего предприятия есть площадки за пределами Москвы, то это становится серьезной проблемой, поскольку у аутсорсеров обычно всего один Security Operaton Center (SOC) – в Москве, а для западных компаний – за пределами РФ;

2) проблемы с качеством каналов связи: хорошая связь обычно есть в крупных городах. Продолжать мысль нет смысла (как быть с портами Севморпути?);

3) сложно представить, как с такими расстояниями и каналами связи будут решены вопросы: «Почему произошел инцидент ИБ?», «Кто виноват?», «Что делать?», «Как этого не допустить впредь?»;

4) может ли аутсорсер оперативно выехать на место нарушения за несколько сотен или тысяч километров?

5) ошибочные стереотипы мышления руководителей российских предприятий всех уровней: «Содержать штат сотрудников, которые в круглосуточном режиме будут заниматься мониторингом и отражением компьютерных атак, может позволить себе далеко не каждая компания», однако при этом воспринимают всерьез посыл аутсорсера: «Специалисты компании «XXX» выполнят следующие работы: «Предоставление рекомендаций по выявленным инцидентам безопасности», то есть иными словами: - вам предлагают смотреть телевизор за вас, но в случае его поломки ремонтировать самому!

Если и после этого руководство предприятия решило «экономить» на подразделении ИБ путем привлечения внешнего исполнителя, то подумайте о еще более серьезных и коварных последствиях:

1) вы не развиваете своих специалистов ИБ, а соглашаетесь с уровнем знаний и развития технологий компании-аутсорсера, при этом чаще всего аутсорсер по этим характеристикам для вашего предприятия неизвестен (т.е. «кот в мешке») и вероятнее всего его специалисты не грамотнее и не компетентнее ваших – попробуйте объяснить это руководству предприятия. В России жесточайшая нехватка квалифицированных специалистов по ИБ, а квалифицированный специалист по ИБ не будет заниматься рутинной работой по «просиживанию штанов за консолью». Кроме того, если персонал аутсорсера квалифицированней вашего, то почему его услуги должны стоить дешевле?

2) возможно, что для выполнения своей деятельности ваше предприятие должно поддерживать лицензии ФСТЭК (ФСБ) РФ, но уровень аутсорсера вдруг перестает удовлетворять требованиям регулятора, аутсорсер прекращает свою работу с вами (одновременно аннулируются выданные им документы), и что при этом будете делать вы и руководство предприятия?

3) наконец, о реальности обещаний и заявлений аутсорсеров: один из российских аутсорсеров заявляет об «…архивировании данных сроком до 7 лет». Исходные данные (усредненные): длина сигнала тревоги (без дампа) - 100 байт; число сигналов тревоги с одного СЗИ в секунду - 1000 (в зависимости от типа); объем лога от одного СЗИ за сутки - 8.64 Гб; объем лога от одного СЗИ за 7 лет - 22.08 Тб. Теперь необходимо умножить этот объем на количество СЗИ и поинтересоваться – а у каких российских аутсорсеров ИБ есть такой замечательный центр обработки данных?

Заключение. Возможные выводы на основе вышеизложенного:

– при условии нехватки персонала в области ИБ в России аутсорсинг ИБ ни в коем случае не может быть средством экономии;

– аутсорсинг ИБ в России на данном этапе применим только в Москве (реалистично) или в крупных федеральных центрах (оптимистично);

– много ли объектов морского (речного) транспорта находится в Москве и крупных федеральных центрах? Открытый вопрос к руководству данных объектов и ФАМРТ;

– вопрос о возможности\невозможности передачи функций ИБ внешнему исполнителю нормативными актами основного регулятора (ФСТЭК РФ) никак не отрегулирован. В правовом плане – это правовой пробел. Конкретно в данном вопросе – еще и проблема, требующая внимания и вариантов решения.

«Народ, не желающий кормить свою армию, вскоре будет кормить чужую» (Наполеон Бонапарт).

СПИСОК ЛИТЕРАТУРЫ

1. Статья: «Что такое аутсорсинг ИБ?» [Электронный ресурс] – URL: https://www.anti-malware.ru/analytics/Market_Analysis/Outsourcing_Information_Security_overview_of_the_market (Дата обращения: 20.06.2021).
2. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ. [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 21.06.2021).
3. Постановление Правительства РФ от 8 февраля 2018 г. № 127 «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». [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_290595/ (Дата обращения 21.06.2021).
4. Кириков А.В. Информационная безопасность на объектах транспортной инфраструктуры / А. В. Кириков, А. П. Нырков, С. С. Соколов, В. Д. Гаскаров // Материалы межвузовской научно-практической конференции «Современные тенденции и перспективы развития водного транспорта России» 01 октября 2020 года: Часть 3. – СПб. : Изд-во ГУМРФ им. адм. С. О. Макарова, 2020. – С. 67–69.
5. Sokolov, S.S. The Safety Assessment of Critical Infrastructure Control System / S. S. Sokolov, N. B. Glebov, E. N. Antonova, A. P. Nyrkov // Proceedings of the 2018 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
6. Михайлов Д. В. Аутсорсинг. Новая система организации бизнеса. Учебное пособие. — М.: КноРус, 2006. — ISBN 5-85971-180-8.
7. А. Д. Воронченок, А. С. Тихомиров, С. В. Скородумов. Аутсорсинг высоких технологий при создании новой техники. — М., 2006.

УДК 004.056

НАЗНАЧЕНИЕ И ЗАДАЧИ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОЦЕНКИ И ПРОГНОЗИРОВАНИЯ КИБЕРУГРОЗ НА МОРСКИХ СУДАХ ПОД ФЛАГОМ РФ

Когтев Алексей Валерьевич
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mail: xx.ww.zz@ya.ru

Аннотация. В статье представлены назначение и основные задачи автоматизированной информационной системы оценки и прогнозирования киберугроз на морских судах под флагом РФ.

Ключевые слова: автоматизированная информационная система; киберугрозы; кибербезопасность; морские суда.

PURPOSE AND OBJECTIVES OF THE AUTOMATED INFORMATION SYSTEM FOR ASSESSING AND PREDICTING CYBER THREATS ON SEA VESSELS UNDER THE FLAG OF THE RUSSIAN FEDERATION

Kogtev Alexey
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mail: xx.ww.zz@ya.ru

Abstract. The article presents the purpose and objectives of the automated information system for assessing and predicting cyber threat on sea vessels under the flag of the Russian Federation.

Keywords: automated information system; cyber threat; cybersecurity; sea vessels.

Введение. В настоящее время общемировой тенденцией является цифровизация различных сфер экономики и её отраслей. Это в полной мере касается и отрасли морского транспорта: увеличивается количество автоматизированных процессов, активно развивается электронная навигация, происходят дистанционные обновления бортовых судовых систем во время плавания, датчики телеметрии передают на берег данные о состоянии систем судна и экипажа, у команды имеется возможность выхода в интернет и использования электронных ресурсов. Для того чтобы функционирование этих и многих других автоматизированных процессов не несло угроз для безопасности судна и экипажа в рейсе, необходимо выполнять требования по обеспечению кибербезопасности.

В последние годы наблюдается значительный рост количества киберинцидентов в области морского судоходства. Только за последний год количество попыток морских кибератак увеличилось на 400% [1, 2]. Одними из причин этого является масштабный процесс автоматизации судовых процессов и развитие безэкипажного судоходства [3-6], диктует необходимость разработки и принятия мер, направленных на противодействие

киберугрозам, снижение вероятности наступления негативных последствий от их реализации и получения возможности прогнозирования возникновения и реализации киберугроз на морских судах.

Одной из таких мер, реализующих потребность морской отрасли в обеспечении кибербезопасности, может стать создание автоматизированной информационной системы оценки и прогнозирования киберугроз на морских судах под флагом РФ (автоматизированная ИС ОиПК).

Назначение автоматизированной ИС ОиПК, представлено на рис. 1.

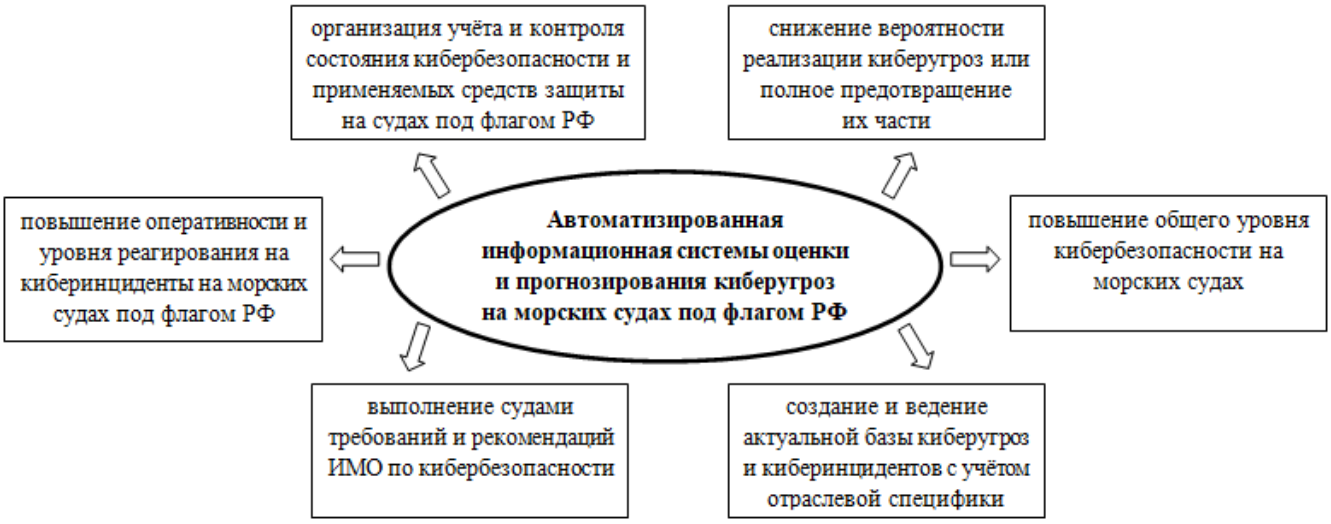


Рис. 1. Назначение автоматизированной ИС ОиПК.

Представленное назначение автоматизированной ИС ОиПК можно считать перечнем основных целей системы, достижение которых ожидается от её эксплуатации.

Достижение целей создания автоматизированной ИС ОиПК может предполагать реализацию следующих основных задач, представленных на рис. 2:

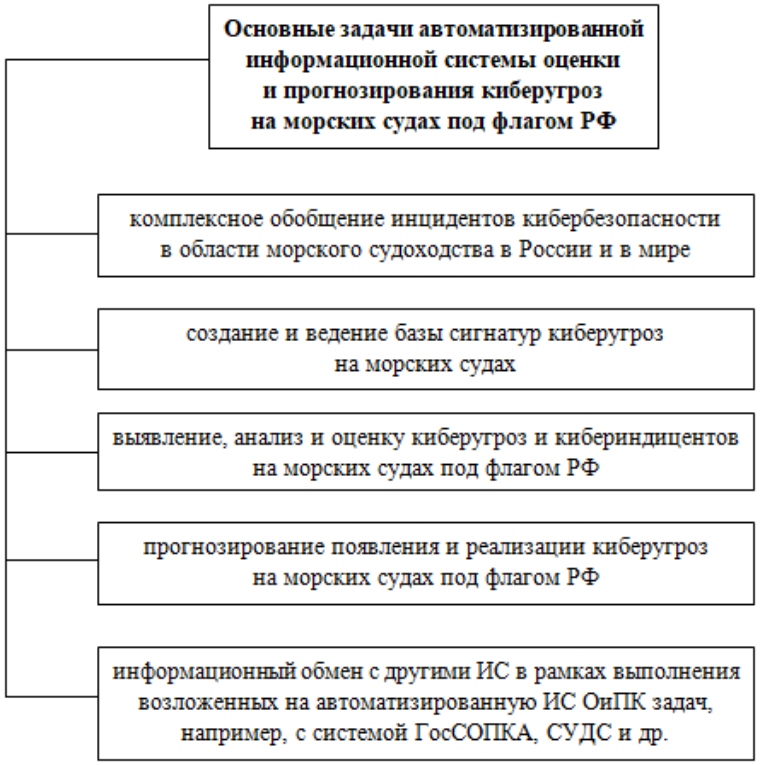


Рис. 2. Основные задачи автоматизированной ИС ОиПК.

Исходя из назначения и задач автоматизированной ИС ОиПК, сфера её применения, представленная на рис. 3, может быть следующая:

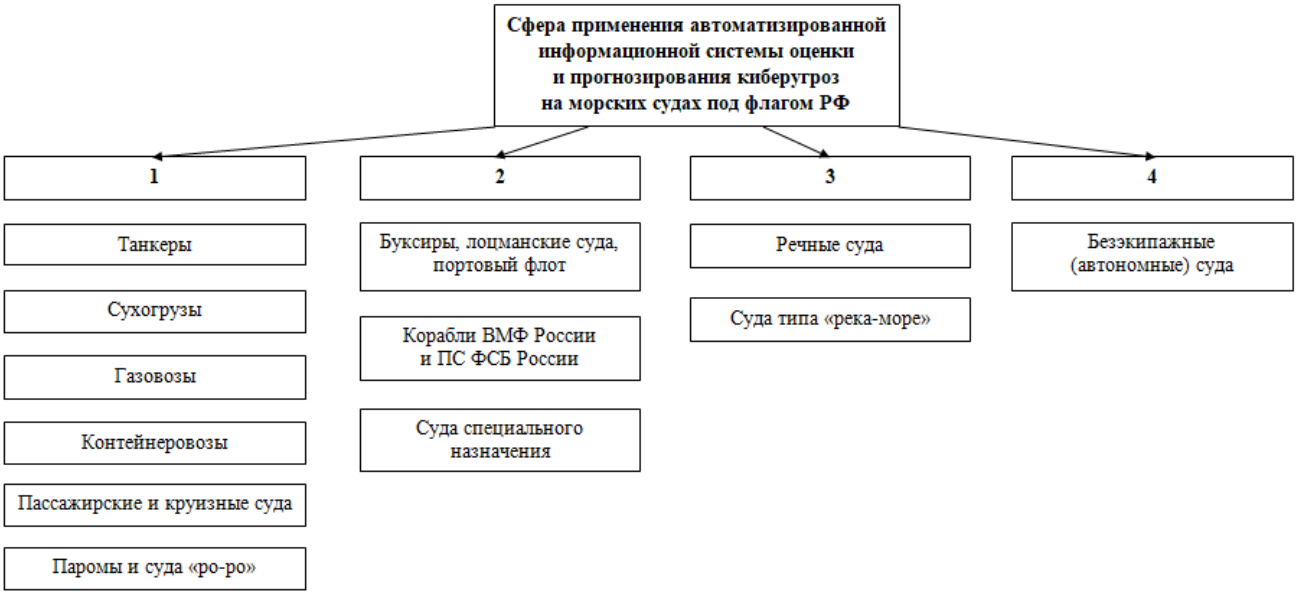


Рис. 3. Сфера применения автоматизированной ИС ОиПК.

Сфера применения автоматизированной ИС ОиПК представлена разделённой на четыре подгруппы в зависимости от типов (классов) судов, их назначения и особенностей:

1 группа включает в себя морские суда различных типов (классов);

2 группа включает в себя суда, выполняющие различные специализированные задачи;

3 группа включает в себя речные суда и суда типа «река-море»;

4 группа включает в себя безэкипажные (автономные) суда.

Автоматизированная ИС ОиПК должна предусматривать возможность расширения и сужения сферы её возможного применения в зависимости от поставленных перед ней целей и оперативных задач.

Создание и эксплуатация автоматизированной ИС ОиПК может способствовать решению ряда конкретных проблем в области морской кибербезопасности в РФ, таких как:

отсутствие в России транспортного отраслевого центра компетенции по информационной безопасности, в сферу деятельности которого входила бы организация работ по обеспечению кибербезопасности судов под флагом РФ [7];

разработка ФСТЭК России требований в области информационной безопасности без учёта отраслевых особенностей, в частности в сфере водного транспорта [8];

База данных угроз безопасности информации ФСТЭК России не отражает отраслевые особенности, что делает сложным процесс оценки актуальности киберугроз для морских судов и прогнозирования их реализации [9];

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА) на данный момент имеет незначительное количество подключений субъектов критической информационной инфраструктуры (КИИ) в области морского транспорта [10, 11], имеется проблематика в вопросе необходимости и организации категорирования в качестве субъектов КИИ морских судов;

отсутствие в России аналогичных систем по видам транспорта, в том числе, направленных на обеспечение кибербезопасности водного транспорта.

Исходя из назначения, задач, сферы возможного применения, автоматизированной ИС ОиПК и проблематики в области морской кибербезопасности в РФ, можно выделить перечень внешних систем и служб, взаимодействие с которыми может потребоваться для выполнения возложенных на автоматизированную ИС ОиПК задач. Такими внешними системами и службами могут быть:

- ФСБ России;
- ФСТЭК России;
- Минтранс России;
- РосМорРечФлот;
- ГосСОПКА;

– Служба управлением движения судов (СУДС).

На рис. 4 представлена возможная схема взаимодействия автоматизированной ИС ОиПК с внешними системами и службами.

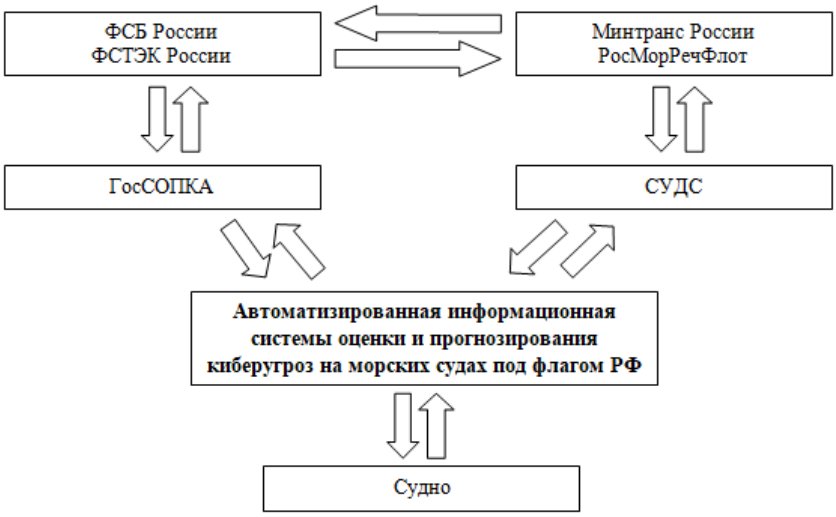


Рис. 4. Схема взаимодействия автоматизированной ИС ОиПК с внешними системами и службами.

Схема отображает возможный процесс обмена и передачи оперативной и служебной информации между автоматизированной ИС ОиПК, судами, системами и службами, взаимодействие с которыми может потребоваться для выполнения возложенных на автоматизированную ИС ОиПК задач.

Заключение. Таким образом, совокупность широкого круга поставленных перед автоматизированной ИС ОиПК задач, наличие определённых целей, достижение которых ожидается от её эксплуатации, а также возможность решения ряда конкретных проблем в области морской кибербезопасности в РФ, позволяют считать создание автоматизированной ИС ОиПК потенциально эффективным решением по обеспечению и повышению уровня кибербезопасности морских судов в России.

СПИСОК ЛИТЕРАТУРЫ

1. Training crucial as maritime cyber-attacks attempts surge // [Электронный ресурс]. URL: https://www.rivieramm.com/news-content-hub/training-is-crucial-as-maritime-cyber-attack-attempts-surge-66008 (дата обращения: 15.06.2021).
2. Sokolov S. Countering Cyberattacks During Information Operations / S. Sokolov, A. Nyrkov, T. Knysh, A. Shvets // In: Mottaeva A. (eds) Proceedings of the XIII International Scientific Conference on Architecture and Construction 2020. Lecture Notes in Civil Engineering, vol 130. Springer, Singapore. – 2021. – Pp. 84 - 100. https://doi.org/10.1007/978-981-33-6208-6_8
3. Zhilenkov, A.A. Intelligent autonomous navigation system for UAV in randomly changing environmental conditions / A. A. Zhilenkov, S. S. Sokolov, S. G. Chernyi, A. P. Nyrkov // Journal of Intelligent and Fuzzy Systems, Vol. 38, No. 5. – 2020. – Pp. 6619 - 6625. https://doi.org/10.3233/JIFS-179741
4. Kardakova M. Cyber Security on Sea Transport / M. Kardakova, I. Shipunov, A. Nyrkov, T. Knysh // Advances in Intelligent Systems and Computing, Vol. 982. – 2020. – Pp. 481 - 490. https://doi.org/10.1007/978-3-030-19756-8_46
5. Shipunov I.S. Information System for Monitoring and Analyzing the Technical Condition of Autonomous Vehicles / I. S. Shipunov, A. P. Nyrkov, M. V. Kardakova, Y. F. Katorin, V. V. Vychuzhanin // Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). – 2020. – Pp. 497 - 500. https://doi.org/10.1109/EIConRus49466.2020.9039181
6. Shipunov, I.S. About the Problems of Ensuring Information Security on Unmanned Ships / I. S. Shipunov, K. S. Voevodskiy, A. P. Nyrkov, Y. F. Katorin, Y. A. Gatchin // Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). – 2019. – Pp. 339 - 343. https://doi.org/10.1109/EIConRus.2019.8657219
7. Когтев А.В. Проблемы создания единой отраслевой политики по кибербезопасности в сфере морского транспорта // Сборник трудов. Выпуск 9 / СПОИСУ. – СПб., 2020. – С. 95-96.
8. Семенов С.А. Морская кибербезопасность: оценка состояния и пути решения // Морские вести. 2020. № 1 [Электронный ресурс]. URL: http://www.morvesti.ru/analitika/1692/82776/ (дата обращения: 17.06.2021).
9. Nyrkov, A.P. Databases Problems for Maritime Transport Industry on Platform Highload / A. P. Nyrkov, N. B. Glebov, R. O. Novoselov, O. M. Alimov, S. G. Chernyi // Proceedings of the 2018 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies», IT and QM and IS 5 November 2018, 2018. – Pp. 132-135 https://doi.org/10.1109/ITMQIS.2018.8525058
10. Кириков А.В. Информационная безопасность на объектах транспортной инфраструктуры / А. В. Кириков, А. П. Нырков, С. С. Соколов, В. Д. Гаскаров // Материалы межвузовской научно-практической конференции «Современные тенденции и перспективы развития водного транспорта России» 01 октября 2020 года: Часть 3. – СПб. : Изд-во ГУМРФ им. адм. С. О. Макарова, 2020. – С. 67–69.
11. Нырков А.П. К вопросу о категорировании объектов критической информационной инфраструктуры водного транспорта / А. П. Нырков, Р. И. Кислов, А. В. Белов // Материалы конференции «XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ-2018)». Санкт-Петербург, 24-26 октября 2018. - СПб.: СПОИСУ, 2018. – С. 316–318.

УДК 519.876.5

РАЗРАБОТКА ИМИТАЦИОННОЙ МОДЕЛИ МНОГОКОМПОНЕНТНОЙ ТЕХНИЧЕСКОЙ СИСТЕМЫ С ОПРЕДЕЛЕННЫМИ ПАРАМЕТРАМИ

Цымай Юлия Валериевна, Кардакова Мария Владимировна, Железнов Эдуард Геннадьевич, Комиссаров Петр Вениаминович

Государственный университет морского и речного флота имени адмирала С.О. Макарова»
ул. Двинская, 5/7, Санкт-Петербург, 198035, Россия
e-mails: m-walua@yandex.ru, m.v.kardakova@ya.ru, eduardz76@mail.ru, komissarovp@yandex.ru

Аннотация. Рассматриваются алгоритмы и логика включения компонентов, обычно используемые в аппаратных стендах для тестирования систем жёсткого реального времени. Имитационная модель рассматривается как виртуальная машина, использующая программные и аппаратные ресурсы компьютера. Виртуальные порты ввода-вывода обеспечивают имитацию подключения внешних компонентов с заданными характеристиками. Объект управления моделируется в виде управляющего сигнала с заданным алгоритмом включения. Для реализации имитационной модели многокомпонентной технической системы с определенными параметрами использован минимальный набор компонентов, соединенных с управляющим контроллером. Функционал модели ограничен во избежание появления неопределенных параметров. Основной задачей проектируемой информационной модели является имитация процесса тестирования последовательностей срабатывания сигналов на программном уровне.

Ключевые слова: имитационное моделирование; многокомпонентная техническая система; управляющий контроллер; определенные параметры; алгоритм включения.

DEVELOPMENT OF A SIMULATION MODEL OF A MULTICOMPONENT TECHNICAL SYSTEM WITH CERTAIN PARAMETERS

Tsymay Yulia, Kardakova Mariia, Zheleznov Eduard, Komissarov Pyotr

Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya street, Saint-Petersburg, 198035, Russia
e-mails: m-walua@yandex.ru, m.v.kardakova@ya.ru, eduardz76@mail.ru, komissarovp@yandex.ru

Annotation. The algorithms and logic of switching on components commonly used in hardware stands for testing hard real-time systems are considered. The simulation model is considered as a virtual machine using computer software and hardware resources. Virtual I/O ports provide simulated connection of external components with specified characteristics. The control object is modeled as a control signal with a specified activation algorithm. To implement a simulation model of a multicomponent technical system with certain parameters, a minimum set of components connected to a control controller was used. The functionality of the model is limited in order to avoid the appearance of undefined parameters. The main task of the designed information model is to simulate the process of testing sequences of triggering signals at the software level.

Keywords: simulation modeling; multicomponent technical system; controller; certain parameters; inclusion algorithm.

Введение. При проектировании и эксплуатации систем управления транспортировкой грузов используются заранее определенные параметры для воспроизведения предусмотренных алгоритмов срабатывания. От степени точности исходных данных зависят коэффициенты накопления ошибок, погрешностей и отказов в системе. Для получения высокоточных исходных данных для безотказного функционирования систем необходим предварительный анализ, который позволит создать модель, описывающую зависимость между предполагаемыми исходными данными и наиболее вероятными алгоритмами срабатывания. Такой анализ можно выполнить на базе имитационной модели многокомпонентной системы с определенными параметрами.

В основе идеи проекта использованы алгоритмы и логика включения компонентов, обычно используемые в аппаратных стендах для тестирования систем жёсткого реального времени [1]. Имитационная модель может рассматриваться как виртуальная машина, использующая программные и аппаратные ресурсы компьютера. Виртуальные порты ввода-вывода обеспечивают имитацию подключения внешних компонентов с заданными характеристиками. Объект управления моделируется в виде управляющего сигнала с заданным алгоритмом включения. Внешняя и внутренняя конфигурации подбираются для каждого моделируемого процесса в зависимости от конкретной задачи. Параметрами внешней конфигурации являются количество и тип интерфейсов для подключения оборудования. Внутренняя конфигурация описывается параметром производительности.

Для реализации имитационной модели многокомпонентной технической системы с определенными параметрами использован минимальный набор компонентов, соединенных с управляющим контроллером. Функционал модели ограничен во избежание появления неопределенных параметров. Основной задачей проектируемой информационной модели является имитация процесса тестирования последовательностей срабатывания сигналов на программном уровне. Также данную модель можно использовать для разработки, отладки

и тестирования программного обеспечения для управляющих систем реального времени. Технические требования, предъявляемые к имитационной модели, представлены в таблице 1. Структурная схема модели показана на рис. 1.

Таблица 1

Технические требования, предъявляемые к модели многокомпонентной технической системы с определенными параметрами [2-8]

№ пп	Параметры	
1	Объем управляющей программы	до 8 Кбайт
2	Напряжение питания	4.5÷5.5 В
3	Частота кварцевого резонатора	3.5÷4.5 МГц
4	Сопротивление резистора	1.9÷2.1 КОм
5	Емкость конденсатора	20÷25 пФ
6	Управляющее устройство	микроконтроллер серии Atmega

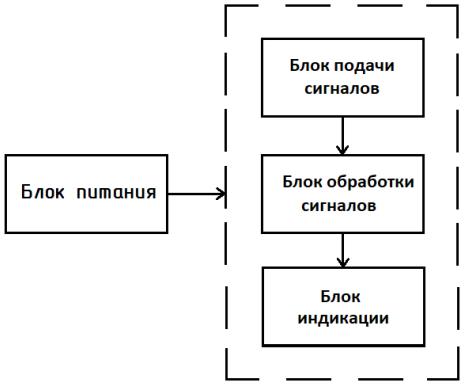


Рис. 1. Структурная схема модели многокомпонентной системы с определенными параметрами

Схема электрическая принципиальная, отражающая содержание аппаратной части, транслируемой в виртуальную имитационную модель, представлена на рис.2

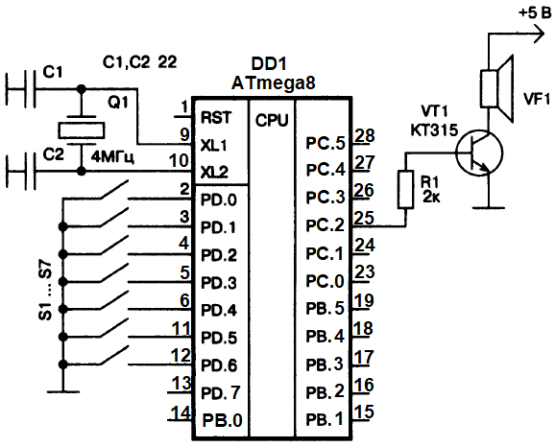


Рис.2. Схема электрическая принципиальная аппаратной составляющей имитационной модели

В качестве управляющего устройства рассматривается контроллер ATmega 8 [2] со следующими техническими характеристиками:

- ширина шины данных: 8 бит;
- тактовая частота: 16 МГц;
- количество входов/выходов: 23;
- объем памяти программ: 8 КБ (4k x 16);
- напряжение питания: 4.5…5.5 В;
- рабочая температура: -20°C…+85°C.

Входной тестовый сигнал формируется с помощью кнопки B3F-1000 [3]. Ее параметры приведены ниже:

- рабочее напряжение: 24 В;

– предельное напряжение: 250 В;
– рабочий ток: 0,05 А;
– рабочая температура: -25°С…+70°С.

Для задания определенного значения силы тока и напряжения в электрической цепи используется резистор [4] со следующими параметрами:

– сопротивление: 1 кОм;
– мощность: 0.25Вт;
– температурный коэффициент: ±350ppm/°С;
– допустимые отклонения емкости: ±5%.

Для усиления сигнала используется биполярный кремниевый высокочастотный транзистор [5] типа N-P-N, средней мощности в диапазоне от 300 мВт до 1,5 Вт. Для стабилизации частоты колебаний используется кварцевый резонатор с резонансной частотой 4 МГц. Так же в модели используется конденсатор 22 пФх50В и пьезоизлучатель с частотой 2,3 КГц, номинальным напряжением 5 В и номинальным током 30 мА. [6-8]

Описанные выше характеристики компонентов электрической схемы формируют набор параметров технической системы, являющихся исходными данными для математического анализа динамической системы с определенными параметрами.

Алгоритм функционирования имитационной модели заключается в следующем:

1. Формируется проектный файл с указанием параметров аппаратной части модели.
2. Определяется число периферийных компонентов системы для формирования входных сигналов. В соответствии со структурной схемой это может быть число управляющих кнопок или количество управляющих сигналов, инициируемых одной кнопкой и идентифицируемых очередью нажатия.
3. Определяется число периферийных компонентов системы для отображения выходных сигналов. Это может быть заданное количество светодиодных или звуковых индикаторов, или, в случае одного выходного индикатора, заданные характеристики выходного сигнала, отличающиеся таймингом включения/выключения.
4. Модель переключается в режим ожидания.
5. При активации одного из тестируемых входных сигналов запускается соответствующая подпрограмма обработки. Результат работы подпрограммы транслируется через виртуальный порт вывода.
6. Встроенный код, имитирующий работу измерительных устройств, позволяет определить задержку сигнала, текущий уровень напряжения, скорость передачи сигнала при использовании цифровых и аналоговых преобразований.
7. Цикл тестирования можно выполнять до тех пор, пока не поступит команда STOP от пользователя.

```
; *****************************************************************
; PROJECT:
; AUTHOR:
; *****************************************************************

; Micro + software running
; ---------------------------------------------------------
.MICRO "ATmega8"
.PROGRAM "ttr.asm"
.TARGET "ttr.hex"

.TRACE              ; Activate micro trace

; Following lines are optional; if not included
; exactly these values are taken by default
; ---------------------------------------------------------
.POWER VDD=5 VSS=0  ; Power nodes
.CLOCK 1meg         ; Micro clock
.STORE 250m         ; Trace (micro+signals) storage time

; Micro nodes: RESET, AREF, PB0-PB7, PC0-PC6, PD0-PD7, ACO, TIM1OVF, ADC6, ADC7
; Define here the hardware around the micro
; ---------------------------------------------------------
K0 VSS PD0
K1 VSS PD1
K2 VSS PD2
K3 VSS PD3
K4 VSS PD4
K5 VSS PD5
K6 VSS PD6
D1 VDD PC2
;----------------------------------------------------------
.PLOT v(PD0) v(PD1) v(PD2) v(PD3) v(PD4) v(PD5) v(PD6) v(PC2)
-
```

Рис.3. Проектный файл имитационной модели системы с определенными параметрами.

Программная модель реализована на языке Assembler (файл с расширением *.asm). Проектный файл формируется с расширением *.hex.

В пределах одной симуляции можно работать со светодиодами или звуковыми излучателями, использовать подпрограмму осциллографа для определения параметров выходного сигнала, программно моделировать изменение температуру окружающей среды в пределах изначально определенного диапазона температур, частоту кристалла, и в режиме реального времени наблюдать за изменением тока потребления, содержания виртуальной регистровой и постоянной памяти. В соответствии с получаемыми данными можно определить скорость передачи сигналов в имитационной модели и параметры задержек. На рис.3 представлен проектный файл, описывающий аппаратные характеристики тестируемой системы с определенными параметрами.

Данная модель описывает подключение периферийных устройств (управляющих кнопок) к портам контроллера PD0-PD6. Светодиодный или звуковой индикатор подключен к порту вывода PC2. После указания исходной информации об аппаратной части моделируемой системы происходит компиляция кода. Процесс тестирования предполагает последовательное исполнение рабочих алгоритмов.

В блоке обработки выполняется математический анализ поступающей информации. Имитационная модель имеет гибкую структуру и может быть адаптирована под любой математический аппарат. [9]

Используя метод расчета, описанный в [10], проверяется верность выбранного баланса параметров системы по формуле (1).

$$N = n^{p*n} \prod_{i=0}^{n-1} (q^p - i), \quad (1)$$

где N - множество конечных событий в системе, p - входные параметры системы, n - состояния системы, q - выходные параметры системы.

В случае выполнения условия $N > 0$ активируется заданный алгоритм анализа данных. В рассматриваемой модели значение N определяется двадцати пяти разрядным числом, что соответствует условию и позволяет предположить существование множества состояний в каждый момент времени работы изучаемой системы.

В соответствии с имеющимися параметрами имитационная модель многокомпонентной технической системы позволяет реализовать алгоритм маршрутизации [11], который даст представление о степени нагруженности в различные моменты времени, определит критические точки и наиболее вероятностные точки накопления ошибок и погрешностей [12]. На рис. 4 приведены результирующие параметры работы имитационной модели.

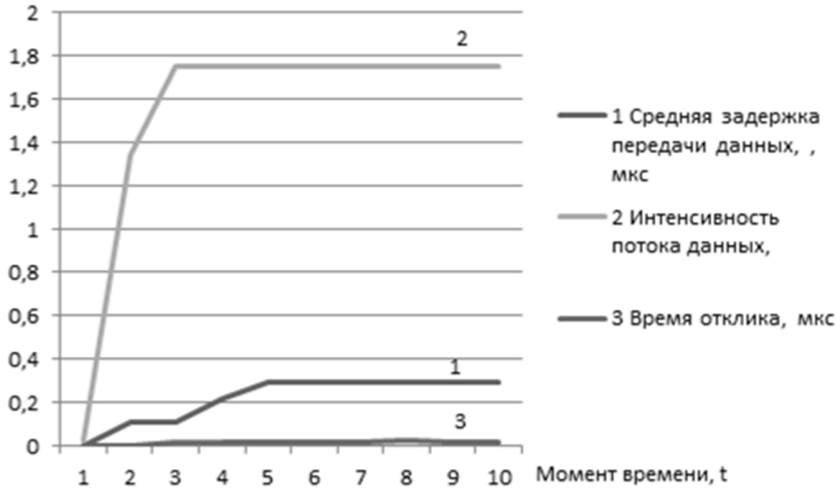


Рис. 4. Результирующие параметры работы имитационной модели многокомпонентной технической системы

Результаты анализа имитационной модели показывают, что исходных данных достаточно для получения характеристик системы. Система функционирует равномерно практически во всех контрольных точках, за исключением момента времени, описывающего старт модели. Это объясняется тем, что происходит адаптация программных настроек к аппаратным характеристикам персонального компьютера. Интенсивность потока при работе системы колеблется в допустимых приделах. Для одного такта при максимальной частоте управляющего устройства необходимо 0,125 мкс [13]. Время для поступления и обработки информации можно принять как константу.

Заключение. Исходные и конечные параметры модели предсказуемы благодаря минимальной наполняемости аппаратной части и гибкой логике управляющего контроллера. Ограниченный диапазон задач в дальнейшем позволит скорректировать исходные данные в соответствии с возникающими систематическими погрешностями результатов экспериментов данных, определить логико-алгоритмическое описание поведения отдельных элементов системы и правил их взаимодействия.

Имитационная модель может быть использована для описания, анализа и предварительного тестирования контроллерных систем различного уровня сложности. Программа позволяет произвести первичный анализ полноты выбора исходных данных, расчет нагруженности системы и относительного уровня ее сложности, расчет максимально возможной интенсивности потока данных, среднюю задержку передачи данных, ресурс общей пропускной способности.

СПИСОК ЛИТЕРАТУРЫ

1. Зубанова А.А., Шипунов И.С., Ныркov А.П. «О возможностях применения программируемых логических контроллеров для целей мониторинга состояния судового оборудования» // Материалы конференции «Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября 2020 г.: Материалы конференции. Часть 1. – СПб, СПОИСУ, 2020. – С. 345–348.
2. Характеристики микроконтроллера Atmega8 [Электронный ресурс] URL: https://www.chipdip.ru/
3. Характеристики кнопки B3F-1000 [Электронный ресурс] URL: https://www.compel.ru/
4. Характеристики резистора [Электронный ресурс] URL: https://spb.tiu.ru/
5. Характеристики транзистора [Электронный ресурс] URL: https://www.radiolibrary.ru/
6. Характеристики кварцевого резонатора [Электронный ресурс] URL: https://www.platan.ru/
7. Характеристики конденсатора [Электронный ресурс] URL: https://www.chipdip.ru/
8. Характеристики пьезоизлучателя [Электронный ресурс] URL: https://ru.mouser.com/
9. Nyrkov A., Kardakova M., Kolesnichenko S., Tsymay Y., Goloskokov P. Modeling the operating range of the fire safety system response parameters on board// Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). 2020. C 434-437
10. Ныркov А.П., Дмитриева Т.В. Математическая модель резервирующей системы и оптимизация ее работы // Журнал университета водных коммуникаций. – № 2, 2011. – С. 98 – 101.
11. Ныркov А.П., Соколов С.С., Белоусов А.С. Мультисервисная сеть транспортной отрасли // «Вестник компьютерных и информационных технологий». – № 4, 2014. – С. 33 – 38. https://doi.org/10.14489/vkit.2014.04.pp.033-038
12. Цымай Ю.В. Моделирование передачи управляющего сигнала при транспортировке объекта // Сборник научных статей национальной научно-практической конференции профессорско-преподавательского состава ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова» Сборник статей конференции. 2019. С. 238-241.
13. Афанасьева Т. В. Разработка подхода к построению информационной модели управления / Т. В. Афанасьева, М. Ш. Муртазина // Инновационные кластеры цифровой экономики: теория и практика : монография. - Санкт-Петербург : Изд-во Политехн. ун-та, 2018. – Гл. 5.6. - С. 602-625. - 500 экз. - ISBN 978-5-7422-6290-9. - DOI: 10.18720/IEP/2018.4/26.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ

УДК 004.67

СЛУЧАЙНЫЕ ДАТЧИКИ НОМЕРА ЗАДАНИЯ И НОМЕРА ИСПОЛНИТЕЛЯ КАК СРЕДСТВА ИНФОРМАЦИОННОЙ ЗАЩИТЫ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ

Большакова Людмила Валентиновна, Сибаров Константин Дмитриевич, Яковлева Наталья Александровна
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: l.v.bolshakova@mail.ru, konstantin_siba@mail.ru, kumirova@mail.ru

Аннотация. В статье рассматриваются случайные датчики номера задания и номера исполнителя (для электронных таблиц Excel), которые могут найти разнообразные применения при принятии управленческих решений, связанных с выбором из нескольких возможных вариантов, на примере проверки знаний при обучении: выбора номера вопроса в списке вопросов при сдаче зачёта и выбора номера, отвечающего в списке группы при сплошном опросе.

Ключевые слова: случайный датчик; электронные таблицы Excel; управленческое решение; случайный выбор; выбор в списке; электронный экзаменационный лист; информационная безопасность.

RANDOM SENSORS OF THE TASK NUMBER AND THE PERFORMER'S NUMBER AS MEANS OF INFORMATION PROTECTION OF MANAGEMENT DECISIONS

Bolshakova Lyudmila, Sibarov Konstantin, Yakovleva Natalia
St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: l.v.bolshakova@mail.ru, konstantin_siba@mail.ru, kumirova@mail.ru

Abstract. The article considers random sensors of the task number and the performer's number (for Excel spreadsheets), which can find various applications in making managerial decisions related to choosing from several possible options, using the example of knowledge testing during training: choosing the question number in the list of questions when passing the test and choosing the number of answering person in the list of groupe during a total survey.

Keywords: random sensor; Excel spreadsheets; management decision; random selection; selection in the list; electronic examination sheet; information security.

Введение. Предлагаемые случайные датчики номера задания и номера исполнителя могут найти разнообразные применения при принятии управленческих решений, связанных с выбором из нескольких возможных вариантов. Наиболее распространённым и понятным их приложением является проверка знаний при обучении: выбор номера вопроса в списке вопросов при сдаче зачёта и выбор номера, отвечающего в списке группы при сплошном опросе. Прилюдный вызов такого датчика, во-первых, даёт всем уверенность в непредвзятости выбора со стороны преподавателя, во-вторых, на зачёте исключает возможность вытаскивания двух билетов с передачей одного из них следующему, вызываемому для подготовки тем ответа на заведомо известный вопрос. Следовательно, применение такого датчика является своего рода информационной защитой как управленческого решения по выбору, так и качества выборочной проверки знаний.

Для того, чтобы уверенность в достоинствах применения случайного датчика была полной, перед его использованием присутствующим должен быть объявлен источник случайного значения, показана работа случайного датчика и обращено внимание на полное соответствие порождаемых случайных значений требованиям к такому датчику.

Работа с исходными данными выполняется в электронных таблицах Excel с использованием встроенных датчиков случайных чисел. Устройство датчиков основывается на схожих приёмах, поэтому начнём с более простого датчика выбора номера задания. Объяснение будем вести на примере проверки знаний.

Датчик номера задания. Пусть имеется группа обучающихся, которым предстоит сдать зачёт по дисциплине. На зачёт вынесен нумерованный список вопросов. После выбора очередного вопроса, его номер записывается и в дальнейшем выборе не участвует. Выбор оставшихся номеров должен быть всегда равновероятным.

Встроенный случайный датчик Excel СЛУЧМЕЖДУ, равномерно выдающий случайные целые числа из заданного промежутка, не подходит, т.к. он не позволяет автоматически исключать уже выпадавшие номера. В Excel есть ещё встроенный датчик СЛЧИС [1], но он выдаёт вещественное случайное число равномерно в промежутке от 0 до 1. Однако если умножить значение этого датчика на какое-то значение, например, 10, то итогом будет вещественное случайное число в промежутке от 0 до 10. Теперь надо от вещественного числа как-то перейти к целому с исключением уже выпадавших номеров. Ниже рассматривается способ учёта ранее выпадавших номеров в списке из 10 вопросов.

Выполняется разбивка промежутка от 0 до 10 числовой оси на отрезки единичной длины – по количеству вопросов, изначально участвующих в выборе, рис.1. Номер отрезка – номер вопроса.

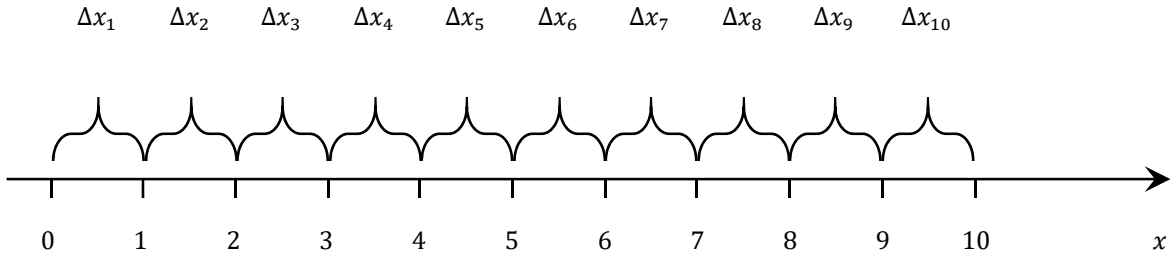


Рис. 1. Разбиение промежутка от 0 до 10 числовой оси на отрезки по числу вопросов.

Запускается датчик СЛЧИС с множителем 10, и определяется, в какой из отрезков попало его значение. Предположим, вещественное значение попало в отрезок от 3 до 4 – значит, выпал вопрос № 4. Учёт выбора вопроса производится сжатием длины отрезка 4 до нуля, рис.2.

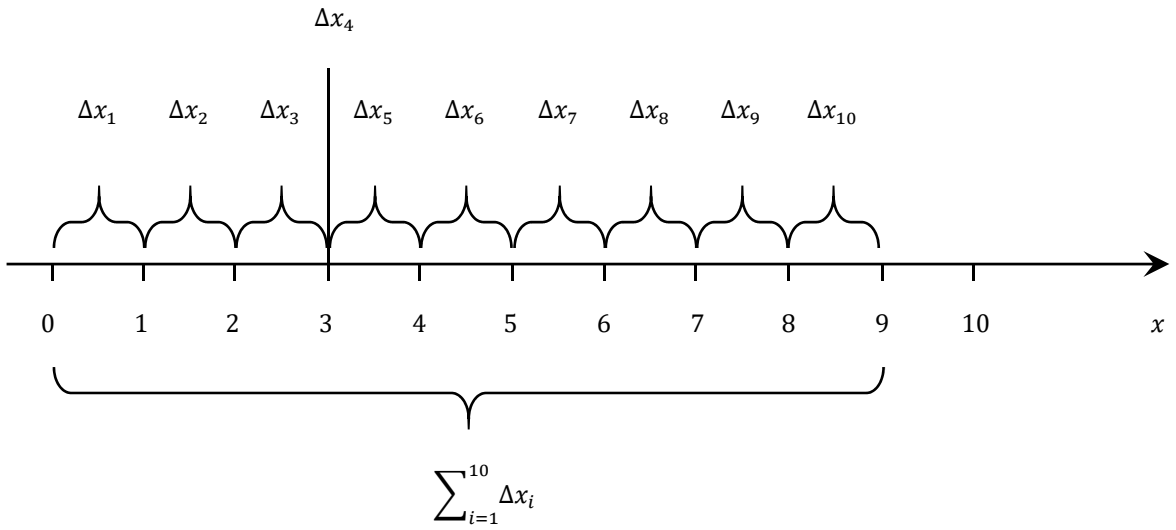


Рис. 2. Сжатие до нуля длины отрезка выпавшего вопроса № 4.

Перед следующим обращением к случайному датчику множитель при СЛЧИС уменьшается на единицу. При этом случайное число будет порождаться в промежутке от 0 до 9, рис.2. Вероятность, что случайное число попадёт в отрезок 4 с нулевой длиной, равна нулю, следовательно, вопрос 4 больше не будет выдан.

Сколько вопросов было выбрано, длина стольких отрезков и должна быть сокращена до нуля. И номера соответствующих вопросов будут изъяты из исходного перечисления по порядку.

Воплощение этого способа в электронных таблицах Excel рассмотрим по рис.3. В списке из 10 вопросов уже выбраны вопросы №№ 4, 7 и 8. Для возможности пометки номеров выпавших вопросов, введён отдельный столбик «Участие» В нём напротив использованных номеров исходные «1» заменены на «0».

	A	B	C	D	E	F	G
1	6. Информационные процессы и их виды						
2							
3	№ вопроса	Участие	Нарастающим итогом	4,4645		№ вопроса	Содержание вопроса
4	1	1	1	0		1	Общенаучное определение информации
5	2	1	2	0		2	Информатика. Информация в информатике и теории инфор
6	3	1	3	0		3	Единицы измерения информации
7	4	0	3	0		4	Понятие информационной технологии
8	5	1	4	0		5	Понятие и состав информационной системы
9	6	1	5	6		6	Информационные процессы и их виды
10	7	0	5	0		7	Знаковое представление информации
11	8	0	5	0		8	Аналоговое и цифровое представление информации
12	9	1	6	0		9	Кодирование информации
13	10	1	7	0		10	Кодирование чисел. Системы счисления
14			7	6			
15							

Рис. 3. Вид электронной таблицы случайного выбора номера вопроса с исключением уже выпадавших номеров 4, 7 и 8.

Правее этого столбика ведётся суммирование значений «Участие» нарастающим итогом. Например, в строке второго вопроса стоит формула: =СУММ(C4;B5).

Столбик «Нарастающим итогом» представляет собой значения верхних границ соответствующих отрезков. Видно, что, например, у отрезка 4 верхняя граница такая же, как у предыдущего отрезка 3, следовательно, его длина равна 0.

В заголовке четвёртого столбика находится формула: =СЛЧИС()*C14. В ячейке C14 выводится последнее значение суммирования с нарастающим итогом: =C13.

В четвёртом столбике проверяется попадание случайного значения в ячейке D4 в пределы между верхней и нижней границами каждого отрезка (для первого отрезка нижняя граница – 0). Если выявлено попадание, то выводится номер из первого столбика «№ вопроса», если нет, то 0. Так в строке первого вопроса стоит формула: =ЕСЛИ(И($D$3>=0;$D$3<C4);A4;0). В строке второго вопроса: =ЕСЛИ(И($D$3>=C4;$D$3<C5);A5;0).

Внизу четвёртого столбика вычисляется сумма всех его значений: =СУММ(D4:D13). Она будет равна единственному значению в столбике, отличному от 0. Это и есть искомый номер вопроса.

В соответствии с порождённым номером в ячейке A1 выводится содержание вопроса с помощью формулы, соединяющей подстроки: =D14&». «&ВПР(D14;F4:G13;2;0). ВПР – вертикальный просмотр – встроенная функция Excel [2].

Желаемая цель достигнута: после простановки 0 в столбике «Участие» в строке соответствующего вопроса больше он выпадать не будет. Однако в действительности на зачёте учёт выпавших вопросов ведётся не по списку вопросов, а по списку обучающихся. Предположим, таковых пять человек, рис.4.

	A	B	C	D
16				
17	№ п/п	Фамилия	№ вопроса	
18	1	Аистов	7	
19	2	Лунёв		
20	3	Орлов	8	
21	4	Уткин	4	
22	5	Чижов		
23				

Рис. 4. Список обучающихся с вписанными номерами выпавших вопросов.

Для автоматического заполнения столбика «Участие» сведениями о выпавших вопросах, например, для первого вопроса, в ячейке B4 используется следующая формула: =ЕНД(ВПР(A4;$C$18:$C$22;1;0))*1. Умножение на 1 – это способ перевода значений ИСТИНА или ЛОЖЬ встроенной функции ЕНД в числа 1 или 0. ЕНД – «если нет данных» [3] – функция выявления случая, когда с помощью функции ВПР – «вертикальный просмотр» – не найдено точное совпадение значения ячейки A4 в столбце 1 блока ячеек $C$18:$C$22.

Датчик номера исполнителя. Рассмотрим вторую задачу: случайный выбор отвечающего с учётом того, сколько раз и насколько давно он вызывался на предыдущих занятиях. Она решается с использованием приёмов, которые рассмотрены выше, но с некоторым развитием.

Допустимо ли вызывать человека на одном занятии второй раз? Как учесть вызовы обучающегося на предыдущих занятиях с учётом их временной отдалённости? Предлагается следующий подход.

Следует изначально задать для всех обучающихся степень участия в выдаче задания равной 1. Пусть в рассмотрение принимаются вызовы обучающегося на текущем и трёх предыдущих занятиях – не глубже. Чем дальше отстоит предыдущий вызов обучающегося, тем больше должна быть степень его участия на данном занятии, и наоборот, наименьшая степень участия должна оказаться у тех, кто уже на данном занятии отвечать был вызван.

Зададим снижение участия, если человек вызывался ранее, для позапозапрошлого занятия – в 2 раза, для позапрошлого – в 4, для прошлого – в 8, для текущего – в 16 раз. Значение 16 – это кратность снижения участия для повторного вызова на текущем занятии. Его можно заменить на другое по своему усмотрению. Обозначим эту ключевую величину как K.

Теперь надо учесть положение дел, когда обучающийся вызывался больше одного раза в пределах всех рассматриваемых четырёх занятий – для общности, на M занятиях. Предлагается следующее составное выражение для вычисления степени участия:

$$V_M = \frac{1}{D_{-(M-1)}(E_{-(M-1)})\cdot\ldots\cdot D_m(E_m)\cdot\ldots\cdot D_0(E_0)}, \quad (1)$$

где m – номер занятия; $m = -(M-1), -(M-2), \ldots, -1, 0$;

E_m – количество оценок, полученных на занятии номер m; $E_m = 0, 1, 2$ ...;

$D_m(E_m)$ – кратность снижения участия в текущем занятии с учётом оценок, полученных на занятии номер m.

Кратность снижения от того, сколько раз на рассматриваемом занятии вызывался человек, и от номера этого занятия можно выразить следующим образом:

$$D_m(E_m) = \begin{cases} 1, E_m = 0 \\ K^{(M+m+E_m-1)/M}, E_m = 1, 2, \ldots \end{cases}. \quad (2)$$

Например, позапозапрошлое занятие имеет номер $m = -3$ среди четырёх рассматриваемых, т.е. $M = 4$. Если обучающегося на нём не вызывали ни разу, т.е. $E_{-3} = 0$, то кратность снижения участия будет

$$D_{-3}(0) = 1\,. \quad (3)$$

Если вызывали один раз, т.е. $E_{-3} = 1$, то при $K = 16$:

$$D_{-3}(1) = 16^{(4+(-3)+1-1)/4} = 16^{1/4} = 2\,. \quad (4)$$

Если вызывали два раза, т.е. $E_{-3} = 2$, то при том же K:

$$D_{-3}(2) = 16^{(4+(-3)+2-1)/4} = 16^{2/4} = 4\,. \quad (5)$$

Подобным образом вычисляются все множители в знаменателе выражения для степени участия обучающегося в выдаче задания на занятии V_M.

Пример расчётов по вышеприведённым формулам – на рис. 5 в графе «Участие», исходя из оценок в столбцах C, D, E и F.

	A	B	C	D	E	F	G	H	I	J	K
1	6. Окунев							16	- кратность снижения		
2									для текущего занятия		
3	№ п/п	ФИО	Позапоза прошлое	Позапро шлое	Прошло е	Текуще е занятие		Участие	Вероят ность	Нараст ающим итогом	2,09
4	1	Голавлёв						1,0000	39,8%	1,000	0
5	2	Ершов	3					0,5000	19,9%	1,500	0
6	3	Карасёв		5				0,2500	9,9%	1,750	0
7	4	Карпов			5			0,1250	5,0%	1,875	0
8	5	Налимов				3		0,0625	2,5%	1,938	0
9	6	Окунев	33					0,2500	9,9%	2,188	6
10	7	Плотвин		54				0,1250	5,0%	2,313	0
11	8	Сомов			55			0,0625	2,5%	2,375	0
12	9	Судаков	3	3				0,1250	5,0%	2,500	0
13	10	Щукин	5	5	4			0,0156	0,6%	2,516	0
14								2,5156		2,516	6
15											

Рис. 5. Расчёт степени участия обучающегося в выдаче задания. Итог случайного выбора отвечающего.

Часть формулы в ячейке H4 для вычисления сомножителя $D_{-3}(E_{-3})$ в знаменателе следующая:

ЕСЛИ(ДЛСТР(C4)=0;1;$H$1^((4-3+ДЛСТР(C4)-1)/4))

В следующем столбике «Вероятность», исходя из суммы степеней участия всех обучающихся в ячейке H14, для наглядности вычислена вероятность вызова для каждого.

Поскольку цель разработки – выдача номера отвечающего, в столбике «Нарастающим итогом» вычислены верхние границы отрезков для каждого обучающегося – так же, как для случайной выдачи номера вопроса. Но в отличие от предыдущей задачи длины отрезков сокращаются не до нуля, как на рис.1 и рис.2, а до значений в столбике «Участие».

Под столбиком «Нарастающим итогом» в ячейку J14 вынесена полученная сумма. Она служит множителем для встроенного датчика СЛЧИС в ячейке K3. В столбике K обнаруживается попадание значения в ячейке K3 между границами каждого отрезка, и в этом случае выводится номер обучающегося, иначе 0 – всё как с определением номера вопроса. Внизу вычисляется сумма по столбику. Она даёт искомый номер обучающегося. Он вместе с фамилией вынесен в ячейку A1 с помощью формулы: =K14&». «&ВПР(K14;A4:B13;2;0).

Заключение. Захваты экранов, приведённые на рис.3, 4 и 5, отображают предельно упрощённые примеры, подготовленные намеренно для рассмотрения сути разработанных способов. В учебном процессе СПб Университета МВД России используются более развитые исполнения. Желающие могут скачать их по следующим ссылкам:

1) случайный выбор билета – https://disk.yandex.ru/i/WFhDcsJACdifSw

2) случайный выбор отвечающего – https://disk.yandex.ru/i/pIEbluARvGLeVA

Случайный датчик номера билета уже трижды успешно применялся нами на зачётах. В имеющемся исполнении допускается численность группы – до 30 человек, количество билетов – до 100. Пометка «зачёт» в этой своего рода электронной ведомости возникает автоматически при одновременных: положительной оценке ответа на выпавший вопрос, положительной оценке за прикладное задание, наличии конспекта с заданным количеством лекций и отсутствии хвостов.

Случайный датчик номера, отвечающего используется нами постоянно при сплошных опросах. Электронная таблица во время занятия постоянно высвечена на стене перед обучающимися. Наибольшим текущим спросом у них пользуются данные столбика «Вероятность». Но из него, в частности, следует, что только что ответивший может быть вызван на данном занятии повторно. Эта вероятность достаточно мала, но её ненулевое значение внутренне воспринимается ответившим как грозное предзнаменование, и расслабится не позволяет. Также добавлено условие, что при подстановке нечислового значения в столбик текущего занятия, например, «Б», т.е. обучающийся болен, степень его участия обнуляется.

Первоначально в ходе разработки датчика номера, отвечающего было испробовано исполнение для $M = 3$ и $K = 27$ (27 – как третья степень числа 3). Из двух возможностей выбора ключевой величины – 1) кратности снижения участия для повторного вызова на текущем занятии (K) и 2) кратности снижения участия по мере приближения предыдущего занятия, на котором вызывался обучающийся, к текущему – более легко воспринимаемой обучающимися оказалась величина K. Причём уже после первых нескольких применений датчика в учебном процессе для повышения вероятности повторного вызова на текущем занятии значение K при $M = 3$ было решено снизить до 20. Сочетание $M = 3$ и $K = 20$ также является вполне рабочим.

Смена значения встроенного датчика в электронных таблицах Excel производится нажатием клавиши F9. Для наглядности выполнения этого судьбоносного действия условились с обучающимися выполнять его с проговариванием счёта вслух до трёх с показным взмахом руки при нажатии F9 (во избежание недоразумений при повторе значения – вероятность повторения значений отлична от нуля). При сплошном опросе смены значений датчика выполняет преподаватель, объявив содержание очередного вопроса. На зачёте это делает сам сдающий своей рукой – для примирения с глубинной суеверностью, которая у большинства в этот волнующий миг оказывается сильнее уверенности в непредвзятости работы неодушевлённой электронно-вычислительной машины.

СПИСОК ЛИТЕРАТУРЫ

1. Функция СЛЧИС – Служба поддержки Office – Microsoft Support. URL: https://support.microsoft.com/ru-ru/office/функция-слчис-4cbfa695-8869-4788-8d90-021ea9f5be73 (Дата обращения – 20.07.2021).
2. Функция ВПР – Служба поддержки Office – Microsoft Support. URL: https://support.microsoft.com/ru-ru/office/функция-впр-0bbc8083-26fe-4963-8ab8-93a18ad188a1 (Дата обращения – 20.07.2021).
3. E (функции E) – Служба поддержки Office – Microsoft Support. URL: https://support.microsoft.com/ru-ru/office/e-функции-e-0f2d7971-6019-40a0-a171-f2d869135665 (Дата обращения – 20.07.2021).

УДК 004.588

ИНТЕРАКТИВНОЕ ИНТЕРНЕТ-ОБУЧЕНИЕ С ПРИМЕНЕНИЕМ ИНТЕРНЕТ-РЕСУРСОВ

Демакова Анастасия Ивановна
Российский государственный гидрометеорологический университет
Воронежская ул., 79, Санкт-Петербург, 192007, Россия
e-mail: dnimol@yandex.ru

Аннотация. Обсуждается проблема интерактивного обучения с применением интернет-ресурсов. При подготовке онлайн курса предлагается использовать концепцию кривой интереса, которая активно используется в индустрии видеоигр. Концепция направлена на поддержание внимания обучающихся к изучаемому материалу.

Ключевые слова: обучение; онлайн-курсы; интерактивное обучение; кривая интереса.

INTERACTIVE INTERNET LEARNING USING INTERNET RESOURCES

Demakova Anastasiia
Russian State Hydrometeorological University
79 Voronezhskya St, St. Petersburg, 192007, Russia
e-mail: dnimol@yandex.ru

Abstract. The problem of interactive learning using Internet resources is discussed. When preparing an online course, it is proposed to use the concept of an interest curve, which is actively used in the video game industry. The concept is aimed at maintaining the attention of students to the material being studied.

Keywords: training; online courses; interactive training; interest curve.

Без преподавателя и без правильной методики подачи материала изучить новую тему быстро и надежно тяжело. Преподаватель нужен, чтобы дать новую информацию быстро и понятно при помощи вызова интереса, увлекательной беседы, экспериментов и постановки контрольных вопросов. На этих принципах строятся методы интерактивного обучения, их использование помогает «оживить» учебный процесс. Ниже рассмотрим их.

Первая теория, доказанная экспериментально, это теория активного обучения. Ключевая мысль теории: люди запоминают больше, когда применяют новые знания на практике, а не просто слушают и конспектируют лекции. Другими словами: лучше делать, чем смотреть [1].

Есть теория антихрупкости – извлечь выгоду из неудач, но антихрупкость не равно НЕ ХРУПКИЙ. Смысл антихрупкости – это адаптирование к постоянно меняющемуся миру не путем его прогнозирования и предугадывания будущего, а путем увеличения диапазона ситуаций, с которыми мы готовы работать (хороший пример антихрупкости - эволюция) [2].

Концентрация внимания или теория потока – это настрой аудитории на особое эмоциональное состояние (поток), при котором задается ритм прохождения курса. Чтобы обучаемые вошли в поток, нужно нащупать баланс между их способностями и сложностью обучения. На рис. 1 можно отметить, что, если задача слишком сложная, это вызовет разочарование, а если слишком легкая – скуку. Но когда задание удерживает на верхней границе способностей, обучение становится увлекательным.

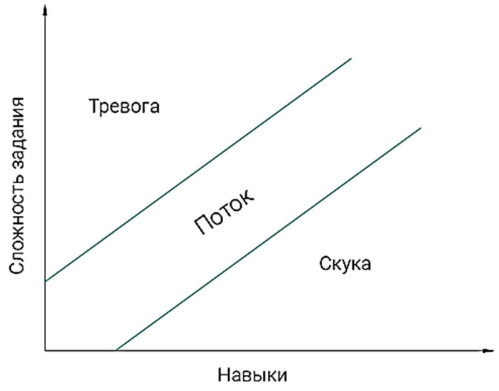


Рис. 1 Модель потока.

Подстроить обучение под каждого обучаемого в рамках электронного курса практически невозможно, но продуманный баланс между сложностью и навыками необходим. Самый простой пример того, как отыскать баланс между сложностью задания и навыками – создать несколько вариантов сценария курса (начальный, средний, высокий уровень сложности) и предложить учащимся самим выбрать подходящий или провести предварительное тестирование. По такому принципу устроено изучение иностранных языков. Человека, владеющим английским на уровне upper-intermediate, бессмысленно помещать в группу, где у всех только elementary.

Другая сложная задача, с которой интерактивное обучение помогает справиться, – снижающаяся продолжительность концентрации внимания человека. Согласно исследованиям, за пятнадцать лет она сократилась на 3,75 секунды и к 2015 году составила 8,25 секунд. Именно поэтому важно запланированно вставлять интерактивные элементы в курс.

Чтобы удержать внимание пользователей, в индустрии видеоигр используют концепцию кривой интереса. Кривая интереса – это график, на котором зафиксированы ключевые моменты игры. По графику можно с высокой точностью предсказать, когда игра начинает надоедать, и добавить на проблемный участок что-нибудь захватывающее. Об этом подробно рассказывает Джесси Шелл в книге «Искусство гейм-дизайна: книга линз». Хотя Шелл использовал кривую интереса для разработки игр, концепция подходит и для обучения.

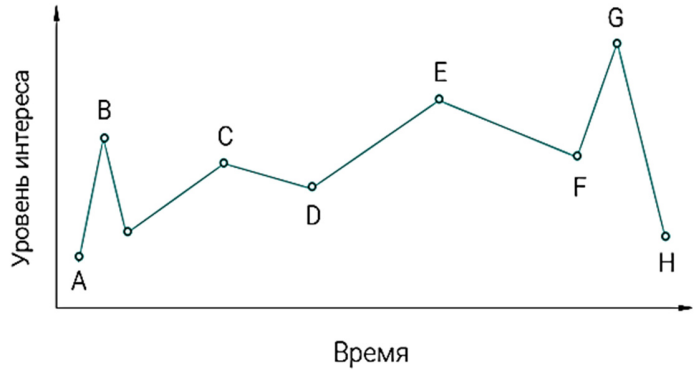


Рис. 2. Пример кривой интереса из книги «Искусство гейм-дизайна: книга линз».

При разработке интерактивного обучения важно уделить внимание четырем элементам кривой интереса (рис. 2):

Изначальный интерес (A). Для обучения гораздо эффективнее, когда обучающиеся сами в нем заинтересованы. Для этого используются вводные видеоролики, аннотации, примеры практического применения, чтобы сформировать позитивные ожидания от обучения.

Крючок (B). Заинтересованность до старта обучения – в самом начале курса нужно заинтересовать обучающихся, например, задачей, мини-игрой, обсуждением актуальной проблемы. Тогда сформируется запас интереса, который поможет удержать внимание во время менее увлекательных частей лекции.

Долина (D, F). Представляет собой тот запас интереса, который помогает удерживать внимание обучающихся.

Кульминация (G). Завершение занятия (лекции), где могут быть сделаны выводы, подведены итоги, переброшен «мостик» на следующее занятие.

Такой подход при планировании онлайн обучения позволит удерживать внимание обучающихся от начала до конца. Вместе с тем, существуют известные недостатки интерактивного обучения [3]:

1. Перегрузка активностью. Наличие разнообразного контента (аудио, видео, текст) при отсутствии собственной дисциплины со стороны обучающихся может стать проблемой для них. С этой целью на многих курсах существует тайм-менеджмент, стимулирующий обучающихся вовремя знакомиться с материалами курса.

2. Асинхронное обучение. Обучение происходит не одновременно, а каждый обучающийся осваивает программу обучения в собственном ритме. Хотя в последнее время этот недостаток стали относить к достоинствам!

3. Отсутствие самодисциплины, кураторства, помощи извне. Не все люди способны дисциплинировать себя, вести правильный тайм-менеджмент, многим нужен внешний контроль. Этот недостаток тоже в последнее время устраняется – многие курсы предлагают онлайн поддержку в режиме реального времени, предоставляют кураторов.

В настоящее время популярны онлайн институты IT-профессий, таких как разработчик ПО, веб-разработчик, веб-дизайнер, Data Science, тестировщик программного обеспечения, системный администратор, специалист по кибербезопасности – всему этому можно научиться онлайн на интерактивных платформах как Udemy.com, GeekBrains.ru, Skillbox.ru, Netology.ru.

СПИСОК ЛИТЕРАТУРЫ

1. Как создать интерактивный онлайн-курс. Теория и практика [Электронный ресурс] – URL: https://www.ispring.ru/elearning-insights/kak-sozdat-elektronnyiy-kurs-s-nulya/interaktivniy-kurs (Дата обращения: 03.06.2021).
2. Об антихрупкости. URL: https://www.notion.so/a82f608836b0445ba28bfdb24394741b (Дата обращения 03.06.2021)

3. Палкин И.И., Татарникова Т.М., Краева Е.В. Информационные технологии в дистанционном обучении. В сборнике: Информационные системы и технологии в моделировании и управлении. Сборник трудов V Международной научно-практической конференции. Отв. редактор К.А. Маковейчук. 2020. С. 427-431.

УДК 811.116.1

РОЛЬ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ СРЕДСТВ В ПРЕПОДАВАНИИ ФИЛОЛОГИЧЕСКИХ ДИСЦИПЛИН

Колоколова Лидия Петровна
Стерлитамакский филиал Башкирского государственного университета
Ленина пр., 49, Стерлитамак, 453100, Россия
e-mail: 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.

ROLE OF INFORMATION AND TECHNICAL TOOLS IN TEACHING PHILOLOGICAL DISCIPLINES

Kolokolova Lidia
Sterlitamak Branch of Bashkir state university
49 Lenin Av, Sterlitamak, 453100, 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.

«Новая реальность» информационных технологий стала в последние годы очевидной. Такой стремительно изменяющийся мир бросает вызов способности человека правильно в нем ориентироваться, принимать решения, использовать средства информационно-технической поддержки в сфере той или иной деятельности.

В российской системе образования наблюдается устойчивый интерес исследователей к привлечению информационно-коммуникативных технологий в преподавание дисциплин филологического направления. 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 [1].

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, 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 «Лингвостилистический анализ текста» ключевыми понятиями являются теоретические вопросы изучения языковой природы текста, где текст рассматривается как объект лингвистического анализа. Бесспорно, используя интерактивные технические средства, можно детально изучить экстралингвистические параметры текста, признаки жанрово-стилевой организации текста, продемонстрировать классификации и типологии текстов, а также студенты могут на занятии заниматься поисковой деятельностью, например, систематизировать и обобщить информацию, касающуюся истоков лингвистики текста и познакомиться с опытом интерпретации текста представителями разных школ и научных воззрений.

Технические средства найдут достойное применение при изучении фонетической системы современного русского языка. В частности, 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 языка. Например, артикуляционная характеристика системы вокализма предполагает следующие артикуляционные признаки:

1) характеристика гласных звуков по ударности/безударности;
2) характеристика гласных звуков по степени подъема языка при их образовании;
3) характеристика гласных звуков по месту подъема языка в ротовой полости;
4) характеристика гласных звуков по наличию/отсутствию лабиализации;
5) характеристика гласных звуков по долготе и краткости.

Таким образом, предложенная информация на занятиях по «Фонетике» современного русского языка будет способствовать образному, зрительному восприятию учебного материала.

При изучении лексической системы современного русского 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.

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 [2].

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 информационные и коммуникационные технологии (ИКТ) – 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 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.

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.

Также студенты и магистры 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», познакомиться с презентацией доклада М.В. Копотева «Синтаксическая разметка в ХАНКО: проблемы и достижения», посетить сайт, посвященный семинару по корпусной лингвистике в Институте лингвистических исследований РАН и т.д.

Важно подчеркнуть, что работа пользователей с корпусом осуществляется с помощью специализированных программных средств – корпусных менеджеров, предоставляющих разнообразные возможности по получению из корпуса необходимой информации: поиск конкретных словоформ; поиск словоформ по леммам; поиск группы словоформ в виде разрывной или неразрывной синтагмы; поиск словоформ по набору морфологических признаков; отображение информации о происхождении, типе текста и т.п.; вывод результатов поиска с указанием контекста заданной длины; получение различных лексико-грамматических статистических данных; сохранение отобранных строк конкорданса в отдельном файле на компьютере пользователя и др.

В рамках магистерской программы, направленность: «Филология в диалоге языков и культур» выделяется дисциплина «Менеджмент в системе филологического образования», где технические средства помогают реализовать профессиональную подготовку специалистов-филологов, используя проектную технологию, кейс-технологию и др.

Таким образом, рассмотрено содержание таких понятий, как компьютерное обучение; учебная деятельность, интерактивная доска; программное обеспечение в преподавании филологических дисциплин.

Совершенно очевидно, эффективность обучения может быть значительно повышена с помощью информационно-технических средств, применяемых в различных оптимальных для данных занятий сочетаниях с методическими средствами обучения.

СПИСОК ЛИТЕРАТУРЫ

1. Колоколова Л.П. Современный русский язык. Лексикология. Фразеология. Лексикография: Учебное пособие для филол. фак. вузов. – СПб: Политехника-сервис, 2012,147 с.
2. Современный русский литературный язык и методика его преподавания: Учебный словарь. – М.: ИПЦ «Маска», 2015, 383 с.

УДК 004

ВОПРОСЫ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ В ПОДГОТОВКЕ КАДРОВ

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 субъекты информационных отношений, вопросы информационного взаимодействия с учетом привлечения информационной этики, при этом подчеркивается, что профессиональная этика в современном обществе носит информационный оттенок.

Ключевые слова: информационные отношения; информационное взаимодействие; информационная этика; информационные технологии; информационная безопасность.

QUESTIONS OF INFORMATION RELATIONS IN PERSONNEL TRAINING

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. The article examines the subjects of information relations, the issues of information interaction, taking into account the involvement of information ethics, while emphasizing that professional ethics in modern society has an information connotation.

Keywords: information relations; information interaction; information ethics; information technology; information security.

Введение. Сегодня использование информационных технологий в обществе естественно порождает проблемы, связанные с информационной безопасностью личности, общества, и государства, что обусловлено все большей «прозрачностью» и уязвимостью различных сторон жизни и деятельности людей для внешнего воздействия. Социальные институты информационной безопасности, определяющие систему «правил игры» в обществе и активно формирующиеся в настоящее время, нацелены на решение этих проблем. Это правовые, этические (моральные), корпоративные и технические нормы [1]. Все они затрагивают глобальные вопросы становления информационного общества.

Субъекты информационных отношений. С точки зрения технических норм субъектами информационных отношений являются пользователь и информационная система, а регуляторами отношений являются правила пользования информационной системой. С точки зрения корпоративных норм субъектами информационных отношений являются администрация, потребитель и исполнитель, а регуляторами отношений являются устав, правила внутреннего распорядка организации, должностные инструкции и т.п. С точки зрения правовых норм субъектами информационных отношений являются государство, юридические лица и физические лица, а регуляторами отношений являются законы. С точки зрения этических норм субъектами информационных отношений являются государство, личность и общество, а регуляторами отношений являются общественное мнение, мораль [1].

Информационная этика. Особое значение здесь имеют этические нормы. Во-первых, по той причине, что саморегуляция на основе нравственных норм является одним из естественных и эффективных способов защиты от антисоциального поведения участников информационного взаимодействия. Во-вторых, в перспективе,

выработанные обществом нормы морали могут стать базой для формирования новых и совершенствования существующих правовых норм, обеспечиваемых силой государственного воздействия. Таким образом, обогатившись новым содержанием, адекватным новой реальности информационного общества, этические нормы могут стать настоящей гарантией обеспечения информационной безопасности личности и общества. Именно они определяют границы должного и возможного поведения.

Важность этого института информационной безопасности способствовала появлению отрасли знаний – «информационной этики». Этот термин стал употребляться учеными и специалистами по компьютерной этике и смежным дисциплинам с 2002 года. Информационная этика занимается изучением природы социального воздействия компьютерных технологий на общество, формулированием на этой основе моральных норм и проведением политики их внедрения в сознание разработчиков и пользователей компьютерных технологий. Информационная этика – обширная дисциплина, включающая в себя профессиональную этику, потребительскую этику и некоторые вопросы политики государства. Естественно, что первоначально она возникла как элемент профессиональных знаний и культуры в области информационных технологий.

На сегодняшний день до 90% всех технологий, влияющих на уровень профессиональной этики любой отрасли знаний, связаны с информацией, то есть с ее сбором, передачей, обработкой, способами хранения, техническими средствами и т.п. Это обстоятельство определяет повышенный уровень требований к специалистам – программистам, системным администраторам, и, конечно, к аналитикам, связанным с информационно-аналитическим обеспечением безопасности. Поэтому вопросы профессиональной этики в современном обществе носят информационный оттенок, причем эта тенденция будет сохраняться [1].

Кодекс компьютерной этики. Первый кодекс компьютерной этики был разработан и принят в Институте инженеров электроники и электротехники (IEEE) в 1979 г. Принятие кодекса было продиктовано пониманием того, что инженеры, учёные и технологи результатами своей деятельности определяют качество и условия жизни всех людей в информационном обществе. Поэтому в преамбуле кодекса подчёркивается жизненно важная необходимость соблюдения всех норм этики при разработке и эксплуатации средств информационных технологий. Позднее были разработаны и приняты кодексы этики Ассоциацией разработчиков компьютерных технологий (ACM), Ассоциацией пользователей информационных технологий в США (ITAA), Ассоциацией сертифицированных компьютерных профессионалов (ICCP). В 1987 г. был разработан и принят кодекс компьютерной этики для преподавателей высшей и средней школ. Эти кодексы послужили основой для создания специальных курсов, которые сейчас преподаются во всех школах и большинстве университетов США. В обиход широко вошли понятия компьютерная этика, этика рекламодателей, нэтикет или этика поведения в сети Интернет.

На основе этических стандартов, используемых в перечисленных выше кодексах, Международная федерация по информационным технологиям (IEIP) рекомендовала принять кодексы компьютерной этики национальным организациям других стран с учётом местных культурных и этических традиций, основой которых служат следующие десять моральных постулатов, представленных ниже [1]:

– Вы не будете использовать компьютер с целью повредить другим людям;
– Вы не будете создавать помехи и вмешиваться в работу других пользователей компьютерных сетей;
– Вы не будете совать нос в файлы, не предназначенные для свободного использования;
– Вы не будете использовать компьютер для воровства;
– Вы не будете использовать компьютер для распространения ложной информации;
– Вы не будете использовать ворованное программное обеспечение;
– Вы не будете использовать компьютерное оборудование или сетевые ресурсы без разрешения или соответствующей компенсации;
– Вы не будете присваивать чужую интеллектуальную собственность;
– Вы будете думать о возможных общественных последствиях программ, которые Вы пишите или систем, которые Вы разрабатываете;
– Вы будете использовать компьютер с самоограничениями, которые показывают Вашу предупредительность и уважение к другим людям.

Во всех кодексах наряду с перечисленными заповедями и общечеловеческими моральными нормами, такими как честное исполнение своих обязанностей, профессиональная и социальная ответственность, повышение квалификации, расовое равноправие и т.п., содержатся нормы, основанные на соблюдении четырёх главных моральных принципов: privacy (тайна частной жизни), accuracy (точность), property (частная собственность) и accessibility (доступность).

Перечисленные принципы нашли отражение и в «Национальном кодексе деятельности в области информатики и телекоммуникаций», разработанном Торгово-промышленной палатой Российской Федерации еще в 1996 году, основные положения которого включают [1]:

– не производить (копировать) и не использовать программные и технические средства информатики и телекоммуникаций без разрешения (лицензии) собственника (изготовителя) или правовладельца и не приобретенные на законных основаниях;

– не нарушать законодательство об охране интеллектуальной собственности и признанные нормы авторского права на программные средства и базы данных;

– не нарушать тайны передачи сообщения, не практиковать вскрытие информационных систем и сетей передачи данных;

– не использовать наименования и аббревиатуры других фирм, компаний и организаций без их согласия;

– не извлекать прибыль от использования товарного знака или символа, принадлежащего другой фирме или продукции.

Кодекс включал и другие моральные нормы и был открыт для добровольного присоединения любого физического или юридического лица, действующего в области информатики или телекоммуникаций. Кодекс распространялся на все виды деятельности: производство, продажу, пользование средствами информатики и телекоммуникаций и определял, что эта деятельность должна быть законной, пристойной, честной и правдивой.

Об информационном взаимодействии. К сожалению, подобные кодексы часто существуют отдельно от пользователей компьютерной техники. По разным оценкам уровень использования пиратского программного обеспечения в России достигает 90%, в то время как в странах, где уделяется достаточное внимание проблемам этического использования информационных технологий, этот уровень не превышает 30%. Нередко предпринимаются попытки несанкционированного доступа в защищаемые информационные системы, многие начинающие программисты считают своей доблестью написать программу-вирус, можно свободно приобрести вредоносные программы. Как следствие, российский рынок информационной безопасности растет в среднем, на 30% в год. Причем продажи антивирусного программного обеспечения увеличиваются более чем на 50% в год, при том, что в мире в среднем на 15% - 20% в год [2].

С развитием информационных систем угрозы, исходящие от сотрудников организаций, стали особенно серьезными, ущерб от их действий исчисляется десятками миллиардов долларов. К сожалению, увеличивается поток сообщений об инцидентах, связанных с нарушением своих обязательств и прав авторизованными пользователями, которые саботируют свою компанию и передают информацию конкурентам. Необходимо отметить, что изменяется бизнес-среда, которая часто полагается на аутсорсинг, подрядные компании и сторонние технологические платформы, что приводит к тому, что ценная информация становится доступной большому количеству людей. При инсайдерских утечках контроль доступа и защита периметра не помогут от находящегося внутри периметра вредителя.

В 2020 году резко выросли доли умышленных утечек, а также утечек по вине внешних нарушителей. В первую очередь эта ситуация связана с существенным ростом ликвидности данных в период пандемии: в это время недобросовестные сотрудники активно искали дополнительный заработок, а хакеры пользовались тем, что компании в авральном режиме меняли привычные формы реализации процессов и могли при этом ослабить контроль информационных активов. В результате совокупная доля умышленных утечек пользовательской информации достигла 72,5%, тогда как годом ранее она составила 60,2%. Действия хакеров и неизвестных лиц из-за пределов информационного контура организаций привели к 55,9% утечек. Соответственно, 44,1% утечек были спровоцированы различными действиями, а порой и бездействием персонала [3].

Следует обратить особое внимание на использование социальных сетей, ведь они сегодня для многих являются основным местом проведения времени в Интернете. При этом у людей существует множество психологических барьеров и в результате не все способны общаться в реальной жизни. Социальные сети, позволяют совершенно незнакомым людям найти общий язык, как посредством общения, так и посредством открытой информации, которую оставляют пользователи. Эта информация позволяет различным компаниям, не тратя много сил и времени, воздействовать на нужных ей людей и работать с ними.

Социальные сети можно рассматривать как инструмент для продвижения как коммерческих, так и социальных проектов.

Ежедневно миллионы пользователей ведут беседы о компаниях, их товарах и услугах, делясь своим мнением и впечатлениями. В результате отдельно взятый участник сетевого сообщества может испортить или наоборот улучшить репутацию компании с многомиллионным оборотом.

Ежемесячная аудитория соц. сети ВКонтакте составляет 87 млн. человек. Суммарная мобильная аудитория соц. сети составляет 71 млн. человек, т. е. 76% пользователей заходят в социальную сеть с помощью мобильного устройства. В среднем, ежедневно российские пользователи проводят в ВКонтакте 33 минуты — для примера, в Instagram этот показатель равен 17 минутам. Также каждый пользователь мобильного приложения ВК в среднем просматривает около 100 постов в сутки [2].

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.

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. Социальные сети вузов могут служить инструментом развития, однако необходимо учитывать таящиеся в них опасности [2].

Значительный вклад в решение задачи внедрения в сознание участников информационного взаимодействия необходимости соблюдения норм компьютерной этики и привития навыков ее применения может и должна внести система образования, как социальный институт «производства социального человека» [4]. Разъяснение и пропаганду этих норм необходимо проводить в лекционных курсах информатики, информационных технологий и других информационных дисциплин. Студенты должны понимать основные правовые, социальные и этические аспекты обеспечения информационной безопасности общества. Они должны сознавать свою личную роль в этом процессе. Студенты должны также развивать в себе способность задавать серьезные вопросы о социальном влиянии информатизации и оценивать предлагаемые ответы на них. Социально-личностное развитие обучаемых по различным специальностям, как техническим, так и сугубо гуманитарным, имеет чрезвычайно важное значение для обеспечения информационной безопасности общества.

Об этом говорится и в одном из пунктов проекта «Этического кодекса для информационного общества» Юнеско [5], а именно:

– всем действующим лицам в информационном обществе следует стремиться поднять каждого участника на тот уровень, где он поймет, как работает система и как он может действовать коллективно со всеми, разделяя ответственность за успех системы в целом;

– открытое, интегрированное и межкультурное образование, совмещенное с обучением навыкам информационного и коммуникационного управления, является решающим; не следует ограничивать его получением технических знаний, но также включать осведомленность о моральных принципах и ценностях;

– людям следует быть готовыми к получению базовых навыков в области информационно-коммуникационных технологий и этики в информационном обществе.

Дисциплина «Информационная этика». Одним из элементов решения указанных выше задач может стать введение информационной этики в разряд дисциплин, изучаемых в высшей школе. Целями этой дисциплины должны стать: ознакомление студентов с историческими и философскими предпосылками этических традиций, связанных с социальными аспектами построения информационного общества; внедрение в сознание обучаемых необходимости следования на практике принципам, декларированным в кодексах информационной этики; развитие навыков информационной этики. Введение данной дисциплины позволит привлечь внимание к этическим требованиям глобальной информационной инфраструктуры, к которым относятся:

– вопросы языка и грамотности и разрыв между странами в области развития информационных технологий;

– риски, связанные с применением компьютерных систем, их оценка и управление ими;

– интеллектуальная собственность и обмен ею;

– этические и законодательные основы личной безопасности, конфиденциальность информации, гражданские свободы (свобода самовыражения) в киберпространстве.

В период пандемии, в связи с существенным ростом ликвидности данных, увеличения объемов работ в дистанционном формате необходимо особенно обратить внимание на изучение информационной этики.

Заключение. Таким образом, необходимо еще раз подчеркнуть, что рассмотрение социальных и этических аспектов информационных технологий должно стать обязательной темой для разговора при проведении занятий по всем информационным дисциплинам, что будет способствовать формированию здорового современного информационного общества.

СПИСОК ЛИТЕРАТУРЫ

1. Кононов О.А., Кононова О.В. Социальные и этические аспекты обеспечения информационной безопасности // Проблемы управления, №1. М.: ИПУ РАН, 2009. – С.76-80.
2. Кононов О.А., Кононова О.В. Социальные сети вузов и информационная безопасность. Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 5 / СПОИСУ. - СПб, 2018. - с.350-353.
3. Утечки данных. [Электронный ресурс] – URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D1%82%D0%B5%D1%87%D0%BA%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85#.D0.A4.D0.B8.D0.BD.D0.B0.D0.BD.D1.81.D0.BE.D0.B2.D1.8B.D0.B5_.D0.BF.D0.BE.D1.82.D0.B5.D1.80.D0.B8_.D0.BE.D1.82_.D1.83.D1.82.D0.B5.D1.87.D0.B5.D0.BA (Дата обращения 30.08.2021).
4. Кононов О.А., Кононова О.В. Образовательный процесс и ИКТ. XV Санкт-Петербургская международная конференция «Региональная информатика – 2016 (РИ-2016)»: материалы конференции. – СПб.: СПОИСУ, 2016. - С.368.
5. Этический кодекс для информационного общества. [Электронный ресурс] – URL: https://ifap.ru/ofdocs/unesco/etcodex.pdf (Дата обращения 30.08.2021).

УДК 378.14

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ КЛЮЧЕВЫХ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ (KPI) К СИСТЕМЕ ОЦЕНКЕ СОТРУДНИКОВ С ПОМОЩЬЮ ЦИФРОВИЗАЦИИ

Одинокая Мария Александровна, Дмитриева Наталия Владимировна
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., д. 29, Санкт-Петербург, 195251, Россия
e-mail: World.Maria@hotmail.com, dmitrieva_nv@spbstu.ru

Аннотация. В тезисах доклада рассматривается необходимость применения ключевых показателей эффективности (KPI). На современном этапе в образовательной сфере цифровизация представляет собой необратимый процесс, затрагивающий самые разные аспекты жизни, в том числе – цифровую экономику. В связи с этим, резко возрастает значимость системы управления, адаптированной к современным реалиям. Особое внимание уделяется тому, какие задачи исследователь сможет решить с помощью применения ключевых показателей эффективности. В контексте сказанного, не вызывает сомнений актуальность, своевременность и перспективность исследований, направленных на совершенствование корпоративной практики управления персоналом с учётом новых возможностей, предоставляемых цифровизацией экономики. Анализируется возможность повышения эффективности управления персоналом (HR) и прогнозирования производительности сотрудников.

Ключевые слова: ключевые показатели эффективности; система оценки; сотрудник; управление персоналом; цифровизация.

POSSIBILITIES OF APPLYING KEY PERFORMANCE INDICATORS (KPI) TO THE EMPLOYEE ASSESSMENT BY DIGITALIZATION

Odinokaya Maria, Dmitrieva Natalia
Peter the Great St. Petersburg Polytechnic University
29 Politechnicheskaya str., St. Petersburg, 195251. Russia,
e-mail: World.Maria@hotmail.com, dmitrieva_nv@spbstu.ru

Abstract. The abstract of the report addresses the need to apply key performance indicators (KPI). At the present stage in the educational sphere, digitalization is an irreversible process that affects a variety of aspects of life, including the digital economy. In this regard, the importance of a management system adapted to modern realities is sharply increasing. Particular attention is paid to what tasks the researcher can solve using the use of key performance indicators. In the context of the above, there is no doubt about the relevance, timeliness and prospects of research aimed at improving the corporate practice of personnel management, taking into account the new opportunities provided by the digitalization of the economy. The possibility of improving the efficiency of personnel management (HR) and forecasting the performance of employees is analyzed.

Keywords: key performance indicators; rating system; employee; personnel management; digitalization.

В настоящее время в современной образовательной практике наблюдается тенденция измерять производительность сотрудников. Работников оценивают по компетенциям: умеет/не умеет или на основе субъективного мироощущения. Из-за этого руководители теряют целый пласт полезных данных. Например, насколько соответствует сложность задач компетенциям сотрудника, его опыту и статусу [1-3].

KPI (Key Performance Indicator) – ключевые показатели эффективности – система количественных индикаторов, отражающих результативность работы каждого сотрудника.

Система KPI пришла в практику российских компаний несколько лет назад. В настоящее время не разработано единой методики оценки ключевых показателей эффективности для российских предприятий, используется комплекс зарубежных индикаторов.

Преимуществом системы KPI является активная мотивация персонала и сопоставимые показатели. Эффективность – относительный показатель, который охватывает все сферы деятельности работников и выражает результаты количественно. Оптимальное число KPI для одного сотрудника – не более пяти.

Правильно выстроенная система ключевых показателей эффективности (KPI) позволит исследователю возможность принимать решения на основе цифр (рис. 1). Исследователь сможет заглянуть вперед, спрогнозировать, какие процессы в будущем могут дать сбой, что особенно важно в ситуации кризиса и неопределенности.

Систему ключевых показателей эффективности (KPI) можно назвать цифровым двойником компании: она описывает, какие параметры компании завязаны друг на друга, и закрепляет систему функциональной ответственности сотрудников. С помощью KPI исследователь может решить три принципиально важные задачи.

Первая задача, которую решает система KPI - создание для сотрудника линии видимости. Сотрудник сможет в конце запланированного периода отчета ответить себе на вопрос: эффективно ли я поработал. На самом деле это важнее, чем жесткий контроль. В кризисный период важно контролировать сотрудника по результату его труда, а не по тому, насколько активно он имитирует бурную деятельность.

Рис. 1. Место системы KPI в системе бизнес-процессов

Вторая возможность, которую дает система KPI – это подсчет эффективности сотрудников, позволяющий исследователю начать подсчитывать эффективность HR. Чтобы подсчитать эффективность HR, надо считать воронку найма, продолжительность жизни и сроки выбытия, затраты на найм и обязательно производительность сотрудников. И вот этот параметр исследователю может помочь закрыть система KPI. Исследователь сможете, например, более осознанно расставаться с сотрудниками. Чем больше будет прозрачности в работе каждого работника, тем больше будет возможностей увольнять, не теряя в результативности и производительности.

Рис. 2. Структура основных показателей KPI

Третья возможность, которую дает система KPI - глубокий анализ. Например, если исследователь начнет считать производительность сотрудников, у него появится возможность понять, с какого месяца они выходят на плато производительности и от них больше получить ничего нового и серьезного нельзя (рис. 2).

Исследователь сможет осознать и понять, какие факторы и как именно влияют на производительность, какие компетенции, навыки и инструменты позволят ее повысить. Эти три задачи исследователь сможет решить, когда введет KPI.

KPI не решит вопросы, связанные с дисциплиной или корпоративной культурой. Любые KPI - это так называемые запаздывающие индикаторы, они постфактум отражают, как сотрудник поработал. Если работник будет знать, что его эффективность оценят, его желание хорошо работать вырастет. Но одного желания недостаточно, нужна технология, а ее никакая система KPI не обеспечит. Отсюда вывод: KPI нужны не столько для сотрудника, сколько для руководителя. Не для того, чтобы сотрудники лучше работали, а чтобы руководителю было проще

руководить и принимать решения. Руководитель может увидеть, какие показатели выбиваются из нормативных значений и исходя из этого сможет выстраивать с сотрудниками дальнейшее взаимодействие.

У руководителей департаментов или отделов самую большую роль должны занимать кросс-функциональные KPI, на втором месте должны быть командные KPI. Персональные KPI практически никакой роли не играют, иногда их вес равен нулю. Предполагается, что основная задача таких сотрудников – создавать синергетические эффекты от взаимодействия с другими отделами. Для средних менеджерских позиций, руководителей цехов нужно ввести принцип, при котором командные KPI играют наибольшую роль (порядка до 70% от переменных показателей). Устанавливаем личные, командные и кросс-функциональные KPI Персональные KPI для них играют вторую по важности роль. На третьем месте кросс-функциональные KPI. Важно добавить, что у командных исполнителей персональные KPI тоже должны играть роль, но не большую, а кросс-функциональные KPI – практически не играют никакой роли.

KPI должны лежать в основе кадровых решений – повышения зарплат, расставания с сотрудниками, изменения должностных обязанностей. На мой взгляд, оптимальный срок для принятия таких решений – это год. Таким образом, стандартный порядок пересмотра KPI: показатели первого уровня - раз в год, второго уровня – раз в полгода, KPI отделов - раз в квартал, исполнителей - раз в месяц.

Отказываться от KPI и резко менять принципы его начисления не стоит. Рекомендуется пересмотреть его структуру и, возможно, коэффициенты/ проценты/ удельный вес. Так исследователь сможет настроить систему показателей более точечно, при этом сохранив внешнюю структуру неизменной. Можно привлечь к этой работе линейных руководителей, контролируя конечный результат.

Часто сотрудники без понимания смысла системы KPI достигают показателей, но при этом страдает содержание работы.

Для малого бизнеса лучше взять хронологическую систему, потому что малый бизнес движется короткими спринтами. Для среднего бизнеса подойдет либо причинно-следственная, либо структурная система.

Рекомендуется разрабатывать KPI совместно с сотрудниками. Если их разрабатывать сверху, то это будут акценты, на которое руководство хочет обратить внимание. Вопрос в том, будут ли эти цифры и задачи считаться достижимыми. Когда исследователи разрабатывают KPI, то рекомендуется вовлекать рабочую группу сотрудников, например, территориальных управляющих или линейных сотрудников и разрабатывать те показатели, которые будут выглядеть выполнимыми.

Проведение анализа показателей эффективности KPI в компании имеет как положительные, так и отрицательные стороны. К достоинствам KPI-анализа можно отнести:

- каждый сотрудник компании получает конкретный перечень требуемых результатов;
- сотрудники наглядно могут оценить свой вклад в достижение поставленных компаний целей;
- руководство всегда имеет актуальную информацию о работе каждого сотрудника, что повышает контроль качества выполнения сотрудником служебных обязанностей.

К основным недостаткам относятся:

- иногда случается, что низкая продуктивность отдела накладывает негативный отпечаток на высокую производительность конкретного сотрудника, как следствие сотрудник может уволиться, не получив должной оценки своего труда;
- не все сотрудники получают материальное поощрение в результате достижения поставленной цели;
- иногда, результатом проведения KPI-анализа является так называемая обратная мотивация. То есть вместо поощрения за достигнутые результаты, сотрудники ничего не получают, в то время как не справившиеся с задачей штрафуют или наказывают.

Таким образом, мы приходим к заключению, что KPI поможет создать линию видимости для сотрудников, измерить эффективность HR и спрогнозировать производительность сотрудников. KPI не научит сотрудников дисциплине. Чем выше сотрудник располагается в иерархии компании, тем больше должна быть доля оплаты от KPI. У руководителей департаментов самую большую роль должны играть кросс-функциональные KPI, у руководителей среднего звена - командные KPI, у младших менеджеров - личные KPI. Рекомендуется ставить сотрудникам только те KPI, на которые они могут влиять. Необходимо следить, чтобы KPI не дублировали друг друга, но и не упустить знаковые процессы. Следует обратить внимание на использовании одного из четырех подходов к формированию системы KPI - хронологический, причинно-следственный, структурный и приоритетный. Другие подходы не сработают. Необходимо создавать систему KPI совместно с сотрудниками.

СПИСОК ЛИТЕРАТУРЫ

1. Е. Н. Лавриенко, Н. А. Багута Подходы к реализации системы KPI для персонала организации в условиях цифровой трансформации экономики // Московский экономический журнал, № 2, 2021. С. 194-199.
2. Г. Л. Тульчинский Гуманитарные науки и цифровизация // Человек. Культура. Образование. Серия: педагогические и психологические науки, № 2 (36), 2021. С. 43-57.
3. О. А. Козлова, Е. А. Селезнева Особенности мотивации работников в условиях формирования цифровой экономики // Human progress, № 4(10), 2018. С. 2.

УДК 378.14

ФОРМИРОВАНИЕ ЦИФРОВОЙ ГРАМОТНОСТИ ОБУЧАЮЩИХСЯ В СОВРЕМЕННОЙ ШКОЛЕ

Одинокая Мария Александровна[1], Жигадло Надежда Владимировна[2]
[1]Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., д. 29, Санкт-Петербург, 195251, Россия
[2]Гимназия № 652
пр. Тореза, 41, Санкт-Петербург, 194223, Россия
e-mail: World.Maria@hotmail.com, zve@mail.ru

Аннотация. В тезисах доклада рассматривается актуальная на современном этапе развития образования проблема формирования цифровой грамотности обучающихся в современном «цифровом» мире. Предпринята попытка уточнить термин «цифровая грамотность». Важно, что учебная деятельность современных обучающихся реализуется в условиях информатизации жизни общества и образования. Уделено внимания необходимости различения понятий «компьютерная и информационная грамотность» и «цифровая грамотность», которые являются синонимичными по семантическому полю. Особое внимание уделяется вопросу необходимости формирования цифровой грамотности, включающей в себя личностные, технические и интеллектуальные навыки, необходимые для безопасной и комфортной жизни в цифровом мире.

Ключевые слова: цифровая грамотность; обучающийся; современная школа; цифровизация; обучающийся; педагог.

FORMATION OF DIGITAL LITERACY OF STUDENTS IN A MODERN SCHOOL

Odinokaya Maria[1], Zhigadlo Nadezhda[2]
[1]Peter the Great St. Petersburg Polytechnic University
29 Politechnicheskaya str., St. Petersburg, 195251. Russia,
[2]Gymnasium No. 652,
41 Torez Ave., Saint Petersburg, 194223, Russia
e-mail: World.Maria@hotmail.com, zve@mail.ru

Abstract. In the theses of the report, the problem of the formation of digital literacy of students in the modern «digital» world, which is relevant at the present stage of the development of education, is considered. An attempt is made to clarify the term «digital literacy». It is important that the educational activities of modern students are implemented in the conditions of informatization of the life of society and education. Attention is paid to the need to distinguish between the concepts of «computer and information literacy» and «digital literacy», which are synonymous in the semantic field. Special attention is paid to the need for the formation of digital literacy, which includes personal, technical and intellectual skills necessary for a safe and comfortable life in the digital world.

Keywords: digital literacy; student; modern school; digitalization; student; teacher.

В настоящее время в современной образовательной практике наблюдается тенденция цифровизации самых разнообразных сфер жизнедеятельности мирового сообщества, в том числе и сферы образования. В этой ситуации образование занимает лидирующие позиции, так как цифровые технологии уже сейчас стали высокотехнологическим средством, способствующим коммуникации, эффективным инструментом развития Российского цифрового образовательного пространства [1-3].

Проблема удовлетворения желания обучающихся использовать арсенал цифровых технологий для более широкого и разнообразного доступа к учебным ресурсам, обеспечения информационной и электронной безопасности обучающихся, обеспокоенность их неготовностью к работе в цифровой образовательной среде стал одним из ключевых вопросов. Наблюдается несоответствие между восприятием обучающихся своих цифровых навыков и способностью перемещаться по безопасному и осмысленному пути в сетевом ландшафте. На наш взгляд, обучающиеся нуждаются в дополнительных навыках для удовлетворения своих информационных образовательных потребностей и лучшего понимания норм онлайн-среды.

Формирование умений самостоятельно выполнять действия должно проходит путь от деятельности обучающегося под непосредственным руководством педагога к деятельности «под собственным руководством». Предлагая обучающимся выполнить то или иное учебное задание, педагог сначала руководит работой: объясняет суть учебного задания, показывает последовательность необходимых для осуществления требования действий. В дальнейшем при выполнении аналогичных учебных заданий обучающийся при необходимости получает дифференцированную помощь и таким образом постепенно овладевает умением самоорганизовываться в распределении учебных действий во времени и осуществлять самоконтроль их выполнения [4, 5]. Педагогу

необходимо обеспечить условия для присвоения обучающимися социальных норм, культурных ценностей и образцов поведения.

Возможности организации учебной деятельности обучающихся в глобальной сети Интернет создают затруднительные ситуации, которые педагогу необходимо учитывать в практической деятельности. К таким образовательным рискам правомерно отнести:

формальное выполнение обучающимся учебных заданий;

неумение выделить главную и второстепенную учебную информацию;

неверная формулировка информационного запроса, соответствующего образовательным потребностям;

неумение оценить ресурсы с точки зрения их достоверности.

Кроме того, возможность выполнять учебные задания в любом месте и в любое время, без соблюдения техники безопасности при работе с цифровыми гаджетами и гигиены умственного труда может способствовать развитию различных информационных зависимостей и информационной перегрузки обучающегося и влиять в конечном итоге на качество выполняемы ими учебных заданий.

Под цифровой грамотностью нами понимается особая система когнитивных, социальных и технических навыков, которые гарантируют качественное существование обучающегося в технологически оснащенной информационной среде, а также готовность и способность обучающегося продуктивно использовать в собственных целях весь арсенал цифрового инструментария (в частности, цифровых технологий и ресурсов сети Интернет), уверенно, критично, безопасно, комфортно и творчески работать в данной среде, а также готовность к непрерывному овладению соответствующих компетенций (системой соответствующих знаний, умений, мотивации и ответственности) (рис. 1).

Рис. 1. Многокомпонентный состав цифровой грамотности

Цифровая грамотность занимает приоритетное место в перечне базовых навыков, востребованных в XXI веке практически в любом профиле подготовки. Цифровая грамотность включает в себя личностные, технические и интеллектуальные навыки, необходимые для комфортной жизни в цифровом мире.

Синонимичными по семантическому полю к понятию «цифровая грамотность», являются «компьютерная и информационная грамотность». Необходимо различать данные понятия. Под компьютерной и информационной грамотностью понимаются умения и навыки работы на компьютере, управление файлами и папками, знание основ информатики, минимальные знания основных офисных программ.

Владение цифровой грамотностью предполагает развитие трех компонентов:

– технические аспекты (в частности, свободно и в тоже время безопасно ориентироваться в цифровом пространстве; умение использовать программы защиты информации, избавляться от спама, кукис, бороться с вирусами, трояками и т.п.; умение оценить достоверность информации, как умение сохранить свои личные и персональные данные, умение защитить свои и не нарушить чужие авторские и интеллектуальные права;

использовать программные средства и пакеты программ, просматривать и осуществлять поиск учебной информации; умение создавать тексты разного типа дли различных адресатов сообщении, умение создавать фотографии, аудио- и видеоматериалы на компьютере и пересылать их другим и т.п.; умение пользоваться инструментами поиска, хранения и передачи информации, е том числе браузерами, облачными технологиями, умение использовать технические каналы коммуникации (электронная почта, чат, блог, видеоконференции, телекоммуникационные проекты, Skype и т.п,);

– информация в сети Интернет (навыки поиска нужной информации и инструментов работы с ней, умения быстро освоить эти инструменты; способность различать качество учебной информации, найденной в сети Интернет);

– коммуникация в сети Интернет (в частности, мотивацию обучающегося на развитие и его ответственность как гражданина цифрового мира; общение о сети Интернет, социальных сетях; социокультурное участие обучающихся в сетевом обществе, их самовыражение, формирование сетевой идентичности и активное осознанное участие в цифровом мире; умение производить информацию в ее разнообразных формах и форматах; наличие правильных личных ценностных установок, уровня воспитания, модели культуры, преобладающей в обществе, общественных трендов и запросов; наличие умений создавать, развивать и поддерживать здоровые отношения с людьми, умения презентовать себя и поддерживать свою репутацию), цифровое потребление (в частности, умение использовать онлайн-сервисы для получения услуг и товаров) (рис. 2) [6].

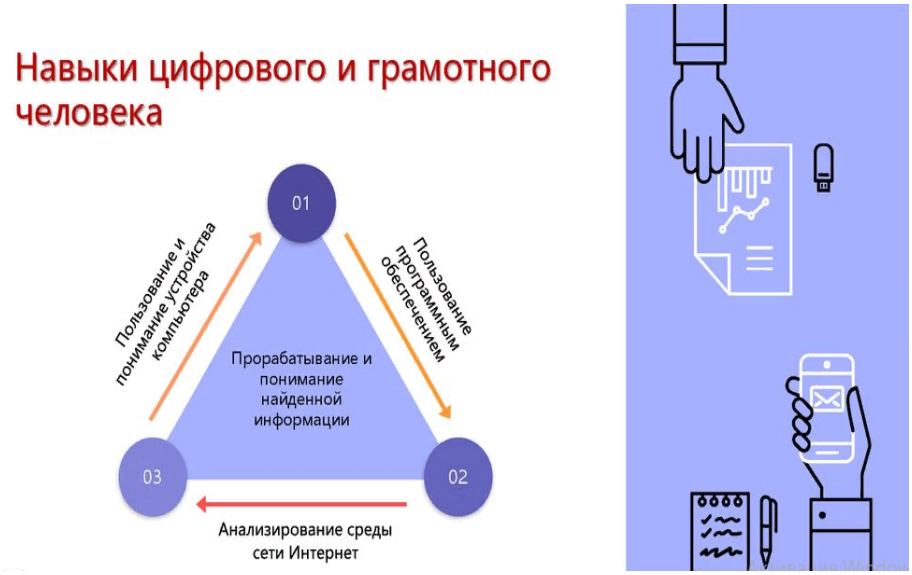


Рис. 2. Навыки цифрового и грамотного человека

Из всего вышесказанного можно сделать вывод о том, что вопрос формирования цифровой грамотности обучающихся является значимым и само его существование дает возможность осмыслить вызовы, ожидающие человечество на пути цифровизации образования, что принципиально важно в условиях быстрого обновления знаний; повышением доступности образования, удовлетворением потребностей разных категорий обучающихся и т. д.

СПИСОК ЛИТЕРАТУРЫ

4. И. Г. Алмазова, Е. В. Долгошеева, Е. В. Игонина, Г. А. Корякина, С Н. Числова WIKI-площадка как средство развития числовой грамотности и умений самостоятельной работы младших школьников // КПЖ, № 3 (140), 2020, С. 127-134.
5. В. Э. Жигадло, М. А. Одинокая Роль электронных учебных пособий в процессе организации и проведении самостоятельной работы студентов технического вуза (на примере электронного пособия по дисциплине «Иностранный язык в профессиональной деятельности» // Ученые записки Санкт-Петербургского университета технологий управления и экономики, № 4 (60), 2019, С. 5-16.
6. В.. Э. Жигадло, М. А. Одинокая Использование технологии учебных подкастов при обучении языку хинди в техническом вузе как средства повышения качества дополнительного гуманитарного образования // Язык и культура, № 38, 2017, С. 207-226.
7. Е. О. Иванова Организация самостоятельной работы учащихся в информационно-образовательной среде: возможности и проблемы / Е.О. Иванова // Вестник Владимирского государственного гуманитарного университета. Серия: педагогические и психологические науки, № 11(30), 2011, С. 276-281.
8. Т. А. Бороненко, А. В. Кайсина, В. С. Федотова Развитие цифровой грамотности школьников в условиях создания цифровой образовательной среды // ПНиО, № 2 (38), 2019, С. 167-193.
9. О. В. Ельцова, М. В. Емельянова К вопросу о понятии цифровой грамотности // Вестник ЧГПУ им И.Я. Яковлева, № 1(106), 2020,С. 155-161.
10. Т. А. Бороненко, А.В. Кайсина, В. С. Федотова Концептуальная модель понятия цифровой грамотности // ПНиО, № 4 (46), 2020, С. 47-73.

УДК 378

ПОДХОДЫ К ОЦЕНКЕ КАЧЕСТВА ПОДГОТОВКИ СПЕЦИАЛИСТОВ ВЫСШЕГО ОБРАЗОВАНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Прудникова Марина Валерьевна
Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
1-я Красноармейская ул., 1, Санкт-Петербург, 190005, Россия
email: prudnikova_mv@mail.ru

Аннотация. В данной статье проводится анализ различных подходов к системе оценки качества подготовки специалистов высшего образования в Российской Федерации как со стороны государственных органов курирующих деятельность вузов, так и со стороны системного психолого-педагогического и компетентностного подходов.

Ключевые слова: система высшего образования; качество образования; методика оценки качества образования; оценка качества подготовки специалистов; человеческие ресурсы; государственная политика в сфере образования; образовательная деятельность.

APPROACHES TO ASSESSMENT OF THE QUALITY OF TRAINING OF HIGHER EDUCATION SPECIALISTS IN THE RUSSIAN FEDERATION

Prudnikova Marina
BALTIC STATE TECHNICAL UNIVERSITY «VOENMEH» named after D.F. Ustinov
1 1st Krasnoarmeyskaya St., St. Petersburg, 190005, Russia
email: prudnikova_mv@mail.ru

Abstract. This article analyzes various approaches to the system of assessing the quality of training of specialists in higher education in the Russian Federation, both from the side of state bodies supervising the activities of universities, and from the side of systemic psychological, pedagogical and competence approaches.

Keywords: higher education system; quality of education; methodology for assessing the quality of education; assessing the quality of training; human resources; state policy in the field of education; educational activities.

В быстроменяющемся современном мире, когда многие профессии заменяются искусственным интеллектом, необходимо поддерживать значимость человеческих ресурсов и формировать высокоразвитое общество. Современная система подготовки квалифицированных специалистов требует постоянного контроля и совершенствования внутренних и внешних механизмов для предоставления качественного образования. Существующее разнообразие методик, которые содержат механизмы и рекомендации для оценки различных аспектов деятельности высших учебных заведений требует систематизации и совершенствования согласно внедряемым изменениям.

Целью исследования выступает изучение современных подходов к оценке качества подготовки специалистов высшего образования.

Согласно ст. 2 ФЗ№273 от 29.12.2012 «Об образовании в Российской Федерации» качество образования - комплексная характеристика образовательной деятельности и подготовки обучающегося, которая должна соответствовать федеральным государственным образовательным стандартам и иным стандартам [1]. Существуют различные подходы к осуществлению контроля качества образования посредствам мониторинга результатов реализации образовательных программ, проведения внутренней и внешней экспертизы качества образовательной деятельности и оценки стратегии развития образовательных программ. В Таблице 1 представлен анализ основных действующих методик по оценке качества подготовки специалистов учреждений высшего образования [3]:

Таблица 1

Обзор современных методик по оценке качества образования

Подход	Описание
Методика Рособрнадзора	Проводится анализ документов на соответствие требованиям ФГОС, текущему контролю успеваемости, промежуточной и итоговой аттестации студентов и др. Негативные стороны методики: • основывается только на данных, предоставляемых вузами дистанционно, что увеличивает риски подмены данных
Методика по подходам ГИВЦ Минобрнауки России	К основным направлениям относится: сбор, обработка данных и анализ получаемой статистической отчетности. Негативные стороны методики:

	• одним из важных недостатков методики является ее неспособность учитывать потребности работодателей
Методика по подходам НИИ	К основным направлениям относятся: • тестирование в рамках различных проектов, например, «Интернет-тренажеры в сфере образования»; • подготовка отчетов и др. Негативные стороны методики: • отсутствие данных о качестве полученных знаний, которая может быть предоставлена работодателями. Оценка происходит только на основании результатов подготовки по ООП. • невозможность оценить востребованность специалистов на рынке труда

Таким образом, необходим более глубокий подход к оценке качества подготовки специалистов. Важным критерием, который не учитывается большинством методик, является потребность работодателей в конкретных кадрах, которая подкрепляется определенными требованиями к квалификации и навыкам, также необходим более детальный контроль на всех стадиях оценки, что обеспечит объективную оценку.

Также следует выделить и другие подходы к контролю качества, например, системный и компетентностный подходы к оценке качества подготовки специалистов.

Таблица 2

Подходы к осуществлению контроля качества образовательного процесса
(таблица составлена на основании данных статьи)

Подход	**Описание**
Системный психолого-педагогический	Критерии оценки: соответствие психологическим требованиям к специалисту. • структура оценки соответствует тенденциям современного развития; • качество трудового потенциала; • возможна качественная оценка уровня подготовки специалистов
Компетентностный	Критерии оценки: уровень развития компетентностей, компетенций, мета-качеств. Для системы профессионального образования актуальными являются базовые компетентности. К ним можно отнести: • общенаучные - понятия, основные законы природы; • социально-экономические; • гражданско-правовые; • информационно-коммуникационные; • общепрофессиональные, присущие группе профессий и др.

Таким образом, оценка качества подготовки специалистов в вузе основывается на интегративных критериях и показателях. Совместное применение этих подходов может послужить стимулом для повышения качества подготовки специалистов.

Обзор научных источников показал, что существуют различные подходы к оценке качества подготовки специалистов высшего образования в РФ, которые позволяют трактовать оценку качества высшего образования по отношению к различным объектам: уровню образовательных систем, уровню благосостояния общества, уровню удовлетворенности общества, применимости полученных знаний в реальной жизни и др. Однако существует ряд проблем, которые негативно влияют на полученные результаты.

В настоящей статье представлены различные подходы к оценке качества подготовки специалистов, которые базируются на методиках, в основе которых лежат разработки и нормативные положения государственных структур, включающие критерии системной оценки.

Направления дальнейших исследований в данной области лежит в изучении проблем, возникающих в ходе реализации данных подходов.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (с изм. с 01.09.2020). URL: http://www.consultant.ru/document/cons_doc_LAW_140174/ (дата обращения: 25.03.2021).
2. Соколова, И.Ю. Качество подготовки специалистов в профессиональном образовании с позиций системного и компетентностного подходов // Вестник Томского государственного педагогического университета. - 2011. - (13). С. 162-168.
3. Федоров С.В., Анисимова О.В., Владимирова Ю.Н. Методика оценки качества подготовки специалистов высшего образования с применением технологий краудсорсинга, соответствующая целям резолюции генеральной ассамблеи ООН в области образования для устойчивого развития // Устойчивое инновационное развитие: проектирование и управление». - 2019. Т. 15. № 2 (43). С. 3.

УДК 004.7

ОНТОЛОГИЧЕСКОЕ СОПРОВОЖДЕНИЕ ЖИЗНЕННОГО ЦИКЛА ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Птицына Лариса Константиновна[1], Птицын Никита Алексеевич[1], Птицын Алексей Владимирович[2]
[1] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
р. Мойки наб., 61, Санкт-Петербург, 191186, Россия
[2] Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: ptitsina_lk@inbox.ru, nikita_pti@ inbox.ru, pticin@inbox.ru

Аннотация. Рассмотрены причины для систематизации и представления знаний об образовательных программах по информационной безопасности. Акцентировано внимание на объективной необходимости интеллектуализации жизненного цикла образовательных программ по информационной безопасности. Приведено описание обстоятельств для выбора онтологического подхода к сопровождению жизненного цикла образовательных программ по информационной безопасности. Представлены вариации в выборе среды для реализации онтологического подхода. Описаны преимущества проектирования рабочих образовательных программ в средах для реализации онтологического подхода. Раскрыто представительное многообразие интеллектуального представления знаний об образовательных программах и последующей их обработки в целях выбора приоритетных путей их совершенствования.

Ключевые слова: образовательная программа; рабочий учебный план; жизненный цикл; систематизация; интеллектуализация; обработка знаний.

ONTOLOGICAL SUPPORT OF THE LIFE CYCLE OF EDUCATIONAL PROGRAMS ON INFORMATION SECURITY

Ptitsyna Larisa[1], Ptitsyn Nikita[1], Ptitsyn Alexey[2]
[1] The Bonch-Bruevich Saint Petersburg State University of Telecommunications
61 Moika River Emb, St. Petersburg, 191186, Russia
[2] ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mails: ptitsina_lk@inbox.ru, nikita_pti@inbox.ru, pticin@inbox.ru

Abstract. The reasons for the systematization and presentation of knowledge about educational programs on information security are considered. The attention is focused on the objective necessity of intellectualization of the life cycle of educational programs on information security. A description of the circumstances for choosing an ontological approach to support the life cycle of educational programs on information security is given. Variations in the choice of environment for the implementation of the ontological approach are presented. The advantages of designing working educational programs in environments for the implementation of the ontological approach are described. The representative variety of intellectual representation of knowledge about educational programs and their subsequent processing in order to select priority ways of their improvement is disclosed.

Keywords: educational program; working curriculum; life cycle; systematization; intellectualization; knowledge processing.

При современных темпах стремительного развития достижений гипертехнологий IT-индустрии цифровая трансформация во всех сферах жизнедеятельности социума признается одной из основных движущих сил развития национальной экономики и необходимым условием для обеспечения её безопасности. Агрессивное воздействие биологических вирусов в большей степени повышает уровень значимости цифровой трансформации во всех сферах жизнедеятельности социума. Расширение масштабов и возрастание интенсивности погружения различных процессов жизнедеятельности социума в разнообразные по архитектуре и предоставляемым возможностям среды информационных инфраструктур, с одной стороны, создает неоспоримые преимущества для повышения качества выполняемой деятельности, а, с другой стороны, является тем фактором, который приводит к разрастанию поля угроз информационной безопасности. В подобной обстановке подготовка бакалавров, специалистов и магистров по информационной безопасности приобретает повышенную значимость при подготовке кадров для цифровой экономики.

Совершенствование образовательных программ подготовки кадров по информационной безопасности в университетах осуществляется посредством непрерывного расширения знаний по защите информации и покрытия существующих профессиональных стандартов в соответствующих сферах [1, 2]. На рис. 1 приведен онтограф классификации профессиональных стандартов Российской Федерации.

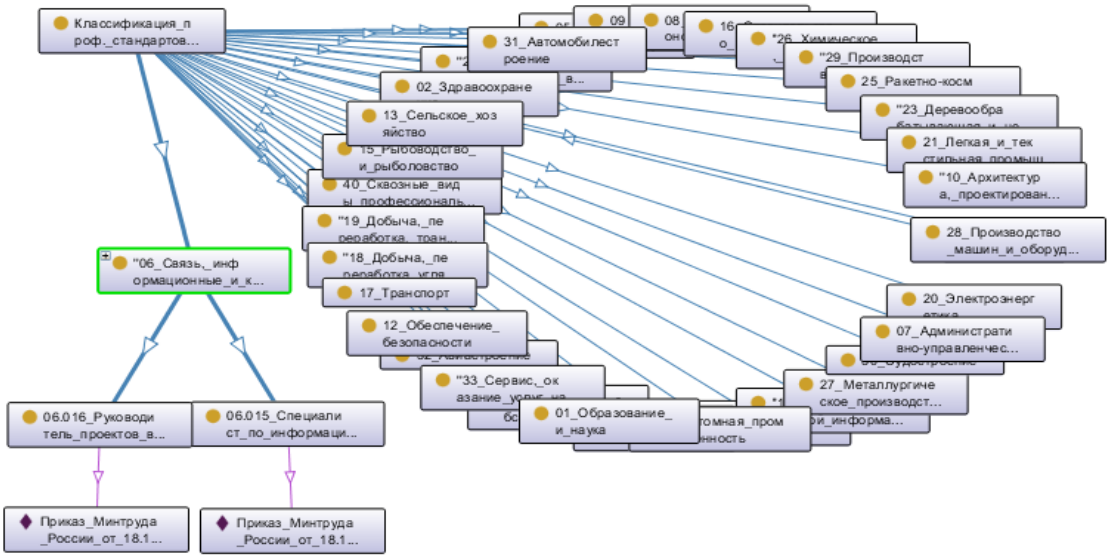


Рис.1. Классификация профессиональных стандартов.

Накопленный опыт реализации образовательных программ подготовки кадров по информационной безопасности выражается в образовании их множества и появлении объективной необходимости обработки его компонентов в целях систематизации и представления знаний о технологических аспектах их жизненного цикла и последующего анализа, необходимого для выбора приоритетных принципов их развития и совершенствования. Повышение качества подобной работы неразрывно связано с интеллектуализацией жизненного цикла образовательных программ по информационной безопасности. Стартовый этап жизненного цикла образовательных программ подготовки кадров по информационной безопасности реализуется в виде разработки рабочего учебного плана. В существующей реальности результатом этого этапа является рабочий учебный план, представляемый в табличном виде в различных инструментальных средах и специализированных оболочках. В глобальной сети рабочие учебные планы представляются в виде файлов текстовых процессоров. При этом поддерживается лишь возможность ознакомления с результатом деятельности и в ряде случаев дозволенная мера их редактирования. Концепция разработки рабочей учебной программы остается вне образа его представления. Систематизация и обработка знаний при подобных образах рабочих учебных планов не представляется возможной. В то же время, стремительность обновления знаний о технологических достижениях IT-индустрии предопределяет объективную необходимость систематизации, представления и обработки знаний о рабочих учебных планах подготовки кадров по информационной безопасности.

В описанных условиях для разрешения рассмотренной проблемной ситуации предлагается применить онтологический подход к разработке рабочих учебных планов подготовки бакалавров, специалистов и магистров по информационной безопасности. О необходимости реализации предлагаемого подхода свидетельствует и успешный опыт интеллектуализации систематизации профессиональных стандартов для научно-образовательной сферы посредством построения, представления и обработки соответствующих онтологических моделей [3]. На рис. 2 изображён онтограф трудовых функций профессионального стандарта 06.016.

Указанное обстоятельство имеет огромное значение в силу того, что в современной компетентностной парадигме образования предусматривается обязательность формирования систем компетенций, определяемых как образовательными, так и профессиональными стандартами.

Для подключения онтологического подхода к сопровождению жизненного цикла образовательных программ по информационной безопасности предоставляются широкие возможности по выбору инструментальных сред онтологического моделирования, которые сами находятся в состоянии непрерывного развития по мере проявления новых проблемных ситуаций и совершенствования технологий программирования, а также технологий представления и обработки знаний. При этом наблюдается многообразие отличительных признаков, заложенных в различные системы их классификации, которыми целесообразно воспользоваться для определения критериев выбора конкретного варианта инструментальной среды онтологического моделирования.

В составе рассматриваемого многообразия присутствуют требования к платформам информатизации, характеристики функциональных возможностей, представления различий в компонентах поддерживаемых методологий онтологического проектирования, формализмы, языки и форматы. При таком обширном многообразии отличительных признаков открываются возможности реализации многокритериального выбора инструментальной среды онтологического моделирования на основе использования формальных методов оптимизации.

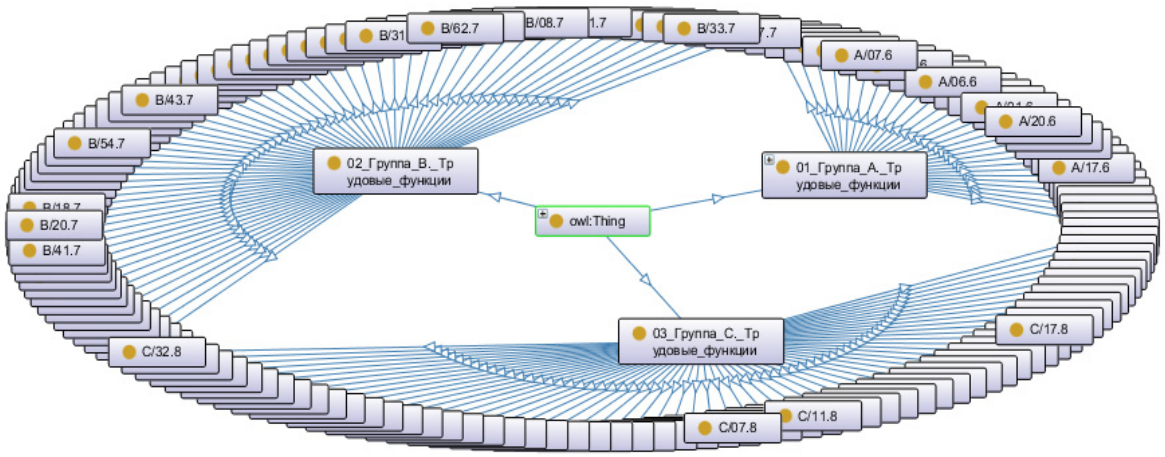


Рис.2. Онтограф трудовых функций профессионального стандарта 06.016.

Введение инструментальной среды онтологического моделирования в сопровождение жизненного цикла образовательных программ по информационной безопасности расширяет степень интеллектуализации автоматизированных процессов подготовки необходимых учебно-методических комплексов и снижает степень субъективизма в оценивании их состоятельности и уровня развития.

Неоспоримые преимущества проектирования рабочих образовательных программ в средах для реализации онтологического подхода проявляются не только на уровне систематизации, представлении и обработке знаний о различных образовательных программах по информационной безопасности, но и на расширении многообразия форм отображения знаний об индивидуальных образовательных траекториях. Подтверждением тому являются результаты выполнения проектов по представлению цифрового следа при персонализации подготовки кадров для цифровой экономики, описанные в [4, 5, 6].

На рис. 3 представлен онтограф цифрового следа студента, выделенный в семействе образовательных траекторий при онтологическом моделировании рабочего учебного плана.

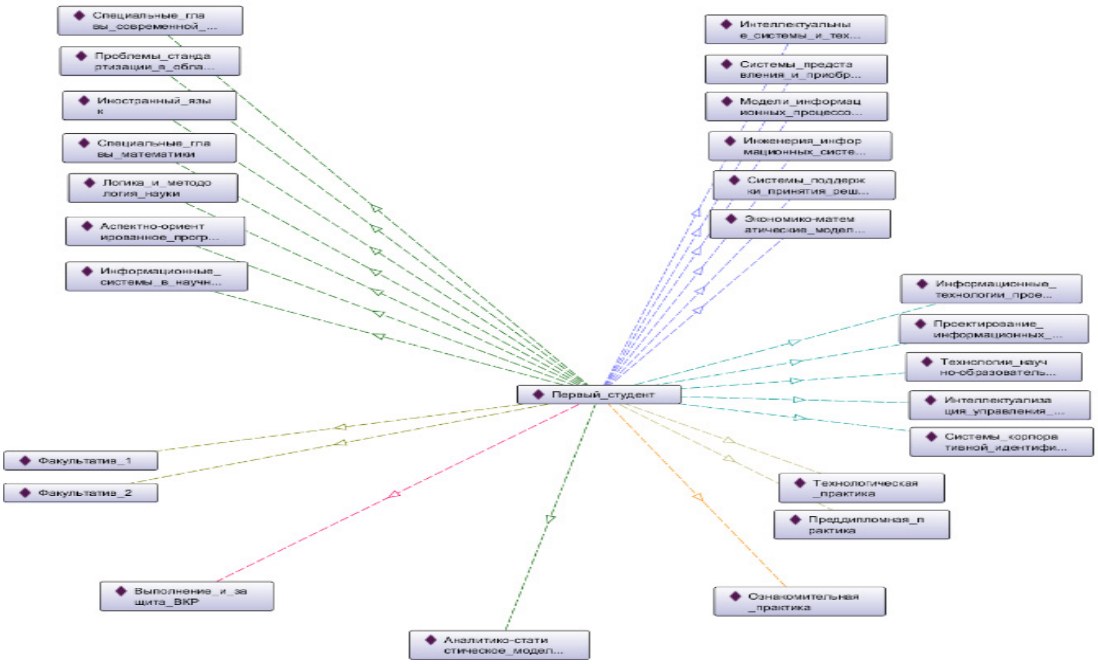


Рис.3. Онтограф цифрового следа студента.

Демонстрируемые приёмы онтологического моделирования рабочих учебных планов образовательных программ показывают широкие возможности в отображении различных парадигм организации и реализации подготовки кадров.

На рис. 4 приведен пример онтографа дисциплин участников образовательного процесса.

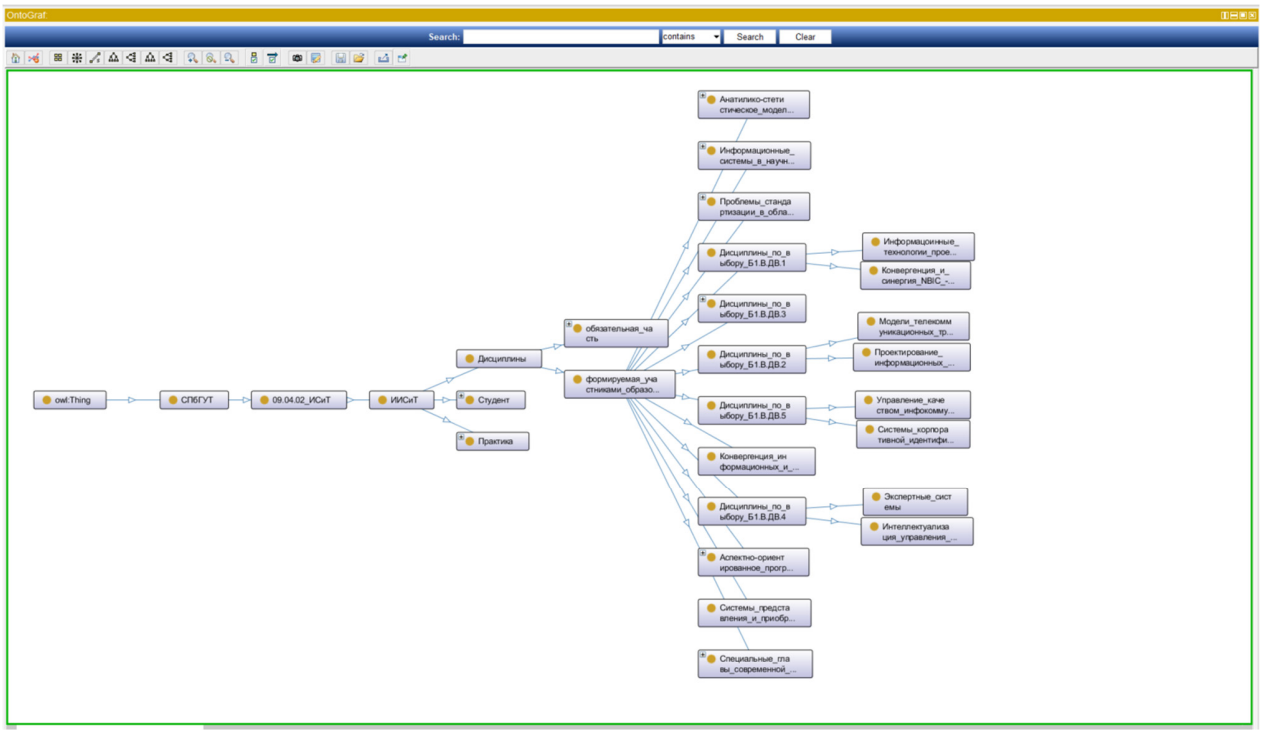


Рис. 4. Онтограф дисциплин участников образовательного процесса.

На рис. 5 продемонстрирован процесс подготовки онтологических моделей рабочих учебных планов для сравнительного анализа.

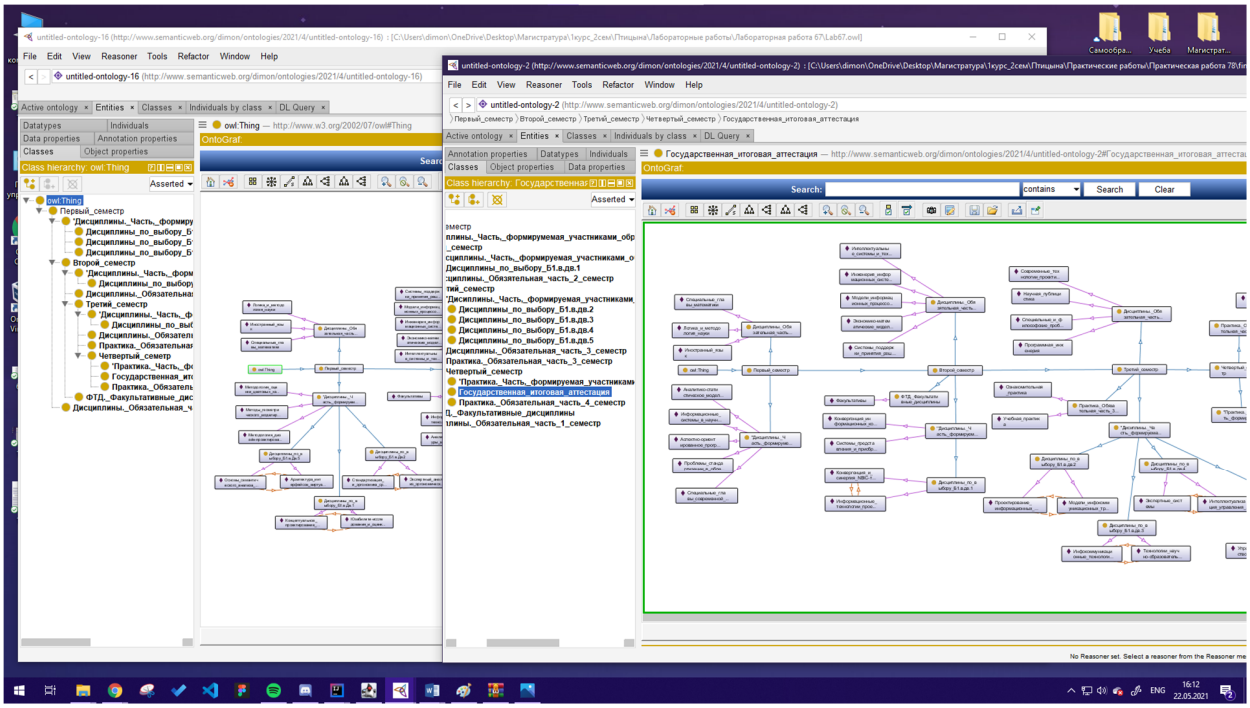


Рис.5. Подготовка онтологических моделей рабочих учебных планов для сравнительного анализа.

При онтологическом подходе к сопровождению жизненного цикла образовательных программ по информационной безопасности одновременно с интеллектуализацией процессов создания, обработки, анализа и представления рабочих учебных планов предоставляются обширные возможности в вариациях представлений персональных образовательных траекторий в глобальном информационном пространстве.

На рис. 6 представлен пример сравнения онтологий рабочих учебных планов двух образовательных программ.

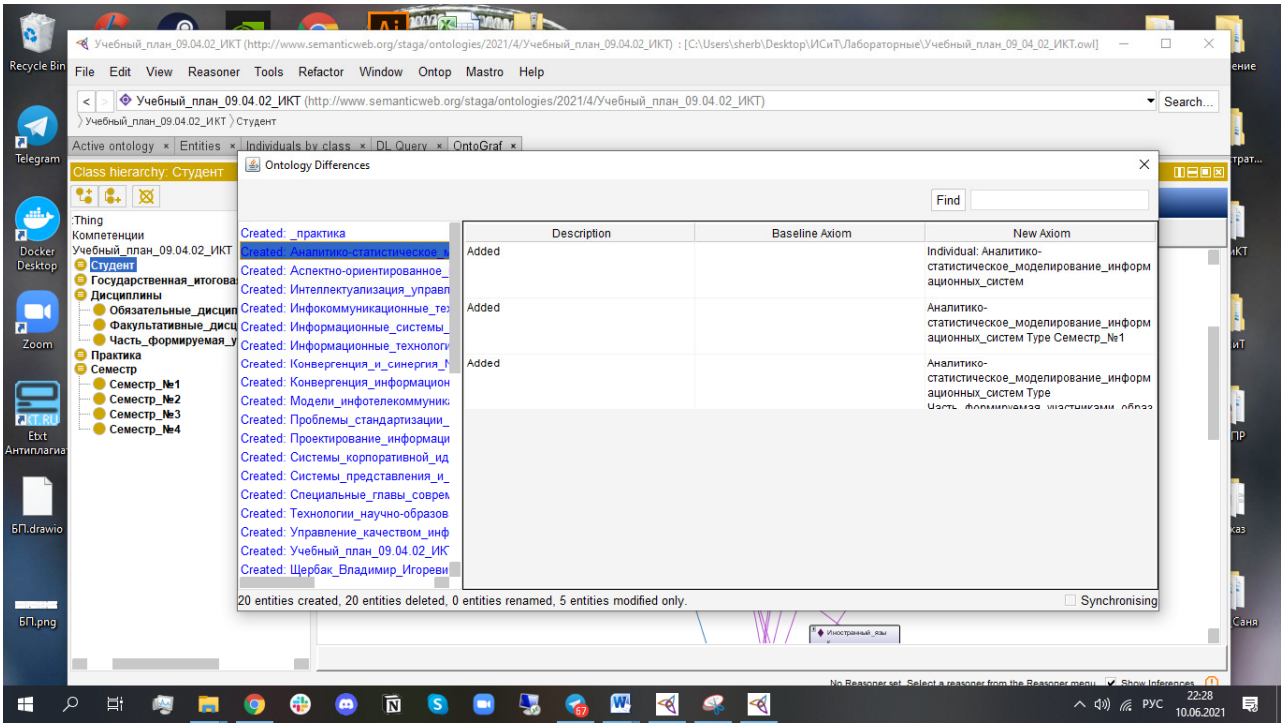


Рис. 6. Пример сравнения онтологий рабочих планов двух образовательных программ.

Указанное преимущество имеет повышенную значимость для субъектов экономики, осуществляющих целевую подготовку кадров в университетах, а также для абитуриентов разного уровня подготовки в сфере профессионального образования для принятия решения о выборе образовательной программы основного или дополнительного образования.

Научная новизна представляемых результатов выполненных исследований заключается в сквозном объединении интеллектуальных автоматизированных процессов создания, представления, анализа и критериального выбора компонентов технологического сопровождения образовательных программ по информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Птицына Л. К., Птицын А. В. Расширение знаний о защите информации в образовательных программах магистратуры // Новые информационные технологии в образовании и науке: материалы XII междунар. науч.-практ. конф., Екатеринбург, 25 февраля – 1 марта 2019 г.: // ФГАОУ ВО «Рос. гос. проф.-пед. ун-т». Екатеринбург, 2019. С. 629-635.
2. Птицына Л. К., Птицын А. В. Технологический базис формирования кадрового обеспечения цифровой экономики // Новые информационные технологии в образовании: материалы XI междунар. науч.-практ. конф., Екатеринбург, 27 февраля – 3 марта 2018 г.: // ФГ АОУ ВО «Рос. гос. проф.-пед. ун-т». Екатеринбург, 2018. С. 583-589.
3. Птицына Л. К., Птицын А. В. Интеллектуализация систематизации профессиональных стандартов для научно-образовательной сферы // Наука. Информатизация. Технологии. Образование : материалы XIV международной научно-практической конференции «Новые информационные технологии в образовании и науке НИТО-2021», г. Екатеринбург, 1–5 марта 2021 г. // ФГАОУ ВО «Российский государственный профессионально-педагогический университет». Екатеринбург, 2021. 576 с. (С. 151-157).
4. Птицына Л. К., Птицын А. В., Птицын Н. А. Индивидуализация и персонализация процессов формирования компетенций при подготовке кадров для сферы ИТ-технологий // Современное образование: содержание, технологии, качество. Материалы XXVI международной научно-методической конференции. СПб.: Изд-во СПбГЭТУ. 2020. С. 466-468.
5. Птицына Л. К., Птицын Н. А., Птицын А. В. Интеллектуализация определения цифрового следа при персонализации подготовки кадров для цифровой экономики // Наука. Информатизация. Технологии. Образование : материалы XIV международной научно-практической конференции «Новые информационные технологии в образовании и науке НИТО-2021», г. Екатеринбург, 1–5 марта 2021 г. // ФГАОУ ВО «Российский государственный профессионально-педагогический университет». Екатеринбург, 2021. С. 144-151.
6. Птицына Л. К., Птицын Н. А., Птицын А. В. Онтологическое представление и обработка знаний об индивидуализации и персонализации образовательных траекторий // Современное образование: содержание, технологии, качество. Материалы XXVII международной научно-методической конференции. СПб.: Изд-во СПбГЭТУ. 2021. С. 391-393.

УДК 378

ОСОБЕННОСТИ ЦИФРОВИЗАЦИИ ОБРАЗОВАНИЯ: НАПРАВЛЕНИЯ, ВОЗМОЖНОСТИ

Шередекина Оксана Анатольевна, Михайлова Ольга Юрьевна, Пятницкий Алексей Николаевич
Санкт-Петербургский политехнической университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, Россия, 195251
e-mail: World.Maria@hotmail.com

Аннотация. В тезисах доклада предпринята попытка рассмотреть одно из приоритетных направлений государственной политики в современной России – цифровизацию, которая доминирует в дискурсе практически всех сфер человеческой мысли и деятельности, в частности, в образовании, являющейся самой медленной областью в отношении внедрения цифровых технологий, имеющей тенденцию к сохранению устаревших методов обучения и образовательных практик.

Ключевые слова: цифровизация, образование, цифровая образовательная среда, перспективное направление, цифровая технология.

FEATURES OF EDUCATION DIGITALIZATION: DIRECTIONS, OPPORTUNITIES

Sheredekina Oksana, Mikhailova Olga, Pyatnitsky Alexey
Peter the Great St.Petersburg Polytechnic University
Polytechnicheskaya St., 29, St.Petersburg, Russia, 195251
e-mail: World.Maria@hotmail.com

Abstract. In the theses of the report, an attempt is made to consider one of the priority directions of state policy in modern Russia - digitalization, which dominates the discourse of almost all spheres of human thought and activity, in particular, in education, which is the slowest area in relation to the introduction of digital technologies, which tends to persist. outdated teaching methods and educational practices.

Keywords: digitalization, education, digital educational environment, promising direction, digital technology.

Пространственные измерения реального образования становятся по-настоящему многомерным и открытым, любой участник образовательного процесса может участвовать в творческой деятельности, предъявлять результаты своего творчества, вступая во взаимодействие с сообществами, объединяющими людей из различных точек планеты посредством такого эволюционирующего инструмента как цифровые технологии [1-3] (рис. 1).

Рис. 1. Педагогический потенциал информационно-образовательной среды

Первое, с чего нужно начать – это с ответа на вопрос: зачем, для чего, с какой целью необходима цифровизация? Исследователю необходимо задать себе этот вопрос в разных интерпретациях и искать правдивый и честный ответ, почему. Потому что это модно? Или потому что страшно упустить? Есть даже такая болезнь FoMO (Fear of missing out) – боязнь что-то упустить, что-то потерять. Если это действительно так, то, наверное, не нужно, лучше этот вопрос отложить.

Благодаря полной оцифровке образовательной среды (включая оборудование, класс и т.д.), ресурсов (таких как книги, раздаточные материалы, учебные материалы и т.д.) и приложений (включая обучение, управление, обслуживание, офис и т.д.), на основе традиционного кампуса строится цифровое пространство, чтобы расширить временные и пространственные измерения реального кампуса, повысить его операционную эффективность, профессиональный уровень, расширить его бизнес-функции, достичь эффективности управления им (Рис. 2.).

Рис. 2. Возможности цифровой трансформации в современном мире

Начинать цифровизацию стоит в том случае, если исследователь понимает, что проигрывает по технологиям, по скорости, по клиентскому сервису, по внутренним оптимизационным вещам. Исследователю не стоит откладывать, если он понимает, что цифровые технологии могут повлиять на две ключевые вещи в вашей компании: 1. Расходы. Прекрасно, если цифровизация и технологии сократят затраты. 2. Выручка, прибыль. Отлично, если исследователь сможет с помощью цифровизации повысить выручку на единицу товара, единицу клиента, зарабатывать больше валового, принять больше клиентов, повысить средний чек, вернуть себе больше клиентов. Если исследователь может работать с теми клиентскими и бизнесовыми метриками, на которые сможет воздействовать с помощью новых технологий, с помощью цифровизации, и с помощью работы с данными.

Для бизнес-компаний, работающих в B2C, привлечение новых клиентов, работа с ними является детальным процессом. И представляется важным принимать решения на основе данных и цифр, а не на основе каких-то интуитивных предположений, где и в каких каналах можно кого-то привлечь. Бизнес-компании не используют инструменты, которые не смогут оцифровать, только те, где есть цифровые метрики.

Когда начинается трансформация, любая, в том числе цифровая, людям ближе не изменения, а статус-кво – стабильность, устойчивость. Поэтому усредненная корпоративная культура отторгает любые изменения, любую трансформацию, потому что считает ее чужеродной, вредной, опасной, нарушающей статус-кво. Каждому человеку эмоционально неприятно ощущать изменения на себе. Поэтому первое, что в организации необходимо из ресурсов, в частности, в образовательной организации – это человеческие ресурсы, которые включают в себя и компетенцию, и культуру. Либо способность нарастить такие компетенции или поменять культуру.

Цифровизация не может существовать сама по себе. У организации должно быть что-то, к чему она применяется. Это могут быть станки, оборудование, процессы, клиенты, данные. Исследователь должен посмотреть, к чему он будет применять новые технологии и цифровизацию [4]. Если окажется, что точек приложения усилий нет или немного, ничего не получится. Исследователю необходимо представлять себе цифровизацию как мультипликатор, на который ему нужно будет умножать собственный бизнес. Невозможно, имея нулевую или низкую базу, умножить ее на какой-то большой мультипликатор.

Некоторые исследователи рассматривают цифровизацию как инвест-бюджет, некоторые как операционные расходы, некоторые зашивают это внутрь операционного бизнеса. Рекомендуется выделять бюджет на цифровизацию как отдельный инвестиционный проект и отслеживать его по инвестиционной модели [5-7]. Также необходимо смотреть на четкие метрики ARR, возврата на инвестиции. Если у компании есть объект трансформации и есть бюджет на его трансформацию, у исследователя должно быть понимание, в какой момент это выйдет в ноль, когда это начнет сказываться либо на оптимизации затрат, либо на повышении прибыли. Компетенции, точки приложения усилий и отдельный бюджет являются ключевыми вещами, которые нужны исследователю. Все

остальное – технологии, подрядчики, инфраструктура, – вторично. Оно в любом случае потребуется, но первые приоритетные ресурсы – это люди, деньги и точки приложения усилий (Рис. 3) [8].

Рис. 3. Модель цифровой трансформации вуза

Персонализированное образование, позволяющее выстраивать личный образовательный маршрут – еще одно перспективное направление развития цифровой образовательной сферы. Другим перспективным направлением развития цифровой образовательной сферы является использование технологий геймификации.

Цифровизация образования является самой медленной областью в отношении внедрения цифровых технологий, имеющей тенденцию к сохранению устаревших методов обучения и образовательных практик. Начинать цифровизацию рекомендуется с ответа на вопрос: «зачем, для чего исследователю нужна она». Цифровизация – это набор технологий и процессов, которые должны повлиять на бизнес и не более того. Исследователю необходимо представлять себе цифровизацию как мультипликатор, на который он будет умножать собственный бизнес. Компетенции, точка приложения усилий и отдельный бюджет – это ключевые вещи, которые нужны исследователю. Все остальное – технологии, подрядчики, инфраструктура – вторично. Укоренившиеся в социуме ментальные установки, замедляют цифровизацию образования. Образование должно идти в ногу со временем, а учебные заведения также должны своевременно внедрять цифровые технологии для удовлетворения растущих потребностей участников образовательной сферы, принимая во внимание, сохранение лучшего опыта традиционного образования.

СПИСОК ЛИТЕРАТУРЫ

1. Жигадло В. Э., Одинокая М. А., Шередекина О.А. Использование технологий мобильного обучения в самостоятельной работе студента в техническом вузе // Современные информационные технологии и ИТ-образование. 2014, № 3. С. 68-72.
2. Основы компетентностного подхода в профессиональной подготовке специалиста в российской системе образования: учебное пособие / М.А. Одинокая. – Москва: РУСНАЙС, 2019. 128 с.
3. Жигадло В. Э., Одинокая М. А. Использование технологии учебных подкастов при обучении языку хинди в техническом вузе как средства повышения качества дополнительного гуманитарного образования //Язык и культура, 2017, №. 38.
4. Яковлева Е. В. Важнейшие тенденции устойчивого развития профессионального образования // МНИЖ, 2021, № 6-4 (108). С. 200-205.
5. Алибаева Г .М., Стеблякова А. А., Костина И. А. Цифровизация экономики как генеральное направление НТП и качественное изменение системы образования высшей школы // Вестник Донецкого педагогического института, 2018, № 3. С. 298-307.
6. Халяпин А. А., Усачева Ю. А., Руденко А .И. Методы информационного менеджмента для оценки эффективности инвестиционных проектов в эпоху цифровизации // Вестник академии знаний, 2021, № 2(43). С. 427-433.
7. Медникова О. В., Матвиевская Т. В. Дигитализация рынка транспорта и логистики: интеграция информационных систем. Российский опыт внедрения цифровых технологий в организации логистических процессов // Вестник академии знаний, 2021, № 4(45). С. 197-204.
8. Модель цифровой трансформации вуза https://static.tildacdn.com/tild3031-6134-4138-a464-396139333138/67624480_21585781209.jpg

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОЛОГИИ

УДК 004.67; 004.89; 621.3.068

ЦИФРОВИЗАЦИЯ – ОПАСНОСТИ ВНЕДРЕНИЯ И РАЗВИТИЯ

Витковский Владимир Валентинович[1], Горохов Владимир Леонидович[2], Бузников Анатолий Алексеевич[2]
[1] Специальная астрофизическая обсерватория РАН
пос. Нижний Архыз, Карачаево-Черкесская республика, 369167, Россия
[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: vvv@sao.ru, vlgorohov@mail.ru

Аннотация. Рассматриваются опасности трактовок термина «цифровизация», принятые различными научными направлениями.

Ключевые слова: цифровизация; телекоммуникационные сети; интернет; браузеры; сайты; блоги; коды с открытыми ключами; облака; машинное обучение; системы распределённого реестра.

DIGITALIZATION – THE DANGERS OF IMPLEMENTATION AND DEVELOPMENT

Vitkovsky Vladimir[1] , Gorokhov Vladimir[2] , Buznikov Anatoly[2]
[1] Special Astrophysical Observatory of the Russian Academy of Sciences
Nizhny Arkhyz village, Karachay-Cherkessia, 369167, Russia
[2] Saint Petersburg State Electrotechnical University
5 Professor Popov St, St.-Petersburg, 197376, Russia
e-mails: vvv@sao.ru, vlgorohov@mail.ru

Abstract. The dangers of interpretations of the term digitalization adopted by various scientific directions are considered.

Keywords: digitalization; telecommunication networks; Internet; browsers; websites; blogs; public key codes; clouds; machine learning; distributed registry systems.

Введение. Цифровизация из фантазий, разговоров и дискуссий быстро и прочно вошла в общественную жизнь, закреплена правительственными постановлениями и поддержана государственным финансированием. Посыпались проекты цифровой трансформации в любой прикладной области: от нефтегазового сектора до образования, оптимизации бизнес-процессов, больших данных (Big Data), машинного обучения (Machine Learning), интернета вещей (Internet of Things) и т.д., и т.п., и др., и проч. Научное сообщество делает попытки формализации этого явления. На этом этапе появилась опасность непонимания и радикально отличающейся трактовки смысла термина цифровизация в точных и гуманитарных науках. Если первоначально бурное развитие вычислительной техники и телекоммуникационных технологий позволило математикам и инженерам ввести термин «цифровизация», который отражал сущность технических явлений, то огромное влияние информационных технологий на общество заставило социологов и политологов ввести социологические термины «информационное общество», «коммуникации в социуме» и проч. В рамках социологических и политологических наук цифровизация стала отражать определенный круг социальных явлений. Аналогично поступили и экономисты, введя термин «цифровая экономика» и отделив это понятие от реальной экономики. Опасность заключаются в том, что эти термины в разных науках трактуются по-разному, что приводит к возможным трагическим недоразумениям, которые могут привести к серьезным технологическим, экономическим и социальным катастрофам. Возникают угрозы безопасности жизнедеятельности на уровне социума, экономики, экологии и техники.

Плюсы и минусы. Дело в том, что достижения вычислительной техники и компьютерных наук (обработка и передача данных в цифровом представлении) создали такие технические новации (информационно-телекоммуникационные сети, интернет, браузеры, сайты, блоги, коды с открытыми ключами, облака, машинное обучение, системы распределённого реестра), которые привели к фундаментальным социальным явлениям типа социальных сетей и криптовалюты, которые при неправильном понимании сути этих достижений могут привести к техносферным, экологическим и социальным катастрофам. Принятый обществом термин цифровизация включает в

себя оба эти явления (технику обработки цифровых данных и социальные последствия внедрения этой техники). По степени доступности и активного использования цифровой экономики: электронной коммерции, интернет-банкинг, электронные платежи, интернет-рекламу и электронный доступ к государственным услугам определяют DEI, Digital Evolution Index - индекс цифровизации государства [1, 2]. Однако не следует забывать, что эти социальные явления помимо положительных последствий несут и огромную, пока плохо предсказуемую угрозу для социума. Отчасти причина многих негативных социальных последствий, кроется в природе технических новаций. Недопонимание гуманитариями технических особенностей, а подчас и технической сути процессов цифровизации является серьезной техносферной опасностью. Этот факт был отмечен в работе Ричарда Кларка и Роберта Нейка «Третья мировая война, какой она будет?» [3]. Аналогичная ситуация уже возникала в атомной промышленности и потребовались серьезные усилия со стороны инженеров и физиков для разъяснения этого недопонимания гуманитариям.

Термины и смысл. Для преодоления сформулированных выше опасностей требуется, прежде всего, тщательно установить особенности трактовки ряда терминов, принятых в гуманитарных и технических науках. Требуется внимательное прочтение и адекватная трактовка ключевых административных документов, определяющих процессы цифровизации. Разумеется, это трудная задача, требующая междисциплинарной эрудиции, но другого пути нет! Сделаем первые робкие усилия, чтобы начать решение этой трудной задачи с термина ставшего ключевым – цифровизация на примере анализа текстов ряда руководящих административных документов. Утверждённая Распоряжением Правительства РФ № 1632-р от 28 июля 2017 г. Программа «Цифровая экономика Российской Федерации» определяет данные в цифровой форме ключевым фактором производства во всех сферах социально-экономической деятельности, что по убеждению её разработчиков повысит конкурентоспособность страны и качество жизни граждан, а также обеспечит экономический рост и национальный суверенитет. Целями Программы были объявлены «создание экосистемы цифровой экономики Российской Федерации», в которой будут реализованы «условия для развития общества знаний». В рамках программы «Цифровая экономика» определено девять, названных «сквозными», ключевых технологий, причём любая из них может полностью поменять правила игры сразу в нескольких отраслях экономики. Для реализации и внедрения каждой из них подготовлены поэтапные планы развития и меры организационной, финансовой и юридической поддержки («дорожные карты»).

В целом, осознание требующих решения проблем цифровизации экономики выглядит удовлетворительно, хотя к тексту Программы можно предъявлять терминологические и смысловые претензии. К примеру, основными «сквозными цифровыми» технологиями, объявленными в Программе, являются в весьма эклектическом наборе: «большие данные; нейротехнологии и искусственный интеллект; системы распределённого реестра; квантовые технологии; новые производственные технологии; промышленный интернет; компоненты робототехники и сенсорика; технологии беспроводной связи; технологии виртуальной и дополненной реальностей». Иерархия эклектики начинается с самого новообразованного понятия «сквозные цифровые технологии». Под него можно подложить любую технологию, где хоть раз появляется цифра. Следующий уровень – это сами термины, в основном неустоявшиеся и неоднозначные. Если, например, «новые производственные технологии», «технологии беспроводной связи» и «большие данные» подразумевают смысловую конкретику по времени, технике или наборам данных, то «нейротехнологии» в общепринятом понимании [4] это «любые технологии, которые оказывают фундаментальное влияние на то, как люди понимают мозг и различные аспекты сознания, мыслительной деятельности, высших психических функций», а в понимании С. Шишкина, заведующего отделом Курчатовского комплекса НБИКС-технологий [5] это «создание новых технологий на основе объединения возможностей интерфейса «мозг – компьютер» и других технологий, и, прежде всего, управления компьютером с помощью взгляда».

Системы распределённого реестра распределённого реестра – это не технология, а продукт технологий, главным образом блокчейн технологии. Блокчейн (block chain) – буквально, цепь блоков, это технология, которая позволяет создавать распределённую в информационной сети многомерную книгу аналогичную бухгалтерской, которая существует в единственном экземпляре, но все страницы (блоки) которой хранятся у всех пользователей и разделяются между участниками посредством пиринговых сетей. Каждый блок имеет уникальный неизменяемый параметр идентификации – хэш-сумму. Для защиты хэш-сумм в блокчейн применяется два алгоритма – Proof of Work (PoW, доказательство работы) и Proof of Stake (PoS, доказательство владения). Все блоки расположены в определённой последовательности, изменение которой невозможно. В этой книге можно регистрировать любую информацию и/или любые действия, но внести подделать или внести изменения в записи невозможно, поскольку система в реальном времени сканирует страницы всех пользователей и не допускает несанкционированных изменений. Так в основанных на технологии блокчейн криптовалютах сохраняются данные об их объёме и всех транзакциях. Эта технология применима во многих сферах человеческой деятельности, в частности для создания распределённых реестров. Ещё хуже обстоит дело с «сенсорикой» [6]. Сенсо́рика (лат. sensus, «восприятие») — категория, описывающая непосредственное восприятие ощущений, внешних воздействий. В физиологии сенсорика — функция нервной системы, заключающаяся в восприятии раздражителей, выполняемая при помощи сенсорной системы. В аспектонике и соционике сенсорика — тип воспринимаемой человеком информации, обобщённое название для аспектов «белая сенсорика» (информация об ощущении) и «чёрная сенсорика» (информация о форме). В технике сенсорика — совокупность первичных преобразователей, сенсоров, преобразующих внешнее воздействие,

являющееся контролируемым параметром, в удобный для обработки сигнал. Какой технологический смысл вложен в это понятие, остаётся только догадываться. Можно только понадеяться, что вовлечённые в программу передовые частные и государственные фирмы, корпорации, центры, НИИ, университеты, учёные и инженеры смогут осознать смысл и наполнить содержанием написанные слова.

Немного истории. Не так уж давно Борис Ельцин, не особенно разбираясь в отличии девальвации от деноминации и плохо понимая происходящее в экономике, понадеялся, что как-то все «разрулится» само собой. Не разрулилось. Если заглянуть в прошлое подальше, увидим ещё раз, что «новое – это хорошо забытое старое». Первое предложение создать в СССР общенациональную компьютерную сеть многоцелевого назначения для экономического управления в масштабе всей страны, поступило от инженер-полковника ВС СССР Анатолия Ивановича Китова [7]. Идею подхватил В. М. Глушков, академик АН СССР, герой социалистического труда, главный редактор журнала «Кибернетика», вице-президент АН УССР и проч., и проч. [8]. Ему удалось убедить Н. С. Хрущёва в необходимости создания ОГАС (Общегосударственная Автоматизированная Система Управления Хозяйством) для скорейшего построения коммунизма в СССР. Проект ОГАС — простое и элегантное средство создания полного коммунизма. Глушковым предполагалось создание трехступенчатой системы обработки информации и управления экономикой. Первичная ступень — уровень отдельного предприятия. В режиме реального времени автоматически собирается вся необходимая информация о выпускаемой продукции, состоянии дел на складах, количестве рабочих рук и т. д. Вторая ступень — отраслевой и территориальный уровень. Вся информация, собранная на отдельных предприятиях, перенаправляется в промежуточный центр, где обрабатывается и также доступна для восприятия в удобной форме. В общем-то, повторяется ситуация с отдельной производственной единицей, но на более высоком уровне. Наконец, третья и последняя ступень — управление всей экономикой из центра. Преимущества такой системы казались очевидными. Первое, бросающееся в глаза — сокращение бюрократического аппарата. Все очень просто: раз машина может выполнять роль советских плановиков (собирать и обрабатывать информацию), да еще и лучше, то бюрократический аппарат становится не нужен. Второе, вытекающее из первого — это полная победа над дефицитом. Машина, учитывающая в реальном времени всю экономическую информацию, позволяет эффективно планировать выпуск необходимой продукции. Третье преимущество — преодоление необходимости использования денег, т.е. прямой переход к коммунизму. Однако, этот проект так никогда и не был реализован. Вместо него начались реформы Косыгина, направленные на увеличение роли хозрасчета в советском хозяйстве и, как следствие — к неуправляемому расцвету товарно-денежных отношений, что, в конечном счёте, сыграло свою роль в разрушении СССР.

Взгляд за рубеж. Важность искусственного интеллекта и прочих современных цифровых технологий хорошо понимают и на высшем государственном уровне в странах, которые претендуют на звание технологических держав. Администрация Барака Обамы ещё в 2016 году выпустила несколько докладов о будущем ИИ, а в 2018 году в эту гонку официально вступил Китай – заявив о задаче к 2030 году довести объем рынка технологий ИИ до $150 млрд. Фактически, цифровизация, как в своё время Интернет, осуществляется неопределённым кругом лиц, организаций и государств. При этом детерминировано направлять и управлять развитием процесса не в состоянии ни государство, ни политики, ни чиновники, ни бизнесмены. Можно утверждать, что здесь работают неотвратимые механизмы эволюции сложных больших систем. Сервисами технологических гигантов, таких, как Facebook, Google и Microsoft, пользуются миллиарды людей в мире. Однако, по мнению Майкла Квета [9], крупные американские ИТ-компании становятся монополистами отрасли в развивающихся странах Южного полушария. Способствуют этому их значительные финансовые и технические ресурсы. Он назвал поведение корпораций «цифровым колониализмом», сравнив его с поведением европейских государств в XVI–XX веках, когда они захватывали и эксплуатировали экономически менее развитые народы. Помимо этого, корпорации аккумулируют в своих руках данные о пользователях, которые в дальнейшем обрабатываются и используются ими в коммерческих целях. У более бедных стран нет экономических возможностей создавать свои компании в сфере высоких технологий, которые смогли бы конкурировать с крупными корпорациями Кремниевой долины.

В странах Южной Африки Google и Facebook доминируют на рынке онлайн-рекламы, вытесняя местных игроков медиарынка. В этом, по мнению авторов статьи, и заключается характерная черта цифрового колониализма. Он развивает технологическую экосистему, целью которой является получение прибыли. Помимо этого, Google благодаря многочисленным сервисам обладает огромным массивом данных о пользователях по всему миру. Крупнейшая социальная сеть Facebook функционирует как «информационный посредник» между пользователями. Чтобы поделиться информацией или фотографией со своими друзьями, их необходимо сначала загрузить в Facebook. Бывший сотрудник ЦРУ и АНБ Эдвард Сноуден заявлял, что компания позволяла американским спецслужбам следить за пользователями своих программ Outlook, Skype и SkyDrive.

Заключение. Национальные проекты задают общую архитектурную логику взаимодействия людей, государства и бизнеса в цифровой экономике. В том числе логику так называемых цифровых профилей. И общая логика — это правильно не только с точки зрения обеспечения безопасности, но и с точки зрения обеспечения обмена данными, как между государственными органами, так и между бизнесом и гражданами. Цифровизация — это историческая эволюционная неизбежность, а не пожелание людей, бизнесменов, политиков или государства. Невовлечённый в цифровизацию субъект обречён. Что же делать политикам? Ответ давно известен

– Если движение нельзя остановить, его нужно возглавить! Но возглавить, вникая в естественнонаучный смысл этих процессов! Теперь можно сделать основной вывод из представленного выше – цифровизация неизбежна, но для осознания этого потребуются ещё очень многие усилия человеческого разума, чтобы удержаться в рамках давно известного принципа «Не Навреди».

СПИСОК ЛИТЕРАТУРЫ

1. https://sites.tufts.edu/digitalplanet/files/2020/03/DEI-LAC_Executive-Summary_27Nov2018.pdf
2. http://www.fa.ru/fil/orel/science/nirs/Documents/meroprijtij/NPS%20doklad%206.pdf
3. https://bookshake.net/b/tretya-mirovaya-voyna-kakoy-ona-budet-richard-klark
4. Нейротехнологии — Википедия (wikipedia.org)
5. https://intalent.pro/interview/sergey-shishkin-o-budushchem-neyrotehnologiy-i-interfeysah-mozg-kompyuter.html
6. https://dic.academic.ru/dic.nsf/ruwiki/681778
7. http://magazines.russ.ru/nz/2011/1/ge4.html
8.https://statehistory.ru/5697/Akademik-V-M-Glushkov-i-proekt-sozdaniya-printsipialno-novoy--avtomatizirovannoy--sistemy-upravleniya-sovetskoy-ekonomikoy-v-1963-1965-gg/
9. https://www.aljazeera.com/opinions/2019/3/13/digital-colonialism-is-threatening-the-global-south/

УДК 504.064.37

ОПТИЧЕСКИЕ ХАРАКТЕРИСТИКИ МАЛЫХ ГОРОДСКИХ ВОДОЕМОВ КАК ПОКАЗАТЕЛЬ ИХ ЭКОЛОГИЧЕСКОГО СОСТОЯНИЯ

Горяинов Виктор Сергеевич, Антоненко Ксения Георгиевна, Хасенова Мариям, Бузников Анатолий Алексеевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: vsgoriainov@etu.ru, mariyam-98@mail.ru, kgantonenko@yandex.ru, aabuznikov@mail.ru

Аннотация. В статье описаны методы, использованные для измерения спектров отражения малых городских водоемов Санкт-Петербурга при помощи полевого спектрометра, а также спектров ослабления излучения в пробах вод с использованием многократного прохождения излучения через кювету. Полученные результаты позволяют разделить проточные и стоячие водоемы по форме спектров отражения и ослабления, а также оценивать экологическое состояние водоемов по близости их оптических характеристик к одной из двух групп.

Ключевые слова: городские водоемы; малые водоемы; эвтрофикация; дистанционное зондирование; спектры отражения; спектры ослабления; полевой спектрометр; волоконный спектрометр.

OPTICAL CHARACTERISTICS OF MINOR URBAN WATER BODIES AS AN INDICATOR OF THEIR ECOLOGICAL STATE

Goryainov Viktor, Antonenko Kseniya, Khasenova Mariyam, Buznikov Anatoliy
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: vsgoriainov@etu.ru, mariyam-98@mail.ru, kgantonenko@yandex.ru, aabuznikov@mail.ru

Abstract. The article describes the methods used to measure the reflection spectra of small urban water bodies of St. Petersburg using a field spectrometer, as well as the spectra of radiation attenuation in water samples using multiple transmission of radiation through a cuvette. The results obtained make it possible to separate flowing and stagnant water bodies according to the shape of the reflection and attenuation spectra, as well as to assess the ecological state of water bodies judging by closeness of their optical characteristics to one of the two groups.

Keywords: urban water bodies; minor water bodies; eutrophication; remote sensing; reflection spectra; attenuation spectra; field spectrometer; fiber spectrometer.

Введение. В современных условиях малые городские и пригородные водоемы испытывают воздействие целого ряда антропогенных факторов стресса. Проточные водоемы – ручьи, малые реки – используются для отведения канализационных стоков (в Санкт-Петербурге примером в этом отношении может служить Муринский ручей, в последние несколько лет привлекающий внимание как объект исследований химическими, гидрофизическими и гидрооптическими методами [1-4]). Стоячие воды (пруды, малые озера) испытывают рекреационную нагрузку [5], загрязнение смывом с прилегающих автомобильных дорог и пестицидами, а кроме того, возможные негативные последствия перепланировки, осушения, водной подпитки и других антропогенных преобразований [6]. Замедленный водообмен повышает склонность таких водоемов к эвтрофикации и «цветению» воды по сравнению с естественными водами [5, 6].

В связи с вышесказанным приобретает актуальность регулярный мониторинг влияния антропогенных факторов и современных изменений климата на экологическое состояние малых городских и пригородных водоемов, в том числе с применением дистанционных методов. Оптические дистанционные методы, основанные на

использовании спектров отражения солнечного излучения водной поверхностью, отличаются меньшей трудоемкостью по сравнению с контактными гидрохимическими методами и обеспечивают одновременный охват большей акватории. Тем не менее, данные спектральных приборов спутникового базирования малопригодны для исследования оптических характеристик малых городских и пригородных водоемов из-за малого пространственного разрешения, влияния облачности и окружающей растительности. С учетом этого с осени 2020 года по настоящее время авторы провели серию полевых и лабораторных измерений оптических характеристик некоторых водоемов Санкт-Петербурга и Ленинградской области в рамках проекта «Водоемы–2020». В статье описаны использованные методы и некоторые результаты измерений.

Объекты исследования. Всего исследование охватило 17 водоемов Санкт-Петербурга и Ленинградской области, среди которых 3 пруда, 2 малых озера, а остальные водоемы относятся к системе дельты Невы. В табл. 1 приведены обозначения водоемов, дата, широта и долгота (определенные при помощи GPS), а также комментарий, описывающий приблизительное место проведения исследования. Следует отметить, что не для всех водоемов из таблицы далее приведены результаты и полевых, и лабораторных измерений.

Пробы воды отбирались в пластиковые емкости объемом 0,5 – 1 л, предварительно промытые проточной водой. По возможности лабораторные измерения проводились в день отбора проб, в противном случае последние хранились в холодильнике, при температуре не выше +5 °С, в течение 2 – 3 дней.

Полевые съемки спектров отражения малых водоемов. Для съемки спектров отражения природных вод в полевых условиях использовался портативный спектрометр «Радуга» [7], обеспечивающий спектральное разрешение не хуже 1 нм в диапазоне длин волн 400 – 1100 нм за счет применения вогнутой дифракционной решетки (120 штр/мм) в оптической схеме на основе модифицированного круга Роуланда. Фокусное расстояние входного объектива составляет 58 мм, а угол поля зрения спектрометра равен 12' × 5°. Кремниевая ПЗС-линейка Toshiba TCD1304AP с 3648 пикселями размером 80 × 200 мкм используется в качестве фотоприемника, а сигнал с нее обрабатывается цифровым сигнальным процессором eZdsp F2802 с микроконтроллером TMS320F2808. Управление спектрометром и сохранение данных для дальнейшей обработки осуществляет персональный компьютер, связанный с прибором по последовательному порту.

Таблица 1

Места проведения спектральных съемок и отбора проб

Обозначение	Водоем	Дата	Широта	Долгота	Комментарий
БН	р. Большая Невка	23.09.20	59,97402	30,32733	Аптекарская набережная
ГК	Гребной канал	07.10.20	59,97585	30,22047	Крестовский о-в
ИП	Иорданский пруд	30.09.20	59,99366	30,33595	Парк СПбГЛТУ
МК	Морской канал	23.09.20	59,8947	30,2104	Канонерский о-в
МН	р. Малая Невка	07.10.20	59,9669	30,2422	Яхт-клуб «Крестовский»
РК-осень	р. Карповка	07.10.20	59,96752	30,33002	вблизи Аптекарского моста
РК-весна	р. Карповка	12.04.21	59,96752	30,33002	вблизи Аптекарского моста
СП	Сердобольский пруд	30.09.20	59,99527	30,33198	Парк СПбГЛТУ
ЦП	Цветочный пруд	30.09.20	59,99184	30,34155	Парк СПбГЛТУ
ЧР	р. Черная речка	30.04.21	59,98197	30,32014	вблизи Головинского моста

Спектральные съемки водоемов проводились с берега, спектрометр при этом устанавливался на штативе, на высоте порядка 1,5 м над землей. Поле зрения прибора наводили на интересующую область водной поверхности, ближе к центру водоема. Вследствие этого оптическая ось спектрометра проходила весьма полого, под углом от 45° до 88° относительно нормали к поверхности водоема.

Чтобы учесть различия абсолютной облученности водной поверхности, обусловленные облачностью и временем суток, перед каждым измерением регистрировались спектры белого эталона. Коэффициент диффузного отражения определяли по формуле $R(\lambda) = [L_O(\lambda) - L_D(\lambda)] / [L_S(\lambda) - L_D(\lambda)]$, в которой $L_O(\lambda)$ – монохроматическая яркость объекта на длине волны λ; $L_S(\lambda)$ – монохроматическая яркость эталона на той же длине волны; $L_D(\lambda)$ – условная яркость, соответствующая темновому шуму в канале, на который приходится выбранная длина волны. На рис. 1 приведены примеры спектров диффузного отражения, усредненных по 16 последовательным измерениям, для некоторых из водоемов, указанных в табл. 1.

Лабораторные измерения гидрооптических характеристик. Параллельно полевым спектральным измерениям проводилось определение первичных гидрооптических характеристик отобранных проб воды в лабораторных условиях, при помощи спектрометра USB650 Red Tide производства компании Ocean Insight. Прибор построен по асимметричной скрещенной схеме Черни–Тернера с входным фокусным расстоянием 42 мм и выходным фокусным расстоянием 68 мм, обеспечивающей полуширину разрешаемой линии 2 нм в спектральном диапазоне 350 – 980 нм. Приемником излучения служит кремниевая ПЗС-линейка Sony ILX-511 из 650 элементов размером 14 × 200 мкм. Время интегрирования может быть задано в пределах от 3 мс до 65 с.

Ввиду малых концентраций оптически активных компонент в естественных водах для выделения характерных оптических признаков требуется достаточно длинный путь излучения в кювете с пробой воды. Авторами использовалась кювета длиной 50 мм с многократным прохождением излучения.

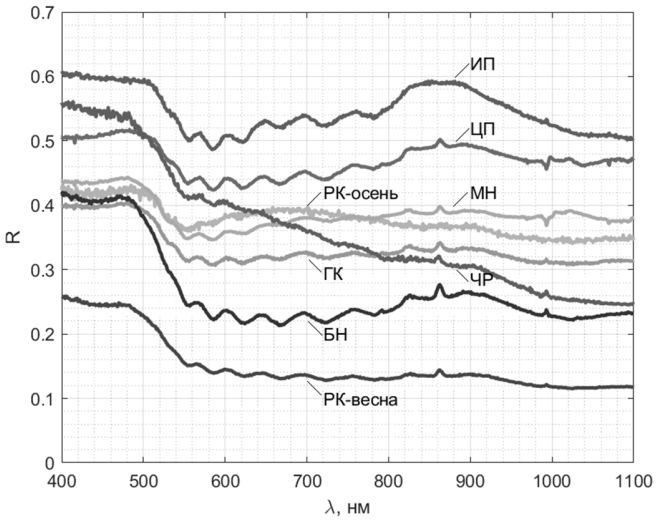


Рис. 1. Примеры спектров диффузного отражения водоемов.

В статье [8] описан первый вариант измерительной установки, в котором одно плоское зеркало обеспечивало двукратное прохождение излучения через кювету. На рис. 2 показана схема более поздней модификации, дающей трехкратное прохождение за счет отражения от двух вогнутых зеркал *8* и *9*, установленных наклонно с торцов кюветы *7*. Излучение галогенной лампы накаливания *3*, установленной в непрозрачном кожухе *2* и питающейся от стабилизированного источника *1*, фокусируется линзой *4* на торце оптического волокна *5*. Коллиматор *6* формирует узкий параллельный световой пучок. Окончательно покинув кювету, излучение проходит фильтр *10* (цветное стекло) и собирается линзой *11* в волокно *12*, а затем попадает на вход спектрометра *14*, подключенного к компьютеру *13*.

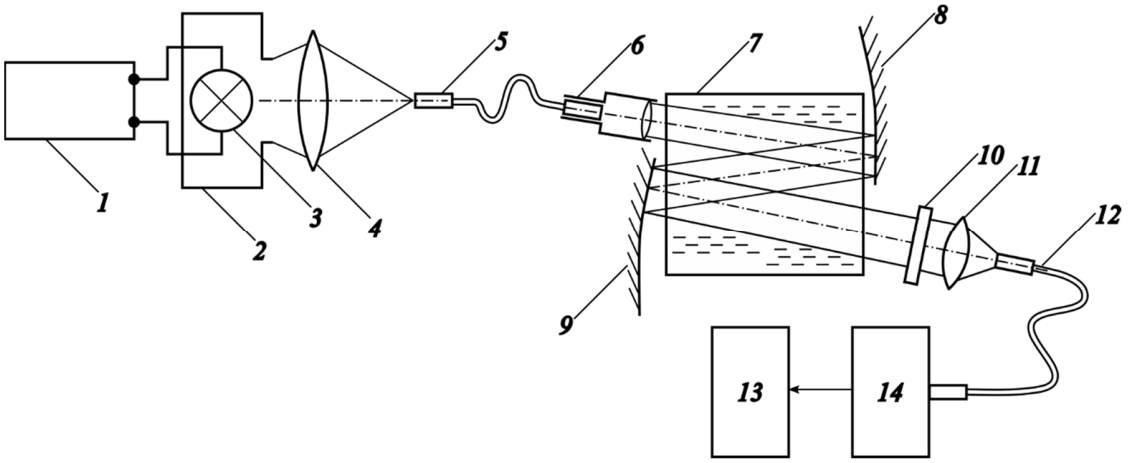


Рис. 2. Схема лабораторного измерителя первичных гидрооптических характеристик проб воды.

Перед началом каждой серии измерений кювета заполнялась дистиллированной водой, и, после необходимых регулировок установки, регистрировалось спектральное распределение интенсивности излучения $I_{0\lambda}$. Затем в кювету заливали исследуемую пробу воды и регистрировали распределение $I_{T\lambda}$ интенсивности излучения, прошедшего через нее. Спектр натурального показателя ослабления рассчитывался по формуле

$$\mu'(\lambda) = \frac{1}{3d} \ln\left(\frac{I_{0\lambda} - I_{D\lambda}}{I_{T\lambda} - I_{D\lambda}} \right), \quad (1)$$

где $3d$ – утроенная толщина кюветы (соответствующая троекратному прохождению излучения), а $I_{D\lambda}$ – интенсивность, соответствующая уровню шумов в канале при выбранной длительности интегрирования,

предварительно зарегистрированная в отсутствие излучения. На рис. 3 приведены примеры полученных спектров ослабления. Обозначения водоемов соответствуют введенным ранее.

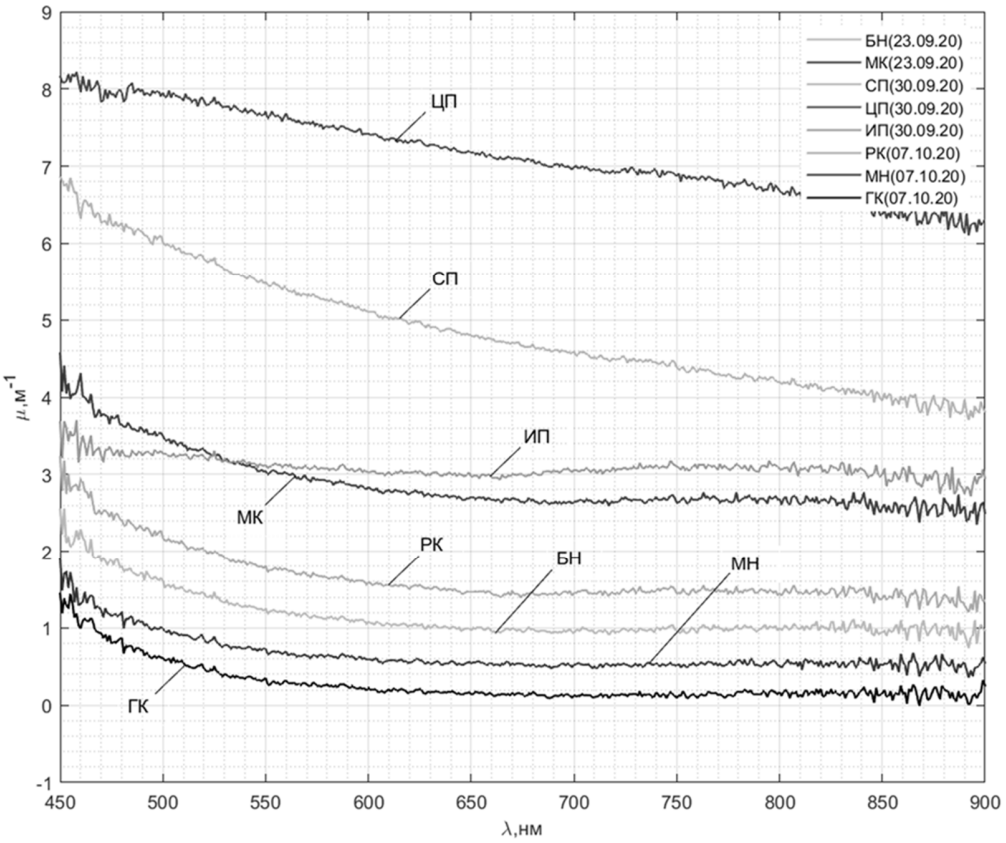


Рис. 3. Примеры спектров натурального показателя ослабления проб воды.

Анализ результатов измерений. Графики на рис. 1 показывают различие в распределениях коэффициента отражения поверхности стоячих и проточных водоемов. Для первых характерен широкий максимум рассеяния в области 800 – 1000 нм, сравнимый по значениям с коротковолновой областью. У вторых же этот максимум выражен слабо, причем некоторое исключение составляет Большая Невка в сентябре (БН).

Интерес представляет также сравнение характеристик одного и того же водоема в разное время года на примере р. Карповки (РК-осень, РК-весна). Прозрачные весенние воды реки дают почти равномерное распределение малых значений коэффициента отражения в красной и ближней инфракрасной области, в то время как коротковолновый максимум определяет их сине-зеленый цвет. В октябре, после окончания летнего «цветения» воды, длинноволновый максимум рассеяния смещен из инфракрасной области спектра в красную, что соответствует бурому цвету воды.

Аналогичное разделение спектров по типам водоемов присутствует среди результатов лабораторных измерений (рис. 3). Для проточных вод характерно быстрое уменьшение коэффициента ослабления при переходе от сине-зеленой области спектра к красной (примерно до 600 нм) и сохранение его почти неизменным на больших длинах волн. Более мутные пробы стоячих водоемов дают спектры, почти линейно убывающие на всем интервале измерений. Следует особо отметить пробу воды Иорданского пруда (ИП), для которой спектральная кривая ослабления идет практически горизонтально по сравнению с другими пробами.

Наконец, поскольку характеристики ослабления излучения в лабораторных условиях и отражения его от поверхности воды при полевых измерениях формируются одними и теми же механизмами и компонентами природных вод, то представляет интерес сравнение результатов, полученных двумя методами. На рис. 4 приведена точечная диаграмма, сравнивающая значения коэффициента отражения R и усредненные значения коэффициента ослабления μ на одной и той же длине волны. Длина волны 685 нм выбрана как соответствующая вторичному максимуму поглощения излучения хлорофиллом-*a* и максимуму его флуоресценции. Интенсивность обоих процессов является показателем содержания фитопланктона в природных водах и, косвенно, степени эвтрофикации водоема.

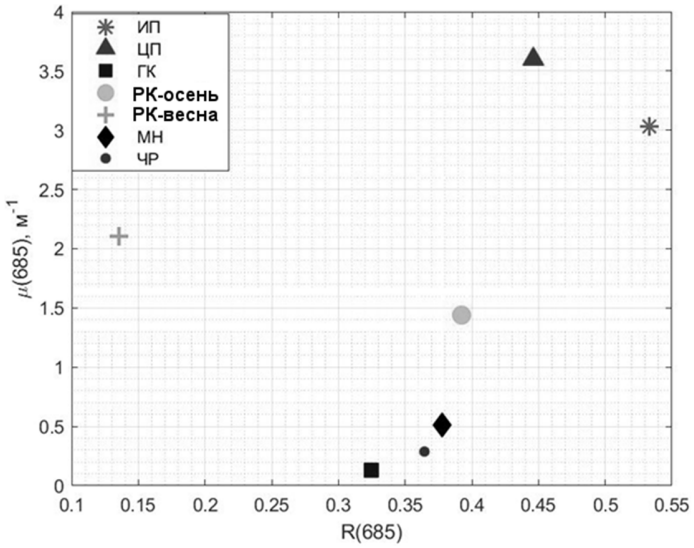


Рис. 4. Точечная диаграмма зависимости натурального показателя ослабления от коэффициента отражения (для длины волны 685 нм).

Точки для 5 из 7 рассматриваемых пар выстраиваются вдоль кривой, соответствующей степенной зависимости: с ростом коэффициента отражения квадратично возрастает показатель ослабления. Исключение составляет Иорданский пруд, у которого высокому значению μ соответствует необычно высокое значение коэффициента *R*, указывающее на большую концентрацию фитопланктона. Напротив, среднему значению μ у реки Карповки в апреле (РК-весна) соответствует малый показатель *R*. Это может свидетельствовать о преобладании поглощения над рассеянием при формировании общего показателя ослабления излучения в относительно прозрачных проточных водами в начале весны.

Заключение. Измерения спектров отражения поверхности малых городских водоемов имеют ряд специфических особенностей, в числе которых необходимость съемки вдоль пологой траектории, достаточно высокая мутность и влияние отражения излучения от дна. Несмотря на это, полученные данные позволили разделить исследуемые водоемы на две группы (проточные и стоячие) по форме спектра отражения, в частности, по степени выраженности вторичного длинноволнового максимума отражения на длинах волн 800 – 1000 нм.

Аналогичным образом при помощи лабораторного измерителя установлено различие формы спектров ослабления излучения в пробах из проточных и стоячих водоемов. Для первых характерно быстрое уменьшение ослабления в области 450 – 600 нм и слабое его изменение в инфракрасной области. Для вторых показатель ослабления убывает почти линейно по всей спектральной области измерений.

Сравнение полевых и лабораторных спектров показывает зависимость, близкую к квадратичной, между показателем ослабления и коэффициентом отражения на длине волны 685 нм. От этой зависимости отклоняются водоемы с особенно высоким содержанием фитопланктона (Иорданский пруд) и относительно прозрачные проточные воды весной (Карповка, апрель).

Таким образом, использованные методы измерений позволяют оценивать экологическое состояние исследуемого водоема, в том числе его склонность к эвтрофикации, по близости спектров отражения и ослабления излучения к одному из двух выделенных типов, характерных для проточных или стоячих водоемов.

СПИСОК ЛИТЕРАТУРЫ

1. Bondarenko E. A., Starkov V. A., Andrianova M. Ju. Fluorimetric tracing of sewage effluents in the Murinsky creek // Construction of Unique Buildings and Structures. V. 24, 2014, No. 9. P. 27-38.
2. Андросова Е. Д., Петрова И. В. Биомониторинг Муринского ручья по макрозообентосу // XXII Международный Биос-форум 2017. Сборник материалов. Санкт-Петербург. 2017. С. 124-128.
3. Иванов И. Б., Петрова И. В., Кожевникова О. Г. Продолжение гидрохимического мониторинга Муринского ручья // XXII Международный Биос-форум 2017. Сборник материалов. Санкт-Петербург. 2017. С. 142-146.
4. Копылова В. И., Зеленковский П. С. Оценка экологического состояния Муринского ручья биологическими и экологогеохимическими методами // Экологические проблемы недропользования. Материалы Шестнадцатой международной молодежной научной конференции. Санкт-Петербург. 2016. С. 264-267.
5. Цупикова Н. А., Севостьянова Е. А. Некоторые гидролого-гидрохимические особенности и проблемы малых городских прудов на примере пруда Поплавок // Известия КГТУ. 2021, № 62. С. 50-64.
6. Козлов А. В., Вершинина И. В. Оценка экологического состояния техногенно преобразованного водного объекта в зоне отдыха «Мухинское озеро» города Бора Нижегородской области // Успехи современного естествознания. 2020, № 5. С. 50-55.
7. Бузников А. А., Тимофеев А. А. Региональный экологический мониторинг: метод и аппаратно-программный комплекс для дистанционной оценки загрязнения индикаторных видов растительности тяжелыми металлами // Региональная экология. Том 29, 2010, № 3. С. 9-18.
8. Горяинов В. С., Хасенова М., Антоненко К. Г., Бузников А. А. Лабораторный измеритель гидрооптических характеристик на основе волоконно-оптического спектрометра // Известия СПбГЭТУ «ЛЭТИ». 2021, № 2. С. 5-14.

УДК 535.233, 771.5345

КАЛИБРОВКА СЕРИЙНОГО АВИАЦИОННОГО ТЕПЛОВИЗОРА

Груздев Виктор Николаевич[1], Кудряшов Николай Николаевич[2], Пономарёв Станислав Александрович[2], Шилин Борис Владимирович[1]

[1] Санкт-Петербургский научно-исследовательский центр экологической безопасности Российской академии наук
Корпусная ул., 18, Санкт-Петербург, 197110, Россия
[2] Военно-космическая академия имени А.Ф. Можайского
Ждановская ул., 13, Санкт-Петербург, 197198, Россия
e-mails: vicgruz@gmail.com, nick59nick@gmail.com, psamail@mail.ru, bshilin@rambler.ru

Аннотация. Приводятся результаты использования при аэросъёмке различных методов калибровки авиационного тепловизора по внешним температурным эталонам, с использованием инфракрасного радиометра, а также возможное использование внутренних эталонов.

Ключевые слова: авиационный тепловизор; калибровка; температурные эталоны.

CALIBRATION OF A SERIAL AVIATION THERMAL IMAGER

Gruzdev Victor[1], Kudryashov Nikolay[2], Ponomarev Stanislav[2], Shilin Boris[1]

[1] St. Petersburg Research Center for Environmental Safety of the Russian Academy of Sciences
18 Korpusnaya St, St. Petersburg, 197110, Russia
[2] Mozhaysky Military Space Academy
13 Zhdanovskaya St, St. Petersburg, 197198, Russia
e-mails: vicgruz@gmail.com, nick59nick@gmail.com, psamail@mail.ru, bshilin@rambler.ru

Abstract. The results of using various methods of calibrating an aviation thermal imager using external temperature standards, using an infrared radiometer in aerial photography, as well as the possible use of internal standards are presented.

Keywords: aviation thermal imager; calibration; temperature references.

Введение. Во второй половине прошлого века активно развивалась тепловая аэросъёмка как новый современный метод дистанционного зондирования. Были разработаны основные вопросы методики аэросъёмки и интерпретации её материалов при решении широкого круга задач изучения природных ресурсов и охраны окружающей среды [1-3]. Было выпущено две модификации серийных авиационных тепловизоров – «Вулкан» и «Малахит», последний из которых успешно эксплуатируется и в настоящее время. Тепловизоры не имели системы температурной калибровки, но, как показал многолетний опыт работ, для некоторых, главным образом экологических, задач необходимы данные о температуре поверхности. Это позволит, например, выделить первоочередные аномалии при контроле подземных теплосетей, оценить теплопотери зданий, объёмы сбросов в акватории и т. п. Использовать широко распространённые в последнее время зарубежные калиброванные в лаборатории матричные тепловизоры затруднительно из-за неясности вопроса стабильности калибровки и низкой производительности (почти на порядок ниже, чем у тепловизора «Малахит»). Поэтому представляется целесообразным разработка отдельных методов калибровки конкретного тепловизора.

1. Использование на борту авианосителя отдельного калиброванного прибора. При проведении экспериментальных аэросъемок с цифровым вариантом тепловизора «Малахит» использован ИК радиометр Optris MS Plus фирмы Optris GmbH (Германия), имеющий поле обзора 1/20 высоты полёта и чувствительность 0,1 °С. При высоте поле та S = 300 м ширина регистрируемой полосы *D* около 15 м. Радиометр устанавливается на одной платформе с тепловизором «Малахит». Моменты включения и выключения радиометра и тепловизора на начало и конец записи данных маршрута тепловой аэросъемки синхронизованы.

На рис. 1 показан результат аэросъемки – тепловое изображение с нанесенной трассой температурного профиля и совмещение его с синхронной термограммой.

На рис. в его верхней части дана только средняя часть теплового изображения. Рисунок 2 представляет увеличенный фрагмент его центральной части с хорошо выделяющимися яркими линейными аномалиями теплосетей.

Далее на синхронной термограмме выбираются участки маршрута, содержащие равномерно излучающие объекты, размер которых существенно превышает поле зрение радиометра на земной поверхности. Это часть маршрута с водной поверхностью (температура 2,7 °С) и однородная по структуре крыша хозяйственного здания с температурой 10,9 °С у правого края изображения на рис. 2. При выборе на тепловом изображении объектов для температурной привязки могут быть полезны материалы аэрофотосъемки сопровождения, позволяющие более уверенно оценить однородность структуры объектов.

Температурная калибровка теплового изображения производится специальным программным продуктом SPEP, разработанным для обработки растровых изображений. Используя меню программы, вводят значения температуры нулевого уровня и приращения температуры на один уровень. Эти исходные данные рассчитываются

по температурным значениям термограммы для выбранных участков и соответствующих им значениям уровней сигнала теплового изображения (аэроснимка). В результате для данного маршрута нулевой уровень – 0,3 °С, приращение на один уровень – 0,08 °С. При установке курсора на объект теплового аэроснимка в окошке программы отображается его радиационная температура.

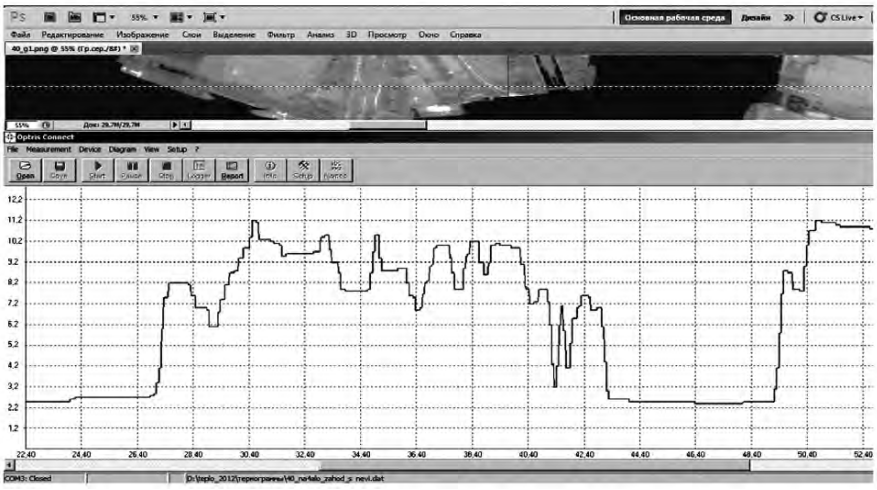


Рис. 1. Привязка термограммы к маршруту тепловой аэросъемки.

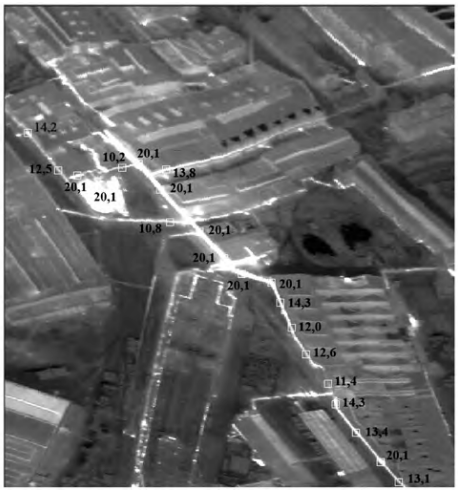


Рис. 2. Пример определения температуры поверхности над теплотрассой.

Программа обработки изображений SPEP позволяет делать отметки в интересующих интерпретатора-диагноста точках изображения (на рис. 2 в виде условных квадратов размером в несколько пикселей). Может быть выбран и другой условный знак. Центр квадрата соответствует положению пикселя, где определяется температура. Каждый такой пиксель автоматически нумеруется и характеризуется координатами X и Y маршрута аэросъемки и температурой в соответствии с данными калибровки.

На рис. 2 показаны произвольно выбранные точки. Программа формирует текстовый файл с данными по каждой точке измерений. Для наглядности номера точек на изображении заменены на значения их температур.

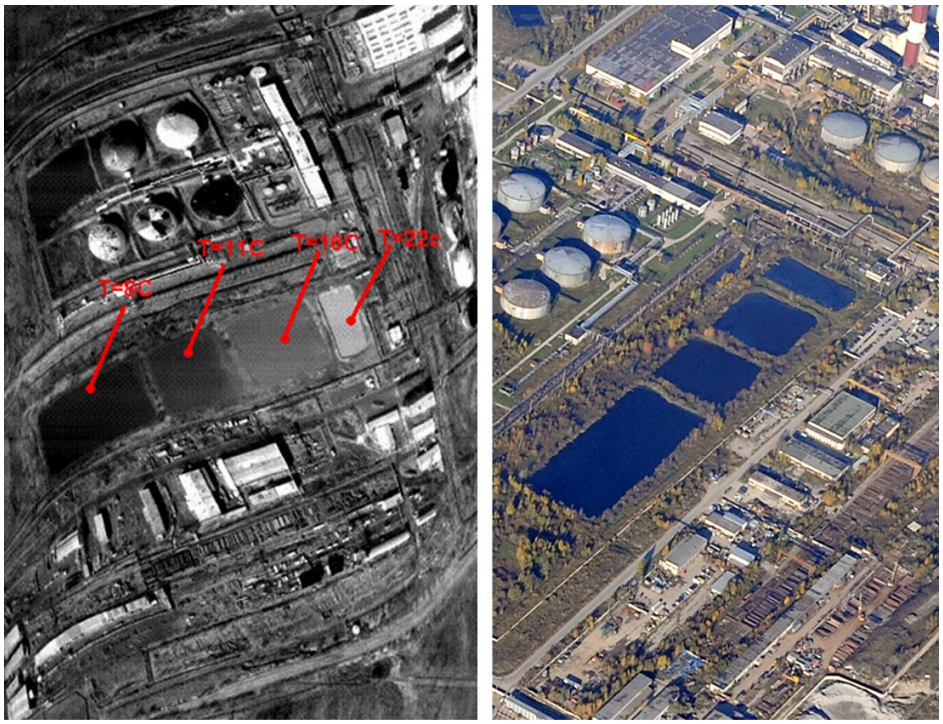
Если в файл маршрута аэросъемки вводится информации GPS, то файл архивируется в формате GeoTIF и в текстовую информацию о точке измерения температуры поступают географические координаты. Эти данные могут составить дополнительный слой геоинформационной системы.

2. Использование эталонных объектов на земной поверхности. Этот вариант хорошо известен в аэрогеофизике (например, в аэромагнитной съемке). Недостаток – возможный заметный дневной дрейф температурного фона в процессе аэросъемки (даже при полетах под облачностью) и необходимость, в связи с этим повторных залетов над эталонными объектами, что неудобно и дорого. Второе – эталонные объекты бывают организационно труднодоступны.

Для Санкт-Петербурга в качестве эталонов были выбраны бассейны-шламоотстойники ТЭЦ, показанные на рис. 3-Б. Размеры бассейнов: ширина около 50 метров, длина соответственно около 180 м, 50 м, 50 м и 30 м. Глубина

бассейнов 2.5 – 3,0 м, поэтому большая масса воды обеспечивает высокую тепловую инерцию и стабильность их температурного режима. Разница температуры поддерживается гидравлической связью через заглублённые в перемычках трубы – нагретая технологическая вода подаётся в первый маленький бассейн, и он имеет наибольшую температуру. Самый холодный – четвёртый дальний и наибольший по площади бассейн.

Измерения температуры бассейнов в процессе аэросъёмки проводились 21 апреля в утренние часы инфракрасным радиометром AGEMA TPT 40 L2 и ртутными термометрами. На тепловом аэроснимке (рис. 3-А) видно, что бассейны формируют чёткий стабильный температурный клин со следующими значениями радиационных температур: 18 °С (пруд №1), 14 °С (пруд №2), 9 °С (пруд №3), 2 °С (пруд №4). Контактные температуры составили соответственно 22 °С, 16 °С, 11 °С, 4 °С, то есть эти значения чуть выше радиационных. Объясняется это небольшим отличием коэффициента излучения воды от единицы. Так как тепловая аэросъёмка регистрирует радиационную температуру, для калибровки материалов аэросъёмки используются данные радиационных измерений бассейнов.



А **Б**

Рис. 3. А – Цифровое тепловое изображение (аэроснимок) с четырьмя бассейнами-шламоотстойниками. Указаны температуры водной поверхности. Не исправлены краевые искажения за счёт большого поля обзора тепловизора (120 градусов). Б – Аэрофотоснимок бассейнов.

Полученные цифровые тепловые изображения состоят из 256 градаций уровня входного сигнала. При калибровке каждому уровню присваивается соответствующее значение радиационной температуры. Для бассейна с температурой 8 ºС уровень равен 15, для 11 ºС – 50, для 16 ºС – 105 и для 22 ºС – 180. По этим данным строится линейная зависимость радиационной температуры от уровня яркости теплового изображения. По ней определяется радиационная температура других поверхностей на тепловых аэроснимках и могут быть построены карты в изолиниях.

3. Использование калибраторов в оптическом блоке тепловизора. Основными элементами оптической системы тепловизора «Везувий» являются зеркальная призма в виде вращающегося куба и два боковых плоских зеркала для изменения направления лучей [4]. Эти элементы образуют систему сканирования, перпендикулярную движению авианосителя. Строки теплового изображения при авиасъемке формируются в пределах 22,5° поворота призмы в обе стороны от вертикали.

На рис. 4 приведена оптическая схема оптико-механического блока (ОМБ) тепловизора. Для регистрации излучения внутренней поверхности корпуса, оптимальным является угол поворота призмы на 40° относительно визирования в надир. При этом угле поворота призмы на входе оптического канала полностью отсутствует излучение объектов аэросъемки земной поверхности. [5].

Для построения калибровочной кривой и обеспечения градуировки объектов тепловой аэросъемки по температуре необходимо иметь как минимум две точки привязки к известным температурам, которыми являются регистрируемые излучения стенок корпуса ОМБ.

Учитывая жесткие требования по стабильности температуры приемника излучения (7), величина автоколлимационного сигнала также может быть использована в качестве опорного источника. Совместная регистрация величины автоколлимационного импульса и излучения внутренней поверхности корпуса оптического блока позволяет учесть изменение параметров приемника излучения и электронных устройств обработки сигналов тепловизора.

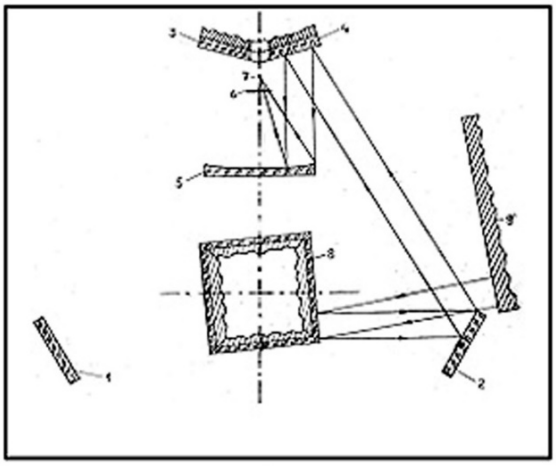


Рис. 4. Оптическая схема градуировки тепловизора «Везувий» с регистрацией излучения внутренней стенки корпуса оптического блока:
1, 2, 3, 4 – плоские зеркала;
5 – сферическое зеркало;
6 – фильтр;
7 – приёмник излучения;
8 – зеркальный корпус призмы;
9' – стенка корпуса сканирующей головки.

Заключение. Все рассмотренные способы получения количественной информации при использовании отечественных серийных авиационных тепловизоров в той или иной степени апробированы авторами в условиях реальных авиасъемок.

Показана целесообразность их применения, но необходимо провести дополнительные лабораторные исследования и лётные эксперименты по сравнению точности методов в каждом конкретном случае.

Результаты экспериментов показали, что пока реально могут быть использованы первые два метода. Из них наиболее точным и надежным оказался первый.

Методика совместного использования тепловизора и ИК радиометра может быть рекомендована к производственному внедрению после небольшого усовершенствования программ совместной обработки данных этих приборов. Точность измерения температуры поверхности может быть улучшена при проведении синхронных с аэросъемкой наземных измерений на эталонных объектах.

СПИСОК ЛИТЕРАТУРЫ

1. Горный В.И., Груздев В.Н., Крицук С.Г., Латыпов И.Ш., Тронин А.А., Шилин Б.В. Сравнение теплопотерь теплопроводов с различными типами изоляции методом полевой инфракрасной радиометрии // Тепло-энергоэффективные технологии. 1997. № 4. С. 54–59.
2. Горный В.И., Шилин Б.В., Ясинский Г.И. Тепловая аэрокосмическая съемка. М.: Недра, 1993. 128 с.
3. Шилин Б.В., Молодчинин И.А. Контроль состояния окружающей среды тепловой аэросъемкой. М.: Недра, 1992. 85 с.
4. Тепловизор «Вулкан». Техническое описание АЯ1.470.015 ТО 1978.
5. Мирошников М. М. Теоретические основы оптико-электронных приборов. – 2-е изд., перераб. и доп. – Л.: Машиностроение, Ленингр. отд-ние, 1983.

УДК 551.509.6+504.05

МЕТОДЫ И СРЕДСТВА МОДИФИЦИРОВАНИЯ ТЕПЛЫХ ТУМАНОВ И ВОЛНИСТООБРАЗНЫХ ОБЛАКОВ НИЖНЕГО ЯРУСА В ИНТЕРЕСАХ РЕШЕНИЯ ЭКОЛОГИЧЕСКИХ И ХОЗЯЙСТВЕННЫХ ЗАДАЧ

Доронин Александр Павлович, Козлова Наталья Александровна, Петроченко Вячеслав Михайлович, Новиков Николай Сергеевич, Межнина Ирина Романовна
Военно-космическая академия имени А.Ф. Можайского
Ждановская ул., 13, Санкт-Петербург, 197198, Россия
e-mail: cozlowa.nat2012@yandex.ru

Аннотация. В статье предлагается использовать методы и средства модифицирования теплых туманов и волнистообразных облаков нижнего яруса для решения широкого круга экологических и хозяйственных проблем, связанных с деятельностью человека.

Ключевые слова: экологические проблемы; волнистообразные облака; туманы; облачность; модифицирование; метод; средства; способ; рассеяние.

METHODS AND MEANS FOR MODIFYING WARM FOGS AND WAVE-SHAPED LOWER CLOUDS IN INTEREST OF SOLVING ENVIRONMENTAL AND ECONOMIC PROBLEMS

Doronin Alexander, Kozlova Natalya, Petrochenko Vyacheslav, Novikov Nikolay, Mezhina Irina
Mozhaysky Military Space Academy
13 Zhdanovskaya St, St. Petersburg, 197198, Russia
e-mail: cozlowa.nat2012@yandex.ru

Abstract. The article proposes to use methods and means of modifying warm fogs and wave-shaped lower clouds to solve a wide range of environmental and economic problems associated with human activities.

Keywords: ecological problems; wave-shaped lower clouds; fogs; cloud cover; modification; method; means; way; scattering.

Введение. Известно, что туманы, облака и связанные с ними опасные явления погоды (низкая облачность, плохая видимость, осадки в виде дождя и снега и др.) оказывают существенное влияние на деятельность человека. В литературе имеются примеры такого негативного влияния на хозяйственную деятельность человека, нередко сопровождающегося также и наличием экологических проблем (например, увеличение загрязнения атмосферного воздуха в крупных городах при наличии низких волнистообразных облаков и др.) [1-6]. Однако, приведённые в этих исследованиях сведения, даются без их конкретизации по формам облаков.

В то же время такого рода исследования в последние годы становятся все более востребованными. Например, для районов Краснодарского края и Северного Кавказа значительный интерес имеют сведения о повторяемости конвективных облаков (в частности, мощно-кучевых и кучево-дождевых) и их характеристиках (вертикальная протяжённость, водность и водозапас, высоты нижней и верхней границы и др.), величине возможного ущерба [7]. Особое значение эти исследования имеют при обосновании целесообразности разработки методов и средств модифицирования облаков разных форм с целью устранения (или значительного снижения) их негативного влияния на деятельность человека, включая и экологические аспекты.

С целью восполнения данного пробела в настоящей работе выполнено качественное оценивание и получены количественные оценки влияния теплых волнистообразных (слоистых, слоисто-кучевых) облаков на деятельность человека, указывающие на необходимость обоснования путей снижения их негативного влияния.

Пути снижения негативного влияния теплых волнистообразных (слоистых, слоисто-кучевых) облаков и туманов на деятельность человека. Результаты качественного оценивания и количественных оценок влияния теплых волнистообразных облаков и туманов (ТВОТ) и связанных с ними опасных явлений погоды на хозяйственную деятельность человека могут быть охарактеризованы данными, приведенными на рис.1 и в таблице 1 [1, 2, 5, 6].

Анализ данных, приведенных на рис. 1 и в таблице 1 показывает, что практически все сферы экономической деятельности человека подвержены влиянию опасных явлений погоды, связанных с этими облаками.

Существенное влияние облачности и туманов на хозяйственную деятельность человека обуславливает необходимость поиска путей, позволяющих устранить или в значительной мере снизить их негативное влияние.

Анализ работ в этом направлении позволил установить, что на современном этапе развития РФ таких путей несколько (главным образом, пять) (рис. 2).

Более детальное рассмотрение каждого из приведенных на данном рис. путей устранения негативного влияния облаков и туманов на деятельность человека позволяет констатировать следующее: реализация первого и четвертого путей в современных условиях вряд ли осуществима на практике из-за сложного экономического положения России.

Второй путь, заключающийся в повышении качества гидрометеорологического обеспечения (ГМО) за счет повышения оправдываемости прогнозов погоды (особенно средне- и долгосрочных), является чрезвычайно сложным. Действительно, с учетом достигнутых к настоящему времени оценок оправдываемости прогнозов погоды на сутки, которые составляют 90-95%, а на трое суток - значительно ниже, не более 75-80%, и, вряд ли, можно ожидать какого-либо существенного улучшения состояния дел в этом вопросе.

Третий путь также требует значительных материальных вложений, связанных как с совершенствованием существующих, так и созданием новых технических средств получения, сбора, обработки и доведения до потребителей гидрометеорологической информации.

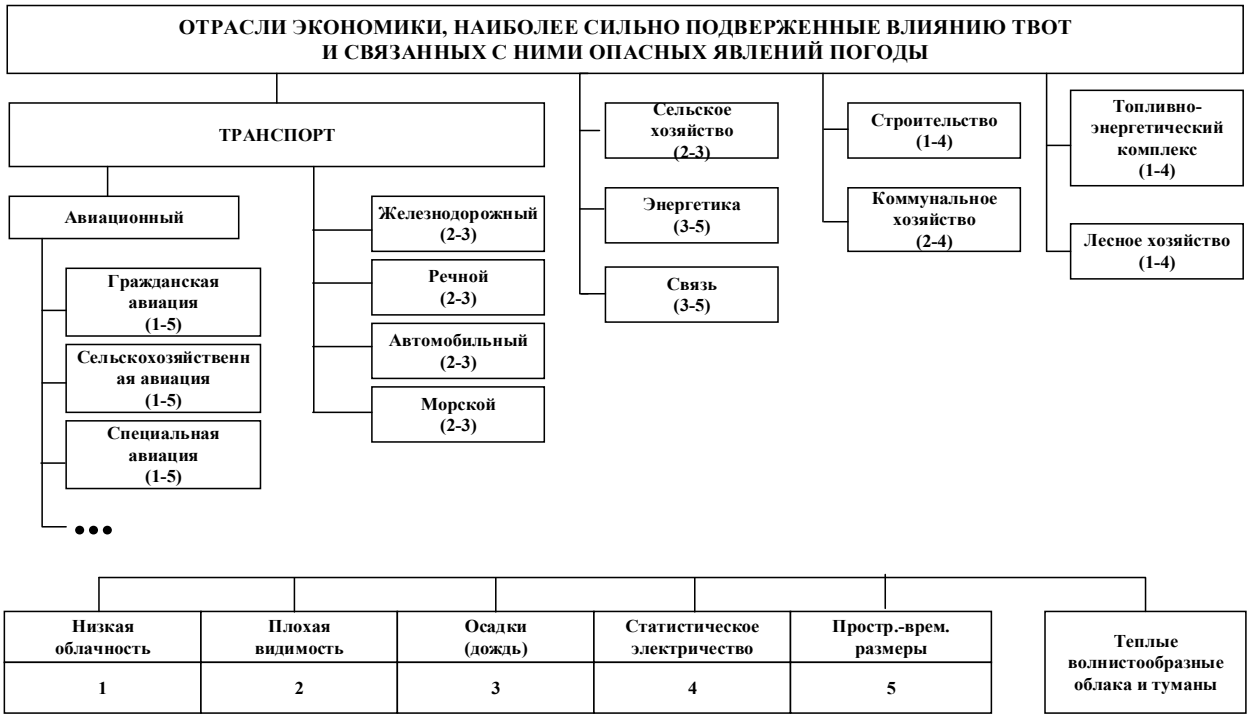


Рис. 1. Качественное оценивание влияния теплых волнистообразных облаков и туманов на хозяйственную деятельность человека.

Таблица 1

Количественные оценки влияния волнистообразных облаков и туманов на хозяйственную деятельность человека

№ п/п	Отрасли экономики	Виды атмосферного образования	Степень влияния атмосферного образования
1.	Гражданская авиация, США	туман, низкая облачность	Ежегодный ущерб составляет порядка 100 млн. долларов
2.	Автомобильный транспорт, США	туман, низкая облачность	Ежегодный ущерб составляет порядка 300 млн. долларов
3.	Гражданская авиация, Россия	туман, низкая облачность	18 октября – 25 октября 1987 года. Закрыты на неделю аэропорты Московской зоны и ряда других городов центральной части России. 52 тысячи пассажиров сдали билеты
4.	Гражданская авиация, Россия	туман, низкая облачность	13 марта 1993 г. Закрыты все аэропорты Самарской области на срок от 6 до 12 часов
5.	Автомобильный транспорт, Россия	туман, осадки, низкая облачность	Снижение потока автомобилей на 25-50% по сравнению с потоком в ясные дни

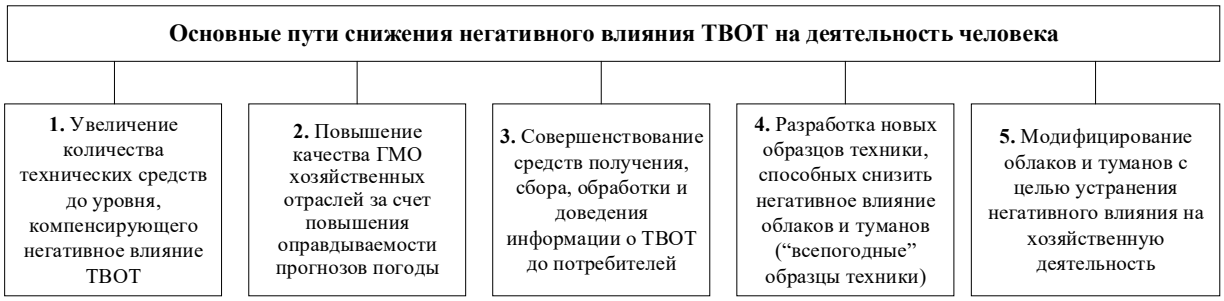


Рис. 2. Основные пути снижения негативного влияния теплых волнистообразных облаков и туманов на деятельность человека.

Поэтому в последние годы все чаще предлагается использовать на практике пятый путь устранения негативного влияния облаков и туманов на деятельность отраслей экономики, заключающийся в применении методов и средств модифицирования теплых волнистообразных облаков и туманов. В связи с этим важным представляется изучение вопросов, связанных с анализом физических основ, методов и технических средств модифицирования теплых волнистообразных облаков и туманов.

Интерес к проблеме модифицирования облаков и туманов (включая и тёплые) обусловлен следующими обстоятельствами:

– во-первых, методы и средства модифицирования атмосферных процессов и явлений могут быть использованы для воздействия на облака различных форм (волнистообразные, слоистообразные, конвективные);

– во-вторых, применение методов и средств модифицирования облаков и туманов позволяет получить значительный экономический эффект (в среднем отношение затрат к доходам составляет 1:10);

– в-третьих, применение методов и средств модифицирования облаков и туманов позволяет решать широкий круг прикладных задач (обеспечение посадки летательных аппаратов, высадка аварийно-спасательных групп, вымывание вредных примесей из атмосферы и др.);

– в-четвёртых, за рубежом (в частности, в США) широким фронтом проводятся работы по созданию методов и средств модифицирования облаков и туманов.

В связи с вышеизложенным актуальным является проведение исследований по разработке физических основ способов, методов и технических средств модифицирования тёплых волнистообразных облаков и туманов. Результатом таких исследований представлены ниже.

Физические принципы способов модифицирования тёплых волнистообразных облаков и туманов основываются на [6, 8, 9]:

– возможности испарения капель тумана (облака) за счет подвода в них тепла;

– возможности испарения капель тумана (облака) за счет создания в них нисходящих потоков воздуха с помощью определенных технических средств;

– возможности осаждения капель тумана (облака) за счет укрепления в них капель воды (или капель раствора гигроскопических реагентов) большего (100-200 мкм) размера, чем размеры облачных капель для реализации коллоидальной неустойчивости.

Физические принципы воздействия на тёплые облака и туманы являются основой для разработки соответствующих методов модифицирования атмосферных облачных образований. Анализ и обобщение отечественных и зарубежных методов модифицирования тёплых облаков и туманов с целью их рассеяния позволяют разработать обобщенную классификацию способов, применительно к упомянутым выше физическим принципам (рис.3) [6, 8, 9].

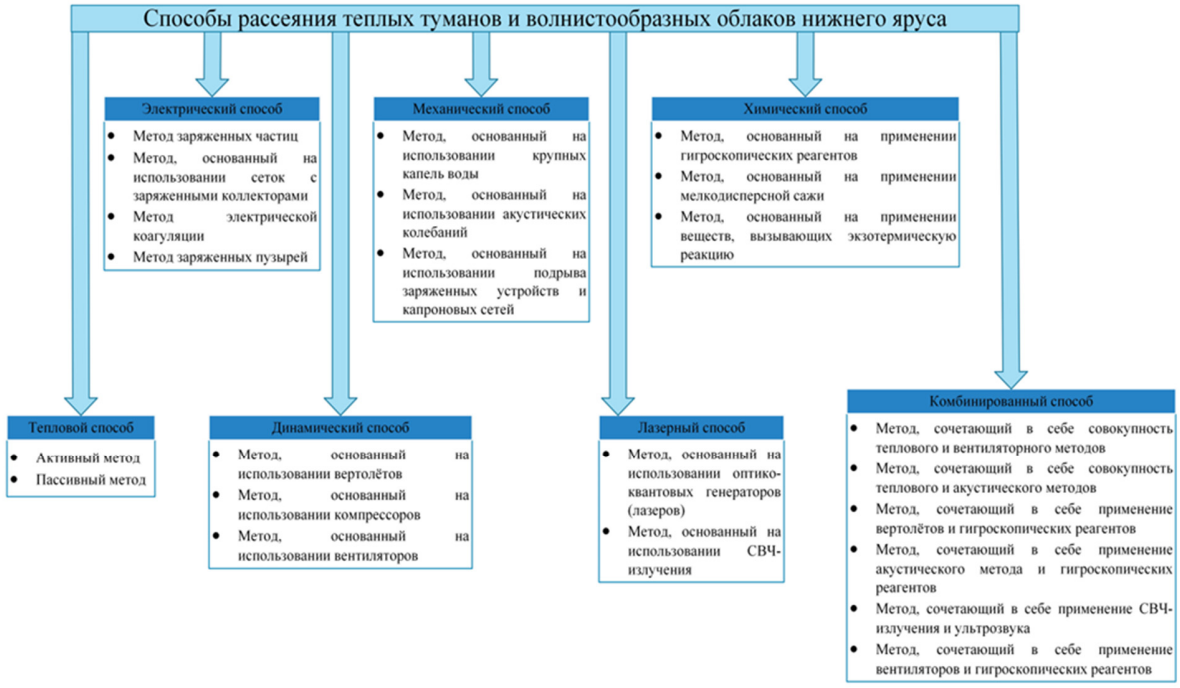


Рис. 3. Классификация способов рассеяния теплых туманов и волнистообразных облаков нижнего яруса.

Из анализа представленных на рис. данных можно видеть, что в настоящее время существует около десятка способов рассеяния тёплые облака и туманы. При этом можно отметить, что из представленных способов рассеяния каждый из них включает в себя, как правило, несколько методов рассеяния таких атмосферных образований, характеристика которых представлена в [10].

Основными способами рассеяния тёплых туманов (облаков) в настоящее время являются: тепловой, динамический, химический, механический, лазерный, электрический и комбинированный.

Наиболее перспективными с точки зрения их практической реализации являются следующие способы и методы:

- тепловой способ (активный метод);
- динамический способ (метод, основанный на использовании вертолётов);
- механический способ (метод, основанный на использовании крупных капель воды);
- электрический способ (метод, основанный на использовании заряженных капель воды);
- комбинированный способ (метод, сочетающий в себе совокупность теплового и вентиляторного методов, а также применение вертолётов и гигроскопических реагентов).

Наличие способов и методов рассеяния тёплых туманов и волнистообразных облаков обуславливает необходимость разработки соответствующих технических их реализации. Исходя из этого, на рис. 4 представлена в общем виде классификация технических средств воздействия на тёплые волнистообразные облака и туманы.

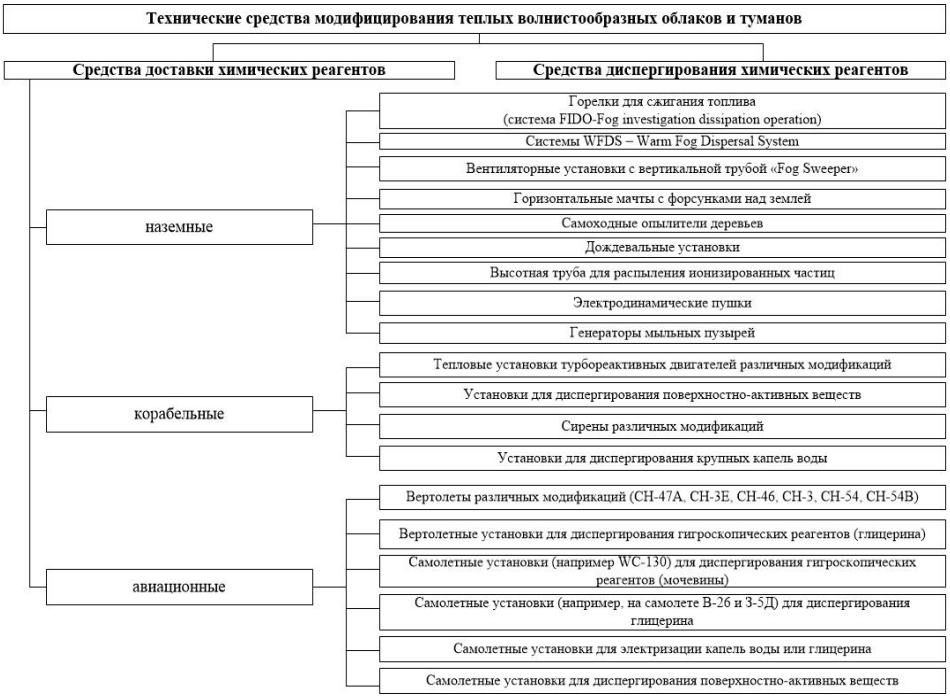


Рис. 4. Технические средства модифицирования теплых волнистообразных облаков и туманов.

Можно видеть, что эти средства подразделяются на средства доставки химических реагентов (ХР) (наземные, корабельные и авиационные) и средства диспергирования ХР (специальные горелки для сжигания топлива, установки, генераторы и др.). Наибольшее применение на современном этапе нашли наземные и авиационные средства модифицирования тёплых волнистообразных облаков и туманов.

Для реализации ряда методов модифицирования тёплых волнистообразных облаков и туманов к настоящему времени разработаны определенные технические средства, которые прошли апробацию на практике и используются в повседневной деятельности. К их числу можно отнести такие технические средства, как: система WFDS (Warm Fog Dispersal System) для рассеяния теплых туманов, смонтированная на авиабазе Оттис (США) и состоящая из нескольких десятков тепловых установок различной мощности: генераторы, установки для диспергирования глицерина или мочевины, размещенные как на борту вертолета (например, СН-16), так подвешенные к нему снизу на тросе, а также самолетные установки, для диспергирования глицерина, мочевины и заряженных капель воды, расположенные на самолетах (например, на самолете В-26). Следует отметить, что применение методов и средств модифицирования ТВОТ позволяет решать широкий перечень не только хозяйственных, но и экологических задач. Например, при рассеянии теплых туманов и низких волнистообразных облаков в их перечень могут быть включены такие задачи, как: обеспечение взлета и посадки летальных аппаратов, высадки поисково-спасательных и ремонтных

групп, очищение воздушных бассейнов крупных городов от загрязняющих примесей, обеспечение бесперебойной работы открытых угольных и песчаных карьеров, проведение экологического мониторинга и др.

Следовательно, можно заключить, что проблема исследования и модифицирования тёплых волнистообразных облаков и туманов на современном этапе является актуальной и востребованной.

Заключение.

1. Установлено, что тёплые волнистообразные облака и туманы оказывают существенное влияние на хозяйственную деятельность человека, нередко сопровождающиеся наличием серьезных экологических проблем. Показано, что практически нет ни одной отрасли экономики страны, на деятельность которой тёплые волнистообразные облака и туманы не оказывали бы негативное влияние. Экономический ущерб, наносимый хозяйственной деятельности ТВОТ может составить десятки миллионов долларов. Сделан вывод о необходимости и целесообразности применения средств модифицирования тёплых волнистообразных облаков и туманов с целью устранения (значительного снижения) их негативного влияния на деятельность человека.

2. Приведена классификация способов рассеяния тёплых волнистообразных облаков и туманов, включающих в себя тепловой, динамический, химический, механический, лазерный, электрический и комбинированный способы. Показано, что каждый из способов включает в себя ряд соответствующих методов воздействия на ТВОТ.

3. Для реализации ряда методов модифицирования ТВОТ к настоящему времени разработаны (главным образом, в США) и прошли практическую апробацию определённые технические средства, такие как: система WFDS (Warm Fog Dispersal System) для рассеяния теплых туманов, смонтированная на авиабазе Оттис (США) и состоящая из нескольких десятков тепловых установок различной мощности: генераторы, установки для диспергирования глицерина или мочевины, размещенные как на борту вертолета (например, CH-16), так подвешенные к нему снизу на тросе, а также самолетные установки, для диспергирования глицерина, мочевины и заряженных капель воды, расположенные на самолетах (например, на самолете B-26).

4. Сделан вывод о том, что проблема исследования и модифицирования тёплых волнистообразных (слоистых, слоисто-кучевых) облаков и туманов на современном этапе является актуальной и востребованной, поскольку применение методов и средств их модифицирования позволяет решать широкий круг экологических и хозяйственных задач.

СПИСОК ЛИТЕРАТУРЫ

1. Беляев В.П. О влиянии туманов и низкой облачности на безопасность полетов // Проблемы безопасности полетов. – М., 1981, № 7, С.33-84.
2. Астапенко П.Д., Баранов А.М., Шварев И.М. Погода и полеты самолетов и вертолетов. – Л.: Гидрометиздат, 1980, 280 с.
3. Дейнекин П.С. Война в Чечне // Авиация и космонавтика. – 1995, № 11, С.10-13.
4. Рог В. Воздушное наступление и воздушная оборона: отныне они подчинены единой воле// Армейский сборник. – М., 1997, № 11, С. 10-13.
5. Девятьяров Е. Об испытаниях противоспутникового лазера // Новости космонавтики. – 1997, №7, Том 7.
6. Доронин А.П. Воздействия на атмосферные процессы и явления: учебное пособие. – СПб.: ВКА имени А.Ф. Можайского, 2014, 292 с.
7. Этапы развития противогрозовых работ /М.Т. Абшаев, А.М. Малкарова, С.В. Тасенко, И.А. Шумаков // Доклады Всероссийской конференции по физике облаков и активным воздействиям на гидрометеорологические процессы: сборник научных трудов 23-27 октября 2017. – Нальчик-Уфа: АЭТЕРНА, 2017, С.7-27.
8. Качурин Л.Г. Физические основы воздействия на атмосферные процессы. –Л.: Гидрометеоиздат, 1990, 464 с.
9. Методы и средства рассеяния тёплых туманов и слоистообразной облачности в интересах гидрометеорологического обеспечения деятельности военно-морского флота России /А.П. Доронин, В.М. Петроченко, Н.А. Козлова, С.А. Шмалько, А.А. Свинарчук // Перспективы развития гидрографической службы военно-морского флота до 2030 года: матер. научн. конф. – СПБ., 2017, №301, С.68-74.
10. Классификация способов рассеяния теплых туманов и волнистообразных облаков нижнего яруса в интересах решения прикладных задач/А.П. Доронин, Н.А. Козлова, Н.С. Новиков, В.М. Петроченко // Проблемы военно-прикладной геофизики и контроля окружающей среды: матер. конф. – СПб.: ВКА имени А.Ф. Можайского, 2020, С.110-116.

УДК 681.785.554

ВЫБОР ХАРАКТЕРИСТИК КАЛИБРОВОЧНОГО УСТРОЙСТВА ПОРТАТИВНОГО СПЕКТРОМЕТРА

Хасенова Мариям, Горяинов Виктор Сергеевич, Антоненко Ксения Георгиевна, Бузников Анатолий Алексеевич

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: mariyam-98@mail.ru, vsgoriainov@etu.ru, kgantonenko@yandex.ru, aabuznikov@mail.ru

Аннотация. В статье описаны методика и результаты спектральной и энергетической калибровки модернизированного варианта портативного спектрометра РСС, а также устройство и принцип действия его калибровочного устройства. Сравниваются характеристики пропускания трех различных белых экранов, предназначенных для получения эталонных спектров источника излучения при съемке объектов природной среды.

Ключевые слова: дистанционное зондирование; спектрометрия природных объектов; портативный спектрометр; калибровка; спектры пропускания.

SELECTION OF CHARACTERISTICS OF THE PORTABLE SPECTROMETER'S CALIBRATION DEVICE

Khasenova Mariyam, Goryainov Viktor, Antonenko Kseniya, Buznikov Anatoliy
St. Petersburg State Electrotechnical University «LETI»
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: mariyam-98@mail.ru, vsgoriainov@etu.ru, kgantonenko@yandex.ru, aabuznikov@mail.ru

Abstract. The article describes the methods used and results obtained during spectral and energetic calibration of the modernized version of the RSS portable spectrometer, along with the setup and principle of operation of its calibration device. Transmission parameters of three white screens, intended for obtaining reference spectra of radiation sources during the surveys of natural objects, are compared.

Keywords: remote sensing; spectrometry of natural objects; portable spectrometer; calibration; transmission spectra.

Введение. В настоящее время основная часть данных об экологическом состоянии объектов природной среды, в том числе растительности и водоемов, получается методом спектрального дистанционного зондирования с космических аппаратов, авиационных носителей и беспилотных летательных аппаратов [1]. Одними из первых спектральных приборов космического базирования стали ручные спутниковые спектрометры РСС–2 и РСС–3, применявшиеся на советских космических кораблях «Союз» и орбитальных станциях «Салют» и «Мир» [2–4]. Удачная конструкция и хорошие оптические характеристики спектрометра РСС привели к появлению ряда его дальнейших модификаций, в которых фотопленка как регистрирующий элемент была заменена массивом фотоэлектронных приемников излучения [5, 6]. При участии авторов статьи была разработана одна из таких модификаций на базе микроконтроллерной платы MEGA 2560 PRO с AVR-микроконтроллером ATmega2560, имеющим тактовую частоту 16 МГц [7]. В статье приводятся методы, использованные при калибровке с целью уточнения спектральных и энергетических характеристик модернизированного спектрометра, и полученные при этом результаты.

Конструкция модернизированного портативного спектрометра. Оптическая схема прибора, показанная на рис. 1, была затронута модернизацией в наименьшей степени. Излучение от объекта съемки собирается входным объективом 1 с фокусным расстоянием 135 мм. Револьверная диафрагма 3, установленная на оси датчика угла поворота 4, служит для регулировки входного светового потока. Передний конец оси свободно вращается в упоре 2.

Система видоискателя включает в себя светоделительный куб 5, собирающую линзу 6, которую можно перемещать в зависимости от расстояния до объекта фокусировки, и зеркало 7, направляющее излучение в выходное отверстие.

На входе спектрометра излучение проходит через вертикальную входную щель 8 шириной 0,4 мм.

Для получения опорных спектров излучения Солнца или другого источника в конструкцию включен белый экран 9, закрепленный в пластиковой вилке, вращающейся вручную вместе с осью. При проведении калибровки он ставится перпендикулярно оси прибора, а во время съемки объекта поворачивается на 90°.

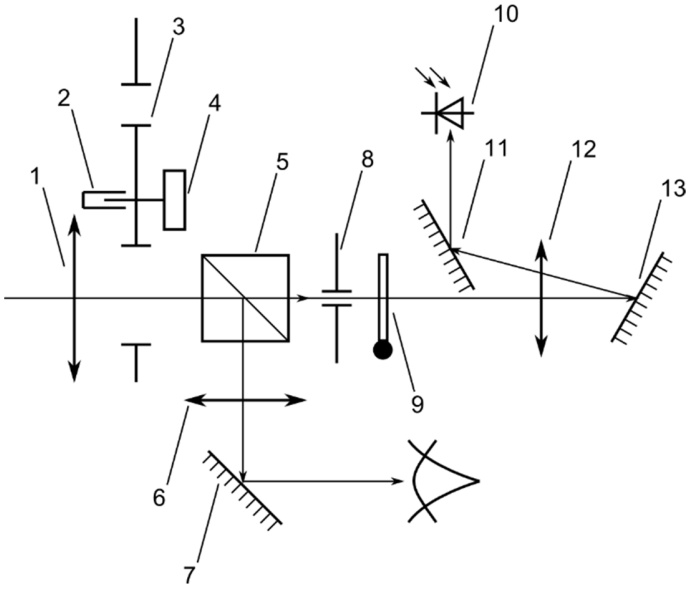


Рис. 1. Оптическая схема модернизированного спектрометра РСС

Дважды, до разложения в спектр дифракционной решеткой 13 и после него, излучение проходит через коллимационную собирающую линзу 12. Решетка имеет 600 штр/мм, фокусное расстояние линзы равно 95 мм, результирующая линейная дисперсия в фокальной плоскости коллиматора в первом порядке спектра составляет 62 мм/мкм.

Наклонное зеркало 11 направляет излучение перпендикулярно главной оси прибора, на фотодиодную линейку 10, которая преобразует оптический поток в электрический сигнал.

Спектральная калибровка спектрометра. В ходе спектральной калибровки для каждого элемента фотоприемника определяется соответствующая область длин волн, излучение в которой падает на этот элемент, и, соответственно, спектральное разрешение и границы рабочей области спектрометра. С этой целью авторами была использована ртутная разрядная лампа, спектр яркости которой L (в произвольных единицах) приведен на рис. 1.

При помощи фиолетового стекла ФС-5 был выделен максимум в 19 канале, соответствующий линии 436 нм в спектре излучения ртути, а при помощи комбинации желто-зеленого стекла ЖЗС-5 и пурпурного ПС-7 – максимум на 546 нм (канал 33). Исходя из этого, было определено разрешение прибора, равное примерно 8 нм на канал, и общая охватываемая спектральная область – от 290 до 790 нм.

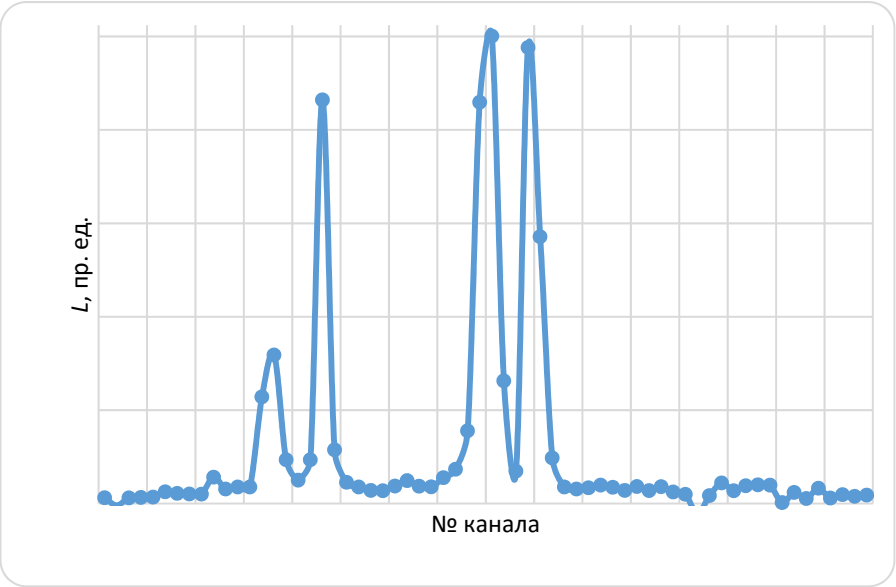


Рис. 2. Спектр излучения ртутной лампы, зафиксированный спектрометром РСС

Следует отметить, однако, что реальная рабочая спектральная область прибора оказывается меньше. С одной стороны, как видно из рис. 2, стеклянные элементы оптической системы спектрометра поглощают излучение в ближней ультрафиолетовой области. С другой стороны, чувствительность фотодиодной линейки неоднородна по спектру, как будет показано далее.

Сравнение вариантов калибровочного экрана. Белый калибровочный экран (9 на рис. 1) предназначен, как уже было сказано, для получения опорных (калибровочных) спектров солнечного излучения при проведении измерений. Следовательно, экран должен изменять только пространственное распределение излучения в потоке на более равномерное, не затрагивая его спектрального состава. Коэффициент пропускания экрана должен быть, во-первых, достаточно высоким (иначе спектр объекта может оказаться более «ярким», нежели опорный спектр), а во-вторых, возможно более однородным по спектру.

В ходе измерений сравнивались характеристики трёх экранов: первый представлял собой целлулоидную пленку, покрытую царапинами с одной стороны до непрозрачности; второй экран – стекло толщиной 1 мм, обработанное лазером с одной стороны; третий экран – стекло толщиной 2 мм с двусторонним молочным покрытием.

Измерения проводились с использованием излучения Солнца и галогенной лампы накаливания мощностью 1 кВт. При этом спектрометр наводили на источник излучения, устанавливали диафрагму в положение, обеспечивающее максимальный уровень сигнала без выхода его за границы динамического диапазона приемника, и регистрировали спектральное распределение яркости $L_0(\lambda)$. Затем вводили в оптический тракт белый экран, корректировали при необходимости положение диафрагмы и регистрировали новое распределение $L(\lambda)$. На рис. 3 приведены примеры таких спектров (учитывающих разницу в пропускании диафрагмы) для 3 экрана и солнечного излучения.

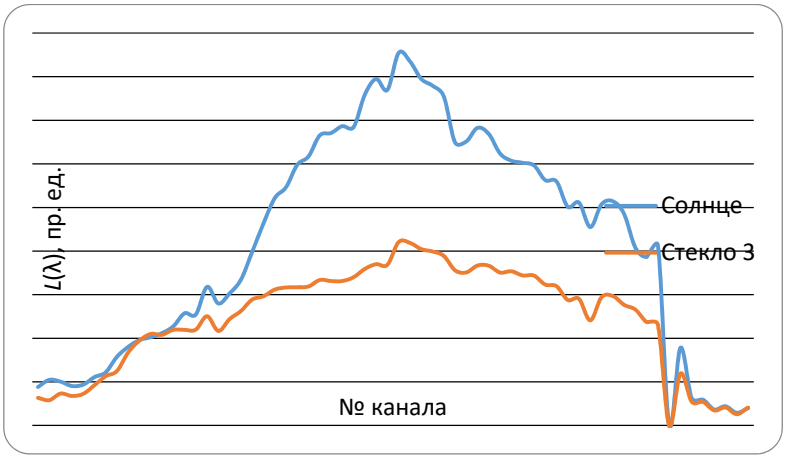


Рис. 3. Спектры солнечного излучения, полученные с использованием белого экрана и в его отсутствие

Из рис. 3 заметно уменьшение чувствительности фотоприемников у «инфракрасного» конца линейки; резкий провал графиков на 57-м элементе объясняется, видимо, дефектом соответствующего фотодиода.

Спектр коэффициента пропускания экрана определялся по следующей формуле:

$$K_{\text{п}}(\lambda) = \frac{L(\lambda)}{L_0(\lambda)}\left(\frac{d_0}{d}\right)^2,$$

где d_0 и d – диаметры отверстий в диафрагме, использовавшихся при съемке без экрана и с экраном соответственно. Результирующие спектры пропускания для лампы накаливания показаны на рис. 4, а для Солнца в безоблачную погоду – на рис. 5. Все кривые получены путем усреднения по 20 повторениям. «Усы» на графиках показывают величину среднеквадратичного отклонения σ.

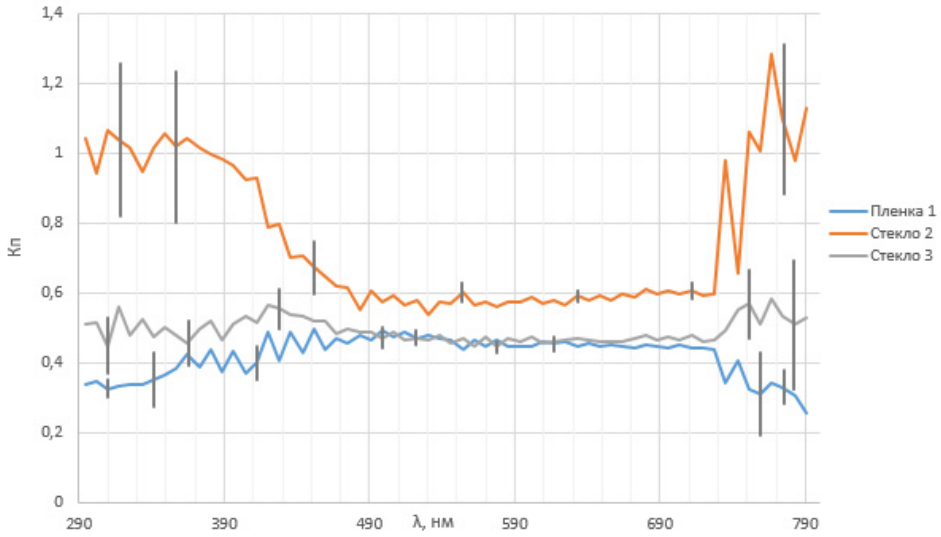


Рис. 4. Спектры пропускания экранов для излучения лампы накаливания

Из графиков видно резкое возрастание ошибки измерений на краях спектров, за пределами видимой области, что соответствует слабым сигналам. При этом расчет может давать даже заведомо ошибочный результат с $K_{\text{п}} > 1$. Очевидно, относительно достоверными оказываются результаты измерений в видимой области, в диапазоне 400 – 700 нм.

Следует отметить также разницу распределений коэффициента пропускания для одного и того же экрана при измерениях с использованием разных источников излучения. Эта разница может объясняться как нелинейностью чувствительности фотоприемника относительно величины падающего потока излучения, так и различием спектрального распределения яркости самих источников. Так, например, температуры солнечной поверхности и нити накала галогенной лампы отличаются почти вдвое, и в спектре последней крайне малая энергия приходится на синюю и фиолетовую области спектра с длинами волн короче 450 нм.

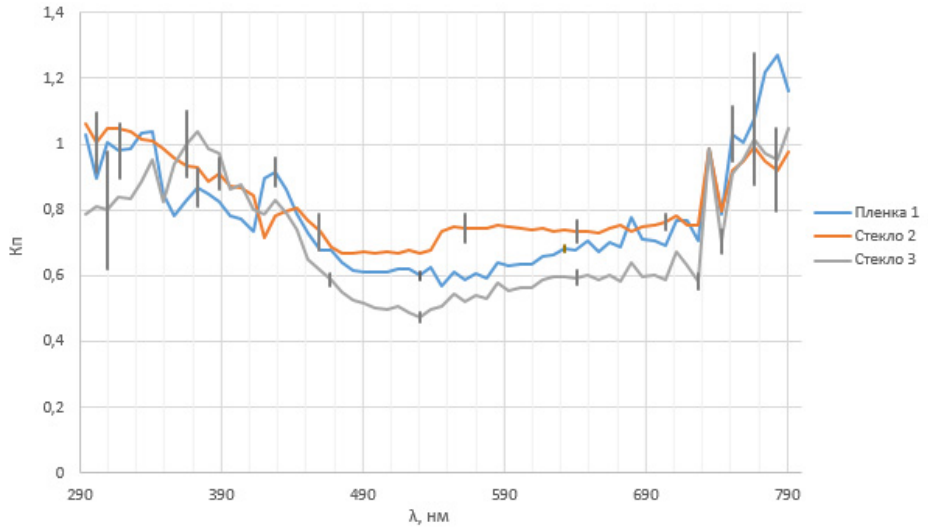


Рис. 5. Спектры пропускания экранов для солнечного излучения

Данные в таблице 1 подытоживают результаты, показанные на графиках, и позволяют более наглядно сравнить характеристики пропускания трех экранов. Для каждого сочетания экрана и источника излучения приведено среднее по спектру значение коэффициента пропускания и величина среднеквадратичного отклонения.

Таблица 1

Характеристики пропускания трех белых экранов

Экран	Лампа накаливания		Солнце	
	$\overline{K_{\text{п}}}$	σ	$\overline{K_{\text{п}}}$	σ
Пленка 1	0,42	0,06	0,78	0,17
Стекло 2	0,76	0,21	0,81	0,12
Стекло 3	0,49	0,03	0,71	0,18

Видно, что для обоих источников наибольшее среднее пропускание характерно для второго экрана. Что же касается спектральной селективности коэффициента пропускания, то 1 и 3 экраны показывают почти совпадающие значения среднеквадратичного отклонения, причем в случае с галогенной лампой этот параметр оказывается наилучшим у 3 экрана.

Заключение. Сравнение полученных в проведенном исследовании характеристик пропускания трех белых экранов позволяет выделить экран номер 2 как наиболее предпочтительный для применения. Данные измерений с солнечным излучением следует, видимо, считать более значимыми, поскольку в этом случае достаточно высокая яркость присутствует в более широком спектральном диапазоне по сравнению с лампой накаливания.

Линейка фотодиодов, используемая в текущей модификации РСС, показывает сильное снижение чувствительности в ближней инфракрасной области. Для расширения возможностей спектрометра целесообразен переход к применению фотоприемника на основе приборов с зарядовой связью (ПЗС). Последние имеют большее число элементов по сравнению с массивами фотодиодов, а также обеспечивают более широкий динамический диапазон за счет возможности изменять время накопления заряда.

СПИСОК ЛИТЕРАТУРЫ

1. Transon, J. Survey of current hyperspectral Earth observation applications from space and synergies with Sentinel-2 / J. Transon, R. d'Andrimont, A. Maugnard, et al. // 2017 9th International Workshop on the Analysis of Multitemporal Remote Sensing Images (MultiTemp). – Brugge: IEEE, 2017. – P. 1–8.
2. Кондратьев К. Я. Некоторые результаты спектрофотометрирования природных образований с пилотируемого космического корабля «Союз–9» / К. Я. Кондратьев, А. А. Бузников, О. Б. Васильев [и др.] // Космические исследования. – 1972. – Т. 10. – Вып. 2. – С. 245–254.
3. Кондратьев К. Я. Некоторые результаты спектрофотометрирования Земли с космического корабля «Союз–7» / К. Я. Кондратьев, А. А. Бузников, В. Н. Волков [и др.] // Докл. АН СССР. – 1970. – Т. 195. – № 5. – С. 1084–1087.
4. Бузников, А. А. Ручной спутниковый спектрограф РСС–3 для спектрометрирования Земли из космоса / А. А. Бузников, В. М. Орлов // XI Всесоюзное совещание по актинометрии. Ч. II. Приборы и методы наблюдений. – Таллинн: АН ЭССР, 1980.
5. Бузников, А. А. Полевой фотоэлектрический спектрометр / А. А. Бузников, В. И. Леус, Н. Б. Леус // Известия ГЭТУ. – 1995. – Вып. 481. – С. 3–7.
6. Бузников, А. А. Особенности спектральной аппаратуры для проведения полевых исследований растительности / А. А. Бузников, А. В. Андреева, А. В. Буданов // Естественные и технические науки. – 2009. – Т. 40. – № 2. – С. 298–301.
7. Горяинов В. С. Модернизация портативного спектрометра РСС / В. С. Горяинов, А. А. Бузников, Е. В. Костиков // Известия СПбГЭТУ «ЛЭТИ». – 2020. – № 2. – С. 5–17/

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ ОБЪЕКТАМИ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

УДК 629.12

КВАЛИМЕТРИЧЕСКИЙ АСОР-АНАЛИЗ ПРОГРАММНЫХ КОМПЛЕКСОВ РОБОТИЗАЦИИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ИНЦИДЕНТАМИ

Алексеев Анатолий Владимирович
Институт автоматизации процессов борьбы за живучесть корабля, судна
Ленинский пр., 101, Санкт-Петербург, 198262, Россия
e-mail: iapbgks@bk.ru

Аннотация. Роботизация управления информационной безопасностью (РУБ) автоматизированных систем в защищенном исполнении (АСЗИ) сегодня рассматривается как основной способ снижения негативного влияния человеческого фактора операторов АСЗИ, является актуальнейшей, но, одновременно, и весьма сложной научно-практической задачей. Выбор перспективного направления ее решения предусматривает формирование квалиметрической базы данных и знаний (КБДЗ) и обоснование лучшего из возможных (оптимального) альтернативных вариантов. Лучшего из многочисленных программно-аппаратных комплексов (ПК), предлагаемых на рынке и декларирующих возможность автоматического управления информационными инцидентами. В дополнение к ранее выполненному экспресс-анализу вариантов РУБ по технологии QSWOT приведены результаты их многокритериального анализа по технологии АСОР, которые подтвердили перспективность вариантов интеграции SGRC & СПРУ, а также SOC & СПРУ. Это позволяет в реальном масштабе времени оценивать наиболее значимые системные показатели обстановки, прогнозировать ее развитие и принимать упреждающие автоматические решения по управлению информационными инцидентами и информационной безопасностью в целом, контролировать их результативность.

Ключевые слова: роботизация управления инцидентами; квалиметрический анализ; технология QSWOT; технология АСОР; оптимизация решений; реальный масштаб времени.

QUALIMETRIC ASOR-ANALYSIS OF SOFTWARE SYSTEMS FOR ROBOTIZATION OF INFORMATION INCIDENT MANAGEMENT

Alekseyev Anatoly
Institute of automation of processes of struggle for survivability of the ship, vessel
101 Leninsky Av, St. Petersburg 198262, Russia
e-mail: iapbgks@bk.ru

Abstract. Robotization of information security management (RUB) of automated systems in protected execution (ASSI) is considered today as the main way to reduce the negative impact of the human factor of ASSI operators, is the most urgent, but at the same time, a very difficult scientific and practical task. The choice of a promising direction for its solution provides for the formation of a qualimetric database and knowledge (KBDZ) and the justification of the best possible (optimal) alternative options. The best of the numerous software and hardware complexes (PCs) offered on the market and declaring the possibility of automatic management of information incidents. In addition to the previously performed express analysis of RUB variants using QSWOT technology, the results of their multi-criteria analysis using ASOR technology are presented, which confirmed the prospects of SGRC & SPRU integration options, as well as SOC & SPRU. This allows you to evaluate the most significant system indicators of the situation in real time, predict its development and make proactive automatic decisions on managing information incidents and information security in general, monitor their effectiveness.

Keywords: robotization of incident management; qualimetric analysis; QSWOT technology; ASOR technology; optimization of solutions; real-time scale.

Актуальность. Минимизация негативного влияния субъективных свойств операторов при управлении обеспечением информационной безопасности (ОИБ) АСЗИ продолжает и сегодня оставаться одной из острейших и нерешенных проблем. Конструктивным направлением ее решения, по нашему мнению, следует считать роботизацию управления безопасностью [1-5], позволяющую перейти к автоматическому режиму управления информационными

инцидентами (киберугрозами), их анализу, синтезу наиболее рациональных (оптимальных) решений и их реализации. В контексте управления ОИБ это означает концептуальный переход от целераспределения, ранее выполнявшегося операторами, к так называемому целеполаганию и по существу – исключению операторов из контура оперативного (административного, диспетчерского) управления, делегирования им прав системного управления (управления более высокого уровня).

В этой связи развитие систем автоматизированной поддержки принятия решений в направление систем поддержки решений и управления (СПРУ) [6] позволяет обеспечить этот переход, но требует ускоренного их технологического развития в части интеллектуализации процессов управления (ИСПРУ). Наблюдаемый сегодня рост соответствующих предложений на рынке АСЗИ подтверждает данную тенденцию [1-3], но требует пристального внимания и разделению вопросов фактической реализации процедур автоматического (роботизированного) управления информационными инцидентами, ОИБ в целом и их декларации.

Методический подход. С этой целью воспользуемся известным и наиболее совершенным методом многокритериального сравнения качества альтернативных вариантов ИСПРУ, формированием соответствующих КБДЗ. Методом сравнения качества объектов анализа как системной меры (комплекса свойств и характеристик) их соответствия своему предназначению.

Причем, сравнения с учетом всех стадий их жизненного цикла (ЖЦ). От стадии создания с оценкой проектного качества (КП) Q по агрегированному (интегральному, сводному, обобщенному) показателю качества (АПК) до стадии эксплуатации. С оценкой эффективности эксплуатации (КЭ) как меры реализации КП $W=Q_э/Q$, где $Q_э$ – проектное качество, рассчитываемое [7] по исходным данным на стадии эксплуатации.

Более того, с оценкой качества жизненного цикла (КЖ) в целом с учетом всех его 8 стадий (для автоматизированных систем согласно ГОСТ 34.601-90, включающих: формирование требований (к АСЗИ), разработку концепции, технического задания, эскизного проекта, технического проекта, рабочая документация, ввод автоматизированной системы в действие, сопровождение) по модели

$$G = C_K^Г[\beta_k, C_I^Г(\propto_i, W_i)], \quad (1)$$

где $C_K^Г[\beta_k, \dots], C_I^Г(\propto_i, \dots)$ – согласно [7] операторы свертки с соответствующими индексами критериальных предпочтений (весовыми коэффициентами) $\propto_i$ и β_k по гармоническому алгоритму (Г) показателей КЭ W_i для всех стадий ЖЦ $k \in [1, K]$ с их общим числом $K = 8$ с соответствующими этапами ЖЦ $i \in [1, I]$ при общем числе этапов, приведенном в ГОСТ 34.601-90, $I = 26$.

Состояние предмета исследования. В дополнение и развитие к ранее выполненному экспресс-анализу 14 вариантов РУБ по технологии QSWOT-экспресс-анализа [8] на рис. 1 приведен фрагмент КБДЗ программных комплексов ПК роботизированного управления информационными инцидентами (ИСПРУ) по 7 лидирующим из 14 рассмотренных альтернативных вариантов ПАК РУБ АСЗИ (из более 50 вариантов в КБДЗ).

Квалиметрический SWOT-анализ альтернативных вариантов решения комплекса задач СУИБ

i			*ИКЗ свойств:*	0,4		0,25		0,2		0,15	0,5	
Шифр средства, сертификат	*Назначение средства, сертификация. Включённые в КРОПУР варианты выделены зелёным фоном*	**S.Сильные (внутренние) стороны**	**S**	**W.Слабые (внутренние) стороны**	**W**	**O.Возможности развития с учетом внешних факторов**	**O**	**T.Угрозы развития с учетом внешних факторов**	**T**	**Q**	**Rq**
17. МДО ПК "СПРУ-ИБ" (ИП, 2018, СПбГМТУ)	Мониторинг системных показателей качества обеспечения ИБ. Интеллектуальная поддержки принятия (ИПП) проектных и управленческих решений (ПУР). Идентификация образов инцидентов, атак, вторжений (ИОВ).	Оценка и эффективная визуализация системных показателей качества ОИБ АСЗИ. Ранжированное представление вариантов ПУР.	7,5	Необходимость заимствования данных со сканеров ИБ. Отсутствие промышленного (по результатам ОФР) образца серии. Зависимость от качественных источников данных.	1,5	Роботизированное решение задач управления инцидентами при интеграции со сканерами ИБ. Инвариантность технологии. Имеется отработанный МДО, обеспечивающий доступность серийной	8,7	Отсутствие в настоящее время инвестиций в создание промышленного образца, варианта интеграции. Зависимость от вендеров сканеров ИБ.	1,5	8,12	4
40. Security Vizion SGRC 3.4	Система управления информационной безопасностью ПМУБ СКЗИ АСЗИ. Декларация возможностей (превышающих вариант 52).	Один из первых промышленных ПК автоматизации ИБ с формируемой БДЗ. Оценивается риск ИБ.	8,3	Ограниченные возможности визуализации данных при мониторинге обстановки. Нет оценки системных показателей ИБ.	2,6	Необходимость наращивания возможностей автоматического решения задач.	8,0	Технологическая избыточность (сложность) гетерогенного пути развития	2,0	7,96	9
41. Security Operations Center (SOC)	Система управления информационной безопасностью ПМУБ СКЗИ АСЗИ для Центра управления ИБ.	Автоматическая обработка контента с автоматической блокировкой инцидентов по 5 уровням их критичности и 16 типам.	8,5	Ограниченные возможности по автоматической блокировке контента, минимизации потока ложных срабатываний.	3,0	Необходимость наращивания возможностей автоматического решения задач.	8,5	Технологическая избыточность (сложность) гетерогенного пути развития	2,0	8,02	5
45.SGRC & СПРУ	Интегрированная роботизированная система управления информационной безопасностью ПМУБ СКЗИ АСЗИ, обеспечивающая автоматическое управление ИБ.	Максимально автоматизированный (роботизированный) режим обработки контента с автоматическим блокированием инцидентов по 5 уровням критичности и 16 типам инцидентов.	9,0	Опасность потери конкурентного превосходства разработанного технологического решения.	2,4	Необходимость практической отработки вариантов автоматического решения задач, оптимизации системного решения, минимизации структурно-функциональной избыточности.	8,5	Необходимость поддержания конкурентного превосходства в условиях рынка.	2,0	8,38	2
46.SOC & СПРУ	Интеграция вариантов 41 и 17 с целью наращивания возможностей за счет системной квалиметрии (оценки), мониторинга обстановки, контроля и управления обстановкой.	Практическая работизация процессов управления инцидентами.	9,0	Необходимость формирования КБДЗ с учетом специфики объекта информатизации.	2,5	Возможность масштабирования технологии в широкий круг задач с соответствующим ускоренным их развитием, отработкой.	8,9	Необходимость особого контроля доступности и целостности КБДЗ с целью предотвращения инцидентов рефлексивного управления.	1,8	8,46	1
51. DeviceLock DLP 9 & СПРУ	Интеграция вариантов 52 (32) и 17 с целью наращивания возможностей: системной квалиметрии (оценки), мониторинга обстановки, контроля и управления обстановкой.	Контроль доступа к устройства и интерфейсам, контроль сетевых коммуникаций, контентная фильтрация, удобный интерфейс (СПРУ)	8,6	Отсутствие реагирования на инциденты ИБ и отсутствие управления рисками. Невозможность раскрытия полного функционала СПРУ (СППР)	2,0	Необходимость наращивания возможностей автоматического решения задач.	8,5	Технологическая избыточность (сложность) гетерогенного пути развития	2,0	8,34	3
52. DeviceLock DLP 9	Набор инструментов для администрирования: разграничения доступа, определения разрешенных устройств и сервисов, контроль поведения пользователей. Подробнее см. вариант 32.	Отработанная технология с 2015 г., опыт использования и продаж. Наличие сертификата АМ TestLab № 150, 23.07.2015.	8,3	Интерфейс (работа с деревом консоли) сильно устарели, нуждаются в доработке. Основной упор сделан на организацию процесса работы пользователей и автоматизацию процесса администрирования. Все встроенные процедуры	2,5	Стабильное развитие и совершенствование ПК. Декларация полной интеграции.	8,0	Иностранный вендер, возможность санкций. Необходима высокая квалификация (системы, сервер. БД). Под ОС Windows требует установки MS SQL Server.	2,0	7,99	7

Рис.1 Фрагмент КБДЗ программных комплексов роботизированного управления информационными инцидентами.

Как показано в [8], в сравнении с первоначальным вариантом КБДЗ по состоянию на февраль 2021 г. введение в рассмотрение и практическое тестирование варианта 52 (DLP) и варианта 51 (интеграции варианта 52 с вариантом 17 (СПРУ), названного DLP & СПРУ) позволило, с одной стороны, уточнить свойства и количественные оценки по типовым 4 критериям S, W, O, T и критерию Q, а, с другой стороны, выйти, по мнению авторов, на более корректные сравнительные оценки ПК РУБ по качеству ОИБ с Q=8,46 (вариант 46).

Из рассмотренных декларируемых вариантов РУБ задачу в полном объеме и с требуемым качеством в реальном масштабе времени (РМВ) без интеграции с СПРУ не решает ни один из ПК. Именно интеграция ПК типа DLP, SIEM, SGRC, SOC с ПК типа СПРУ позволяет в РМВ, по существу, автоматически реагировать на

информационные инциденты за счет квалиметрической оценки системных свойств и характеристик процессов РУБ, их безизбыточной визуализации с цветовым кодированием, а также системного мониторинга и контроля.

Приведенные на рис. 1 с использованием технологии QSWOT - экспресс-анализа (по 5 критериям) сравнительные свойства и количественные оценки конкурентного превосходства 14 альтернативных вариантов ПК РУБ подлежат дополнительной проверке и возможному уточнению в соответствии с концепцией полимодельного подхода. В том числе путем сопоставления с результатами многокритериального анализа качества, например, по технологии АСОР, АСПИД, МАИ [2, 6, 7]. Более того, дальнейшая актуализация КБДЗ представляется уже более доступной, так как сравнение новых вариантов ПК удобнее оценивать и анализировать в сопоставлении с выявленными лидерами рынка, что одновременно позволит повысить точность оценивания, корректировать ранее введенные данные.

Вместе с тем, перспективными направлениями дальнейших исследований по обоснованию, разработке технологии и созданию программно-аппаратных средств РУБ, по мнению [8], следует считать интеграцию усилий разработчиков по согласованию позиций в части выбора системы критериев и формированию требований к ПК РУБ, учету широкого спектра вариантов реагирования на информационные вторжения. По согласованию позиций разработчиков и заказчиков в части системы критериальных предпочтений.

В развитие полученных результатов оценки качества ПК по 5 критериям представляется ***актуальным*** выполнить многокритериальное оценивание и анализ предлагаемых технологий и ПК РУБ по технологии квалиметрического анализа, синтеза, оптимизации проектных и управленческих решений (технологии АСОР) с оценкой системных показателей качества по критерию АПК [7]. С последующим обоснованием наиболее предпочтительных ПК ОИБ при решении задач анализа (задача IDS) и предотвращения (задача IPS) информационных вторжений в типовых условиях функционирования АСЗИ. В том числе ПК РУБ для использования на судах, АСЗИ портов и пароходств, систем навигационного обеспечения, АСЗИ береговых центров экстренного реагирования и других объектов морской техники и морской инфраструктуры (ОМТИ).

Модель угроз и система критериев оценивания ИСПРУ. Для реализации названного подхода и многокритериального выбора перспективных из 14 ранее рассмотренных альтернативных вариантов ИСПРУ в классе систем РУБ [8] на рис. 2 представлены в систематизированном виде типовые информационные инциденты ОИБ и типовые меры реагирования на киберугрозы, а на рис. 3 - сформированная 4-х уровневая система критериев оценивания качества ИСПРУ применительно к стадии ЖЦ «5.Технический проект».

Типовые информационные инциденты (киберугрозы) ОИБ

У1 – Несанкционированный доступ в сеть Интернет.
У2 – DDoS-атака (превышение трафиком пропускной способности).
У3 – Многократный ввод неправильного логина/пароля.
У4 – Несанкционированная смена настроек устройства.
У5 – Стихийное бедствие.
У6 – Многократная попытка входа по карточке сотрудника.
У7 – Установка программного обеспечения из «Черного списка».
У8 – Ошибка доступности устройства.
У9 – Ошибка доступа в локальную сеть.
У10 – Вход в систему с просроченной учетной записи.
У11 - Нарушение целостности данных.
У12 – Нарушение требований заказчиков, бизнеса.
У13 – Нарушение требований, регламентов безопасности.
У14 – Нарушение законодательных и нормативных требований.
У15 – Превышение допустимого уровня риска.
У16 – Попытка использования SQL-инъекций.
У17 – Вирусная атака.
У18 – Сетевые, сетецентрические вторжения, атаки, операции.
У19 – Хищение данных, носителей данных.
У20 – Несанкционированное управление доступом.
У21 – Комбинированные угрозы ОИБ.
У22 – Другие виды угроз ОИБ.

Типовые меры (задачи) реагирования на инциденты ОИБ (киберугрозы)

Р1 – Анализ, вербальное моделирование, идентификация инцидента.
Р2 - Формирование, актуализация карточки инцидента (идентификация), включая локализацию (по времени, пространству, диапазону значений).
Р3 – Разработка и актуализация сценария реагирования.
Р4 – Оповещение, уведомление об инциденте.
Р5 – Эвристическое («ручное») принятие решения и его реализация.
Р6 – Автоматическое принятие решения и его реализация (реагирование).
Р7 – Автоматическое реагирование в составе АСЗИ, контроль результата.
Р8 – Автоматическое реагирование через API, контроль результата.
Р9 – Авторегистрация уязвимостей (по ГОСТ Р 56545 - кода, конфигурации (настройки), архитектуры (проектирования), организационной (реализации ОРД, НМД), многофакторной).
Р10 – Адаптация модели, оценка критичности (категоризация) уязвимостей.
Р11 – Классификация инцидентов, моделирование угроз, нарушителей.
Р12 – Визуализация, мониторинг уязвимостей, угроз, инцидентов ОИБ.
Р13 – Формирование алгоритмов реагирования (дерева сценариев).
Р14 – Регламентирование в СМК политик (алгоритмов) реагирования.
Р15 – Верификация мер реагирования, идентификация ложных тревог.
Р16 – Оценка валидности мер реагирования, целей и регламентов ОИБ.
Р17 – Автоматическое распределение полномочий (диспетчеризация).
Р18 – Визуализация обстановки, информирование по статусам уязвимостей
Р19 – Системная оценка (ретроспективный анализ, аналитика киберугроз, политик, концепций, парадигм) обстановки (качества, рисков, проблем).
Р20 – Управление (администрирование) обстановкой (изменениями) по ОИБ (системное планирование, решения, целераспределение, инструктаж, визуализация (информирование), контроль, верификация, валидность, масштабирование, интеграция, когниктивация, целеполагание).
Р21 - Перехват трафика (копирование).
Р22 - Блокирование трафика устройств (флэш, принтер и т.п.).
Р23 – Блокировка трафика сетевых каналов.
Р24 - Карантин трафика («песочница»).
Р25 – Формирование теневых копий.
Р26 – Блокировка по содержимому.
Р27 – Анализ трафика с использованием архивов, КБДЗ.
Р28 – Формирование отчетов, статистическая обработка результатов ОИБ.
Р29 – Запрет передачи многотомного архива (баз данных).
Р30 – Запрет передачи заполненных договоров.
Р31 – Временная выдача прав на файл, папку.
Р32 – Замена пароля.
Р33 – Блокирование неактуальных учетных записей.
Р34 – Комплексные меры реагирования на инциденты ОИБ.
Р35 – Другие меры реагирования на инциденты ОИБ.

Рис. 2. Типовые информационные инциденты ОИБ и типовые меры реагирования на киберугрозы.

Следует отметить, что среди широкого спектра представленных мер реагирования с учетом условий высокой динамики процессов информационного взаимодействия и информационного противоборства [2] лишь немногие (Р6, Р7, Р8. Р17, Р18, Р19, Р22, Р23, Р26, Р27, Р29) могут быть реализованы в реальном масштабе времени. Именно поэтому в качестве базовых свойств и соответствующих групповых показателей качества (ГПК) ИСПРУ, как подсистемы управления, в приоритетном порядке определены их оперативность (своевременность) управления, достоверность используемых данных для управления, устойчивость, скрытность и непрерывность управления, ресурсная обеспеченность (ресурсность) управления.

В качестве частных показателей (ЧПК) на рис. 3 приведены лишь некоторые, наиболее характерные по влиянию на качество управления ОИБ АСЗИ из всего множества ЧПК, отражающих качество решения задач реагирования на киберугрозы Р1…Р35 согласно рис. 2.

При этом, традиционные критерии оценки информационной безопасности (ИБ, как состояния защищенности информации, отражающего устойчивость (живучесть в условиях информационного противоборства) ОИБ, как процесса управления) - конфиденциальности, доступности, целостности информации, вошли в соответствующие ГПК, отражающие свойства процесса управления ОИБ и характеризующие его скрытность, непрерывность управления и достоверность используемых при этом данных.

Интересно отметить, что число критериев в отдельных публикациях достигает 180 [9] и, казалось бы, позволяет достоверно оценивать качество ПК РУБ. Однако, это справедливо лишь в случае агрегирования ЧПК в единый (обобщенный, интегральный) показатель качества типа АПК (см. рис. 3), который единственный позволяет количественно оценить и сравнивать альтернативные варианты ПК АСЗИ. Без данной процедуры процесс моделирования качества АСЗИ сводится, по существу, к вербальному описанию и не дает возможности количественного анализа, синтеза, а, тем более, оптимизации проектных решений.

Следует также отметить, что ЧПК на рис. 3 могут рассматриваться как результат отдельного сведения к данным ЧПК других показателей качества, детальнее отражающих соответствующие процессы. Так, например, ЧПК «1.6.Полнота мониторинга обстановки, %» оценивается через отношение числа используемых для мониторинга каналов к их общему числу, равному числу 35 возможных киберугроз У1…У22 (рис. 2).

Рис. 3. Принятая для оценки качества ПК РУБ система критериев и показателей.

Модель оценки качества ПК РУБ (ИСПРУ). В качестве аналитической модели оценки альтернативных вариантов ПК ИСПРУ в классе систем РУБ примем реализованный в ПК «АСОР.21» [6, 7] полимодельный квалиметрический метод оценки АПК и системной оптимизации (ПКМ СО) ОМТИ в виде [7]

$$Q_k = C^{\text{А}}_{k,12}\{w_m, C^{\text{М}}_{m,7}[w_g, C^{\text{Г}}_{g,31}(w_n, q_n)]\}, \quad (2)$$

где: $C^{t_N}_{g,31}(w_n, q_n)$, $C^{\text{М}}_{m,7}[w_g, \dots]$, $C^{\text{А}}_{k,12}\{w_m, \dots\}$ – соответствующие обобщенные операторы свертки ЧПК q_n при их общем числе $N = 31$ (см. рис. 2) в g - ый ГПК при их общем числе $G = 7$. Соответственно свертки ГПК в МПК при принятом их общем числе $M = 12$ и МПК в АПК по алгоритму типа для: аддитивного (линейного) алгоритма (А), впервые предложенного А.Н. Крыловым; мультипликативного алгоритма (М), предложенного Д. Нэшем; гармонического алгоритма (Г) и других алгоритмов свертки.

Наличие возможности количественной оценки качества ПК (2) позволяет на основе числового (цифрового) моделирования перейти от задач анализа к задачам параметрического синтеза вариантов построения и эксплуатации средств РУБ с выбором оптимального (лучшего из возможных) варианта. Более того, формирование и актуализация соответствующих КБДЗ обеспечивает возможность их обоснованного научно-технического, инновационного и инвестиционного развития. Причем, включение в состав КБДЗ новых вариантов ПК производится на основе сопоставления с соответствующими рейтинг-лидерами, что, как показывает практика, не только повышает достоверность оценивания их ЧПК, ГПК, МПК, АПК, но и позволяет корректировать уже имеющиеся в КБДЗ данные, т.е. повышать достоверность данных в целом.

В качестве ЧПК для программных и аппаратно-программных средств ОИБ, в том числе в составе критериев 1.7, 2.3, 3.4, 4.5 и др., следует также принять рекомендуемые критерии, предусмотренные ГОСТ Р 52447-2005, с соответствующим согласованием их с организациями заказчиков, вендеров и учетом в составе регламентов системы менеджмента качества предприятий-проектантов.

Результаты цифрового моделирования. На рис. 4 приведены результаты квалиметрического сравнения названных выше 7 альтернативных вариантов ПК РУБ АСЗИ с использованием ПК «АСОР.21» [7] и исходных данных, в том числе представленных в подробном аналитическом обзоре [9].

Анализ полученных результатов подтверждает с некоторым смещением оценок перспективность приоритетного развития варианта «45.SGRC & СПРУ» при конкурентным превосходстве по отношению к варианту «46.SOC & СПРУ» порядка 100%*(0,77/0,75-1)=3%, а в сравнении с вариантом 52 – на 64%. Как показывает практика квалиметрических многокритериальных оценок [1-5, 7, 8], подобные оценки можно считать достаточно значимыми. Близость оценок по значению АПК конкурентных вариантов 45, 46, 51 с учетом погрешностей задания исходных данных дополнительно указывает на их конкурентность и целесообразность организационного объединения усилий вендеров DLP, SGRC, SOC, СПРУ и соответствующую возможность форсированной разработки перспективной технологии создания ПАК РУБ.

Тем самым ускоряя переход от декларации возможностей к их фактической цифровизации. В свою очередь, наличие методического и технологического аппарата позволит обоснованно принимать соответствующие проектные и организационные, инновационные и инвестиционные решения.

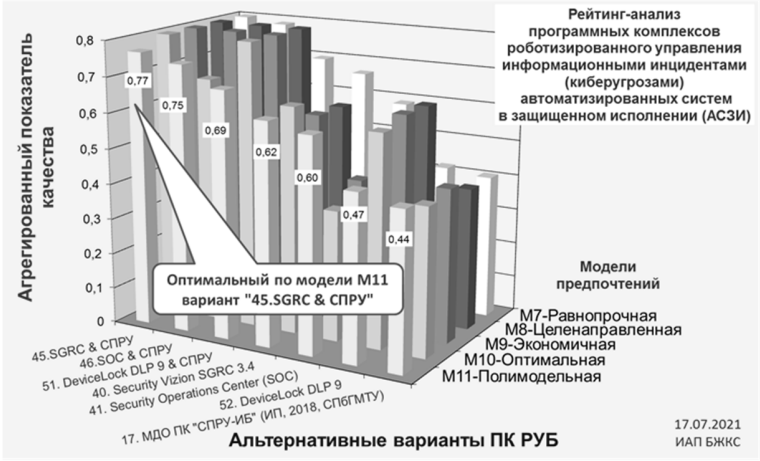


Рис. 4. Сравнительная оценка качества ПК РУБ АСЗИ.

В свою очередь, приведенные данные можно рассматривать как результат цифровизации качества технологического управления информационными инцидентами (киберугрозами) на данный момент времени.

Заключение. Ранее выполненный экспресс-анализ и представленный выше АСОР-анализ вариантов РУБ АСЗИ подтвердили перспективность развития технологий и программных комплексов SGRC, SOC, DLP в сочетании с вариантами их интеграции SGRC & СПРУ и SOC & СПРУ. Это позволит в реальном масштабе времени

оценивать наиболее значимые системные показатели качества обстановки, прогнозировать ее развитие и принимать упреждающие автоматические (роботизированные) решения по управлению информационными инцидентами и информационной безопасностью в целом, а также контролировать их результативность.

Перспективными направлениями дальнейших исследований по обоснованию, разработке технологии и созданию программно-аппаратных средств роботизированного управления инцидентами информационной безопасности, по нашему мнению, следует считать интеграцию усилий разработчиков по согласованию позиций в части выбора системы критериев и критериальных предпочтений, по формированию требований к ПАК РУБ, по учету широкого спектра вариантов реагирования на информационные вторжения.

Более того, по реализации структурной, функциональной, алгоритмической и системной оптимизации автоматизированных систем в защищенном исполнении в целом, что в условиях тенденции критического роста их сложности и сложности процессов информационного взаимодействия и возможного информационного противоборства является весьма значимым и актуальным.

СПИСОК ЛИТЕРАТУРЫ

1. 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). XII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2021 г.: Материалы конференции / СПОИСУ. – СПб., 2021.
2. Алексеев А.В., Воробьев В.И. Информационное противоборство: 20 лет концептуального и технологического развития // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 1 / СПОИСУ. – СПб., 2015, с. 153 – 159.
3. Алексеев А.В., Балицкая К.В. Роботизация управления как способ снижения негативного влияния человеческого фактора на информационную безопасность АСЗИ / Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 7 / СПОИСУ. – СПб., 2019, с. 237-242.
4. Алексеев А.В., Куприянов Д.О., Заведеев Ю. М., Стефанович И.Д. QSWOT-Анализ интеллектуальных технологий управления ИБ морских интегрированных автоматизированных систем // Актуальные проблемы морской энергетики: материалы десятой международной научно-технической конференции в рамках Пятого Всероссийского научно-технического форума «Корабельная энергетика: из прошлого в будущее». – СПб.: Изд-во СПбГМТУ, 2021, с. 363 – 369.
5. Алексеев А.В., Москаленко В.А., Куприянов Д.О., Заведеев Ю. М., Стефанович И.Д., Гадаев Е.М. Программный комплекс поддержки принятия решений по оценке технической готовности корабля к выходу в море / Перспективные направления развития отечественных информационных технологий: материалы VII межрегиональной научно-практической конф. Севастополь, 21-25 сентября 2021 г. / Севастопольский государственный университет; науч. ред. Б.В. Соколов. – Севастополь: СевГУ, 2021.
6. Алексеев А.В., Смольников А.В., Ушакова Н.П., Сус Г.Н. Программный комплекс Макетного действующего образца Системы информационной поддержки судоводителей при обеспечении безопасности эксплуатации в части грузовых операций, локализации аварийных ситуаций, аварий и борьбы за живучесть морских объектов повышенного риска (ПК МДО СИП ЛА-ГО о3) – Свидетельство о государственной регистрации программ для ЭВМ (Реестр программ Федеральной службы по интеллектуальной собственности) № 2014614620, 29.04.2014 (заявка № 2014611813, 05.03.2014).
7. Алексеев А.В. Модель инвариантной оценки качества и эффективности объектов морской техники / Морские интеллектуальные технологии/Marine intellectual technologies, № 2 том 2, 2020, с. 53-60.
8. Алексеев А.В., Куприянов Д.О., Заведеев Ю.М., Гадаев Е.М., Стефанович И.Д. Квалиметрический SWOT-анализ программных комплексов роботизации управления информационными инцидентами / Информационная безопасность регионов России (ИБРР-2021). XII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30.10.2021: Материалы конференции / СПОИСУ. – СПб., 2021.
9. Как мы DLP-систему выбирали (практический опыт) - https://habr.com/ru/post/440838/ (Дата обращения – 7.01.2021).

УДК 629.12

МЕТОДОЛОГИЯ ОЦЕНКИ, МОНИТОРИНГА, АНАЛИЗА И КОНТРОЛЯ КОНФИДЕНЦИАЛЬНОСТИ, ДОСТУПНОСТИ, ЦЕЛОСТНОСТИ ИНФОРМАЦИИ

Алексеев Анатолий Владимирович
Институт автоматизации процессов борьбы за живучесть корабля, судна
Ленинский пр., 101, Санкт-Петербург, 198262, Россия
e-mail: iapbgks@bk.ru

Аннотация. Вопрос оценки и контроля качества предоставляемых услуг по обеспечению информационной безопасности и информационной живучести (ОИБ) любых объектов информатизации является центральным как на стадии создания автоматизированных систем в защищенном исполнении (АСЗИ), так и на стадиях их эксплуатации, модернизации. Вместе с тем, задача цифровизации качества и эффективности ОИБ АСЗИ как в теоретическом, методологическом, так и в прикладном аспектах сегодня практически ждет своего приоритетного решения. Обобщены и представлены методология и результаты предыдущих исследований по реализации концепции полимодельной квалиметрической оценки, мониторинга, анализа и контроля качества ОИБ, включая традиционные свойства конфиденциальности, доступности, целостности информации в процессе информационного взаимодействия и информационного противоборства. Приведен пример количественной оценки проектного качества и эффективности ОИБ применительно к объектам критической инфраструктуры (КИИ) типа АСЗИ «Большой порт «Санкт-Петербург». Показана возможность прогнозирования программ развития, выявления, анализа и нейтрализации соответствующих угроз ОИБ.

Ключевые слова: система критериев информационной безопасности; квалиметрия защищенности систем; методология; полимодельный квалиметрический метод; контроль качества; мониторинг управления.

METHODOLOGY OF ASSESSMENT, MONITORING, ANALYSIS AND CONTROL OF CONFIDENTIALITY, AVAILABILITY, INTEGRITY OF INFORMATION

Alekseev Anatoly
Institute of automation of processes of struggle for survivability of the ship, vessel
101 Leninsky Av, St. Petersburg 198262, Russia
e-mail: iapbgks@bk.ru

Abstract. The issue of evaluating and controlling the quality of services provided to ensure information security and information survivability (OIB) of any informatization objects is central both at the stage of creating automated systems in protected execution (ASSI), and at the stages of their operation and modernization. At the same time, the task of digitalizing the quality and efficiency of the OIB ASZI, both in theoretical, methodological, and applied aspects, is practically waiting for its priority solution today. The methodology and results of previous studies on the implementation of the concept of polymodel qualimetric assessment, monitoring, analysis and quality control of OIB, including the traditional properties of confidentiality, accessibility, integrity of information in the process of information interaction and information confrontation, are summarized and presented. An example of a quantitative assessment of the project quality and efficiency of the OIB in relation to critical infrastructure facilities (CII) of the ASZI «Big Port «St. Petersburg»type is given. The possibility of forecasting development programs, identifying, analyzing and neutralizing the corresponding OIB threats is shown.

Keywords: system of information security criteria; system security qualimetry; methodology; polymodel qualimetric method; quality control; management monitoring.

Актуальность проблемы. Сегодня комплексная безопасность любых объектов информатизации, включая объекты морской техники и морской инфраструктуры (ОМТИ), их информационная безопасность (ИБ) [1, 2] и информационная живучесть (ИЖ) в условиях информационного противоборства [3], не могут рассматриваться в прикладном контексте без соответствующей методологии, средств, систем и технологии количественной оценки, анализа и синтеза (методологии цифровизации ИБ и ИЖ), как не могут рассматриваться, например, процессы движения электронов в проводнике без знания законов Ома и Кирхгофа.

Тем более, без цифровизации (количественной оценки, анализа и синтеза) динамики процессов ИБ и ИЖ, включая мониторинг (наблюдение во времени и пространстве совокупности показателей процессов), анализ и контроль качества предоставляемых услуг по обеспечению (управлению) ИБ и ИЖ (ОИБ), включая традиционные свойства конфиденциальности (К), доступности (Д), целостности (Ц) информации.

Вместе с тем, сложность процессов информационного взаимодействия различных объектов, включая ОМТИ, в сочетании с необходимостью учета влияния субъективных (положительных и негативных) свойств операторов в составе АСЗИ практически любого объекта информатизации, но, особенно, объектов КИИ типа «Большой порт «Санкт-Петербург», породили сегодня проблему особой сложности. Проблему, которая по данным многолетнего анализа источников не имеет своего решения. Проблему и задачу, по существу, цифровизации качества и эффективности ОИБ АСЗИ, которая как в теоретическом, методологическом, так и в прикладном аспектах сегодня ждет своего внеочередного (приоритетного) научно-практического решения [1].

Более того, проблема разработки методологии и технологии контроля качества ОИБ является сегодня как никогда востребованной и актуальной при анализе и сравнении многочисленных предложений рынка, существующих АСЗИ. При синтезе АСЗИ в инновационных компаниях и организациях различных форм собственности. А, тем более, при оптимизации их архитектуры, функционала, свойств и характеристик в процессе поиска новых высокоэффективных технологических решений по ОИБ АСЗИ.

Направление решения проблемы. Определенные предпосылки успешного решения данной проблемы появились в связи с разработкой концепции и методологии полимодельного квалиметрического оценивания и системной оптимизации сложных объектов (ПКМ СО) [2, 3], инвариантных к специфике объектов анализа и исследовательского проектирования (ОИП).

Именно неизменность (инвариантность) предложенного математического аппарата и последовательности методических процедур для разнородных ОИП [2] позволили сформулировать, апробировать и предложить концепцию и комплекс (по существу – методологию цифровизации ОИБ) взаимосвязанных методов и методик оценки, мониторинга, анализа, контроля проектного качества (КП) средств и систем ОИБ на стадии их создания (проектного обоснования и внедрения), а также эффективности эксплуатации (КЭ, как меры реализации проектного качества) на стадии их эксплуатации [2, 4, 5].

Методология цифровизации ОИБ АСЗИ. Предлагаемый комплекс взаимосвязанных методов количественной оценки, анализа и синтеза качества ОИБ АСЗИ (как совокупности свойств и характеристик, как меры соответствия предназначению), включает, как показано на рис. 1.

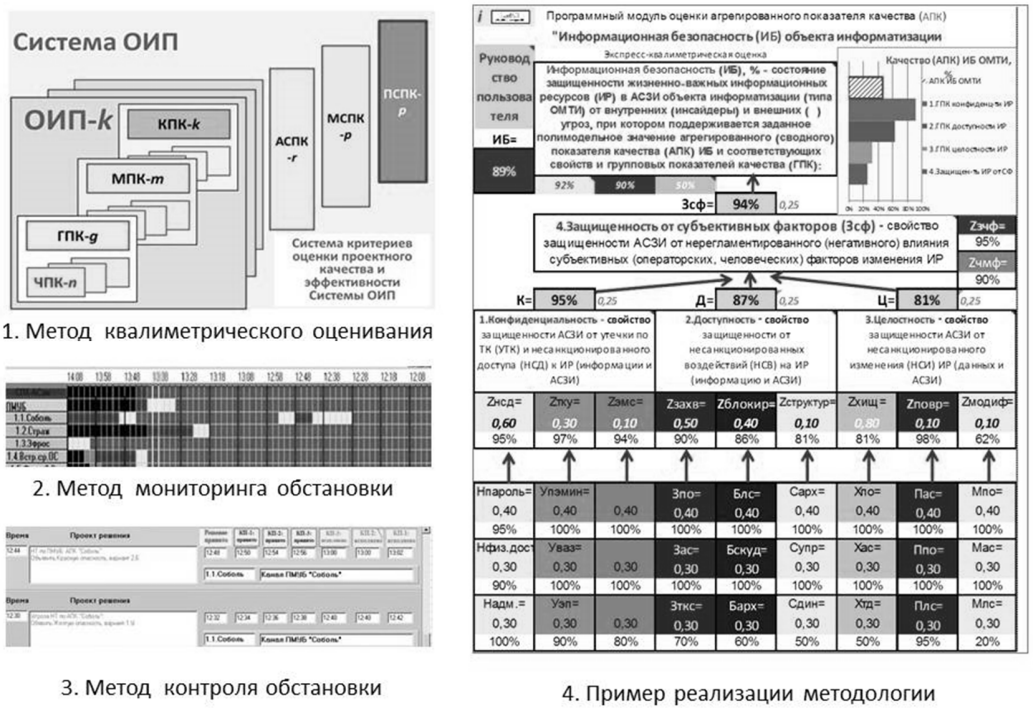


Рис. 1. Методология цифровизации, контроля качества ОИБ на примере АСЗИ «Большой порт Санкт-Петербург».

Метод квалиметрической оценивания качества объектов исследовательского проектирования (ОИП), включая качество ОИБ (рис. 1.1), включающий описание и рекомендации по основным положениям методических и технологических процедур:

разработки и обоснования 7-уровневой системы критериев оценки качества системы ОИБ, отражающих: частные технические и организационные параметры функционирования (ЧПК) АСЗИ (включая требования по ГОСТ Р 52447-2005); их функциональные свойства (ГПК, включая оценку конфиденциальности, доступности, целостности [5]); свойства используемых моделей агрегирования с учетом матриц индексов критериальной значимости (МПК); комплексный (сводный, агрегированный) показатели качества (КПК) отдельных средств в составе АСЗИ (как элементов сложной системы); агрегированный системный показатель качества для всего комплекса средств в составе АСЗИ (АСПК); модельный системный показатель качества, учитывающий свойства и матрицу индексов значимости средств в составе АСЗИ (МСПК); полимодельный системный показатель качества АСЗИ, отражающий в целом качество АСЗИ по предназначению, включая ОИБ (ПСПК);

– цифровизации частных (включая процедуры нормирования), групповых, модельных, комплексных, агрегированных системных, модельных системных и полимодельного системного показателей качества, включая их нормирование;

– агрегирования ЧПК, ГПК, МПК, КПК, АСПК, МСПК по оптимальному (гармоническому) алгоритму свертки и другим альтернативным алгоритмам свертки показателей качества в единый (интегральный) показатель качества (ПСПК) АСЗИ:

– использования автоматизированных средств поддержки квалиметрической оценки качества (цифровизации ОИБ) и управления АСЗИ.

Метод мониторинга обстановки на основе системной визуализации обстановки по ОИБ (рис. 1.2), включающий описание и рекомендации по основным положениям методических и технологических процедур:

– обоснования требований, формирования и эргономической оптимизации интерфейсных форм (видеокадров) системной визуализации данных, их структуры, состава и свойств;

– обоснования возможностей прогнозирования обстановки с учетом динамики системы показателей ОИБ на основе, например, регрессионного анализа ЧПК, ГПК, МПК, КПК, АСПК, МСПК, ПСПК;

– систематизации и анализа системных данных на основе использования малоизбыточного (2-х битового) цветового кодирования, анализа, классификации ситуационных образов и их идентификации.

Метод контроля и управления обстановкой на основе системного анализа обстановки по ОИБ, ситуаций (информационных инцидентов, киберугроз) с информационной, информационно-аналитической и интеллектуальной поддержкой принятия решений операторами (центров управления, ситуационных центром) по ОИБ (рис. 1.3), включающий описание и рекомендации по основным положениям методических и технологических процедур:

– формирования и актуализации когнитивной квалиметрической базы данных и знаний (КБДЗ), порядка ее актуализации и использования в составе подсистем поддержки принятия решений АСЗИ;

– автоматического контроля заданных регламентов (уровней требований), требований организационно-распорядительной и нормативно-методической документации с соответствующим оповещением;

– использования автоматизированных средств поддержки квалиметрической оценки качества АСЗИ при принятии решений по контролю проектного качества и эффективности эксплуатации АСЗИ, включая контроль безопасности информации, конфиденциальности, доступности, целостности информации;

– использования полимодельного дискреционного алгоритма синтеза проектов решений и их последующей оптимизации операторами АСЗИ;

– интерпретации результатов оценки, мониторинга, анализа, синтеза и контроля конфиденциальности, доступности, целостности информации, системного анализа ситуаций и обстановки в целом;

– верификации полученных результатов цифровизации ОИБ АСЗИ и оценки их валидности.

Примеры реализации методологии цифровизации ОИБ АСЗИ. На рис. 1.4 для иллюстрации приведен пример реализации рассмотренной методологии цифровизации ОИБ применительно к объектам критической инфраструктуры (КИИ) типа АСЗИ «Большой порт «Санкт-Петербург» с учетом характерных решаемых задач и проведения вариантных оценок в части оценки ГПК проектного качества по критериям конфиденциальности (К=95% в условиях принятых на рис. 1.4 исходных данных), доступности (Д=87%), целостности (Ц=81%), защищенности от субъективных факторов (Зсф=94%), а также информационной безопасности (ИБ=89%).

Приведенные результаты подтверждают возможность многокритериального оценивания качества ОИБ АСЗИ, их интерпретации, верификации и оценки валидности.

На рис. 2 приведен пример реализации методологии цифровизации ОИБ в части агрегирования показателей качества для аппаратно-программных и программных средств ОИБ АСЗИ.

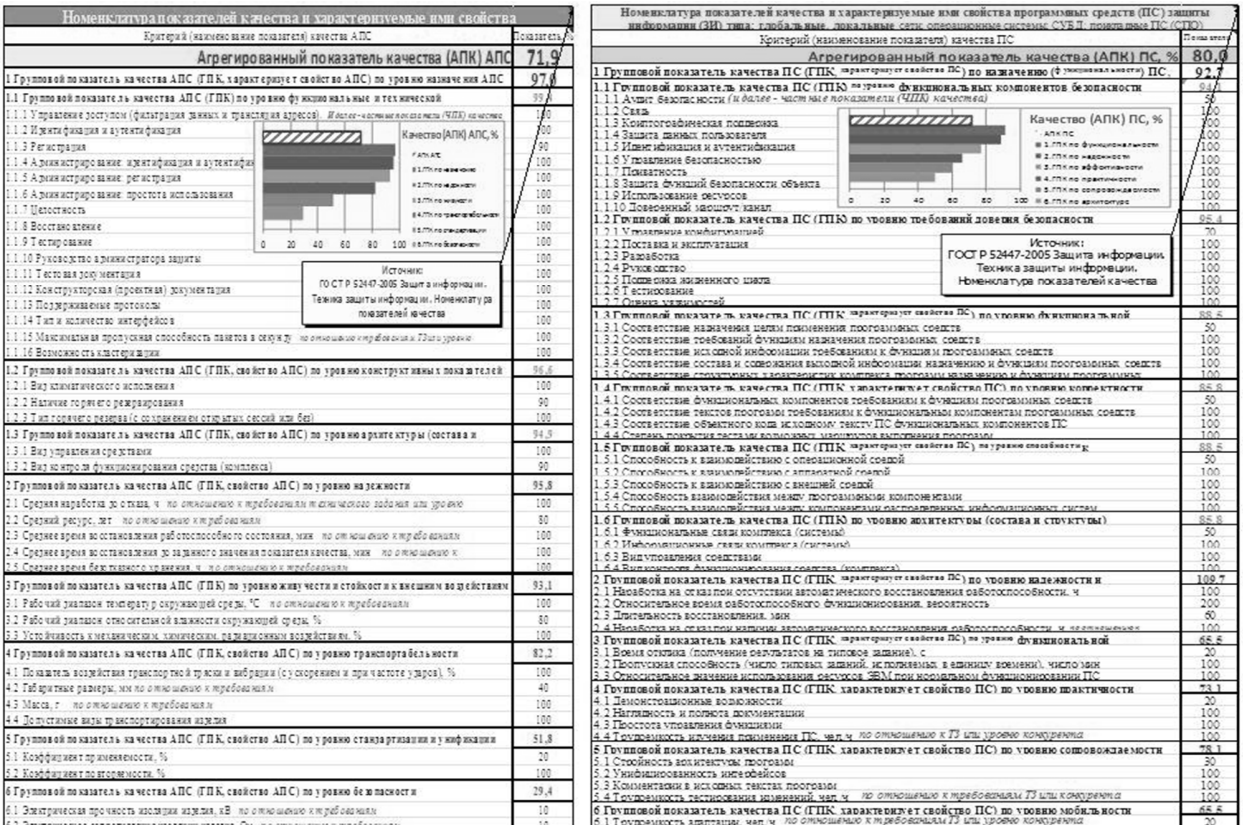


Рис. 2. Система критериев оценки качества аппаратно-программных и программных средств ОИБ АСЗИ.

Особенности реализации методологии цифровизации ОИБ АСЗИ. Весьма важным вопросом при агрегировании показателей качества является вопрос обоснованного выбора индексов критериальной значимости (ИКЗ, весовых коэффициентов). Для этого могут быть использованы в качестве предварительных оценок известные методы анализа иерархий Т. Саати, анализа и синтеза при информационном дефиците профессора Н.В. Хованова и другие [1, 2]. Тем не менее, решение и формирование матрицы ИКЗ должны проводиться в согласованном режиме между заказчиками и разработчиками при лидирующей роли заказчиков. Именно они наиболее полно представляют

модель и порядок реализации методов и способов эффективного использования средств ОИБ АСЗИ. Более того, именно им принадлежит право корректировки параметров, характеристик и выбора моделей оценивания качества ОИБ АСЗИ, оценки получаемых результатов, их верификации и оценки валидности.

Другим важным вопросом реализации представленной методологии цифровизации ОИБ АСЗИ следует считать обоснование и принятие решений по используемым исходным данным и оценки их допустимых погрешностей. Одним из перспективных направлений в этом вопросе следует считать систематизацию и актуализацию данных при формировании КБДЗ, использование метода оценки сопоставимости при обосновании исходных данных и, безусловно, их экспериментальной апробации, физического и цифрового моделирования, экспертного оценивания, их верификации и документального подтверждения.

В условиях возрастания сложности объектов и процессов информатизации, значимости процессов моделирования сложных систем и роста числа предлагаемых моделей на качественно новом уровне должен решаться и вопрос квалиметрии моделей и полимодельных комплексов. На уровне, заданном, концептуально и методологически представленным членом-корреспондентом РАН Р.М. Юсуповым, профессором Микони С.В. и профессором Соколовым Б.В. в монографии [6]. В этой связи и данное предложение по реализации и развитию полимодельного квалиметрического метода и методологии системной оптимизации [2, 3] можно рассматривать в качестве альтернативного при формировании соответствующей базы моделей и полимодельных комплексов.

Особое значение также имеют вопросы автоматизации процедур цифровизации и поддержки принятия решений, без качественного решения которых в условиях критического роста объема обрабатываемых данных практически не возможно сегодня обеспечить ожидаемые результаты, их достоверность, возможность использования и реализации при исследовательском, проектном обосновании перспективных вариантов АСЗИ, а также в процессе их эксплуатации.

На рис. 3 для иллюстрации приведен пример реализации методологии цифровизации ОИБ АСЗИ в части оценки, прогнозирования и мониторинга качества жизненного цикла (ЖЦ) с использованием модели (1) из [5].

ПК "Прогноз_9.3"_ЖЦ АСЗИ	**Мониторинг качества Жизненного цикла АСЗИ по состоянию на:**						**18.12.21 15:09**		
Цель	**Стадии ЖЦ АСЗИ**	**Этапы ЖЦ АСЗИ**	**ИКЗ (важность),%**	**Начало этапа**	**Срок окончания**	**Текущий результат**	**Прогноз по этапу**	**Прогноз по стадии ЖЦ**	**Качество ЖЦ**
Информационно-аналитическая поддержка: ИАП БЖКС, iapbgks@bk.ru, 8-909-580.2150	**1. Формирование требований к АСЗИ "БП СП" (ее модернизацию)**	1.1. Обследование объекта и необходимости создания (модернизации) АСЗИ.	40,0%	29.10.21	03.11.21	100	100,0	100,0	**86,3**
		1.2. Формирование требований Заказчика к АСЗИ.	40,0%	03.11.21	08.11.21	100	100,0		
		1.3. Оформление отчета о выполненной работе и заявки на разработку АСЗИ (тактико-технического задания).	20,0%	08.11.21	18.11.21	100	100,0		
Обеспечение заданного качества жизненного цикла АСЗИ применительно к объекту морской инфраструктуры "Большой порт "Санкт-Петербург" (проект)	**2. Разработка Концепции модернизации АСЗИ**	2.1. Изучение объекта.	20,0%	18.11.21	08.12.21	99	44,6	73,2	
		2.2. Проведение необходимых НИР.	50,0%	03.11.21	03.11.22	10	80,0		
		2.3. Разработка вариантов Концепции модернизации АСЗИ и выбор варианта концепции, удовлетворяющего требованиям Заказчика.	25,0%	08.11.21	23.12.21	75	83,1		
		2.4. Оформление отчета о выполненной работе.	5,0%	23.12.21	02.01.22	0	90,0		
	3. Техническое задание	3.1. Разработка и утверждение ТЗ на модернизацию АСЗИ.	100,0%	02.01.22	01.02.22	0	90,0	90,0	
	4. Эскизный проект (ЭП)	4.1. Разработка предварительных проектных решений по системе и ее частям (элементам).	80,0%	01.02.22	03.03.22	0	90,0	90,0	*Цель достигнута*
		4.2. Разработка документации на АСЗИ по ее частям.	20,0%	03.03.22	23.03.22	0	90,0		
	5. Технический проект (ТП)	5.1. Разработка проектных решений по системе и её частям.	45,0%	03.03.22	06.03.22	0	90,0	90,0	
		5.2. Разработка документации на АСЗИ и её части.	10,0%	06.03.22	26.03.22	0	90,0		
		5.3. Разработка и оформление документации на постъавку изделий для комплектации АСЗИ и (или) технических требований (ТЗ) на их разработку.	35,0%	26.03.22	25.04.22	0	90,0		
		5.4. Разработка заданий на проектирование в смежных частях	10,0%	25.04.22	25.05.22	0	90,0		
	6. Рабочая документация (РД)	6.1. Разработка РД на систему и её части.	30,0%	25.05.22	24.06.22	0	90,0	90,0	
		6.2. Разработка или адаптация программного обеспечения	70,0%	24.06.22	03.08.22	0	90,0		
	7. Ввод в действие	7.1. Подготовка объекта информатизации к вводу АСЗИ в	10,0%	03.08.22	23.08.22	0	90,0	90,0	
		7.2. Подготовка (переподготовка) персонала АСЗИ.	10,0%	23.08.22	22.09.22	0	90,0		
		7.3. Комплектация АСЗИ поставляемыми изделиями (ПС, АПС, программно-техническими комплесами, информационными изделиями).	15,0%	22.09.22	22.10.22	0	90,0		**85**
		7.4. Строительно-монтажные работы.	25,0%	22.10.22	21.11.22	0	90,0		**80**
		7.5. Пусконаладочные работы.	5,0%	21.11.22	01.12.22	0	90,0		**50**
		7.6. Проведение предварительных испытаний (ПИ).	10,0%	01.12.22	08.12.22	0	90,0		
		7.7. Проведение опытной эксплуатации (ОЭ).	15,0%	08.12.22	08.03.23	0	90,0		
		7.8. Проведение приемочных испытаний (СИ).	10,0%	08.03.23	23.03.23	0	90,0		
	6. Сопровождение АСЗИ	8.1. Выполнение работ в соответствии с гарантийными обязательствами.	50,0%	23.03.23	22.03.24	0	90,0	90,0	Резерв времени:
		8.2. Послегарантийное обслуживание.	50,0%	23.03.23	**22.03.24**	0	90,0		824

Рис. 3. Система критериев оценки качества аппаратно-программных и программных средств ОИБ АСЗИ.

Приведенные результаты (по модельным исходным данным на 18.12.2021 г.) подтверждают целесообразность системного анализа и мониторинга качества процессов обеспечения ЖЦ АСЗИ. Подобные оценки ожидаемого качества и результативности на срок окончания соответствующих мероприятий, их этапов и стадий ЖЦ с учетом

текущих данных мониторинга позволяют принимать обоснованные и своевременные проектные и управленческие решения по созданию и эксплуатации АСЗИ, включая ОБИ.

Без подобной цифровизации качества реализации долгосрочных программ развития типа приведенной на рис. 3 программы модернизации АСЗИ, включая развитие подсистемы ОБИ, применительно к объекту информатизации «Большой порт «Санкт-Петербург», практически не представляется возможной.

Заключение. Предлагаемая методология и соответствующий комплекс методик [4] позволяют переходить от решения задач анализа качества АСЗИ, включая ОИБ с оценкой, мониторингом и контролем системных свойств и показателей качества, включая конфиденциальность, доступность, целостность информации, к задачам синтетической квалиметрии (в терминологии профессора А.И. Субетто) с выявлением направлений и технологических путей совершенствования свойств и системных характеристик АСЗИ.

Задача квалиметрического синтеза, конечно, является отдельной задачей исследовательского проектирования и требующей, прежде всего, достоверных исходных данных. Среди них «нетиповые» процессы согласования и регламентирования системы критериев, системы индексов критериальной значимости (модельных предпочтений Заказчика), верификации и оценки валидности модели и получаемых оценок. Кроме того, предоставления достоверных значений по частным показателям качества используемой АСЗИ, включая характеристики субъективных свойств персонала. А также по принятой модели угроз информационной безопасности и типовых сценариев действий при возникновении информационных инцидентов, вариантах реагирования на них и мер информационного противодействия. Это, конечно, усложняет для Заказчика задачу выдачи исходных данных, но может быть «упрощено» путем, например, задания по результатам многовариантного моделирования качества с использованием предложенной методологии диапазона исходных данных и вариантов целеполагания.

Представленные в обобщенном виде методология и результаты проведенных исследований по реализации концепции полимодельной квалиметрической оценки, мониторинга, анализа и контроля качества ОИБ, включая традиционные свойства конфиденциальности, доступности, целостности информации в процессе информационного взаимодействия, позволяют на качественно новом уровне с выполнением многовариантных количественных оценок решать задачи исследовательского и проектного обоснования требований и характеристик ОБИ современных АСЗИ, а также обеспечивать требуемую эффективность их эксплуатации, модернизации, возможность выявления, анализа и нейтрализации соответствующих угроз ОИБ.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А.В., Воробьев В.И. Информационное противоборство: 20 лет концептуального и технологического развития // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 1 / СПОИСУ. – СПб., 2015, с. 153 – 159.
2. Алексеев А.В. Модель инвариантной оценки качества и эффективности объектов морской техники / Морские интеллектуальные технологии/Marine intellectual technologies, № 2 том 2, 2020, с. 53-60.
3. 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). XII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2021 г.: Материалы конференции / СПОИСУ. – СПб., 2021.
4. Алексеев А.В. Методика оценки, мониторинга, анализа и контроля конфиденциальности, доступности, целостности информации/ Информационная безопасность регионов России (ИБРР-2021). XII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2021 г.: Материалы конференции / СПОИСУ. – СПб., 2021.
5. Алексеев А.В. Квалиметрический АСОР-анализ программных комплексов роботизации управления информационными инцидентами / Информационная безопасность регионов России (ИБРР-2021). XII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2021 г.: Материалы конференции / СПОИСУ. – СПб., 2021.
6. Микони С.В., Соколов Б.В., Юсупов Р.М. Квалиметрия моделей и полимодельных комплексов: монография. – М.: РАН, 2018. – 314 с.

УДК 629.561

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЗАДАЧЕ КОНТРОЛЯ И УПРАВЛЕНИЯ ГРУЗОПЕРЕВОЗКАМИ МОРСКОЙ ИНФРАСТРУКТУРЫ

Алексеев Сергей Алексеевич, Гончар Артем Александрович, Парфенов Николай Петрович, Стахно Роман Евгеньевич

Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: ksgati@yandex.ru

Аннотация. Представленное в статье решение обеспечивает повышение избирательности, помехоустойчивости и надежности дуплексной радиосвязи между диспетчерским пунктом и объектами управления, которое базируется на материале Патентов РФ авторов статьи № 2733054, Компьютерная система дистанционного контроля и управления объектами морской инфраструктуры, 2020 и № 2725100, Экологический дирижабль, 2020. Предлагаемая система относится к области дистанционного контроля и управления логистикой движения транспорта морской инфраструктуры и может быть использована для принятия решений на всех уровнях контроля и управления процессами на указанных объектах с использованием компьютерной техники.

Ключевые слова: организационное управление; логистика; помехоустойчивость; надежность; фазоманипулированный сигнал.

INFORMATION SECURITY IN THE TASK OF MONITORING AND MANAGING CARGO TRANSPORTATION OF MARINE INFRASTRUCTURE

Alekseyev Sergey, Gonchar Artem, Parfenov Nikolai, Stakhno Roman
St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mail: ksgati@yandex.ru

Abstract. The solution presented in the article provides an increase in the selectivity, noise immunity and reliability of duplex radio communication between the control room and control objects, which is based on the material of the Russian Federation Patents of the authors of article No. 2733054, Computer system for remote monitoring and control of marine infrastructure objects, 2020 and No. 2725100, Environmental Airship, 2020. The proposed system relates to the field of remote control and management of logistics of transport traffic of marine infrastructure and can be used for decision-making at all levels of control and management of processes at these facilities using computer technology.

Keywords: organizational management; logistics; noise immunity; reliability; phase-manipulated signal.

Введение. Реальностью современного транспортного движения является постоянный рост грузопотока, обеспечивающего функционирование объектов морской инфраструктуры. Система контроля и управления движением портовых средств (СКУДПС) представляет собой социальную организационно-техническую, экономическую и производственную структуру. СКУДПС имеет как свою внутреннюю связь, так и связь с внешними, обеспечивающими ее целевую деятельность системами. Управление функционированием этой системой требует широкого спектра информационных решений организационных, технических, социальных, правовых, экономических и хозяйственных вопросов для принятия управленческих команд. В состав СКУДПС входят объекты управления, к которым можно отнести как объекты морской инфраструктуры: здания, сооружения, внутренние и внешние дороги, дорожные ресурсы и сооружения, так и динамические устройства и оборудование: транспортные средства, инженерные и технические конструкции, расположенные на подконтрольной территории. Перечень этих объектов морской инфраструктуры, которые входят в зону ответственности СКУДПС утверждается уполномоченным федеральным органом исполнительной власти, реализующим функции государственной политики и нормативно-правовое регулирование в сфере транспорта в данном регионе.

В условиях роста интенсивности транспортного движения использование крупнотоннажных транспортных средств, перевозка опасных грузов, интенсивность движение транспорта на основных городских путях и подходах к порту увеличивает вероятность транспортных аварий и их неблагоприятных экологических последствий. Среди них одним из самых опасных видов аварийных ситуаций являются столкновения транспортных средств, как на дорогах, так и в акватории порта. Столкновения, аварии в наибольшей степени определяются проблемами организации движения транспорта и в первую очередь в пригородных и загородных зонах, территориях, прилегающих к хозяйствующим инфраструктурам порта и на дорогах с повышенной интенсивностью движения. Экологическая опасность таких происшествий усугубляется отсутствием специальных коридоров для движения транспорта. Учащающиеся аварийные случаи на транспорте, ведущие к катастрофическим последствиям, гибели людей, экологическим катастрофам, а также возросшая угроза террористических актов выдвигают проблему управления обеспечения безопасности на транспорте в ранг общенациональной безопасности.

Основная часть. Наиболее эффективным средством обеспечения безопасности движения транспорта вблизи городских, пригородных и загородных зон могут быть объекты СКУДПС, осуществляющие мониторинг и контроль за соблюдением водителями правил движения, а при необходимости, помощь в определении координат местоположения и при возникновении аварийных ситуаций необходимых характеристик объектов. СКУДПС включает сложный комплекс стационарных технических сооружений вблизи дорожных служб. К основным недостаткам современных СКУДПС относятся ограниченность зоны действия мониторинга дорожной сети, стационарность размещения (местоположения), «привязка» к морской инфраструктуре, громоздкость и сложность применяемых процедур управления, которые требуют дорогостоящего специализированного оборудования и развитой инфраструктуры энергоснабжения. Ключевая функция в основном контуре управления отводится оператору диспетчерского центра СКУДПС, что определяет большое влияние человеческого фактора на принятие решения.

Управление функционированием морской инфраструктуры требует решения широкого спектра технических, организационных, экономических, правовых, социальных и хозяйственных вопросов путем принятия управленческих решений на основе определенных принципов, методов и форм их реализации. Здесь можно выделить три задачи: расширение грузовой базы и других услуг, совершенствование экономического хозяйствования, повышение эффективности оперативного управления. Основные мероприятия по повышению безопасности транспортных перевозок в районах ответственности морской инфраструктуры направлены на совершенствование

организационной и технической оснащенности СКУДПС, что делает эти системы еще более дорогостоящими и громоздкими. В результате использование современных СКУДПС эффективно только в экономически развитых регионах с достаточно мощной транспортной инфраструктурой, связанной с обслуживанием крупнотоннажных перевозок. При этом недостаточно внимания уделяется совершенствованию и усилению роли информационных и интеллектуальных технологий в управлении, которые являются альтернативой технической модернизации. Информационная инфраструктура транспортной системы, основанная на использовании достижений современных информационных технологий, в настоящее время становится ключевым элементом в обеспечении эффективного управления безопасностью транспортных процессов.

Современное развитие и совершенствование информационных технологий, а также технологий искусственного интеллекта позволяет существенно расширить область задач контроля за обстановкой в районе ответственности СКУДПС, которые создают реальную угрозу безопасности его функционирования. К интегральной проблеме из всего выше названного можно выделить проблему организации связи между всеми перечисленными объектами, проблему организации информационной безопасности передачи цифровых данных, проблему эффективности организации сбора и обработки информации.

СКУДПС морской инфраструктуры содержит диспетчерский центр управления, на котором размещены дуплексные передающие радиостанции для связи с объектами управления, компьютерная система обработки информации, приемник GPS-сигналов с антенной, рис. 1.

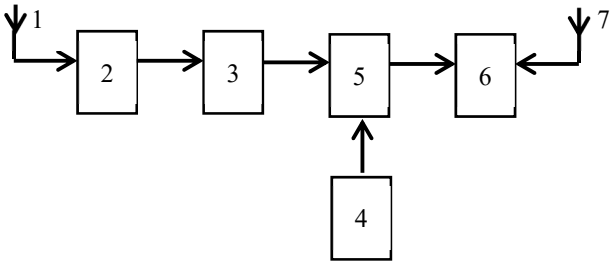


Рис. 1. Схема приемо-передающей радиостанции диспетчерского центра.

В составе 1 – антенна; 2 - приемник ГЛОНАС-GPS сигналов; 3 - прибор дифференциальных поправок; 4 - задающий генератор; 5 - фазовый манипулятор; 6 - усилитель мощности; 7 - передающая антенна [1].

СКУДПС также включает распределенную систему диспетчерских пунктов контроля местоположения и состояния транспортных средств, объектов административного назначения, объектов пожарной безопасности, специального назначения и ретрансляции управленческих сигналов из центра на приемники, находящиеся на объектах контроля.

Каждое транспортное средство или динамической объект морской инфраструктуры должны быть оборудованы специальным контейнером, снабженным радиочастотной меткой, выполненной в виде пьезокристалла с нанесенным на его поверхность алюминиевым тонкопленочным встречно-штыревым преобразователем поверхностных акустических волн (ПАВ) и набором отражателей. Контейнер оборудован дуплексной радиостанцией, приемником навигационных GPS-сигналов, датчиками номера и технического состояния транспортного средства или динамического объекта, а также микропроцессором, к которому они подключены [1]. ПАВ включает: 11 - встречно-штыревой преобразователь, состоящий из двух гребенчатых систем электропроводов в виде гребенок, которые соединены друг с другом шинами 12 и 13, соединенными, в свою очередь, с микрополосковой приемопередающей антенной 10, изготовленной также на поверхности пьезокристалла 19, рис. 2 [1].

В качестве среды приема и передачи информации может использоваться городская радиотелефонная система общего пользования с сотовой структурой.

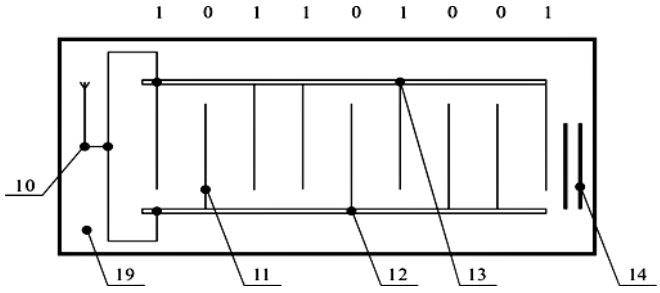


Рис. 2. Функциональная схема радиочастотной метки.

Практические расчеты использования сотовых систем связи показывают, что радиусы зон ячеек могут быть в пределах от 2 до 10 км. В составе предлагаемой СКУДПС для геодезической привязки могут быть использованы возможности космического сегмента связи, состоящего из космических аппаратов и сети наземных станций наблюдения за их работой. Приемники ГЛОНАС-GPS сигналов, установленные в диспетчерском центре, динамических и стационарных пунктах контроля, а также на транспортных средствах и объектах позволяют определять координаты объектов (широту и долготу), скорость их движения и точное время. Каждый ГЛОНАС-GPS спутник излучает на двух частотах (ω1=1757 МГц и ω11=12,275 МГц) специальный навигационный сигнал в виде защищенного бинарного фазоманипулированного (ФМн) сигнала, манипулированного по фазе псевдослучайной последовательностью [3].

Решать подобные проблемы возможно с помощью использования специальных мобильных систем управления движением транспортных средств (МСУДТС). В данной статье рассматриваются вопросы построения эффективных систем мониторинга и управления движением в районе ответственности с использованием МСУДТС, основным элементом информационного обеспечения и связи которого может стать дирижабль. Дирижабль, как элемент МСУДТС, выполняет функции организации связи и ведения дистанционного мониторинга всех объектов морской инфраструктуры, пригородной и загородной дорожной сети, железнодорожных и автомобильных магистралей, линий электропередач и других объектов социальной инфраструктуры, в том числе и природных, а также функции управления всем движением грузоперевозок. Дирижабль имеет аппаратуру оперативной двухсторонней связи между дирижаблем и наземными стационарными и мобильными центрами управления (далее центры управления) с использованием двух частот и сложных сигналов с фазовой манипуляцией (Фмн), что повышает надежность и достоверность обмена дискретной информацией [2]. Дирижабли могут быть использованы качестве ретрансляторов спутниковой системы геодезической привязки. При этом дирижабли могут размещаться на разных высотах и сами выполнять функции объекта геодезической привязки.

Организация связи методом, предложенным в патенте РФ № 2725100, Экологический дирижабль [2] и описанным в предлагаемой статье обеспечит повышение эффективности функционирования СКУДПС за счет улучшения избирательности, помехоустойчивости и надежности дуплексной радиосвязи между дирижаблем, диспетчерским центром, стационарными пунктами контроля и транспортными средствами путем подавления ложных сигналов (помех), принимаемых по дополнительным каналам. Системы фазовой автоподстройки частоты (ФАПЧ) обеспечивают автоматическое слежение за изменениями несущих частот принимаемых сложных Фмн сигналов, которые могут возникать над влиянием различных дестабилизирующих факторов, в том числе и эффекта Доплера.

Приемники ГЛОНАС-GPS сигналов, размещенные на дирижабле также, как и в центре управления СКУДПС и в системе стационарных пунктов контроля, построены по классической схеме, см. рис. 1. Одно и то же значение промежуточной частоты $\omega_{пр}$ здесь получают в результате приема сигналов на двух частотах ω_s и $\omega_з$: $\omega_{пр}= \omega_s - \omega_г$ или $\omega_{пр} = \omega_г - \omega_з$. Следовательно, если частоту настройки ω_s принять за основной канал приема, то наряду с ним будет иметь место зеркальный канал приема, частота $\omega_з$ которого отличается от частоты ω_s на $2\omega_{пр}$ и расположена симметрично (зеркально) относительно частоты $\omega_г$ гетеродина [3].

Преобразование сигнала по зеркальному каналу приема происходит по тому же алгоритму и с тем же коэффициентом преобразования, как и по основному каналу связи. Это обеспечивает избирательность и помехоустойчивость преобразователя частоты. Сложными для использования являются комбинационные каналы, которые формируются в результате взаимодействия первой гармоники частоты сигнала и гармониками частоты гетеродина малого порядка (второй, третьей), т.к. чувствительность преобразователя частоты по таким каналам близка к чувствительности основного канала [3].

Технической задачей решения, представленного в данной статье и подтвержденного патентом [2] является построение общей структуры построения комплекса управления СКУДПС за счет использования специальных контейнеров, оборудованных дуплексной радиостанцией, приемником навигационных ГЛОНАС-GPS сигналов, датчиками номера и технического состояния транспортного средства или динамического объекта, а также микропроцессором, к которому они подключены [1]. Важнейшей частью задачи является повышение помехоустойчивости и достоверности определения местоположения МСУДТС на базе дирижабля, диспетчерского центра управления и объектов, управляемых ими в режиме реального времени. Что позволит обеспечить повышение эффективности функционирования СКУДПС морской инфраструктуры в целом.

Структурная часть задачи решается, приборным составом СКУДПС морской инфраструктуры в целом и в частности МСУДТС на базе дирижабля, состоящего из корпуса с несколькими отсеками, заполненными несущим газом легче воздуха, гондолы с двигателями и топливными баками, кабины управления и салонов для экипажа, группы управления и отряда спасателей, ликвидаторов аварий. На дирижабле имеется рабочий технический отсек с приборами наблюдения и бортовой химической лабораторией, а также другие аппаратно-программные системы, обеспечивающие профессиональное функционирование МСУДТС [4].

Реализуемость этого проекта подтверждается широкой демонстрацией дирижаблей на международных авиационных и морских выставках, оснащение же их специальной аппаратурой управления не представляет технической сложности.

Предлагаемый дирижабль в составе МСУДТС обеспечивает повышение надежности и достоверности обмена дискретной информацией между дирижаблем, диспетчерским центром и управляемыми объектами. С точки зрения обнаружения сложные ФМн сигналы обладают высокой энергетической и структурной скрытностью. Это достигается за счет использования двух частот и сложных сигналов с фазовой манипуляцией. Указанные сигналы открывают новые возможности в технике передачи сообщений [4].

Энергетическая скрытность данных сигналов определяется их высокой сжимаемостью по спектру и во времени, что позволяет снизить мгновенную излучаемую мощность. Энергия сложного сигнала не мала, но распределена по частотно-временной области таким образом, что в каждой точке этой области мощность сигнала меньше мощности шумов и помех. Вследствие этого сложный Фмн сигнал в точке приема оказывается замаскированным шумами и помехами.

Скрытность структуры сложных сигналов с фазовой манипуляцией определяется разнообразием их форм, широким диапазоном вариаций параметров, что затрудняет повышение чувствительности приемника при обработке сложных, априорно неизвестной структуры сигналов.

Подавление ложных сигналов (помех), принимаемых по дополнительным каналам, происходит за счет преобразования принимаемых сложных ФМн сигналов на нулевую частоту. Указанное преобразование позволяет выделять модулирующие коды из принимаемых сложных ФМн сигналов, т.е. синхронное их детектирование. Совмещение двух указанных процедур обеспечивается гетеродинами, смесителями и фильтрами нижних частот, которые одновременно выполняют роль преобразователей частоты и синхронных демодуляторов принимаемых сложных ФМн сигналов. Такие схемные конструкции свободны от дополнительных каналов приема, а системы ФАПЧ обеспечивают автоматическое слежение за изменениями несущих частот принимаемых сложных ФМн сигналов [3].

Заключение. Предлагаемая структура СКУДПС обеспечивает повышение эффективности функционирования за счет помехоустойчивости и достоверности связи между СКУДПС и объектами управления. Это достигается системами акустоэлектронных меток на ПАВ, которые позволяют с высокой точностью идентифицировать все объекты управления морской инфраструктуры, включая динамические. Важным достоинством таких меток по сравнению с полупроводниковыми является высокая помехоустойчивость и стойкость к электромагнитным и радиационным воздействиям за счет подавления ложных сигналов (помех), принимаемых по дополнительным (зеркальному и комбинационным) каналам, устранением явления «обратной работы» и автоматического поддержания указанного равенства сигналов с помощью системы ФАПЧ.

Внедрение в структуру СКУДПС объектов группы МСУДТС на базе дирижабля позволяет существенно расширить площадь контроля и управления объектами морской инфраструктуры, включая динамические. Использование дирижаблей а качестве МСУДТС значительно расширяет функциональные возможности их применения, включая оперативную переброску спасателей на место аварии.

Подавление ложных сигналов (помех), принимаемых по дополнительным каналам, происходит за счет преобразования принимаемых ГЛОНАС-GPS сигналов на нулевую частоту, выделять модулирующий код и обеспечивать синхронное их детектирование. Такие схемные конструкции свободны от дополнительных каналов приема и явления «обратной работы», а системы ФАПЧ, обеспечивают автоматическое слежение за изменениями несущей частоты принимаемых ГЛОНАС-GPS сигналов, которые могут возникать под воздействием различных дестабилизирующих факторов, в том числе и эффекта Доплера.

СПИСОК ЛИТЕРАТУРЫ

1. Патент РФ № 2733054, Компьютерная система дистанционного контроля и управления объектами жизнеобеспечения городской инфраструктуры. Алексеев С.А., Дикарев В.И., Парфенов Н.П., Стахно Р.Е. Заявка № 2019135858 от 08.11.2019 г.
2. Патент РФ № 2725100, Экологический дирижабль. Алексеев С.А., Дикарев В.И., Парфенов Н.П., Стахно Р.Е. Заявка № 2019140886 от 11.12.2019г.
3. Дикарев В.И., Ефимов В.В., Калинин В.А., Мельников В.А. Радиочастотная идентификация в нашей жизни. / Изд. Трактат. СПб., 2018. – 246 с.
4. Алексеев С.А., Гончар А.А., Стахно Р.Е., Яковлева Н.А. Повышение эффективности функционирования системы управления движением судов морского порта. / Информационные технологии управления объектами морской техники и морской инфраструктуры. Сборник трудов Морской техники. Выпуск 1 / ИАП БЖКС, эл. изд. - СПб., 2020. - 105 с.

УДК 629.12

КВАЛИМЕТРИЧЕСКИЙ SWOT-АНАЛИЗ ПРОГРАММНЫХ КОМПЛЕКСОВ РОБОТИЗАЦИИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ИНЦИДЕНТАМИ

Алексеев Анатолий Владимирович, Куприянов Дмитрий Олегович, Заведеев Юрий Михайлович, Гадаев Егор Михайлович, Стефанович Игорь Денисович

Институт автоматизации процессов борьбы за живучесть корабля, судна
Ленинский пр., 101, Санкт-Петербург, 198262, Россия
e-mail: iapbgks@bk.ru

Аннотация. В развитие вопросов роботизации управления информационной безопасностью автоматизированных систем в защищенном исполнении (АСЗИ) как основного способа снижения негативного

влияния человеческого фактора операторов АСЗИ, сформирована квалиметрическая база данных и знаний (КБДЗ) программно-аппаратных комплексов (ПАК), декларирующих возможность автоматического управления информационными инцидентами. Выполненный по технологии QSWOT анализ показал, что данная задача является исключительно сложной и далеко нерешенной при ее особой востребованности в настоящее время. Приведены сравнительные свойства и количественные оценки конкурентного превосходства 14 вариантов ПАК роботизированного управления информационными инцидентами информационной безопасности (РУБ), среди которых конкурентно способным определен вариант интеграции SOC & СПРУ, рекомендуемый для судов, портового оборудования, систем навигационного обеспечения, АСЗИ управления портами и пароходствами.

Ключевые слова: роботизация управления инцидентами; квалиметрический анализ; синтез; оптимизация; технология сравнения свойств; конкурентное превосходство.

QUALIMETRIC SWOT ANALYSIS OF SOFTWARE SYSTEMS FOR ROBOTIZATION OF INFORMATION INCIDENT MANAGEMENT

Alekseyev Anatoly, Kupriyanov Dmitry, Zavadeev Yuri, Gadaev Egor, Stefanovich Igor
Institute of automation of processes of struggle for survivability of the ship, vessel
101 Leninsky Av, St. Petersburg 198262, Russia
e-mail: iapbgks@bk.ru

Abstract. In the development of issues of robotization of information security management of automated systems in protected execution (ASSI) as the main way to reduce the negative impact of the human factor of ASPI operators, a qualimetric database and knowledge (KBDZ) of software and hardware complexes (PAK) declaring the possibility of automatic management of information incidents has been formed. The analysis performed using SWOT technology showed that this task is extremely complex and far from unsolved, given its special demand at the present time. Comparative properties and quantitative estimates of the competitive advantage of 14 variants of the automated control system for information security Information incidents (RUB) are presented, among which the SOC & SPRU integration option recommended for ships, port equipment, navigation support systems, ASSI management of ports and shipping companies is determined to be competitive.

Keywords: robotization of incident management; qualimetric analysis; synthesis; optimization; property comparison technology; competitive advantage.

В развитие вопросов роботизации управления информационной безопасностью АСЗИ [1-4] как основного способа снижения негативного влияния человеческого фактора операторов АСЗИ, в результате исследований [3] была впервые сформирована и опубликована КБДЗ ПАК РУБ, декларирующих возможность автоматического управления инцидентами информационной безопасности (ИБ).

Актуализация КБДЗ на настоящий момент позволила перейти к ее анализу по технологии QSWOT, который подтвердил, что задача РУБ, в решение которой участвуют более десятка вендеров, является исключительно сложной и далеко нерешенной в настоящее время при ее особой востребованности и актуальности для обоснования облика, структуры и характеристик ПАК роботизированного управления ИБ.

В этой связи представляется ***актуальным*** обобщить полученные данные и сформулировать результаты сравнительного количественного анализа с определением наиболее предпочтительных ПАК обеспечения информационной безопасности (ОИБ) при решении задач анализа (задача IDS) и предотвращения (задача IPS) информационных вторжений в типовых условиях функционирования АСЗИ. В том числе ПАК РУБ для использования на судах, АСЗИ портов и пароходств, систем навигационного обеспечения, АСЗИ береговых центров экстренного реагирования и других объектов морской техники и морской инфраструктуры (ОМТИ).

На рис. 1 приведен фрагмент КБДЗ с данными по 7 лидирующим из 14 рассмотренных альтернативных вариантах ПАК РУБ АСЗИ, анализ которых позволил сделать следующие выводы:

В сравнении с первоначальным вариантом КБДЗ [3] по состоянию на февраль 2021 г., в котором конкурентно способными вариантами были ПК по вариантам 45 (при обобщенной оценке качества Q=9,4), 41 (Q=8,6), введенные в рассмотрение и практическое тестирование варианта 52 (DLP), а также рассмотрение варианта 51 (DLP & СПРУ) его интеграции с вариантом 17 (СПРУ), позволило, с одной стороны, уточнить свойства и количественные оценки по критериям S, W, O, T и Q, а, с другой стороны, выйти, по нашему мнению, на более корректные сравнительные оценки ПАК РУБ по качеству ОИБ с Q=8,46 (вариант 46).

Из рассмотренных декларируемых вариантов ПАК РУБ, по нашему мнению, задачу в полном объеме и с требуемым качеством в реальном масштабе времени (РМВ) без интеграции с СПРУ не решает.

Именно интеграция с ПАК типа СПРУ позволяет в РМВ за счет квалиметрической оценки системных свойств и характеристик процессов РУБ, их безизбыточной визуализации с цветовым кодированием, а также системного мониторинга и контроля позволяет практически автоматически реагировать на инциденты.

Квалиметрический SWOT-анализ альтернативных вариантов решения комплекса задач СУИБ

i		ИКЗ свойств:	0,4		0,25		0,2		0,15	0,5	
Шифр средства, сертификат	Назначение средства, сертификация. Включённые в КРОПУР варианты выделены зелёным фоном	S.Сильные (внутренние) стороны	S	W.Слабые (внутренние) стороны	W	O.Возможности развития с учетом внешних факторов	O	T.Угрозы развития с учетом внешних факторов	T	Q	Rq
17. МДО ПК "СПРУ-ИБ" (ИП, 2018, СПбГМТУ)	Мониторинг системных показателей качества обеспечения ИБ. Интеллектуальная поддержки принятия (ИПП) проектных и управленческих решений (ПУР). Идентификация образов инцидентов, атак, вторжений (ИОВ).	Оценка и эффективная визуализация системных показателей качества ОИБ АСЗИ. Ранжированное представление вариантов ПУР.	7,5	Необходимость заимствования данных со сканеров ИБ. Отсутствие промышленного (по результатам ОКР) образца, серии. Зависимость от качественных источников данных.	1,5	Роботизированное решение задач управления инцидентами при интеграции со сканерами ИБ. Инвариантность технологии. Имеется отработанный МДО, обеспечивающий доступность серийной	8,7	Отсутствие в настоящее время инвестиций в создание промышленного образца, варианта интеграции. Зависимость от вендеров сканеров ИБ.	1,5	8,12	4
40. Security Vizion SGRC 3.4	Система управления информационной безопасностью ПМУБ СКЗИ АСЗИ. Декларация возможностей (превышающих вариант 52).	Один из первых промышленных ПК автоматизации ИБ с формируемой БДЗ. Оценивается риск ИБ.	8,3	Ограниченные возможности визуализации данных при мониторинге обстановки. Нет оценки системных показателей ИБ.	2,6	Необходимость наращивания возможностей автоматического решения задач.	8,0	Технологическая избыточность (сложность) гетерогенного пути развития	2,0	7,96	9
41. Security Operations Center (SOC)	Система управления информационной безопасностью ПМУБ СКЗИ АСЗИ для Центра управления ИБ.	Автоматическая обработка контента с автоматической блокировкой инцидентов по 5 уровням их критичности и 16 типам.	8,5	Ограниченные возможности по автоматической блокировке контента, минимизации потока ложных срабатываний.	3,0	Необходимость наращивания возможностей автоматического решения задач.	8,5	Технологическая избыточность (сложность) гетерогенного пути развития	2,0	8,02	5
45.SGRC & СПРУ	Интегрированная роботизирования система управления информационной безопасностью ПМУБ СКЗИ АСЗИ, обеспечивающая автоматическое управление ИБ.	Максимально автоматизированный (роботизированный) режим обработки контента с автоматическим блокированием инцидентов по 5 уровням критичности и 16 типам инцидентов.	9,0	Опасность потери конкурентного превосходства разработанного технологического решения.	2,4	Необходимость практической отработки вариантов автоматического решения задач, оптимизации системного решения, минимизации структурно-функциональной избыточности.	8,5	Необходимость поддержания конкурентного превосходства в условиях рынка.	2,0	8,38	2
46.SOC & СПРУ	Интеграция вариантов 41 и 17 с целью наращивания возможностей за счет системной квалиметрии (оценки), мониторинга обстановки, контроля и управления обстановкой.	Практическая работизация процессов управления инцидентами.	9,0	Необходимость формирования КБДЗ с учетом специфики объекта информатизации.	2,5	Возможность масштабирования технологии в широкий круг задач с соответствующим ускоренным их развитием, отработкой.	8,9	Необходимость особого контроля доступности и целостности КБДЗ с целью предотвращения инцидентов рефлексивного управления.	1,8	8,46	1
51. DeviceLock DLP 9 & СПРУ	Интеграция вариантов 52 (32) и 17 с целью наращивания возможностей: системной квалиметрии (оценки), мониторга обстановки, контроля и управления обстановкой.	Контроль доступа к устройства и интерфейсам, контроль сетевых коммуникаций, контентная фильтрация, удобный интерфейс (СПРУ)	8,6	Отсутствие реагирования на инциденты ИБ и отсутствие управления рисками. Невозможность раскрытия полного функционала СПРУ (СППР)	2,0	Необходимость наращивания возможностей автоматического решения задач.	8,5	Технологическая избыточность (сложность) гетерогенного пути развития	2,0	8,34	3
52. DeviceLock DLP 9	Набор инструментов для администрирования: разграничения доступа, определения разрешённых устройств и сервисов, контроль поведения пользователей. Подробнее см. вариант 32.	Отработанная технология с 2015 г., опыт использования и продаж. Наличие сертификата AM Test Lab № 150, 23.07.2015.	8,3	Интерфейс (работа с деревом консоли) сильно устарели, нуждаются в доработке. Основной упор сделан на организацию процесса работы пользователей и автоматизацию процесса администрирования. Все встроенные процедуры	2,5	Стабильное развитие и совершенствование ПК. Декларация полной интеграции.	8,0	Иностранный вендер, возможность санкций. Необходима высокая квалификация (системы, сервер, БД). Под ОС Windows требует установки MS SQL Server.	2,0	7,99	7

Рис.1. Фрагмент КБДЗ программных комплексов роботизированного управления информационными инцидентами.

Конкурентные варианты 46, 45, 51 близки по уровню качества РУБ, что указывает на целесообразность организационного объединения усилий вендеров DLP, SGRC, SOC, СПРУ и соответствующую возможность форсированной разработки перспективной технологии создания ПАК РУБ.

Приведенные с использованием технологии QSWOT - экспресс-анализа (по 4 критериям) сравнительные свойства и количественные оценки конкурентного превосходства 14 альтернативных вариантов ПАК роботизированного управления информационными инцидентами подлежат дополнительной проверке и возможному уточнению в соответствии с концепцией полимодельного подхода путем сопоставления с результатами многокритериального анализа качества, например, по технологии АСОР, АСПИД, МАИ [3 - 8].

Дальнейшая актуализация КБДЗ представляется нам уже более доступной, так как сравнение новых вариантов ПАК будет удобно оценивать и анализировать в сопоставлении с выявленными лидерами рынка, что одновременно позволит повысить точность оценивания, корректировать ранее введенные данные.

Перспективными направлениями дальнейших исследований по обоснованию, разработке технологии и созданию программно-аппаратных средств роботизированного управления инцидентами информационной безопасности, по нашему мнению, следует считать интеграцию усилий разработчиков по согласованию позиций в части выбора системы критериев и формированию требований к ПАК РУБ, учету широкого спектра вариантов реагирования на информационные вторжения, системы критериальных предпочтений.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А.В., Воробьев В.И. Информационное противоборство: 20 лет концептуального и технологического развития // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 1 / СПОИСУ. – СПб., 2015, с. 153 – 159.
2. Алексеев А.В., Балицкая К.В. Роботизация управления как способ снижения негативного влияния человеческого фактора на информационную безопасность АСЗИ / Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 7 / СПОИСУ. – СПб., 2019, с. 237-242.
3. Алексеев А.В., Куприянов Д.О., Заведеев Ю. М., Стефанович И.Д. Анализ интеллектуальных технологий управления ИБ морских интегрированных автоматизированных систем // Актуальные проблемы морской энергетики: материалы десятой международной научно-технической конференции в рамках Пятого Всероссийского научно-технического форума «Корабельная энергетика: из прошлого в будущее». – СПб.: Изд-во СПбГМТУ, 2021, с. 363 – 369.
4. Куприянов Д.О., Стефанович И.Д., Заведеев Ю.М., Алексеев А.В. Развитие технологии IDS и комплексная безопасность мореплавания // Межвузовская научно-практическая конференция студентов, аспирантов и молодых ученых «Развитие инфраструктуры внутреннего водного транспорта: традиции, инновации» (РИВВТ-2020) – ГУМРФ, 2020.12.4.
5. Заведеев Ю.М., Куприянов Д.О., Алексеев А.В. Анализ технологий интеграции программных комплексов CRS и СПРУ в интересах роботизации управления информационной безопасностью // Актуальные проблемы морской энергетики: материалы десятой международной научно-технической конференции в рамках Пятого Всероссийского научно-технического форума «Корабельная энергетика: из прошлого в будущее». – СПб.: Изд-во СПбГМТУ, 2021.
6. 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). XII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2021 г.: Материалы конференции / СПОИСУ. – СПб., 2021.
7. D.O. Kupriyanov, I.D. Stefanowitsch, Ju.M. Zavedeev, Je.M. Gadaev, A.V. Alekseev. Analyse der intelligenten Technologie der Datensicherhetssteuerung «A-SGRC + SPRU» / Д.О. Куприянов, И.Д. Стефанович, Ю.М. Заведеев, Е.М. Гадаев, А.В. Алексеев/ Анализ интеллектуальной технологии управления ИБ «a-SGRC + СПРУ» // 2-я региональная научно-практическая конференция «Диалог поколений», Санкт-Петербург, 23 апреля 2021 г., СПБГУПТД - ВШТЭ.
8. Алексеев А.В., Москаленко В.А., Куприянов Д.О., Заведеев Ю. М., Стефанович И.Д., Гадаев Е.М. Программный комплекс поддержки принятия решений по оценке технической готовности корабля к выходу в море / Перспективные направления развития отечественных информационных технологий: материалы VII межрегиональной научно-практической конф. Севастополь, 21-25 сентября 2021 г. / Севастопольский государственный университет; науч. ред. Б.В. Соколов. – Севастополь: СевГУ, 2021.

УДК 629.12, 681.518

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ПРЕВОСХОДСТВА В ИНФОРМАЦИОННОЙ СФЕРЕ И ПУТИ ИХ РЕШЕНИЯ

Алексеев Анатолий Владимирович[1], Михальчук Андрей Васильевич[2], Давыдчик Виталий Владимирович[3]

[1] Институт автоматизации процессов борьбы за живучесть корабля, судна
Ленинский пр., 101, Санкт-Петербург, 198262, Россия
[2] Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
[3] ПАО «Информационные телекоммуникационные технологии «Интелтех»
Кантемировская ул., 8, Санкт-Петербург, 197342, Россия
e-mails: iapbgks@bk.ru, mikhalchuk@oogis.ru, zavit@bk.ru

Аннотация. На основе системного анализа тенденций развития вопросов информационного противоборства, включая по традиции, в первую очередь, обеспечения информационной безопасности (ИБ) автоматизированных систем в защищенном исполнении (АСЗИ) различного назначения, включая объекты критической информационной инфраструктуры (ОКИИ), анализ ТОР-21 примеров информационного превосходства, обоснованы приоритетные проблемы обеспечения превосходства в информационной сфере и перспективные пути их решения. В том числе на основе технологических путей реализации концепции и технологий роботизированного управления, системной визуализации и мониторинга, имитостойкости каналов управления и информационным противоборством в целом.

Ключевые слова: системный анализ; превосходство в информационной сфере; синтетическая квалиметрия; информационная живучесть; роботизированное управление; имитостойкость управления; исследовательское проектирование.

CURRENT PROBLEMS OF PROVIDING EXCELLENCE IN THE INFORMATION SPHERE AND WAYS OF THEIR SOLUTION

Mikhalchuk Andrey[1], Davydchik Vitaly[2], Alekseev Anatoly[3]

[1] Institute of automation of processes of struggle for survivability of the ship, vessel
101 Leninsky Av, St. Petersburg 198262, Russia
[2] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
[3] JSC «INTELTECH»
8 Kantemirovskay St, St. Petersburg, 197342, Russia
e-mails: iapbgks@bk.ru, mikhalchuk@oogis.ru, zavit@bk.ru

Abstract. Based on a systematic analysis of trends in the development of issues of information warfare, including, according to tradition, first of all, ensuring information security (IS) of automated systems in protected execution (ASSI) for various purposes, including objects of critical information infrastructure (OKII), the analysis of TOP-21 examples of information superiority, the priority problems of ensuring superiority in the information sphere and promising ways to solve them are substantiated. Including on the basis of technological ways to implement the concept and technologies of robotic control, system visualization and monitoring, the stability of control channels and information warfare in general.

Keywords: system analysis; excellence in the information sphere; synthetic qualimetry; information survivability; robotic control; control stability; research design.

Актуальность. Проблема обеспечения превосходства в информационной сфере (ПОПИС), включая обнаружение, выявление информационных угроз, прогнозирование и нейтрализацию их воздействия на личность, общество, государство, социум, различные корпоративные и государственные структуры с особой остротой встала в 90-х годах XX-го века ввиду интенсивного развития информационных технологий и бурной информатизации общества. Первоначально «обозначенная» в Директиве НАТО концепция «информационной войны» получила бурное развитие, а сегодня в обществе уже открыто признаётся существование и непрерывность ведения не только информационных вторжений, атак, сетецентрических и кибервойн, но и ментальных войн как высшей формы на сегодняшний день информационного противоборства.

Наибольший размах «информационные атаки», «компьютерные атаки», «операции», «сражения» получили при комплексном использовании традиционных и нетрадиционных видов оружия в Гренадском конфликте, войне в Ираке («Буря в пустыне»), войне в Чечне, а также в целом ряде других конфликтов и вооружённых столкновений. Сегодня трудно представить себе область деятельности организаций, компаний, корпораций, государства, где бы не применялись средства ведения информационной разведки, информационных вторжений в различных формах и информационного противоборства в целом [1-7].

Более того, в интересах защиты информационных ресурсов (ИР) ключевых объектов информационной инфраструктуры России в настоящее время создана и активно развивается Государственная система «СОПКА», предназначенная для обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Её создание можно рассматривать как национальное средство подготовки и обеспечения информационного превосходства, ответа на вызов времени – широкомасштабное противоборство в информационной сфере. На рис. 1 в систематизированном и ранжированном виде (TOP-21) приведены наиболее значимые по состоянию на настоящее время компьютерные атаки, инциденты и факты информационного противоборства, каждый из которых ярко демонстрирует особую значимость необходимости концентрации национальных ресурсов (интеллектуальных, научных, технологических, организационных и многих других) на решение этой архиважной сегодня комплексной проблемы.

Рис. 1. TOP-21 событий и фактов противоборства в информационной сфере.

Среди вопросов развития АСЗИ различного назначения, включая объекты морской техники и морской инфраструктуры (ОМТИ) и, особенно, ОКИИ, сегодня традиционно первостепенное значение имеют вопросы обеспечения их информационной безопасности (ИБ) в сравнении с вопросами информационного противодействия (ИПД). Именно ИБ в сочетании с мерами ИПД в условиях широкомасштабного внедрения информационных технологий и тренда цифровизации национальной экономики в целом имеют наибольшее влияние на технологическое, организационное и методологическое развитие и эффективное освоение АСЗИ [7].

Системный анализ данных вопросов на основе положений теории синтетической квалиметрии [6], включая оценку и анализ факторов корневой чувствительности интегрированных показателей качества АСЗИ с использованием аппарата типа QSWOT-анализа и синтеза, позволяют выявить следующие наиболее актуальные и наиболее значимые (критичные) проблемы обеспечения превосходства в информационной сфере:

1. Методологическая проблема обеспечения качества управления ИБ и ИПД (ИП в целом), обусловленная разрывом между масштабом требований к АСЗИ, технологической сложностью их реализации и возможностью эффективного управления ИП на объектах информатизации типа ОМТИ и, особенно, ОКИИ в реальном масштабе времени. Для решения данной проблемы должно быть предусмотрено, по нашему мнению, внеочередное научно-методологическое решение задач концептуального и технологического развития.

2. Формирование центров компетенции, центров освоения технологий ИП и управления технологическим развитием ОКИИ на основе согласованных программ и планов взаимодействия, включая некоммерческие партнерства, сообщества и объединения, а также ранжирования ожидаемой результативности и сертификации качества соответствующих технологических решений с использованием активно развивающейся сегодня технологии квалиметрии моделей и полимодельных комплексов.

3. Создание межнациональных центров обмена информацией по ИП на основе открытых протоколов взаимодействия и предоставления каналов выявления угроз информационной безопасности, создания региональных, национальных полигонов открытого тестирования демонстрационного программного обеспечения для практической отработки конкурентноспособных технологических решений.

4. Организационно-техническая проблема управления структурной, процессной и алгоритмической адаптацией АСЗИ к постоянно изменяющейся инфраструктуре объектов информатизации путем внеочередного решения задачи создания роботизированных комплексов управления АСЗИ.

5. Программно-аппаратная и методическая проблема критической потребности в системном мониторинге обстановки в информационной сфере в реальном масштабе времени, включая информационное противоборство (ИП), как технологической платформе эффективного управления ИП на основе создания национальных средств и систем поддержки принятия решений и управления ИП (СПРУ-ИП), форсированного развития средств роботизированного управления ИБ в классе IPS типа SIEM, PDM, SOAR, CRS, SGRC с выделением, полагаем, Министерством цифрового развития соответствующих инвестиций на внедрение лучших образцов по результатам сравнительных сертификационных испытаний.

6. Ситуационная проблема потери контроля качества обеспечения ИБ в условиях масштабного перехода к технологиям удаленного доступа к критически значимым информационным ресурсам граждан, предприятий, организаций и компаний, определенной технологической их неготовности по обеспечению ИБ в этих условиях. Приоритетное решение данной проблемы на основе совершенствования нормативно-правового регулирования вопросов охраны ИР личности, общества, государства в обеспечение их прогрессивного развития в соответствующим принятыми в РФ нормативно-правовыми документами.

7. Медленно разрешаемые «традиционные» проблемы обеспечения импортозамещаемости, конкурентной способности отечественных технологий, ограниченной результативности сертификации продукции и услуг в области ИБ, аттестации объектов и лицензирования деятельности. В том числе путем административно-правового регулирования, совершенствования и обеспечения нормативных регламентов.

8. Традиционные проблемы планирования бюджета на ИБ и, особенно, комплексное научно-технологическое решение задач ИП, его ресурсной отдачи (результативности, экономичности). В первую очередь, за счет обеспечения соответствующей информационной прозрачности управления ресурсами, а также объявления грантов на создание унифицированных комплексов ИП, инвариантных к специфике решаемых типовых задач обработки информации в защищенном исполнении, в том числе для формирования базы данных и знаний администраторов ИП в интересах отработки лучших практик ситуационного управления ИП.

9. Проблема повышения квалификации специалистов не только в части ИБ в целом, но, в первую очередь, эффективного управления ИБ и ИПД (ИП в целом), их переподготовки и сдерживания ротации на основе систематизации и целевого освоения лучших практик, качественной отработки научно-методических регламентов и их актуализации, лицензирования соответствующих видов деятельности.

10. Традиционная проблема эффективного планирования и обеспечения гарантированной реализации программ и планов (дорожных карт и т.п.) на основе современных средств автоматизации с мониторингом в реальном масштабе времени результативности их реализации, с безбумажным документооборотом и информационной прозрачностью системных результатов.

Решение сформулированных проблем и их решение, в том числе на основе названных технологических путей, позволят, по нашему мнению, путем их публичного обсуждения и развития сконцентрировать усилия разработчиков и специалистов по практическому решению наиболее значимых из актуальных проблем обеспечения превосходства в информационной сфере, эффективного обеспечения информационной безопасности в сочетании с мерами информационного противодействия соответствующим угрозам и вторжениям в рамках превосходства в управлении информационным противоборством.

СПИСОК ЛИТЕРАТУРЫ

1. Волков В.И., Тычинин И.Ю., Алексеев А.В. Анализ системных аспектов управления развитием критических объектов морской техники и морской инфраструктуры // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 1 / СПОИСУ. – СПб., 2015, с. 520 – 526.
2. Алексеев А.В. Информационная война: актуальность, возможности, концепции / В/ч 10729: 1318, 1995. – 17 с.
3. Алексеев А.В., Воробьев В.И. Информационное противоборство: 20 лет концептуального и технологического развития // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 1 / СПОИСУ. – СПб., 2015, с. 153 - 159.
4. Алексеев А.В., Воробьев В.И. 20 лет концептуального и технологического развития проблем информационного противоборства / Региональная информатика (РИ-2016). Юбилейная XV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2016)». Санкт-Петербург, 26-28 октября 2016 г.: Материалы конференции. \ СПОИ-СУ. - СПб, 2016, с. 421-422.
5. Юсупов Р.М., Жигадло В.Э. Особенности реализации функций информационной безопасности в условиях информационного противоборства

и ментальных войн / Перспективные направления развития отечественных информационных технологий: материалы VII межрегиональной научно-практической конф. Севастополь, 21-25 сентября 2021 г. / Севастопольский государственный университет; науч.ред. Б.В.Соколов. – Севастополь: СевГУ, 2021, с. 10-11.

6. Алексеев А.В., Михальчук А.В. Перспективные направления развития технологии полимодельного квалиметрического анализа, синтеза и оптимизации организационных и технических решений / Перспективные направления развития отечественных информационных технологий: материалы VII межрегиональной научно-практической конф. Севастополь, 21-25 сентября 2021 г. / Севастопольский государственный университет; науч.ред. Б.В.Соколов. – Севастополь: СевГУ, 2021, с. 40-41.
7. Михальчук А.В., Давыдчик В.В., Алексеев А.В. Семь актуальных проблем обеспечения ИБ, пути и дорожная карта их решения / Информационная безопасность регионов России (ИБРР-2021). XII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2021 г.: Материалы конференции / СПОИСУ. – СПб., 2021.

УДК 629.12.001.2

ОСОБЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ СТЕНДОВОЙ ДИАГНОСТИКИ ГАЗОТУРБИННЫХ ДВИГАТЕЛЕЙ

Баркова Наталия Александровна[1], Грищенко Дмитрий Вячеславович[2], Селищев Кирилл Павлович[1]

[1] Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, 190121, Санкт-Петербург, Россия
[2]Ассоциация ВАСТ
Стачек пр., 140, Санкт-Петербург, 198207, Россия
e-mails: barkova@vast.su, gdv@vast.su, skp98@yandex.ru

Аннотация. Рассматривается вопрос создания информационной системы диагностики газотурбинных двигателей на низких частотах вращения в стендовых условиях при холодной прокрутке. Показаны преимущества низкоскоростной диагностики за счет снижения вибрационных помех, вызываемых потоками воздуха и газа при работающей камере сгорания. Практическая диагностика группы двигателей ВК-2500 на стенде завода изготовителя подтвердила возможность вибрационной диагностики их механической системы, а также дополнительные возможности диагностики, которые дает анализ тока приводных электродвигателей.

Ключевые слова: газотурбинный двигатель; вибрация; безопасность; информационная система; диагностика; холодная прокрутка.

FEATURES OF THE INFORMATION SYSTEM FOR BENCH DIAGNOSTICS OF GAS TURBINE ENGINES

Barkova Natalia[1], Grishchenko Dmitriy[2], Selishev Kirill[1]

[1] St. Petersburg State Marine Technical University
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia
[2]Association VAST
140 Stachek Av, St. Petersburg, 198207, Russia
e-mails: barkova@vast.su, gdv@vast.su, skp98@yandex.ru

Abstract. The issue of creating an information system for gas turbine engines diagnostics at low rotational speeds in bench conditions with cold scrolling is considered. The advantages of low-speed diagnostics are shown by reducing vibration interference caused by air and gas flows when the combustion chamber is running. The practical diagnostics of the VK-2500 engines group at the manufacturer's stand confirmed the possibility of their mechanical system vibration diagnostics, as well as additional diagnostic capabilities provided by the analysis of the drive electric motors current.

Keywords: gas turbine engine; vibration; safety; information system; diagnostics; cold scrolling.

Безопасность эксплуатации и живучесть судна во многом определяется состоянием его движительной установки, оценку которого призваны давать бортовые системы мониторинга и диагностики. Большинство из бортовых систем ориентированы на обнаружение опасных дефектов установки незадолго до отказа, поэтому часто времени на их устранение без нарушения условий эксплуатации судна не хватает.

Естественный путь совершенствования бортовой системы – обеспечение периодического диагностирования с повышением глубины диагноза, обнаружением зарождающихся дефектов и отслеживанием их развития, позволяющая оценивать интервал безопасной эксплуатации до следующего диагноза. В этом случае систему диагностики лучше всего делить на две части – бортовую, задача которой – обнаружить опасную ситуацию, а также собрать и передать на берег необходимые данные для глубокой диагностики, и береговую, решающую задачи ранней диагностики и прогноза безопасного функционирования, а также планирования работ по обслуживанию и ремонту после возвращения судна в порт.

Существует, однако, энергетические установки, не вписывающиеся в такую концепцию диагностирования, так как объема данных, получаемых бортовой системой в номинальных режимах работы, не хватает для глубокой диагностики и на борту, и в береговых диагностических центрах. К ним в первую очередь относятся установки с высокооборотными газотурбинными двигателями. Основным процессом, по которому производится их глубокая

диагностика, является вибрация. Но в номинальном режиме работы шумы потока в газотурбинном двигателе велики и создают такие вибрационные помехи при диагностировании механических узлов двигателя, которые не позволяют проводить глубокую диагностику энергетической установки, особенно подшипников компрессора и силовой турбины.

Предлагается расширить возможности диагностики высокооборотных движительных установок на основе газотурбинных двигателей, проводя дополнительное диагностирование двигателя в режиме его прокрутки от внешнего привода на низких скоростях вращениях, не запуская камеру сгорания, как это делается в авиастроении при обслуживании авиационных двигателей между полетами. В режиме «холодной» прокрутки на скоростях вращения в 10 раз ниже номинальных уровни шумов двигателя падают более, чем в 30 раз, позволяя диагностировать механическую систему двигателя – валы компрессора и силовой турбины с подшипниками, а также навесные коробки передач, систему смазки, электрогенератор и пусковую турбину с использованием традиционных методов вибрационной диагностики роторных машин.

Все необходимые исследования по созданию стендовой системы диагностики проведены в рамках создания технологического стенда холодной прокрутки авиационных газотурбинных двигателей ВК-2500, используемых в составе многих типов вертолетов, после их изготовления или ремонта. В качестве привода, используемого для вращения как турбокомпрессора, так и свободной турбины двигателя, при разработке стенда использовался 4-полюсный синхронный электродвигатель с ротором из постоянных магнитов, подключаемый к статическому преобразователю частоты питающего напряжения. На время холодной прокрутки электродвигатель крепится непосредственно на корпус газотурбинной установки взамен одного из навесных агрегатов, в частности электрогенератора, пусковой турбины или других, передавая крутящий момент через шлицевое соединение.

Так, на рис.1. приведен стенд холодной прокрутки с газотурбинным двигателем, закрепленным на передвижной технологической раме. С двух сторон на него установлены синхронные электродвигатели, один из которых вращает турбокомпрессор, а второй – свободную турбину.

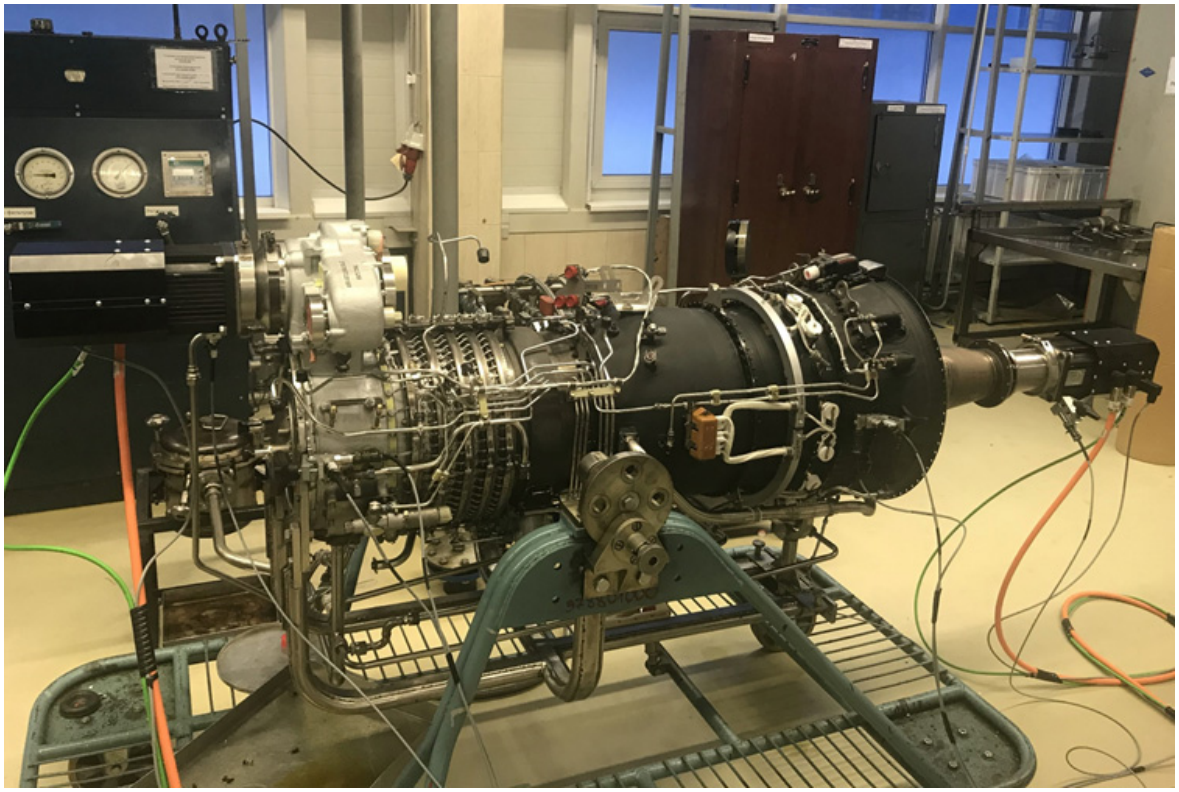


Рис.1. Технологический стенд холодной прокрутки газотурбинного двигателя ВК-2500.

Для выполнения работ по диагностированию ВК-2500 обеспечивается два последовательных этапа прокрутки турбокомпрессора с заторможенной свободной турбиной и свободной турбины с заторможенным турбокомпрессором. Частота вращения при прокрутке валов и компрессора, и свободной турбины в стендовых условиях выбирается близкой к 30Гц, для чего используются синхронные электродвигатели мощностью 3кВт и массой 17кг. При прокрутке газотурбинного двигателя в полевых условиях может использоваться и менее мощный электропривод, однако при этом частоту вращения валов при диагностировании двигателя потребуется снизить в 2–3 раза.

Низкоскоростная диагностика газотурбинного двигателя проводится по вибрации в 4 стандартных точках его крепления к промежуточной раме, а также в дополнительных точках корпуса в плоскостях, соединяющих компрессор, свободную турбину и навесное оборудование. Всего на газотурбинный двигатель с помощью специальных узлов крепления устанавливается до 12 датчиков вибрации и, кроме синхронного измерения вибрации во всех точках контроля также синхронно измеряется и силовой ток в электродвигателях, вращающих компрессор и свободную турбину.

В качестве средства измерения вибрации и тока используется 16-канальная мобильная система мониторинга и диагностики СМД-4 производства Ассоциации ВАСТ приведенная на рис.2, поскольку в ней предусмотрены режимы как онлайн анализа сигналов, так и предварительной синхронной записи сигналов с их последующим офлайн анализом. Измерения проводятся при установившейся частоте вращения турбокомпрессора или свободной турбины. Синхронная запись сигналов вибрации, тока и частоты вращения в память системы производится в течение 15–30 секунд в частотном диапазоне от 2Гц до 50кГц.

Рис.2. Мобильная система мониторинга и диагностики СМД-4, используемая в режиме предварительной записи сигналов вибрации, тока и частоты вращения с их последующим анализом.

Мобильная система СМД-4 с предварительной записью сигналов может использоваться для вибрационной диагностики механической части газотурбинного двигателя в полевых условиях на пониженных скоростях вращения при прокрутке от пусковой газовой турбины, однако при этом не все оптимальные точки контроля ее вибрации оказываются доступными для проведения измерений, количество одновременно вращающихся узлов растет, а стабильность их вращения – падает. Все это существенно усложняет автоматизацию процессов диагностирования.

Анализ возможностей и особенностей стендовой системы диагностики ВК-2500 при прокрутке от электропривода был выполнен на примере оценки состояния группы из семи новых двигателей. Для оценки состояния используются результаты:

– узкополосного спектрального анализа тока электродвигателя в диапазоне частот до 25 кГц;

– узкополосного спектрального анализа вибрации в диапазоне частот до 25кГц с построением дополнительных широкополосных спектров выделяемых случайных составляющих вибрации;

– анализа импульсной вибрации, возбуждаемой ударными взаимодействиями механических узлов на средних и высоких частотах.

Так, спектральный анализ тока приводного электродвигателя дает возможность обнаруживать дефекты, приводящие к действию на его вал пульсирующих моментов. Если это периодические моменты, они обнаруживаются по модуляции силового тока, если непериодические – по нестабильности его величины. Так, на рис 3 приведены спектр тока привода свободной турбины и зависимость амплитуды основной составляющей тока с частотой 90Гц от времени при наличии нарушений в подаче смазки в подшипники одного из диагностируемых двигателей.

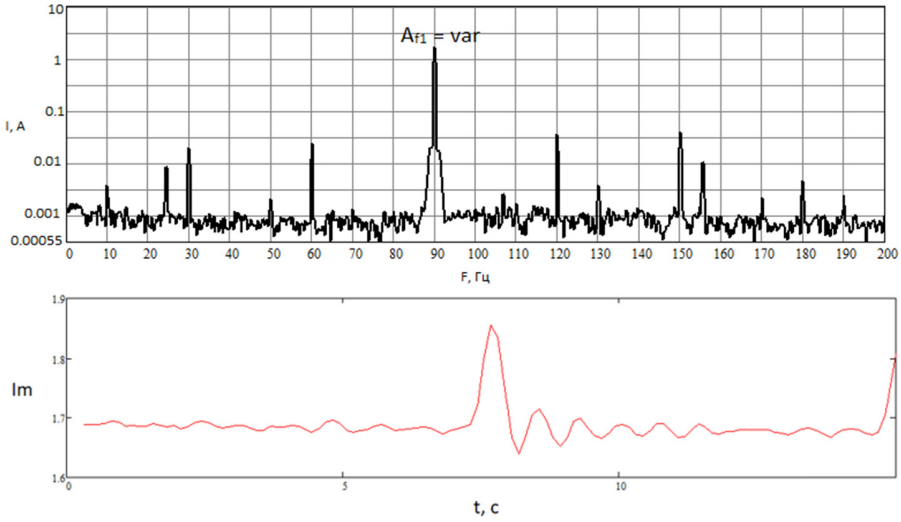


Рис. 3. Низкочастотная часть спектра тока электропривода и зависимость величины его основной составляющей во времени при нарушениях в подаче смазки в газотурбинный двигатель.

В спектре тока электродвигателя проявился признак еще одного дефекта – несоосности валов электрической машины и свободной турбины, причиной которого является незначительный дефект собственно стенда холодной прокрутки - конечная точность изготовления промежуточного вала, используемого для передачи крутящего момента от электродвигателя на вал свободной турбины. Признак заключается в появлении модуляции основного тока гармониками частоты вращения указанных валов. Кроме указанных дефектов к модуляции тока привода приводят и дефекты шестерен и зацеплений нагруженных зубчатых передач, номенклатура которых во вспомогательных механизмах газотурбинного двигателя весьма велика.

Узкополосный спектральный анализ вибрации в стандартных точках ее контроля необходим, прежде всего, для обнаружения развитых дефектов подшипников качения валов турбокомпрессора и свободной турбины, низкочастотные составляющие вибрации которых проявляется как в ближних, так и в удаленных точках контроля. Кроме этого, доступными для обнаружения по спектру вибрации оказываются развитые дефекты шестерен и зубчатых зацеплений наиболее нагруженных вспомогательных механизмов, признаками которых является многократный рост вибрации на частотах, кратных частоте вращения дефектной шестерни и на зубцовой частоте, однако более точную диагностику вспомогательных механизмов лучше выполнять по узкополосным спектрам вибрации, измеряемой в дополнительных точках контроля, максимально приближенных к точкам крепления каждого из вспомогательных механизмов к корпусу газотурбинного двигателя.

Так, на рис. 4 приведен спектр низкочастотной вибрации корпуса одного из обследуемых ВК-2500 в плоскости соединения корпусов турбокомпрессора и свободной турбины с признаками дефекта радиально-упорного подшипника компрессора.

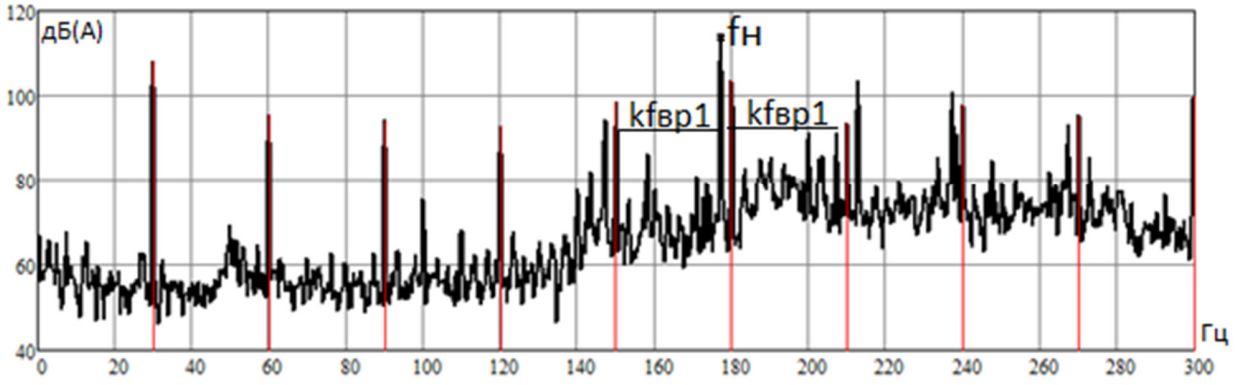


Рис.4. Низкочастотная часть спектра вибрации корпуса газотурбинного двигателя с признаками дефекта (наклепа) наружного кольца радиально-упорного подшипника компрессора.

Узкополосный спектр среднечастотной вибрации турбокомпрессора одного из обследуемых ВК-2500 на корпусе в зоне крепления маслоагрегата к центральному приводу к турбокомпрессору приведен на рис. 5.

Крутящий момент от электродвигателя к валу компрессора передается через два нагруженных зубчатых зацепления – промежуточного вала с вертикальным и вертикального с валом центрального привода. Повышенная по сравнению с другими ВК-2500 вибрация на зубцовых гармониках указывает на наличие дефектов зацепления (перекоса вертикального вала).

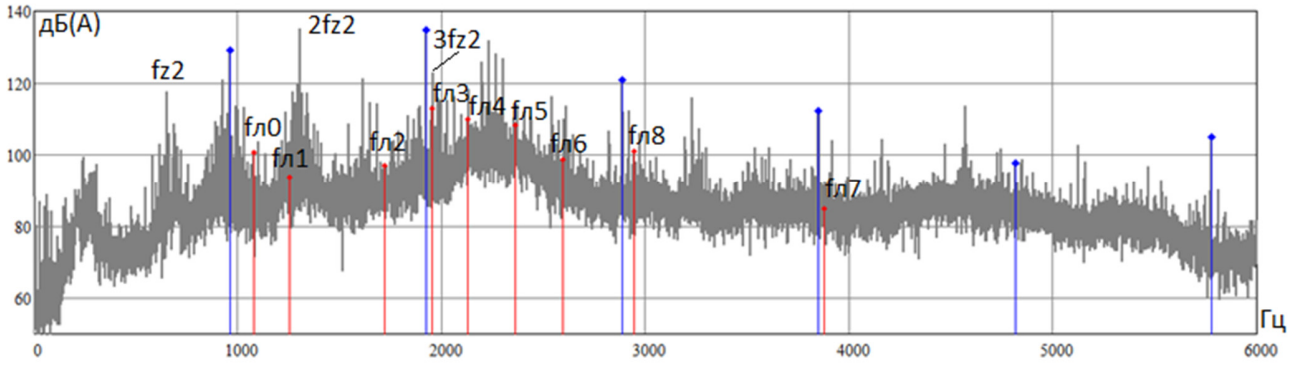


Рис. 5. Среднечастотная часть спектра вибрации корпуса турбокомпрессора.

Важной задачей диагностирования газотурбинного двигателя является оценка состояния проточной части турбокомпрессора и свободной турбины, состоящей из двух частей. Первая – контроль турбулентности потока по росту лопаточных составляющих вибрации, вторая – обнаружение импульсной вибрации, возбуждаемой нелинейными процессами при нарушении зазоров между вращающимися и неподвижными элементами двигателя, вплоть до задевания.

При холодной прокрутке на частотах вращения роторов компрессора и свободной турбины около 30Гц аэродинамического взаимодействия бездефектных лопаток с неоднородным воздушным потоком еще недостаточно для возбуждения заметной лопаточной вибрации. Так, на рис.5 показано, что лишь некоторые лопаточных гармоник, которые существенно меньше зубцовых, можно выделить в спектре вибрации корпуса двигателя. В то же время при появлении развитых дефектов, приводящих к значительной неоднородности потока воздуха в проточной части компрессора и турбины, лопаточные гармоники вибрации могут стать заметными даже при вращении рабочих колес с частотами около 30Гц.

При появлении дефектов сборки газотурбинного двигателя, приводящих к резкому локальному уменьшению зазоров между рабочими колесами и направляющим аппаратом, могут появиться импульсные колебательные силы, возбуждающие импульсную вибрацию корпуса двигателя даже на более низких частотах вращения. Однако из семи обследованных новых двигателей ни в одном не было обнаружено импульсных составляющих вибрации, возбуждаемых на лопаточных частотах.

Несмотря на это, в разрабатываемую методику диагностирования газотурбинных двигателей при их холодной прокатке вошли признаки дефектов не только их механических узлов на основе анализа узкополосных спектров тока и вибрации а также импульсной вибрации от возможных ударов, но и проточной части по широкополосным спектрам случайной вибрации корпуса, возбуждаемой как трением в подшипниках и зубчатых зацеплениях, так и турбулентностью воздушного потока.

По результатам исследований разработано программное обеспечение для автоматической обработки результатов измерений вибрации и тока, а также по обнаружению и идентификации наиболее вероятных видов дефектов, которое может использоваться в составе стендовых систем диагностики на основе систем СМД-4.

Пороговые значения в используемых диагностических моделях строятся на основе групповой обработки данных измерений вибрации и тока в каждой из точек контроля, большой группы идентичных газотурбинных двигателей, вращающихся в идентичных условиях. По мере увеличения группы контролируемых двигателей пороговые значения автоматически уточняются.

СПИСОК ЛИТЕРАТУРЫ

1. Barkova, N. A. Vibration diagnostics of equipment units with gas turbine engines /Natalia Barkova, Aleksey Barkov, Dmitriy Grishchenko // Vibroengineering Procedia. – 2019. – Vol. 25. – P. 89 – 94. – ISSN 2345-0533.
2. Неразрушающий контроль: Справочник: В 7 т. Под общ. ред. В. В. Клюева. Т.7. В 2 кн. Кн. 2. Вибродиагностика / Ф. Я. Балицкий, А. В. Барков, Н. А. Баркова и др. – М.: Машиностроение, 2005. – 829 с.
3. Рандалл, Р. Б. Частотный анализ / Р. Б. Рандалл. – Глоструп, Дания : К. Ларсен и сын, 1989. – 389 с. – IBSN 87-87355-25-6.
4. Barkov, A. Condition Assessment and Life Prediction of Rolling Element Bearing / A. Barkov N. Barkova, J. Mitchell // Sound and Vibration. – 1995. – Issue 6, P. 10-17.

УДК 629.59

СПОСОБ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ РАБОТЫ КОРАБЕЛЬНОГО ЭНЕРГЕТИЧЕСКОГО ОБОРУДОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ЭКСПЛУАТАЦИОННЫХ ЭНЕРГЕТИЧЕСКИХ ХАРАКТЕРИСТИК

Воронин Константин Павлович, Лапидус Алексей Яковлевич, Поляков Сергей Алексеевич
Военный учебно-научный центр Военно-Морского флота «Военно-Морская академия им. Н.Г. Кузнецова»
Ушаковская наб., 17, Санкт-Петербург, 197045, Россия
e-mail: 424756b@mail.ru

Аннотация. Предложен способ получения и использования эксплуатационной энергетической характеристики корабля в системе учёта потребления энергии применительно к задаче автоматизированного и автоматического управления в информационно защищенном исполнении энергопотреблением корабля.

Ключевые слова: корабль; эффективность; энергетическая характеристика; опытный; расчетный; смешанный; комбинированный.

A METHOD FOR INCREASING THE EFFICIENCY OF SHIP POWER EQUIPMENT USING OPERATIONAL ENERGY CHARACTERISTICS

Voronin Konstantin, Lapidus Aleksey, Polyakov Sergey
Military training and research center of the Navy «Naval Academy named after N. G. Kuznetsov»
17 Ushakovskaya Emb, St. Petersburg, 197045, Russia
e-mail: 424756b@mail.ru

Abstract. The article discusses a method for obtaining energy characteris/tics for energy metering systems and control tasks for the ship's energy consumption.

Keywords: ship; efficiency; energy characteristic; experimental; calculated; mixed; combined.

В основе методов нормирования судовых энергозатрат лежит энергетическая характеристика объекта энергопотребления, необходимость использования которой сформулирована в работах ученых И.В. Гофмана и А.А. Тайца. Известно определение: *Энергетическая характеристика* объекта – комплекс зависимостей номинальных и исходно-номинальных значений технико-экономических показателей его работы в абсолютном, удельном или относительном исчислении от нагрузки или других нормообразующих показателей при фиксированных значениях внешних факторов. Известные методы ее получения приведены в таблице 1.

Таблица 1

Методы получения энергетической характеристики объекта энергопотребления

Метод получения энергетической характеристики	**Достоинства**	**Недостатки**
Опытный	высокая точность	большое число натурных испытаний, в том числе и на больших по нагрузке режимах; не учитывает изменения в составе оборудования.
Расчётный	высокая детализация расчета (агрегат-операция)	большой объем исходных данных; высокая трудоёмкость получения энергетической характеристики; не учитывает техническое состояние оборудования сложность определения энергопотребления оборудования на холостом ходу
Смешанный	учитывает изменения в составе и режимах работы оборудования;	большой объём исходной информации, для сбора которой необходима автоматизированная система технического учёта эксплуатационных параметров; техническое состояние энергопотребляющего оборудования считается неизменным;

Комбинированный	высокая точность; простота расчёта энергетической характеристики; учитывает изменения в составе, режимах работы и техническом состоянии оборудования.	необходимость наличия на корабле автоматизированных систем учета, контроля и управления режимами работы.

Энергетические характеристики могут выражать как функциональную связь между расходом энергии и той или иной переменной величиной, так и соответствующую статистическую связь. Функциональную связь можно установить либо расчётным путем, либо на основе специально подготовленных испытаний.

Для выявления статистических связей, как правило, пользуются учетными данными и проводят достаточно большое число сокращенных испытаний (замеров).

Согласно рис. 1 различают опытный, расчетный и смешанный метод получения энергетической характеристики. В табл. 2 приведены условия, при которых возможен выбор того или иного метода получения энергетической характеристики в зависимости от систем учёта энергопотребления. В табл. 3 приведены условия выбора метода получения энергетической характеристики в зависимости от задач управления энергопотреблением корабля.

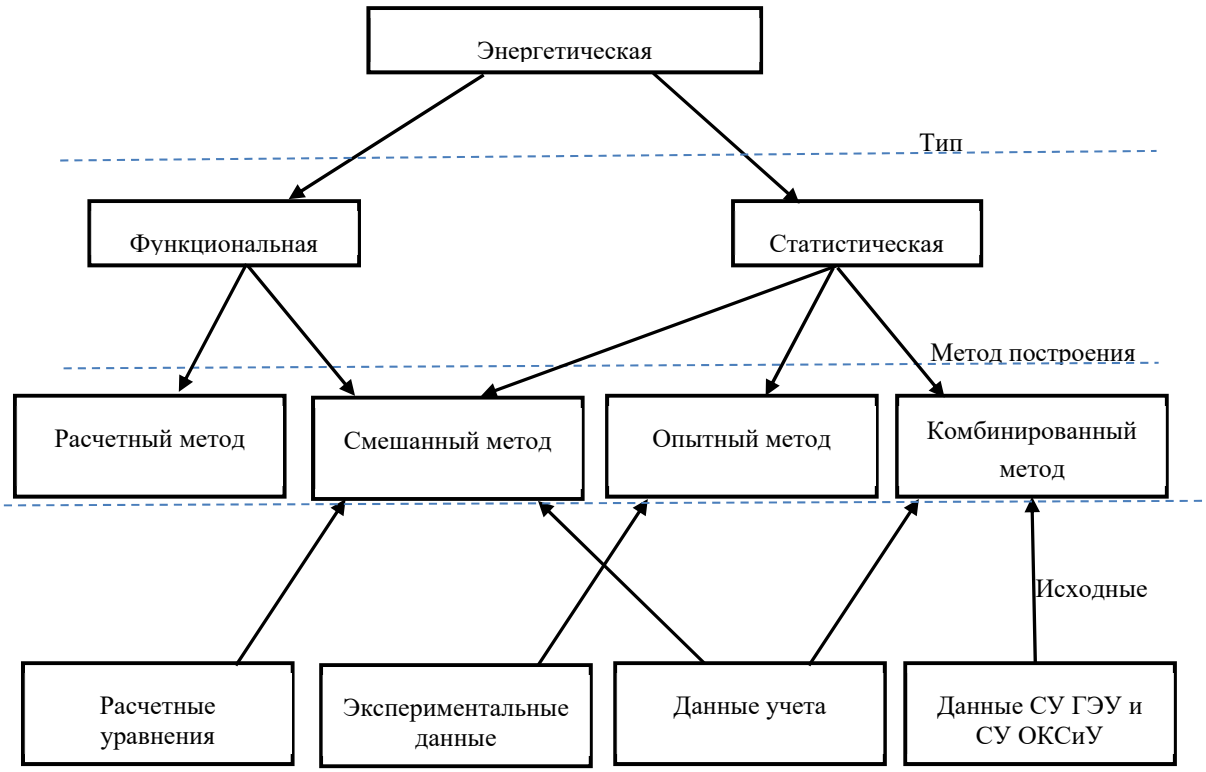


Рис. 1. Методы получения энергетической характеристики.

Определить какой метод получения энергетической характеристики предпочтителен для того или иного объекта, исходя из уровня автоматизации управления всеми процессами и автоматизации учёта энергопотребления на корабле, а также из задач управления энергопотреблением корабля, возможно, используя механизм выбора наилучшего метода получения энергетической характеристики, приведенный на рис. 2.

Комбинированный метод получения ЭХ наиболее актуален для современных кораблей и перспективных кораблей на полном электродвижении, на которых внедрение современных систем автоматического управления и учета потребления энергетических ресурсов осуществлено в соответствии с конструкторской документацией и не требует дополнительных капиталовложений (корабли проектов 22350, 11356 и 20385(6).

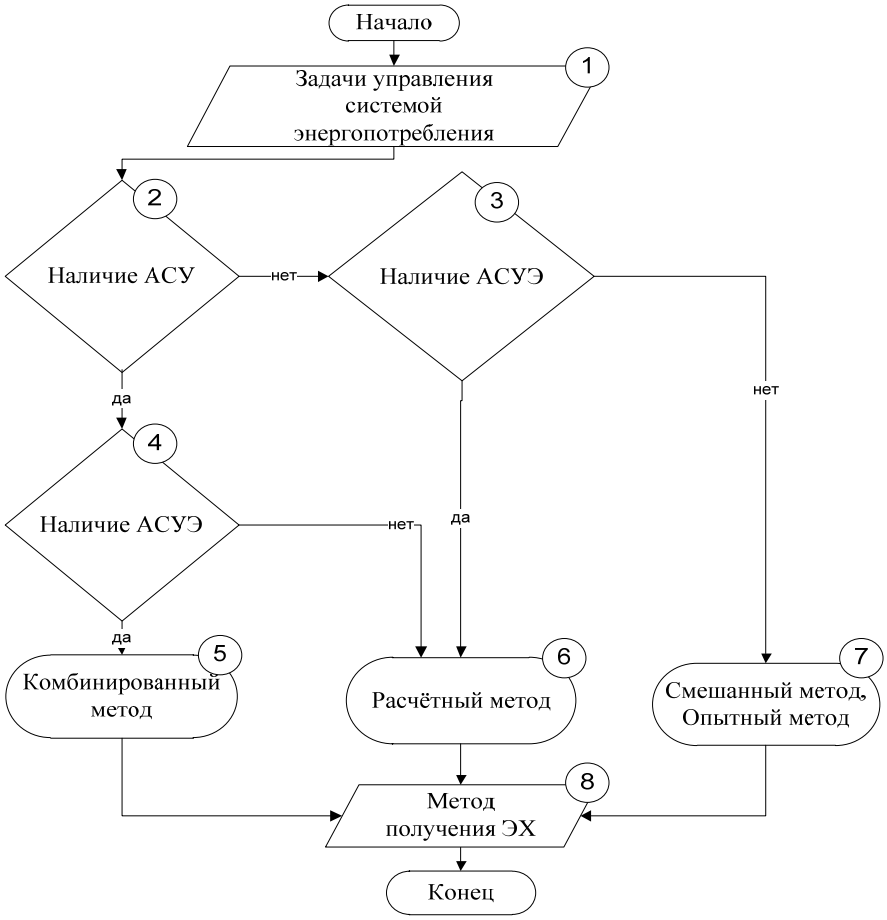


Рис. 2. Механизм выбора метода получения энергетической характеристики.

Таблица 2

Соответствие метода получения энергетической характеристики системам учёта потребления энергии на корабле.

Метод получения ЭХ	Система учёта энергопотребления			Система управления ВВСТ		
	Автоматическая	Автоматизированная	Ручная	Автоматическая	Автоматизированная	Ручное
1. Опытный	+	+	-	+	+	+
2. Смешанный	+	+	-	+	+	+
3. Расчётный	+	+	+	+	+	+
4.Комбинированный	+	+	-	+	+	-

Комбинированный метод обеспечивает получения ЭХ в оперативном режиме (режиме реального времени), с использованием которой может производиться обоснованное определение величины энергопотребления корабля.

Введем понятие «Эксплуатационная энергетическая характеристика» (ЭЭХ) – зависимость энергопотребления технологического процесса от влияющих на него факторов (эксплуатационных, социально-экономических, гидрометеорологических), учитывающая их изменение в режиме реального времени.

Таблица 3

Соответствие метода получения энергетической характеристики
задачам управления энергопотреблением корабля

Метод получения ЭХ	Задачи управления энергопотреблением			
	Оптимизация энергопотребления	Обеспечение расчёта энергоэффективности корабля (боевой части)	Планирование, прогнозирование заправок топливом, минимизация затрат материальных ресурсов	Ранжирование каждой выполняемой задачи по уровню энергопотребления
1. Опытный	-	+	+	-
2. Смешанный	-	+	+	-
3. Расчётный	+	+	+	-
4.Комбинированный	+	+	+	+

Современное развитие АСУ и АСУЭ позволяет разработать комбинированный метод получения ЭХ. Причем, не только для ускорения процессов и точности оценки ЭХ, но и для исключения ошибок операторов, негативного влияния их субъективных свойств (так называемого «человеческого фактора») и обеспечения информационной защищенности в целом системы управления электроэнергетикой корабля.

Основным отличием комбинированного метода от существующих является использование им как данных о времени работы и нагрузке, так и данных с АСУ всего энергетического оборудования и т.п.

Комбинированный метод, сочетая в себе достоинства опытного и расчётного метода, позволяет производить получение энергетической характеристики, используя статистические данные, собираемые системами учёта корабля, с меньшей трудоёмкостью, чем опытный и большей точностью, чем расчётный метод. Это достигается за счёт разделения всего энергопотребляющего оборудования на группы – энергетические профили (ЭПр) и обработки статистических данных о потреблении ТЭР кораблём с учётом работы того или иного ЭПр, что позволяет производить получение энергетической характеристики и расчет НОЭ с детализацией выше чем существующая на корабле система учёта потребления ТЭР.

Например, АСУЭ определяет в режиме реального времени энергопотребление конкретного оборудования в электромеханической боевой части. Большинство изделий имеет резервные приводы или резервные источники питания, работой которых управляет программа под наблюдением оператора, предоставляющая в режиме реального времени данные о состоянии любой системы и агрегатах, работающих в ней (включен/выключен).

С использованием комбинированного метода могут быть получены ЭХ любого стандартного (неаварийного) набора агрегатов. С использованием расчётного метода можно получить только ЭХ боевой части (боевого поста), а для получения ЭХ включенных агрегатов необходимо организовать учет энергопотребления каждого возможного набора работающих агрегатов при выполнении определенной задачи, создание энергетического подобия инструкции по использованию средств движения при заданных режимах работы ГЭУ. Организация автоматизированного учета энергопотребления отдельного набора агрегатов потребует значительных временных затрат.

Таким образом, для повышения точности расчёта НОЭ применение комбинированного метода получения ЭХ экономически целесообразно в отличие от расчётного метода.

С использованием ЭЭХ для конкретного набора факторов (конкретных условий плавания) может быть получена технически и экономически обоснованная величина энергопотребления необходимого и достаточного набора оборудования в каждой боевой части и корабля в целом.

Системы учёта энергопотребления и управления механизмами корабля, задачи управления энергопотреблением корабля определяют возможность применения того или иного метода получения ЭХ.

Возможность применения одного из вышеописанных методов получения энергетической характеристики также обусловлено наличием на корабле необходимых для расчётных моделей исходных данных, т.к. каждый метод предъявляет свои требования к полноте, количеству и точности исходных данных.

Современное развитие АСУ и АСУЭ позволяет разработать метод, учитывающий связь энергопотребления со структурой и режимом работы ВВСТ на корабле – комбинированный метод получения энергетической характеристики.

Метод наиболее актуален для современных кораблей, на которых внедрение современных систем автоматического управления оборудованием и учета потребления энергетических ресурсов осуществлено по проекту и не требует дополнительных капиталовложений.

Комбинированный метод, сочетая в себе достоинства опытного и расчётного метода, позволяет производить получение энергетической характеристики, используя статистические данные, собираемые системами учёта корабля, с меньшей трудоёмкостью, чем опытный и большей точностью, чем расчётный метод. Это достигается за счёт

разделения всего энергопотребляющего оборудования на группы – энергетические профили (ЭПр) и обработки статистических данных о потреблении ТЭР кораблём с учётом работы того или иного ЭПр, что позволяет производить получение ЭХ и производить управление и учёт потребления ТЭР.

Таким образом, предложенный способ получения и использования эксплуатационной энергетической характеристики корабля в системе учёта потребления энергии применительно к задаче автоматизированного и автоматического управления в информационно защищенном исполнении энергопотреблением корабля позволяет, по нашему мнению, ускорить процесс и точность оценки ЭХ, а также исключить ошибки личного состава, исключить негативное влияние его субъективных свойств, обеспечить в целом информационную защищенность и существенно повысить эффективность управления электроэнергетической системы корабля.

СПИСОК ЛИТЕРАТУРЫ

1. Кудрин Б.И. О теоретических основах и практике нормирования и энергосбережения. «Промышленная энергетика», №6, 2000 г., с.33-36.
2. Гринев А.В. Повышение эффективности нормирования потребления энергоресурсов на промышленных предприятиях [Текст]/ А.В. Гринев, О.В. Новикова, С.В. Лозовский // Научно-технические ведомости СПбГПУ. Экономические науки. -2013. № 5(180) - С. 54-59.
3. Котов В.С. К вопросу повышения надежности энергетических установок кораблей дальней морской зоны / В. С. Котов, А. Ю. Харин, А. Г. Новиков, Р. К. Резникова // Материалы конференции «Управление в морских системах» (УМС-2018), Санкт-Петербург, 02–04 октября 2018 года. – Санкт-Петербург: «Концерн «Центральный научно-исследовательский институт «Электроприбор», 2018. – С. 53-58.

УДК 629.59

ПРОРАБОТКА ВОЗМОЖНОСТИ СОЗДАНИЯ НОВОЙ СИСТЕМЫ КОНТРОЛЯ ДЕЖУРНО-ВАХТЕННОЙ СЛУЖБЫ ПОДВОДНОЙ ЛОДКИ НА ЭТАПЕ ИССЛЕДОВАТЕЛЬСКОГО ПРОЕКТИРОВАНИЯ

Захаров Андрей Владимирович, Иванов Борис Григорьевич, Москаленков Василий Александрович, Поляков Сергей Алексеевич

Военный учебно-научный центр Военно-Морского флота «Военно-Морская академия им. Н.Г. Кузнецова»
Ушаковская наб., 17, Санкт-Петербург, 197045, Россия
e-mail: 424756b@mail

Аннотация. Рассмотрен вопрос упрощения архитектуры и процедур автоматизированной системы контроля дежурно-вахтенной службы за счет перехода к современным коммуникационным технологиям в защищенном исполнении.

Ключевые слова: обход, контроль, дежурно-вахтенная служба, подводная лодка, оператор.

ELABORATION OF THE POSSIBILITY OF CREATING A NEW CONTROL SYSTEM FOR THE WATCH-KEEPING SERVICE OF A SUBMMARINE AT THE STAGE OF RESEARCH DESIGN

Zaharov Andrey, Ivanov Boris, Moskalenko Vasiliy, Polyakov Sergey

Military training and research center of the Navy «Naval Academy named after N. G. Kuznetsov»
17 Ushakovskaya Emb, St. Petersburg, 197045, Russia
e-mail: 424756b@mail.ru

Abstract. The issue of simplifying the architecture and procedures of the automated control system of the duty-watch service due to the transition to modern communication technologies in a secure design is considered.

Keywords: bypass; control; watch duty; submarine; operator.

Дежурно-вахтенная служба (ДВС) на кораблях и судах Военно-морского флота России должна совершать обход своих заведований, механизмов и работающих устройств каждые 30 минут, чтобы предотвратить аварийную ситуацию, которая может повлечь за собой смерть личного состава и вывод из строя техники. Ранее для определения был ли совершен обход в отсеке, устанавливали картонные часы, на которых ДВС должна была передвигать вручную стрелку на циферблате. Со временем часы были заменены на тумблеры. Это неудобно и нужно затрачивать драгоценное время вахты. Мы предлагаем совершено другую систему с учетом развития возможностей современных безопасных информационных технологий.

Данная система контроля позволяет определять точное количество посещенных мест в ходе обхода и количество неосмотренных мест, время прибытия, персональные данные проверяющего, а также информацию о наличии какой-либо неисправности в том или ином технологическом узле осматриваемого отсека. Каждый член дежурно-вахтенной службы получает персональное устройство, на котором прописаны его персональные данные (для идентификации личности при приложении устройства к терминалу) и количество посещений контрольных точек при обходе в течение смены [1].

Известна локальная система контроля и сбора данных, при которой связь между главным (центральным) терминалом и второстепенными (локальными) терминалами осуществляется за счет каналов связи (в качестве

которых выступает канал радиосвязи или же коммутируемый канал сети телефонной связи). К локальным терминалам посредством подключения силовой сети электропитания и контроллера подключены группы датчиков.

Описанные терминалы в свою очередь подключены к центральному терминалу, который оснащен модемом данных и так же через блок сопряжения подключен к силовой сети электропитания. Сбор данных при этом осуществляется раз в сутки или же в месяц согласно прописанной программе. Данное устройство требует дополнительных источников электропитания, что усложняет конструкцию системы в целом. Передача данных осуществляется по каналам телефонной или радиосвязи, которые уже используются другими потребителями, т.е. необходимо выбирать, что важнее связь на подводной лодке между отсеками или сбор данных с устройства, что является неприемлемым [2].

Известно устройство автоматического табельного учета, применяемое в шахтах и рудниках, которое предназначено для фиксации времени прибытия людей в различные помещения. Оно включает в себя следующие блоки: связи, печати, управления, памяти и считывания. Однако, данная система является мало эффективной в связи со своей малой функциональностью.

Наиболее близким техническим решением и принятым за прототип является система контроля посетителей. Устройство представляет собой приемопередающее устройство размером с брелок, которое способно принимать, хранить и обновлять информацию, содержащуюся в нем. Оно позволяет отслеживать персонал в контрольных точках, размещенных в необходимых местах зданий. Обработка сигналов осуществляется в информационно-вычислительном центре, куда она поступает за счет двухсторонней беспроводной связи или двухпроводной силовой информационной сети с приемопередающими блоками [3].

Задача системы контроля за несением корабельной вахты подводной лодки заключается в формировании и выдаче команд управления исполнительным устройствам (установленных в отсеках) при считывании зарегистрированного в памяти подсистемы идентификационного признака (кода), а также отслеживание времени проверки личным составом дежурно-вахтовой службы необходимых технологических узлов подводной лодки и обеспечение передачи информации о состоянии системы на главный пульт управления.

На рис. 1 для иллюстрации представлена упрощенная схема системы контроля дежурно-вахтовой службы, на рис. 2 - расположение терминалов на подводной лодке.

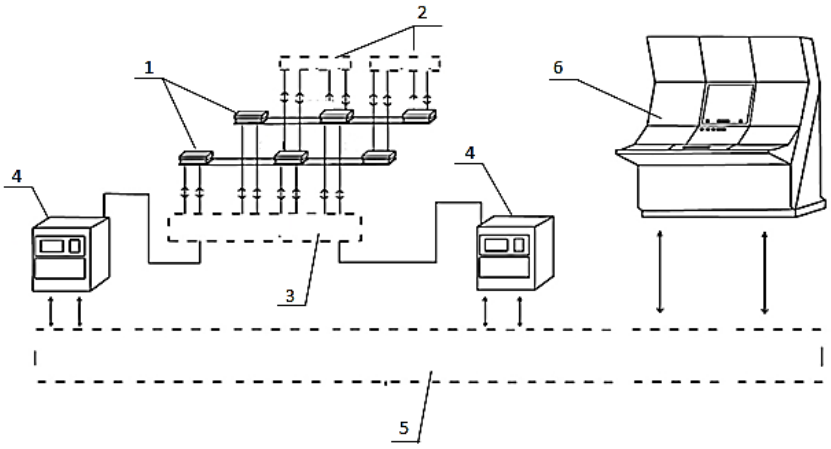


Рис. 1 - Структурная схема системы контроля дежурно-вахтовой службы, где ЦП (6) – центральный пост, АКП (4) – автоматический контрольный пункт, ГРЩ (3) – главный распределитель, БСМ (1) – блок считывания магнитных карт, СОД (5) – система обработки данных, контроллеры (2)

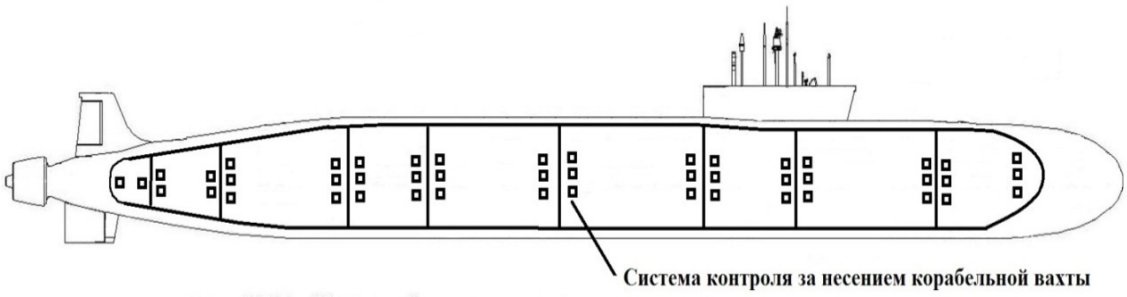


Рис. 2. Расположение терминалов (условно) на подводной лодке.

Принцип работы системы заключается в следующем: при проведении осмотра технологических узлов, расположенных в контрольных точках отсеков подводной лодки, оператор прикладывает устройство ввода (в нашем случае – это персональная карта) к блоку считывания магнитных карт 1.

Впоследствии система идентифицирует личность проверяющего, отмечает время проведения диагностики и активирует возможность выбора подачи сигнала на пульт управления центрального поста 6. При этом оператору доступны для нажатия две кнопки, первая – «Система исправна», вторая – «Система неисправна».

После обработки данных информация проходит через контроллеры 2 и поступает в главный распределитель 3, откуда она отправляется на ближайший и менее загруженный автоматический контрольный пункт 4. Здесь обеспечивается контроль и проверка данных, после чего они отправляются в систему обработки данных 5, в которых формируется отчет, поступающий на центральный пост 6. Он обеспечивает контроль и управление работой системы, включая блок управления и блок памяти.

Тем самым ответственное лицо, находящееся в центральном посту 6, незамедлительно получает информацию о своевременной проверке каждого узла и о наличии неисправности в отсеке, не дожидаясь доклада вахтенного.

Данная система контроля дежурно-вахтенной службы подводной лодки, отличается от известных тем, что применяются персональные карты дежурно-вахтовой службы, которые содержат в себе информацию о личных данных лиц, находящихся в наряде, количество пройденных и оставшихся контрольных точек при обходе подводной лодки с использованием «мгновенной» передачи сигнала от блока считывания магнитных карт к центральному посту о наличии неисправности или исправности конкретного узла в отсеке, а так же данные о лице, отправившего сигнал, и точное время его отправки.

Таким образом, предлагаемая система, с учетом технического прогресса в области информационных технологий, позволит повысить качество контроля несения дежурно-вахтовой службы, конфиденциальность, доступность и целостность данных.

Личный состав обеспечивается персональным приемопередающим устройством с блоком памяти, куда осуществляется запись различных сведений, например, персональные данные, количество пройденных и оставшихся контрольных точек при проведении обхода (осмотра) подводной лодки. Это устройство может также подавать и принимать сигналы тревоги.

СПИСОК ЛИТЕРАТУРЫ

1. Арцыкова Л.А., Парфенов Ю.М., Соколов В.С. Оценка живучести технических систем на ранних этапах проектирования. Алгоритм № 249. В кн.: Сборник алгоритмов и программ, выпуск №11. Л.: ВМА, 1987, с.53-70.
2. Руденко Ю.И., Ушаков И.А. Надежность систем энергетики. Новосибирск: Наука, 1989.
3. Котов В.С., Харин А.Ю., Новиков А.Г., Резникова Р.К. К вопросу повышения надежности энергетических установок кораблей дальней морской зоны / Материалы конференции «Управление в морских системах» (УМС-2018). 2018. С. 53-58.

УДК 629.59

ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ КОРАБЛЯ КАК СЛОЖНОГО СВОЙСТВА

Иванов Борис Григорьевич, Москаленко Василий Александрович, Поляков Сергей Алексеевич, Ревин Алексей Дмитриевич

Военный учебно-научный центр Военно-Морского флота «Военно-Морская академия им. Н.Г. Кузнецова»
Ушаковская наб., 17, Санкт-Петербург, 197045, Россия
e-mail: 424756b@mail.ru

Аннотация. Выполнен анализ и исследована на основе декомпозиции уровней состояния комплексная безопасность корабля как сложного его свойства, включая защищенность информационных ресурсов. Показана возможность эффективного управления безопасностью корабля в условиях воздействия противника.

Ключевые слова: безопасность; корабль; классификация; анализ; скрытность; неуязвимость; живучесть.

STUDY OF SHIP SAFETY AS A COMPLEX PROPERTY

Ivanov Boris, Moskalenko Vasiliy, Polyakov Sergey, Revin Aleksey

Military training and research center of the Navy «Naval Academy named after N. G. Kuznetsov»
17 Ushakovskaya Emb, St. Petersburg, 197045, Russia
e-mail: 424756b@mail.ru

Abstract. The complex safety of the ship as its complex property, including the security of information resources, is analyzed and investigated on the basis of the decomposition of state levels. The possibility of effective ship safety management in the conditions of enemy influence is shown.

Keywords: safety; ship; classification; analysis; stealth; invulnerability; survivability.

Одним из важных свойств корабля является его комплексная безопасность, включая защищенность информационных ресурсов. Как правило, в основе расчетных алгоритмов и методик оценки комплексной

безопасности лежит структура объекта исследования. Однако, не всегда существующие классификации объекта изучения устраивают исследователя, поэтому возникает необходимость в разработке такой его структуры, которая позволит выполнить многоаспектный анализ свойств корабля. Подобная ситуация сложилась при нашей попытке разработать алгоритм получения количественного показателя безопасности корабля [1].

Для анализа безопасности корабля и выявления свойств, ее составляющих, рассмотрены возможные состояния корабля в условиях воздействия по нему противника на основе декомпозиции уровней состояния по методу Марковских цепей (рис. 1).

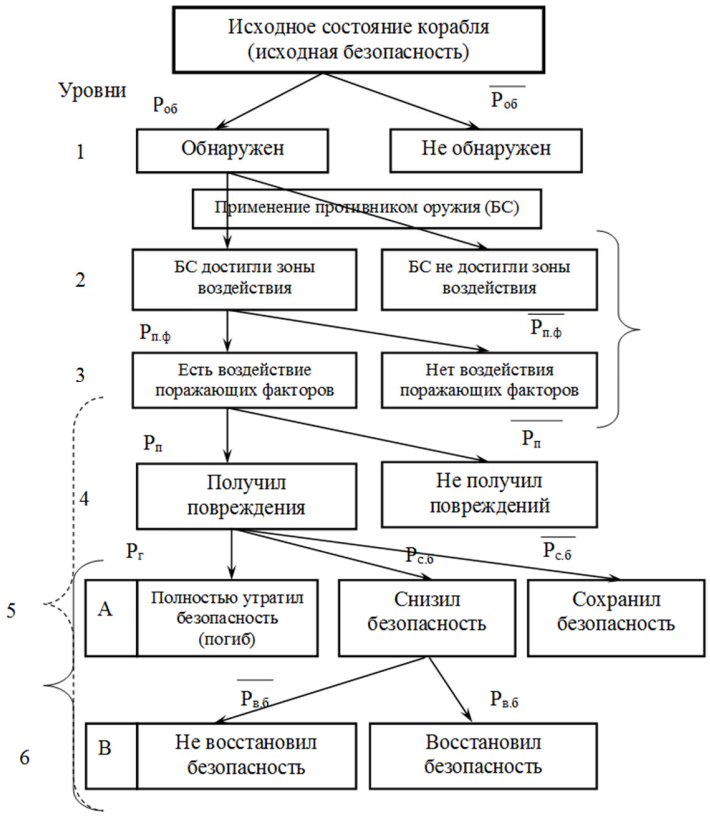


Рис. 1. Уровни состояний корабля в условиях воздействия по нему противника.

Для нанесения удара по кораблю или воздействия иного вида противник сначала должен его обнаружить. На первом уровне возможны два несовместных события: либо корабль обнаружен, либо корабль не обнаружен. Каждому из этих событий соответствует вероятность его наступления. Если корабль не обнаружен $P_{об}$, то его состояние ничем не отличается от исходного, а для анализа остается событие обнаружения корабля $P_{об}$.

В случае обнаружения корабля противник применяет по нему оружие. Рассматривая все возможные варианты событий на втором уровне, можно выделить два: либо боевые средства (БС) противника достигли зоны воздействия по кораблю, либо не достигли этой зоны. Если БС не достигли зоны воздействия, то состояние корабля ничем не отличается от исходного. Для анализа остается событие, когда БС достигли зоны воздействия. Чтобы сохранить свою безопасность корабль должен стремиться избежать попадания в него боевых средств противника, используя все имеющиеся средства и способы. На этом (третьем) уровне возможны два несовместных события: либо по кораблю есть воздействие поражающих факторов оружия противника ($P_{п.ф}$), либо корабль сумел уклониться или нейтрализовать боевые средства противника, т. е. избежать воздействия поражающих факторов ($P_{п.ф.}$). Если корабль не подвергся воздействию поражающих факторов оружия противника, то его состояние ничем не отличается от исходного, а для анализа остается событие воздействия по кораблю поражающих факторов оружия противника [2].

Если отмечается воздействие поражающих факторов, то на следующем (четвертом) уровне возможны следующие несовместные события: либо корабль получил повреждения ($P_{п}$), или корабль не получил повреждений ($P_{п}$). Если корабль не получил повреждений ($P_{п}$), то его состояние ничем не отличается от исходного, а для анализа остается событие наличия повреждений на корабле.

На пятом уровне раскрываются последствия получения кораблем повреждений, следствием повреждений могут быть три состояния корабля: корабль полностью утратил безопасность (погиб); у корабля в какой-то мере снижена безопасность ($Р_{с.б}$); повреждения не повлияли на безопасность корабля, т.е. безопасность не снижена.

Если корабль погиб, то это конечное состояние объекта «А». Если у корабля безопасность не снижена ($Р_{с.б}$), то его состояние ничем не отличается от исходного, а для анализа остается событие, когда у корабля в какой-то мере снижена безопасность ($Р_{с.б.}$)

В том случае, когда корабль получил повреждения и не погиб, но у него снижена безопасность, личный состав начинает действия по восстановлению безопасности корабля. Результатом действий могут быть два состояния: либо корабль восстановил безопасность ($Р_{в.б}$) и тогда его состояние не отличается от исходного, либо экипаж не смог восстановить безопасность ($Р_{в.б}$) и тогда это конечное положение анализа, поскольку ему соответствует уже другой корабль с новой исходной безопасностью. Поскольку достигнуто два конечных состояния, то декомпозиция может считаться законченной [3].

Каждому уровню проведенной декомпозиции можно сопоставить соответствующее ему свойство корабля. На первом уровне состояний корабля его способность не быть обнаруженным обеспечивается таким свойством, как скрытность. Материальными объектами, обеспечивающими данное свойство, являются средства и системы снижения первичных и вторичных физических полей [4].

Второй и третий уровни можно объединить в способность корабля избежать воздействия поражающих факторов. Эту способность корабля С.О. Макаров называл неуязвимостью. Он писал «Способность судна оставаться невредимым от действия неприятельских ударов - будет ли то достигнуто броней или другим способом - есть один из элементов оборонительной силы судов, называемый неуязвимостью". "…неуязвимость есть главный элемент оборонительной силы судов». В современной классификации такого свойства у корабля нет. Материальными объектами, обеспечивающими неуязвимость, являются системы оружия самообороны, системы отвлечения боевых средств, движительно-рулевой комплекс, обеспечивающий маневренность при уклонении от обнаружения и поражения.

На четвертом уровне способность корабля не получать повреждений при воздействии по кораблю поражающих факторов оружия противника называется стойкостью. Строго говоря, в соответствии с приведенным выше высказыванием Макаров Степан Осипович считал стойкость элементом неуязвимости. В настоящее время большинство исследователей считают ее самостоятельным свойством. Материальным объектом, обеспечивающим стойкость корабля, является его конструктивная защита [5].

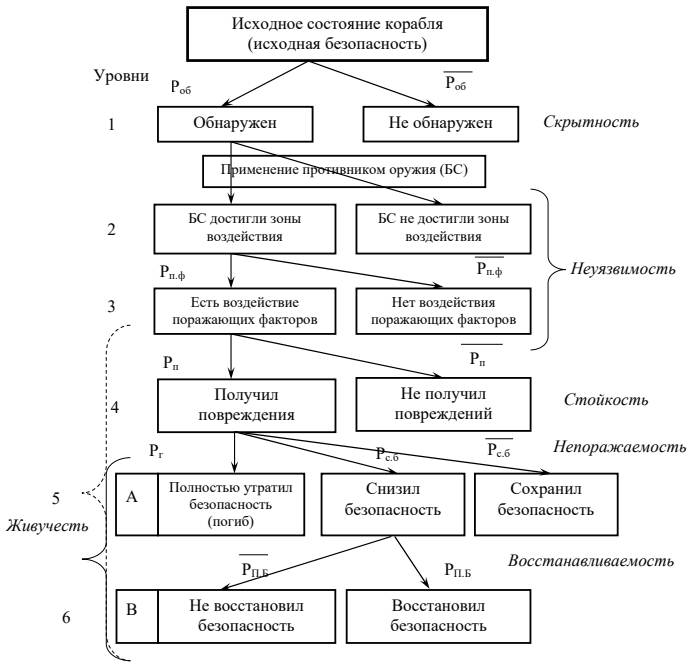


Рис. 2. Соответствие свойств уровням состояний корабля в условиях воздействия противника.

С.О. Макаров в [6] впервые сформулировал понятие живучести корабля как «способность судна продолжать бой, имея повреждения в различных боевых частях». В соответствии с этим определением свойство корабля, отвечающее пятому уровню, следует назвать живучестью. Материальными объектами, обеспечивающими это свойство, являются средства и системы по борьбе с водой и пожаром, по обеспечению функционирования оружия и технических средств в экстремальных условиях, по защите личного состава. Шестой уровень определяет вероятность

восстановления безопасности корабля и такое его свойство, как восстанавливаемость. Соответствие свойств корабля уровням воздействия приведено на рис. 3.

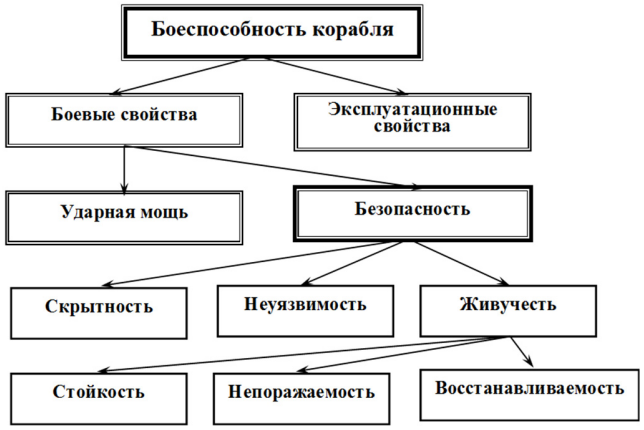


Рис. 3. Структура боеспособности корабля.

Выполненный анализ состояний корабля наглядно показывает, что безопасность обеспечивается следующими свойствами: скрытностью, неуязвимостью и живучестью. Именно их максимизация в комплексе, в том числе с учетом широкого спектра вопросов обеспечения информационной безопасности, должна быть главной задачей исследовательского проектирования корабля на стадии концептуального формирования его облика.

СПИСОК ЛИТЕРАТУРЫ

1. Безнос Л.А. Обеспечение живучести надводного корабля. Учебное пособие. Л.: ВМА,1985.
2. Арцыкова Л.А., Парфенов Ю.М., Соколов В.С. Оценка живучести технических систем на ранних этапах проектирования. Алгоритм № 249. В кн.: Сборник алгоритмов и программ, выпуск №11. Л.: ВМА, 1987, с.53-70.
3. Васюнькин В.В. Живучесть надводных кораблей. Учебное пособие. СПб: ВМА, 1992.
4. Фисай В.Г., Иванов Б. Г. Обоснование внедрения системы информационной поддержки для обеспечения живучести кораблей и судов Научно-технический сборник Российского морского регистра судоходства. 2016. № 42-43. С. 130-133.
5. Котов В.С., Харин А.Ю., Новиков А.Г., Резникова Р.К. К вопросу повышения надежности энергетических установок кораблей дальней морской зоны // Материалы конференции «Управление в морских системах» (УМС-2018). 2018. С. 53-58.
6. Макаров С.О. Разбор элементов, составляющих боевую силу судов / Морской сборник, 1894, № 6, с. 1–106.

УДК 621.391.63

МОДЕЛИРОВАНИЕ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ПРЕДПРИЯТИЯ МОРСКОГО ПРИБОРОСТРОЕНИЯ

Кобзев Валентин Васильевич, Шилов Антон Константинович
АО «Концерн «НПО «Аврора»
Карбышева ул., 15, Санкт-Петербург, 194021, Россия
e-mail: aspin.avrora@inbox.ru

Аннотация. В статье рассмотрены основные положения, связанные с моделированием технологического процесса на основе нового математического аппарата – многомерных функциональных сетей. Описываются слова алгоритмического языка и синтаксис языка, которые составляют основу алгебраических функциональных сетей. Приводятся модели типовых функциональных структур с конкретными примерами их применения. Представлен технологический процесс как объект моделирования и его графическая интерпретация. Введен целый ряд понятий, характеризующий технологический процесс как производственную человеко-машинную систему.

Ключевые слова: моделирование; технологический процесс; сеть; алгоритм; язык; алгебра; оператор; операция; цикл; итерация; дефект; ошибка; ситуация; структура; объект; принцип; система; граф.

SIMULATION OF TECHNOLOGICAL PROCESS ON ENTERPRISES JF MARIN INSTRUMENTATION

Kobzev Valentin, Shilov Anton
JSC «Concern «NGOs «Aurora»
15 Karbysheva St, St. Petersburg, 194021, Russia
e-mail: aspin.avrora@inbox.ru

Abstract. The article deals with fundamental provisions, connected with simulation of technological process based on new mathematical tool – multidimensional functional networks. The words of algorithmic language and the syntax of language

are described, which form the basis of algebraic functional network. The models of standard functional structures are presented with specific examples of their use. Technological process is proposed as an object of simulation and its graphic interpretation. Wide range of notions is introduced, which characterize technological process as production man-machine system.

Keywords: simulation; technological process; network; algorithm; language; algebra; operator; cycle; iteration; defect; error; situation; structure; object; principle; system; graph.

Введение. Любой технологический процесс (за исключением полностью автоматизированного) можно представить в виде производственной человеко-машинной системы, под которой будем понимать систему, преобразующую предметы труда в продукт труда посредством взаимодействия субъектов труда с орудиями труда [1].

Продукт труда в нашем случае – это системы управления корабельными техническими средствами и их составные части. Продукт труда является целью производственной человеко-машинной системы (ЧМС). Введем несколько определений.

Предмет труда – это материальные или информационные объекты, в процессе преобразования которых получается продукт труда.

Субъекты труда – это специалисты, принимающие непосредственное участие в получении продукта труда (рабочие, инженеры, техники и т.п.).

Орудия труда – это технические и любые другие средства, используемые для получения продукта труда (станки, инструменты, средства контроля, роботозированные комплексы, вычислительная техника и т.п.).

В настоящее время есть целый ряд гостированных понятий. Они соотносятся с масштабом производственный ЧМС (завод, цех, производственный участок, рабочее место).

Под производственным процессом понимается совокупность всех действий специалистов и орудий производства, необходимых на данном предприятии для изготовления выпускаемых изделий.

Под технологическим процессом понимается часть производственного процесса, содержащая действия по изменению и последующему определению состояния предметов производства.

Под рабочим местом понимается часть производственной площади, на которой размещены один или несколько исполнителей работы и обслуживаемая им (ими) часть технологического оборудования, а также оснастка и предметы производства.

Как следует из приведенных выше определений, производственный и технологический процессы являются многофакторными, многокомпонентными динамическими системами, что, в свою очередь, предъявляет повышенные требования к управлению ими и обеспечению заданного качества продуктов труда.

Кроме того, из определения производственной ЧМС следуют факторы, обуславливающие качество предметов труда: человеческий фактор, надежность орудий труда, структура процесса функционирования, способы контроля.

Влияние перечисленных выше факторов на качество продукции предприятия можно оценить на основе моделирования технологического процесса, что и является целью данной статьи.

Язык алгоритмических алгебр В.М. Глушкова. Язык алгоритмических алгебр [2] был впервые применен для целей проектирования человеко-машинных технологий в работе [3] и развит в моделях процессов управления корабельными техническими средствами [4]. Не повторяя материал работ [3,4], введем несколько базовых понятий, применительно к технологическому процессу.

Под алгебраической функциональной сетью (АФС) будем понимать представление технологического процесса в двух алгебрах: $a_{оп}$ и $a_{оц}$, где $a_{оп}$ - алгебра описания процесса, $a_{оц}$ алгебра оценивания процесса с помощью количественных характеристик. Такими характеристиками могут быть: надежность, трудоемкость, стоимость. Поскольку речь идет о едином процессе, алгебры описания и оценки представляют собой биекцию (взаимно-однозначное соответствие), т.е. пары множеств:

$$a_{оп} = < M_{оп.э}, M_{оп.о} >; a_{оц} = < M_{оц.э}, M_{оц.о} >, \quad (1)$$

где $M_{оп.э}$ – множество описательных элементов, с помощью которых строится математическое описание процесса (слова алгоритмического языка). Описательные элементы могут иметь различную форму представления в виде графа, сети, ЛСА и т.п.; $M_{оп.о}$ – множество описательных операций, которые задают отношения между описательными элементами (синтаксис алгоритмического языка); $M_{оц.э}$ – множество оценочных элементов, т.е. количественных характеристик, с помощью которых оценивается качество выполнения описательных элементов; $M_{оц.о}$ – множество оценочных операций, т.е. операции над оценочными элементами, с помощью которых вычисляются характеристики фрагментов процесса или процесса в целом.

Процедура замены описательных операций их оценочными операциями называется укрупнением.

В теории функциональных сетей атомарной единицей процесса является функциональная единица (ФЕ). Функциональная единица – это группа или комбинация элементарных операций, представляющая собой самостоятельные в технологическом отношении операции.

Более высоким уровнем рассмотрения процесса является функциональная структура (ФС), представляющая собой группу или комбинацию ФЕ.

В системе алгоритмических алгебр В.М. Глушкова описание технологического процесса будет иметь вид:

$$a = < U, B, \Omega_1, \Omega_2 >, \quad (2)$$

где U = {A, B, C,…} – множество математических операторов;

B = {α, β, γ,…} – множество логических условий;

Ω_1 – множество операций, порождающих логические условия;

Ω_2 – множество операций, порождающих операторы из множества U.

К операциям из Ω_1 относятся операции дизъюнкции, конъюнкции и отрицания (булевы операции).

К операциям из Ω_2 относятся операции: композиция, суперпозиция, α-дизъюнкция, α-итерация, цикл, обратная α-итерация, структурообразователь S (α).

Рассмотрим несколько примеров применения аппарата АФС для моделирования ситуаций, возникающей по ходу технологического процесса.

Пример 1. Для правильного выполнения алгоритма, состоящего из последовательно выполняемых четырех операций A_i, необходимо и достаточно правильно выполнить любые три из них. Функциональная сеть, соответствующая этой ситуации, будет иметь вид:

$$= (A_1, A_2, A_3, A_4)\ S\ (\alpha);\ \alpha = \alpha_1, \alpha_2, \alpha_3\ V\ \alpha_1, \alpha_3, \alpha_4\ V\ \alpha_1, \alpha_2, \alpha_4\ V\ \alpha_2, \alpha_3, \alpha_4, \quad (3)$$

где α_i - условие правильного выполнения алгоритма.

Пример 2. Алгоритм B состоит из четырех параллельно выполняемых операций. Он будет считаться начатым, если начаты три из четырех операций (условие на входе).

Функциональная сеть, соответствующая этой ситуации, будет иметь вид:

$$B = [A_1, A_2, A_3, A_4]\ S\ (\alpha).$$

Выражение для α аналогично выражению (3).

Алгоритм B будет считаться правильно выполненным, если хотя бы две любые операции выполнены правильно (условие на выходе). Функциональная сеть будет иметь вид:

$$\alpha = \alpha_1, \alpha_2\ V\ \alpha_1, \alpha_3\ V\ \alpha_1, \alpha_4\ V\ \alpha_2, \alpha_3\ V\ \alpha_2, \alpha_4\ V\ \alpha_3, \alpha_4 \quad (4)$$

Типовые функциональные структуры. Функциональные структуры составляют основу многомерных функциональных сетей. Они используются в двух видах: операторном и логическом [3]. Типовая линейная операторная ФС показана на рис. 1.

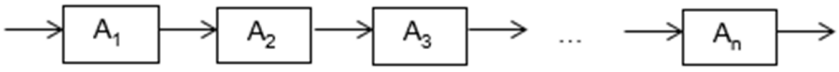


Рис. 1. Линейная операторная ФС.

Типовая альтернативная операторная ФС показана на рис. 2.

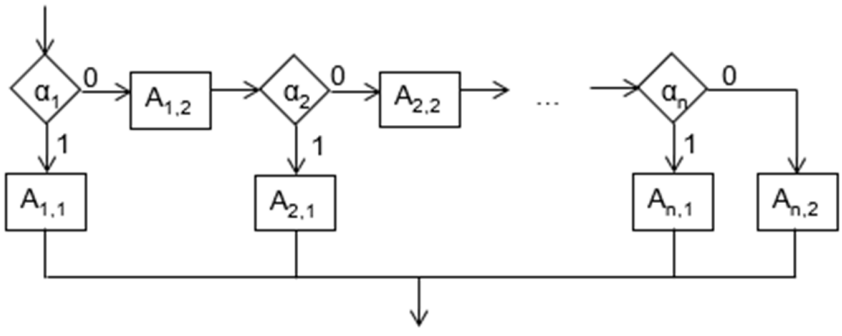


Рис. 2. Альтернативная операторная ФС.

Другие более сложные типовые функциональные структуры рассмотрим на конкретных фрагментах технологического процесса.

Пример 3. Производится однофазная обработка заготовки корпуса датчика давления с выходным контролем качества изготовления. Необходимо изготовить N корпусов из N+n заготовок, где n – число запасных заготовок с

учетом возможного брака. Операторная ФС будет состоять из следующих элементов сети: A – рабочая операция изготовления изделия из заготовки; α – контрольная операция, проверяющая качество изделия с альтернативами

α = 1, если нет дефектов;
0, если дефекты есть;

η_j - циклоформирователь, проверяющий условие равенства изготовленных изделий заданному «j = N» с альтернативами

η_j = 1, если j = N;
0, если j = 0,1,2,…, N – 1;

μ_i - циклоограничитель, проверяющий текущее число израсходованных запасных заготовок с альтернативами

μ_i = 1, если i = 0, 1, 2, …, n – 1;
0, если i= n

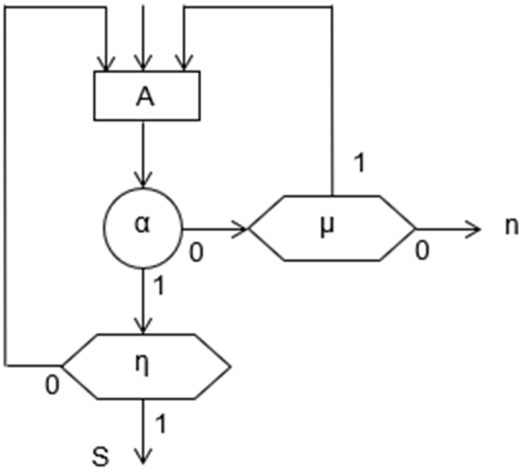


Рис. 3. Операторная ФС.

Фрагмент имеет следующие исходы: S – конец фрагмента с передачей изделий, n – прерывание процесса из-за нехватки запасных заготовок. Число циклов α-итерации является случайной величиной. Число циклов η_j-итерации является детерминированной величиной, ограниченной числом N. При многофазной обработке заготовки ФС будет отличаться от показанной на рис.3 только числом пар Aα, то есть числом рабочих и контрольных операций.

Пример 4. Производится процесс сборки изделия, состоящий из n этапов. При обнаружении дефектных комплектующих изделий (КИ) они заменяются из числа запасных. Сборка производится из разнотипных КИ. Многоитеративная операторная ФС показана на рис. 4.

A_i и α_l – рабочая и контрольная операции на l-м этапе сборки, требующем КИ l-го типа (l=1-n) с альтернативами:

α_i = 1 – операция выполнена правильно;
0– операция выполнена неправильно;

Циклоограничитель μ_i проверяет условие «$i<n_l$», i_l (n_l) – число израсходованных запасных КИ l-го типа, с альтернативами :

μ_i = 1, если i_l = 1, 2, …, n_i – 1;
0, если $i_l = n_i$.

Циклоформирователь η_j проверяет условие «j = N», j(N) – текущее число собранных изделий; с альтернативами:

η_j = 1, если j = N;
0, если $j \neq$ N, где N число требуемых изделий.

Технологический процесс как объект моделирования. В целом технический процесс (ТП) как объект моделирования многомерными функциональными сетями можно представить в виде следующей формулы [3]:

$$ТП=<X, H, S, Y>, \quad (5)$$

где: X, H, S – множество предметов, субъектов и орудий труда; Y – продукт труда. В производственном процессе осуществляется преобразование X в Y с помощью H и S.

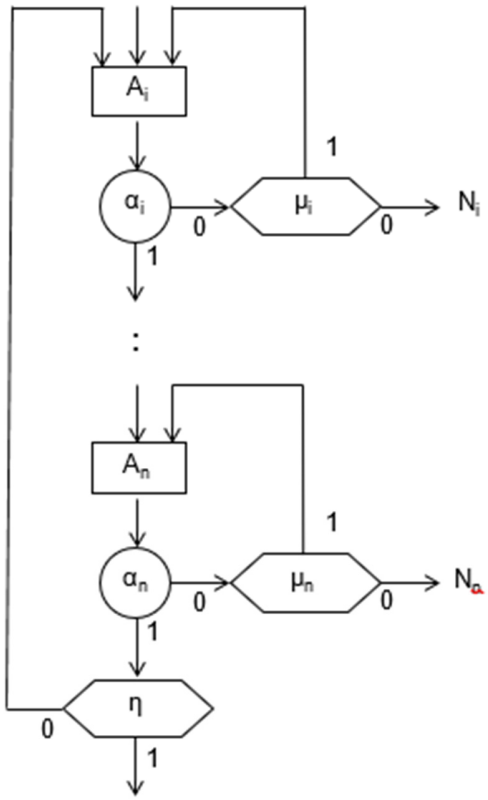


Рис. 4. Многоитеративная ФС.

Одним из базовых принципов функциональной сети является принцип модульности, позволяющий представить ТП в виде совокупности вложенных друг в друга сетей разного размера.

Для предприятия функциональную сеть можно представить в виде сетей рабочих мест, участков, цехов и завода в целом. Это же относится и к продукту труда – системам управления. В динамике (с учетом процесса функционирования F) формула (5) будет иметь вид:

$$F=HVS \longrightarrow X \longrightarrow Y \tag{6}$$

Технологический процесс в виде ориентированного графа как методический пример показан на рис. 5.

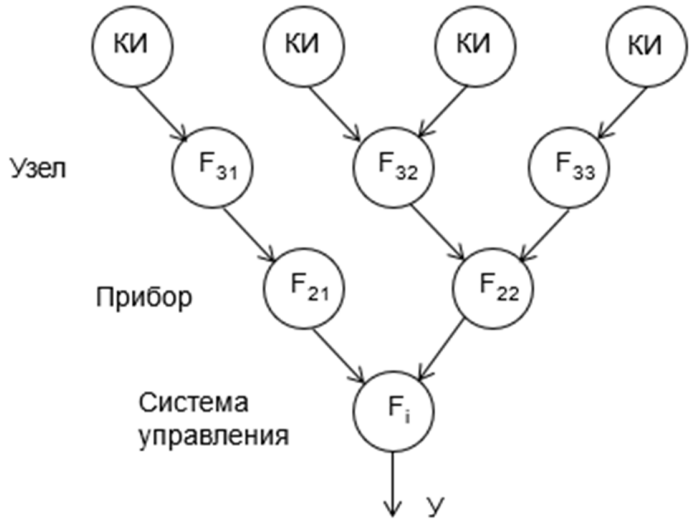


Рис. 5. ТП в виде графа.

Каждый узел графа является частью производственного процесса, соответствующей изготовлению элементов (части) продукта труда – системы управления (СУ).

Дуги-стрелки – это результаты процессов, происходящих в узлах, из которых выходят стрелки. Корневая (выходная) стрелка – итоговый продукт труда. Реальный технологический процесс имеет более сложный вид.

Заключение. Практика производства корабельных систем управления показывает, что и конечный продукт, и компоненты конечного продукта могут иметь дефекты различных типов. Поэтому математический аппарат моделирования технологического процесса должен учитывать это обстоятельство и иметь возможность одновременного их описания. В этом заключается принципиальное отличие многомерных функциональных сетей от известных моделей алгоритмических процессов [5], в которых оценка ведется на основе бинарного принципа «да - нет».

Наиболее распространенной мерой качества любого продукта труда, удобной для измерения, является количество дефектов, т.е. несоответствие изделий заранее установленным требованиям. Необходимо различать понятия «дефект» и «ошибка». Применительно к технологическому процессу ошибка – это неправильное выполнение специалистом или техникой технологической операции (фрагмента процесса, работы, действия).

Дефект – это следствие ошибки, выражающиеся в нарушении требуемых характеристик продукта труда на любом этапе его изготовления.

Вклад ошибок специалистов в уровень бездефектности выпускаемой продукции особенно значителен для слабо автоматизированных производств. В этом смысле создание универсальных автоматизированных рабочих мест на производстве может существенно повысить уровень бездефектности выпускаемой продукции.

СПИСОК ЛИТЕРАТУРЫ

1. Кобзев В.В., Дарминова М.М. Об оценке надежности технологических процессов. //Надежность и контроль качества, 1978, № 8. с. 26-32.
2. Глушков В.М., Цейтлин Г.Е., Ющенко Е.Л. Алгебра. Языки. Программирование. – Киев.: Наукова думка, 1980. – 320 с.
3. Ротштейн А.П., Кузнецов П.Д. Проектирование бездефектных человеко-машинных технологий. – Киев.: Техника, 1992. – 180 с.
4. Кобзев В.В., Шилов К.Ю. Методы создания технических средств обучения корабельных операторов. – СПб: Наука, 2005. – 156 с.
5. Сафонов И.В. О формализованном надежностном анализе алгоритмических процессов. //Управляющие системы и машины. – 1973. - № 3. – с. 92-95.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СОЦИОКОМПЬЮТИНГЕ

УДК 004.8

ПОДХОДЫ ПО ПРИМЕНЕНИЮ АЛГЕБРАИЧЕСКИХ БАЙЕСОВСКИХ СЕТЕЙ К ОТКРЫТЫМ ИСТОЧНИКАМ ИНФОРМАЦИОННЫХ СИСТЕМ В РАМКАХ АНАЛИЗА ЗАЩИЩЕННОСТИ ПОЛЬЗОВАТЕЛЯ ОТ СОЦИОИНЖЕНЕРНЫХ АТАК

Бушмелев Федор Витальевич[1, 2], Харитонов Никита Алексеевич[1]
[1] Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
[2] Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: fvb@dscs.pro, nak@dscs.pro

Аннотация. В работе изучается вопрос применения алгебраических байесовских сетей, являющихся представителями вероятностных графических моделей, для получения вероятности успеха социоинженерной атаки на пользователя информационной системы в рамках корпоративного моделирования на основе данных, получаемых из открытых источников, например, социальных медиа.

Ключевые слова: социоинженерные атаки; вероятностные графические модели; алгебраические байесовские сети; информационная безопасность; социальные медиа.

APPROACHES TO THE APPLICATION OF ALGEBRAIC BAYESIAN NETWORKS TO OPEN-SOURCE INFORMATION SYSTEMS IN THE ANALYSIS OF USER SECURITY AGAINST SOCIAL ENGINEERING ATTACKS

Bushmelev Fedor[1, 2], Kharitonov Nikita[1]
[1] Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
[2] Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: fvb@dscs.pro, nak@dscs.pro

Abstract. This paper explores the application of algebraic Bayesian networks, which are representatives of probabilistic graphical models, to obtain the probability of success of a social engineering attack on an information system user in the framework of corporate modeling based on data obtained from open sources, for example, social media.

Keywords: social engineering attack; probabilistic graphical networks; algebraic Bayesian networks; information security; social media.

Введение. Сегодня жизнь современного человека неразрывна связана с информационными технологиями [2]. Вместе с тем, сложившаяся в последнее время эпидемиологическая обстановка обусловила активную цифровизацию общества и задала направление развития почти каждой отрасли на ближайшие годы [11]. Подобное стремительное и глубокое вовлечение рядового пользователя в цифровое пространство позволило вывести, например, сферу услуг на качественно новый уровень. В целом увеличилось количество генерируемого и поглощаемого цифрового контента [2], но также, это повлекло за собой появление множества новых узких мест и уязвимостей, затрагивающих вопросы соблюдения существующих правил и политик информационной безопасности [3, 5, 7, 8]. Стоит отметить, что еще до массового перехода в цифровое окружение, уже существовали технологии, обеспечивающие необходимый уровень безопасности передачи конфиденциальных данных и удаленного доступа. Повседневная жизнь в условиях пандемии показала, что одним из основных уязвимых мест информационных является пользователь [3, 5-8]. Тем самым выводя задачу по повышению защищенности пользователя и опосредованно информационных систем от социоинженерных атак [6].

Зачастую социальные инженеры при подготовке атаки и начальных этапах проведения атакующего воздействия на пользователя используют открытые, общедоступные данные, например, контактную информацию об организации и цифровые следы, оставляемые ее сотрудниками [3, 6]. Последние в свою очередь могут содержать

в себе ряд маркеров, отвечающих за ту или иную психологическую особенность пользователя и показывающих их выраженность [4, 6]. Давайте представим, что мы уже располагаем неким аппаратом, который может определить в публикуемом контенте необходимые маркеты и выдать вероятностную оценку того, что злоумышленник сможет воспользоваться эмпирически извлеченной информацией из данного контента и успешно провести социоинженерную атаку [1, 4, 6]. А теперь представим, что рассматривается не одну какую-то публикацию, а несколько и для них всех строим оценки. На следующем шаге усложним систему и представим, что пользователей теперь не один, а несколько. В данном представлении также может появиться новая информация, уже о связях между пользователями, притом они может быть зафиксирована в тех же цифровых следах, и она также будет влиять на вероятность совершения успешного социоинженерного воздействия. Подобным несложным представлением может быть получена даже сложная, состоящая из большого количества неоднородных данных, с пропусками и неточностями, вероятностная структура целой компании. В связи с чем, решение задачи по получению вероятностной оценки степени защищенности конкретного пользователя с некоторым набором открытых данных в рамках представленной структуры компании может потребовать значительных вычислительных мощностей и временных ресурсов. Необходимо совершенствование существующих методов хранения и обработки информации. Одним из классов таких методов являются вероятностные графические модели, в которых в виде графа представлены зависимости между случайными величинами; частным примером подобных систем являются алгебраические байесовские сети.

В работе изучается вопрос применения алгебраических байесовских сетей, являющихся представителями вероятностных графических моделей, для получения вероятности успеха социоинженерной атаки в рамках ее симуляции.

Целью работы является получение представления о применении алгебраических байесовских сетей в описываемом контексте для проведения дальнейших исследований на реальных данных.

Алгебраические байесовские сети представляют собой набор фрагментов знаний, каждый из которых представим в виде идеала конъюнктов, дизъюнктов или набора квантов квантов, при этом каждому элементу фрагмента знаний сопоставляется интервальная или скалярная оценка вероятности его истинности. При этом представление сети унифицировано, например, все фрагменты знаний представлены в виде идеала конъюнктов со скалярными оценками вероятности их истинности [9, 10]. Алгебраические байесовские сети позволяют как получать вероятности события на основе имеющихся в сети вероятностей (априорный вывод), так и обновлять вероятности на основе поступивших свидетельств (апостериорный вывод) [9, 10].

Рассмотрим применение предлагаемого подхода на примере упрощенной модели социоинженерной атаки, разворачивающейся в корпоративной среде, и рассчитаем вероятность того, что злоумышленник успешно проведёт необходимые атакующие воздействия на сотрудников с последующим приобретением прав допуска к интересующему его критичному документу. Не умаляя общности на рис.1 представлен социальный граф взаимодействия двух сотрудников *П1* и *П2*, где *П2* имеет доступ к критичному документу. Будем считать, что социальный инженер желает заполучить данные, которыми обладает *П2,* но обратиться напрямую пока он к нему не может. При этом он взаимодействовать только с *П1.* Рассмотрим ситуация, когда злоумышленник пытается добраться к критичному документу и начинает действовать с *П1*. После успешной атаки на *П1* происходит переход злоумышленника от *П1* к *П2* и последующее воздействие на *П2.*

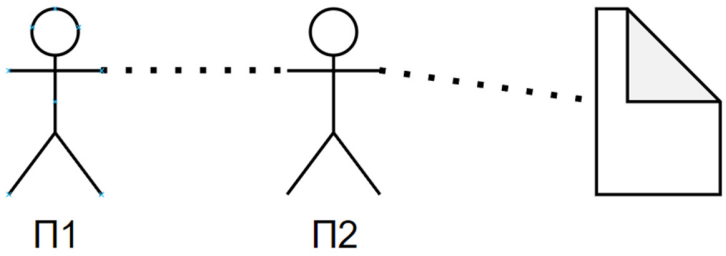


Рис. 1. Упрощенная модель социального графа.

Опишем множество событий для нашей смоделированной ситуации в вероятностном пространстве. Пусть:

x1 – вероятность того, что социоинженерная атака на *П1* пройдет успешно;

x2 – вероятность того, что социоинженерная атака на *П2* пройдет успешно;

x3 – вероятность того, что произойдет переход атаки, например, что *П2* отреагирует на просьбу *П1* «помочь» нашему злоумышленнику.

Тогда: P(успешная_атака) = $x1 \,\&\, x3 \mid x2$;

А возможные алгебраические байесовские сети, задающие данную вероятность, могут представлены на рис.2.

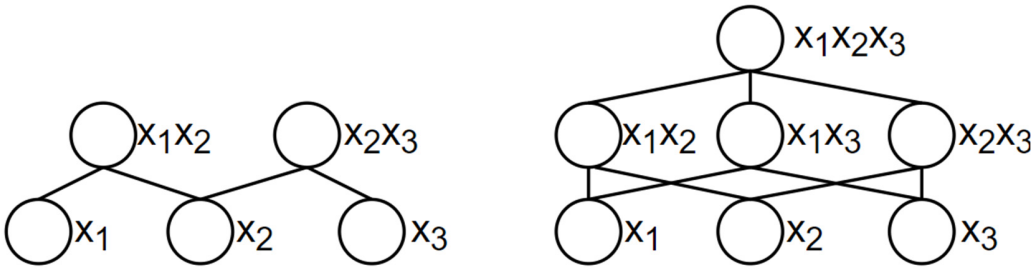


Рис. 2. Возможные фрагменты знаний, описывающие вероятность проведения смоделированной социоинженерной атаки.

В рамках поставленной цели был смоделирован контекст социоинженерной атаки. Были сформулированы предположения о вероятностях доступа сотрудников к критическим документам и вероятностях успешного воздействия социоинженерной атаки на каждого из сотрудников. На основе представленных данных была построена алгебраическая байесовская сеть, на основе которой в рамках априорного вывода была рассчитана вероятность успеха моделируемой социоинженерной атаки.

Теоретическая и практическая значимость представленной работы заключается в том, что описанный в ней подход позволяет перейти к построению алгебраических байесовских сетей для анализа защищенности информационной системы от социоинженерных атак, основываясь на реальных данных. Вместе с тем формируя научный задел для дальнейших исследований в областях алгебраических байесовских сетей и анализа защищенности пользователей от социоинженерных атак.

Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН № 0073-2019-0003, при финансовой поддержке РФФИ проект №20-07-00839; поддержана Санкт-Петербургским государственным университетом, проект № 73555239.

СПИСОК ЛИТЕРАТУРЫ

1. Bushmelev F.V., Abramov M.V., Tulupyeva T.V. Adaptive Method of Color Selection in Application to Social Media Images // 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)», 2020. P. 252-257.
2. Digital 2021 report // WeAreSocial [Электронный ресурс]. URL: https://wearesocial.com/digital-2021 (дата обращения: 01.10.2021).
3. 2021 Data Breach Investigations Report // Verizon [Электронный ресурс]. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата обращения: 01.10.2021).
4. Oliseenko V.D., Tulupyeva T.V., Abramov M.V. (2022) Online Social Network Post Classification: A Multiclass approach. // Proceedings of the Fifth International Scientific Conference «Intelligent Information Technologies for Industry» (IITI'21). IITI 2021. Lecture Notes in Networks and Systems, vol 330. Springer, Cham. DOI:10.1007/978-3-030-87178-9_21
5. Zhernova K., Chechulin A. 2022. Overview of Vulnerabilities of Decision Support Interfaces Based on Virtual and Augmented Reality Technologies. Lecture Notes in Networks and Systems. Vol. 330 LNNS. DOI:10.1007/978-3-030-87178-9_40
6. Абрамов М.В., Тулупьева Т.В., Тулупьев А.Л. Социоинженерные атаки: социальные сети и оценки защищенности пользователей. СПб.: ГУАП, 2018. 266 с.
7. Объем украденных у россиян мошенниками средств вырос почти на 40% // Ведомости [Электронный ресурс]. URL: https://www.vedomosti.ru/finance/news/2021/09/02/884870-obem-ukradennih-u-rossiyan-sredstv-viros (дата обращения: 01.10.2021).
8. Сбербанк описал схему работы типичного мошеннического колл-центра // РИА новости [Электронный ресурс]. URL: https://ria.ru/20210601/sberbank-1735112983.html/ (дата обращения: 01.10.2021).
9. Тулупьев А.Л., Николенко С.И., Сироткин А.В. Байесовские сети: логико-вероятностный подход. — СПб.: Наука, 2006. 607 с.
10. Тулупьев А.Л., Сироткин А.В., Николенко С.И. Байесовские сети доверия: логико-вероятностный вывод в ациклических направленных графах. — СПб.: Изд-во С.-Петерб. ун-та, 2009.
11. Чернышенко Д.Н. Дмитрий Чернышенко: По поручению Президента регионы России утвердили стратегии цифровой трансформации // Правительство России. Новости. [Электронный ресурс]. URL: http://government.ru/news/43149/ (дата обращения: 01.10.2021).

УДК 004.8

ПРОВЕРКА НЕПРОТИВОРЕЧИВОСТИ АЛЬТЕРНАТИВНЫХ МОДЕЛЕЙ ФРАГМЕНТОВ ЗНАНИЙ С НЕОПРЕДЕЛЕННОСТЬЮ

Владимирова Элина Вячеславовна[1], Стельмах Татьяна Дмитриевна[1], Ельцов Данил Андреевич[1], Вяткин Артём Андреевич[1], Абрамов Максим Викторович[2], Тулупьев Александр Львович[2]

[1] Санкт-Петербургский государственный университет
Университетский пр., 28, Старый Петергоф, Санкт-Петербург, 198504, Россия

[2] Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия

Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия

e-mails: alivolf@icloud.com, tanya252002@gmail.com, sthfaceless@gmail.com, vyatkin.artex@gmail.com, mva@dscs.pro, alt@dscs.pro

Аннотация. Статья посвящена разработке инструмента для проверки и поддержания непротиворечивости альтернативных математических моделей фрагментов знаний в теории алгебраических байесовских сетей с возможностью дальнейшего расширения функционала.

Ключевые слова: машинное обучение; вероятностные графические модели; байесовские сети; алгебраические байесовские сети; фрагмент знаний; непротиворечивость.

CHECKING THE CONSISTENCY OF ALTERNATIVE MODELS OF KNOWLEDGE PATTERNS WITH UNCERTAINTY

Vladimirova Elina[1], Stelmakh Tatiana[1], Danil Eltsov[1], Vyatkin Artyom[1], Abramov Maxim[2], Tulupev Aleksander[2]

[1] Saint Petersburg State University

28 Universitetskiy Av, Stary Peterhof, St. Petersburg, 198504, Russia

[2] Saint Petersburg State University

7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia

St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)

39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia

e-mails: alivolf@icloud.com, tanya252002@gmail.com, sthfaceless@gmail.com, vyatkin.artex@gmail.com, mva@dscs.pro, alt@dscs.pro

Abstract. The article is devoted to the development of a tool for checking and maintaining the consistency of alternative mathematical models of knowledge patterns in the theory of algebraic Bayesian networks with the possibility of further expanding the functionality.

Keywords: machine learning; probabilistic graphical models; Bayesian networks; algebraic Bayesian networks; knowledge pattern; consistency.

Введение. В процессе принятия решений мы часто опираемся на накопленный опыт — знания, которые можно представить в виде модели системы утверждений. В качестве элементов этой системы в указанной модели могут выступать фрагменты знаний (ФЗ). Их совокупности могут быть объединены как четко определенными логическими связями, так и заметно менее жесткими, стохастическими, зависимостями. Для анализа данных с учетом их корреляции между собой можно обратиться к вероятностным графическим моделям (ВГМ) [1], работающим с математическими моделями ФЗ — утверждениями с приписанными им вероятностными скалярными или интервальными оценками [4]. Теория ВГМ принадлежит к областям искусственного интеллекта, дающим возможность связать понятия данных, вероятностной логики и теории графов, и рассматривает такие имеющие широкую область применения модели как марковские цепи и байесовские сети доверия, родственные алгебраическим байесовским сетям (АБС).

ВГМ активно применяются в различных системах машинного обучения и искусственного интеллекта для распознавания образов [5], оценивания и мониторинга состояния здоровья [6], моделирования отклика экологических систем на различные воздействия внешних факторов [7] и т.д. [8] Подклассом ВГМ являются алгебраические байесовские сети — математическая модель стохастической системы утверждений, позволяющая характеризовать вероятность истинности утверждения как степень уверенности в нём. Математической моделью фрагментов знаний в теории АБС выступает идеал конъюнктов с оценками вероятности их истинности — эти оценки могут быть как скалярными, так и интервальными. В работе рассматриваются также альтернативные модели фрагментов знаний: идеал дизъюнктов и кванты.

Преобладание в большом объёме информации неполных или не вызывающих абсолютного доверия данных приводит к необходимости рассматривать вероятности истинности составляющих их высказываний. Ввиду неточности сведений такие вероятности часто имеют интервальные значения. Все это накладывает ограничения на получаемые на вход данные: ФЗ должны удовлетворять определенным свойствам как из теории вероятностей, так и из теории алгебраических байесовских сетей, т.е. быть непротиворечивыми. Таким образом, необходим удобный инструмент, позволяющий быстро определять непротиворечивость фрагментов знаний.

Проверка непротиворечивости во фрагменте знаний. В классическом представлении ФЗ строятся над идеалом конъюнктов, однако в настоящее время активно развивается теоретический аппарат АБС над их альтернативными моделями — этой теме посвящен ряд исследований [2-4, 9-10]. Примерами таких моделей являются идеал дизъюнктов и набор квантов, проверка непротиворечивости которых и поставлена целью данной работы.

На множествах дизъюнктов и квантов удобно ввести перенумерацию, которая позволит работать с ними как с векторами, содержащими в своих компонентах вероятности истинности соответствующих пропозициональных формул. Основа для алгоритма проверки непротиворечивости фрагментов знаний в теории АБС вытекает из требований аксиоматики вероятностной логики. Изначально устанавливается пара ограничений на кванты – условие

«нормировки» и «неотрицательности». Далее с использованием результатов из вероятностной логики путем применения матрично-векторных преобразований можно получить ограничение на вероятности истинности дизъюнктов. Последнее будет представлять из себя покомпонентное неравенство, сравнивающее произведение матрицы и вектора вероятностей истинности дизъюнктов с вектором, почти всеми компонентами которого являются нули, за исключением одной единицы. Далее действия по проверке непротиворечивости зависят от типа оценок – являются ли данные скалярными или интервальными. В случае скалярных оценок достаточно проверить вышеописанные условия, для интервальных же потребуется решение задачи линейного программирования, покомпонентно находящее минимумы и максимумы соответствующих пропозициональных формул. Решение задачи линейного программирования также позволит согласовывать оценки вероятности истинности.

В ходе проекта была разработана и опубликована библиотека на языке программирования Python, которая может быть установлена из открытого репозитория Python пакетов - PyPi. На вход библиотеке подается набор скалярных оценок на элементы идеала дизъюнктов или множества квантов, на выходе пользователь получает результат проверки на непротиворечивость фрагмента знаний, а также скорректированные оценки в случае его непротиворечивости. К реализованной библиотеке был создан REST API, предоставляющий доступ с помощью HTTP запросов из других языков программирования. Для удобства использования библиотеки в прикладных задачах был также создан интуитивно понятный браузерный клиент, адаптированный под различные платформы. На рис. 1 представлен веб-интерфейс библиотеки.

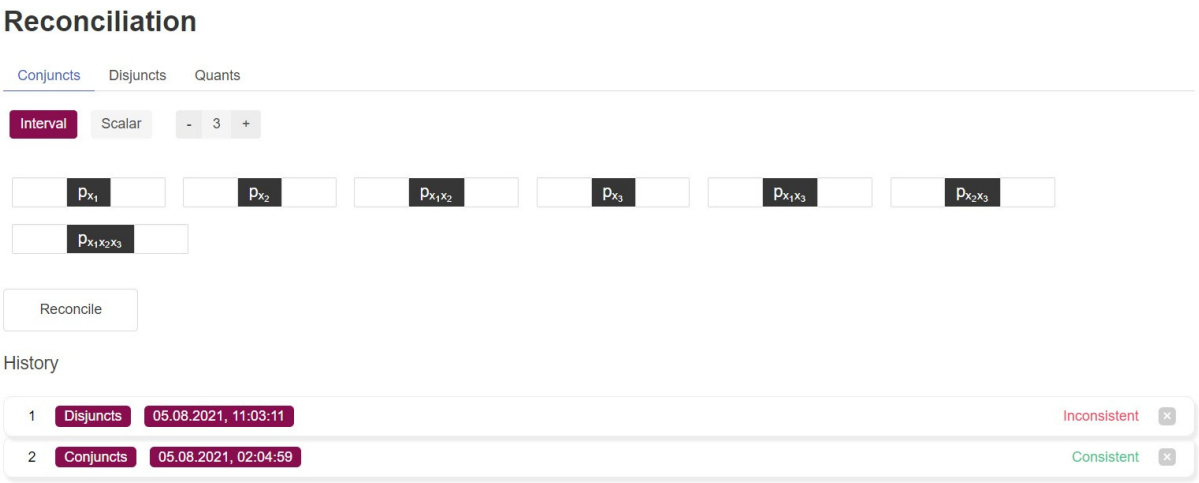


Рис. 1. Браузерный клиент.

Заключение. Полученная работа при дальнейших улучшениях может найти свое практическое применение с целью моделирования социоинженерных атак [11-12]. На текущий момент функционал библиотеки состоит в проверке непротиворечивости трёх моделей фрагментов знаний: конъюнктов, квантов и дизъюнктов, а также в согласовании интервальных оценок, если это допустимо. Перспективами работы являются как расширение функционала в сторону априорного и апостериорного вывода, так и дальнейшее исследование алгебраических байесовских сетей с последующей имплементацией прикладных аспектов.

Благодарности. Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН № 0073-2019-0003, при финансовой поддержке РФФИ проект №20-07-00839; поддержана Санкт-Петербургским государственным университетом, проект № 73555239.

СПИСОК ЛИТЕРАТУРЫ

1. Тулупьев А.Л., Сироткин А.В., and Николенко С.И. Байесовские сети доверия: логико-вероятностный вывод в ациклических направленных графах. СПб.: Изд-во Санкт-Петербургского унта, 2009.
2. Золотин А.А., Тулупьев А.Л., and Сироткин А.В. Матрично-векторные алгоритмы локального апостериорного вывода в алгебраических байесовских сетях над пропозициями-квантами. Научно-технический вестник информационных технологий, механики и оптики, 15(4), 2015.
3. Тулупьев А.Л. Ациклические алгебраические байесовские сети: логико-вероятностный вывод. Нечеткие системы и мягкие вычисления: Научный журнал Российской ассоциации нечетких систем и мягких вычислений, 1(1):57–93, 2006.
4. Тулупьев А.Л. Алгебраические байесовские сети: логико-вероятностная графическая модель баз фрагментов знаний с неопределенностью. Учреждение Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН, 2009.
5. Peng P., Tian Y., Wang Y., Li J., and Huang T.. Robust multiple cameras pedestrian detection with multi-view bayesian network. Pattern Recognition, 48(5):1760–1772, 2015.

6. Arangio S. and Bontempi F. Structural health monitoring of a cable-stayed bridge with bayesian neural networks. Structure and Infrastructure Engineering, 11(4):575–587, 2015.
7. Hamilton S., Pollino C., and Jakeman A. Habitat suitability modelling of rare species using bayesian networks: Model evaluation under limited data. Ecological Modelling, 299:64–78, 2015.
8. Фильченков А.А., Бирилло А. И., Тулупьев А. Л. Алгебраические байесовские сети: представление данных, алгоритмы обработки и реинжиниринг комплекса программ (проектная работа): диплом. работа. Санкт-Петербург. гос. университет, Санкт-Петербург, 2017.
9. Тулупьев А.Л., Николенко С.И., and Сироткин А.В. Байесовские сети: логико-вероятностный подход, 2006.
10. Тулупьев А.Л., Сироткин А.В., and Золотин А.А. Матричные уравнения нормирующих множителей в локальном апостериорном выводе оценок истинности в алгебраических байесовских сетях. Вестник Санкт-Петербургского университета. Серия 1. Математика. Механика. Астрономия, 2(3), 2015.
11. Khlobystova A. O., Abramov M. V., Tulupyev A.L., Zolotin A.A. Search for the shortest trajectory of a social engeneering attack between a pair of users in a graph with transition probabilities//Informatsionno-Upravliaiushchie Sistemy Volume 2018, Issue 6, Pages 74 - 81, 2018.
12. 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// CEUR Workshop ProceedingsVolume 2782, Pages 264 - 268, 2020 Russian Advances in Fuzzy Systems and Soft Computing: Selected Contributions to the 8th International Conference on «Fuzzy Systems, Soft Soft Computing and Intelligent Technologies», FSSCIT 2020, Smolensk, 29 June 2020 through 1 July 2020.

УДК 004.4

РАЗРАБОТКА ПРОГРАММНОГО ОБЕПЕЧЕНИЯ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ РАСЧЕТА АППАРАТОВ ХИМИЧЕСКОЙ ТЕХНОЛОГИИ

Арипова Ольга Владимировна[1], Кузьмин Алексей Михайлович[1,2], Гашевский Егор Михайлович[1], Ценева София Николаевна[1]

Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
1-я Красноармейская ул., 1, Санкт-Петербург, 198000, Россия
ООО «Генератор синтез-газа» ул. Ольги Форш д.15 к.1, Санкт-Петербург, 195297, России
e-mails: aripova_ov@voenmeh.ru, gashevskii_em@voenmeh.ru, tseneva_sn@voenmeh.ru, kuzmin.lex@gmail.com

Аннотация. В статье рассматриваются вопросы разработки программного обеспечения автоматизированной информационной системы расчета аппаратов химической технологии для организации эффективного взаимодействия «пользователь – информационная система».

Ключевые слова: программное обеспечение; информационная система; пользователь; эффективность; газогенератор синтез-газа.

DEVELOPMENT OF SOFTWARE FOR AN AUTOMATED INFORMATION SYSTEM FOR CALCULATING CHEMICAL TECHNOLOGY DEVICES

Aripova Olga Vladimirovna[1], Kuzmin Alexey Mikhailovich[1,2], Gashevsky Egor Mikhailovich[1], Tseneva Sofia Nikolaevna[1]

Baltic State Technical University «VOENMEH» by D.F. Ustinov
1st Krasnoarmeyskaya st., 1, St. Petersburg, 198000, Russia
LLC «GSG»
15/1. O. Forsh, st, St. Petersburg, 195297, Russia
e-mails: aripova_ov@voenmeh.ru, gashevskii_em@voenmeh.ru, tseneva_sn@voenmeh.ru, kuzmin.lex@gmail.com

Abstract. The article discusses the issues of software development of an automated information system for calculating chemical technology devices for the organization of effective interaction «user - information system».

Keywords: software; information system; user; efficiency; syngas generator.

В настоящее время большинство автоматизированных информационных систем (АИС) содержат в себе большой объем специальной информации, для них необходимо правильно организовать управление потоками информации, как запрашиваемыми пользователями системы, так и ответными реакциями самой системы на эти запросы. Таким образом, возникает задача разработки такой системы «пользователь-АИС», которая позволит организовать эффективное взаимодействие пользователя и АИС с помощью программного обеспечения на основе личностно-ориентированного подхода [1].

Дадим основные понятия и определения, которые в дальнейшем будем использовать в процессе разработки системы «пользователь-АИС». Автоматизированная система – это система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций. Пользователь – это лицо, участвующее в функционировании автоматизированной системы или использующее результаты ее функционирования. Компоненты системы: информационное, организационное, методическое, математическое, техническое, программное обеспечения [2].

Информация, появляющаяся при использовании данных в процессе решения конкретных задач с формированием нового личного знания субъекта, позволяет рассмотреть еще один вид АИС – личностно-ориентированных,

разрабатываемых как автоматизированные системы обработки информации для пользователя, задачи которого наперед неизвестны или достаточно широки, чтобы их можно было свести к какому-либо ограниченному набору информации и способов ее обработки, призванная повысить успешность поиска необходимой информации [1].

Жизненный цикл АИС – совокупность взаимосвязанных процессов создания и последовательного изменения состояния системы от формирования исходных требований к ней до окончания эксплуатации и утилизации комплекса средств автоматизации [2].

В соответствии с [3] схема классификации разработки программного обеспечения (ПО) состоит из 16 видов, которые в рамках решения поставленной задачи можно объединить в следующие группы:

1. Внутренние виды: функциональные возможности, требуемые рабочие характеристики, исходный язык, требование защиты, требование надежности, стабильность, масштаб, функция, режим эксплуатации.
2. Виды среды: прикладная область АИС, вычислительная система и среда, класс пользователя, требование к вычислительным ресурсам, критичность, готовность программного продукта.
3. Виды данных: представление и использование программных данных.

Разработку программного обеспечения для АИС разобьем на следующие основные этапы: определение требований; проектирование; программирование; тестирование; отладка; разработка документации; эксплуатация и сопровождение [4].

Эффективность АИС – свойство, характеризуемое степенью достижения целей, поставленных при ее создании. Показатель эффективности – мера или характеристика для оценки эффективности АИС [2].

В настоящее время АИС широко применяются в различных областях науки и техники: в медицине, атомной промышленности, машиностроении, кораблестроении, на нефтеперерабатывающих производствах и т.д.

Однако сложность разработки АИС заключается в отсутствии универсального программного обеспечения, которое позволило бы оперировать с данными различного характера.

Для реализации АИС рассматривались математические пакеты:

– *Mathcad* – система компьютерной математики, сочетающая в себе удобный редактор текста и формул, численный и символьный процессоры;

– *Maple* – математический пакет, предназначенный для символьных вычислений, имеющий: ряд средств для численного решения дифференциальных уравнений и нахождения интегралов, и графический интерфейс;

– *Scilab* – пакет прикладных математических программ, предоставляющих открытое окружение для инженерных (технических) и научных расчётов, является альтернативой *Matlab*;

– *Matlab* – пакет прикладных программ для решения задач технических вычислений и одноимённый язык программирования, используемый в этом пакете, является главным инструментом для решения широкого спектра научных и прикладных задач, в таких областях как: моделирование объектов и разработка систем управления, проектирование коммуникационных систем, обработка сигналов и изображений, измерение сигналов и тестирование, финансовое моделирование, вычислительная биология и другие.

В результате этого исследования для реализации АИС «Газогенератор синтез-газа», позволяющей произвести расчёт условной формулы исходных компонентов и геометрических параметров узлов газогенератора синтез-газа (ГСГ): смесительной головки, камеры сгорания, узла впрыска и испарительной камеры [5], используется интерактивная среда программирования численных расчётов с визуализацией результатов с помощью *GUIDE MATLAB*. *GUIDE* – это приложение в составе пакета прикладных программ *MATLAB* для решения задач технического вычисления и создания надёжного и удобного программного обеспечения с графическим интерфейсом пользователя.

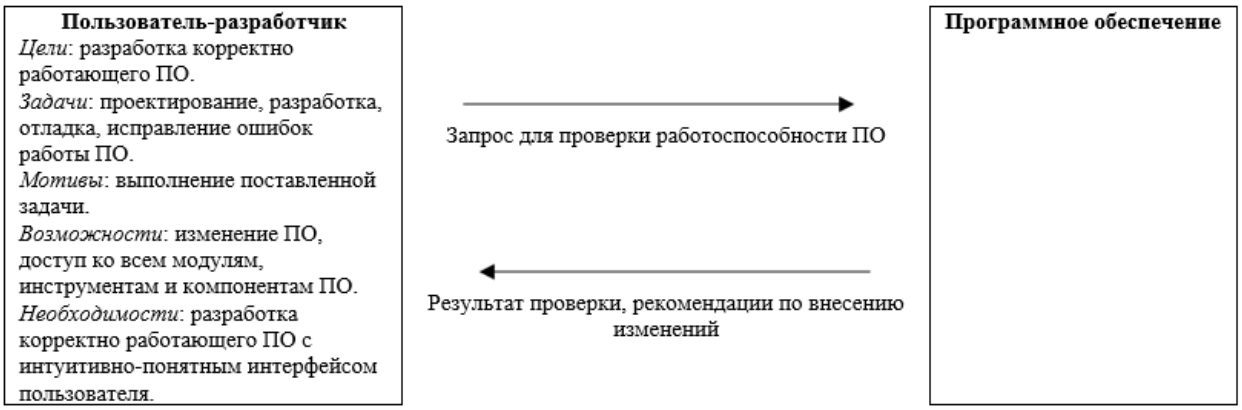


Рисунок 1 – Модель взаимодействия пользователя-разработчика с программным обеспечением

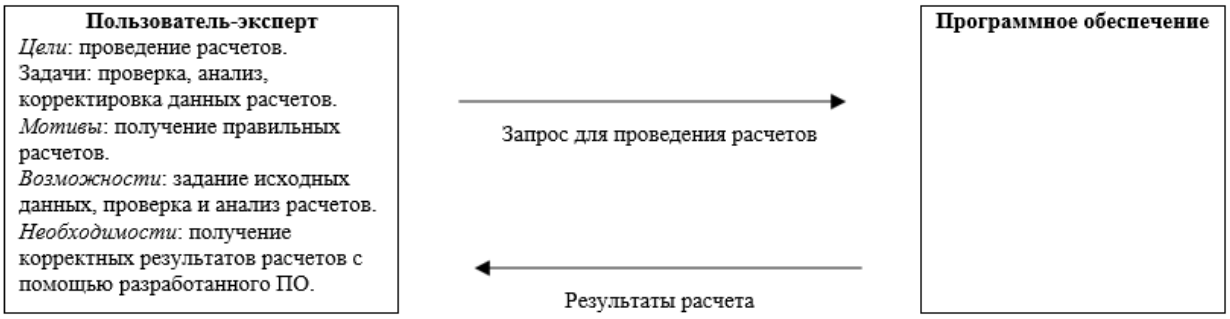


Рисунок 2 – Модель взаимодействия пользователя эксперта с программным обеспечением

С учётом модели взаимодействия пользователя с программным обеспечением АИС «Газогенератор синтез-газа» [2] следует отметить, что с ПО взаимодействует три вида пользователей: пользователь-разработчик, пользователь-эксперт и пользователь-пользователь. Целью пользователя-разработчика (рис. 1) является создание корректно работающего программного обеспечения с удобным пользовательским интерфейсом. Для пользователя-эксперта (рис. 2) важным в программном обеспечении является правильность выполняемых расчётов и получения корректных результатов. Пользователь-пользователь является конечным пользователем и при обращении к программному обеспечению руководствуется желанием при минимальных затратах (временных, трудовых и т.д.) получить результаты расчётов для дальнейшего их применения.

В настоящее время программное обеспечение находится на этапах проектирования, разработки и отладки, поэтому с программным обеспечением взаимодействуют только два вида пользователей: пользователь-эксперт и пользователь разработчик (программист и администратор). При этом оба пользователя между собой взаимодействуют при помощи программного обеспечения: так пользователь-эксперт обращается к программному обеспечению для проверки и анализа полученных в результате расчётов данных, и, при наличии ошибок, сообщает пользователю-разработчику о необходимости внесения изменений, а пользователь-разработчик, в свою очередь, внося изменения в программное обеспечение, передаёт пользователю-эксперту данные на проверку.

Взаимодействие пользователей с программным обеспечением осуществляется при помощи форм ввода исходных данных, форм ввода дополнительных данных, а также корректирующих форм, позволяющих пользователю при необходимости уточнять результаты расчёта (рис. 3-4). В программном обеспечении для пользователей предусмотрены подсказки и проверки введённых данных, по результатам которых расчёт может быть продолжен или приостановлен для повторного запроса данных [6].

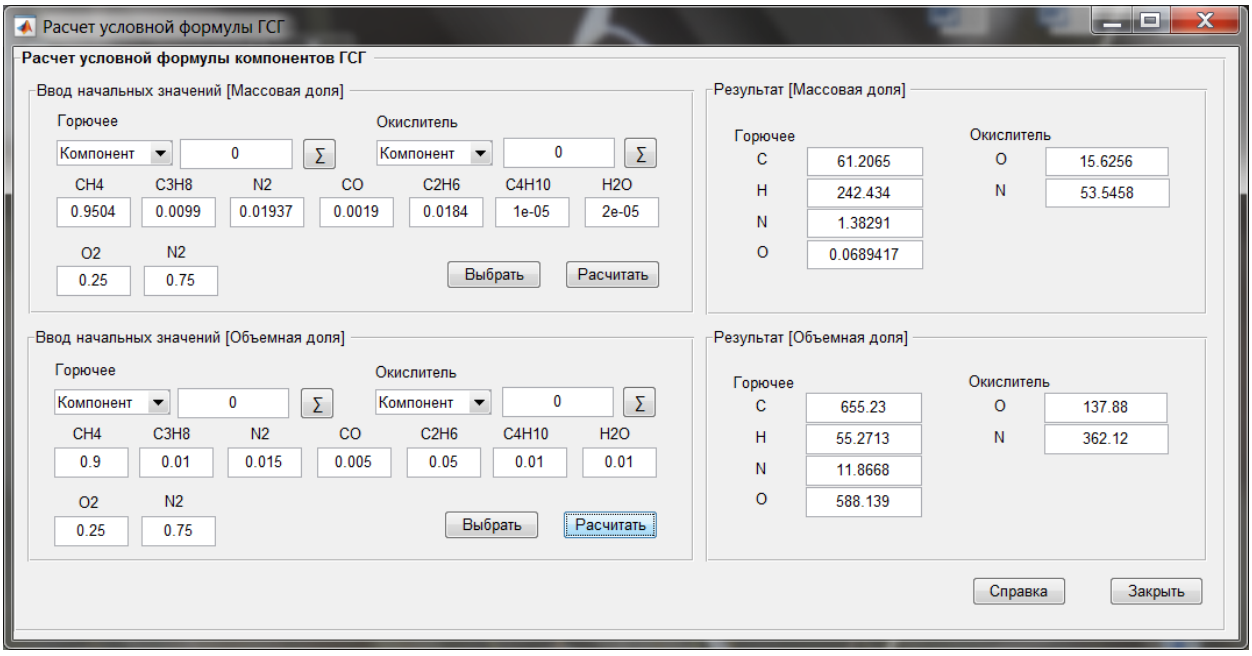


Рисунок 3 – Форма расчета условной формулы исходных компонентов

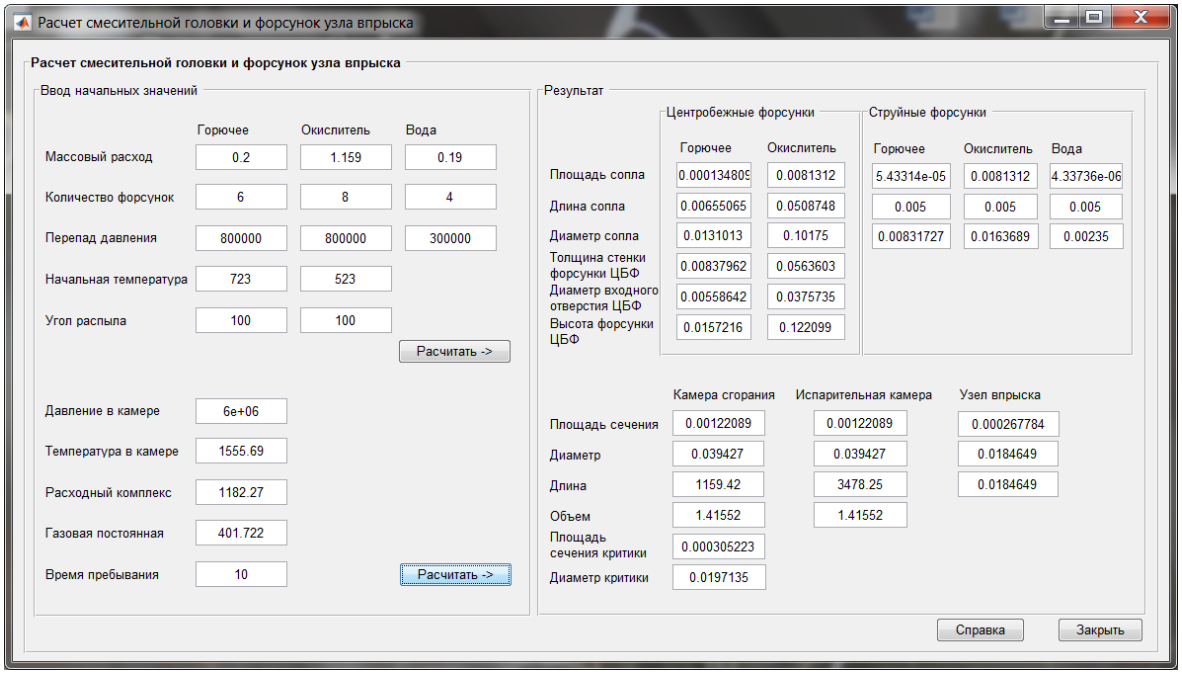


Рисунок 4 – Форма расчета геометрических параметров газогенератора синтез-газа

В ходе анализа взаимодействия пользователей с программным обеспечением, проводимого с целью выявления возможностей увеличения точности расчёта за счёт уменьшения количества ошибок пользователей, были выработаны рекомендации по улучшению интерфейса пользователя.

Внедрение подобного программного обеспечения устранит сложность проведения работ по обработке и анализу получаемых в ходе измерений данных.

СПИСОК ЛИТЕРАТУРЫ

1. Гущин А. Н. Основные концепции построения личностно-ориентированных информационных систем: «Военмех. Вестник Балтийского государственного технического университета». – СПб.: Балтийский государственный технический университет, 2008. – с. 34–44.
2. ГОСТ 34.003-90. Государственный стандарт Российской Федерации: «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».
3. ГОСТ Р ИСО/МЭК ТО 12182-2002. Государственный стандарт Российской Федерации: «Информационная технология. Классификация программных средств».
4. Арипова О.В., Каневская Ю.С. Разработка программного обеспечения с помощью пакетов прикладных программ – Тезисы докладов IV общеросс. науч.-техн. конф. «Старт-2018». – СПб.: БГТУ, 2018. – С. 13-14.
5. Кузьмин А.М., Кулаков К.В., Кулаков С.В., Ценева С.Н. Особенности конструирования газогенераторов синтез-газа для малотоннажного производства метанола, Электронный научный журнал Нефтегазовое дело №3, 2021, С. 124-146.
6. Кузьмин А.М., Гашевский Е.М., Арипова О.В., Ценева С.Н. Свидетельство о государственной регистрации программы для ЭВМ № 2021616736 «Газогенератор синтез-газа», 26 апреля 2021 г.

УДК 004

ВЫГРУЗКА ДАННЫХ ПО API ВКОНТАКТЕ

Корепанова Анастасия Андреевна[1], Москаленко Иван Николаевич[2]
[1] Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
[2] Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: aak@dscs.pro

Аннотация. Социальные сети - огромный источник данных о пользователях и взаимоотношениях между ними. Таким образом информация из социальных сетей становится крайне полезной для исследователей разного рода; для ее сбора было бы удобно использовать автоматизированный софт. Эта статья посвящена разработке программы для работы с социальной сетью «ВКонтакте». В ходе работы было реализовано приложение со всем необходимым функционалом для сбора больших объёмов данных. В будущем оно может оказаться нужным для проведения анализа информации из одной из крупнейших российских социальных сетей.

Ключевые слова: большие объёмы данных; социальные сети.

INFORMATION PARSING WITH VK API

Korepanova Anastasia[1], Moskalenko Ivan[2]
[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
[2] Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: aak@dscs.pro

Abstract. Social networks are a huge source of data about users and the relationships between them. Thus, information from social networks becomes extremely useful for researchers of various kinds; it would be convenient to use automated software to collect it. This article is devoted to the development of a program for working with the VKontakte social network. During the work, an application was implemented with all the necessary functionality for collecting large amounts of data. In the future, it may be necessary to analyze information from one of the largest Russian social networks.

Keywords: big data; social networks; data science.

Введение. Во все сферы нашей жизни всё больше и больше проникают информационные технологии. Это способствует переносу в виртуальное пространство разнообразной информации о людях. Одним из главных «аккумуляторов» подобной информации служат социальные сети [1]. Это неудивительно: например, социальной сетью «ВКонтакте» каждый месяц пользуются более 97 млн человек [2]. Понятно, что информация из соцсетей может многое рассказать не только о конкретном человеке, но и о взаимоотношениях между разными пользователями. Поэтому подобные данные могут заинтересовать исследователей, которые занимаются исследованиями взаимодействий людей в цифровой среде [3, 4].

Таким образом, крайне актуальным становится вопрос о выгрузке больших объёмов данных из социальных сетей. Делать вручную это неудобно, поэтому было принято решение написать программу, которая автоматизирует этот процесс. Данная работа посвящена разработке такого решения. Практическая значимость программы заключается в дальнейшем использовании полученных данных в исследованиях разного рода, например, в работах, посвященных защите пользователей от социоинженерных атак [5].

Обзор аналогов. Был проведён анализ изучаемой области на наличие приложений со схожим функционалом. В итоге было найдено три продукта, которые частично похожи на желаемый продукт. Стоит отметить, что ни один из аналогов не подходит полностью под задуманную идею.

Phantombuster: инструмент, позволяющий автоматизировать загрузку данных из социальных сетей Twitter, Instagram и LinkedIn [6]. Однако данный сервис не поддерживает выгрузку из «ВКонтакте». Также стоит отметить, что бесплатная версия имеет ряд ограничений [7].

ZennoPoster: приложение с возможностью автоматизировать действия на любом сайте, что делает его пригодным для социальной сети «ВКонтакте». Так же, как и прошлый вариант, не является бесплатным [8].

Instaloader: open-source продукт, с помощью которого можно загружать изображения, видео и другие данные из социальной сети Instagram. Версия для «ВКонтакте» отсутствует [9].

Таким образом, отсутствие бесплатного приложения с нужным функционалом делает его разработку ещё более необходимой.

Цель. Разработать приложение с удобным пользовательским интерфейсом, которое бы поддерживало гибкий формат запросов с возможностью составлять различные цепочки из них. Цепочка — это несколько последовательных запросов к VK API, но при этом каждому такому такому звену для начала работы нужны идентификаторы пользователей. Поэтому было решено реализовать звенья цепи как функции от типа «идентификаторы», возвращающие тот же тип. Итоговая реализация должна уметь выгружать информацию асинхронно с применением сразу нескольких токенов, записывать текстовые данные в файл, скачивать изображения в формате .jpg. Токен — это ключ доступа, выдаваемый после успешной авторизации, поэтому на самом деле программа должна уметь работать с несколькими аккаунтами социальной сети «ВКонтакте».

Описание реализации. Для программирования приложения были выбраны следующие технологии:

– Python — мультипарадигменный язык программирования с минималистичным синтаксисом, обладающий полным набором всех библиотек, необходимых для разработки.
– VKBottle – кастомизируемый асинхронный фреймворк для работы с API «ВКонтакте» [10].
– PyQT. Qt – кроссплатформенный фреймворк для разработки GUI [11]. PyQt же является его версией для языка программирования Python.
– Qt-Material – таблица стилей для PyQt. С её помощью можно реализовать интерфейс в стиле Material Design [12].

Основная возможность, предусмотренная в приложении – создавать цепочки запросов. Были реализованы следующие звенья для составления цепочек:

– IDs -> users.get -> IDs. На вход поступают идентификаторы пользователей, запрашивается и записывается в файл анкетная информация этих пользователей, на выходе возвращаются те же идентификаторы.

– IDs -> friends.get -> IDs. На вход поступают идентификаторы пользователей, запрашиваются все списки друзей, на выходе возвращаются идентификаторы, полученные с помощью запросов.

– IDs -> groups.get -> groups.getMembers -> IDs. На вход поступают идентификаторы пользователей, запрашивается списки групп, во всех группах запрашиваются подписчики. На выходе - идентификаторы подписчиков.

– IDs -> photos.get -> IDs. По списку идентификаторов получаем и сохраняем все фотографии пользователей в текстовом формате. Возвращаются те же идентификаторы.

– IDs -> photos.get (with download) -> IDs. Это звено похоже на прошлое. Однако оно не просто записывает текстовую информацию о фотографиях, но также скачивает их в .jpg формате.

– IDs -> wall.get -> IDs. Данное звено принимает на вход идентификаторы пользователей, получает и записывает в файл все записи со стен этих пользователей, возвращает те же идентификаторы.

Существует возможность загружать не все поля из анкет пользователей, а лишь те, которые необходимы в данный момент времени. Также был добавлен функционал для ограничения размера возвращаемых результатов. Например, можно задать такое условия:

– Выгрузить посты, только если их меньше 100.

– Выгрузить друзей, только если их меньше 1000.

– Выгрузить подписчиков группы, только если их меньше 10000.

Была решена большая проблема, связанная с существующими ограничениями на количество запросов к VK API. При превышении лимита токен не используется некоторое время, а затем производится попытка вернуть его в работу. Так продолжается до тех пор, пока токен не станет работать. Такая схема позволяет использовать лимиты по максимуму.

Стандартный алгоритм работы:

– При запуске приложения пользователь составляет необходимую ему цепочку запросов. На рис. 1 можно увидеть интерфейс программы с составленной из трёх звеньев цепочкой; после нажатия кнопки «GO» начнётся её выполнение.

– Получаемая информация динамически записывается в файл.

В любой момент могут превыситься существующие лимиты запросов на одном или сразу нескольких токенов. Все токены, находящиеся под действием ограничительных мер, не используются приложением некоторое время; затем снова возвращаются в работу.

Также во время выполнения запросов может возникнуть какая-нибудь ошибка, если, например, попытаться запросить посты со стены закрытого профиля. Подобные ошибки сразу же выводятся в консоль.

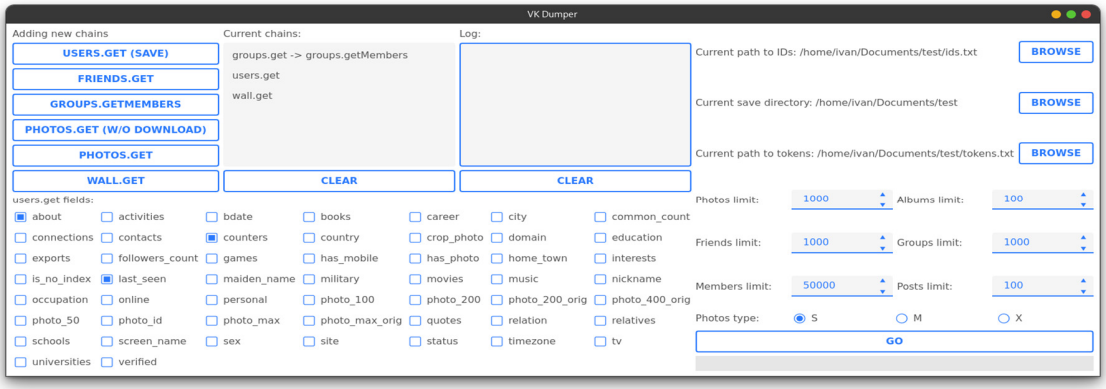


Рис. 1. Интерфейс программы.

Заключение. Целью работы являлась разработка удобного инструмента для выгрузки больших объёмов данных с возможностью составлять цепочки запросов. Поставленная цель была достигнута.

Для реализации проекта были решены следующие задачи:

1. Было нужно исследовать рынок на наличие приложений с необходимым функционалом. Такой анализ был проведён. В результате выяснилось, что существующие продукты не соответствуют всем критериям. Поэтому разработка приложения стала ещё более актуальной.

2. Необходимо было освоить технологии, необходимые для разработки. Все технологии были изучены и применены на практике.

3. Было необходимо создать прототип приложения. Такой прототип был разработан, а наработки активно использовались при воплощении в жизнь финальной версии.

4. Требовалось реализовать полноценную финальную версию. В итоге она была разработана со всем функционалом, который планировался. Последняя версия поддерживает шесть различных звеньев для составления цепочек, возможность гибко задавать запросы к API, ограничивать возвращаемую информацию.

Реализованное приложение полностью удовлетворяет поставленной цели. Оно позволяет удобно выгружать большие объёмы информации. Полученные в результате работы данные могут оказаться полезными при различных исследованиях.

Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН № 0073-2019-0003, при финансовой поддержке РФФИ проект №20-07-00839; поддержана Санкт-Петербургским государственным университетом, проект № 73555239.

СПИСОК ЛИТЕРАТУРЫ

1. Korkmaz M., Celebi N., Yucel A. S. Practical review of the place of social networks in our daily life and their effect on today's youth // International Journal of Academic Research. 2014. Т. 6. № 1. С. 250–261.
2. editor@roem.ru Roem. ru /. Игры остаются самым быстро растущим направлением в бизнесе Mail.ru Group → Roem.ru [Электронный ресурс]. URL: https://roem.ru/28-04-2017/248830/mrg-results-1q17/ (Дата обращения: 12.10.2021).
3. Azarov A. и др. Models and Algorithms for the Information System's Users' Protection Level Probabilistic Estimation // Proceedings of the First International Scientific Conference «Intelligent Information Technologies for Industry» (IITI'16). Cham: Springer International Publishing, 2016. С. 39–46.
4. Azarov A. и др. Users of Information Systems Protection Analysis from Malefactor's Social Engineering Attacks Taking into Account Malefactor's Competence Profile // Advances in Intelligent Systems and Computing. Cham: Springer International Publishing, 2016a. С. 25–30.
5. Bagretsov G. и др. Подходы к автоматизации сбора, структурирования и анализа информации о сотрудниках компании на основе данных социальной сети // НЕЧЕТКИЕ СИСТЕМЫ, МЯГКИЕ ВЫЧИСЛЕНИЯ И ИНТЕЛЛЕКТУАЛЬНЫЕ ТЕХНОЛОГИЯ (НСМВИТ-2017)., 2017.
6. Phantombuster [Электронный ресурс]. URL: https://phantombuster.com/ (Дата обращения: 12.10.2021a).
7. Phantombuster [Электронный ресурс]. URL: https://phantombuster.com/pricing (Дата обращения: 12.10.2021b).
8. ZennoPoster — ZennoLab [Электронный ресурс]. URL: https://zennolab.com/ru/products/zennoposter/ (Дата обращения: 12.10.2021).
9. Instaloader — Download Instagram Photos and Metadata [Электронный ресурс]. URL: https://instaloader.github.io/ (Дата обращения: 12.10.2021).
10. vkbottle. GitHub - vkbottle/vkbottle: Customizable asynchronous VK API framework [Электронный ресурс]. URL: https://github.com/vkbottle/vkbottle (Дата обращения: 12.10.2021).
11. Qt [Электронный ресурс]. URL: https://www.qt.io/ (Дата обращения: 12.10.2021).
12. UN-GCPDS. GitHub - UN-GCPDS/qt-material: Material inspired stylesheet for PySide6, PySide2 and PyQt5 [Электронный ресурс]. URL: https://github.com/UN-GCPDS/qt-material (Дата обращения: 12.10.2021).

УДК 004.42, 378.147

ВЕБ-ФРЕЙМВОРК DJANGO КАК ПЛАТФОРМА ДЛЯ ОБУЧЕНИЯ

Олисеенко Валерий Дмитриевич
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: vdo@dscs.pro

Аннотация. В представленной статье рассматривается веб-фреймворк Django как платформа для обучения программированию, визуализации результатов и решению исследовательских задач. Поднимаются вопросы изучения актуального стека технологий (Python 3, PostgreSQL, Bootstrap 4, HTML, CSS, JavaScript), методов программирования (объектно-ориентированного программирования, паттернов разработки) и системы для размещения готового проекта во всемирной паутине.

Ключевые слова: обучение разработки; веб-фреймворк Django; облачные технологии; социоинженерные атаки.

DJANGO WEB FRAMEWORK AS A LEARNING PLATFORM

Oliseenko Valerii
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: vdo@dscs.pro

Abstract. The presented article deals with Django web framework as a platform for learning programming, visualizing results and solving research problems. It raises the issues of learning the current technology stack (Python 3, PostgreSQL, Bootstrap 4, HTML, CSS, JavaScript), programming methods (object-oriented programming, development patterns) and the system for placing the finished project on the World Wide Web.

Keywords: development training; Django web framework; cloud technologies; social engineering attacks.

Введение. Современный рынок IT труда всё чаще требует широких компетенций (способность к самостоятельному обучению; способность к поиску решений задач, постановке цели и методов её достижения; способность к работе в команде и т.д.) и большого опыта даже у начинающих разработчиков. К примеру, по статистике компании hh.ru около 51% вакансий требуют опыт работы от 1 до 3 лет, при этом только 9% меньше

1 года. Именно поэтому вопрос наработки таких компетенции и опыта является ключевым в образовательном процессе любого высшего учебного заведения. Помимо этого, высшим учебным заведениям также необходимо решать вопрос начальной подготовки будущих научно-педагогических кадров с первой ступени высшего образования (бакалавриата). Такая необходимость вызвана существующей проблемой нехватки кадров, в том числе для реализации программ развития (Научно-Технологическое Развитие Российской Федерации, Приоритет-2030 и т.д.). Именно поэтому целью данной статьи является изучение веб-фреймворка Django, как платформа для обучения программированию, визуализации результатов и решению исследовательских задач.

Платформа веб-фреймворка Django позволяет решить широкий спектр задач в обучении: познакомить обучающегося с языком разработки Python 3, получить навыки разработки на актуальном стеке веб-технологий (Python 3, PostgreSQL, Bootstrap 4, HTML, CSS, JavaScript), привить понимание устройства облачных технологий, дать возможность применить современные методы программирования (объектно-ориентированного программирования, паттернов разработки) и т.д. Кроме того, представленный веб-фреймворк и Python 3 имеет средний порог входа, который является гораздо меньшим, чем например у C/C++, Java, Go, Kotlin и др., что по мнению авторов позволяет не только обучиться навыкам программирования, но и попутно решать научно-технические задачи и погружаться в рабочие условия научно-исследовательских работ.

В рамках учебной практики обучающемуся первого курса бакалавриата было предложено разработать прототип программного комплекса, способного агрегировать и представлять некоторые данные из аккаунтов пользователей социальных сетей «ВКонтакте» и «Одноклассники». Кроме того, в предложенной задаче присутствовало условие по внедрению существующих разработок для анализа аккаунтов пользователей [1–4] с целью последующего выявления уязвимостей пользователей к социоинженерным атакам. Причём для ознакомленья обучающемуся был предоставлен только текст статей, без существующего кода. Таким образом, необходимо было фактически восстановить программные эксперименты, с поправкой на включения их в рабочую систему. Этим решалась не только практическая, но и теоретическо-научная задача обучения.

Основными условиями разработки прототипа программного комплекса являлось использование веб-фреймворка Django [5], языка Python 3 [6]. Также для закрепления навыков веб-разработки была предложена реализация пользовательского графического интерфейса по созданным ранее макетам (рис. 1, 2).

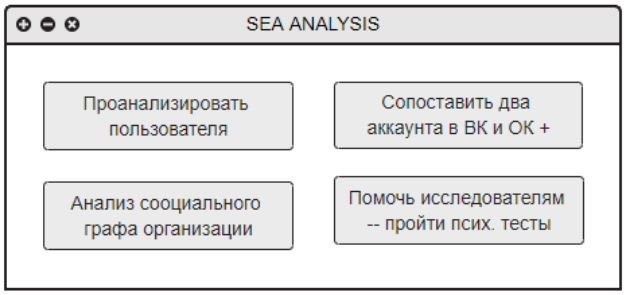


Рис. 1. Макет графического интерфейса «Главное меню».

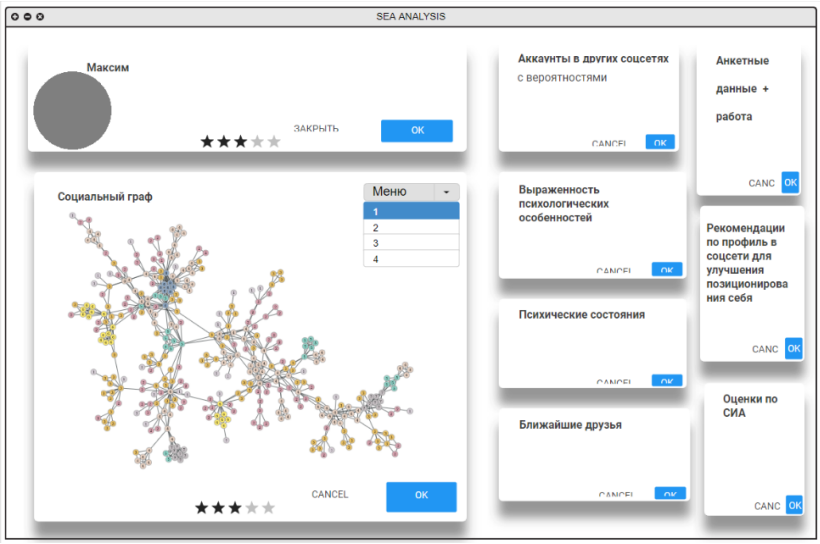


Рис. 2. Макет графического интерфейса «Анализ пользователя».

В рамках учебной практики двух семестров обучающийся успешно освоил Python 3, научился разрабатывать веб-приложение на актуальном стеке технологий, получил понимание работы облачных технологий (в частности get/post запросов, создания сервера и т.д.), применил современные методы программирования, использовал систему контроля версий Github. Результат был размещен на виртуальном хостинге по адресу sea.dscs.pro. На (рис. 3) представлена главная страница разработанного прототипа.

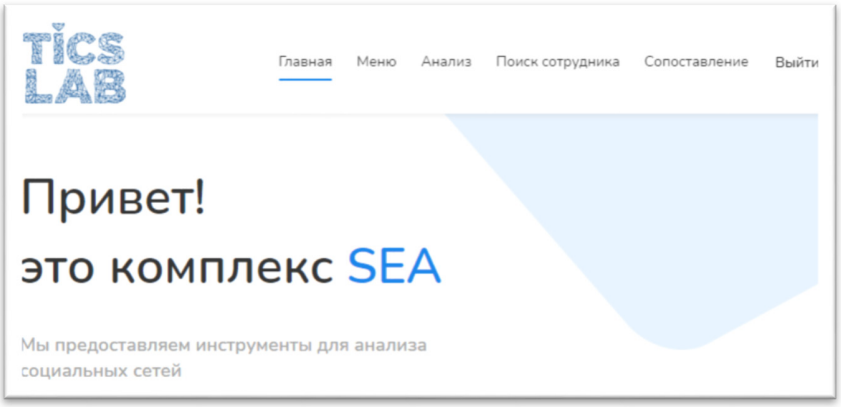


Рис. 2. Главная страница прототипа.

Заключение. Как показал полученный опыт веб-фреймворк Django действительно показал себя как платформа для обучения программированию, визуализации результатов и решению исследовательских задач. Все поставленные цели перед обучающимся были достигнуты, а задачи выполнены. Кроме того, полученный результат разработки был размещён на виртуальном хостинге у провайдера по адресу https://sea.dscs.pro, а теоретические результаты закреплены в отчёте по научной практике и в статье, отправленной в журнал из «списка ВАК».

Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН № 0073-2019-0003, при финансовой поддержке РФФИ проект №20-07-00839.

СПИСОК ЛИТЕРАТУРЫ

1. Абрамов М.В., Тулупьев А.Л., Тулупьева Т.В. Агрегирование данных из социальных сетей для восстановления фрагмента мета-профиля пользователя // Шестнадцатая Национальная конференция по искусственному интеллекту с международным участием КИИ-2018 Труды конференции: в 2-х томах. 2018. С. 189–197.
2. Корепанова А.А., Олисеенко В.Д., Абрамов М.В., Тулупьев А.Л. Применение методов машинного обучения в задаче идентификации аккаунтов пользователя в двух социальных сетях // Компьютерные инструменты в образовании. 2019. № 3. С. 29–43. doi:10.32603/2071-2340-2019-3-29-43.
3. 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: сб. статей студентов, магистрантов, аспирантов и молодых ученых. Казань. 2019. С. 312–317. ISBN 978-5-00130-159-2.
4. Тулупьева Т.В., Тафинцева А.С., Тулупьев А.Л. Подход к анализу отражения особенностей личности в цифровых следах // Вестн. психотерапии. 2016. № 60 (65). С. 124–137.
5. Vincent W. S. Django for Beginners: Build websites with Python and Django. WelcomeToCode, 2020.
6. Matthes E. Python crash course: A hands-on, project-based introduction to programming. no starch press, 2019.

УДК 004.89

ПАТТЕРН ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЯ ОНЛАЙН СОЦИАЛЬНОЙ СЕТИ: ИНТЕНСИВНОСТЬ ДЕЙСТВИЙ И ПОДХОДЫ К ОЦЕНКЕ

Столярова Валерия Фуатовна
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: vfs@dscs.pro

Аннотация. В статье рассматривается задача моделирования профиля пользователя онлайн социальной сети с точки зрения оценки риска, связанного с использованием. Чтобы при оценке частоты поведения учесть различные источники неопределенности и иные факторы, оказывающих влияние на поведение индивида, предложена вероятностная графическая модель: непрерывная непараметрическая байесовская сеть доверия.

Ключевые слова: паттерн поведения; вероятностные графические модели; поведенческая эпидемиология.

BEHAVIOR PATTERN OF THE ONLINE SOCIAL MEDIA USER: FREQUENCY OF ACTIONS AND ITS MODELLING

Stoliarova Valerie
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: vfs@dscs.pro

Abstract. The paper is devoted to the problem of the behavior pattern modelling of the online social media user in the context of behavior risk assessment. The use of the non-parametric Bayes belief networks is proposed in order to model different types of uncertainty arising in the knowledge domain, and to incorporate possible risk factors.

Keywords: behavior pattern; probabilistic graphical models; behavior epidemiology.

Введение. Онлайн социальные сети (ОСС) играют все возрастающую роль в повседневной жизни человека, и служат источником информации о личности для проведения различных социологических и психологических исследований [1]. Однако порой использование ОСС связано с определенными рисками здоровью самого пользователя, такими как зависимое использование ОСС [2] и склонность к употреблению алкоголя и наркотиков [3] или связанной с ним инфраструктуры, к примеру, критичным документам организации [4]. Таким образом, актуальной является задача моделирования паттерна поведения пользователя ОСС с целью дальнейшего использования при оценке риска. Отметим, что одной из ключевых характеристик поведения, использующейся в различных шкалах оценки риска, является его частота [8]: частота обращения к ОСС или же частота совершения различных действий в ОСС.

Паттерн поведения пользователя ОСС является составным понятием, включающим в себя как объективные технические данные из профиля пользователя, такие как даты публикации постов, число друзей, число сообществ, так и информацию, предоставляемую самим пользователем (имя, возраст, город, образование). Отметим, что последний блок информации относится к самоотчетам пользователя о себе, и потому содержит неточную и неполную информацию. Кроме того, существуют ситуации, когда при оценке частоты действий в ОСС необходимо также прибегать к самоотчетам пользователя (ограничения приватности), как при оценке частоты обращения к ОСС при моделировании риска зависимого использования.

При оценке характеристик поведения по данным об эпизодах поведения, полученным в рамках самоотчетов респондентов, актуальной является задача получения наименее искаженной информации, так как она подвержена различным когнитивным искажениям (искажение припоминания, искажение социальной ожидаемости) [10]. Для уменьшения влияния таких искажений, в исследованиях обращаются к наиболее запоминающимся эпизодам поведения, такие методы носят название методов обратной связи по временной шкале (timeline followback methods) [11]. Для построения оценок интенсивности поведения, в работах [7, 11] был предложен метод, опирающийся лишь на несколько последних эпизодов поведения.

В данной работе, чтобы учитывать возникающие в области знаний источники неопределенности, а также разнородную информацию профиля пользователя, предлагается использовать вероятностные графические модели и байесовский вывод. В работе предложена структура модели непрерывной непараметрической байесовской сети доверия, отражающей взаимосвязь информации из профиля пользователя. Численные значения получены на основе данных, собранных из онлайн социальной сети ВКонтакте. Использование байесовского вывода позволяет использовать предлагаемую модель в тех задачах, где основным источником данных является информация от экспертов.

Структура байесовской сети доверия. Ранее [5] была предложена структура непрерывной непараметрической байесовской сети доверия для задачи оценки интенсивности поведения по данным о нескольких последних эпизодах. Такая модель позволяет учитывать неопределенность в количестве возможной доступной информации об эпизодах поведения: изменение числа наблюдаемых эпизодов в такой модели не приводит к пересчету параметров модели.

Непрерывная непараметрическая байесовская сеть доверия [12] представляет собой вероятностную графическую модель, с узлами которой ассоциированы непрерывные или дискретные случайные величины, а арки отражают причинно-следственные связи предметной области. Численно взаимосвязь между узлами сети осуществляется посредством копул, параметризованных (условными) коэффициентами ранговой корреляции.

В данной работе предложена структура сети, включающей различные характеристики профиля пользователя в ОСС. Эпизодическое поведение предлагается характеризовать посредством его частоты (интенсивности), которая при помощи математической модели поведения [6] может оцениваться только по нескольким последним эпизодам.

Важной особенностью предлагаемой вероятностной графической модели является использование гамма-пуассоновской модели поведения [7]. Такая структура позволяет внедрить в модель данных профиля пользователя индивидуальные характеристики пользователя ОСС, так называемую *склонности к поведению*. Склонность к поведению может оставаться ненаблюдаемой характеристикой, имеющей гамма-распределение в популяции, или может наблюдаться косвенно посредством измеряемых психологических характеристик.

На рис. представлена структура данных о поведении пользователя ОСС по данным его профиля. Используется один тип эпизодического поведения.

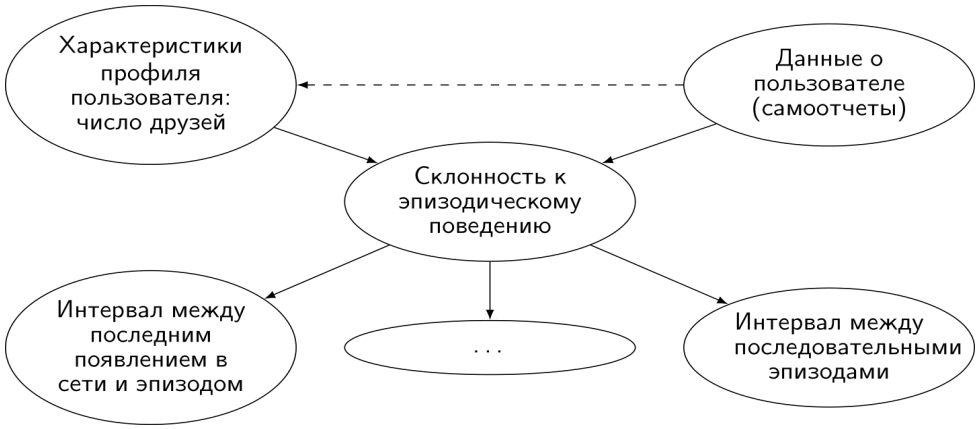


Рис. 1. Общая структура информации из профиля пользователя ОСС, включающая эпизодическое поведение и индивидуальную склонность к поведению.

Предложенная модель была апробирована на данных из онлайн социальной сети ВКонтакте. Были собраны следующие данные о профилях пользователя: число друзей, пол, возраст, даты публикации постов [9], по этим данным оценены как параметры маргинальных распределений, так и параметры копул, осуществляющих взаимосвязь переменных модели.

Заключение. Предложенная модель является гибкой и позволяет при оценке риска, связанного с поведением пользователя в ОСС, учитывать разнообразные факторы, как объективные характеристики профиля пользователя, так и индивидуальные особенности личности.

Работа выполнена при финансовой поддержке СПБ ФИЦ РАН, тема госзадания № 0073-2019-0003, грант РФФИ № 20-07-00839 А.

СПИСОК ЛИТЕРАТУРЫ

1. Bachrach Y., Kosinski M., Graepel T., Kohli P., Stillwell D. Personality and patterns of Facebook usage // In Proceedings of the 4th annual ACM web science conference. 2012. С. 24–32.
2. Kuss D.J., Griffiths M.D. Online Social Networking and Addiction—A Review of the Psychological Literature // International Journal of Environmental Research and Public Health. 2011, 8(9). С. 3528–3552.
3. Ilakkuvan V., Johnson A., Villanti A.C., Evans W.D., Turner M. Patterns of social media use and their relationship to health risks among young adults // Journal of Adolescent Health. 64(2), 2019. С. 158–164.
4. Frolova M. S., Korepanova A. A., Abramov M. V. Assessing the Degree of the Social Media User's Openness Using an Expert Model Based on the Bayesian Network //2021 XXIV International Conference on Soft Computing and Measurements (SCM). IEEE, 2021. С. 52-55.
5. Stoliarova V. Non-Parametric Bayes Belief Network for Intensity Estimation with Data on Several Last Episodes of Person's Behavior // in Dolinina O. et al. (eds) Recent Research in Control Engineering and Decision Making. ICIT 2020. Studies in Systems, Decision and Control, vol 337. Springer, Cham., p. 486-497.
6. Пащенко А. Е., Тулупьев А. Л., Тулупьева Т. В., Красносельских Т. В., Соколовский Е. В. Косвенная оценка вероятности заражения ВИЧ-инфекцией на основе данных о последних эпизодах рискованного поведения // Здравоохранение Российской Федерации, 2010, (2), 32-35.
7. Пащенко, А. Е., Тулупьев, А. Л., & Николенко, С. И. Статистическая оценка вероятности заражения ВИЧ-инфекцией на основе данных о последних эпизодах рискованного поведения // Труды СПИИРАН, 2006, 2(3). С. 257-268.
8. Ellison N.B., Steinfield C, Lampe C. The Benefits of Facebook «Friends:» Social Capital and College Students' Use of Online Social Network Sites // Journal of Computer-Mediated Communication, Vol.12, № 4, 2007.
9. Столярова В.Ф., Торопова А.В., Тулупьев А.Л. Модель для оценки частоты публикации постов в онлайн социальной сети по неполным данным с учетом объективных детерминант поведения // Нечеткие системы и мягкие вычисления. Принято к публикации.
10. Тулупьева Т. В., Пащенко А. Е., Тулупьев А. Л., Красносельских Т. В., Казакова О. С. Модели ВИЧ-рискованного поведения в контексте психологической защиты и других адаптивных стилей. 2008. (монография).
11. Sobell, L. C., Agrawal, S., Sobell, M. B., Leo, G. I., Young, L. J., Cunningham, J. A., & Simco, E. R. (2003). Comparison of a quick drinking screen with the timeline followback for individuals with alcohol problems // Journal of Studies on Alcohol, 64. С. 858–861.
12. Hanea A., Napoles O. M., Ababei D. Non-parametric Bayesian networks: Improving theory and reviewing applications //Reliability Engineering & System Safety, 2015, Т. 144. С. 265-284.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

УДК 629.12

КВАЛИМЕТРИЧЕСКИЙ АНАЛИЗ ПУБЛИКАЦИОННОЙ АКТИВНОСТИ: УГРОЗЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Алексеев Анатолий Владимирович[1], Касаткин Виктор Викторович[2], Равин Александр Александрович[1], Соколов Борис Владимирович[2], Хруцкий Олег Валентинович[1]

[1]Санкт-Петербургский государственный морской технический университет
Лоцманская ул., д. 3, Санкт-Петербург, 198262, Россия
[2]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
14 линия, 39, Санкт-Петербург, Россия
e-mails: iapbgks@bk.ru

Аннотация. Обобщены данные и выполнен квалиметрический SWOT-анализ пяти вариантов системы регулирования публикационной активности авторов, включая аспекты национальной безопасности и авторского права. Результаты количественных оценок выявили высокую критичность информационной инфраструктуры участия отечественных авторов при публикации научных трудов в действующих сегодня наукометрических системах Web of Science, Scopus, открывающих широкие возможности технологического заимствования, осуществления аналитической разведки недружественными странами, оказания санкционного давления и информационно-психологического воздействия на авторов, а также возможность рефлексивного и ментального управления процессами развития отечественной науки. В качестве альтернативы с конкурентным превосходством более 70% согласно результатам проведенного квалиметрического полимодельного анализа показана перспективность развития национальной системы обеспечения и стимулирования публикационной активности отечественных авторов (с применением независимой ранговой квалиметрической аттестации публикаций), направленной на защиту национальных интеллектуальных ресурсов, сохранение информационного суверенитета и обеспечение национальных интересов России.

Ключевые слова: публикационная активность; ранговый квалиметрический анализ; критическая информационная инфраструктура; рефлексивное управление; ментальное управление; национальные интеллектуальные ресурсы; информационная безопасность; национальные интересы.

QUALIMETRIC ANALYSIS OF PUBLICATION ACTIVITY: THREATS TO NATIONAL SECURITY

Alekseev Anatoly[1], Kasatkin Viktor[2], Ravin Alexander[1], Sokolov Boris[2], Khrutsky Oleg[1]

[1]Saint Petersburg State Marine Technical University
3 Lotsmanskaya str., St. Petersburg, 198262, Russia
e-mail: iapbgks@bk.ru, +7 (909) 580-21-55
[2] St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th Line Str., St. Petersburg, Russia
e-mails: iapbgks@bk.ru

Abstract. Data are summarized and qualification SWOT-analysis of five versions of the system of regulation of authors publication activity, including aspects of national security and copyright, is performed. The results of quantitative assessments revealed the high criticality of the information infrastructure of the participation of domestic authors in the publication of scientific papers in the currently operating science-metric systems Web of Science, Scopus, which open up wide opportunities for technological borrowing, the implementation of analytical exploration by unfriendly countries, the application of sanction pressure and information-psychological impact on authors, as well as the possibility of reflexive and mental management of the development processes of domestic science. As an alternative with competitive superiority of more than 70%, according to the results of the qualification polymodel analysis, the prospects for the development of the national system of ensuring and stimulating the publication activity of domestic authors (using independent rank qualification certification of publications) aimed at protecting national intellectual resources, preserving information sovereignty and ensuring the national interests of Russia are shown.

Keywords: publication activity; rank qualimetric analysis; critical information infrastructure; reflexive management; mental management; national intellectual resources; information security; national interests.

Среди вопросов обеспечения информационной безопасности (ИБ), информационного противодействия (ИПД) и информационного противоборства (ИП), в целом, неоправданно мало уделяется внимания вопросам количественных оценок, анализа, синтеза, критичности и практического их использования при управлении сложными техническими, организационно-техническими и социальными системами [1]. Среди проблемных вопросов обеспечения ИБ, ИПД, ИП, по мнению авторов, весьма односторонне и, в ряде случаев тенденциозно декларируется необходимость повышения публикационной активности отечественных авторов, в первую очередь, научных работников в зарубежных изданиях с необходимостью регистрации в целях повышения авторского импакт-фактора в действующих международных наукометрических базах данных, (призванных отражать квалиметрические показатели востребованности и качества публикаций) включая [2]:

Web of Science – старейшая база данных, индексирующая свыше 12 тысяч научных изданий (в том числе – около 170 российских). Основной разработчик – компания Thomson Reuters. Среди специфических особенностей: весьма упрощенный поиск актуальных научных тенденций; отслеживание показателей цитирования, начиная с 1900 года; строгий отбор научных изданий, добавляемых в базу; учет взаимного цитирования публикаций; поиск не только по статьям, но и целым книгам, материалам конференций.

2. Scopus – самая крупная и популярная реферативная база, принадлежащая издательству Elsevier. В нее включено свыше 23 тысяч изданий из самых разных областей знаний (российских – около 350 журналов). Среди особенностей: декларируемая возможность доступа к полным текстам научных трудов; обширный обзор источников литературы на любую тему; сравнительно простой и быстрый поиск; анализ деятельности ученого, без расчета импакт-фактора; сравнение нескольких журналов по определенным критериям.

3. Российский индекс научного цитирования (РИНЦ) – национальная система поиска, содержащая свыше 7 миллионов публикаций и данные по ним из 4500 русскоязычных журналов. Сервис принадлежит научной электронной библиотеке eLIBRARY. Особенности РИНЦ: оперативное получение нужной информации из актуальных источников; полные тексты работ с платным и бесплатным доступом; мощный аналитический инструмент, выполняющий оценку эффективности научной деятельности ученых, организаций; сравнительно объективное оценивание и анализ публикационной активности отечественных исследователей.

4. Академия Google (Google Scholar) – база данных в виде поисковой системы, в которой данные хранятся и обрабатываются в запрограммированных репозиториях. Особенности Google Академии: обработка и учет полных текстов научных трудов по самым разным направлениям; максимальное количество русскоязычных изданий; создание личного профиля ученого, где отображается список всех его публикаций, показатели цитируемости; реальная статистика цитируемости, учитывающая источники в интернете и библиотеках; пользование сервисом бесплатно для каждого, но при переходе по ссылке с интересующим документом может потребоваться оплата за скачивание полного текста.

5. Другие поисковые системы, включая: Microsoft Academic, Index Copernicus, SJR, MedLine, PubMed, Science Direct, Arxiv.Org, CiteSeerX, WorldWideScience, BASE, AMiner.

В указанных системах к наукометрическим показателям авторов относят количество публикаций, частоту их цитирований, число премий, стипендий, грантов, индекс Хирша, (учитывающий количество публикаций автора и число их цитирований. Так, при наличии 5 статей у исследователя, на каждую из которых ссылаются не менее 5 раз, h-индекс составляет 5), импакт-фактор (определяет число цитирований конкретного научного труда за последние два года), индекс цитирования (определяется числом ссылок на эту работу или фамилию автора), участие в составе редколлегии, сотрудничество с иностранными партнерами.

Как можно заметить, к качеству самих публикаций (как мере соответствия содержания работы ее целевому предназначению, которое, как правило, отражается в ее названии) эти показатели прямого (непосредственно оцениваемого) отношения не имеют и носят, скорее, маркетинговый характер, в то время как читателя в первую очередь интересует существо и содержание самой публикации, а имидж автора формируется и зависит от широкого спектра условий и факторов субъективного характера.

При привлекательных и бесспорных на первый взгляд данных факторов, критериев (как меры соответствия свойств предназначению) и показателей (как численного выражения критериев) при этом наряду с позитивными свойствами этих процессов и известной мотивированностью авторов исследований подчас совершенно не учитываются их бесспорные негативные свойства (последствия), уязвимости, угрозы информационной безопасности и, более того, угрозы национальным интересам России [1, 7-10].

С учетом этого на базе опыта исследований [11-15] был выполнен полимодельный квалиметрический анализ влияния наиболее значимых, по мнению авторов, уязвимостей и угроз информационной безопасности для основных вариантов обеспечения публикационной активности отечественных авторов.

С этой целью были систематизированы исходные данные и выполнен по семи моделям критериальных предпочтений квалиметрический SWOT-анализ (QSWOT) пяти вариантов (1, 3, 4, 5 (базовый для сравнения) – для

национальных наукометрических систем, 2 – для вненациональных систем) обеспечения публикационной активности авторов, результаты которого представлены на рис. 1.

i	QSWOT-анализ вариантов обеспечения публикационной активности авторов															
Модель ИКЗ:	2	2. Модель прогрессивного развития.	0,35		0,15		0,35		0,15							
Парадигма, концепция	Существо, базовые принципы концепции	S.Сильные (внутренние) стороны	qi (0…10)	W.Слабые (внутренние) стороны	qi (0…10)	O.Возможности развития с учетом внешних факторов	qi (0…10)	T.Угрозы развития с учетом внешних факторов	qi (0…10)	QSWOT Q	RQ	КП	КС	QSWOT Qпм	RQпм	КСпм
1.Концепция повышения национальной публикационной активности отечественных авторов	Индексация публикаций по национальной системе критериев. РИНЦ, ВАК, а также Google, Microsoft Academic, Index Copernicus, SJR, MedLine, PubMed, Science Direct, Arxiv.Org, CiteSeerX, WorldWideScience, BASE, Aminer и др.	1.Получение удовлетворения и чувства самореализации. 2.Получение возможности аргументированного участия в научных дискуссиях. 3.Повышение авторской репутации. 4.Улучшение качества публикаций при рецензирование. 5.Мотивирование дальнейших исследований при рецензирование. 6.Повышение возможности дополнительного финансирования исследований автора и организации. 7.Повышение научной узнаваемости авторов. 8.Повышение научного статуса и результативности научной деятельности. 9.Расширение поля деятельности, неформального общения, совместных публикаций.10.Возможность повышения рейтинга организации. 11.Отсутствие или снижение уровня языкового барьера.	7,0	1.Очень «консервативная» процедура процесса рецензирования. 2.Рецензирование заведомо носит предвзятый характер. 3.Весьма длительный процесс, но не препятствие развитию исследований. 4.Если результаты научного труда не опубликованы, то данная работа не считается законченной. 5.Необходимо изучать труды ведущих журналов типа Elsevier, Springer, Wiley, Taylor&Francis, OUP, CUP, AIP, APS, Nature, Science, журналов специализированных издательств и обществ. 6.Финансовые проблемы публикации.	2,0	1.Формирование национальной КБДЗ технологического развития. 2.Национальная система ранжирования научных результатов, концентрации усилий, иньестиций. 3.Система государственного управления научным развитием.	8,0	1.Необходимость государственной защиты КИИ КБДЗ. 2.Коррупция. 3.Научные фейки.	6,0	6,88	2	38%	38%	7,05	2	41%
2.Технология современного "цифрового" мотивирования авторов и организаций	Индексация публикаций по вненациональной системе критериев. Web of Science, Scopus, …	По п. 1-8 варианта 1	6,5	По п. 1, 4, 6 варианта 1.	7,5	Прогрессивные возможности развития практически не выявлены.	4,5	1.Технологическое заимствование. 2.Широкое поле и возможности антигосударственной аналитической разведки недружественными странами. 4.Санкционное давление и унижение авторов. 5.Возможность рефлексивного управления развитием национальной науки.	8,5	3,97	5	-21%	-21%	4,04	5	-19%
3.Технология независимой экспертной квалиметрической аттестации публикаций "КСПР"	Квалиметрическое ранжирование и сертификация качества публикаций в системе РПС ИАП БЖКС	По п. 1-11 варианта 1. 12.Высокая "прозрачность" анализа и публичности результатов сравнения. 13.Наличе конструктивных рекомендаций авторам. 14.Простота реализации и финансовая доступность. 15.Междисциплинарная и межведомственная инвариантность. 16.Перспективность и мотивирование молодых авторов. 17.Научный демократизм" сравнен ия качества. 18.Персональная ответственность экспертов. 19.Возможность повышение рейтинга экспертов. 20.Другие.	9,0	По п. 1, 2, 5, 6 варианта 1	1,5	1.Маркетинговые преимущества технологии сравнения. 2.Национальная мотивация. 3.Возможность привлечения иностранных авторов. 4.Конкурентное превосходство на "консервативной" технологией варианта 2. 5.Возможность научного противодействия санкциям.	9,0	1.Межнациональная конкуренция авторов, государств и национальных научных школ. 2.Непредвиденные форсмажорные обстоятельства.	5,0	8,17	1	63%	63%	8,35	1	67%
4.Концепция публичной квалиметрической аттестации публикаций "Голос"	Квалиметрическое ранжирование и сертификация качества публикаций в системе РПС ИАП БЖКС (вариант публичной экспертизы)	По п. 1-20 варианта 3.	8,0	1.Негативная возможность влияния группообразования	3,0	1.Позитивная возможность формирования творческих коллективов и их публичная доступность. 2.Возможность оперативного разрешения конфликтных ситуаций.	8,0	Возможность конфликтования групп с использованием СМИ и недобросовестного пиара	7,0	6,77	3	35%	35%	6,99	3	40%
5.Возможные альтернативные варианты	При наличие	Обобщенные другие варианты оценивания	5,0	Условно: средний уровень.	5,0	12.10.2021	5,0	Эксперт: Алешин А.В.	5,0	5,00	4	0%	0%	5,00	4	0%

Рис. 1 – Результаты полимодельного квалиметрического анализа пяти вариантов наукометрического оценивания публикационной активности с учетом факторов обеспечения информационной безопасности

При экспертной оценке позитивных свойств (сторон) варианта 1 (РИНЦ, по перечню ВАК и др.) с уровнем QS=7,0 по 10-бальной шкале оценивания были приняты во внимание следующие основные факторы:

S.1. Получение удовлетворения и чувства самореализации автора публикации.

S.2. Обеспечение возможности аргументированного участия автора в научных дискуссиях.

S.3. Повышение авторской (научной) репутации в процессе рецензирования и публикации трудов.

S.4. Улучшение качества публикаций при рецензировании.

S.5. Мотивирование дальнейших исследований по результатам рецензирования.

S.6. Появление возможности дополнительного финансирования исследований автора и организации.

S.7. Повышение научной узнаваемости авторов в научном сообществе.

S.8. Повышение научного статуса (авторитета) и результативности научной деятельности автора.

S.9. Расширение поля деятельности автора, неформального общения, возможных совместных публикаций.

S.10. Возможность повышения рейтинга организации за счет авторитета ее авторов и их публикаций.

S.11. Отсутствие или снижение уровня языкового барьера в процессе публикации трудов.

При экспертной оценке негативных свойств варианта 1 с уровнем QW=2,0 были приняты во внимание следующие шесть основных факторов:

W.1. В ряде случаев весьма «консервативная» процедура рецензирования трудов.

W.2. Рецензирование заведомо, как правило, носит предвзятый характер с проявлением субъективных предпочтений экспертов.

W.3. Достаточно длительный процесс публикации, в целом, как правило, не препятствующий развитию исследований.

W.4. Приоритетность широко применяемого на практике подхода: если результаты научного труда не опубликованы, то данная работа не считается законченной.

W.5. Необходимость изучать труды ведущих журналов типа Elsevier, Springer, Wiley, Taylor&Francis, OUP, CUP, AIP, APS, Nature, Science, журналов специализированных издательств и обществ, что далеко непросто.

W.6. Финансовые проблемы публикации трудов, включая несопоставимую «себестоимость» публикуемого труда (интеллектуальные затраты и ценность публикуемого материала) с интеллектуальной ценностью «отдаваемого» автором научного труда издательству и приобретаемым им соавторским правом.

Среди внешних негативных свойств варианта 1 с достаточно высоким уровнем QT=6,0 (в дополнение к позитивным свойствам с принятым уровнем QO=8,0) приняты следующие факторы:

T.1. Необходимость информационно-правовой защиты государством, формируемой в процессе открытой публикации научных трудов (как правило, обладающих соответствующей новизной, уникальностью) соответствующих информационных ресурсов национального масштаба от угроз практически беспрепятственного и свободного (лигитимного) доступа и «безвозмездного» технологического заимствования и плагиата представленных в публикациях результатов высокотехнологичной интеллектуальной деятельности многочисленных авторов, авторская защита интересов которых носит, как правило, условный характер.

Т.2. Еще большее значение эти факторы приобретают применительно к объектам критической информационной инфраструктуры, к числу которых в полной мере могут быть отнесены квалиметрические базы данных и знаний, включая наукометрические базы данных по соответствующим отраслям знаний, предметным областям, ведомствам, предприятиям и территориальным образованиям.

Т.3. Отдельные коррупционные проявления в части, например, лоббирования интересов отдельных групп с использованием служебного положения и соответствующих ссылок на наукометрические показатели (без должного предметного анализа и учета содержания) и их необъективным формированием.

Кроме того, в целом ряде случаев книжные издательства, редколлегии журналов, патентные ведомства, организаторы конференций вместо объективного оценивания, ранжирования и поощрения авторов преследуют исключительно коммерческие цели, а наукометрические данные используют исключительно в маркетинговых целях. Более того, в ряде случаев сами наукометрические индексы при этом отражают не качество публикаций, а финансовые возможности их авторов. Организации, в которых трудятся авторы, попадая в зависимость от наукометрических, а не квалиметрических требований, вынуждены идти на оплату публикации авторских трудов ради наращивания массы импакт-факторов, косвенно участвуя тем самым в возможном снижении их качества.

Т.4. Возможность формирования и использования наукообразных фейков (фальшивых, поддельных данных) в условиях межгрупповой конкуренции и недобросовестного противоборства научных школ. В этом контексте также следует учитывать, что значительную часть уже опубликованных результатов, в том числе в высокорейтинговых журналах, далеко не всегда удается воспроизвести. Так, в онкологии (трансграничной и прикладной научной отрасли знаний) сегодня невоспроизводимость опубликованных данных по экспертным оценкам достигает 75 процентов.

Квалиметрическая оценка качества варианта «1. Концепции повышения национальной публикационной активности отечественных авторов», выполненная по гармоническому алгоритму агрегирования QSWOT-показателей качества (QSWOT, Q – для каждой модели) и по семи моделям (полимодельная оценка – QSWOT, QПМ) индексов критериальной значимости (ИКЗ) в сопоставлении с другими четырьмя вариантами при базовом варианте «5. Возможные альтернативные варианты» (со средними оценками) позволяет сделать следующие выводы (рис. 1).

1. Результаты анализа показали высокую критичность информационной инфраструктуры участия отечественных авторов при публикации научных трудов в действующей сегодня системе (вариант «2. Технология современного «цифрового» мотивирования авторов и организаций») с индексацией публикаций по вненациональной системе критериев Web of Science, Scopus и других ($Q_{ПМ,2}$=4,04) при сопоставлении с отечественной системой (вариант 1, $Q_{ПМ,1}$=7,05) с конкурентной неспособностью порядка 7,05/4,04=1,74 раза, что составляет весьма значительную величину;

2. Наряду с восемью позитивными свойствами варианта 2 (из 11 для варианта 1) учтены и имеют критическое значение шесть негативных свойств (аспектов), открывающих широкие возможности «нецивилизованного» технологического заимствования, осуществления аналитической разведки недружественными странами, оказания санкционного давления и информационно-психологического воздействия на авторов (в том числе унижения их достоинства) при отборе материалов к опубликованию, а также возможность рефлексивного и ментального управления процессами развития отечественной науки в целом;

3. Еще большую критичность указанные выше факторы приобретают при открытой публикации таких наукоемких публикаций как авторефераты многолетних целенаправленных диссертационных исследований отечественных авторов, в том числе в узких и специфических областях знаний на прорывных направлениях развития науки, техники и технологий.

С другой стороны, с конкурентным превосходством по данным выполненных квалиметрических полимодельных оценок варианта «3. Технология независимой экспертной квалиметрической аттестации публикаций «КСПР» (конкурентно-способных технологических решений [12-15], $Q_{ПМ,3}$=8,35) порядка 8,35/4,04 = 2,1 раза представляется перспективным совершенствование и развитие национальной системы обеспечения и повышения национальной публикационной активности авторов, технологий независимой квалиметрической оценки и аттестации, ранжирования публикаций авторов по критериям качества с использованием подходов, методов и программных средств обеспечения информационной «прозрачности» экспертизы [8-10] в интересах гарантированного обеспечения информационной безопасности (в том числе в контексте проблем представления российских публикаций [16]) отечественной системы повышения публикационной активности отечественных авторов в сочетании с их реальным стимулированием и организационно-правовым обеспечением.

В этой связи представляется целесообразным рассмотреть возможность поэтапного отказа от безальтернативного признания западных систем рейтингования научно-образовательных организаций и оценивания эффективности научных исследований, способствующих перекачке в зарубежные базы данных стратегических информационных ресурсов, а также применения освоенных ранее эффективных методов и практики стимулирования публикационной активности авторов статей, книг, изобретений, докладов, мастер-классов, руководства научными школами с выплатой на конкурсной основе авторских гонораров, оплаты участия в конференциях в сочетании со снижением плановой учебной нагрузки в качестве компенсации соответствующих трудозатрат и других результативных и многократно апробированных способов поощрения.

Представленные данные и полученные квалиметрические оценки, по мнению авторов, должны послужить количественной основой для критического анализа и пересмотра подхода к организационно-правовому обеспечению системы регулирования публикационной активности отечественных авторов и информационной защиты национальных интеллектуальных ресурсов, направленных на сохранение информационного суверенитета, обеспечение национальных интересов и, в конечном счете, укрепление национальной безопасности России.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А.В., Воробьев В.И. Информационное противоборство: 20 лет концептуального и технологического развития // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 1 / СПОИСУ. – СПб., 2015, с. 153 – 159.
2. Субачев Ю.В. Наукометрические базы данных: полный и актуальный перечень / [Электронный ресурс]. – URL: https://научныепереводы.рф/naukometricheskie-bazy-dannyh/
3. Проблема публикаций в зарубежных научных изданиях / [Электронный ресурс]. – URL: https://bstudy.net/777970/sotsiologiya/problema_publikatsiy_zarubezhnyh_nauchnyh_izdaniyah.
4. Островский А.Н. Зачем и как публиковать научные статьи в иностранных журналах? / Островский А.Н. II Химия и химики. – 2009. – № 2 [Электронный ресурс]. – URL: http://www.library.fa.ru/files/publ6.pdf
5. Погосян А. РАН сообщает о негласных санкциях против российских ученых /Погосян А. // Известия. 2014. – № 92
6. Околонаучный бизнес: масштабы фальсификаций при публикации научных работ / [Электронный ресурс]. – URL: https://habr.com/ru/company/leader-id/blog/526530/
7. Советов Б.Я., Касаткин В.В. Концептуальные основы совершенствования системы подготовки ИТ-специалистов. // Перспективные направления развития отечественных информационных технологий: материалы VI межрегиональной научно-практической конф. Севастополь, 22-26 сентября 2020 г. / Севастопольский государственный университет; науч. ред. Б..В. Соколов. – Севастополь: СевГУ, 2020. – 305 с. С. 5-9.
8. Бобрович В.Ю., Антипов В.В., Смольников А.В., Алексеев А.В., Мусатенко Р.И. Анализ опыта организации ранговой партнерской сертификация качества объектов морской техники / Информационная безопасность регионов России (ИБРР-2015). IX Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2015 г.: Материалы конференции / СПОИСУ. – СПб., 2015, с. 263 – 265.
9. Бобрович В.Ю., Алексеев А.В., Антипов В.В., Смольников А.В. От декларации и сертификации соответствия к цифровизации и интеллектуализации управления качеством и конкурентной способностью морской техники / Актуальные проблемы морской энергетики: материалы десятой международной научно-технической конференции в рамках Пятого Всероссийского научно-технического форума «Корабельная энергетика: из прошлого в будущее». – СПб.: Изд-во СПбГМТУ, 2021, с. 363 – 369.
10. Волков В.И., Тычинин И.Ю., Алексеев А.В. Системные аспекты управления развитием современных критических объектов морской / Санкт-Петербург, 29-31 октября 2014 г.: Материалы конференции \ СПОИСУ. – СПб, 2014. С. 447–448.
11. Микони С.В., Соколов Б.В. Юсупов Р.М. Квалиметрия моделей и полимодельных комплексов : монография С. В. Микони, Б. В. Соколов, Р. М. Юсупов. – М : РАН, 2018. – 314 с.
12. Алексеев А.В., Мусатенко Р.И., Равин А.А., Согонов С.А., Хруцкий О.В. Метод и технология автоматической оценки и мониторинга компетентности и подготовленности экипажа судна / Корабельная энергетика: из прошлого в будущее: материалы Всероссийского межотраслевого научно-технического форума. – СПб.: Изд-во СПбГМТУ, 2017, с. 334 – 338.
13. Алексеев А.В., Согонов С.А., Равин А.А., Хруцкий О.В., Мусатенко Р.И., Потехин В.С. Метод оценки компетентности и подготовленности экипажа судна / Региональная информатика (РИ-2016). Юбилейная XV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2016)». Санкт-Петербург, 26-28 октября 2016 г.: Материалы конференции. \ СПОИСУ. - СПб, 2016, с. 429-430.
14. Алексеев А.В., Сус Г.Н., Ушакова Н.П. Системный анализ и ранжирование качества вариантов интеллектуальной поддержки принятия решений и управления борьбой за живучесть корабля, судна / Материалы 9-й конференции «Информационные технологии в управлении» (ИТУ-2016). – СПб.: АО «Концерн «ЦНИИ «Электроприбор», 4-6.10.2016 г. - Спб., ГНЦ РФ АО «Концерн «ЦНИИ «Электроприбор», 2016, с. 786-790.
15. Алексеев А.В., Равин А.А., Согонов С.А., Хруцкий О.В. Оптимизация процессов управления качеством и конкурентной способностью объектов морской техники и инфраструктуры / International Conference on Naval Architecture and Ocean Engineering. Collection of Pa-pers. Труды Международной конференции по судостроению и океанотехнике: Сборник статей / СПбГМТУ, НТОС им. акад. А.Н. Крылова. – СПб: СПбГМТУ, 2016, с. 14-22.
16. Москалева О.В. Проблемы представления российских публикаций в индексах цитирования и их адекватного учета / [Электронный ресурс]. - URL: https://elar.urfu.ru/bitstream/10995/33920/1/seminar_06.10.15_Moskaleva.pdf

УДК 004.724.4

АЛГОРИТМ АУТЕНТИФИКАЦИИ С ПРИМЕНЕНИЕМ SMART CARD В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ДВОЙНОГО НАЗНАЧЕНИЯ

Доценко Сергей Михайлович, Шаблюк Станислав Маркович
АО «НПО «Импульс»
Киришская ул., 2, Санкт-Петербург,195299, Россия
emails: dotsenko_s@mail.ru, st_shabluk@mail.ru

Аннотация. В данной статье приведены направления применения интеллектуальных карт для обеспечение защищённой аутентификации пользователей автоматизированных систем на современной отечественной элементной базе.

Ключевые слова: носители информации; интеллектуальная карта; современная отечественная элементная база.

SMART CARD AUTHENTICATION ALGORITHM IN AUTOMATED DUAL-USE SYSTEMS

Dotsenko Sergey, Shablyuk Stanislav
JSC «NPO «Impuls»
2 Kirishskaya St., St. Petersburg, Russia, 195299
emails: dotsenko_s@mail.ru, st_shabluk@mail.ru

Abstract. This article presents the directions of application of smart cards for providing secure authentication of users of automated systems on the modern domestic element base.

Keywords: data carriers; an intelligent map; a modern domestic element base.

Введение. Современная отечественная элементная база позволяет создавать компактные защищенные (в том числе и от внешнего воздействия) носители информации с встроенным микропроцессором. На рис. 1 представлена интеллектуальная карта (smart card) разработки АО «НПО «Импульс».

Рис. 1. Общий вид интеллектуальной карты

Применение исключительно отечественной элементной базы позволяет обеспечить полную независимость от поставки импортных комплектующих и сертифицировать СЗИ на базе данных карт для применения в РФ, как альтернативу модельному ряду Рутокен.

Одним из направлений применения интеллектуальных карт является обеспечение защищенной аутентификации пользователей автоматизированных систем. Наличие встроенного в карту процессора и памяти делает возможным выполнение криптографических вычислений прямо в карте без передачи по незащищенным каналам аутентификационной информации.

Предложенный алгоритм позволяет повысить защищённость автоматизированных систем за счёт повышения стойкости процедуры аутентификации.

В состав системы должны входить интеллектуальные карты разграничения доступа (КРД), необходимое количество считывателей, сервер доступа (СД) и АРМ оператора системы. Сервер доступа может быть задублирован. На рис. 2 представлена структура СЗИ на базе КРД.

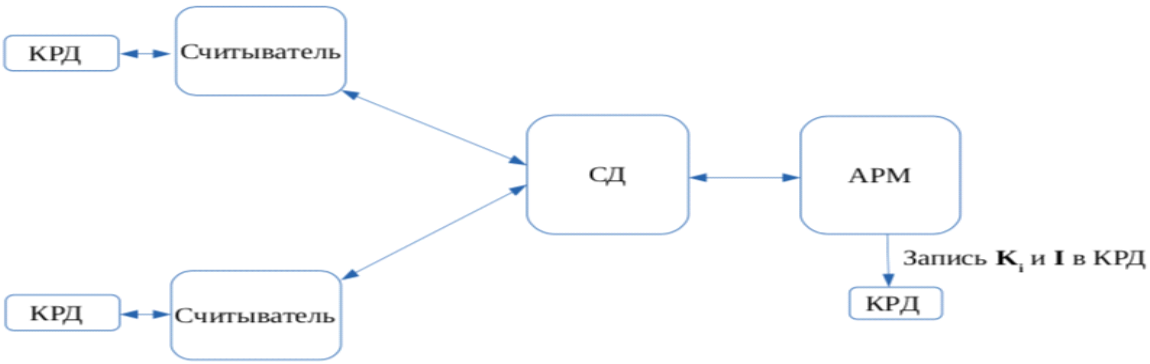


Рис. 2. Структура СЗИ с применением интеллектуальных карт КРД

Оператор системы выполняет начальное программирование КРД. При этом, на каждую КРД, используя датчик случайных чисел, генерируется уникальный ключ Ki (не менее 8 байт) и идентификатор КРД - I (16 байт). После проверки на уникальность ключ Ki и идентификатор I записываются на КРД и сохраняются в базе данных пользователей, которая создаётся заранее.

При вставке КРД в считыватель стартует внутренний микроконтроллер КРД. При загрузке проверяется целостность программного кода, ключа K_i и идентификатора I во flash-памяти КРД криптостойким алгоритмом [1-4].

При успешном результате контроля целостности, идентификатор I передаётся через считыватель на сервер доступа СД. СД, используя датчик случайных чисел, генерирует случайную последовательность S_1, длиной не менее длины ключа K_i, по I из базы данных выбирается K_i и шифруется с использованием ключа K_i заданным криптоалгоритмом (например, Магма, Кузнечик или другой). Результат шифрования $S_ш$ передаётся в КРД. Полученная последовательность в КРД расшифровывается в последовательность S_2, которая передаётся обратно

на СД. На СД сравниваются исходная последовательность с полученной от КРД. Если результат сравнения положителен – процедура аутентификации завершается успехом. В противном случае- КРД блокируется.

При этом, ключ K_i не передаётся между КРД и считывателем, повышая устойчивость к взлому.

Учитывая, что при каждой авторизации генерируется новая случайная последовательность, обмен данными между КРД и считывателем будет уникальным на каждом сеансе авторизации. На рис. 3 представлена Блок-схема описанного алгоритма.

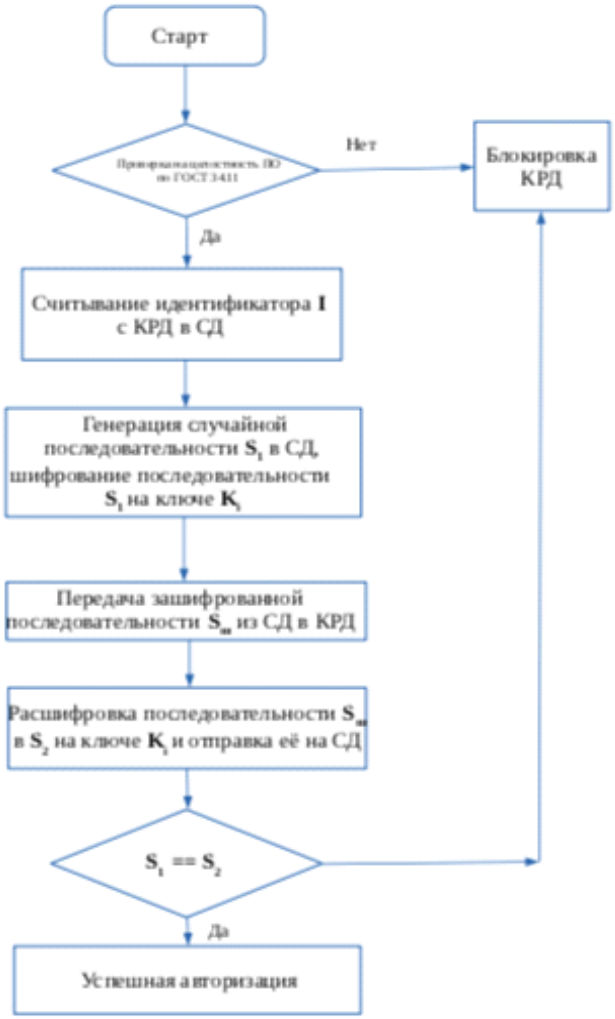


Рис. 3. Блок-схема алгоритма аутентификации с применением КРД

Настройка стойкости алгоритма к взлому может производиться путем выбора генератора случайных чисел, криптоалгоритма, максимального числа попыток аутентификации до блокировки КРД.

Предлагаемый алгоритм может быть применен не только в системах специального назначения, обрабатывающих сведения, составляющие государственную тайну, но и в критичных областях промышленности.

Заключение. Таким образом, применение исключительно отечественной элементной базы при разработке КРД позволяет обеспечить полную независимость от поставки импортных комплектующих и сертифицировать СЗИ на базе данных карт для применения в РФ.

СПИСОК ЛИТЕРАТУРЫ

1. Р 1323565.1.022-2018 Информационная технология(ИТ). Криптографическая защита информации. Функции выработки производного ключа.
2. Р1323565.1.006-2017 Информационная технология (ИТ). Криптографическая защита информации. Механизмы выработки псевдослучайных последовательностей.
3. ГОСТ 34.11-2018 Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования.
4. Р 50.1.113-2016. Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования.

УДК 531.011

ВЫВОД ВАРИАЦИОННОГО ПРИНЦИПА ИЗ УРАВНЕНИЙ НЬЮТОНА КЛАССИЧЕСКОЙ МЕХАНИКИ

Логвинов Дмитрий Петрович
Акционерное общество «Научно-производственное объединение «Импульс»
Киришская, ул., 2, Санкт-Петербург, Россия
e-mail: dlogwinow@yandex.ru

Аннотация. В статье рассматривается последовательный математический вывод принципа наименьшего действия из уравнений классической механики. На каждом шаге вывода обсуждаются лежащие за ним математические вопросы.

Ключевые слова: классическая механика; вариационный принцип; принцип наименьшего действия; уравнения Ньютона.

DERIVATION OF THE LAST ACTION PRINCIPLE FROM NEWTON'S EQUATIONS

Logvinov Dmitrii
Joint Stock Company «Scientific and Production Association» «Impulse»
2 Kirishskaya St., St. Petersburg, Russia, 195299
e-mail: dlogwinow@yandex.ru

Abstacts. The article considers a consistent mathematical derivation of the last action principle from the equations of classical mechanics. At each step of the output, the underlying mathematical issues are discussed.

Keywords: classical mechanic; last action principle; Newton's equation.

Введение. Практическое использование космических аппаратов основано на разработанной аппаратуре связи с ними. Это не только обмен прикладными и служебными данными, но и необходимость постоянного отслеживание местоположения космического аппарата от старта до его выхода из строя. Высокочастотные средства радиосвязи требуют не только точного наведения, но и возможности предсказания координат. Излагаемый в статье математический подход, возможно, позволит лучше осознать связь уравнений Ньютона и метода наименьшего действия, но, вдобавок, показывает метод для улучшения вычислений координат движущегося тела при наличии трения. Принцип наименьшего действия используется в теоретической механике для быстрого вывода дифференциальных уравнений, которые уже используются для решения практических задач. Само же обоснование принципа относят чуть ли не к области философии. На самом деле уравнения и вариационный принцип являются просто различными точкам зрения на процесс реального развития механической системы. Только уравнения смотрят с локальной точки зрения, а вариационный принцип позволяет сделать то же с глобальной точки зрения. Простой математический метод получения функционала действия из уравнений Ньютона позволяет лучше ощутить взаимосвязь этих двух подходов и, возможно, позволит более наглядно численно оценить влияние дополнительных локальных факторов на эволюцию системы в целом.

Вариационный принцип, он же принцип наименьшего действия утверждает, что материальные тела перемещаются по наикратчайшему пути. Слова «наикратчайший путь» нуждаются в уточнении, но само утверждение кажется понятным и было сформулировано без детальной формализации еще во времена античной цивилизации. Сейчас тяжело установить уровень развития науки в те древние времена, но по мере развития науки нового времени (нашей цивилизации) наши оценки достижений ученых прошлого все более повышаются [1]. Во всяком случае считается, что во времена Аристотеля господствовал атомизм, то есть все окружающее считалось состоящим из мельчайших неделимых элементов, а причиной перемещения тел считали приложенные к ним силы. Телега двигалась тем быстрее, чем большую силу прикладывал впряженный осел. Если силы осла кончались, воз останавливался.

Перед учеными древности вставали две проблемы. Во-первых, с точки зрения атомизма было непонятно, как в геометрии из счетного числа точек можно было построить непрерывный отрезок, соответственно в физике непонятна концепция скорости, то есть как летящая стрела переходит из одной дискретной точки пространства в другую. Без решения этих проблем невозможно было построить науку механику в части динамики.

Невзирая на то, что античные ученые знали понятие бесконечности и умели интегрировать, считается, что решение проблем с бесконечностями как большими, так и малыми является достижением ученых нового времени, которые, начиная с Галилея, осознали, что сила пропорциональна не скорости, а ускорению тела, что остановка движущейся без осла телеги обеспечивается силой трения о дорогу. Исаак Ньютон уточнил этот закон, постулировав существование инерциальной системы отсчета, в которой данное утверждение верно, оскольку для первоначальной формулировки утверждения существовало опровержение в виде бесконечно долго вращающихся вокруг Солнца планет.

Определив закон связи ускорения $\vec{a}$ материальной точки массы m под действием силы $\vec{F}$ в виде

$$m\vec{a} = \vec{F},$$

Ньютон предложил идею, которая позволила использовать распространить использование данного уравнения не только для материальных точек, но для сложных тел, а механику сделать самодостаточной наукой. Все тела можно представить в виде взаимодействующих материальных точек. Внешнее воздействие на тело можно разнести на составляющие его элементы, а неизвестное взаимодействие элементов тела между собой Ньютон предложил счесть взаимно компенсирующим, так называемый закон действия и противодействия: два тела влияют друг на друга одинаковыми по величине силами, направленными вдоль оси их расположения, но в противоположном направлении друг к другу. Реальной компенсации этих сил нет, так как приложения этих сил приходятся на разные тела, но если тела сливаются, то силы взаимно уничтожаются.

Идея использовать материальные точки кажется аналогичной атомистической теории древних греков, но в Новом времени ученые стали более неразборчивыми в использовании понятий и использовали материальные точки только в виде математического способа для вычислений, не привязывая их к атомам. Но после открытия атомов в XX веке такое отождествление возможно. С тех самых пор, как царица всех наук математика стала служанкой физики, любое словесное понимание природы физик записывает дополнительно в виде математической формулы. В нашем случае имеется тело, разбитое на некоторое неопределенное, но заданное количество взаимодействующих материальных точек. Если пронумеровать все точки числами от 1 до N и, соответственно, пронумеровать все характеристики этих точек, а именно: массы точек m_n, координаты положения точек $\overrightarrow{r_n}$, скорости $\overrightarrow{v_n} = \dot{\overrightarrow{r_n}}$ и ускорения $\overrightarrow{a_n} = \ddot{\overrightarrow{r_n}}$ движения точек, действующие на них силы $\overrightarrow{F_n}$, , то получается набор уравнений

$$\left\{m_n \cdot \ddot{\overrightarrow{r_n}} = \overrightarrow{F_n}\right\}_{n=1..N}$$

Введя величину $\overrightarrow{p_n} = m_n \cdot \dot{\overrightarrow{r_n}}$, называемую количеством движения или импульсом (латинское слово impulsus означает толчок), получаем окончательную форму уравнений

$$\left\{\dot{\overrightarrow{p_n}} = \overrightarrow{F_n}\right\}_{n=1..N}$$

Величина силы может (и как правило) зависит от положения точки и времени, поэтому было бы правильно писать явно функцию$\vec{F}(\vec{r}, t)$, но обычно данный факт всегда подразумевают.

Зная начальные координаты и скорости точек, а также действующие силы, можно с помощью данного уравнения рассчитать эволюцию системы точек для любого будущего. Конец, классическая механика объясняет весь мир. Именно в этом смысле механика стала замкнутой, то есть самодостаточной теорией.

Для целей статьи ограничимся важным частным случаем движения одной материальной точки под действием внешних сил. Для того, чтобы определить окончательное положение катающегося по земной поверхности шарика, совершенно не обязательно решать данные уравнения. На шарик действует притяжение Земли, трение и реакция опоры (поверхности), не дающая шарику проваливаться. Реакцией опоры всегда перпендикулярна плоскости касания, ее величина может быть любой, но такой, чтобы обозначить невозможность ухода с поверхности. Любое возможное перемещение шарика перпендикулярно этой силе, поэтому можно убрать ее, умножая уравнение на вектор возможного перемещения

$$\dot{\vec{p}} \cdot \overrightarrow{dr} = \vec{F} \cdot \overrightarrow{dr}$$

Получается, что для понимания движения шарика по поверхности, нужно не знание вектора силы в каждой точке поверхности, а знание скалярной величины $\vec{F} \cdot \overrightarrow{dr}$. В некоторых случаях эта кажущаяся непонятной величина упрощается. Случай такого упрощения называется потенциальными силами, когда в процесс движения сумма значений величин по пути движения не зависит от пути движения. Иначе говоря, определив некоторый путь в виде функции $\vec{r} = \vec{\gamma}(t)$, мы можем посчитать величину

$$\int_{\gamma} \vec{F}\,(\vec{r}) \cdot d\vec{r}$$

Если на двух любых различный путях с одинаковыми начальным и конечным положением данная сумма одинакова, то и на любом замкнутом пути интеграл будет принимать нулевое значение

$$\oint \vec{F}\,(\vec{r}) \cdot \overrightarrow{dr} = 0$$

И наоборот, если на любом замкнутом пути круговой интеграл нулевой, то интеграл по некоторому пути будет зависеть только от концов пути. Такая функция

$$G = \int_{\gamma} \vec{F} \cdot \overrightarrow{dr}$$

будет являться первообразной к $\vec{F}(\vec{r})$, то есть $dG = \vec{F} \cdot \overrightarrow{dr}$.

В механике используют противоположную величину

$$U\left(\overrightarrow{r_0}, \overrightarrow{r_1}\right) = -\int_{r_0}^{r_1} \vec{F} \cdot \overrightarrow{dr}\,,$$

называемую потенциальной энергией. Точка выбора начальной точки приводит в силу потенциальности силы только к изменению функции U на постоянную величину. Поэтому фактически U зависит только от одной переменной.

Смысл потенциальной энергии заключается в том, что на тело действует сила в сторону уменьшения потенциальной энергии аналогично тому, что шарик на склоне скатывается под гору.

Таким образом, зная потенциал силы, можно определить куда скатится потенциальная точка, если скорость ее станет нулевой, – в точку минимума потенциала U.

Минимум функции является частным случаем экстремума, когда уход от этой точки незначительно изменяет величину функции, ищется экстремум по известному правилу

$$\nabla U = 0$$

Возвращаясь к уравнению Ньютона, можно рассмотреть

$$\int_\gamma \dot{\vec{p}}\,\overrightarrow{dr} = \int_\gamma \ddot{\vec{r}}\,\overrightarrow{dr}.$$

Так как $\overrightarrow{dr} = \dot{\vec{r}}dt$, то интеграл считается при любом пути следования и будет равен изменению кинетической энергии на пути γ из точки γ_0 в точку γ_1

$$W = \frac{m\dot{\vec{r}}^2}{2}$$

$$m\int_\gamma \ddot{\vec{r}}\,\overrightarrow{dr} = m\int_\gamma \ddot{\vec{r}}\,\dot{\vec{r}}dt = \int\left(\frac{d}{dt}\frac{m\dot{\vec{r}}^2}{2}\right)dt = \frac{m\dot{\vec{r}}^2}{2}\Bigg|_{\gamma_0}^{\gamma_1} = W|_{\gamma_0}^{\gamma_1}$$

Получается известное из школьной программы уравнение сохранения энергии: сумма кинетической и потенциальной энергии постоянна (при отсутствии трения) E = W+U = const.

Переписывая уравнение Ньютона в другом виде

$$m\ddot{\vec{r}} - \vec{F} = 0,$$

получаем очень похожее на статический случай уравнение: к различным силам добавляется еще одна сила, называемая силой инерции. Как будто бы тело сопротивляется изменению своего движения, а величина сопротивления и отражает инерцию движения.

Аналогично предыдущим рассуждениям, будем рассматривать сумму величин $m\ddot{\vec{r}} - \vec{F}$ вдоль всего пути движения. Но если в случае статики время нас не интересовало, то теперь необходимо контролировать и время. Поэтому интегралов будет два: сначала по пути от начальной точки γ_0 до точки $q = \gamma(\tau)$, потом все интегрируем по времени до конечной точки t_1

$$S[\gamma] = \int_{t_0}^{t_1} dt \int_{\gamma_0}^{q(t)} \overrightarrow{dr}\left(m\ddot{\vec{r}} - \vec{F}\right)$$

Величина зависит не от переменных, как обычная функция, а от целого пути, поэтому называется функционалом действия.

Если материальная точка движется по правильному пути, который соответствует закону Ньютона, то подынтегральное выражение обращается в ноль. Но если путь γ отличается от правильного, то данная величина станет больше. Вышеуказанное утверждение называется вариационным принципом механики или принципом наименьшего действия. Однако в таком виде вариационный принцип является лишь повтором уравнения Ньютона. Нетривиально то, что функционал действия можно преобразовать к другому виду, который приводится в книгах по теоретической механике и используется наоборот, то есть сначала выписывается функционал действия, а потом из него получают уравнения Ньютона [2-4].

Воспользовавшись определениями кинетической и потенциальной энергий, интеграл превращается в

$$S[\gamma] = \int_{t_0}^{t_1} dt\,(W+U)|_{\gamma_0}^{q}$$

Очевидно, что принцип наименьшего действия соответствует тому, чтобы материальная точка двигалась по пути минимального возрастания функции энергии. Однако, если в двойном интеграле переставить порядок интегрирования

$$\int_{t_0}^{t_1} d\,\tau \int_{t_0}^{\tau} dt\left(-\vec{F}\cdot\dot{\vec{r}}\right) = \int_{t_0}^{t_1} dt \int_{t}^{t_1} d\,\tau\left(-\vec{F}\dot{\vec{r}}\right) = \int_{t_0}^{t_1} dt\,U|_{q}^{\gamma_1},$$

то функционал действия запишется в виде

$$S[\gamma] = \int_{t_0}^{t_1} dt\left(W|_{t_0}^{\tau} + U|_{\tau}^{t_1}\right)$$

Учитывая, что

$$U|_{t_0}^{t_1} = U|_{t_0}^{\tau} + U|_{\tau}^{t_1}$$

получается выражение для действия в более привычном виде

$$S[\gamma] = \int_{t_0}^{t_1} dt \left((W - U)|_{t_0}^{\tau} \right) + U|_{\gamma_0}^{\gamma_1} \cdot (t_1 - t_0)$$

Если начальные и конечные точки пути фиксированы, а ищется путь, доставляющий функционалу наименьшее действие, то дополнительный член не оказывает никакого влияние на вид пути и функционал равносилен стандартному виду в форме Лагранжа

$$S[\gamma] = \int_{t_0}^{t_1} dt \, (W - U)$$

Таким образом, поставленная цель выполнена, явно указаны математические операции и стоящие за ними понятия, позволяющие из уравнения Ньютона в случае потенциальной силы получить функционал действия. С одной стороны, результат обосновывает вариационный принцип, с другой стороны, указанный путь вывода позволяет сделать очевидным вид функционала и его связь с полной энергии точки вдоль маршрута движения.

Помимо отмеченных результатов имеется дополнительное достижение, имеющее практическое применение. Как отмечалось выше в статье, если сила имеет непотенциальную часть (трение), то в функционале действия возникает дополнительный член

$$S[\gamma] = S_0[\gamma] + S_1[\gamma].$$

Если пренебречь дополнительным членом, то мы попадаем в классическую ситуацию классической механики, когда надо по функционалу получить уравнения и их решить. Но наличие в функционале явного члена, учитывающего трение, позволяет двигаться другим путем. Получим каким-либо образом параметрическое решение, например, из решения вышеупомянутых дифференциальных уравнений, но можно взять произвольную похожую на реальную функцию движения $\gamma_0(t, a)$. Главное, чтобы были дополнительные параметры a для последующей подгонки. Такими параметрами в случае космического аппарата могут быть параметры орбиты или значения координат и скоростей в какой-либо точке. Подставив данную функцию в функционал, получаем функционал действия в виде

$$S_0[\gamma_0(a)] + S_1[\gamma_0(a)].$$

Использованная функция доставляет функционалу определенное значение, зависящее от параметров, то есть получается обычная функция от чисел-параметров. Получение минимума от функции по параметрам является простой операцией, но она дает, вследствие того, что используется вариационный принцип, наилучшую поправку к реальному уравнению движения. Величина уклонения от верного решения контролируется с помощью вычисления значения функционала действия при различных параметрах. Процесс подгонки можно повторять, позволяя зачастую получать приемлемую точность в определении эволюции системы без сложного решения в лоб дифференциальных уравнений.

Заключение. Рассмотренный в статье метод поправок к фунционалу действия, учитывающих вклад не потенциальных сил, теоретически позволяет находить решения в классической задаче об эволюции механической системы, причем ранее этот метод считался непригодным для проведения вычислений при таких условиях. Учитывая, что данный метод вычислений оценивает движение системы в целом и теоретически дает наилучшую поправку при последовательном приближении к искомому решению, имеет смысл применять его для реальных расчетов координат движения космических аппаратов с проверкой его пригодности на практике.

СПИСОК ЛИТЕРАТУРЫ

1. Мах Э. Механика. Историко-критический очерк ее развития – Ижевск: Ижевская республиканская типография, 2000. 456 с.
2. Поллак Л.С. Вариационные принципы механики – М: Либроком, 2010. 600 с.
3. Ланцош К. Вариационные принципы механики – М: Физматгиз, 1965. 408 с.
4. Ландау Л.Д., Лифшиц Е.М. Курс физики. Том I. Механика.

УДК 004.72

АНАЛИТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ ВЕРОЯТНОСТИ ТРАНСФОРМАЦИИ СООБЩЕНИЙ В РАДИОКАНАЛАХ СПЕЦИАЛЬНЫХ СИСТЕМ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

Михайленко Евгений Иванович
Акционерное общество «Научно-производственное объединение «Импульс»,
Киришская ул., 2, Санкт-Петербург, Россия
email: proimpuls@peterlink.ru

Аннотация. В статье рассмотрена аналитическая модель оценки вероятности трансформации сообщений в радиоканалах специальных систем критических инфраструктур.

Ключевые слова: вероятность трансформации сообщения*;* вероятность необнаруженной ошибки.

ANALYTICAL MODEL OF MESSAGE TRANSFORMATION PROBABILITY ESTIMATION IN RADIO CHANNELS OF SPECIAL CRITICAL INFRASTRUCTURE SYSTEMS

Mihailenko Evgeny
Joint-Stock Company «Research-and-Pproduction Union «Impuls»
2 Kirishskaya St., St. Petersburg, Russia, 195299
email: eimihailenko@yandex.ru

Abstract. The article considers an analytical model of the interface path of special systems of critical infrastructures taking into account the priority of data.

Keywords: probability of message transformation; probability of undetected error.

Введение. В соответствии с предъявляемыми к связи требованиями, системы критических инфраструктур должны обеспечивать своевременный, безопасный и достоверный информационный обмен с использованием всех ресурсов телекоммуникационных сетей, в том числе, при использовании радиоканалов. Телекоммуникационные сети связи являются составной частью единого информационного пространства автоматизированных систем управления. При этом приходится решать вопросы, связанные с реализацией заданных требований по трансформации сообщений для обеспечения безопасности функционирования этих автоматизированных систем. Разработка аналитической модели оценки вероятности трансформации сообщений позволяет проверить эти требования на этапах разработке изделий и их испытаний.

Оценка достоверности обмена информацией определяется путём определения вероятности появления сообщений с необнаруженными ошибками.

Сообщение считается трансформированным, если оно содержит необнаруженные ошибки и семантическая проверка не позволяет обнаружить ошибку, т.е. сообщение трансформируется в другое сообщение.

Оценка вероятности появления сообщения с необнаруженными ошибками производится по выражению [1-4]:

$$Рно = Рно\ спец^* Рно\ к\ ^*Рно\ с^* Рно\ тр,$$

где:

Рно – вероятность трансформации сообщения;

Рно спец – вероятность необнаруженной ошибки на выходе специального уровня;

Рно к – вероятность необнаруженной ошибки в кадрах, состоящих из линейных блоков, поступивших на канальный уровень из каналов связи;

Рно с – вероятность необнаруженной ошибки в пакетах сетевого уровня;

Рноп – вероятность необнаруженной ошибки в сообщениях на транспортном уровне.

При расчётах вероятностей того, что в кодовой комбинации помехоустойчивого кода длиной n будет не менее одной P(≥1, n) или m ошибок P(≥m, n) пользуются верхним граничным значением вероятности:

$$P(\geq 1, n) \leq n^{1-\alpha} \times p_{ош} = Рст + Рош,$$

$$P(\geq m, n) \leq (n/m)^{1-\alpha} \times p_{ош},$$

где:

α и $p_{ош}$ - параметры дискретного канала связи;

α - показатель группирования ошибок;

$p_{ош}$ – вероятность ошибки двоичного элемента.

Для расчёта Рно к - вероятности ошибочного приёма кодовой комбинации помехоустойчивого кода (n,k) с минимальным кодовым расстоянием d min используют формулу:

$$Р\ но\ к(\geq d\ min, n) \leq (n/d\ min)^{1-\alpha} \times p_{ош},$$

где:

Р но к(≥d min, n) – вероятность ошибки или вероятность того, что в кодовой комбинации длиной n число ошибок не менее d min.

Для кадров из k - линейных блоков Рно кk определяется

$$Рно\ кk = 1-(1- Рно\ к)^k;$$

где:

k – количество линейных блоков в кадре;

Режим приёма кадра в радиоканалах может использовать приём по методу мажоритарного исправления.

В тех случаях, когда мажоритарной обработке подвергается (2m– 1) повторений, $p_{ош\ m}$ – вероятность искажения двоичного элемента может быть получена из следующего приближенного выражения (при мажоритарной обработке, например, 5 из 11, m = 5) [5]:

$$p_{ош\ m} = C^{m}_{2m-1}\, p_{мош}\ .$$

Если на транспортном и сетевом уровнях защита от ошибок осуществляется с помощью порождающих полиномов 16-й степени, вероятности Рно с и Рно тр будут равны по 2^{-16} или, переходя к десятичному основанию, $10^{-16\ \log 2} = 10^{-4,82}$.

Кроме того, дополнительно, после транспортного уровня, выполняется семантическая проверка поступившего сообщения, что ещё уменьшает вероятность трансформации.

Заключение. Данная аналитическая модель оценки вероятности трансформации сообщений в радиоканалах специальных систем критических инфраструктур позволяет оценивать, в том числе, и мажоритарную обработку принимаемых сообщений.

СПИСОК ЛИТЕРАТУРЫ

1. Мизин И.А. и др., Протоколы информационно-вычислительных сетей, Москва, Радио и связь, 1990г.
2. Д. Бертсекас, Р. Галагер, Сети передачи данных, М., Мир, 1989г.
3. Вентцель Е.С. Теория вероятностей, Изд. «Наука», 1969г.
4. Захаров А.И. Основы передачи данных. ВАС, 1985. - 157 с.
5. Ключко В.И. Защита от ошибок при обмене информацией в АСУ. – М.: МО, 1980. – 256 с.

УДК 004.75

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОТЕЧЕСТВЕННЫХ И ЗАРУБЕЖНЫХ МОДЕЛЕЙ СТАНЦИЙ ТРОПОСФЕРНОЙ СВЯЗИ. ПЕРСПЕКТИВЫ РАЗВИТИЯ

Плотников Николай Николаевич
310 военное представительство МО РФ
Киришская ул., 2, Санкт-Петербург, Россия
emails: plotniy85@mail.ru

Аннотация: Предлагается сравнительный анализ отечественных и зарубежных моделей станций тропосферной связи. Перспективы развития.

Ключевые слова: тропосферная связь; станции тропосферной связи; пропускная способность.

COMPARATIVE ANALYSIS OF DOMESTIC AND FOREIGN MODELS OF TROPOSPHERIC COMMUNICATION STATIONS. PERSPECTIVES OF DEVELOPMENT

Plotnikov Nikolay
310 military representation of MD RF,
2 Kirichskay str., St. Petersburg, Russia
emails: plotniy85@mail.ru

Abstract: A comparative analysis of domestic and foreign models of tropospheric communication stations. perspectives of development.

Keywords: tropospheric communication; throughput; tropospheric communication stations.

Введение. Системы тропосферной связи появились в 1950-х годах в период интенсивной стратегической конкуренции между странами НАТО и странами, входящими в Организацию Варшавского договора, до появления спутниковой связи. Такие системы широко использовались США и Советским Союзом, и в меньшей степени их союзниками, для обеспечения каналов связи, как правило, в малонаселенных районах. Советские войска развернули обширную сеть радиорелейных станций тропосферной связи через северную Сибирь и Дальний Восток, в то время как США развернули обширную сеть вдоль линий раннего радиолокационного обнаружения, а также через Аляску и Алеутские острова. Впоследствии эти стационарные сети были дополнены мобильными тактическими системами, предназначенными для обеспечения цифровой магистральной связи для элементов маневрирования сухопутных войск.

Тропосферная связь активно используют армии США и стран НАТО. Так, известная тропосферная станция AN/TRC-170 (V3) с цифровым модемом CS67200i обеспечивает скорость передачи данных от 2 до 22 Мб/с. На вооружении стран НАТО и Англии до сих пор находится ТС типа Н7450 разработки фирмы Маркони, которая обеспечивает цифровую засекреченную связь в оперативно-тактическом звене сухопутных войск. Современная тропосферная станция AN/TSC-198 (V3), которая совместима с AN/TRC-170 (V3) (M3) обеспечивает скорость до 50 Мб/сна расстоянии до 150 миль.

ТС типа «ТОРФ» Р-412станции обеспечивали на интервалах до 150-180 км передачу информационного потока со скоростью до 1 Мбит/с.

МНИРТИ в 1981 году развернул мобильную тактическую систему тропосферной системы Р-423-1 Бриг-1. Система обеспечивает пропускную способность 2048 кБ/с до 150 км или до 64 кБ/с до диапазона 230 км. Система работает в двух диапазонах частот, на частотах 4,435-4,55 ГГц и 4,630-4,450 ГГц с использованием 220 подканалов. На выходе передатчика 1,5 киловольт. Цифровые интерфейсы предоставляются со скоростью 48 кБ/с, 480 кБ/с и 2048 кБ/с.

Самый последний вариант Р-423-2А, предназначенный для замены системы тропосферной системы Торф,Торф - 2А, работает в тех же диапазонах, что и вариант -1. Мощность упомянутого передатчика составляет 220 Вт, а приемник - 7 дБ. Система развернута на грузовике КАМАЗ-4310 с использованием буксируемого электрогенератора 2х8-Т400-1ВПС.

Приведенные показатели скорости передачи данных и дальности для Р-423-2А являются полнодуплексными 230 км в 1,2 кБ/с, 210 км - 2,4 кБ/с, 190 км - 4,8 кБ/с, 170 км - 9,6 килобит / с, 130 км на 48 кБ/с, 90 км на 240 кБ/с и полудуплекс 140 км на 480 кБ/с.

Китайские специалисты в области проектирования и изготовления станций тропосферной связи поставляют на рынок станцию тропосферной связи TS-504.Анализ задекларированных характеристик в технической брошюре CETC для TS-504 показал, что эта система является китайским аналогом серии Р-423-1, отличие состоит лишь в конструкции антенн, и, как уверяют китайские специалисты, в более продвинутых методах модуляции. Эта система была представлена во время военного парада в Китае в 2009 году и, как известно, была экспортирована в Пакистан. TS-504 часто используется для обеспечения цифровой связи.

В конце 50-х годов была разработана 60-канальная аппаратура ТРРЛ первого поколения «Горизонт-М», где сигналы многоканальной телефонии передавались с использованием частотной модуляции и применялся четырехкратный разнесенный прием (двукратный по частоте и двукратный по пространству). Радиорелейная линия работала в диапазоне частот 2 ГГц. На этом оборудовании была построена линия связи «Север», обеспечивающая надежной телефонной связью населенные пункты, расположенные за Полярным кругом, в районах Камчатки и Дальнего Востока.

До того времени весьма ненадежная связь поддерживалась с ними с помощью двух- и четырехканальных КВ линий связи.

В период 1981-1984 гг. Были разработаны и развернуты радиорелейные станции для радиолокационных станций Р-444 Эшелон и Р-444-7,5. Эти конструкции обеспечивали пропускную способность 1 мБ/с до 130-150 км или 48 кБ/с до 230 км.

В России ведутся работы по совершенствованию данного типа связи. Созданные во второй половине 20-ого века тропосферные радиостанции (ТРС) на интервалах 100–250 км обеспечивали передачу на скорости до 2 мБ/с. Для компенсации затухания на трассе в 60-80 дБ использовались мощные передатчики и большие антенны, поэтому техника ТРС была сложной, дорогостоящей, энергоемкой, в силу чего её развитие в России в 90-е годы замедлилось, появилась необходимость создания недорогих малогабаритных станций ТРС с низким энергопотреблением. Такими ТРС стали разработанные в рамках инициативных ОКР станции ТРС «Сосник-4ПМ» производства АО «НПП «Радиосвязь») и «Ладья» производства МНИИРС. На линиях протяженности более 100 км они устойчиво работают на скоростях передачи от 64 до 512 кБ/с. Данные ТРС выполняются также и в переносном варианте.

Сравнение характеристик отечественных и зарубежных малогабаритных станций тропосферной связи представлено в таблице 1.

Таблица 1

№ пп	Технические характеристики	«Ладья»	«TELOS» Raytheon США	«TROPO» (ЗТ) ComtechСША	Р−423−ПМ
1	Диапазон рабочих частот, ГГц	4,4 − 5,0 с шагом 10 МГц	14,0	4,4; 5,0	4,4 − 4,5(«Н») 4,9 − 5,0 («В»)
2	Принцип разделения приёма и передачи Защитный разнос приёма и передачи, МГц	временной 0	частотный неизвестен	частотный неизвестен	частотный 500
3	Мощность передатчика, Вт	43	250	неизвестна	80
4	Потребляемая мощность, Вт	350 − 370	~ 2000	неизвестна	700
5	Диаметр антенны, м	1,2	0,75	1,2; 2,0	1,5
6	L 1го интервала тропосферной связи, км для*): 1х64 кбит/с 4х64 кбит/с 8х64 кбит/с 1000 кбит/с	 180 140 105 90	≥64Ethernet	неизвестно	неизвестно
7	Передаваемая информация (сетевые подключения).	1−8х64 кбит/с Ethernet10/100	RS530/422 Ethernet10/100	RS530/422 Ethernet 10/100	через И331 Б отсутствует
8	Масса без транспортной тары, кг	~ 90	200 в упаковках	неизвестна	190

*) Дальность тропосферной связи (L) приведена исходя из пропускной способности станций.

На выставке Связь 2021 компания «Микроволновая электроника» представила новую революционную разработку - тропосферную станцию «Гроза». Холдинг «Росэлектроника» (Ростех), планирует организовать в 2022 г.

серийное производство цифровых помехозащищённых станций тропосферной связи «Гроза». Тропосферная станция позволит обеспечить связью труднодоступные районы в горной местности, вдоль береговых линий, на Крайнем Севере и в других удалённых точках страны. Тропосферная система связи «Гроза» предназначена для организации мультисервисной цифровой радиосвязи стационарных объектов на расстояниях до 200 км при отсутствии прямой видимости между антенными постами с максимальной скоростью передачи до 50 Мбит/с. «Гроза» имеет также существенные преимущества перед спутниковой связью по части задержек передачи информации и стоимости эксплуатации. Для отдалённых более чем на 200 км объектов предлагается каскадное размещение линий связи [1, 2].

Заключение. В современных станциях заложена возможность комбинировать тропосферную и спутниковую связь. Расчеты показывают, что при действующих темпах удешевления электроники, уменьшения линейных размеров станций, внедрения новейших разработок станции тропосферной связи более выгодны в эксплуатации, нежели наращивание спутниковой группировки.

СПИСОК ЛИТЕРАТУРЫ

1. Форум «Связь-2021, http://www.cviaz-expo.ru.
2. Система тропосферной связи «Гроза», http://www.rolos.news.

УДК 654.16

КРИТИЧЕСКИЕ СИСТЕМЫ. МЕТОДИКА ОБОСНОВАНИЯ ВАРИАНТОВ РАЦИОНАЛЬНОГО ТЕХНИЧЕСКОГО ОБЛИКА ИЗДЕЛИЯ

Филиппов Сергей Владимирович
Акционерное общество «Научно-производственное объединение «Импульс»,
Киришская, ул., д. 2, Санкт-Петербург, Россия
emails: proimpuls@peterlink.ru

Аннотация. Рассмотрена методика обоснования выбора вариантов рационального технического облика изделия при известном варианте «эталонного» изделия с известными характеристиками (для сравнения) на основе определения технического облика изделия в соответствии с ГОСТ РВ 15.002-2004 для однотипных изделий в формализованном виде на основе теории множеств.

Ключевые слова: критические территориально-распределенные системы управления; методика обоснования вариантов; технический облик изделия.

CRITICAL SYSTEMS. METHODOLOGY OF SUBSTANTIATION OF VARIANTS OF THE RATIONAL TECHNICAL APPEARANCE OF THE PRODUCT

Filippov Sergey
Joint-Stock Company «Research-and-Pproduction Union «Impuls»
2 Kirishskaya St., St. Petersburg, Russia, 195299
emails: proimpuls@peterlink.ru

Annotation. The method of substantiating the choice of options for the rational technical appearance of the product with a known version of the «reference» product with known characteristics (for comparison) is considered on the basis of determining the technical appearance of the product in accordance with GOST RV 15.002-2004 for single-type products in a formalized form based on set theory.

Keywords: critical geographically distributed control systems; methodology for justifying options; technical appearance of the product.

Введение. В статье рассматривается методика обоснования вариантов без привязки к конкретным изделиям, а только исходя из определения технического облика изделия, данного в ГОСТ РВ 15.002-2004. В статье сведены вместе технические характеристики и стоимости необходимых доработок вариантов изделий до характеристик «эталонного» изделия. Практическая ценность работы состоит в возможности использования полученных результатов (формулы расчёта) при проектировании указанных систем.

Изделия могут рассматриваться однотипные, т.е. не отличающиеся по области назначения и применения. Область назначения можно охарактеризовать функциональными требованиями к изделию, которые оно должно выполнять в процессе эксплуатации. Область применения должна соответствовать области назначения по основным характеристикам изделия.

Оперативная постановка задачи методики.

Дано:

1) различные варианты однотипных изделий (применяемые изделия и перспективные), включая «эталонное» изделие;

2) среди различных вариантов однотипных изделий выделено «эталонное» изделие, по отношению к которому рациональные варианты должны быть не хуже;

3) технический облик изделий ВТ в соответствии с ГОСТ РВ 15.102-2004 [1] определяется совокупностью основных характеристик и параметров, определяющих тип, структуру, а также способность реализовать концептуальный замысел решения функциональных задач.

Требуется: обосновать рациональные варианты технического облика изделий:

Условие: под обоснованием рациональных вариантов технического облика изделий понимается проведение сравнительной технико-экономической оценки с «эталонным» изделием:

а) по технике – соответствие значений характеристик изделий значением характеристик «эталонного» изделия или превосходящих их;

б) по экономике:

- стоимость доработок изделия до соответствия значениям характеристик «эталонного» изделия;
- стоимость изготовления изделия.

Формализованная постановка задачи и общее решение.

Пусть VAR – множество вариантов изделий с элементами var_i.

Пусть ОХП – множество основных характеристик и параметров изделий, определяющих их способность реализовать решение функциональных задач.

Задача обоснования вариантов рационального технического облика заключается в том, чтобы найти вариант изделия по критерию «Макси-Мина»:

- «максимум» по технической оценке соответствия значений характеристик значениям характеристик «эталонного» изделия;
- «минимум» по экономической оценке доработок и изготовления.

Для удобства анализа реализации допустим, что все множество ОХП поделено на подмножества [2], которые рассматриваются в соответствующих блоках расчетной методики.

$\text{охп}^{var_i}_{\text{блок}_j}$ – подмножество ОХП, соответствующее i-му варианту изделия (var_i) и j-му блоку методики (блок_j);

$\text{охп}^{var_i}_{\text{блок}_{jh}}$ – элемент множества ОХП, соответствующий i-му варианту изделия (var_i) в j-м блоке методики (блок_j) и h-й характеристики.

Пусть для каждого элемента охп существует оценка оохп.

$\text{оохп}^{var_i}_{\text{блок}_{jh}}$ – оценка элемента множества ОХП на соответствие значения охп «эталонному» значению изделия для i-го варианта изделия (var_i) в j-м блоке методики (блок_j) и h-й характеристики в блоке.

Допустим, экспертным путем произведена сравнительная оценка элементов охп в каждом блоке (блок_j). Предлагается начислять «бонусные» баллы по сравнительной оценке элементов. Правило начисления: если значение характеристики соответствует значению характеристики «эталонного» изделия или превосходит ее – начисляется «плюс» («1»), если не соответствует – начисляется «минус» («∅»). Чем больше «бонусных» баллов, тем «лучше» вариант изделия.

Значение оценки элемента (оохп) учитывается в соответствующих блоках методики. Для каждого требования, которое принадлежит конкретному блоку для каждого изделия, анализируется оценка охп.

$$\forall\, h = \overline{1,H};\ \forall\, j = \overline{2,5};\ \forall\, i = \overline{1,3}\ \text{оохп}^{var_i}_{\text{блок}_{jh}} \neq \emptyset \Rightarrow bonus_i = bonus_i + 1 \quad (1)$$

Рассмотрев все требования во всех блоках расчетной методики, каждому i-му варианту изделия будет соответствовать свое значение bonus_i.

Определение i-го варианта изделия с максимальным значением bonus_i в формализованном виде можно записать, как

$$i_0 = \underset{i}{\text{argmax}}\{bonus_i\} \Leftrightarrow max\{bonus_i\} = \{bonus_{i_0}\} \quad (2)$$

или, аргумент максимизации (i_0) определяется единственным образом тогда и только тогда, когда максимум достигается в единственной точке [3].

Стоимость доработок может быть определена сложением стоимости доработки по i-му варианту изделия в блоке расчетной методики $C^{var_i}_{\text{блок}_j}$ и в целом как сумма по всем блокам. Критерием приемлемости варианта может быть наибольший бонус при стоимости доработок (изготовления) не выше предельной стоимости (C_0).

Тогда критерий выбора рационального варианта технического облика можно записать

$$i_0 = \left(\underset{i}{\text{argmax}}\{bonus_i\}\right) \,\&\, \left(\sum_j^J C^{var_{io}}_{\text{блок}_j} \leq C_0\right). \quad (3)$$

Количество блоков методики зависит от конкретной ситуации рассматриваемых изделий и однородности характеристик вариантов изделий. Для примера ниже рассмотрена 7-ми блочная схема обоснования вариантов рационального технического облика изделия (рис. 1).

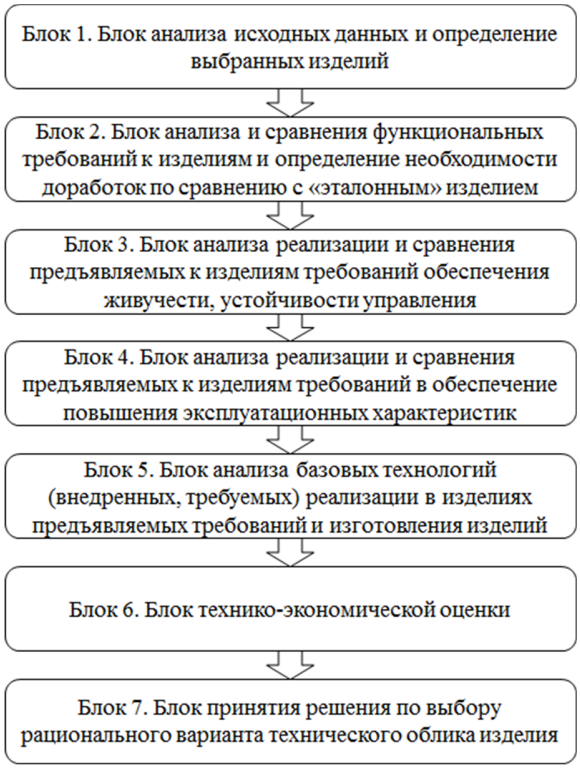


Рис. 1. Поблочная схема обоснования вариантов рационального технического облика изделия

1. Блок анализа исходных данных и определение выбранных изделий.

В данном блоке проводится анализ тактико-технических характеристик (параметров) изделий. Вариантам изделий (var_i) присваиваются порядковые номера i= $\overline{1,N}$. Ниже мощность множества |N|=3.

Вариант изделия, обладающий минимаксными значениями характеристик, получает бонусный бал (bonus):

за минимальные весогабаритные характеристики (ВГХ);

за высокую степень эксплуатационной готовности (ВСЭГ);

за новую электронную компонентную базу и конструктивные решения (ЭКБ).

2. Блок анализа и сравнения функциональных требований к изделиям и определение необходимости доработки по сравнению с «эталонным» изделием.

Функциональные требования к вариантам изделия условно можно представить в виде последовательности элементов множества ФТ мощностью f = $\overline{1,F}$. Допустим (для наглядности) следующее соотношение реализованных функциональных требований к вариантам изделия.

Рис. 2. Множества функциональных требований к изделию

Множество реализованных функциональных требований к 1-му варианту изделия обозначим $ФТ^1$. Они соответствуют 1-й предметной области и являются избыточными по отношению к требованиям для 2-й предметной области.

$ФТ^2$ – множество реализованных функциональных требований ко 2-му варианту изделия, соответствующему 2-й предметной области.

$ФТ^3$ – множество реализованных функциональных требований к 3-му варианту изделия (3-я предметная область).

В зависимости от заданных функциональных требований к вариантам изделия могут быть различные множественные соотношения, которые можно представить тремя пересекающимися множествами (рис. 2).

Различные сочетания элементов указанных множеств функциональных требований будут соответствовать различным предметным областям, которые в том числе могут не иметь значения для конкретной задачи (рис. 3 и 4).

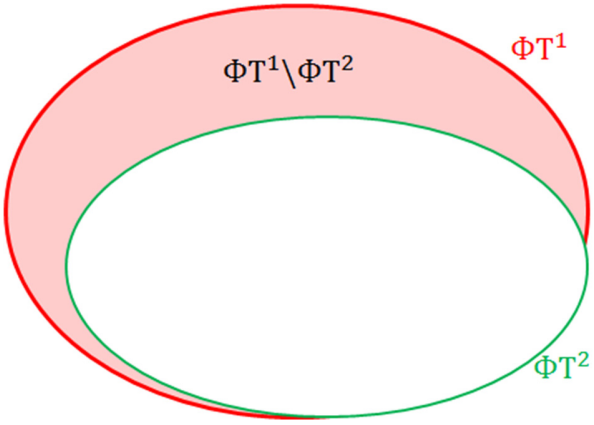


Рис. 3

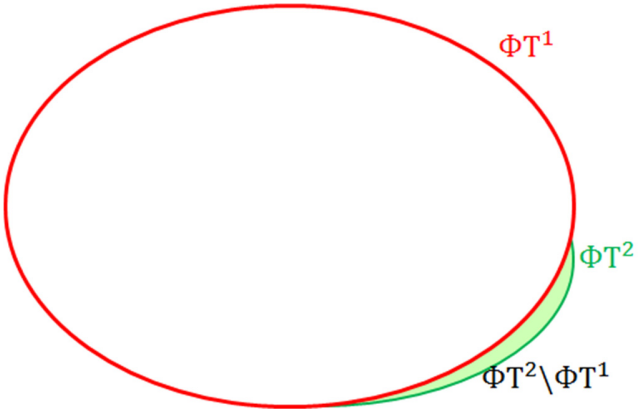


Рис. 4

Правила оценки в блоке 2. Для каждого варианта изделий производится оценка функциональных требований в рассматриваемом варианте изделия. Если рассматриваемый элемент множества функциональных требований реализован, т.е. оценка – не «пустое» множество, то рассматриваемый вариант получает бонус – один балл.

В формализованном виде это можно представить следующим образом:

$$\text{офт}_f^{var_i} \neq \emptyset \underset{\substack{f=\overline{1,18}}}{\overset{i=\overline{1,3}}{\Longrightarrow}} bonus_i = bonus_i + 1 \quad (4)$$

При этом принимается допущение, что неполная реализация функционального требования в варианте изделия, требующая его доработки, будет учтена при рассмотрении стоимости изготовления изделия

$$C_{\text{блок}_j}^{var_i}, \text{где } i = \overline{1,3}, j = \overline{2,5} \quad (5)$$

3. Блок анализа реализации и сравнения предъявляемых к изделиям требований обеспечения живучести, устойчивости управления.

Технические решения по обеспечению устойчивости управления, технические решения, повышающие живучесть, рассматриваются во всех возможных условиях, в различных ситуациях.

Представим рассмотренные требования по устойчивости боевого управления как множество УУ, мощность которого $u = \overline{1,U}$ с элементами $\text{уу}_u^{var_i}$.

По результатам анализа обеспечения устойчивости управления изделия можно подготовить массив оценочных исходных данных (оуу), с учетом которого по правилу, изложенному в блоке 2, можно рассчитать бонусные баллы по вариантам изделий:

$$\text{оуу}_u^{var_i} \neq \emptyset \underset{\substack{u=\overline{1,3}}}{\overset{i=\overline{1,3}}{\Longrightarrow}} bonus_i = bonus_i + 1 \quad (6)$$

При отсутствии реализации требования для достижения i-го варианта изделия уровня устойчивости управления, который обеспечивается «эталонным» изделием, стоимость требуемых доработок можно выразить через функционал:

$$\text{С}_\text{з}^{var_i}\left[F\left(\text{уу}_u^{var_i}\right)\right] \quad (7)$$

Стоимость, выраженная через реализацию (оценку выполнения) требований по устойчивости управления, может быть представлена функционалом:

$$\text{С}_\text{з}^{var_i} = \sum_{u=1}^{U} C_u^{var_i}\left[F\left(\text{оуу}_u^{var_i} = \emptyset\right)\right]. \quad (8)$$

4. Блок анализа реализации и сравнения предъявляемых к изделиям требований в обеспечение повышения эксплуатационных характеристик.

ЭХ – множество эксплуатационных характеристик мощностью $d = \overline{1,D}$. $|\text{ЭХ}| = D$.

ОЭХ – множество сравнительных оценок эксплуатационных характеристик.

Правила начисления бонусных баллов основаны на результатах оценки сравнения характеристик оэх:

$$1)\ \text{оэх}_d^{var_1} = \text{оэх}_d^{var_2} = \text{оэх}_d^{var_3} \underset{d=\overline{1,D}}{\Longrightarrow} d = d + 1 \quad (9)$$

переход к следующему элементу множества оценок эксплуатационных характеристик;

$$2)\ \text{оэх}_d^{var_i} = \text{«плюс»} \underset{d=\overline{1,D}}{\underset{i=\overline{1,3}}{\Longrightarrow}} bonus_i = bonus_i + 1 \quad (10)$$

Стоимость доработок для *i*-варианта изделия, как и ранее, можно было бы представить функционалом:

$$\text{С}_4^{var_i} = \sum_{d=1}^{D} C_d^{var_i} \left[F\left(\text{оэх}_d^{var_i} = \emptyset\right)\right], \quad (11)$$

однако, эксплуатационные характеристики зачастую можно улучшить, только изменив схемно-конструкторские решения, а, по сути, спроектировав изделие заново с учетом требуемых эксплуатационных характеристик и с использованием внедренных технологий.

5. Блок анализа базовых технологий (внедренных, требуемых) реализации в изделиях предъявляемых требований и изготовления.

В данном блоке подводится итог о целесообразности применения внедренных или требуемых технологий.

БТ – множество базовых технологий мощностью $t = \overline{1,T}$. |БТ| = Т.

Целесообразно для сравнительной технико-экономической оценки рассматривать только те технологии, которые оказывают влияние на оценку.

$\text{обт}_t^{var_i}$ – массив оценочных данных.

Оценка производится по существующим технологиям.

$$\text{обт}_t^{var_i} = \emptyset \underset{d=\overline{1,2}}{\underset{i=\overline{1,3}}{\Longrightarrow}} bonus_i = bonus_i + 1 \quad (12)$$

Стоимость, выраженная через реализацию (оценку обеспеченности) базовыми технологиями, может быть представлена функционалом:

$$\text{С}_5^{var_i} = \sum_{t}^{T} C_t^{var_i} \left[F\left(\text{обт}_t^{var_i} = \emptyset\right)\right]. \quad (13)$$

6. Блок технико-экономической оценки.

В данном блоке на основании проведенных ранее сравнительных оценок вариантов изделий подводится итоговая оценка технического облика вариантов изделий. Сравнительные оценки технического облика вариантов изделий суммируются по блокам анализа (блоки 2-5) для итоговых оценок (бонусные баллы и стоимость доработок вариантов изделий, выраженная через функционалы).

7. Блок принятия решения по выбору рационального варианта технического облика изделия.

Рациональный вариант технического облика изделия выбирается по принятому критерию.

Например, критерием выбора варианта может быть наибольший бонус при стоимости доработок (изготовления) не выше предельной стоимости (C_0) согласно формуле (3).

Рассмотренная методика обладает недостатками в части формализованного учета реализованных функциональных требований в различных вариантах изделия (блок 2). В частности, в блоке 2 оценка реализации функциональных требований, по сути, зависит от оценки человека (от уровня квалификации, способности соотнести реализацию функциональных требований к варианту изделия, знания предметной области). Недостаток связан с применением теоретико-множественного подхода для оценки реализации функциональных требований, а, по сути, к формализации (моделированию) предметной области. Для этой цели целесообразно «говорить о необходимости синтеза системно-структурного и объектно-ориентированных подходов» [4].

Заключение. В данной статье в формализованном виде представлена методика обоснования рациональных вариантов технического облика изделия на основе сравнения технических характеристик с «эталонным» вариантом изделия, а также учетом стоимости доработок для каждой характеристики вариантов изделия. В процессе сравнения характеристик у каждого варианта накапливаются бонусные балы, если значение характеристик сопоставимы или превосходят соответствующие показатели «эталонного» варианта изделия (1). Лучший вариант изделия определяется по бонусам (2) и стоимости доработок (3). Достоинством методики является ее простота и возможность использования применительно к широкому спектру вариантов изделий, что наглядно демонстрирует приведенный общий пример ее использования.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ РВ 15.102 – 2004 Система разработки и постановки продукции на производство. Военная техника. Тактико-техническое (техническое) задание на выполнение аванпроекта. – М., 2005. – 24 с.
2. Буфеев С.В., Буфеев И.С. Основы математической логики и теории множеств: Учебное пособие. Изд. 3-е стереотип. – М.: ЛЕНАНД, 2020. – 144 с.
3. Аргументы максимизации и минимизации – Википедия. http://www.wikipedia. ru.
4. Теория систем и системный анализ: учебник / А.Г. Жихарев, О.А. Зимовец, М.Ф. Тубольцев, А.А. Кондратенко; под ред. С.И. Маторина. – Москва: КНОРУС, 2021. – 456 с.

УДК 621.391

МЕТОДИКА ОЦЕНИВАНИЯ СВОЕВРЕМЕННОСТИ ДОВЕДЕНИЯ МНОГОПАКЕТНЫХ СООБЩЕНИЙ ПО ВИРТУАЛЬНЫМ МАРШРУТАМ В СЕТИ ПЕРЕДАЧИ ДАННЫХ

Цимбал Владимир Анатольевич[1], Потапов Сергей Евгеньевич[2]
[1] Филиал Военной академии РВСН им. Петра Великого в г. Серпухове
Бригадная ул., 17, Серпухов, Московская обл., 142210, Россия
[2] Военная академия РВСН им. Петра Великого
Карбышева ул., 8, Балашиха, Московская обл., 143900, Россия
e-mails: tsimbalva@mail.ru, 41kaf_rabota@mail.ru

Аннотация. Рассматривается научно-методический подход к определению характеристик информационного обмена многопакетными сообщениями по сети передачи данных без предварительного установления виртуального соединения. Характеристики виртуального маршрута определятся по характеристикам составляющих его отдельных каналов связи, а своевременность доведения сообщений оценивается на основе неравенств Чебышевского типа с учётом допустимого времени передачи.

Ключевые слова: сеть передачи данных; многопакеные сообщения; своевременность доведения информации; каналы связи; распределение вероятностей случайной величины; информационный обмен.

METHODOLOGY FOR ESTIMATING THE TIMELINESS OF DELIVERY OF MULTIPATCH MESSAGES ON VIRTUAL ROUTES IN THE DATA TRANSMISSION NETWORK

Tsimbal Vladimir[1], Potapov Sergey[2]
[1] Branch of the Military Academy of the Strategic Missile Forces named after Peter the Great in Serpukhov,
Brigadnaya St., 17, Serpukhov, Moscow region, 142210, Russia
[2] Military Academy of the Strategic Missile Forces. Peter the Great
Karbysheva st., 8, Balashikha, Moscow region, 143900, Russia
e-mails: tsimbalva@mail.ru, 41kaf_rabota@mail.ru

Abstract. A scientific and methodological approach to determining the characteristics of information exchange of multi-packet messages over a data transmission network without prior establishment of a virtual connection is considered. The characteristics of a virtual route are determined by the characteristics of its individual communication channels, and the timeliness of delivering messages is estimated on the basis of Chebyshev-type inequalities, taking into account the permissible transmission time.

Keywords: data transmission network; multi-pack messages; timeliness of information delivery; channels of connection; probability distribution of a random variable; information exchange.

Введение. Для обеспечения своевременного и качественного управления распределёнными объектами во многих критически важных отраслях народного хозяйства и силовых ведомствах создаются и функционируют автоматизированные системы управления (АСУ), неотъемлемой составляющих которых являются системы и сети передачи информации. Для обеспечения гарантированного качества управления в таких АСУ необходимо контролировать соответствие характеристик информационного обмена (ИО) требуемым (нормативным) значениям. Одной из наиболее важных характеристик ИО в АСУ является своевременность доведения многопакетных сообщений (МПС) между абонентами (органами управления АСУ) по сети передачи данных. В настоящее время наработан большой методический аппарат для исследования характеристик ИО в соединении «точка-точка», т.е. между смежными узлами связи сети [1], а также существуют методики определения задержек при передаче информации по виртуальным каналам с хорошими по качеству транзитными направлениями связи [2]. В [3, 4] приведены методические основы точного определения характеристик ИО по составным (виртуальным) маршрутам без установления виртуального соединения с разнородными по качеству транзитными каналами связи (КС), однако сложность его применения при большой ёмкости МПС достаточно велика. Поэтому актуальной задачей при проектировании и эксплуатации специализированных АСУ является оценивание характеристик ИО МПС по их сетевой инфраструктуре с учётом качества отдельных направлений связи.

Для обобщения результатов моделирования процессов передачи МПС по ВМ рассмотрим следующую временную диаграмму (рис.1).

При передаче информации по ВМ без установления соединения [3] в каждом промежуточном КС производится квитирование каждого отдельного пакета. При этом время передачи пакета по транзитному КС складывается из времени доставки непосредственно информационного пакета $t_{ип}$ и времени подтверждения его квитанционным кадром $t_{кв}$.

Тогда суммарное время доставки МПС также определяется временем их доставки по КС с наибольшим временем задержки, временем следования первого пакета до этого КС и временем следования последнего пакета до получателя

$$t_c = t_n^{12} + \sum_{i=1}^{l_c} t_{n_i}^{23} + t_n^{34}, \quad (1)$$

где t_n^{ij} - случайная величина, определяемая случайной функцией $t_n^{ij} = \varphi(t_{ш}^{ij}, t_{кв}^{ij})$; l_c–длина передаваемого сообщения в пакетах.

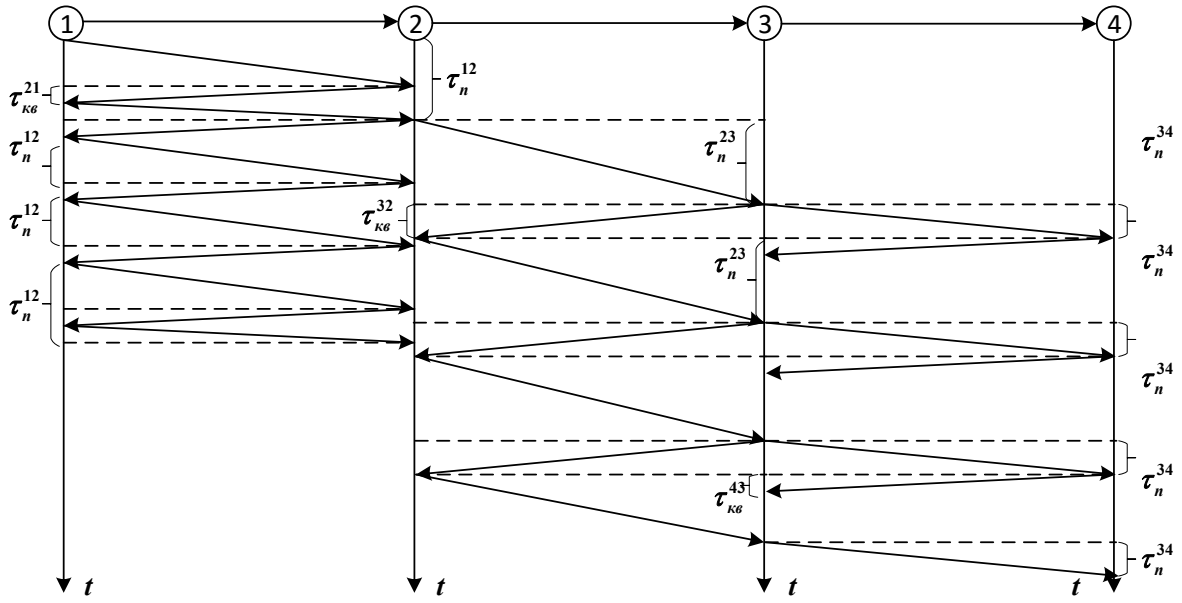


Рис. 1. Пример доставки многопакетного сообщения без установления соединения

В общем случае, время доставки МПС определяется из выражения

$$t_c = \sum_{i=1}^{l_c} t'_{кс_i} + T, \quad (2)$$

где $t'_{кс_i}$ – время передачи *i*-го пакета по КС с наибольшим временем задержки; *T* – суммарное время доставки одного пакета по остальным КС.

Из выражения (2) следует, что время передачи МПС произвольной длины l_c зависит от длины этого сообщения (в пакетах) и от времени задержки на самом «медленном» участке маршрута. Считая эти времена независимыми случайными величинами (СВ), закон распределения времени доведения МПС по ВМ можно получить из производящей функции суммы независимых СВ в виде

$$F(t_c) \Leftrightarrow g_{t_c}(s) = g_T(s) \cdot (g_{t'_{кс}}(s))^{l_c}. \quad (3)$$

Следовательно, получить оценку среднего времени и дисперсии времени доведения МПС по ВМ можно по следующим выражениям (4-5):

$$T_{МПС}^{ij} = l_c \cdot \bar{t}_П^{km} + \sum_{n1 \in ik} \bar{t}_П^{n1} + \sum_{n2 \in mj} \bar{t}_П^{n2}, \quad (4)$$

$$D_{МПС}^{ij} = l_c \cdot D_П^{km} + \sum_{n1 \in ik} D_П^{n1} + \sum_{n2 \in mj} D_П^{n2}, \quad (5)$$

где l_c - количество пакетов МПС;

i – начальное ЗПД ВМ; *j* – конечное ЗПД ВМ; *km* – парциальный КС ВМ с наибольшим средним временем доведения пакета;

$\bar{t}_П^{km}$, $D_П^{km}$ – среднее время и дисперсия времени передачи пакета по *km*-му КС ВМ между *i*-м и *j*-м ЗПД с наихудшим качеством ($\bar{t}_П^{km} = \max_{pr \in ij}(\bar{t}_П^{pr})$);

$\bar{t}_П^{n1}$, $D_П^{n1}$ – среднее время и дисперсия времени передачи пакета по КС ВМ до *km*-го КС ВМ;

$\bar{t}_П^{n2}$, $D_П^{n2}$ – среднее время и дисперсия времени передачи пакета по КС ВМ после *km*-го КС ВМ.

Для анализа погрешности оценки среднего времени и дисперсии времени доведения МПС по ВМ (временных характеристик) с помощью оценочных выражений (4-5) по отношению к рассмотренному выше точному подходу были построены совместные графики зависимостей среднего времени и СКО времени доведения МПС по двухканальному ВМ при исходных данных таблиц 1 и 2, представленные на рис. 2 и 3.

Из анализа представленных зависимостей следует, что, во-первых, при хорошем качестве КС ВМ оценочные выражения (4-5) достаточно точно описывают временные характеристики процесса доведения МПС по ВМ, во-вторых, максимальная погрешность расчёта временных характеристик исследуемого процесса по выражениям (4-5) возникает при близком значении качества КС ВМ. При этом оценки среднего времени и СКО времени доведения МПС получаются несколько заниженными (при хорошем качестве КС не более чем на 5% от времени доведения МПС).

Таблица 1

Параметры КС с высокой вероятностью битовой ошибки

Параметры	$P_п$	$t_п$,с	$P_{кв}$	$t_{кв}$,с
КС – 1	0,75	2	0,89	0,7
КС – 2	0,82	0,7…3,2	0,85	0,1…0,85

Таблица 2

Параметры КС с низкой вероятностью битовой ошибки

Параметры	$P_п$	$t_п$,с	$P_{кв}$	$t_{кв}$,с
КС – 1	0,9	2	0,95	0,7
КС – 2	0,85	0,7…3,2	0,92	0,1…0,85

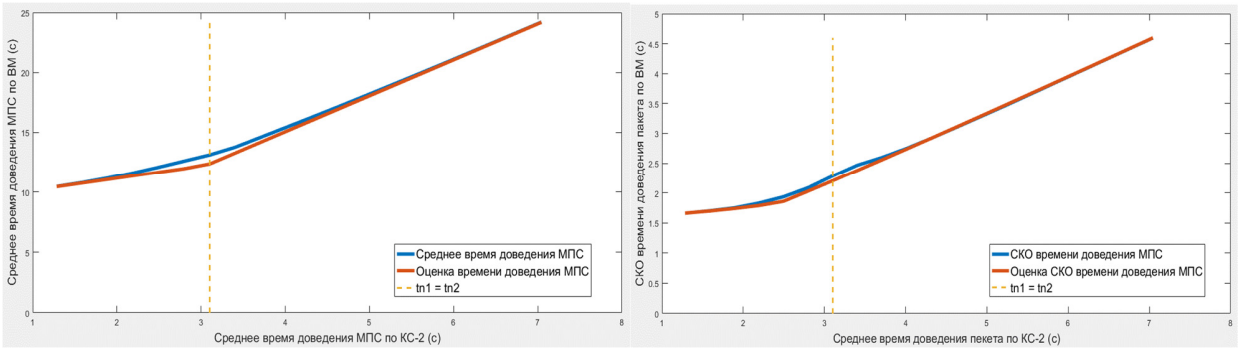


Рис. 2. Точные и оценочные значения среднего и СКО времени доведения МПС по ВМ при низкой вероятности битовой ошибки

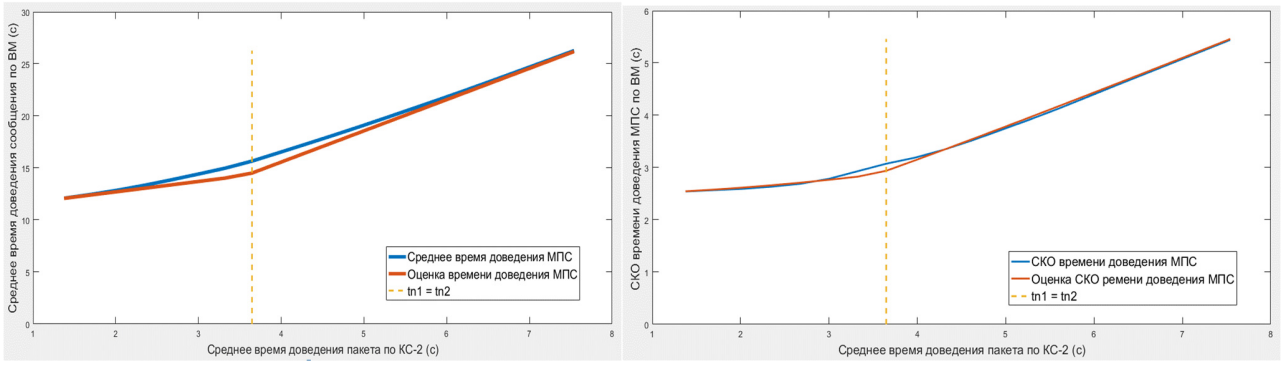


Рис. 3. Точные и оценочные значения среднего и СКО времени доведения МПС по ВМ при высокой вероятности битовой ошибки

Для оценки гарантированной своевременности (ВВХ) доведения МПС по ВМ, то есть минимально-гарантированной вероятности доведения МПС за допустимое время, требуется получить выражения, оперирующие оценками моментов распределения времени доведения пакетов по всем КС ВМ. При этом гарантированность получаемых оценок заключается в их не превышении вероятности своевременного доведения МПС, получаемой точным путём. С другой стороны, при оценивании вероятности своевременного доведения МПС необходимо стремиться к уменьшению погрешности занижения точного значения этой величины.

Наиболее известным способом оценивания характеристик распределения случайных величин по их моментам распределения является неравенство Чебышева и связанные с ним подобные выражения [4]. Причём большинство

таких неравенств получены для двусторонних относительно нуля распределений (неравенство Чебышева, Глессера, К. Пирсона). Однако существуют оценки и односторонних положительных распределений СВ (неравенство Маркова, Вальда, Родена, Ефимова и др.). Из односторонних оценок СВ наибольший интерес представляют неравенства Кантелли (6), Пирсона (7), усиленные неравенства Гаусса (8), Гудриаана (9):

$$P(x > \mathrm{M[x]}+k\sigma) < 1/(1+k^2), \tag{6}$$

$$P(|x - \mathrm{M}[x]| \geq k) \leq \mathrm{D}[x]/k^2, \tag{7}$$

$$P(|x - x_{\mathrm{mod}}| \geq k\tau) \geq 1 - 4/9k^2, \tag{8}$$

$$P(x > \mathrm{M[x]}+k\sigma) < 4/9(1+k^2), \tag{9}$$

где $\tau^2 = \mathrm{D}[x_{\mathrm{mod}}] = \mathrm{D}[x] + (\mathrm{M}[x] - x_{\mathrm{mod}})^2$ – дисперсия от моды; $k>0$ – допустимое отклонение СВ.

Для исследования применимости указанных соотношений к задаче оценивания вероятности сверенного доведения МПС по ВМ преобразуем их к виду $P(t_{дов} \leq T^{доп}) \geq A$. При этом следует учитывать, что данные неравенства справедливы для полных (нормированных к единице) распределений, тогда как получаемые точным реляционно-операторным методом вероятностно-временные характеристики процесса доведения МПС являются усечёнными на величину $P_{недов}$=1-$P_{дов}$ – вероятности не доведения какого-либо пакета за ограниченное число повторов передачи. Поэтому правые части получаемых неравенств следует умножить на величину $P_{дов}$. В результате получены следующие оценочные выражения:

$$P(t_{дов} \leq T^{доп}) \geq \left(1 - \frac{\mathrm{D}[x]}{\mathrm{D}[x] + (T^{доп} - \mathrm{M}[x])^2}\right) \cdot P_{дов}, \tag{10}$$

$$P(t_{дов} \leq T^{доп}) \geq \left(1 - \frac{\mathrm{D}[x]}{(T^{доп} - \mathrm{M}[x])^2}\right) \cdot P_{дов}, \tag{11}$$

$$P(t_{дов} \leq T^{доп}) \geq \left(1 - \frac{4 \cdot (\mathrm{D}[x] + (\mathrm{M}[x] - t_{\mathrm{mod}})^2)}{9 \cdot (T^{доп} - \mathrm{M}[x])^2}\right) \cdot P_{дов}, \tag{12}$$

$$P(t_{дов} \leq T^{доп}) \geq \left(1 - \frac{4 \cdot (\mathrm{D}[x])}{9 \cdot ((T^{доп} - \mathrm{M}[x])^2 + \mathrm{D}[x])}\right) \cdot P_{дов}. \tag{13}$$

Графики зависимости вероятности и оценки вероятностей доведения МПС за требуемое время ($T_{доп}$ = 20 с) для различных граничных выражений от времени передачи пакета по КС-2 представлены на рис. 4.

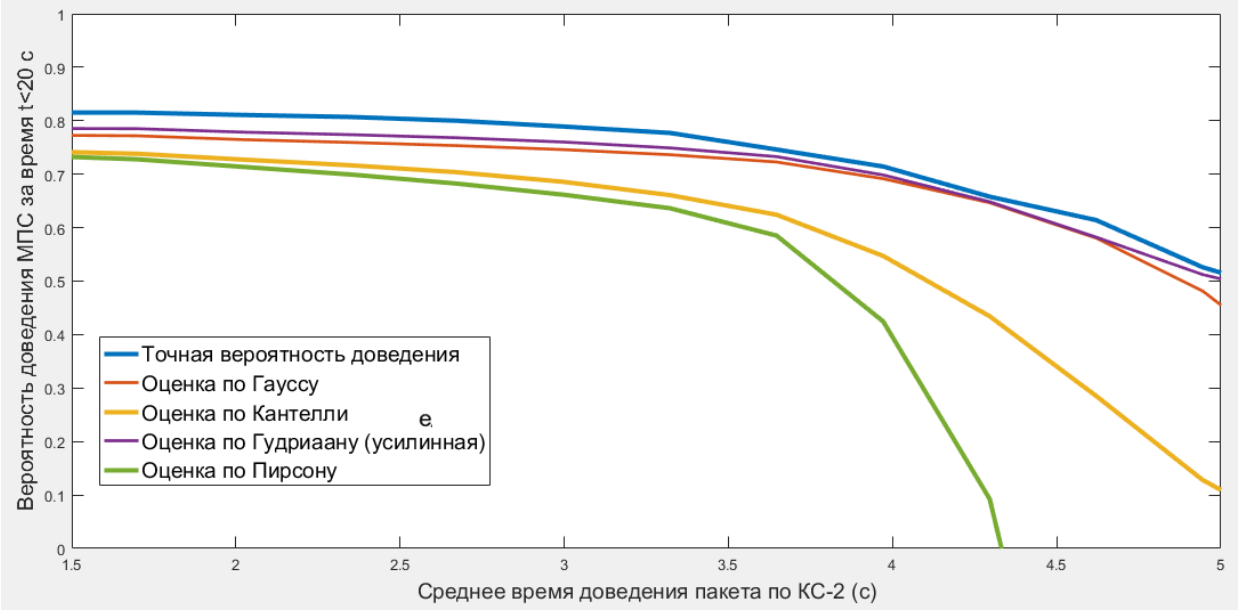


Рис. 4. Точные и оценочные значения своевременности доведения МПС по ВМ

Из анализа графиков следует, что достаточно точное приближение оценки нижней границы вероятности непревышения допустимого времени доведения МПС наблюдается при использовании выражений Гаусса (12) и Гудриаана (13). При этом оценка своевременности доведения МПС по выражению (13) является всё же предпочтительней. Поэтому в методике своевременности доведения МПС по ВМ, общий вид которой представлен

на рис. 5, для определения нижней границы своевременности доведения МПС используется именно выражение (13) на основе неравенства Гудриаана.

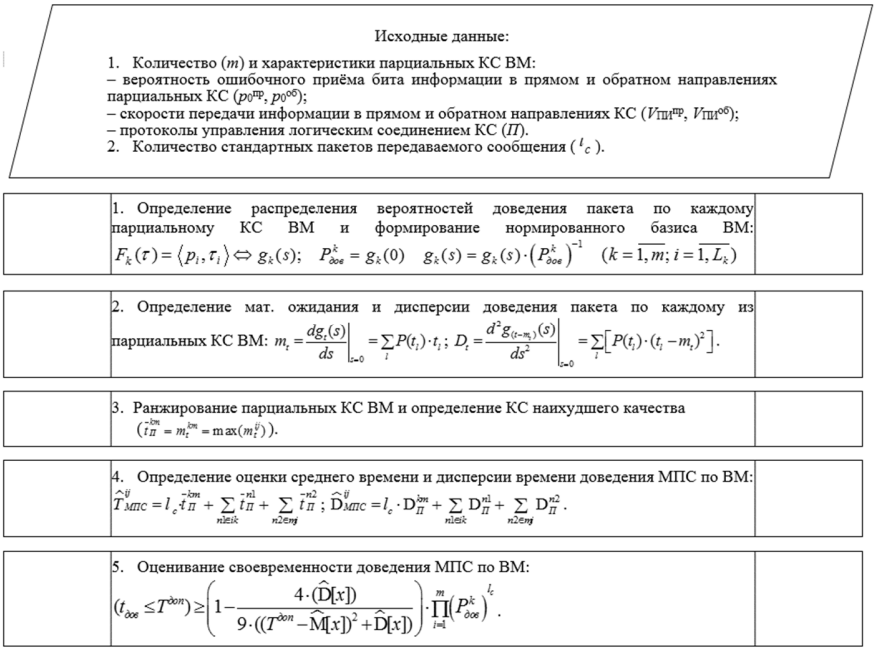


Рис. 5 Методика оценивания своевременности доведения МПС по ВМ

Заключение. Таким образом, для оперативного определения своевременности ИО абонентов сети передачи данных без большого ущерба для точности можно воспользоваться приближёнными вычислениями по выражениям (4-5, 13). Применение разработанной методики оценивания своевременности доведения МПС по ВМ позволяет существенно сократить объём необходимых для этого вычислений.

СПИСОК ЛИТЕРАТУРЫ

1. Потапов, С. Е. Математическая модель доставки многопакетных сообщений в соединении «точка-точка» на сети передачи данных с процедурой «скользящее окно» [Текст] / С. Е. Потапов, В. А. Цимбал, Л.Н. Косарева, Т.А. Исаева, И.Н. Ваганов // Известия Ин-та инженерной физики : науч.-техн. журн. – Серпухов, 2009. – Т. 3 № 13 – С. 13-19.
2. Потапов, С. Е. Исследование адаптивного механизма управления передачей информации по протоколу TCP в условиях динамики параметров каналов связи / С. Е. Потапов, В. А. Цимбал, В.Е. Тоискин // Материалы конф. «Информационные технологии в управлении» / ГНЦ РФ ОАО «Концерн «ЦНИИ «Электроприбор». – СПб, 2016. С. 269-275.
3. Потапов, С. Е. Реляционно-операторный метод математического моделирования передачи многопакетных сообщений по виртуальным маршрутам сети радиосвязи // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 6. С. 61 -73. doi: 10.24411 /2409-5419-2018-10296.
4. Потапов С.Е. Исследование процесса передачи информации по виртуальным маршрутам в радиосети системы связи с подвижными объектами // Теория и техника радиосвязи. 2019. № 3. С. 11-23.
5. Протоколы информационно-вычислительных сетей: Справочник / С.А. Аничкин С.А. Белов, А.В. Бернштейн и др.; под общ. ред. И.А. Мизин, А.П. Кулешова. – М.: Радио и связь, 1990. – 504 с.: ил. ISBN 5-256-00359-3.
6. Бостанджиян В.А. Пособие по статистическим распределениям. – Черноголовка. Редакционно-издательский отдел ИПХВ РАН, 2013. 1060 с.

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «БЕЗОПАСНЫЕ ИНТЕЛЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»

УДК 004.056

РАЗРАБОТКА КОМПЛЕКСНОЙ МЕТОДИКИ ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ WEB-ПРИЛОЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ СТАТИЧЕСКОГО И ИНТЕРАКТИВНОГО ТЕСТИРОВАНИЯ

Акилов Марк Валерьевич, Ковцур Максим Михайлович, Несудимов Евгений Юрьевич, Потемкин Павел Андреевич

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: markakilov@yandex.ru, maxkovzur@mail.ru, enesudimov@gmail.com, potiomkinpa98@gmail.com

Аннотация. С появлением концепции DevOps, процесса разработки ускорился за счет автоматизации и стандартизации процессов для поддержания качества и стабильности разрабатываемого ПО, что привело к новой проблеме - процессы анализа безопасности стали сильно замедлять скорость выпуска программного продукта на рынок. Решением слата интеграция методов проверки безопасности в современные и автоматизированные процессы DevOps – DevSecOps. Одной из самых важных концепций DevSecOps стало внедрение средств автоматизированного тестирования безопасности. Разделяют три технологии тестирования: DAST, IAST и SAST. Целью данной работы является исследование IAST и SAST, их преимуществ и недостатков, а также возможностей совместного применения.

Ключевые слова: SAST; IAST; DAST; DevOps; тестирование; безопасность; веб-приложение; код; инструмент; разработка; уязвимость.

DEVELOPMENT OF A COMPREHENSIVE METHOD FOR DETECTING VULNERABILITIES OF WEB-APPLICATIONS USING STATIC AND INTERACTIVE TESTING

Akilov Mark, Kovzur Maxim, Nesudimov Evgeny, Potiomkin Pavel

The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: markakilov@yandex.ru, maxkovzur@mail.ru, enesudimov@gmail.com, potiomkinpa98@gmail.com

Abstract. With the advent of the concept of DevOps, the development process has accelerated due to the automation and standardization of processes to maintain the quality and stability of the software being developed, which has led to a new problem - security analysis processes have begun to greatly slow down the speed of release of a software product to market. The slat solution is the integration of security verification methods into modern and automated DevOps processes - DevSecOps. One of the most important DevSecOps concepts has been the implementation of automated security testing tools. Three test technologies are shared: DAST, IAST, and SAST. The aim of this work is to study IAST and SAST, their advantages and disadvantages, as well as the possibilities of their joint application.

Keywords: SAST; IAST; DAST; DevOps; testing; security; web application; code; tool; development; vulnerability.

Введение.В последние годы использование веб-приложений возросло во многих типах организаций. Эти приложения должны постоянно развиваться в кратчайшие сроки, чтобы противостоять конкурентам. Это увеличивает риск написания небезопасного кода.

Исследование существующих инструментов тестирования приловений.

Для обеспечения должного уровеня проверки безопасности приложений были разработаны инструменты тестирования безопасности приложений (AST) [4]. Выделяют статический (SAST), динамический (DAST) и интерактивный (IAST) виды тестирования безопасности приложений.

SAST (Static Application Security Testing) - производит тестирование «белого ящика». Данный вид тестирования анализирует как исходный код, так и исполняемый файл, в зависимости от обстоятельств.

DAST (Dynamic Application Security Testing) — это тестирование, которое позволяет анализировать запущенное приложение, атакующее все внешние исходные входные данные веб-приложения.

IAST (Interactive Application Security Testing) - данный вид тестирования позволяет анализировать код, но, в отличие от SAST, делает это в режиме реального времени и в интерактивном режиме, аналогичном инструментам DAST.

Несколько инструментов одного и того же типа могут быть объединены для достижения лучшей производительности с точки зрения истинных и ложных срабатываний [2]. Таким образом, целью данной работы является исследование IAST и SAST, их преимуществ и недостатков, а также возможностей совместного применения.

Для того чтобы изучить эффективность каждого инструмента по отдельности и в совместном применении необходимо определить ряд наиболее распространенных и опасных уязвимостей безопасности веб-приложений. Такой список уже был составлен открытым проектом по обеспечению безопасности веб-приложений (OWASP). Список OWASP Top Ten объединяет наиболее важные категории уязвимостей. По версии OWASP от 2017 года существуют следующие десять видов уязвимостей веб приложений: инъекции, уязвимости аутентификации, раскрытие конфиденциальных данных, внешние объекты XML (XXE), нарушенный контроль доступа, неверная конфигурация безопасности, межсайтовый скриптинг (XSS), небезопасная десериализация, использование компонентов с известными уязвимостями, недостаточное ведение журнала и мониторинг.

Исходя из результатов ряда исследований [7,8], наиболее адекватным тестовым стендом для использования инструментов SAST, DAST и IAST является проект OWASP benchmark project [6]. Это веб-приложение на языке Java, которое содержит тестовые случаи для обнаружения истинных и ложных срабатываний. Из всех видов уязвимостей, представленных на тестовом стенде, случайным образом были отобраны 320 тестовых случаев и распределены поровну между собой. Из них половина случаев ложного срабатывания, а половина - истинно положительные. В таблице 1 показано распределение тестовых случаев для каждого типа уязвимости безопасности [3].

Таблица 1

Распределение тестовых случаев для каждого типа уязвимости

Вид уязвимостей	Количество тестирований
Command Injections	40
Xpath Injections	20
Cross Site Scripting (XSS)	40
LDAP Injection	20
Path Traversal	40
SQL Injection	40
Secure Cookie flag	20
Trust Boundary Violation	20
Weak Randomness	40
Weak Cryptographic	20
Weak Hashing	20
Всего	320

Инструменты SAST и IAST выбираются в соответствии с платформой Java 2, Enterprise Edition (J2EE), наиболее используемой технологией в разработке веб-приложений, языком программирования, используемым J2EE, является Java, один из помеченных как более безопасный.

С учетом сравнений и анализа доступности коммерческих и открытых исходных инструментов были выбраны следующие инструменты:

- FindSecurityBugs - SAST инструмент с открытым исходным кодом.
- Contrast Community Edition - бесплатная версия коммерческого инструмента IAST от Contrast Security.

На рис. 1. представлена схема экспериментальной установки. На виртуальную машину с Ubuntu Server 16.04 были установлены Apache Tomcat и развернут проект OWASP Benchmark. На эту же машину был установлен агент IAST инструмента Contrast CE и SAST инструмент FindSecurityBugs.

Для определения эффективности работы инструментов *SAST* и *IAST* исследование было проведено относительно следующих метрик:

Истинно положительная оценка (ИПО) - отношение обнаруженных уязвимостей к числу реально существующих уязвимостей в коде:

$$ИП / (ИП + ЛО),$$

где ИП (истинно положительные) - - количество истинных уязвимостей, обнаруженных в коде, а ЛО (ложно негативные) - общее количество существующих уязвимостей, не обнаруженных в коде.

Ложно положительная оценка (ЛПО) - Соотношение ложных тревог для уязвимостей, которые на самом деле не существуют в коде:

$$ИО / (ИО + ЛП),$$

где ИО (истинно отрицательные) - количество не обнаруженных уязвимостей, которых на самом деле нет в коде, а ЛП (ложноположительные) - общее количество обнаруженных уязвимостей, которых на самом деле нет в коде.

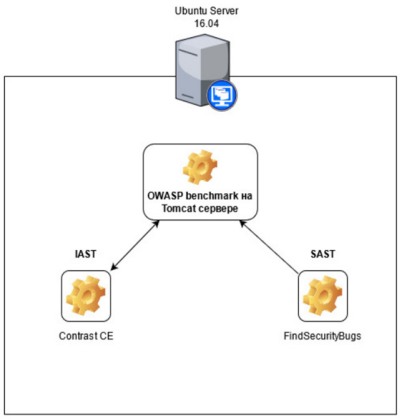


Рис.1. Схема экспериментальной установки.

Для исследования эффективности определения уязвимостей при совместной работе инструментов *SAST* и *IAST* необходимо понимать в каких случаях система из двух инструментов возвращает истинно положительный, истинно отрицательный, ложноположительный или ложноотрицательный результат. Для этих целей была использована логика определения истинности или ложности, представленная в таблице 2 [1].

Таблица 2

Логика получения результатов от проверки двумя инструментами

	Инструмент А	Инструмент Б	Совместно
Положительные случаи	ИП	ИП	ИП
	ИП	ЛО	ИП
	ЛО	ИП	ИП
	ЛО	ЛО	ЛО
Отрицательные случаи	ЛП	ЛП	ЛП
	ЛП	ИО	ЛП
	ИО	ЛП	ЛП
	ИО	ИО	ИО

По результатам исследования нами были составлены графики зависимостей ИПО и ЛПО от каждого вида уязвимостей для инструмента *SAST*, результат которого указан на рис. 2, инструмента *IAST* результат которого указан на Рис. 3 и для их совместного применения результат представлен на рис. 2.

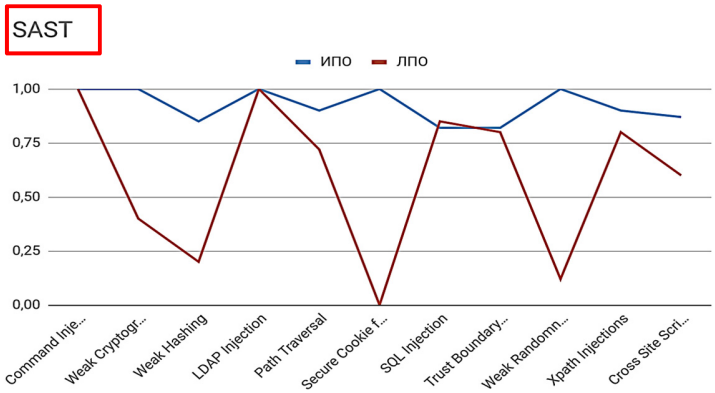


Рис. 2. График зафиксированных ИПО и ЛП для *SAST*.

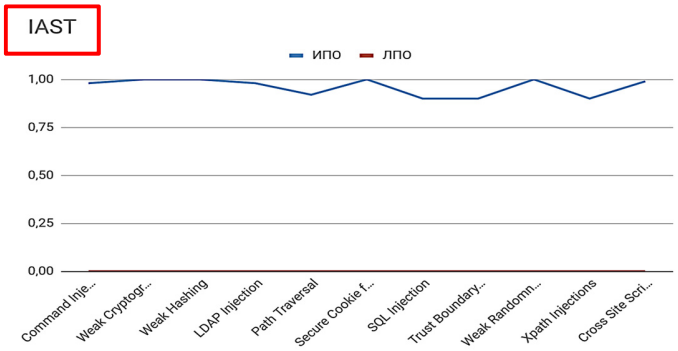


Рис. 3. График зафиксированных ИПО и ЛПО для *IAST*.

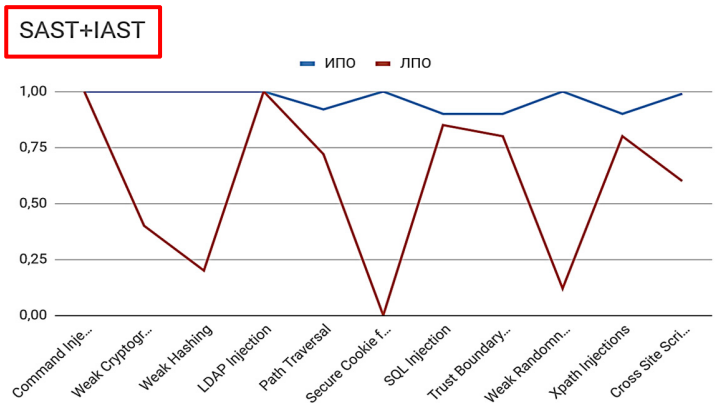


Рис. 4. График зафиксированных ИПО и ЛПО для *SAST* и *IAST*.

Заключение. По итогам проделанной работы можно сделать вывод, что для определения большинства видов уязвимостей SAST менее эффективен, чем IAST, так как у SAST большое количество ЛПО и низкое количество ИПО.

Несмотря на то, что совместное использование SAST и IAST приводит к повышению количества ложно положительных результатов, данная методика тестирования позволяет повысить количество истинно положительных результатов.

СПИСОК ЛИТЕРАТУРЫ

1. Al-Amin, S.; Ajmeri, N.; Du, H.; Berglund, E.Z.; Singh, M.P. Toward effective adoption of secure software development practices. Simul. Model. Pr. Theory 2018, 85, p. 33–46.
2. Antunes, N.; Vieira, M. Assessing and Comparing Vulnerability Detection Tools for Web Services: Benchmarking Approach and Examples. IEEE Trans. Serv. Comput. 2015; pp. 269–283.
3. Felderer, M.; Büchler, M.; Johns, M.; Brucker, A.D.; Breu, R.; Pretschner, A. Security Testing: A Survey. In Advances in Computers; Elsevier: Cambridge, MA, USA, 2016; pp. 18-19.
4. Goseva-Popstojanova, K.; Perhinschi, A. On the capability of static code analysis to detect security vulnerabilities. Inf. Softw. Technol. 2015, 68, pp. 18–33.
5. Mohino, J.D.V.; Higuera, J.B.; Higuera, J.-R.B.; Montalvo, J.A.S.; Higuera, B.; Mohino, D.V.; Montalvo, J.A.S. The Application of a New Secure Software Development Life Cycle (S-SDLC) with Agile Methodologies. Electronics 2019, p. 1218.
6. Monga M., Paleari R., Passerini E. Ahybridanalysisframeworkfordetectingwebapplicationvulnerabilities. In Proceedings of the 2009 ICSE Workshop on Software Engineering for Secure Systems, Vancouver, BC, Canada, 19 May 2009; pp. 25–32.
7. OWASP Foundation. OWASP Top Ten 2017 [Электронный ресурс]. – URL: https://www.owasp.org/index.php/Top_10_ 2017-Top_10 (Дата обращения 12.03.2021).

УДК 004.056

РАЗРАБОТКА ПО ДЛЯ ЭМУЛЯЦИИ ДЕЦЕНТРАЛИЗОВАННОГО ХРАНИЛИЩА ДАННЫХ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

Акилов Марк Валерьевич, Кушнир Дмитрий Викторович, Баталов Антон Сергеевич, Ковцур Максим Михайлович

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails markakilov@yandex.ru, dmitry.kushnir@gmail.com, lein.mydream@gmail.com, maxkovzur@mail.ru

Аннотация. Первоначально блокчейн использовался в сфере криптовалют. С течением времени данная технология начала интеграцию в другие сферы жизни людей, что повлекло за собой обострение проблемы масштабирования блокчейн. Ниже рассматриваются алгоритмы работы блокчейн на примере bitcoin. В статье приведен результат работы созданной программы для эмуляции работы блокчейн.

Ключевые слова: блокчейн; bitcoin; распределенные системы хранения; децентрализованные системы хранения.

DEVELOPMENT OF SOFTWARE FOR EMULATING A DECENTRALIZED DATA WAREHOUSE BASED ON BLOCKCHAIN TECHNOLOGY

Akilov Mark, Kushnir Dmitry, Batalov Anton, Kovzur Maxim
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails markakilov@yandex.ru, dmitry.kushnir@gmail.com, lein.mydream@gmail.com, maxkovzur@mail.ru

Abstract. Blockchain was originally used in the cryptocurrency space. Over time, this technology began to integrate into other spheres of human life, which led to an aggravation of the problem of blockchain scaling. The algorithms of blockchain operation are considered below using the example of bitcoin. The article shows the result of the work of the created program for emulating the blockchain operation.

Keywords: blockchain; bitcoin; distributed storage systems; decentralized storage systems.

Введение. Изначально в идею блокчейна легло стремление сформировать такие альтернативные технологии, которые исключили бы банки как посредников, исключили бы мошенничество и риски, а нормы программного кода заменили бы правовые нормы [1, 2].

В настоящее время появились и другие формы эффективного использования технологии блокчейна: сфера финансовых услуг, платежные сервисы, в государственном секторе – это госуслуги, реестры недвижимости, электронное голосование. Есть примеры применения блокчейна в транспортной логистике, здравоохранении, управлении интеллектуальной собственностью [3, 4]. Для успешного внедрения подобных практик необходимы полевые испытания, для которых лучше всего подходит эмуляция среды и технологий [5].

Исследование технологии блокчейн. Блокчейн (англ. block chain— цепь из блоков) – это технология децентрализованного распределенного хранения данных о транзакциях, совершенных участниками системы. Состоит из последовательно соединенных блоков, представленных на рис. 1. В заголовок каждого последующего блока включается хэш предыдущего. Таким образом составляется неразрывная цепь. Разорвать или изменить ее возможно, только если пересчитать все заголовки блоков и собрать цепочку заново с точки разрыва. Для этого необходимо использовать вычислительные ресурсы, эквивалентные или большие, чем те, что были затрачены при сборке оригинальной цепи [6, 7].

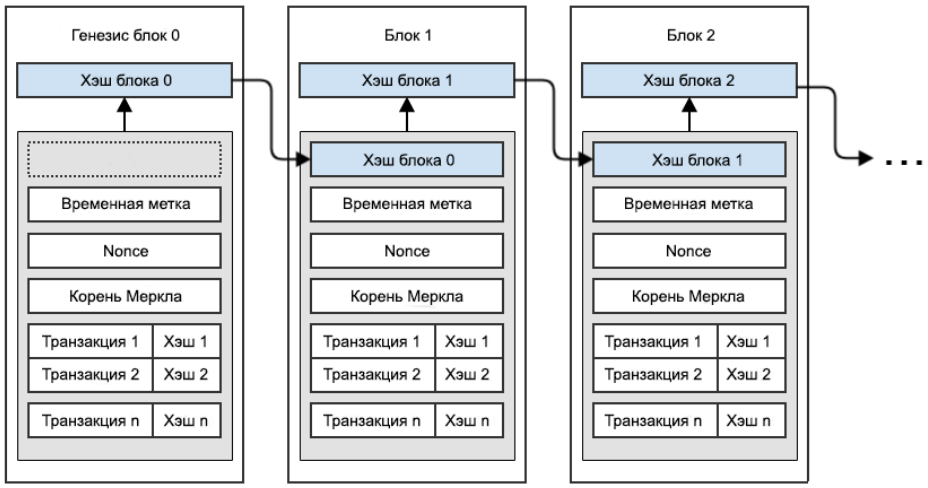


Рис. 1. Схема: Цепочка блоков.

Ключевые особенности блокчейна:

Децентрализация процессов хранения и обработки информации.

В блокчейне вся записанная информация хранится у каждого участника сети в полном объеме. Эта особенность позволяет создавать географически распределенные сети без дорогостоящих дата-центров, централизованных систем хранения данных и резервного копирования, а также обеспечивать локальный доступ к данным для каждого узла сети.

Доказуемая неизменяемость данных

Блокчейн решает проблему нелегитимного изменения данных, являясь неразрывной последовательностью криптографически связанных блоков, когда в любой момент времени имеется возможность проверить всю последовательность добавления информации, таким образом исключая возможность внесения любых изменений в отдельные участки цепи без ее полной перестройки.

Прозрачность операций.

Являясь одноранговой сетью, где все участники являются равноправными. Все участники блокчейна, имея данные обо всех транзакциях, могут проверить историю своих контрагентов при выполнении операций.

Безвозвратность транзакций

Данное свойство вытекает из всего вышеизложенного, так при гарантии хранения и неизменности информации безвозвратность транзакция является обратной стороной этих свойств.

Возможность анонимизации участников.

Каждый адрес в блокчейне является уникальным идентификатором, состоящий из обезличенного набора символов, и не содержит никакой информации, позволяющей провести взаимно-однозначное соответствие кошелька и его владельца, любой дополнительный анализ будет весьма сложным особенно при условии большого количества транзакций, к примеру, в повседневной жизни.

Отсутствие необходимости в доверии.

Данная особенность позволяет проводить транзакции при условии, что она корректна и выполнена проверка принадлежности адреса отправителя инициатору транзакции. В транзакциях используются механизм децентрализованного посредничества(escrow).

Поддержание работы сети самими участниками.

Каждый пользователь блокчейна может создать собственный узел (в публичных блокчейнах) и является владельцем созданных им токенов внутри цепи. Все это накладывает на них и определенный уровень ответственности по поддержанию работы самого блокчейна, так как в публичных блокчейнах нет никакой организации, которая будет делать это вместо них.

К вопросу о доверии в блокчейне.

Вопрос доверия является одним из основополагающих в технологии блокчейна. Доверие достигается с помощью аналога онлайн голосования, постоянно проводимого всеми узлами сети с децентрализованным управлением. В разных блокчейнах это голосование имеет разные формы, но во всех публичных блокчейнах для формирования единственно правильной последовательности блоков необходимо решение большинства или достижение так называемого консенсуса.

Функционирование блокчейна невозможно без консенсуса, то есть процесса согласования вносимых изменений [1].

Механизм консенсуса в системе также помогает предотвратить определенные виды атак. Теоретически злоумышленник может нарушить консенсус, контролируя 51% сети. Механизмы консенсуса разработаны, чтобы сделать эту «атаку 51%» невозможной.

Существует множество алгоритмов консенсуса, перечислим некоторые из них:

Proof-of-Work (PoW) – доказательство работы. Вклад участника вдостижение консенсуса определяется выполняемым им объемом вычислений. Метод PoW используется в Bitcoin и блокчейнах, созданных на его основе.

Proof-of-Stake (PoS) – доказательство доли. Вклад участника в достижение консенсуса определяется долей токенов блокчейна, которыми он владеет, от их общего количества.

Delegated Proof-of-Stake – этот алгоритм очень похож на PoS, но пользователи с большим количеством монет могут голосовать и выбирать представителей (других пользователей, которым они доверяют) для проверки транзакций, а ведущие представители (которые набрали наибольшее количество голосов) получают право проверять транзакции.

Leased Proof of Stake (LPoS) – усовершенствованная версия алгоритма Proof of Stake (PoS). Традиционно в алгоритме Proof of Stake каждый узел содержит определенную сумму криптовалюты и может добавить следующий блок в цепочку блоков. Однако, с помощью Leased Proof of Stake, пользователи могут сдавать в аренду свои монеты пользователям, держащим полные узлы (full nodes).

Proof-of-Capacity (Proof-of-space) – подтверждение емкости (PoC) это алгоритм согласованности используется в блокчейне и позволяет майнинг оборудованию использовать в сети доступное пространство на жестком диске для определения прав на майнинг вместо использования вычислительной мощности устройства.

Proof-of-Weight – каждому пользователю в сети, использующему Proof-of-Weight, присваивается «вес». Этот вес основан на том, сколько денег пользователь держит на своей учетной записи. Пока общая взвешенная часть пользователей честна, обычно две трети или больше, сеть будет оставаться безопасной.

Proof-of-Authority – доказательство полномочий. Находящийся в разработке алгоритм консенсуса, который предполагается использовать в управляемых (частично централизованных) блокчейнах. В этом алгоритме транзакции, подписанные участниками с повышенными полномочиями, будут иметь преимущество.

В качестве примера для разработки модели блокчена был взят алгоритм, успешно использующийся на текущий момент в блокчейне Bitcoin. В случае имитационной модели основные составляющие модели выглядит следующим образом:

- проведение транзакции;
- рассылка транзакции всем участникам сети;
- проверка транзакций, пришедших от других участников сети;
- создание блоков;
- передача блоков на проверку;
- проверка блоков;
- добавление блоков в базу данных, при удачной проверке;
- графическое представление для визуализации работы.

Для написания программы использовался язык программирования C++ с использованием фреймворка Qt и криптографической библиотеки OpenSSL для обеспечения максимально возможного охвата и расширения возможностей реализации.

Общая схема работы программы представлена на рис. 2.

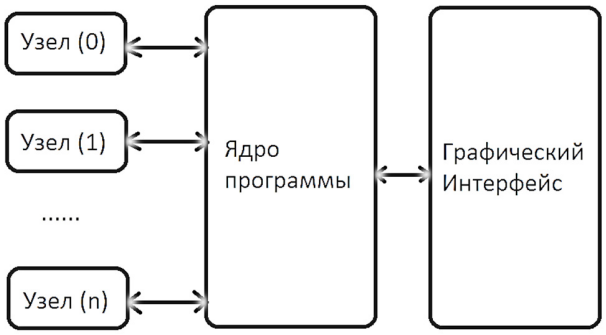


Рис. 2. Схема работы программы.

Узлы отвечают за основной функционал, т.е. работу с транзакциями, блоками и базой данных. Каждый узел имеет свою базу данных для демонстрации того, что сеть приходит к консенсусу. При проверке базы должны быть одинаковыми.

Децентрализованная распределенная система имитируется с помощью узлов и ядра программы, узлы осуществляют связь между собой с помощью ядра, ядро в данном случае можно представить, как среду передачи данных между узлами сети.

Управление осуществляется с помощью графического интерфейса, представленного на рис. 3. Сигналы управления отправляются в ядро программы, ядро либо перенаправляет сигнал узлам, либо выполняет другие необходимые действия.

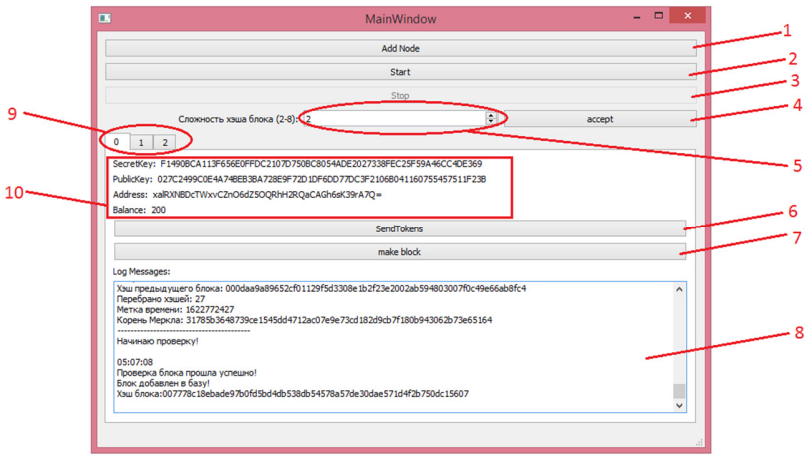


Рис.3. Интерфейс готового программного продукта.

«Add Node» добавить узел – добавляет новый узел.

«Start» – при нажатии все добавленные узлы начинают непрерывно высчитывать блоки.

«Stop» – останавливает вычисление блоков.

«Accept» – применяет заданную в (5) сложность хэша для блока.

Виджет для ввода сложности вычисляемого хэша блока, задается числом от 2 до 8. Это число определяет количество нулей в начале в 16-ричной записи хэша.

«Send Tokens» – открывает окно для осуществления транзакции.

«make block» – при нажатии все узлы начинают высчитывать хэш блока, но только один раз. Это функция применяется для пошагового режима работы.

Поле лога выбранного узла, в него выводится информация для отслеживания текущей работы данного узла.

Вкладки для переключения между узлами сети.

Информация о выбранном в данный момент узле.

При тестировании готового программного продукта выполняется создание узлов и начальный майнинг, в результате данные заполняются корректно, после чего возможно проведение транзакций между узлами.

Для наглядности различия затрат ресурсов для реализации эмуляции вычислений различного уровня сложности использовались графики зависимости создания блоков от времени при использовании четырех узлов.

Сложность 6. Среднее время добавление блока 9 секунд. За 14 минут было добавлено 93 блока. График выполнения операции можно увидеть на рис. 4.

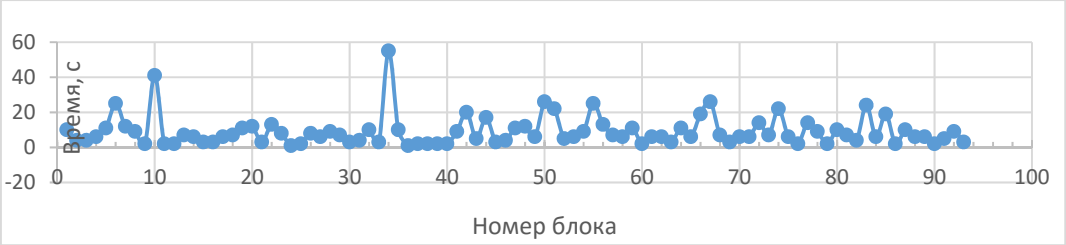


Рис. 4. График зависимости блока и времени его добавления (сложность 6).

Сложность 7. Среднее время добавление блока 96 секунд. За 21 минуту было добавлено 16 блоков. График представлен далее на рис. 5.

Рис. 5. График зависимости блока и времени его добавления (сложность 7).

Сложность 8. При сложности 8 добавление блоков, на используемом компьютере занимает уже слишком много времени, построить график не удалось. Один блок создавался примерно 43 минуты, что можно видеть по журналу операция на рис. 6.

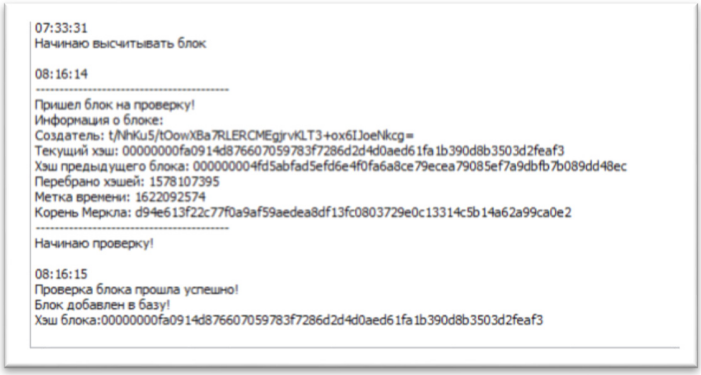


Рис. 6. Пример добавления блока при сложности 8.

Заключение. В связи с непрерывной модернизацией систем, тесно связанных с повседневной жизнью человека, с каждым годом растет спрос на использование блокчейнов [8-10]. Для качественного планирования инфраструктуры необходимо точно знать количественные показатели при использовании блокчейнов, понимать сильные и слабые стороны различных методик их создания [11, 12]. С помощью разработанной программы, эмулирующей работу блокчейна, опытным путем была выяснена разница в показателях быстродействия блокчейна с разными уровнями сложности формирования блоков. Показана возможность определения необходимых для поддержания работы того или иного блокчейна затрат вычислительных ресурсов.

СПИСОК ЛИТЕРАТУРЫ

1. Табернакулов А. Блокчейн на практике / Александр Табернакулов, Ян Койфманн. — Москва: Альпина Паблишер, 2019. — 260 с.
2. Б. Сингхал, Г. Дамеджа, П.С. Панда. Блокчейн. Руководство для начинающих разработчиков: Пер. с англ. / Б. Сингхал, Г. Дамеджа, П. С. Панда. – СПБ.: БХВ-Петербург, 2020. – 288м.: ил.
3. Литвин А.А. Возможности блокчейн-технологии в медицине (обзор)/ Литвин А.А., Коренев С.В., Князева Е.Г., Litvin V. // Современные технологии медицины. -2019. - № 4. -191.
4. Бондарь В.А. Возможности использования технологии блокчейн в системах электронного документооборота // Документ. Архив. История. Современность: сборник статей/ Уральский федеральный университет имени первого Президента России Б.Н. Ельцина. – Екатеринбург. – № 19 -2019. - С.280-290
5. Дорожная карта развития «сквозной» цифровой технологии «Системы распределенного реестра» URL: sdo.krsk.irgups.ru/pluginfile.php/25100/mod_resource/content/0/Дорожная карта Блокчейн.pdf (дата обращения 05.06.2021).
6. Пехтерева Е. А. Инновации в финансовой сфере и практика их применения: технология блокчейн и криптовалюта в России // ЭСПР. 2019. №1. -С.51.
7. Антонопулос А. М. Осваиваем биткойн: программирование блокчейна / Андреас М. Антонопулос; пер. с англ. А. В. Снастина. - Москва: ДМК Пресс, 2018. – 426 с.
8. Поручение Председателя Правительства Дмитрия Медведева по вопросу о возможности применения технологии блокчейн в системе государственного управления и экономике Российской Федерации 6 марта 2917 года // URL: http://government.ru/orders/selection/401/26653/ (дата обращения 05.06.2021).
9. Тапскотт А. Технология блокчейн: то, что движет финансовой революцией сегодня / Дон Тапскотт, Алекс Тапскотт ; [пер. с англ. К. Шашковой, Е. Ряхиной]. – Москва: Эксмо, 2017. -270 с.
10. Звягин Л.С. Цифровая экономика криптовалюты: вызов или угроза традиционному обществу//E-management/ том 1, N2., 2018 - С.80.
11. Красов А.В., Зуев И.П., Карельский П.В., Радынская В.Е., Гераськина В.С. Алгоритмы и методы защиты программного кода на базе обфускации // I-methods. 2020. Т. 12. № 1. С. 1-12.
12. Штеренберг С.И., Стародубцев И.В., Шашкин В.С. Разработка комплекса мер для защиты предприятия от фишинговых атак Защита информации // Инсайд. 2020. № 2 (92). С. 24-31.

УДК 004.056.53

ИССЛЕДОВАНИЕ УСТОЙЧИВОСТИ ОБОРУДОВАНИЯ MIKROTIK К АТАКЕ ASSOCIATION FLOOD НА БЕСПРОВОДНУЮ СЕТЬ СЕМЕЙСТВА IEEE 802.11

Ворошнин Григорий Евгеньевич[1], Ковцур Максим Михайлович[1], Кистуга Антон Юрьевич[2], Докшин Александр Денисович[1]

[1] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия

[2] ООО «Фаст Лайн»
Профессора Попова ул., 37В, Санкт-Петербург, 197136, Россия

e-mails: voroshnin.g@yandex.ru, maxkovzur@mail.ru, anton.kistruga@gmail.com, a.dokshin007@gmail.com

Аннотация. Беспроводные сети семейства IEEE 802.11 получили большую популярность и стали применяться повсеместно. Вместе с распространением сетей Wi-Fi стали популярные атаки на беспроводные сети. Простота реализации некоторых из них, зачастую не требующая никакой специальной подготовки, привела к их широкому распространению. В настоящее время атакам подвергаются как домашние, так и корпоративные сети. Также распространение сетей привело к многообразию сетевого оборудования и компаний, производящих его. Одной из таких компаний является MikroTik, получившая популярность в малых корпоративных сетях благодаря широкому функционалу и низкой стоимости производимого сетевого оборудования. В настоящей статье исследуется механизм атаки association flood, а также устойчивость оборудования компании MikroTik к данной атаке.

Ключевые слова: информационная безопасность; безопасность беспроводных сетей; устойчивость сетевого оборудования; MikroTik; атака association flood.

INVESTIGATION VULNERABILITIES OF EQUIPMENT MIKROTIK TO ASSOCIATION FLOOD ATTACK ON WIRELESS NETWORK OF THE IEEE 802.11 FAMILY

Voroshnin Grigory[1], Kovtsur Maxim[1], Kistruga Anton[2], Dokshin Alexander[1]

[1] The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia

[2] LLC «Fast Lane»
37B Professor Popov St, St. Petersburg, 197136, Russia

e-mails: voroshnin.g@yandex.ru, maxkovzur@mail.ru, anton.kistruga@gmail.com, a.dokshin007@gmail.com

Abstract. Wireless networks of the IEEE 802.11 family have gained great and have become widely used. Simultaneously with the spread of the Wi-Fi network, attacks on wireless networks have become popular. The ease of implementation of some of them, which often does not require any special training, has led to their widespread use. Both home and corporate networks are currently under attack. Also, the proliferation of networks has led to a variety of network equipment and companies that produce it. One of these companies is MikroTik, which has gained popularity in small corporate networks due to its wide functionality and low cost of manufactured network equipment. In this paper, we investigate the mechanism of attacks association flood, as well as the stability of the equipment company MikroTik to this attack.

Keywords: information security; wireless security; network equipment stability; MikroTik; association flood attack.

Введение. Беспроводные сети семейства IEEE 802.11 наряду с большой популярностью и распространенностью имеют очень серьезную уязвимость – общедоступную среду передачи данных. Это означает, что для перехвата данных и проведения различных атак злоумышленнику не требуется подключаться проводом к какому-либо сетевому оборудованию. Таким образом можно передавать в среду любой трафик, который изначально как точкой доступа, так и клиентами, будет рассматриваться как легитимный. Также опасность представляет перехват трафика, который в будущем может быть дешифрован или использован для атаки.

Не смотря на множество исследований атак на беспроводные сети [1-5], методов обеспечения безопасности [6-7], методик действий злоумышленников [9], устойчивость оборудования MikroTik исследовалась крайне мало [10-12]. Данная работа одной из своих целей имеет устранение этого недостатка.

При рассмотрении атаки association flood обратимся к рис. 1. На нем схематично представлен процесс подключения клиента к точке доступа, определенный стандартом IEEE 802.11.

Для успешного соединения клиенту необходимо пройти аутентификацию и ассоциацию, а при отключении – деассоциацию и деаутентификацию. Для поддержания беспроводной связи необходимо оставаться в состоянии 3. Точка доступа, в свою очередь, хранит таблицу состояний (ассоциаций) с информацией о каждом клиенте. Ее размер ограничен либо конкретным заданным числом записей, либо числом, основанным на ограничении физической памяти, выделенной для хранения таблицы.

Аутентификация с общим ключом ненадежна, поэтому используется редко. Альтернативой является открытая система аутентификации, опирающаяся на более высокий уровень проверки подлинности, например WPA-PSK (Pre-Shared Key) или WPA-EAP (Extensible Authentication Protocol). В таком случае любой клиент может пройти этап аутентификации, в результате чего отправляется кадр подтверждения успешной аутентификации и клиент сразу переходит в состояние 2. А после успешного прохождения этапа ассоциации клиент переходит в состояние 3.

Атака association flood направлена на заполнение таблицы ассоциаций точки доступа, в результате чего сетевое оборудование может отказать легитимным пользователям в доступе к сети. Также влияние оказывается на CPU оборудования – нагрузка на него может быть значительно увеличена. Сторонними явлениями при данной атаке может быть нарушение стабильности работы сетевого оборудования, зашумление беспроводной среды, исчерпание ресурсов беспроводного интерфейса.

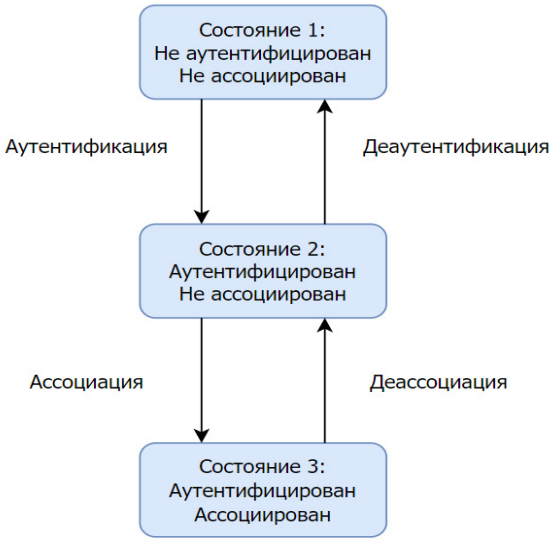


Рис. 1. Схема подключения клиента к точке доступа.

Тестирование производилось на лабораторном стенде [13] на оборудовании MikroTik модели «RB952Ui-5ac2nD».

Для проведения данной атаки злоумышленник отправляется пары кадров authentication и association request с различными MAC-адресами отправителя. Точка доступа воспринимает это как процесс подключения новых клиентов. В результате, после отправки множества пар кадров с разными MAC-адресами таблица ассоциаций, в которую записывается каждый подключающийся клиент, заполняется. Как показано на рис. 2, в результате атаки имитируемые злоумышленником клиенты переходят в состояние 3, а законные клиенты не могут получить доступ к сети.

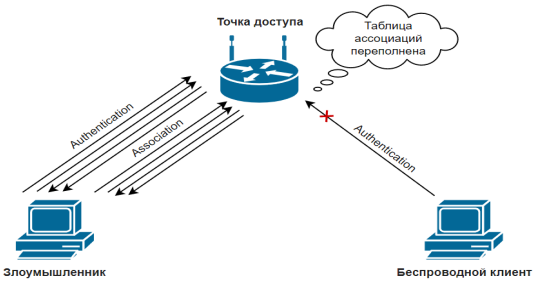


Рис. 2. Схема атаки Association flood.

Для проведения описываемой атаки использовалась утилита mdk4 в режиме «a» и с применяемыми опциями «i» (означает проведение атаки association flood, аргументом опции задается MAC-адрес точки доступа) и «-s» (аргументом задается число клиентов в секунду, подключающихся к ТД).

Для оценки влияния атаки на сетевое оборудование были выделены некоторые критерии:

Успешность атаки – получилось ли у злоумышленника добиться цели атаки.

Показатели оборудования (CPU, записи в log-файле и др.).

Показатели клиента (возможность подключения к сети, сетевые данные и др.).

Атака association flood показала высокую эффективность. Рассмотрим выдержку из дампа трафика, перехваченного во время атаки, обратившись к рис. 3.

686	7.302944	4a:ec:29:cd:ba:ab	Routerbo_b3:7d:3e	802.11	Authentication, SN=0, FN=0, Flags=........
810	7.367516	Routerbo_b3:7d:3e	4a:ec:29:cd:ba:ab	802.11	Authentication, SN=2216, FN=0, Flags=....R...
819	7.374993	4a:ec:29:cd:ba:ab	Routerbo_b3:7d:3e	802.11	Association Request, SN=0, FN=0, Flags=........, SSID=MikroTik
879	7.402836	Routerbo_b3:7d:3e	4a:ec:29:cd:ba:ab	802.11	Association Response, SN=2217, FN=0, Flags=....R...

Рис. 3. Дамп трафика при атаке association flood.

Легко заметить, что имитируемый злоумышленником клиент за доли секунды проходит аутентификацию и ассоциацию. В результате ТД присваивает клиенту состояние 3, ожидая от него продолжения аутентификации на более высоком уровне.

В это время в таблице зарегистрированных клиентов оборудования MikroTik поддерживалось порядка 50-60 записей, что можно увидеть на рис. 4.

Wireless Tables

WiFi Interfaces | W60G Station | Nstreme Dual | Access List | Registration | Connect List | Security Profiles | Channels

oo Reset

Radio Name	MAC Address	Interface	Uptime	AP	W...	Last Activit...	Tx/Rx Signal ...	Tx Rate	Rx Rate
	12:81:09:39:E3:87	wlan1	00:00:03	no	no	2.830	-40	1Mbps	---
	64:5B:EC:CA:B7:08	wlan1	00:00:03	no	no	2.710	-39	1Mbps	---
	B0:9C:8C:E2:76:F3	wlan1	00:00:03	no	no	2.680	-39	1Mbps	---
	C0:59:BE:F9:29:53	wlan1	00:00:03	no	no	2.680	-39	1Mbps	---
	EA:01:59:64:72:69	wlan1	00:00:03	no	no	2.640	-40	1Mbps	---
	84:95:11:11:77:87	wlan1	00:00:03	no	no	2.600	-39	1Mbps	---
	04:37:E1:C3:30:0A	wlan1	00:00:02	no	no	2.480	-40	1Mbps	---
	70:5E:AF:82:6F:26	wlan1	00:00:02	no	no	2.330	-39	1Mbps	---
	48:C2:38:F7:44:A7	wlan1	00:00:02	no	no	1.770	-39	1Mbps	---
	08:2D:A0:B0:2E:5D	wlan1	00:00:02	no	no	1.670	-39	1Mbps	---
	16:1B:0C:70:7F:7E	wlan1	00:00:01	no	no	1.240	-42	1Mbps	---
	D8:AD:F4:11:1D:E2	wlan1	00:00:01	no	no	1.140	-39	1Mbps	---
	68:DD:35:FB:DA:1A	wlan1	00:00:01	no	no	1.030	-38	1Mbps	---
	34:17:39:33:45:8A	wlan1	00:00:01	no	no	1.030	-40	1Mbps	---
	D2:96:CA:25:FE:F2	wlan1	00:00:01	no	no	0.980	-39	1Mbps	---
	08:89:95:20:86:11	wlan1	00:00:01	no	no	0.940	-39	1Mbps	---
	EC:A3:DE:08:1D:16	wlan1	00:00:01	no	no	0.910	-39	1Mbps	---

48 items

Рис. 4. Таблица зарегистрированных пользователей точки доступа во время атаки association flood.

Как видно из рис. 5, в log-файле ежесекундно добавлялись записи об отсоединении имитируемых злоумышленником клиентов в связи с тем, что после присоединения они не проходят аутентификацию более высокого уровня.

83	May/28/2021 23:49:54	memory	caps, info	00:04:E2:E2:B5:CA@CAP_1 rejected, does not provide suitable security method
84	May/28/2021 23:49:55	memory	caps, info	00:20:A6:4D:3D:34@CAP_1 rejected, does not provide suitable security method
85	May/28/2021 23:49:55	memory	caps, info	00:40:05:05:05:AC@CAP_1 rejected, does not provide suitable security method
86	May/28/2021 23:49:55	memory	caps, info	00:05:5D:BE:70:B5@CAP_1 rejected, does not provide suitable security method
87	May/28/2021 23:49:56	memory	caps, info	00:0A:41:41:B3:AF@CAP_1 rejected, does not provide suitable security method
88	May/28/2021 23:49:56	memory	caps, info	00:0D:93:49:FD:82@CAP_1 rejected, does not provide suitable security method
89	May/28/2021 23:49:57	memory	caps, info	00:C0:49:29:54:48@CAP_1 rejected, does not provide suitable security method
90	May/28/2021 23:49:57	memory	caps, info	00:03:2F:44:AC:5B@CAP_1 rejected, does not provide suitable security method
91	May/28/2021 23:49:58	memory	caps, info	00:0F:8F:42:E5:06@CAP_1 rejected, does not provide suitable security method
92	May/28/2021 23:49:58	memory	caps, info	00:30:BD:BD:2D:AD@CAP_1 rejected, does not provide suitable security method
93	May/28/2021 23:49:58	memory	caps, info	00:01:E6:4A:C4:30@CAP_1 rejected, does not provide suitable security method

Рис. 5. Содержимое log-файла сетевого оборудования во время атаки association flood

Рассмотрев все вышеперечисленное, не сложно предположить, что рассматриваемая атака оказывает значительное влияние на загрузку беспроводного интерфейса и CPU оборудования MikroTik. Как видно из рис. 6, нагрузка на CPU увеличилась до 9-10%, что в 3 раза превышает значение в режиме работы без воздействия на сеть.

Name	CPU	Usage
cpu0		9.0
firewall	0	0.5
logging	0	1.5
management	0	1.5
networking	0	0.5
routing	0	0.0
unclassified	0	0.5
winbox	0	0.5
wireless	0	4.0

Рис. 6. Profiling во время атаки association flood.

Также стоит заметить, что подключение к точке доступа легитимных клиентов во время атаки не удавалось. При неудачном подключении к сети, система Windows легитимного клиента, как видно из рис. 7, сообщала «Windows не удалось подключиться к MikroTik».

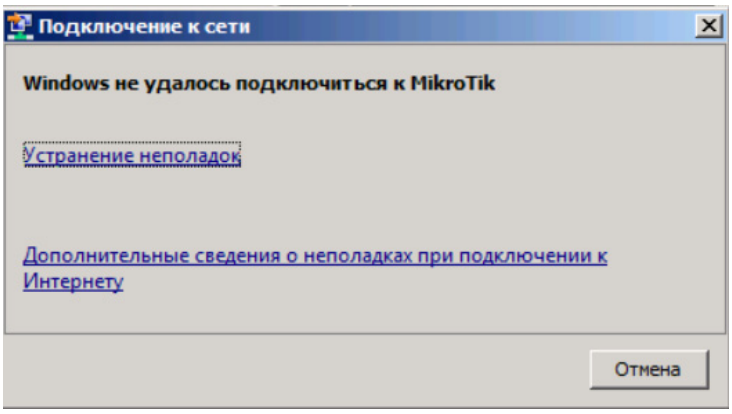


Рис. 7. Сообщение хоста легитимного клиента о неудачном подключении к беспроводной сети.

Для смягчения негативного влияния атаки на оборудование может служить отклонение части пакетов типов authentication и association request. Также требуется следить за состоянием таблицы ассоциаций, ведь последствия ее переполнения могут выражаться не только в невозможности подключения легитимных клиентов, но и в нестабильной работе самого оборудования.

В некоторых критических случаях нагрузки на оборудование следует отбрасывать все пакеты, чтобы сеть оставалась работоспособной, и злоумышленник не смог использовать сбои оборудования. Такие лояльные меры, как отклонение только части трафика, необходимы вследствие того, что легитимные клиенты беспроводной сети также могу отправлять сообщения рассматриваемых типов, а при отклонении всех пакетов достигается цель злоумышленника – клиенты не могут получить доступ к сети. Однако нужно заметить, что при большом количестве клиентов может создаться ситуация, схожая с атакой отказа в обслуживании на сеть.

Заключение. Сетевое оборудование от компании MikroTik является популярным, особенно в малых корпоративных сетях, а значит подвергается риску проведения на него различных атак, в то числе на беспроводные сети. Атака association flood показала высокую эффективность, выраженную в частичном нарушении работы беспроводной сети. Проявлялось нарушение работы сети в невозможности подключения новых клиентов во время атаки, а также значительном повышении нагрузки на CPU оборудования. Обладая достаточно широким функционалом, оно не имеет достаточных средств для противодействия атаке association flood. Но, при помощи встроенных инструментов мониторинга беспроводной среды, оно позволяет специалисту по информационной безопасности обнаружить данную атаку.

СПИСОК ЛИТЕРАТУРЫ

1. Шелухин, О. И. Особенности DDoS атак в беспроводных сетях / О. И. Шелухин, А. Г. Симонян, Ю. А. Иванов // T-Comm: Телекоммуникации и транспорт. – 2012. – Т. 6. – № 11.
2. Капарбек, Б. Анализ угроз информационной безопасности в беспроводных сетях / Б. Капарбек, Г. Э. Жалилов // Современные проблемы механики. – 2020. – № 39(1).
3. Механизмы реализации типовых атак на компоненты беспроводных сетей передачи данных / А. Г. Ломако, В. А. Овчаров, С. А. Акулов, В. С. Коротков // The 2017 Symposium on Cybersecurity of the Digital Economy (CDE'17) : Book of Abstracts, Иннополис, Республика Татарстан, Россия, 19–20 сентября 2017 года. – Иннополис, Республика Татарстан, Россия: Издательский Дом «Афина», 2017. – С. 249-254.
4. Анализ атак man in the middle / А. В. Лысенко, И. С. Кожевникова, Е. В. Ананьин [и др.] // Молодой ученый. – 2016. – № 30(134). – С. 33-36.
5. Исследование атак authentication failure и arp inject и методов их обнаружения в сетях семейства IEEE 802.11 / М. М. Ковцур, А. Ю. Киструга, Г. Е. Ворошнин, А. Э. Федорова // Информационные технологии и телекоммуникации. – 2021. – Т. 9. – № 1. – С. 87-98. – DOI 10.31854/2307-1303-2021-9-1-87-98.
6. Красов А.В., Обеспечение безопасности передачи MULTICAST-трафика в IP-сетях / Красов А.В., Сахаров Д.В., Ушаков И.А., Лосин Е.П. // Защита информации. Инсайд. 2017. № 3 (75). С. 34-42
7. Герлинг Е.Ю., Модели нарушителей информационной безопасности / Герлинг Е.Ю., Кулишкина Е.И., Бирих Э.В., Виткова Л.А. // Известия высших учебных заведений. Технология легкой промышленности. 2017. Т. 35. № 1. С. 27-30.
8. Красов А.В., Аутентификация программного обеспечения при помощи вложения цифровых водяных знаков в исполняемый код / Красов А.В., Верещагин А.С., Цветков А.Ю. // Телекоммуникации. 2013. № S7. С. 27-29.
9. Ахрамеева К.А., Анализ средств обмена скрытыми данными злоумышленниками в сети интернет посредством методов стеганографии / Ахрамеева К.А., Федосенко М.Ю., Герлинг Е.Ю., Юркин Д.В. // Телекоммуникации. 2020. № 8. С. 14-20.
10. Шамсутдинов, Р. Р. Использование маршрутизаторов Mikrotik Rb-951 в качестве средств защиты информационной инфраструктуры малых организаций / Р. Р. Шамсутдинов // European research: innovation in science, education and technology: XXXVII INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE, London, United Kingdom, 07–08 февраля 2018 года. – London, United Kingdom: PROBLEMS OF SCIENCE, 2018. – С. 26-28.
11. Васин, Н. Н. Исследование стабильности работы маршрутизатора Mikrotik с большим объемом маршрутной информации / Н. Н. Васин, А. С. Кондаков // III Научный форум телекоммуникации: теория и технологии ТТТ-2019 : Материалы XXI Международной научно-технической конференции, Казань, 18–22 ноября 2019 года. – Казань: Казанский государственный технический университет им. А.Н. Туполева, 2019. – С. 61-62.
12. Давидюк, Н. В. Обеспечение безопасности абонентского телетрафика путём конфигурирования и настройки маршрутизатора (на примере MikroTik RouterBOARD): Практикум / Н. В. Давидюк. – Санкт-Петербург: Общество с ограниченной ответственностью «Издательский центр «Интермедия», 2020. – 68 с. – ISBN 9785438301950.
13. Красов А.В., Методология создания виртуальной лаборатории для тестирования безопасности распределенных информационных систем / Красов А.В., Штеренберг С.И., Москальчук А.И.//Вестник Брянского государственного технического университета. 2020. № 3 (88). С. 38-46.

УДК 004.056.52

ДОСТУП К IP КАМЕРАМ КАК ОСНОВНОЙ ВОПРОС СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ

Гвоздков Игорь Вячеславович, Денисова Юлия Вячеславовна, Поведайко Максим Дмитриевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: gvozdkov@rambler.ru, mpovedaiko@yandex.ru, khoroshenko@mail.ru

Аннотация. Рассматриваются методы и способы доступа к конфиденциальной информации и её защита.

Ключевые слова: защита; доступ к информации; противодействие взлому информационных систем.

ACCESS TO IP CAMERAS AS THE MAIN ISSUE OF VIDEO SURVEILLANCE SYSTEMS

Gvozdkov Igor, Denisova Yulia, Povedayko Maxim
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: gvozdkov@rambler.ru, mpovedaiko@yandex.ru, khoroshenko@mail.ru

Abstract. Methods and access methods to confidential information and its protection are considered.

Keywords: protection; access to information; counter hacking information systems.

В настоящее время системы видеонаблюдения применяются повсеместно для охраны периметров специальных учреждений, для наблюдения за частной собственностью, а также за детьми. За последнее десятилетие системы видеонаблюдения достаточно качественно эволюционировали, кроме того, серьёзно модернизированы

системы видеофиксации и документирования информации. Произошла смена интерфейсов передачи видеосигнала, а также кардинально изменилась система взаимодействия всех систем.

Однако проблемы информационных систем видеонаблюдения остаются прежними:

Сложность построения системы;

– Задержки при передаче информации;
– «Случайности» удаления данных или самостоятельной переконфигурации системы;

Полный или частичный отказ узлов и компонентов.

Конечно, современные системы видеонаблюдения строятся по следующим принципам (при наличии грамотного персонала):

– Резервирование электропитания для всех узлов и компонентов;
– Разделение прав доступа для устройств и компонентов;
– Оптимизация оборудования и достаточность и т.д.;
– Физическая защита оборудования.

В современных системах видеонаблюдения подлежат защите следующие элементы:

– Идентификаторы пользователя и пароли;
– Неиспользуемые порты;
– Кабельное хозяйство и все оконечные устройства в целом.

Отдельно необходимо упомянуть про контроль активности сетевого окружения. Достаточно часто бывает так, что система видеонаблюдения является частью ЛВС предприятия или организации. Разберём подробнее ситуацию, когда система видеонаблюдения имеет выход в интернет.

Во всемирной паутине (даже не пересекая черту darknet) большое количество подобных форумов (рис. 1), где пользователи сети делятся подобными сообщениями.

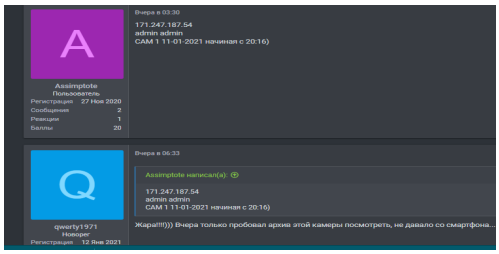


Рис. 1. Пример сообщений форума «https://bhf.im/…».

Отдельное сообщение вызвало особый интерес (рис. 2).

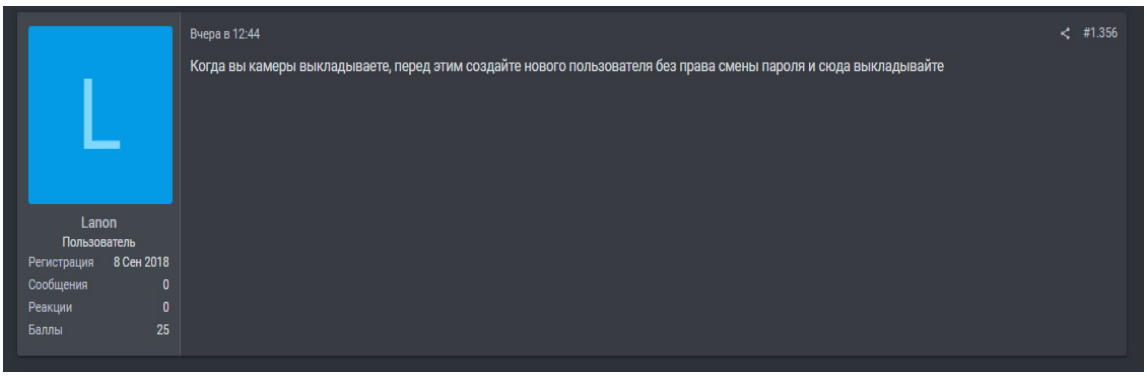


Рис. 2. Пример сообщения форума «https://bhf.im/…», пользователь Lanon.

Как следствие, напрашивается вопрос о соблюдении норм приличия, поскольку сторонние пользователи просматривают содержимое чужих камер, что кардинально влияет на безопасность объекта наблюдения, так как для доступа к камере необходимо иметь имя доступа и пароль. Проанализировав в форумах темы доступа к IP-камерам, было установлено, что пароли к устройствам видеонаблюдения там попадаются весьма разнообразные, от простых, приведённых на рис. 1 выше, до весьма замысловатых и достаточно длинных, составленных по всем правилам. Сервисы по взлому пароля существуют, их краткое описание можно найти на страницах интернет-ресурса Хабр [1]. Для взлома пароля приведёнными ресурсами, допустим из 5 цифр, понадобится около 8 дней, а для пароля из букв и цифр время взлома увеличивается и может варьироваться от года для нескольких десятков лет, не говоря уже о паролях со спецсимволами.

Для решения этих вопросов было принято решение воспользоваться сервисом Shodan [2].

Посредством команды realm=«GoAhead», domain=«:81» (рис. 3) выводим на отображение список камер, передающих видео по порту 81. Необходимо упомянуть, что порт может быть любой.

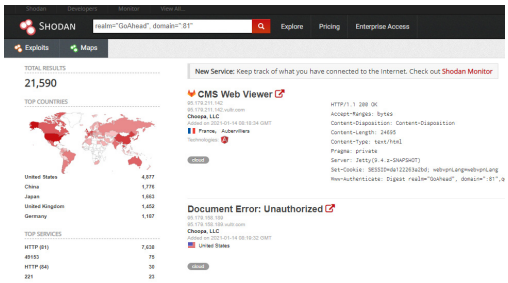


Рис. 3. Диалоговое окно программы Shodan.

В нашем случае это будет выглядеть следующим образом: 181.163.1.209:81/system.ini?loginuse&loginpas. Получаем ответ в виде файла, открываем его (рис. 4, 5).

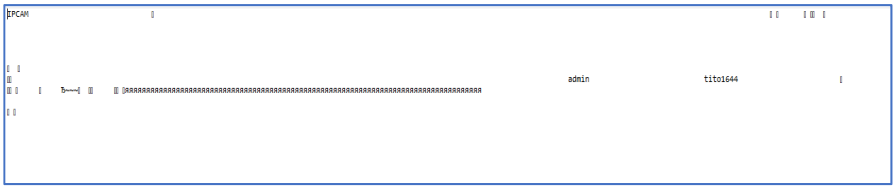


Рис. 4. Файл system.

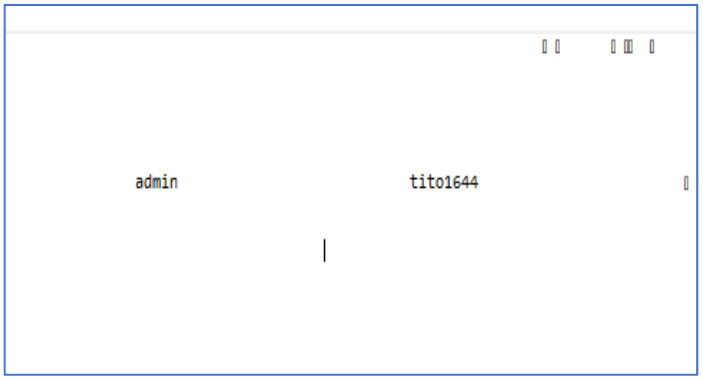


Рис. 5. Файл system. Фрагмент.

К сожалению, во многих IP-камерах есть уязвимость, о которой производители умышленно умалчивают. Получив такой файл system, уже не важна сложность сгенерированного пароля. Выполнив следующую команду (рис. 6), моментально получаем доступ к камере.

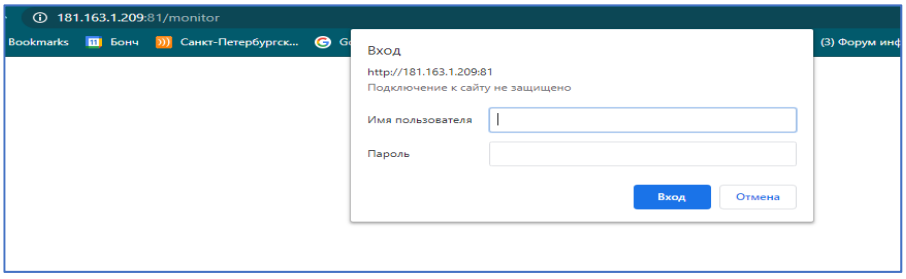


Рис. 6. Получение доступа в IP-камере.

Дальнейшие действия с «tito1644» проводить нецелесообразно, неэтично, да и незаконно, однако можно утверждать, что мы уже проникли в его систему видеонаблюдения и можем делать там всё, что нам вздумается (создавать новых пользователей без права смены пароля).

Подводя итоги, необходимо сказать, что, если IP-камера имеет доступ в интернет, она уязвима, и перенаправить видеопоток с неё можно в любую точку земного шара. Доказательством этому является то, что

местонахождение камеры, с которой мы работали, – США. Очень прискорбно, что многие разработчики IP-камер сознательно игнорируют указанный недостаток и не спешат устранить этот баг.

К сожалению, если возникает необходимость строить действительно конфиденциальную систему, то обязательно нужно учитывать, что такого существенного недостатка лишены лишь локальные системы, которые не имеют связи с внешним миром или обращение к камере которых блокирует файрволл, однако, если провести качественную разведку открытых портов, и это средство можно обойти.

Для нивелирования данного недостатка лицам, занимающимся проектированием и установкой систем видеонаблюдения, необходимо дать следующую основную рекомендацию: в ходе разворачивания систем видеонаблюдения нужно максимально заботиться о локальности системы (применении отдельных серверов, рабочих мест и прокладки отдельных магистралей видеонаблюдения, не задействованных и не подключенных к интернет даже через ПК), также необходимо постоянно помнить о закрытии и постоянном мониторинге портов доступа, установки файрволлов и антивирусного программного обеспечения с обязательным включением брандмауэра.

Все вышеперечисленные методы значительно усложнят несанкционированный доступ в систему, если не предотвратят его в полном объеме.

СПИСОК ЛИТЕРАТУРЫ

1. [Электронный ресурс] URL: https://habr.com/ru/post/67375/ (Дата обращения 10.01.2021).
2. [Электронный ресурс] URL: https://networkguru.ru/kak-ispolzovat-poiskovik-shodan/ (Дата обращения 10.01.2021).

УДК 004.056.53

ИССЛЕДОВАНИЕ ИНСТРУМЕНТОВ ДЛЯ СИСТЕМЫ АВТОМАТИЗАЦИИ ТЕСТИРОВАНИЯ СЕТЕВОГО ОБОРУДОВАНИЯ

Карельский Павел Владимирович, Ковцур Максим Михайлович, Штеренберг Станислав Игоревич, Малинин Никита Игоревич

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: pasha.karelscky@yandex.ru, maxkovzur@mail.ru, shterenberg.stanislaw@yandex.ru

Аннотация. В наши дни во многих направлениях индустрии телекоммуникаций возникает задача тестирования оборудования с целью проверки соответствия заявленных функций устройства принятым стандартам и рекомендациям международных уполномоченных организаций. Вследствие того, что рынок телекоммуникационного оборудования ежегодно обновляется новыми моделями устройств, поддерживающими последние стандарты, специалисты компаний-операторов связи проверяют образцы закупаемого оборудования, внедряемого на сети. В свою очередь производители и дистрибьюторы оборудования проводят собственные тестирования – как на соответствие заявленным характеристикам производительности, так и для проверки работоспособности функционала. В статье представлено исследование основных инструментов для системы автоматизации тестирования телекоммуникационного оборудования.

Ключевые слова: информационная безопасность; система автоматизации; Ansible.

RESEARCH OF INSTRUMENTS FOR AUTOMATION SYSTEM TESTING NETWORK EQUIPMENT

Karelsky Pavel, Kovtsur Maxim, Shterenberg Stanislav, Malinin Nikita

The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: pasha.karelscky@yandex.ru, maxkovzur@mail.ru, shterenberg.stanislaw@yandex.ru

Abstract. Nowadays, in many areas of the telecommunications industry, the task of testing equipment arises in order to verify the compliance of the declared functions of the device with the accepted standards and recommendations of international authorized organizations. Due to the fact that the telecommunications equipment market is annually updated with new models of devices that support the latest standards, the specialists of telecom operators check samples of purchased equipment that are being implemented on the network. In turn, manufacturers and distributors of equipment conduct their own tests - both for compliance with the declared performance characteristics and for checking the functionality of the functionality. The article presents a study of the main tools for a telecommunication equipment testing automation system.

Keywords: information security; automation system; Ansible.

Введение. Автоматизация – это процесс введения в алгоритм действий, необходимых для выполнения той или иной задачи, элементов, выполняемых техническими средствами, в результате чего уменьшается потребность в персональном участии человека в работе по созданию, преобразованию и эксплуатации продуктов, энергии или информации.

В общем случае процесс автоматизации можно описать в несколько этапов [1, 2]. В первую очередь формируется унифицированный алгоритм для выполнения задачи. Стандартизация процесса является необходимым компонентом из-за того, что при произвольном изменении процесса работы, изменении последовательности выполняемых действий невозможно внедрить элементы автоматизации в систему. Второй этап – это моделирование системы автоматизации для стандартизированного процесса, в которое входит определение этапов, на которых можно ограничить участие человека в процессе и создание технических средств для этого.

Изначально автоматизации представляла собой внедрение аппаратных средств в производство – конвейера, машин, выполняющих однотипную работу. В наше время все чаще под автоматизацией подразумевается использование программных элементов в различных сферах человеческой деятельности [3, 4].

Далее приведем сравнение существующих систем автоматизации. Первая система – это Ansible.

Ansible — это простая общедоступная платформа автоматизации IT решений работающая на Python, которая упрощает развертывание и обслуживание приложений и систем. Ansible позволяет автоматизировать все, от развертывания кода до конфигурации сети и управления облаком, на языке YAML, который приближается к простому английскому, с использованием SSH и без агентов для установки в удаленных системах. Ansible имеет модульную структуру и состоит из нескольких компонентов. Базовая структура Ansible представлена на рис. 1 [5, 6].

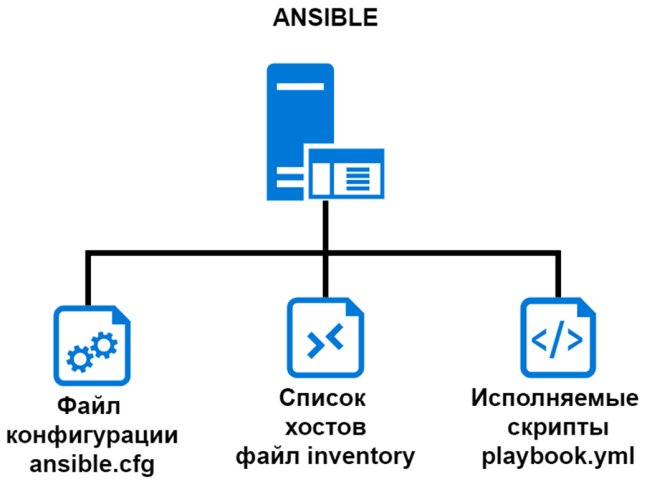


Рис. 1. Базовая структура Ansible.

В состав системы входят:

Inventory – файл, в котором содержаться указания по подключению к удаленным устройствам, такие как IP адрес и метод подключения. Удаленные устройства в этом файле могут быть сгруппированы для одновременной работы с ними.

Playbooks – файл, в котором содержаться команды, предназначенные для выполнения на удаленных устройствах. Playbook написан на YAML. Этот язык имеет максимально упрощенный синтаксис, который поймет любой специалист, имевший опыт работы с системами типа Lnux, вне зависимости от навыков программирования на других языках.

Файл конфигурации – указывает на расположение файла inventory, директорию с модулями Ansible, пользователя и ряд других стандартных параметров.

Ansible имеет ряд ограничений. Главное из них – это возможность работы исключительно через SSH соединение. Поскольку предложенная в данной работе методика подразумевает стартовую конфигурацию тестируемого оборудования «с нуля», необходимо использовать последовательный интерфейс RS-232, не предназначенный для связи по протоколу SSH. Вследствие этого в рамках данного исследования промежуточным звеном между платформой автоматизации и сетевым оборудованием является персональный компьютер, с установленной на нем операционной системой Kali Linux, имеющий несколько консольных портов, к которым подключается настраиваемое оборудование по RS-232. Таким образом оператор Ansible будет подключаться не напрямую к оборудованию, а к ПК, которому подключено тестируемое оборудование, по протоколу SSH, и через интерфейс командной строки (shell) Linux транслировать необходимые команды на сетевое оборудование, перенаправляя их на интерфейс последовательного порта ttyS*.

Помимо конфигурации оборудования Ansible также позволяет автоматизировать работу других элементов стенда тестирования.

Автоматизация тестирования создает ограничение в использовании программного обеспечения. Это ограничение заключается в невозможности использовать программное обеспечения с графическим

пользовательским интерфейсом в качестве автоматизируемого элемента. Из этого следует, что при подборе инструментов для проведения тестирования приходится выбирать только из консольных приложений, выполняющих требующие задачи, для корректного введения команд управления в скрипты. Тем не менее это не следует рассматривать как недостаток конкретного выбранного инструмента автоматизации, то есть Ansible. Для любой системы автоматизации привязка управления приложением исключительно через графический интерфейс приводит к невозможности его внедрения в названную систему. В ходе исследования изучалась также концепция построения системы автоматизации на Bash-скриптах. Плюсом такой системы являлась кроссплатформенность, а также независимость от существующего ПО для автоматизации. С другой стороны, для такого варианта значительно сложнее создать единую систему, способную охватить процесс тестирования целиком. Кроме того, для передачи задач другим исполнительным узлам требовалось бы введение дополнительных инструментов. На рис. 2 представлен пример Bash-скрипта для конфигурации тестируемого оборудования.

В нем используются команды для пакетного клиента ctel, который позволяет передавать команды удаленным устройствам. Данные команды передаются на сетевой контроллер BT-5005, на котором обрабатываются и передаются через консольный интерфейс на настраиваемое устройство. Пример наглядно показывает, что в сравнении системой Ansible, в варианте автоматизации Bash-скриптами возникает гораздо больше промежуточных элементов, что является нежелательным качеством любой системы.

```
cd C:\Ctel
ctel /host:172.16.1.35 /port:23 /ent
/com:admin /ent
/com:qtech /ent
/com:console 1 /ent
/com:raisecom /ent
/com:raisecom /ent
/com:config /ent
/com:create vlan 30 active /ent
/com:int vlan 30 /ent
/com:ip add 172.16.30.112 /ent
/com:exit /ent
/com:ip verify source /ent
/com:ip source binding 172.16.30.80 0000.0000.0020 vlan 30 gigaethernet 1/1/1 /ent
/com:interface gig 1/1/1 /ent
/com:sw mode trunk /ent
/com:sw trunk allowed vlan all confirm /ent
/com:interface gig 1/1/3 /ent
/com:sw mode trunk /ent
/com:sw trunk allowed vlan all confirm /ent
/com:ip verify source trust /ent
/com:exit /ent
/com:exit /ent
/com:hostname ipsg-test_1 /ent
```

Рис. 2. Содержание bash-скрипта для конфигурации коммутатора.

Вторая система – это Puppet. Считается наиболее используемым из четырех, исследуемых систем. Он наиболее полон с точки зрения возможных действий, модулей и пользовательских интерфейсов, представляя полную картину ЦОД, охватывая почти каждую операционную систему и предоставляя утилиты для всех основных ОС. Начальная установка относительно проста, требует развертывания головного сервера и клиентских агентов на каждой управляемой системе.

Следующая система – Chef. Похожа на Puppet с точки зрения общей концепции, в нем также имеется головной сервер и агенты, установленные на управляемых узлах. В дополнение к головному серверу, установка Chef также требует рабочей станции, для управления им. Агенты могут быть установлены с рабочей станции с помощью утилиты knife, которая использует протокол SSH для развертывания, облегчая бремя установки. После этого, управляемые узлы аутентифицируются с головным при помощи сертификатов.

Ansible больше похож на Salt, чем на Puppet или Chef. Ansible фокусируется на оптимизации и скорости, и не требует установки агентов на управляемые узлы — все функции производятся по SSH. Ansible написан на python, в отличие от Puppet и Chef, основанных на ruby.

Salt схож с Ansible в том, что основан на командной строке. Он использует метод push для связи с клиентами. Он может быть установлен через Git или через систему управления пакетами на головном сервере и клиентах. Клиент делает запрос к головному серверу, и если тот дает разрешение, позволяет управлять данным узлом с помощью агента (в терминах Salt — minion).

Тогда как Puppet и Chef ориентированы на разработчиков, Salt и Ansible больше подходят для нужд системных администраторов. Простой интерфейс и удобство использования Ansible подходят мышлению сисадминов в компаниях с большим числом Unix и Linux систем. Ansible быстри и легко запускается «из коробки». Описание выявленных преимуществ и недостатков рассмотренных систем представлено в таблице 1.

Таблица 1

Сравнение систем автоматизации

	Преимущества	Недостатки
Puppet	Модули могут быть написаны на ruby, или на более простом, производном от ruby языке Команды Push позволяют применять изменения немедленно Веб-интерфейс поддерживает отчеты, инвентаризацию и управление узлами в реальном времени Детализированные отчеты о работе агентов и конфигурации узлов	Требуется изучение встроенного языка или ruby Процессу установки недостает отчетов об ошибках
Chef	«Поваренные книги» и рецепты используют всю мощь ruby Централизованные, основанные на JSON массивы данных позволяют скриптам заполнять переменные во время работы Веб-интерфейс позволяет вести поиск и учет узлов, просматривать их активность, применять «поваренные книги» и роли	Требуется знание ruby В данный момент недостает функциональных команд push Документация местами неясная
Ansible	Модули могут быть написаны почти на любом языке Не требуются агенты на управляемых узлах Веб-интерфейс позволяет настраивать пользователей, команды и оборудование, применять сценарии Очень просто настраивается и запускается	Недостает поддержки клиентов для Windows Веб-интерфейс автоматически не связывается с существующей установкой Ansible; данные должны быть импортированы
Salt	Конфигурационные файлы могут быть простыми YAML-шаблонами или скриптами на pyhton и PyDSL Может связываться с клиентами через SSH или с помощью локально установленных агентов Веб-интерфейс позволяет просматривать запущенные задачи, статус подчиненных узлов и позволяет выполнять комнады на клиентах Крайне хорошо масштабируется	Веб-интерфейс не такой зрелый и полный как у конкурентов Не хватает инструментов для детальных отчетов

В качестве инструментов для работы с проходящим через сетевое оборудование трафиком, при разработке системы автоматизации можно использовать консольные утилиты.

Для генерации трафика используется trafgen. Эта утилита входит в пакет анализатора трафика Netsniff-ng и является удобным инструментом для тестирования прохождения трафика в сети [7, 8]. Помимо возможности генерировать пакеты по определяемым пользователем параметрам, данная программа способна передавать в сеть трафик из файлов формата .pcap. Именно этот функционал trafgen задействован в работе при выполнении тестов на коммутаторе. Управляющие скрипты Ansible через данную утилиту, установленную на генераторе трафика, запускают передачу заранее подготовленных дампов трафика, составленных таким образом, что по результатам прохождения тех или иных пакетов при тестировании механизмов безопасности коммутатора можно было судить о корректности их работы.

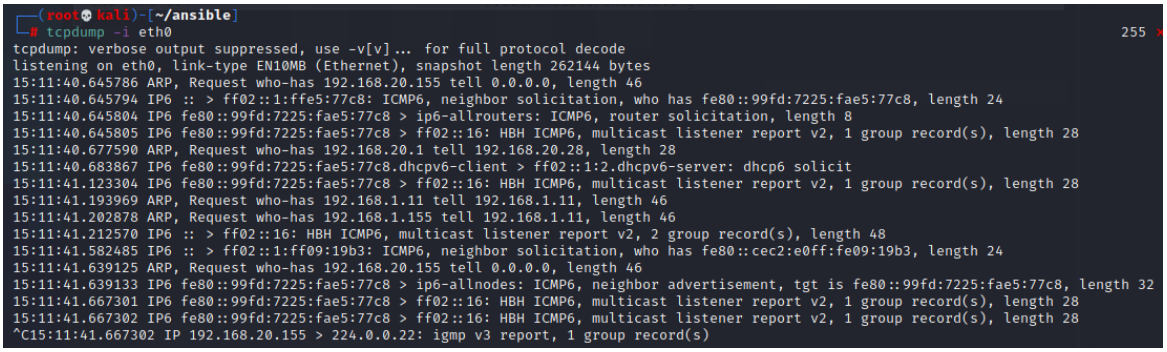


Рис. 3. Вывод tcpdump в окне терминала Kali.

Для захвата трафика на приемной стороне можно использовать tcpdump. Это пакетный сниффер, управляемый через shell. Он позволяет захватывать трафик в соответствии с выбранным интерфейсом и пользовательскими фильтрами. В стандартном режиме работы без введения дополнительных опций весь полученный на интерфейсе график выводится в окно терминала в реальном времени. На рис. 3 представлен стандартный формат вывода захваченного трафика tcpdump.

Помимо этого, программа позволяет записывать дамп трафика в файл для возможности дальнейшего анализа.

Заключение. В статье исследованы и описаны основные инструменты для создания системы автоматизации тестирования сетевого оборудования. В дальнейших работах планируется использовать Ansible.

СПИСОК ЛИТЕРАТУРЫ

1. Красов, А.В., Косов Н.А., Холоденко В.Ю. Исследование методов провижининга безопасной сети на мультивендорном оборудовании с использованием средств автоматизированной конфигурации // Colloquium-journal. 2019. № 13-2 (37). С. 243-247.
2. Красов, А.В., Сахаров Д.В., Ушаков И.А., Лосин Е.П. Обеспечение безопасности передачи multicast-трафика в IP-сетях // Защита информации. Инсайд. 2017. № 3 (75). С. 34-42.
3. 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.
4. Чмутов М.В., Ковцур М.М., Ушаков И.А., Пестов И.Е. Исследование действующей ИТ-инфраструктуры организации для последующего перехода к облачной архитектуре // В книге: Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. 2017. С. 535-537.
5. Герлинг Е.Ю., Ахрамеева К.А. Формирование моделей нарушителей систем контроля и управления доступом на объекте // В сборнике: Инновационные технологии и вопросы обеспечения безопасности реальной экономики. Сборник научных трудов по итогам Всероссийской научно-практической конференции. Под редакцией Г.В. Лепеша, О.Д. Угольниковой, С.Ю. Александровой. 2020. С. 58-65.
6. Ansible Documectation [Электронный ресурс], URL: www.docs.ansible.com/ (Дата обращения: 16.04.2021).
7. Netsniff-NG Toolkit [Электронный ресурс], URL: www.netsniff-ng.org/ (Дата обращения: 16.04.2021).
8. Ахрамеева К.А., Малинин Н.И., Герлинг Е.Ю., Бочаров М.В., Куликов И.А. Автоматизированное тестирование функций безопасности клиентских портов коммутатора // Заметки ученого. 2021 №5 С. 55-61.

УДК 004.056.5

ИССЛЕДОВАНИЯ ФУНКЦИОНАЛА PFSENSE ДЛЯ СРАВНЕНИЯ VPN ПРОТОКОЛОВ

Ковцур Максим Михайлович, Сахаров Дмитрий Владимирович, Мисливский Борис Сергеевич, Михайлова Анастасия Валерьевна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: mislivskyboris@yandex.ru, sguard7@mail.ru, maxkovzur@mail.ru, ova.007@yandex.ru

Аннотация. Рассмотрены понятия и теоретические сведения о технологии VPN, включая следующие технологии: IPsec и OpenVPN. Изучены особенности функциональности сетевой операционной системы pfSense. Был осуществлен обзор инструментов для оценки количественных критериев эффективности VPN. В рамках практической части было осуществлено сравнение ранее указанных протоколов туннелирования на базе развернутого виртуального стенда «подключение удаленного пользователя через VPN-шлюз» и измерение пропускной способности VPN.

Ключевые слова: VPN; IPsec; OpenVPN; pfSense; сравнение; пропускная способность.

PFSENSE FUNCTIONAL STUDIES TO COMPARE VPN PROTOCOLS

Kovzur Maxim, Mislivskij Boris, Saharov Dmitrij, Mihajlova Anastasija

The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: mislivskyboris@yandex.ru, sguard7@mail.ru, maxkovzur@mail.ru, ova.007@yandex.ru

Abstract. The concepts and theoretical information about VPN technology, including the following technologies: IPsec and OpenVPN, are considered. The features of the functionality of the pfSense network operating system have been studied. A review of tools for assessing quantitative criteria for VPN performance was carried out. As part of the practical part, a comparison of the previously mentioned tunneling protocols was carried out on the basis of the deployed virtual stand «connecting a remote user through a VPN gateway» and measuring the VPN throughput.

Keywords: VPN; IPsec; OpenVPN; pfSense; comparison; throughput.

Введение. В настоящее время был осуществлен массовый и быстрый переход на дистанционный формат работы. Такая принудительная мера существенно отразилась на форме организации производственной деятельности: согласно опросу за апрель 2020 года, ВЦИОМ и Social Business Group установили, что число россиян, выполняющих свои профессиональные функции удаленно, возросло в 8 раз (2% до пандемии, 16% после) [1]. Вместе с ростом количества удаленных рабочих мест появляются проблемы, связанные с обеспечением конфиденциальности,

целостности и доступности корпоративных данных. Для решения данных проблем и организации защищенного канала связи с удаленными сотрудниками применяется технология VPN. На данный момент существует большое количество протоколов и готовых решений по организации виртуальных частных сетей, поэтому важно осуществить оптимальный выбор технологии для создания удаленного доступа.

Технология VPN (англ. Virtual Private Network) — используется для создания изолированных сетей на базе открытых каналов связи, например Интернет. За счет использования средств криптографии такие виртуальные частные сети могут обеспечивать требуемый уровень безопасности и секретности, являясь более экономичным аналогом выделенных линий. Популярным способом для организации удаленного доступа являются продукт OpenVPN и решения на базе стандарта IPsec, согласно [2].

OpenVPN является программным продуктом для создания виртуальной частной сети с открытым исходным кодом. В OpenVPN используется протокол TLS для туннелирования трафика, а также виртуальные интерфейсы tap и tun для работы VPN на канальном или сетевом уровне. Для шифрования трафика используется открытая библиотека OpenSSL, которая включает в себя широкий набор алгоритмов шифрования и хэширования, а также может быть расширена модулями с дополнительными алгоритмами, в том числе ГОСТ. Из-за особенности работы библиотеки OpenSSL в OpenVPN ограничено использование ресурсов многоядерных процессоров.

IPsec (сокращение от IP Security) – это группа протоколов, которая включает в себя алгоритмы для обеспечения конфиденциальности данных, аутентификации, проверки подлинности, а также защищенного обмена ключами в интернете. IPsec является популярным, актуальным и востребованным стандартом, реализация которого используется в коммерческих программно-аппаратных комплексах Cisco, Check Point и Juniper, а также в открытых программных продуктах StrongSwan, LibreSwan и других.

Для сравнения протоколов туннелирования необходимо определиться с критериями оценивания. Критерии можно разделить две большие группы: качественные и количественные. Количественные критерии могут быть выражены в числовом виде и измерены экспериментальным путем. Проводить такое измерение VPN протоколов удобнее с помощью специализированной сетевой операционной системы, которая будет отличаться быстротой развертывания, функциональность и встроенной поддержкой рассматриваемых решений. Выбор был сделан в пользу проекта с открытым исходным кодом pfSense.

pfSense — это сетевая операционная система, основанная на ядре FreeBSD, включающая в себя функционал маршрутизатора, межсетевого экрана, а также VPN-сервера и ряда других. Для настройки и управления используется веб-интерфейс, из которого также возможна установка дополнительных пакетов из репозитория. Операционная система может быть установлена как на аппаратном обеспечении, так и в среде виртуализации.

pfSense поддерживает создание всех видов IPsec туннелей, имеется реализация OpenVPN. Также в дистрибутиве присутствует функционал формирователя трафика (traffic shaping) под названием Limiters, поддержка отказоустойчивых кластеров и подробная служба мониторинга состояния система, включающая отображение использования памяти, загрузки центрального процессора и использования сетевых ресурсов. На рис.1 показана главная страница веб-интерфейса pfSense.

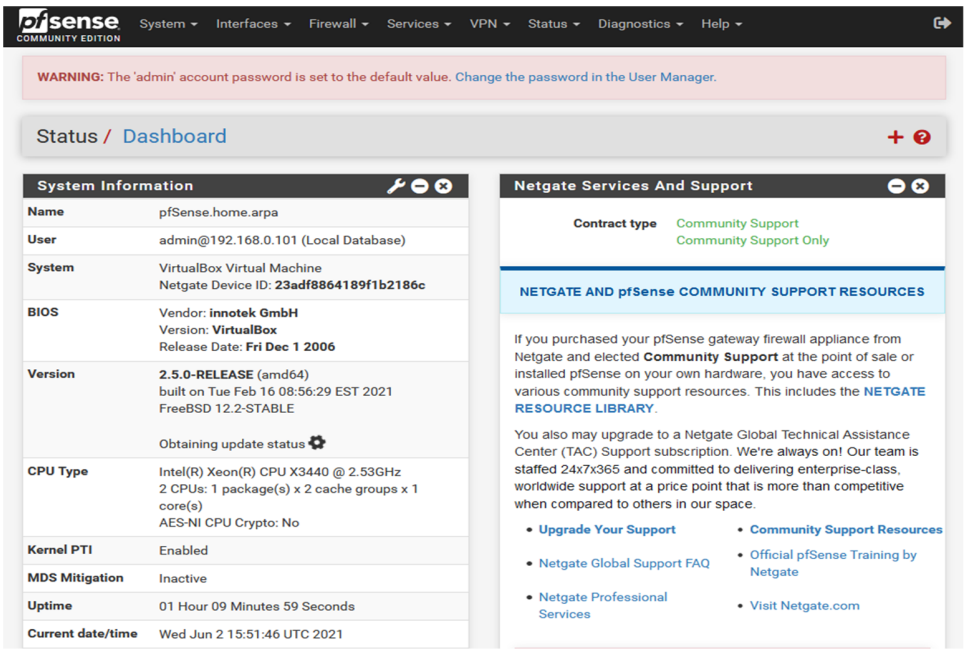


Рис. 1. Графический интерфейс pfSense.

Вся настройка VPN подключений происходит в одноименное вкладке, где возможно создание IPsec, OpenVPN и L2TP туннелей. Также важным является возможность графического управления межсетевым экраном и шейпингом (traffic shaping). Это позволяет быстро разрешать работу VPN, расставлять приоритет трафика или искусственно ограничивать защищенный канал для проверки устойчивости VPN.

Внешний вид настройки межсетевого экрана и шейпинга изображены на рис. 2 и рис. 3.

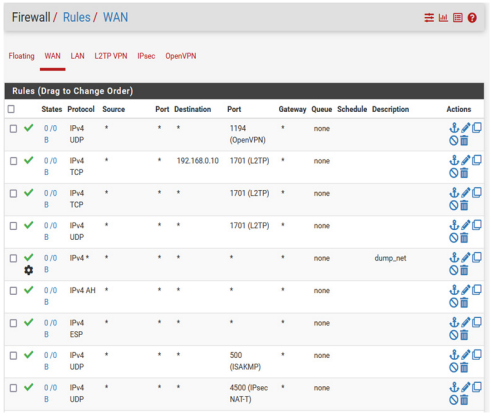


Рис. 2. Пример настройки межсетевого экрана.

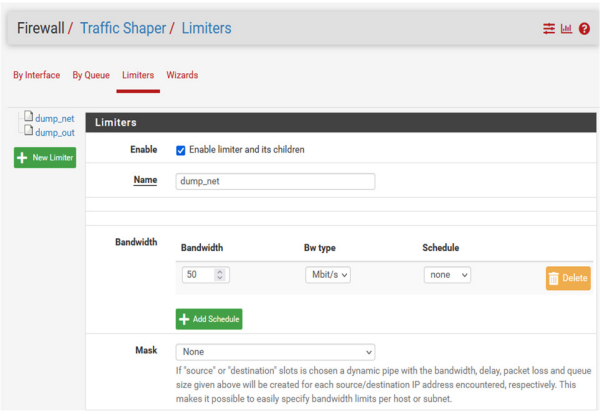


Рис. 3. Пример настройки шейпинга.

Для выполнения сравнения необходимо выполнить следующие действия:

- Создать виртуальные машины;
- Установить на них операционные системы для клиентов и сервера VPN;
- Настроить рассматриваемые VPN подключения;
- Установить дополнительные инструменты для тестирования;
- Произвести измерения и выполнить анализ полученных данных.

С помощью среды виртуализации VirtualBox были созданы 3 виртуальные машины, одна из которых выполняла роль сервера VPN под управлением операционной системы pfSense, а остальные — роли удаленного и локального пользователей. Схема виртуального стенда изображена на рис.4.

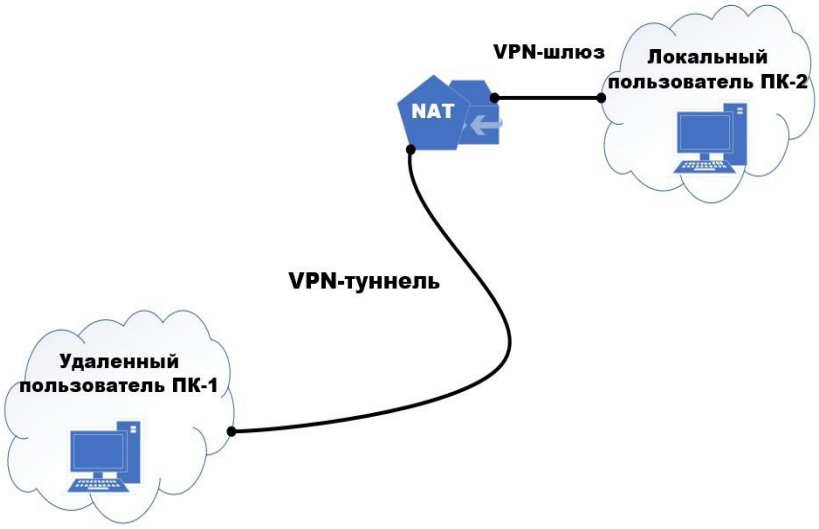


Рис. 4. Схема тестирования.

Сравниваемым критерием была выбрана пропускная способность туннеля. Для получения данных был установлен пакет iperf3, который способен создавать TCP и UDP трафик, а также измерять скорость передачи данных в канале. В процессе измерения размер отправляемых пакетов был установлен значением 1450 бит. Рассматривались IPsec, L2TP/IPsec, Routed IPsec и OpenVPN в режиме UDP. На рис. 5 показаны результаты тестирования пропускной способности.

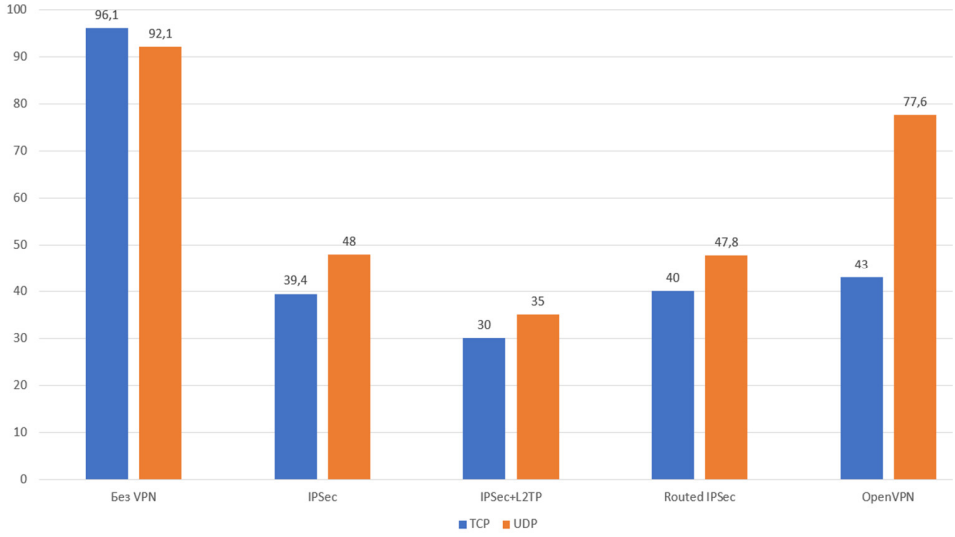


Рис. 5. Измеренная пропускная способность туннелей.

Заключение. Оптимальный выбор решения для организации VPN — важная задача, для которой требуется сравнение по множеству качественных и количественных критериев. Использование сетевой операционной системы pfSense позволяет ускорить развертывание различных протоколов туннелирования и быстрее сравнить их по количественным параметрам.

В практической части работы был проверен функционал операционной системы pfSense для развертывания VPN технологий и их сравнения, а также сделано тестирование пропускной способности IPsec и OpenVPN туннелей.

СПИСОК ЛИТЕРАТУРЫ

1. Некоторые аспекты организации удаленной работы персонала в условиях пандемии / И. И. Сергеева, М. А. Степанова, А. Ю. Бабак, А. Е. Дутиков // Экономическая среда. – 2021. – № 1(35). – С. 47-52.
2. Как организована удаленная работа в России и странах СНГ. [Электронный ресурс] URL: https://www.ptsecurity.com/ru-ru/research/analytics/remote-work-in-russia-and-the-cis-2020 (Дата обращения 10.05.2021).
3. Плетеный, Д. С. Сравнение VPN - соединений для применения в защищенных корпоративных сетях / Д. С. Плетеный, В. В. Аленченко // Аллея науки. – 2020. – Т. 2. – № 5(44). – С. 979-984.
4. Старун, И. Г. Построение математической модели расчета комплексной оценки VPN / И. Г. Старун, А. Н. Югансон, Ю. А. Гатчин // Вестник Тамбовского государственного технического университета. – 2019. – Т. 25. – № 4. – С. 535-546.
5. Экспериментальная оценка количественных характеристик MPLS оборудования для L2 VPN / И. П. Зуев, П. В. Карельский, М. М. Ковцур, П. Э. Луеке // Региональная информатика и информационная безопасность: Сборник трудов, Санкт-Петербург, 23–25 октября 2019 года. – Санкт-Петербург: Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2019. – С. 41-43.

УДК 004.056

ИСПОЛЬЗОВАНИЕ ЗОНАЛЬНОЙ МОДЕЛИ ДЛЯ ГРУППОВОГО УПРАВЛЕНИЯ МОБИЛЬНЫМИ МУЛЬТИАГЕНТНЫМИ РОБОТОТЕХНИЧЕСКИМИ СИСТЕМАМИ

Пантиховский Олег Вальдемарович, Зикратова Татьяна Викторовна
Военно-морской политехнический институт ВУНЦ ВМФ «Военно-морская академия»
Кадетский б-р, 1, Пушкин, Санкт-Петербург, 196602, Россия
e-mails: vp1_oleg@mail.ru, ztv64@yandex.ru

Аннотация. Рассматриваются вопросы управления мультиагентными мобильными робототехническими системами в условиях деструктивного воздействия на информационную структуру: влияние помех, сбоев и отказов узлов информационной сети и др. Предлагается теоретическая модель обмена информации в таких системах. Основная идея предлагаемой субъектно-объектной модели разграничения доступа заключается в использовании понятия «полицейский участок», который является логически самостоятельной сущностью и предназначен для проверки достоверности информации агентов и/или целостности транзакций в границах региона субъектов и объектов. Определяется порядок информационного взаимодействия агентов с полицейскими участками в своей зоне, а также межзональная политика управления.

Ключевые слова: коллектив роботов; мультиагентные робототехнические системы; модель информационного взаимодействия; распределенные киберфизические системы.

USING A ZONAL MODEL FOR GROUP MANAGEMENT OF MOBILE MULTYAGENCY ROBOTIC SYSTEMS

Pantikhovsky Oleg, Zikratova Tatyana
Naval Polytechnic Institute of the VUNC of the Navy «Naval Academy»
1 Kadetsky Blvd, Pushkin, St. Petersburg, 196602, Russia
e-mails: vp1_oleg@mail.ru, ztv64@yandex.ru

Abstract. The issues of management of multi-agent mobile robotic systems in the conditions of destructive impact on the information structure are considered: the influence of interference, failures and failures of information network nodes, etc. A theoretical model of information exchange in such systems is proposed. The main idea that underlies the proposed subject-object model of access differentiation is the use of the concept of «police station», which is a logically independent entity and is designed to verify the reliability of information of agents and/or the integrity of transactions within the boundaries of the region of subjects and objects. The order of information interaction of agents with police stations in their zone, as well as the interzonal security policy, is determined.

Keywords: team of robots; multyagency robotic systems; information interaction model; distributed cyber-physical systems.

Введение. Стремительное развитие и повсеместное внедрение сложных информационных систем, которые могут эффективно интегрировать кибер- и физические компоненты, используя современные сенсорные, вычислительные и сетевые технологии, привело к появлению новых моделей, связанных с концепцией Индустрии 4.0. Киберфизические устройства, также как кибер- и физические компоненты, являются более узким понятием киберфизической системы, которая представляет собой информационно-технологическую концепцию, подразумевающую интеграцию вычислительных ресурсов в физические процессы. В такой системе датчики, оборудование и информационные системы соединены в единое целое. Эти системы взаимодействуют друг с другом с помощью стандартных интернет-протоколов для прогнозирования, самонастройки и адаптации к изменениям [1].

К ним относятся мультиагентные робототехнические системы (МРТС), представителями которых являются, в частности, коллективы беспилотных аппаратов (летательных, наземных, надводных, подводных и т.д.), действующих совместно для достижения общей цели [2]. Мультиагентная робототехническая система (многоагентная) – это система, состоящая из множества взаимодействующих интеллектуальных агентов. Мультиагентные системы могут решить проблемы, которые трудны или невозможны для отдельного агента. Под агентом в данном случае понимается физический/программный объект, который оценивает собственное состояние, состояние других объектов и окружающей среды для выполнения своих действий, включая прогнозирование и планирование, которые максимизируют успешность, в том числе при неожиданном изменении оцениваемых состояний, достижения своих целей [1].

Построение и функционирование МРТС имеют свои особенности, а именно: децентрализация управления, пространственная удаленность киберфизических устройств (агентов), а также нахождение их вне пределов контролируемой территории.

Также к особенностям можно отнести необходимость использования телекоммуникационных технологий для информационного обмена между объектами, непредсказуемость динамики внешней среды и ограниченность представления объектов о системе в целом. С одной стороны, эти факторы делают МРТС максимально уязвимой в нестабильных условиях [2, 3], с другой стороны, создают трудности группового управления робототехническими системами, в основе которых лежат различные виды политик управления.

Функционирование МРТС с децентрализованным управлением в самом общем виде можно описать на примере решения задачи целераспределения. Исходные данные: количество целей M, коллектив из N роботов R_j ($j = \overline{1, N}$). На обеспечение каждой цели задается определенное количество роботов.

В процессе информационного обмена внутри робототехнической системы вырабатывается коллективное решение о распределении роботов-агентов по целям. В процессе выполнения поставленной задачи используется итерационный алгоритм, в основу которого положен анализ каждым роботом-агентом полученной информации и выбора «своей» цели, исходя из условий оптимальности. Затем происходит обмен информацией о выбранных решениях, анализ и «обсуждение» решений, принятых другими роботами. Процедура повторяется до тех пор, пока не будут обеспечены все цели множества M.

Существуют модификации этого алгоритма, позволяющие учитывать различные факторы, влияющие на эффективность принимаемого решения. Например, роботы могут быть образовывать одну, либо несколько взаимодействующих между собой и разнесенных в пространстве групп.

Необходимость решения подобного класса задач привела к появлению новых моделей группового управления, которые хорошо согласуются с принципами построения децентрализованных систем. К ним относятся:

– зональная модель управления в распределённых системах [4]. Здесь распределенная система рассматривается как система, обеспечивающая решение проблемы управления на базе распределенной системы знаний в отличие от мультиагентных (многоагентных) систем, где базы знаний отдельных агентов взаимодействуют [1];

– модель полицейских участков (Police Office Model, POM), предложенная Ксюдонгом [5].

В этих моделях информационное взаимодействие агентов роя осуществляется в условиях влияния дестабилизирующих факторов, что приводит к снижению эффективности принимаемых мультиагентной системой решений.

Соответственно возникает задача интеграции в МРТС экспертной системы. По своей сути экспертная система является системой «интеллектуальной поддержки», обеспечивающей принятие правильного решения в условиях неопределенности.

В данной работе экспертная система, основанная на алгоритмах искусственного интеллекта (управление знаниями), отслеживает текущее местоположение каждого агента, трафик между агентами и делит множество всех доступов *T* субъектов к объектам на два непересекающихся подмножества T_L и T_N :

$$T = T_L \cup T_N, T_L \cap T_N = \emptyset, \quad (1)$$

где T_L – множество доступов, вызываемых безопасными транзакциями, T_N – множество доступов, вызываемыми агентами, подверженными влиянию внешних факторов в робототехнических системах.

Отсюда следует, что модель оценки информационного обмена для МРТС должна определять местонахождение агентов и описывать порядок разграничения доступа физически удаленных субъектов к объектам. Данный алгоритм реализуется правилами информационного обмена агентов в регионе *H* и представляет собой формально описанные доступы множества T_L.

Учитывая цикличность принятия решений коллективом роботов [3] в каждый момент времени на *k*-й итерации информационного обмена, МРТС можно представить конечным множеством элементов $r \in R$, разделенных на два подмножества: субъектов доступа *S* и объектов доступа *O*, где $S \cup O = R$.

В качестве субъектов доступа $s \in S$ выступают роботы-агенты, которые на *k*-й итерации получили право доступа на запись и способны изменять состояние системы, выполняя транзакции в ней посредством своих активных сущностей.

Под объектом доступа $o \in O$ выступают пассивные агенты, на *k*-й итерации получившие право доступа на чтение данных.

Рассмотрим зональную модель группового управления распределенных систем, в которой возможны два варианта реализации: внутризональная и межзональная.

Основные положения модели заключаются в следующем.

В качестве объекта управления выступают основные сущности МРТС, которые представлены множеством непересекающихся зон региона $H(h_1, h_2, \dots, h_M)$ и множеством роботов-агентов $R(r_1, r_2, \dots, r_N)$.

Выделение области *H* на зоны осуществляется несколькими способами обособления подмножества субъектов и объектов в локальный сегмент:

– подмножество субъектов доступа группируется на основе их управления одним общим системным процессом;

– подмножество субъектов и объектов доступа локализуется в рамках некоторой технической/физической компоненты МРТС;

– всем субъектам и объектам присваивается уникальный адрес (идентификатор) в едином информационном пространстве и осуществляется разделение этого пространства на области, обособляющие локальные сегменты.

2. Каждый робот-агент $r \in R$ имеет открытую и закрытую части интерфейса. Открытая часть взаимодействует с агентами МРТС в процессе выполнения группой поставленной задачи. Закрытая часть взаимодействует с программным обеспечением (ПО). Для каждой из частей интерфейса используются различные каналы связи.

3. Роботы-агенты поочередно активизируются в процессе итерационной процедуры и получают статус субъектов доступа. Остальные члены коллектива на данном этапе итерации представляют собой объекты доступа.

4. ПО реализует внутризональную политику группового управления своей зоны и обеспечивает управление доступом и аудит процессов.

Пусть полицейским участком зоны называется системный субъект (процесс), который реализует в отношении объектов зоны $h \in H$ разрешенное множество доступов $T_L(h)$:

$$T(h) = T_L^{in}(h) \cup T_L^{out}(h), \quad (2)$$

где $T_L^{in}(h)$ – множество внутризональных доступов в группе роботов;

$T_L^{out}(h) = T_L^{out}(h \rightarrow) \cup T_L^{out}(h \leftarrow)$ – множество внутризональных доступов для зоны $h \in H$, которое является объединением множества удаленных доступов субъектов зоны h к объектам других зон $T_L^{out}(h \rightarrow)$ и множества удаленных доступов субъектов других зон к объектам зоны h – $T_L^{out}(h \leftarrow)$ [3].

5. Множество всех зон $h \in H$, взаимодействующих между собой посредством безопасного канала связи ПО, образует экспертную систему региона *H*, которая предназначена для реализации межзонального группового управления.

6. Внутризональный доступ субъектов к объектам в своей зоне h организуется в три этапа.

– осуществляется идентификация/аутентификация субъекта $s \in S$ в зоне $h \in H$ под управлением внутризонального ПО, порождается транзакция;

– формируется запрос на доступ $T^{in}(h)$ субъекта s у внутризонального ПО к объектам $o \in O$ зоны h;

– после получения доступа объекты $o \in O$ зоны h получают от ПО соответствующую квитанцию, и транзакция осуществляется.

7. Межзональный доступ субъектов к объектам «чужой» зоны h' организуются следующим образом:

– осуществляется идентификация/аутентификация субъекта $s \in S$ в зоне $h \in H$ под управлением внутризонального ПО, порождается транзакция;

– формируется запрос на доступ $T_L^{out}(h \rightarrow)$ субъекта s у внутризонального ПО к объектам $o \in O$ зоны $h' \in H$;

– происходит удаленное вхождение субъекта $s \in S$ в зону $h' \in H$ под управлением полицейских участков зон h и h', которое представляет собой обмен информацией между полицейскими участками зон h и h' по безопасному каналу связи;

– после удовлетворения запроса осуществляется получение доступа на проведение транзакции $T_L^{out}(h \rightarrow)$ зональной модели управления МРТС.

Заключение. Таким образом, можно сделать следующие выводы.

В условиях влияния дестабилизирующих факторов, которые могут приводить к снижению эффективности принимаемых мультиагентной системой решений, информационное взаимодействие агентов роя осуществляется под контролем экспертной системы, реализованной в виде *зональной модели*.

Рассматриваемая модель позволяет осуществлять два вида политики управления группой роботов: внутризональную и межзональную. И в том, и в другом случае функция проверки доступа и/или целостности транзакций субъектов и объектов реализуется с помощью ПО каждой из сегментированных зон.

Подобная организация управления доступом позволяет решить задачу реализации механизма отслеживания текущего местоположения каждого субъекта и объекта системы.

Использование зональной модели группового управления при решении итерационной задачи распределения роботов по нескольким целям подтверждает ее работоспособность.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 59277-2020. Национальный стандарт Российской Федерации. Системы искусственного интеллекта. Классификация систем искусственного интеллекта: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 23 декабря 2020 г. N 1372-ст.: дата введения 2021-03-01.
2. Neeran K.M., Tripathi A.R. Security in the Ajanta MobileAgent system. Technical Report. Department of Computer Science, University of Minnesota, May 1999. 28 p.
3. Higgins F., Tomlinson A., Martin K.M. Threats to the Swarm: Security Considerations for Swarm Robotics // International Journal on Advances in Security, Vol. 2, No. 2&3, 2009, pp. 288 – 297. [Электронный ресурс]. – Режим доступа: http://www.iariajournals.org/security/sec_v2_n23_2009_paged.pdf, свободный. Яз. англ. (дата обращения 09.08.2016).
4. Зикратов И.А., Викснин И.И., Зикратова Т.В., Шлыков А.А., Медведков Д.И. Модель безопасности мобильных мультиагентных робототехнических систем с коллективным управлением. Научно-технический вестник информационных технологий, механики и оптики. 2017. Т. 17. № 3. С. 439-449.
5. Гайдамакин Н.А. Зональная модель разграничения доступа в распределенных компьютерных системах // НТИ. Сер. информ. процессы и системы. 2002. No 12. С. 15-22.
6. Xudong G., Yiling Ya., Yinyuan Y. POM-a mobile agent security model against malicious hosts // Proceedings of High-Performance Computing in the Asia-Pacific Region. 2000. V. 2. P. 1165–1166.

УДК 004.7

ИССЛЕДОВАНИЕ КАЧЕСТВА ОБНАРУЖЕНИЯ ПОЯВЛЯЮЩИХСЯ УГРОЗ КОМПЛЕКСНЫМИ СИСТЕМАМИ ЗАЩИТЫ ИНФОРМАЦИИ

Птицына Лариса Константиновна, Жаранова Анастасия Олеговна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия

e-mails: ptitsina_lk@inbox.ru, zharanovaan@gmail.com

Аннотация. Определена необходимость формирования методологических и инструментальных средств для оценки показателей эффективности и качества обнаружения появляющихся угроз в распределенных системах. Описано математическое обеспечение для определения динамического профиля комплексной системы защиты информации при параллельной обработке процессов по противодействую возможным внешним негативным воздействиям. Предложен инструментарий для анализа степени доверия к распределенным комплексным системам защиты информации. Представлены результаты анализа влияния конфигурационного профилирования на динамические характеристики систем.

Ключевые слова: информационная инфраструктура; территориальная распределенность; комплексные системы защиты информации; качество.

RESEARCH OF THE QUALITY OF DETECTION OF EMERGING THREATS BY COMPLEX INFORMATION SECURITY SYSTEMS

Ptitsyna Larisa, Zharanova Anastasia
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: ptitsina_lk@inbox.ru, zharanovaan@gmail.com

Abstract. The necessity of forming methodological and instrumental tools for evaluating the effectiveness and quality of detecting emerging threats in distributed systems is determined. The mathematical support for determining the dynamic profile of a complex information security system during parallel processing of processes to counteract possible external negative influences is described. A toolkit for analyzing the degree of trust in distributed complex information security systems is proposed. The results of the analysis of the influence of configuration profiling on the dynamic characteristics of systems are presented.

Keywords: information infrastructure; territorial distribution; complex information security systems; quality.

Введение. Стремительное развитие информационных систем и технологий неразрывно связано с оценкой качества функционирования комплексных распределенных систем защиты информации. Качество функционирования комплексных систем защиты информации определяется оперативностью реагирования системы на возникающие угрозы. Методологические и инструментальные средства по оценке эффективности комплексных систем позволят производить экономический анализ затрат на внедрение и сопровождение систем, определять целесообразность разработки и поддержки систем. Для этого необходимо определять зависимость функционирования системы от аппаратно-программных средств, окружающей среды, архитектуры, условий проведения работ и их профессиональной специфики [1, 2].

Для исследования влияния различных параметров на динамические характеристики комплексной системы защиты информации сформирован математический аппарат, являющийся основой инструментального средства, предназначенного для определения эффективности функционирования комплексных систем защиты информации.

Каждый процесс определяется плотностью вероятностей времени его выполнения. Преобразования производятся на основе модифицированного метода свертки [3, 4].

Проводимые исследования предусматривают поэтапную формализацию:

– преобразование параллельных подпроцессов защиты информации подсистемы на базе функции синхронизации «∨» («∧»);

– преобразование параллельных подсистем на базе функции синхронизации первого уровня «∨» («∧») и узлом соединения параллельных подпроцессов защиты информации подсистем на базе функции синхронизации второго уровня «∨» («∧»).

Базовые операции анализа позволяют оценить плотность распределения вероятностей процессов и отображают объективный анализ моделей систем в соответствии с их структурой и характеристиками.

Математическое ожидание и дисперсия дискретного времени окончания процесса защиты информации, а также риск срыва временного регламента комплексной системы защиты информации с узлом соединения параллельных подсистем на базе функции синхронизации первого уровня «∧» и узлом соединения параллельных подпроцессов защиты информации подсистем на базе функции синхронизации второго уровня «∧» имеют следующий вид:

$$E\left[k_{1\wedge\wedge}\right] = \sum_{\min k_{1\wedge\wedge}}^{\max k_{1\wedge\wedge}} k_{1\wedge\wedge} f_{1\wedge\wedge}\left(k_{1\wedge\wedge}\right), \tag{1}$$

$$D\left[k_{1\wedge\wedge}\right] = \sum_{\min k_{1\wedge\wedge}}^{\max k_{1\wedge\wedge}} \left(k_{1\wedge\wedge} - E\left[k_{1\wedge\wedge}\right]\right)^2 f_{1\wedge\wedge}\left(k_{1\wedge\wedge}\right), \tag{2}$$

$$R\left[C\right] = \sum_{k_{1\vee\vee} > C} f_{1\wedge\wedge}\left(k_{1\wedge\wedge}\right). \tag{3}$$

Результаты проведенного исследования способствуют возможности сравнения различных подходов к обнаружению и противодействию внешним негативным воздействиям, рациональному обоснованию выбранного варианта с позиции наименьшего времени проведения мероприятий по информационной защищенности или меньшего риска срыва временного регламента.

Определенные математические соотношения являются основой математического обеспечения при определении динамического профиля комплексной системы защиты информации при параллельной обработке

процессов по противодействую возможным внешним негативным воздействиям и позволяют управлять показателями качества в процессе функционирования комплексных систем защиты информации. В процессе анализа могут определяться альтернативные и наилучшие варианты архитектур комплексных систем, состав технических средств и механизмов защиты информации, прогнозироваться критические ситуации и уязвимости системы с целью повышения качества ее функционирования при реальном масштабе времени.

Выведенные аналитические оценки статистических характеристик времени реакции на появляющуюся угрозу ориентируются на анализ динамических характеристик комплексных систем защиты информации в распределенных системах.

Аналитические соотношения являются основой при разработке инструментального средства, ориентированного на контроль качества функционирования комплексной системы защиты информации. Согласно выведенным оценкам при исследовании возможно определить влияние различных параметров на динамические характеристики комплексной системы защиты. В состав параметров, влияющих на статистические характеристики времени реакции на появившуюся угрозу, входят: временные характеристики процессов обеспечения информационной защищенности в системе, связи между процессами, число процессов обеспечения информационной защищенности.

Инструментальное средство после обработки введенных данных отображает рассчитанные числовые значения показателей и график зависимости вероятности своевременной реакции на появляющуюся угрозу от определенных временных ограничений.

Инструментальное средство производит расчет итоговой плотности распределения вероятностей времени окончания процесса защиты информации всеми подсистемами, математического ожидания и дисперсии дискретного времени окончания процесса защиты информации, а также риск срыва временного регламента комплексной системы защиты информации с узлом соединения параллельных подсистем на базе функции синхронизации первого уровня «V» («Λ») и узлом соединения параллельных подпроцессов защиты информации подсистем на базе функции синхронизации второго уровня «V» («Λ»).

Для получения результатов пользователю необходимо определить количество подсистем комплексной защиты информации, а также количество сервисов (механизмов) защиты информации в каждой из подсистем, дискретные времена и соответствующие им плотности распределения вероятностей дискретного времени выполнения действия по передаче входной информации, по выполнению подпроцесса защиты информации, по передаче результатов обработки по подпроцессу защиты информации.

На рис 1. Представлен главный экран программы, где пользователь может составить структуру комплексной системы защиты информации, а именно выбрать количество подсистем и количество сервисов (механизмов) защиты информации в каждой из подсистем. С помощью символов «+» и «-» производится добавление или удаление механизма защиты или подсистемы.

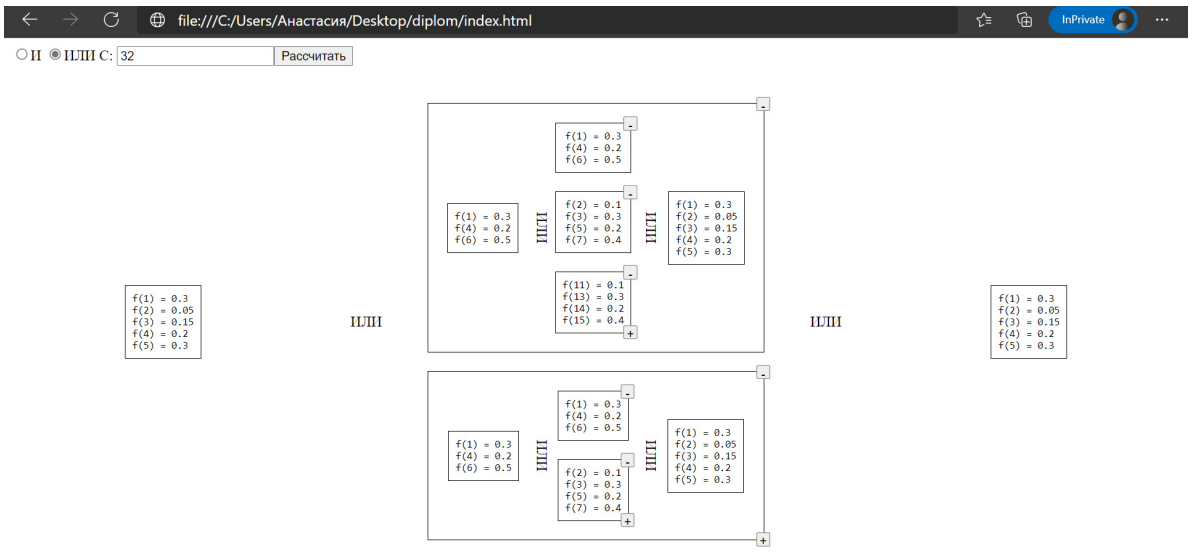


Рис. 1. Окно управления структурой системы.

В случае перехода к конкретному сервису (механизму) защиты открывается диалоговая панель для ввода числовых характеристик: дискретных времен и соответствующих им плотностей распределения вероятностей дискретного времени выполнения действий. При обнаружении некорректного ввода исходных данных инструментальное средство сообщит об этом пользователю и не позволит завершить процесс ввода данных.

Далее пользователю остается выбрать механизм синхронизации и задать числовое значение временного регламента, по которому производится расчет риска срыва.

После проверки корректности исходных данных происходит процесс расчета плотности распределения вероятностей времени окончания принятия интегрального решения всеми подсистемами комплексной системы защиты информации в зависимости от выбранной функции синхронизации параллельных процессов.

На основе полученной итоговой плотности распределения вероятностей времени окончания принятия интегрального решения всеми подсистемами комплексной системы защиты информации рассчитываются динамические характеристики комплексной системы защиты информации: математического ожидания, дисперсии и риска срыва временного регламента по соответствующим аналитическим соотношениям.

Дополнительным рассчитанным параметром является сумма значений вероятностей, необходимая для проверки корректности полученной итоговой плотности распределения вероятностей времени выполнения процесса защиты информации всеми подсистемами комплексной системы защиты информации. Если сумма значений равна единице, то показатель проверки корректности результатов выдает true, а в случае, если система расчета сработала некорректно, – false.

По окончании процесса расчета всех необходимых характеристик инструментальное средство позволяет проанализировать графическое отображение итоговой плотности распределения времени выполнения процесса защиты информации всеми подсистемами комплексной системы защиты информации. Пример графического отображения плотности распределения вероятностей по результатам работы программного средства представлен на рис. 2.

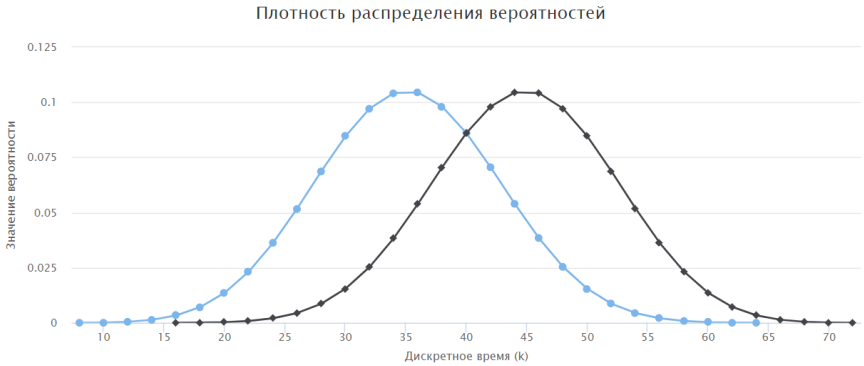


Рис. 2. График плотности распределения вероятностей.

Графическое отображение работы инструментального средства представляет собой кривую на плоскости. На оси абсцисс расположены значения дискретного времени выполнения, на оси ординат – соответствующие значения вероятностей.

Инструментальное средство предназначено для:

– расчета среднего времени вероятности своевременной реакции на появляющуюся угрозу;

– определения требований к разработке комплексных систем защиты информации с достижением необходимой степени оперативности в реакции на внешние негативные воздействия;

– составления рекомендаций по комплексированию программных средств и механизмов с целью достижения необходимых динамических характеристик комплексных систем защиты информации.

При проведении экспериментов по оценке влияния параметров на динамический профиль систем рассматриваются два типа ситуаций. Первый тип характеризуется минимально возможным временем реакции на внешнее негативное воздействие. Второй тип ситуаций соответствует альтернативному варианту, то есть характеризуется максимально возможным временем реакции на внешнее негативное воздействие. Серия экспериментов позволяет оценить степень влияния механизмов комплексирования и степени распределенности на качество функционирования комплексных систем защиты информации.

На основе всех проведенных экспериментов можно сделать следующие выводы:

– в сравнимых условиях время реагирования на возникающую угрозу имеет меньший диапазон при использовании функции синхронизации «ИЛИ», что обуславливается необходимостью завершения процесса защиты хотя бы одной подсистемой, в отличие от функции «И», где интегральный результат возможен после отработки всех подсистем;

– меньшее время реагирования на возникающую угрозу имеет комплексная система защиты информации, объединение результатов в которой осуществляется посредством соединения параллельных подсистем на базе функции синхронизации первого уровня «ИЛИ» и узлом соединения параллельных подпроцессов защиты информации подсистем на базе функции синхронизации второго уровня «ИЛИ»;

– большее время реагирования на возникающую угрозу имеет комплексная система защиты информации, объединение результатов в которой осуществляется посредством соединения параллельных подсистем на базе функции синхронизации первого уровня «И» и узлом соединения параллельных подпроцессов защиты информации подсистем на базе функции синхронизации второго уровня «И»;

– степень масштабируемости влияет на скорость работы системе в части оперативной реакции на появляющуюся угрозу, при этом с возрастанием уровня масштабируемости отчетливее видна разница в оперативности реагировании при использовании механизмов синхронизации «И» и «ИЛИ»;

– риск срыва временного регламента при использовании функции «И» возрастает в сравнении с использованием функции «ИЛИ», при этом заметно влияние показателя С на уровень риска: при значениях С, превышающих средние показатели дискретного времени выполнения действий, риск срыва временного регламента стремится к нулю, а при значениях ниже средних показателей – к единице;

– наличие сервиса с большим диапазоном значений дискретных времен, то есть требующего больше времени на обработку информации, не сказывается на работе системы при использовании функции синхронизации «ИЛИ», напротив, при использовании механизма синхронизации «И» время работы системы увеличивается, как и вероятность срыва временного регламента;

– разнородность технологий передачи данных и различные среды проводного и беспроводного секторов при разнообразной степени территориальной распределенности оборудования оказывают значительное влияние на качество функционирования комплексной системы защиты информации из-за влияния временных затрат на передачу информации подсистемам.

Заключение. Проведено исследование динамических характеристик комплексных систем защиты информации в условиях распределенной коммуникационной среды и анализ влияния организации систем на качество их функционирования. Разработанное инструментальное средство позволяет оценивать эффективность комплексных систем защиты информации в распределенной коммуникационной среде и достигать необходимого уровня качества функционирования. Инструментальное средство является необходимым при выборе механизмов защиты информации и способов их комплексирования в целях сокращения временных затрат по обеспечению безопасности в комплексных системах защиты информации, а также может использоваться для определения требований к комплексным системам защиты информации и составления рекомендаций по комплексированию механизмов защиты с целью достижения необходимого уровня качества функционирования.

СПИСОК ЛИТЕРАТУРЫ

1. Птицына Л. К., Птицын А. В. Расширение возможностей объектно-ориентированного анализа для обеспечения управляемого качества комплексных систем защиты информации // Информационные технологии в проектировании и производстве. 2011. № 2. С. 55-60.
2. Птицын А.В. Аналитическое моделирование комплексных систем защиты информации. Новые формализации аналитического исследования комплексных систем защиты информации / А.В. Птицын, Л.К. Птицына. Гамбург. Saarbrucken: LAP LAMBERT Academic Publishing. 2012. 293 с.
3. Птицына Л. К., Жаранова А. О. Аналитическое моделирование распределенной комплексной системы защиты информации // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 9 / СПОИСУ. – СПб., 2020. С. 284-288.
4. Птицына Л. К., Жаранова А. О. Формирование расширенной объектно-ориентированной модели комплексной системы защиты информации // Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)»: Материалы конференции. Часть 2. \ СПОИСУ. – СПб, 2020. С. 300-301.

УДК 621.391.28

МОДЕЛЬ ЛОГИЧЕСКОГО УРОВНЯ RLC СЕТИ LTE

Птицына Лариса Константиновна, Мошак Андрей Николаевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: ptitsina_lk@inbox.ru, a.moshak@mail.ru

Аннотация. Проводится анализ работы механизма ARQ в радиоканале сети LTE. Строится модель уровня управления радиоканалом RLC архитектуры радиодоступа E-UTRAN сети LTE. Исследуется влияние работы протокола ARQ на характеристики радиоканала сети LTE с учетом длины протокольного блока уровня RLC, величины уровня ошибок и закона их распределения в радиоканале.

Ключевые слова: E-UTRAN; архитектура сети LTE; протоколы HARQ; ARQ.

LTE NETWORK RLC LOGICAL LAYER MODEL

Ptitsyna Larisa, Moshak Andrey
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: ptitsina_lk@inbox.ru, a.moshak@mail.ru

Abstract. The analysis of operation of the ARQ mechanism in a radio channel of LTE network is carried out. The RLC radio control layer model of the E-UTRAN radio access architecture of the LTE is constructed. Influence of ARQ protocol operation on characteristics of radio channel of LTE network is investigated taking into account length of protocol block of RLC layer, value of error level and law of their distribution in radio channel.

Keywords: E-UTRAN; LTE network architecture; HARQ protocols; ARQ.

Введение. Пакетная мобильная сеть связи LTE (Long Term Evolution) в настоящее время рассматриваются как наиболее перспективное направление реализации стандарта беспроводной связи поколения 4G [1-3]. Сеть LTE обеспечивает радиодоступ и мультисервисное обслуживание в пакетной форме как данных реального времени (например, речь, видео), так и эластичных данных (например, web browsing, загрузка файлов и др.). При этом сетью должна обеспечиваться в сеансе связи изохронность передачи пакетов данных реального времени и заданное время передачи пакетов эластичных данных с требуемой достоверностью. Сеть LTE ориентирована на установление соединения для передачи любого типа данных. При этом сеть на участке доступа создает сквозной составной виртуальный канал передачи данных между двумя оконечными устройствами сети (например, оборудованием пользователя UE (User Equipment) и выходным пакетным шлюзом PDN-GW (Packet data network gateway). Это виртуальное соединение называется EPS-каналом или EPS-носителем (bearer) в состав которого входит и радиоканал RAB (Radio Bearer) на участке между UE и базовой станцией eNB. Он предоставляет «услугу переноса информации» с конкретными параметрами качества сервиса QoS (Quality of Service) для каждого сервисного потока SDF (Service Data Flow), в том числе обеспечивает требуемую достоверность передачи для эластичного трафика.

Одной из ключевых задач, решаемых разработчиками любых систем связи (и в первую очередь систем радиосвязи) является задача обнаружения и исправления ошибок, количество которых в сотовых сетях определяется двумя факторами – внешними помехами возникающих, например, из-за шумов, помех и замирания сигнала, а также интерференцией, возникающей от передатчиков соседних базовых станций. Последний фактор является особенно важным для одночастотных систем мобильной связи LTE. Для защиты от ошибок в радиоканале, применяются методы повторной передачи искаженных или утраченных частей блоков данных. В сети радиодоступа E-UTRAN (Evolved Universal Terrestrial Radio Access Network) сети LTE используется двухуровневая система защиты от ошибок, объединяющая 1) гибридный протокол «Автоматический запрос на повтор» Hybrid ARQ (Automatic Repeat Query), или HARQ, реализованный на физическом уровне PHY (Physical layer) архитектуры плоскости пользователя радиодоступа. Этот протокол обнаруживает и восстанавливает поврежденные блоки данных на приеме и 2) протокол «Автоматический запрос на повтор» ARQ, реализованный на уровне управления радиоканала RLC (Radio Link Control). Этот протокол обнаруживает ошибку при приеме блока данных и задействуется для повтора невосстановленных HARQ блоков данных если ошибка не устранена. Классический механизм ARQ предполагает автоматический запрос на повторную передачу поврежденного блока данных в случае обнаружения ошибки. При этом поврежденный блок на приемной стоне отбрасывается и запрашивается повторная передача этого же блока. В этой связи возникает проблема оценки повторной передачи на пропускную способность радиоканала. Чем эффективнее организован протокол повторной передачи, тем рациональнее используются радиоресурсы. В статье строится модель протокола ARQ и исследуется его влияние на пропускную способность радиоканала сети LTE.

Архитектура сети радиодоступа LTE. Архитектура сети радиодоступа E-UTRAN (Evolved Universal Terrestrial Radio Access Network) на рис 1 [4].

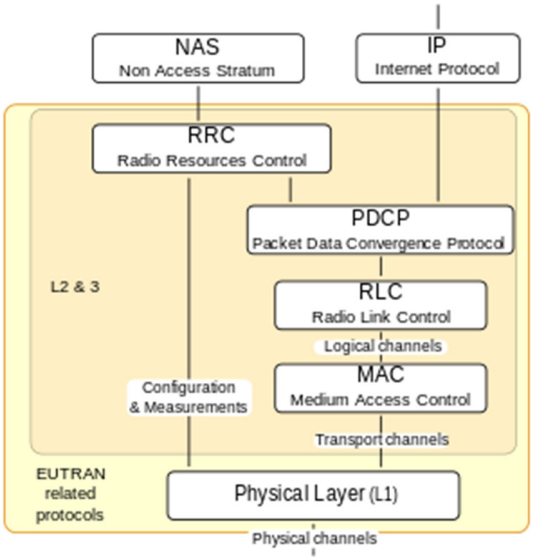


Рис. 1. Архитектура сети радиодоступа E-UTRAN.

Архитектура E-UTRAN включает следующие логические уровни:

NAS (Non-Access Stratum). Уровень «без доступа» NAS обеспечивает: управление сессиями: установление, поддержание и прекращение соединения; механизмы безопасности (security) на NAS уровне, включая контроль целостности (integrity) и шифрование (ciphering) сигнальных сообщений; поддержку мобильности (поддержание связи и активных сеансов с пользовательским оборудованием во время движения пользователя); поддержку процедур установки и поддержания IP связанности между UE и пакетным шлюзом PDN-GW; управление звонками и др.

RRC (Radio Resource Control). Подуровень RRC обеспечивает следующие основные функции: передача системной информации, связанной со слоем доступа и транспортировкой сообщений слоя без доступа (NAS), поиском, установлением и установлением соединения RRC, управлением ключами безопасности, передачей обслуживания, Измерения UE, связанные с мобильностью между системами (между RAT), QoS и т. д.

PDCP (Packet Data Convergence Protocol). Подуровень конвергенции пакетов данных обрабатывает данные более высоких уровней: SDU (Service Data Units) – дейтаграммы трафика и сигнальные сообщения. При этом осуществляют: сжатие (и, соответственно, восстановление) IP-заголовков, используя протокол ROHC (Robust Header Compression), шифрацию и дешифрацию SDU трафика и сигнализации, защиту (проверку) целостности сигнальных сообщений. Кроме указанных функций, уровень PDCP обеспечивает передачу данных без потерь при хэндоверах и обрывах связи.

RLC (Radio Link Control Protocol) [5]. Подуровень управления радиосоединением RLC обеспечивает: сегментацию SDU на PDU (Protocol Data Unit) для передачи и объединение пакетов при приеме в требуемой последовательности, коррекцию ошибок при передаче, используя повторную передачу (ARQ), устранение ошибок в передаче пакетов, вызванных ошибками сигнализации. Возможны три режима обработки пакетов на уровне RLC в зависимости от типа передаваемой информации:

- прозрачный TM (transparent mode) – пакеты не обрабатывают на уровне RLC,
- передача без подтверждения UM (unacknowledged mode),
- передача с подтверждением AM (acknowledged mode).

MAC (Medium Access Control Protocol). Подуровень управления доступом к среде MAC осуществляет размещение и мультиплексирование протокольных блоков логических каналов в транспортные с последующей передачей их по физическим каналам. На уровень MAC возложены следующие функции: управление выделением канального ресурса с учетом приоритетов трафика, т.е. выполняют задачи планирования передач (обрабатывает расстановку приоритетов логических каналов для одного и того же UE и динамическое планирование между UE), выбор транспортных форматов передач, управление повторными передачами непринятых пакетов, организацию процедур доступа UE к сети и периодической синхронизации UE, измерения: объема передаваемого трафика, загрузки канала, состояния буферов передачи UE, относительной мощности передачи UE и ряд других, организацию режима сна/прерывистого приема (DRX) абонентских станций, управляет исправлением ошибок HARQ.

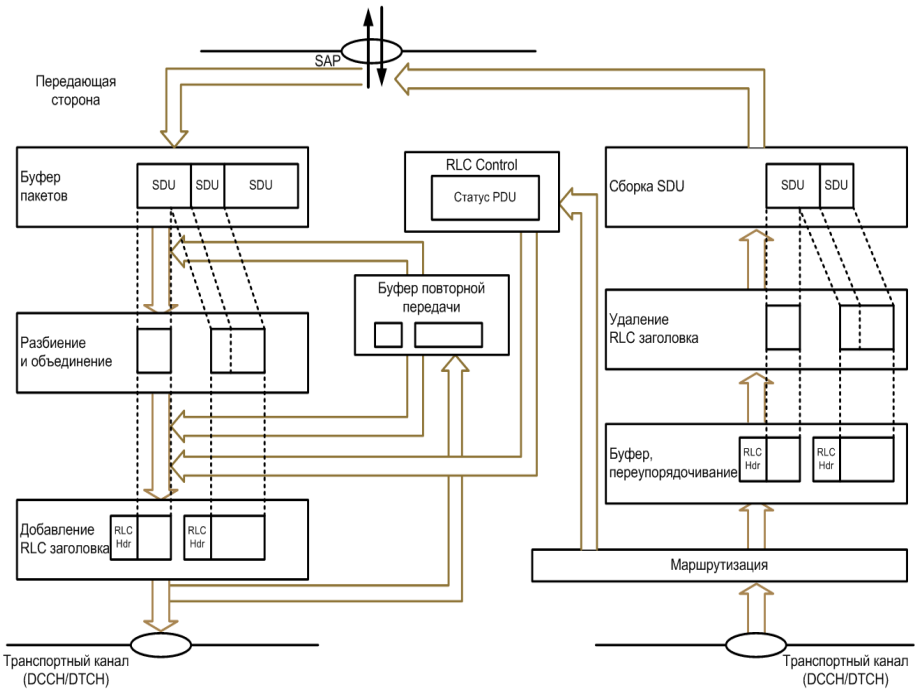


Рис. 2. Схема работы протокола AM RLC.

PHY Физический подуровень обеспечивает перенос информации из транспортных каналов MAC по радиоинтерфейсу. Обеспечивает адаптацию линии, управление мощностью , поиск соты (для целей начальной синхронизации и передачи обслуживания) и другие измерения (внутри системы LTE и между системами) для уровня RRC.

Рассмотрим более подробно работу протокола AM RLC. Наиболее важная функциональность RLC уровня — это повторная передача данных. Для передачи данных без ошибок используется протокол ARQ (Automatic Repeat reQuest) механизм. Поэтому режим AM RLC используется для передачи данных приложений, не предъявляющих жестких требований к задержке передачи данных (например, web browsing и загрузка файлов). Кроме этого, часто передача RRC сообщений так же осуществляется с помощью режима AM RLC для того, чтобы обеспечить надежность передачи данных. Ниже на рис.2 представлена схема AM RLC [5].

Функции, которые выполняются AM RLC:

- разбиение (фрагментация) и упаковка (объединение) RLC SDU;
- переупорядочивание RLC PDU;
- обнаружение повторных RLC PDU;
- сборка RLC SDU.
- повторная передача RLC PDU;
- переразбиение (перефрагментация) повторно передаваемых RLC PDU;
- опрос (polling);
- отчет о статусе (status report);
- запрещение оповещения о статусе.

Автоматический запрос повторной передачи ARQ — метод обнаружения ошибок при передаче данных, использующий сигнал подтверждение приёма и тайм-аут для обеспечения надёжной передачи по ненадёжным сервисам. ARQ также называется механизмом с положительным подтверждением и с повторной передачей PAR (Positive Acknowledgement and Retransmission mechanism). Существует два вида подтверждения о приеме протокольных блоках данных PDU (Protocol Data Unit) RLC, которые не восстановлены или потеряны во время передачи: положительное (ACK) и отрицательное (NACK или NAK). После отправки PDU RLC, это сообщение остается в буфере (рис. 2) для повторных передач до тех пор, пока не поступит квитанция (ACK), подтверждающая успешный прием на стороне получателя. Если отправитель не получает подтверждение переданного PDU RLC в течение определенного периода времени (тайм-аута), то он осуществляет повторную передачу. Этот процесс повторяется до тех пор, пока не будет передан правильный PDU RLC. Команда автоматического запроса на повторную передачу данных блока PDU RLC поступает от нижележащего уровня контроля доступа MAC. Организация повторной передачи поврежденных SDU MAC означает передачу всех AM PDU RLC, входящих в состав поврежденного транспортного блока. В случае повторной передачи исходное сообщение может быть разбито на несколько. Это происходит в том случае, когда MAC уровень указывает при повторной передаче размер меньший, чем начальный. Для различия оригинальных пакетов RLC PDU и их частей, которые передаются повторно, используется специальный флаг в заголовке. В случае повторной передачи в заголовок AM RLC включаются ряд дополнительных полей, содержащих информацию о переформатировании пакета.

Следует заметить, что протокол ARQ только обнаруживает ошибку в принятом блоке данных, но не исправляет ее. Для обнаружения поврежденного блока на приеме в стандартном ARQ избыточные биты добавляются к данным, которые должны быть переданы, с использованием кода обнаружения ошибок ED (Error Detection), например, такого как циклический избыточный код CRC (Check Redundancy Code). Вычисление передатчиком циклического избыточного кода CRC передаваемого блока данных позволяет приемнику путем сравнения вычисленного и принятого значений CRC обнаруживать пакеты, содержащие искаженные данные и запрашивать их повторную передачу (рис. 3).

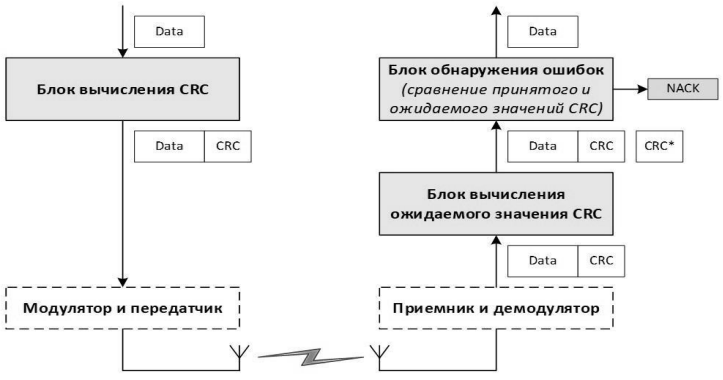


Рис. 3. Блок-схема обнаружения ошибок в протоколе ARQ.

Существует три основные способа обработки ответов на положительные и отрицательные подтверждения механизмов с положительным подтверждением и с повторной передачей PAR:

Стартстопный, или передача с остановкой и ожиданием SAW (Stop And Wait), часто называемый блочным методом передачи.

С возвращением на N кадров GBN (Go Back N), также называемый потоковым методом передачи.

Метод выборочного (селективного) повтора SR (Selective Repeat).

Все они используют некоторую разновидность протокола скользящего окна для указания отправителю на то, какие пакеты (если таковые имеются) должны быть переданы повторно.

Обычно ARQ использует метод, называемый выборочной ретрансляцией, в котором приемник ожидает получение нескольких блоков данных до их подтверждения. Этот метод с одной стороны позволяет передатчику продолжать отправлять пакеты, не дожидаясь их подтверждения, а с другой стороны вносит существенную задержку в случае необходимости повторной передачи. Следовательно, схема ARQ подходит только для потоков эластичных данных non-GBR без гарантии скорости передачи пакетов в сессии. Кроме уже упомянутой задержки, недостатком схемы ARQ является дополнительная нагрузка на канал связи, поскольку даже единичная ошибка требует повторной передачи всего пакета данных.

Построение модели логического уровня RLC архитектуры E-UTRAN. При построении модели логического уровня RLC архитектуры E-UTRAN кроме оценки протокольной избыточности, вносимой заголовками протокольных блоков уровня, большое значение имеет оценка влияния работы протокола ARQ на характеристики радиоканала. В этой связи точное определение таких его характеристик как распределение кратностей переспроса, достоверность, задержка, вероятность невыполнения темпа передачи информации по тракту передачи и т.д., определяющих работу протокола ARQ, является актуальной задачей. Для этого необходимо разработать модель логического уровня RLC архитектуры E-UTRAN и методику определения основных показателей эффективности его работы. Рассмотрим радиоканал с решающей обратной связью (РОС), в котором используются групповые (n, k) коды, обнаруживающие ошибки. Работа радиоканала происходит следующим образом. На приемном конце производится проверка блока из n символов. Если при этом обнаруживается ошибка, то по обратному каналу передается сигнал, требующий повторной передачи блока. Если ошибка не обнаружена, то блок считается правильно принятым, и по обратному каналу посылается сигнал, требующий передачи следующего блока информации.

Уровневая модель логического уровня RLC архитектуры плоскости пользователя радиоканала можно представить выражением [6]:

$$V_{RLC}^{non-CBR} = V_{RAN} \frac{(L_{IP} - H_{IP})\,\beta_{ARQ}}{L_{IP} - H_{IP} + H_{PDCP} + H_{RLC}} \tag{1}$$

Здесь: V_{RAN} - скорость в передачи в радиоканале (бит/с); $\frac{(L_{IP} - H_{IP})}{L_{IP} - H_{IP} + H_{PDCP} + H_{RLC}}$ - протокольная избыточность, вносимая уровнем RLC; $L_{IP}, H_{IP}, H_{PDCP}, H_{RLC}$ - соответственно длина внешнего пакета данных non-GBR, поступающих на уровень PDCP и заголовков: пакета данных, протокольных блоков PDCP и RLC (бит); β_{ARQ} - коэффициент, учитывающий работу протокола ARQ на подуровне RLC и определяет издержки, связанные с дополнительной пропускной способностью радиоканала, затрачиваемую на повторную передачу ошибочных протокольных блоков данных RLC PDU.

Функционал (1) моделируют уровневое логическое соединение для передачи AM PDU RLC и определяют требуемую долю пропускной способности V_{RAN} радиоканала для их передачи. При этом, он зависят не только от необходимой для их работы служебной информации соответствующих объемов и длины протокольных блоков уровня, но и от протокола функционирования механизма ARQ организации обратной связи на уровне RLC для защиты от ошибок в радиоканале.

В [7] показано, что если распределение числа переспрашиваемых PDU RLC подчинено геометрическому закону и они не зависимы друг от друга, то для радиоканала с решающей обратной связью процесс работы механизма ARQ может быть формализован в виде:

$$\beta_{ARQ} = \sum_{k=1}^{\infty} \frac{1}{k} p_0 (1 - p_0)^{k-1} = -\frac{p_0}{1 - p_0} \ln p_0 \tag{2}$$

где p_0 - вероятность отсутствия ошибок в транспортном блоке данных подуровня MAC длины L_{RLC}. В частности, для биномиального канала с вероятностью ошибки в нем равной p , $p_0 = (1-p)^{L_{RLC}}$.

Для каналов с группирующимися ошибками выражение для p_o может быть получено, например, из работ [8, 9].

Оценка влияния механизма ARQ на пропускную способность радиоканала. На рис. 4 и 5 представлены графики зависимостей коэффициента β_{ARQ} от длины PDU RLC для радиоканалов с различными значениями вероятностью ошибки в нем $p_{ош}$.

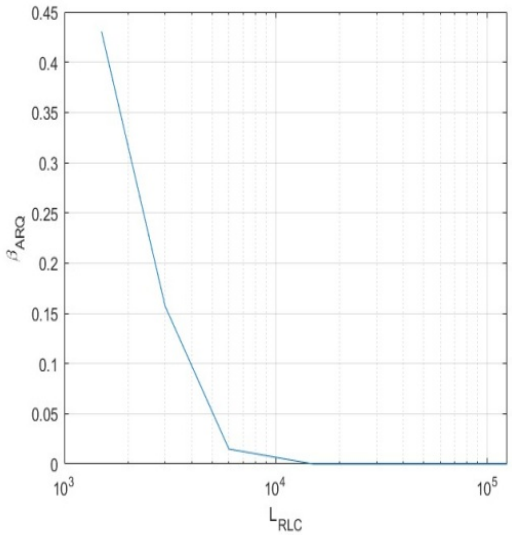


Рис. 4. График зависимости β_{ARQ} от длины PDU RLC L_{RLC}, бит ($p_{ош} = 1 \times 10^{-3}$).

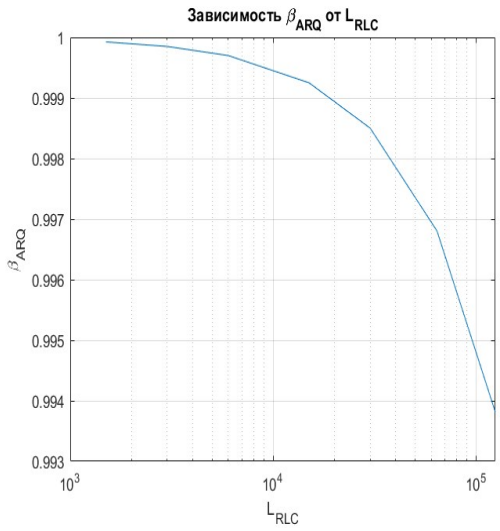


Рис. 5. График зависимости β_{ARQ} от длины PDU RLC L_{RLC}, бит ($p_{ош} = 1 \times 10^{-7}$).

Выводы. В радиоканалах низкого качества (например, $p_{ош} = 1 \times 10^{-3}$) увеличение длины PDU RLC от $L_{RLC} = 1 \times 10^3$ (бит) до $L_{RLC} = 1 \times 10^4$ (бит) снижает значение коэффициента β_{ARQ} от $\beta_{ARQ} = 0,43$ до $\beta_{ARQ} = 0,02$, что приводит к увеличению количества переспросов и блокированию системы.

В радиоканалах высокого качества (например, $p_{ош} = 1 \times 10^{-7}$ бит) выбор длинны PDU RLC зависит только от наличия свободного радиоресурса в данном временном интервале передачи с учетом динамических условий в канале и влиянием работы механизма ARQ на пропускную способность системы практически можно пренебречь.

СПИСОК ЛИТЕРАТУРЫ

1. Ghosh A. Fundamentals of LTE / A. Ghosh, J. Zhang, J.G. Andrews, R. Muhamed. – USA: Prentice Hall, 2010. – 464 p.
2. Dahlman E. 4G: LTE/LTE-Advanced for Mobile Broadband, Second Edition /E. Dahlman, S. Parkvall, J. Skold. – [2nd Edition] – Academic Press, 2013. – 544 p.
3. Sesia S., Toufik I., Baker M. LTE - the UMTS long term evolution. –John Wiley, 2015. – 752 p. https://en.m.wikipedia.org/wiki/E-UTRA
4. 3GPP TS 36.300 E-UTRA Общее описание http://anisimoff.org/lte/rlc.html
5. 3GPP TS 36.322 E-UTRA: спецификация протокола управления радиоканалом (RLC).
6. Мошак Н.Н., Птицына Л.К., Давыдова Е.В., Рудинская С.Р. Метод расчета основных числовых характеристик инфотелекоммуникационной транспортной системы сети lte // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 6 / СПОИСУ. – СПб., 2019. – 446 с. ISBN 978-5-907223-38-7.
7. Птицына Л.К. Мошак А.Н. МОДЕЛЬ ПРОТОКОЛА ARQ В РАДИОКАНАЛЕ СЕТИ LTE. Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября Р32 2020 г.: Материалы конференции. Часть 2. \ СПОИСУ. – СПб, 2020. – 335 с. ISBN 978-5-907223-86-8, с. 302-303
8. Л.П.Пуртов, А.С.Замрай, А.И.Захаров. Основные закономерности распределений ошибок в дискретных каналах связи, «Электросвязь» № 2, 1967, с. 1-8.
9. Элементы теории передачи дискретной информации, под редакцией Л.П.Пуртова. М., «Связь», 1972. С. 232.

УДК 004.057.5

РАЗРАБОТКА ВЕБ-ИНТЕРФЕЙСА ДЛЯ СИСТЕМЫ МОНИТОРИНГА БЕСПРОВОДНЫХ СЕТЕЙ СЕМЕЙСТВА IEEE 802.11

Фёдорова Анастасия Эдуардовна, Герлинг Екатерина Юрьевна, Ахрамеева Ксения Андреевна, Андрианов Владимир Игоревич

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: fyodorova.aaee@gmail.com, gerlingeu@gmail.com, cbor.mail@gmail.com, vladimir.i.andrianov@gmail.com

Аннотация. В статье рассматривается разработка веб-приложения для системы мониторинга беспроводных сетей, развёрнутой на маломощном устройстве, а также предлагается ряд мер для обеспечения информационной безопасности полученного решения. После успешной реализации была проведена оценка работоспособности веб-интерфейса при крайне ограниченных ресурсах.

Ключевые слова: веб-интерфейс; беспроводные сети; система мониторинга.

DEVELOPMENT OF A WEB INTERFACE FOR A MONITORING SYSTEM OF WIRELESS NETWORKS OF THE IEEE 802.11

Fedorova Anastasia, Gerling Ekaterina, Akhrameeva Ksenia, Andrianov Vladimir

The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: fyodorova.aaee@gmail.com, gerlingeu@gmail.com, cbor.mail@gmail.com, vladimir.i.andrianov@gmail.com

Abstract. The article discusses the development of a web application for a wireless network monitoring system deployed on a low-power device, and also proposes a number of measures to ensure the information security of the resulting solution. After successful implementation, the performance of the web interface was assessed with extremely limited resources.

Keywords: web interface; wireless networks; monitoring system.

Введение. С развитием современных технологий и распространением сети Интернет всё больше пользователей прибегают к использованию веб-интерфейса для управления и настройки различных сетевых устройств, таких как маршрутизаторы, модемы, видеокамеры. К числу устройств данного типа может относиться система анализа трафика беспроводной сети, обладающая крайне ограниченными ресурсами.

Преимуществом веб-приложений, в сравнении с приложениями, установленными непосредственно на рабочем месте пользователя, считается хранение данных на общем сервере и осуществление обмена данными по сети. Из этого следует, что для работы с веб-приложением пользователю нужен лишь выход в Интернет и наличие браузера на рабочем месте, у него нет необходимости устанавливать на своё устройство какое-либо дополнительное программное обеспечение и следить за обновлениями используемого продукта.

Другой положительной стороной веб-приложений является масштаб: одновременно им может пользоваться большое количество человек, а также независимость пользователей от операционной системы, потому что такие решения являются кроссплатформенными.

Из-за роста популярности программных комплексов, осуществляющих свою деятельность через сеть Интернет, исследования в области их разработки очень актуальны, однако, требуется уделить внимание работоспособности данных систем при ограниченных ресурсах.

Вследствие вышеизложенного появилась необходимость создания веб-приложения для визуального взаимодействия с системой мониторинга беспроводной сети [1].

Основная часть. Назначение веб-интерфейса для системы мониторинга беспроводной сети заключается в обеспечение возможности визуального взаимодействия пользователя с приложением создания дампов трафика и отслеживания аномалий в части отображения логов с использованием браузера [2].

Другой функцией веб-интерфейса является осуществление входа пользователя в систему по логину и паролю.

Поскольку существующий код системы мониторинга беспроводных сетей написан для применения на Raspberry Pi 3 Model B, то при разработке веб-интерфейса данной системы требуется учитывать ряд особенностей устройств этого типа [3]:

- ограничение в энергопотреблении;
- небольшой запас постоянной памяти;
- отсутствие возможности увеличить оперативную память;
- медленная скорость работы.

Raspberry Pi – это миниатюрный одноплатный компьютер, который с лёгкостью поместится на ладони взрослого человека, также для работы с данным устройством требуется SD-карта, на которую загружается операционная система. В данной работе используется карта 16 Gb.

Основная задача веб-сервера – принимать HTTP-запросы, обрабатывать их и выдавать HTTP-ответы. HTTP-запрос – это сообщение, которое клиент посылает серверу, а HTTP-ответ – это сообщение, которое сервер посылает клиенту.

В данной работе используется Apache HTTP Server. Он обеспечивает надежность, безопасность, стабильность и гибкость настройки, подходит для веб-ресурсов любого масштаба, поддерживает работу как одностраничных сайтов, так и ресурсов с огромной ежедневной аудиторией. Также данный веб-сервер является свободным программным обеспечением и распространяется абсолютно бесплатно.

Веб-разработку можно разделить на две части: frontend и backend. Frontend-специалисты занимаются клиентской стороной – то есть тем, что увидит пользователь.

Backend – это программно-аппаратная часть сервиса, то, что работает на сервере. В зависимости от специализации программист задействует различные технологии создания сайта. Frontend-разработчики обычно не обходятся без таких инструментов, как HTML, CSS и JavaScript. Для Backend трендами разработки являются PHP, Python, Ruby.

Для написания внутреннего кода веб-интерфейса используется язык программирования PHP. Согласно Wappalyzer – приложению, которое позволяет определить используемые технологии на сайте, 82% всех сайтов в интернете сделаны на PHP. Например, Facebook и Wikipedia используют его на своих серверах.

Разработка с помощью PHP дает много возможностей. В отличие от множества других языков программирования, PHP изначально создавался для веб-разработки. Язык PHP имеет ряд неоспоримых преимуществ, среди которых следует отметить высокую скорость работы и, соответственно, общую производительность ресурсов, а также хорошую совместимость с разным программным обеспечением и переносимость, поэтому код, написанный на языке PHP, отлично работает с разными платформами.

База данных — это упорядоченный набор структурированной информации или данных, которые обычно хранятся в электронном виде в компьютерной системе. База данных обычно управляется системой управления базами данных (СУБД).

Поскольку концепция веб-интерфейса для системы мониторинга беспроводных сетей подразумевает хранение логов и информации о пользователях, а именно их логинов и паролей, то возникает необходимость использования подходящей базы данных.

Для хранения нужных администратору сведений была выбрана база данных MySQL. Она имеет в Интернете множество руководств по освоению системы, а также огромное количество всевозможных плагинов и расширений, упрощающих работу с этой системой [4].

Среди главных преимуществ базы данных MySQL можно выделить многопоточность, то есть поддержку обеспечения нескольких одновременных запросов, способность к оптимизации связей с присоединением многих данных за один проход, быструю работу и масштабируемостью

Базы данных MySQL может иметь записи фиксированной и переменной длины, а также обладает гибкая система привилегий и паролей и поддержкой форматов чисел, строк переменной длины и меток времени [5].

Структура выбранного решения представлена на рис. 1.

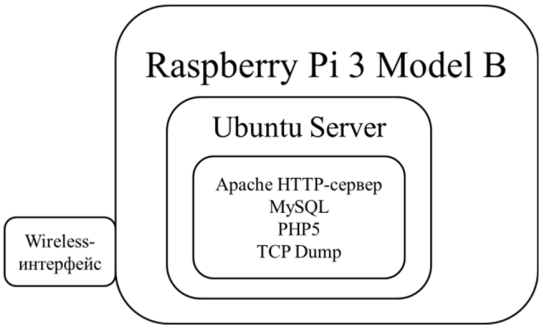


Рис. 1. Структура выбранного решения.

Поскольку система мониторинга беспроводных сетей предполагает осуществление к ней многопользовательского доступа и непрерывное отслеживание аномалий в трафике, возникает проблема осуществления визуального взаимодействия с информацией, полученной в ходе анализа сети [6].

Данную проблему целесообразно решить при помощи разработки веб-интерфейса, который должен содержать следующие модули:

– модуль авторизации, с возможностью вводить логин и пароль пользователя;

– журнал логирования, в котором будут отражаться зафиксированные системой мониторинга аномалии трафика;

– список пользователей, зарегистрированных в системе.

При верном введении адреса веб-сервера в поисковой строке браузера пользователь попадает на страницу авторизации, где ему требуется верно заполнить логин и пароль. При неудачной попытке ввода данных клиент видит сообщение об ошибке и имеет возможность повторно авторизоваться.

После осуществления входа в систему пользователь наблюдает меню, состоящее из трёх модулей: Logs, Users и Dump.

Первый модуль разработанного веб-интерфейса для системы мониторинга беспроводных сетей имеет название Logs и представляет собой журнал логирования, в котором пользователь может наблюдать аномалии, обнаруженные системой мониторинга.

Данный раздел содержит таблицу с двумя столбцами: Date и Message. Они позволяют пользователю узнать дату и время фиксирования аномалии в сети, а также узнать некоторую информацию о ней.

Второй модуль веб-интерфейса под названием Users выводит таблицу, в которой помещена информация о пользователях, имеющих доступ к данной системе мониторинга, а именно их имя и статус.

Все данные, которые пользователь может наблюдать в описанных выше модулях веб-интерфейса, попадают на веб-страницу посредством запросов, выполненных в соответствующие таблицы в базе данных.

Dump является третьим модулем разработанного веб-приложения и обладает возможностью создать дамп трафика и впоследствии скачать его на персональный компьютер.

Среди атак на веб-сервер необходимо выделить следующие:

– DoS-атаки (DDoS-fnfrb);
– атаки грубой силы;
– внедрение кода;
– SQL-инъекции;
– командные инъекции;
– межсайтовый скриптинг.

Чтобы снизить риски возникновения опасностей для веб-сервера Apache требуется выполнить ряд мер по повышению его безопасности.

Основой защиты любого веб-сервера является осуществление его физической безопасности. Из этого следует, что доступ посторонних лиц к серверу должен быть исключен, также администратору необходимо установить пароли для входа в BIOS и в саму систему [7]. Носители информации должны проверяться на вредоносные файлы прежде, чем будут подключены к серверу.

Имеет смысл отключать ненужные модули, скрывать версию Apache и имя операционной системы сервера. По умолчанию Apache перечисляет все содержимое корневого каталога документа при отсутствии индексного файла, эту функцию тоже предусмотрительно будет отключить. Данные действия лишат злоумышленника сведений об атакуемом ресурсе [8].

Также следует совершать регулярные обновления веб-сервера, потому что сообщество разработчиков Apache постоянно работает над различными проблемами уязвимостей и выпускает обновленную версию с новыми параметрами безопасности [9]. Поэтому всегда рекомендуется использовать последнюю версию Apache в качестве веб-сервера.

В дополнение к вышеизложенному, администратору необходимо проводить регулярный мониторинг и аудит журналов, анализируя файлы логирования серверов.

Для повышения уровня безопасности базы данных MySQL также существует ряд рекомендаций. Они включают в себя наличие хороших паролей, чтобы обеспечить данный пункт, целесообразно настроить плагин валидации паролей (VALIDATE PASSWORD PLUGIN). При включении данного плагина будет предложено установить уровень надёжности паролей при валидации [10]. Также снижает риск угроз для базы данных предоставление только необходимых привилегий пользователям и предотвращение инъекций SQL.

Файлы с данными, файлы системного журнала и все файлы приложения должны быть защищены, чтобы гарантировать, что они не читаемы или перезаписываемы неправомочными сторонами.

Чтобы защитить файлы системного журнала от несанкционированного доступа, нужно определить местонахождение их в каталоге, доступ к которому ограничивается администратором базы данных. Если веб-сервер регистрирует в таблицы в базе данных MySQL, нужно дать доступ к тем таблицам только администратору базы данных.

Также существует необходимость контролировать соответствующие резервные копии файлов базы данных, конфигурации и файлов системного журнала, на предмет возможности восстановления утерянных данных для успешного возвращения информации.

В дополнение к вышеизложенным рекомендациям можно поставить и настроить брандмауэр. Это защитит систему от множества различных типов деяний в любом программном обеспечении. Поместить базу данных MySQL необходимо позади брандмауэра или в демилитаризированной зоне [11].

Чтобы произвести оценку работоспособности полученного решения была разработана схема сети, представленная на рис. 2.

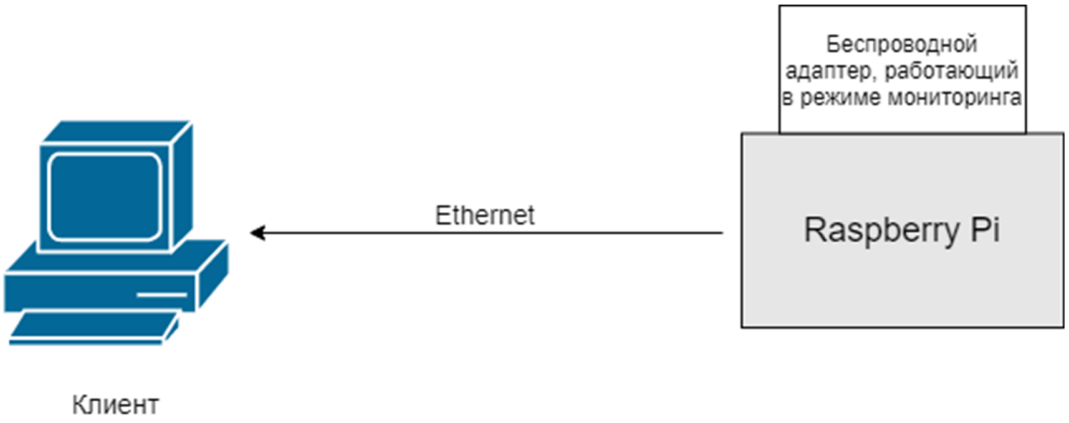


Рис. 2. Схема сети для эксперимента.

Она включает в себя одноплатный компьютер Raspberry Pi, к которому подключен беспроводной USB-адаптер. Именно на данном устройстве развёрнут веб-интерфейс для системы мониторинга беспроводной сети.

Одноплатный компьютер Raspberry Pi соединён кабелем Ethernet с персональным компьютером (ноутбуком).

Для взаимодействия с одноплатным компьютером Raspberry Pi был выбран свободно распространяемый клиент PuTTY, позволяющий осуществить удалённый доступ по протоколу SSH [12].

Исследование производительности маломощного устройства, на котором развёрнут веб-интерфейс системы мониторинга беспроводных сетей, включает в себя четыре эксперимента.

Для проведения всех частей исследования необходимо перевести беспроводной интерфейс в режим мониторинга, чтобы он работал только, а получение пакетов.

Суть первого эксперимента заключается в отслеживание процента использованного времени центрального процессора и процента ОЗУ, используемой процессором у процесса tcpdump при нагрузке беспроводной сети при просмотре видео-контента в качестве 360p.

Во время проведения второго эксперимента показатели процесса tcpdump фиксируются при нагрузке беспроводной сети, порождаемой виде-контентом в качестве 2160p.

Для создания нагрузки в беспроводной сети, чтобы замерить процент использованного времени центральным процессором и процент ОЗУ, используемый процессором у процесса tcpdump, в третьем эксперименте используется сайт Speedtest. Он измеряет максимальную скорость передачи данных между устройством и тестовым сервером при помощи Интернет-соединения.

При четвёртом эксперименте тестовые пакеты со скоростью 30, 45 и 75 Mbps отправляются с персонального компьютера на мобильное устройство, посредством беспроводной сети, создавая при этом нужную нагрузку.

Любой сервер, каким бы мощным он ни был, имеет ограниченный объем ресурсов. Каждая программа, работающая в активном или фоновом режиме, использует определенное количество виртуальной и физической памяти, процессорного времени и т.д. Иными словами, создает определенную нагрузку на сервер. Чтобы посмотреть, насколько система загружена в данный момент времени, используют консольную команду top.

Команда top в Linux системах позволяет вывести в виде таблицы перечень запущенных процессов и оценить, какой объем ресурсов они потребляют, т.е., какую нагрузку создают на сервер и дисковую подсистему. Такая информация помогает в дальнейшем оптимизировать систему, а в данной работе используется для получения информации о проценте использованного времени центральным процессором и проценте ОЗУ, используемого процессором у процесса tcpdump.

В результате проведённого исследования было установлено, что при любой нагрузке беспроводной сети виртуальная память, которую использует процесс tcpdump, равна 8500, процент ОЗУ равен 1,1.

Нагрузка в беспроводной сети возрастает с каждым последующим экспериментом. Однако, когда она порождается отправкой запросов на мобильное устройство с персонального компьютера, значение физической памяти, занятой процессом tcpdump, и общий объем памяти, которую процесс делит с другими, ниже, чем когда нагрузка порождается видео-контентом или тестирование скорости передачи данных в беспроводной сети. Из этого следует вывод, что данные показатели зависят не только от скорости отправки в беспроводной сети Wi-Fi, но и от факторов, определяющих скорость.

Использование центрального процессора увеличивается с ростом нагрузки на беспроводную сеть. Это видно из графика, представленного на рис. 3.

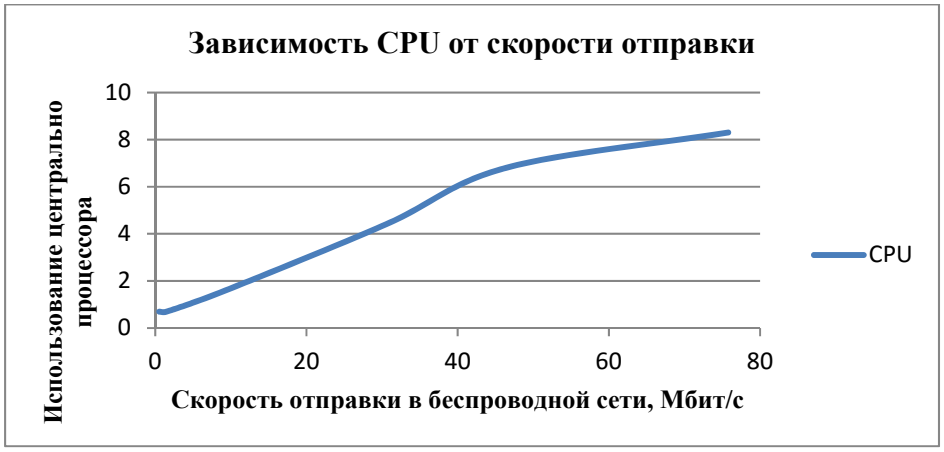


Рис. 3. График зависимости показателя CPU от скорости отправки.

Подводя итог вышеизложенному, можно сделать вывод, что целесообразно использовать маломощное устройство для получения дампа беспроводной сети при малых нагрузках на Wi-Fi, потому что с её увеличением возрастает процент использования центрального процессора утилитой tcpdump, а также время создания дампа трафика необходимого размера.

Также уделить внимание нужно тому факту, что утилита tcpdump сохраняет полученный дамп на SD-карту одноплатного компьютера Raspberry Pi, из этого следует, что пользователю необходимо контролировать количество свободных ресурсов на данном носителе.

Заключение. В результате выполнения данной работы разработан веб-интерфейс для системы мониторинга беспроводных сетей семейства IEEE 802.11, а также выполнены следующие задачи:

- выбраны необходимых для разработки инструменты;
- реализовано разработанное решение;
- исследованы методы обеспечения информационной безопасности веб-интерфейса;
- выявлены особенности реализации полученного решения при крайне ограниченных ресурсах.

СПИСОК ЛИТЕРАТУРЫ

1. Александрова Е.С., Ковцур М.М. Разработка модели нарушителя в беспроводных сетях стандарта IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. Санкт-Петербург. 2017. С. 24-28.
2. Александрова Е.С., Иванов Г.Н., Ковцур М.М. Анализ механизмов защиты WI-FI сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. Санкт-Петербург. 2018. С. 47-51.
3. Габуев А.Г., Красов А.В., Ощенков Ф.Д., Тарасов Н.М. Анализ защищённости современных средств передачи информации посредством портативной лаборатории на основе микрокомпьютера Raspberry Pi // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2020. С. 295-298.
4. Завражнова М. В., Родкина Э. А., Шошина А. В. Разработка базы данных и веб-интерфейса научной электронной библиотеки // Colloquium-journal. 2019. № 19-1 (43). С. 31-34.
5. Ахрамеева К.А., Ковцур М.М., Михайлова А.В. Обеспечение информационной безопасности баз данных web-приложений // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2020. С. 107-110.
6. Ковцур М.М., Луеке П.Э. Разработка системы учёта посещаемости студентов масштаба ВУЗа // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международной научно-технической и научно-методической конференцияи : в 4 т.. 2019. С. 532-537.
7. Штеренберг С. И., Полтавцева М. А. Распределенная система обнаружения вторжений с защитой от внутреннего нарушителя // Проблемы информационной безопасности. Компьютерные системы. 2018. № 2. С. 59–68.
8. Е. Ю. Герлинг, С. Е. Горлов, Д. И. Кириллов Обеспечение информационной безопасности при разработке web-приложений // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2020. С. 326-330.
9. Таргонская, А.И. Разработка защищенного веб-интерфейса для управления устройствами в сети / А.И. Таргонская, А.Ю. Цветков // Актуальные проблемы инфотелекоммуникаций в науке и образование. VIII Международная научно-техническая и научно- методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2019. С. 734-739.
10. Ковцур М.М., Миняев А.А., Потемкин П.А., Хамза Д.Д. Обеспечение информационной безопасности web-приложений с использованием машинного обучения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2020. С. 597-601.
11. Жамишева Н.М., Ташенова Ж.М. Исследование и анализ защиты веб-ресурсов от атак // Актуальные научные исследования в современном мире. 2019. № 12-4 (56). С. 85-89.
12. Стригин С.А. Разработка веб-сайта с применением безопасного стека технологий // Информационная безопасность: современная теория и практика. Сборник научных трудов студентов, аспирантов и преподавателей по материалам III Межвузовской научно-практической конференции. Ответственный редактор З.В. Семенова. Омск, 2020. С. 103-111.

УДК 004.056.53

ИССЛЕДОВАНИЕ АТАК И МЕТОДОВ ЗАЩИТЫ БЕСПРОВОДНЫХ СЕТЕЙ ПРИ АУТЕНТИФИКАЦИИ ПО ПРОТОКОЛУ 802.1X

Храмцов Дмитрий Олегович, Миняев Андрей Анатольевич, Казаков Никита Игоревич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: khramtsov2010@mail.com, minyaev.a@gmail.com, kazakov.ni2.18@gmail.com

Аннотация. В данной статье рассматриваются принципы работы стандарта IEEE 802.1x и представлены четыре DoS-атаки, смоделированных по матрице для корпоративных сетей компанией MITRE, а также смоделированных по БДУ ФСТЭК России. Определяются методы защиты от представленных атак и исследуются способы их реализации на оборудование различных производителей, таких как TP-LINK, ASUS, MikroTik.

Ключевые слова: IEEE 802.1x; Wi-Fi; безопасность беспроводных сетей; RADIUS Server; DoS атаки; механизмы защиты.

RESEARCH OF ATTACKS AND METHODS OF PROTECTION OF WIRELESS NETWORKS DURING AUTHENTICATION OVER THE 802.1 X PROTOCOL

Khramtsov Dmitrii, Minyaev Andrey, Kazakov Nikita
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: khramtsov2010@mail.com, minyaev.a@gmail.com, kazakov.ni2.18@gmail.com

Abstract. This article discusses the principles of the IEEE 802.1x standard and presents four DoS attacks modeled on a matrix for corporate networks by MITRE, as well as modeled on the database of the FSTEC of Russia. The methods of protection against the presented attacks are determined and the ways of their implementation on the equipment of various manufacturers, such as TP-LINK, ASUS, MikroTik, are investigated.

Keywords: IEEE 802.1 x; Wi-Fi; wireless network security; RADIUS Server; DoS attacks; security mechanisms.

Введение. В настоящее время всё чаще применяется технология беспроводного доступа в Интернет. Крупные государственные и частные компании из различных отраслей, образовательные учреждения, имеющие большой список работников, вместо проводной корпоративной сети используют беспроводную.

Для выполнения контролируемого доступа к корпоративной сети часто используется RADIUS сервер, который предназначен для обеспечения централизованной аутентификации, авторизации и учёта пользователей [1]. Однако, существуют проблемы безопасности, связанные с использованием сетей семейства стандартов IEEE 802.11 [2].

Опираясь на статистику Kaspersky [3] DoS и DDoS атаки до сих пор актуальны и легко реализуемы, несмотря на разработанные протоколы безопасности. С каждым годом это число только увеличивается. По диаграмме можно заметить, что общее количество DDoS-атак выросло в 1,5 раза по сравнению с 2020 и 2019 годами соответственно. Диаграмма представлена на рис. 1.

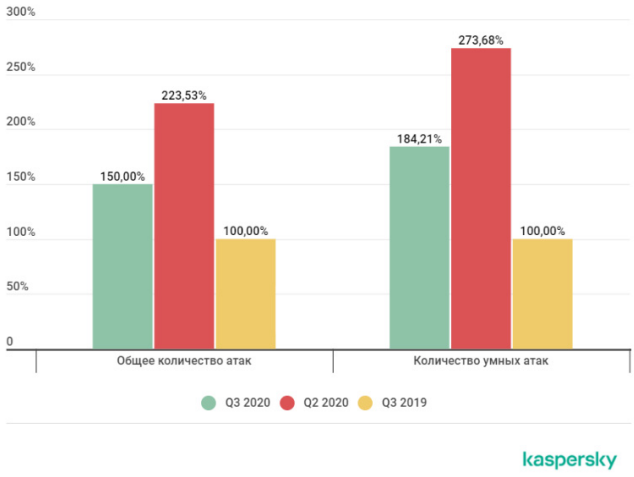


Рис. 1. Диаграмма DDoS-атак за 2019 и 2020 года согласно исследованиям Kaspersky.

Также количество инцидентов в 2020 году увеличилось на 51% по сравнению с 2019 годом по данным компании Positive Technologies, а 86% всех атак были направлены на организации. Больше всего злоумышленников

интересовали государственные и медицинские учреждения, а также промышленные компании. На рис. 2 показана статистика инцидентов в каждом месяце.

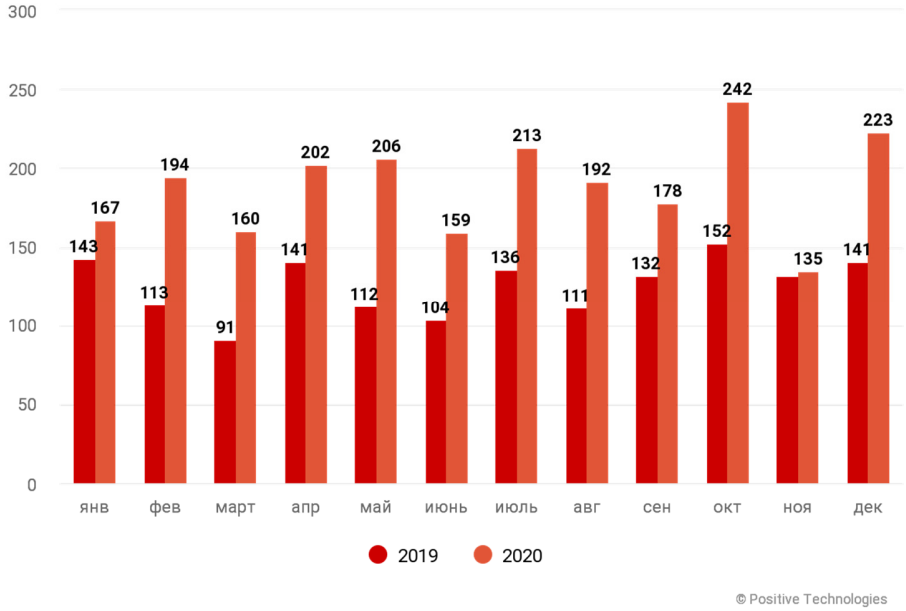


Рис 2. Количество инцидентов в 2019 и 2020 годах.

В рамках данной работы рассматривается наиболее распространенный тип построения корпоративной сети. Для исследуемой информационной системы актуальным является внешний нарушитель, не имеющий доступ в контролируемую зону и к средствам вычислительной техники (в соответствии с методическими документами ФСТЭК России «Методика оценки угроз безопасности информации», утв. 5 февраля 2021 г.). Схема организации сети представлена на рис. 3. В ней есть легитимные клиенты, установлена точка доступа, на которой включен режим WPA2-Enterprise [4]. Развернут RADIUS сервер на операционной системе на ядре Linux, системный администратор и злоумышленник, который отправляет фальшивые сообщения по беспроводной сети [5].

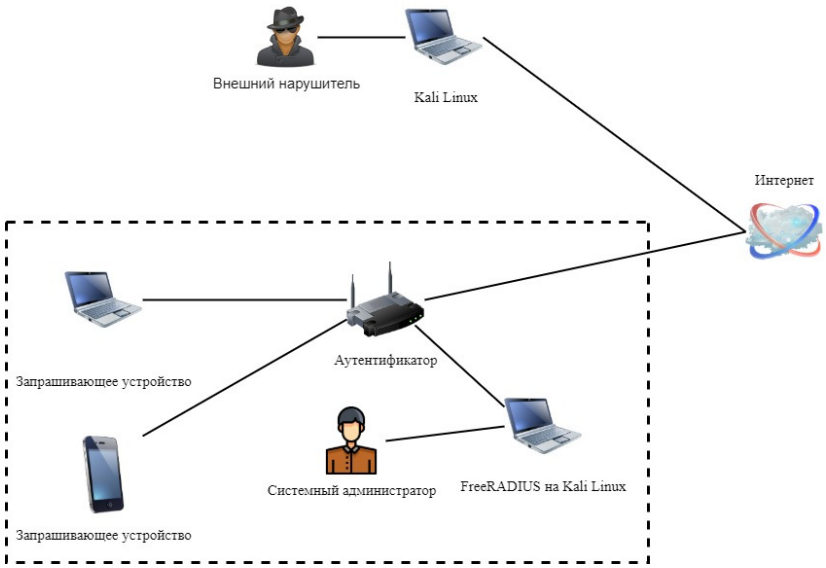


Рис. 3. Схема стенда тестируемой сети.

Корпоративные сети с шифрованием WPA2-Enterprise строятся на аутентификации по протоколу 802.1x через RADIUS-сервер. Протокол 802.1x определяет методы отправки и приема запроса данных аутентификации и обычно встроен в операционные системы и специальные программные пакеты.

802.1x предполагает три роли в сети:

– клиент (supplicant) - клиентское устройство, которому нужен доступ в сеть;
– сервер аутентификации (RADIUS сервер);
– аутентификатор – устройство (маршрутизатор, коммутатор, точка доступа, беспроводной контроллер), которое соединяет множество клиентских устройств с сервером аутентификации и отключает/подключает клиентские устройства.

На рис. 4 показан принцип работы протокола 802.1x, а также смоделированные DoS атаки: EAPOL-Start, EAPOL-Logoff, EAP-Failure, EAP-Success по Mitre att&ck matrix и базы данных угроз ФСТЭК России, которые состоят из одной тактики и техники, представленных в таблице 1 и 2.

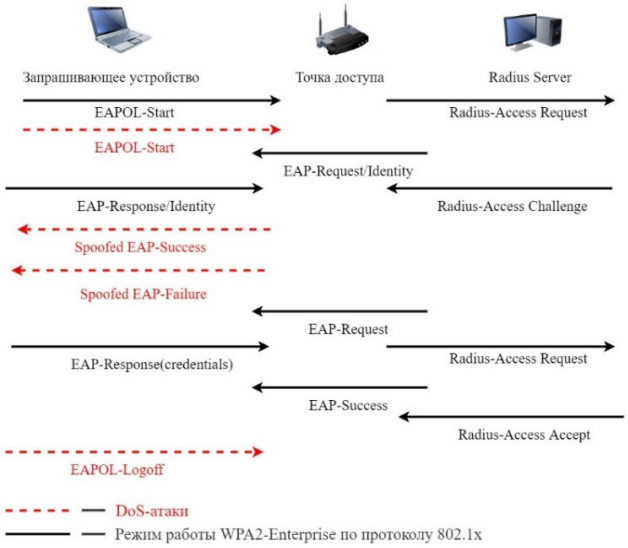


Рис. 3. Схема работы стандарта 802.1x.

Запрашивающее устройство отправляет пакет EAPOL-Start, чтобы инициировать сеанс аутентификации. Затем аутентификатор отвечает пакетом EAP-Request/Identity, инкапсулированным в формат пакета EAPOL. Далее супликант отправляет аутентификатору свои учетные данные в сообщении EAP-Response/Identity. Аутентификатор получает этот пакет и инкапсулирует его в RADIUS Access Request-EAP/Identity сообщение. Точка доступа передаст этот кадр RADIUS на сервер аутентификации. После того, как сервер аутентификации получает сообщение запроса доступа RADIUS, он подтверждает, что идентификатор запрашивающей стороны действителен. Сервер аутентификации отправит сообщение с запросом на основе идентификатора клиента для запроса сертификата клиента. Аутентификатор получит сообщение RADIUS-Access Challenge и передаст его запрашивающей стороне. Запрашивающий ответит сообщением EAP-Response, содержащим его учетные данные. Если сервер аутентификации проверит сертификаты, он ответит сообщением EAP-Success. После успешной аутентификации клиент может использовать контролируемый порт и сетевые ресурсы.

Таблица 1

Смоделированная атака по БДУ ФСТЭК России

Тактика	Техника
Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям, Тактическая задача: достижение нарушителем конечной цели, приводящее к реализации моделируемой угрозы и причинению недопустимых негативных последствий.	Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети.

Таблица 2

Смоделированная атака по MITRE Att&ck matrix

Тактика	Техника
Противник пытается собрать информацию, которую он может использовать для планирования будущих действий. Разведка состоит из методов, которые вовлекают противников в активный или пассивный сбор информации, которая может использоваться для поддержки наведения на цель.	Противники могут выполнять активное разведывательное сканирование для сбора информации, которая может быть использована во время наведения на цель. Активное сканирование — это сканирование, при котором злоумышленник исследует инфраструктуру жертвы через сетевой трафик, в отличие от других форм разведки, не предполагающих прямого взаимодействия.

Для организованной сети была предложена следующая методика для тестирования беспроводной сети:

1. Эмуляция АРМ, атакующего (kali linux);
2. Эмуляция АРМ тестирования (kali linux);
3. Использование анализатора трафика (wireshark);
4. Перехват пакета с помощью анализатора трафика;
5. Формирование большого количества пакетов и отправка их;
6. Обработка результатов и принятие решения.

На трех точках доступа: TP-Link Archer AX50, ASUS WL-520 GU, MikroTik mAP lite RBMAPL-2ND, исследовалось, при каком количестве пакетов в секунду DoS атака была успешна. Результаты представлены в таблице 3.

Таблица 3

Воздействие точек доступа на DoS атаки

Точка доступа	EAPOL Logoff, кол-во пакетов в секунду	Premature EAP-Success, кол-во пакетов в секунду	Premature EAP-Failure, кол-во пакетов в секунду	EAPOL Start, кол-во пакетов в секунду
ASUS WL-520GU	1	5	10	1
TP–LINK Archer AX50	5	10	5	5
MikroTik mAP lite RBMAPL-2ND	1	5	1	1

Для данных DoS атак существуют следующие механизмы защиты [6-7]:

1.В настройках маршрутизатора можно устанавливать канал, на котором будет вещаться Wi-Fi сеть.

2.Используется фильтрация MAC-адресов. При фильтрации подключиться к сети могут только устройства, MAC-адреса которых администратор внес в таблицу доверенных на точке доступа.

3.Рекомендуется выбирать оборудование беспроводной сети, поддерживающее стандарт 802.11w. Данный стандарт обеспечивает защиту управляющего трафика между клиентом и точкой доступа.

4.Внедрение WIPS [8]. Это система, которая осуществляет мониторинг окружающего радиоэфира с помощью сенсоров. Они анализирует полученную информацию об источниках радиосигнала, их взаимодействиях и аномальных (необычных) активностях и предотвращает действия, противоречащие настроенной политике предотвращения вторжений.

5.Ограничение радиовидимости беспроводной сети вне территории, на которой эксплуатируется беспроводная сеть.

6. Наличие логирования событий безопасности на беспроводном оборудовании, в том числе отражение сообщений об ошибках авторизаций и их обработка системой мониторинга и персоналом компании.

7. Скрытие имени SSID.

Заключение. При выполнении работы смоделирована типовая корпоративная среда, использующая беспроводные технологии по протоколу 802.1x. Используя тактики и техники БДУ ФСТЭК России и MITRE ATT&CK разработаны сценарии атаки. Предложена методика тестирования и определены механизмы защиты от атак.

СПИСОК ЛИТЕРАТУРЫ

1. Ковцур М.М., Поляничева А.В. Исследование механизма авторизации пользователей для доступа к IP-ТВ сервисам с применением RADIUS-сервера /VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 1. С. 466–471.
2. Юркин Д. В., Никитин В. Н. Системы обнаружения вторжений в сетях широкополосного радиодоступа стандарта IEEE 802. 11 //Информационно-управляющие системы. – 2014. – №. 2 (69).
3. Отчеты о DDoS-атаках. DDoS-атаки в III квартале 2020 года [Электронный ресурс] URL: https://securelist.ru/ddos-attacks-in-q3-2020/99091/ (дата обращения 05.06.2021).
4. Ковцур М.М., Симанов М.С. Анализ особенностей организации авторизации пользователей в сетях коллективного доступа стандарта IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научнометодической конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 4. С. 537-541.
5. Александрова Е.С., Ковцур М.М. Разработка модели нарушителя в беспроводных сетях стандарта IEEE 802.11 / VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. Т. 2. С. 24-28.
6. Александрова Е.С., Иванов Г.Н., Ковцур М.М. Анализ механизмов защиты Wi-Fi сетей / VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 1. С. 47–51.
7. Казаков Д.Б., Красов А.В., Лоханько Н.О., Подоляк Р.С. Методика защиты сети связи от DDoS атак с помощью BGP FLOWSPEC / V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3-х т. СПб. : СПбГУТ, 2016. Т. 1. С. 386-390.
8. Зуев И.П., Карельский П.В., Ковцур М.М., Юркин Д.В. Разработка методики проведения испытания IPS модулей / IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. Т. 1. С. 492-496.

УДК 004.418

МЕТОДИКА АНАЛИЗА ПОХОДКИ ЧЕЛОВЕКА КАК СРЕДСТВО ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

Шабарова Виктория Александровна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mail: vikashabarova@mail.ru

Аннотация. В данной статье представлен обзор методов идентификации пользователей на основе поведенческих алгоритмов. Рассмотрены варианты применения бихевиоральных паттернов в повседневной жизни человека. Нетрадиционные методы поведенческой биометрии могут выступать достойной и более надёжной альтернативой традиционной биометрии. В особенности была рассмотрена аутентификация пользователя методом анализа походки человека. Применение такого подхода может уменьшить нагрузку на пользователя, пользователю не нужно помнить сложный пароль или предъявлять идентификационную карту. К тому же, данный подход может служить дополнительной мерой по усилению защиты. Несомненно, данное направление является перспективным в дальнейшем исследовании.

Ключевые слова: идентификация пользователя; поведенческие алгоритмы; несанкционированный доступ; клавиатурный почерк; поведенческий анализ; бихевиоральные паттерны; биометрическая аутентификация.

ANALYSIS OF HUMAN WALK AS A USER IDENTIFICATION METHOD ON MOBILE DEVICES

Shabarova Viktoriia
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mail: vikashabarova@mail.ru

Abstract. This article provides an overview of user identification methods based on behavioral algorithms. Variants of application of behavioral patterns in everyday life of a person are considered. The relevance of chosen topic lies in the fact that unconventional behavioral biometrics can provide a worthy and more reliable alternative to traditional biometrics. User authentication by human walk analysis was considered separately. This approach can reduce the burden on the user, since the user would not need to remember a complex password or to present an ID card. In addition, such approach may serve as an additional measure to strengthen security. Undoubtedly, this direction is promising for further research.

Keywords: user identification; behavioral algorithms; unauthorized access; behavioral analysis; behavioral patterns; biometric authentication.

Введение. В настоящее время существует множество различных алгоритмов проверки подлинности введённых данных. Одними из самых широко используемых механизмов являются: традиционные биометрические модальности (лицо, голос, палец, сетчатка глаза, подпись) [1, 2], нетрадиционные биометрические модальности (клавиатурный почерк, движение губ, походка, ДНК, запах), мультимодальности, однофакторная аутентификация, многофакторная аутентификация, цифровые сертификаты и ЭЦП (электронно-цифровая подпись) [2]. Объектом исследования в данной статье являются биометрические методы идентификации. Предметом исследования является мультимодальная нетрадиционная биометрия и её преимущество над традиционной модальностью.

Постановка задачи. Актуальность темы заключается в доказанной слабости и рискованности методов биометрической аутентификации, альтернативой которой служит, выдвигаемая мировыми трендами, поведенческая биометрия. Поведение каждого человека уникально. У каждого из пользователей свои особенности нервной системы, формы мышления, эмоций [1, 3].

Аутентификация человека. Аутентификация человека строится на трёх основных принципах

По собственности (пропуск, пластиковая карта, ключ, документы).

По знаниям (пароли, коды, дополнительная информация).

По биометрическим характеристикам.

Основным минусом верификации пользователя является то, что человеку постоянно нужно носить с собой документы и помнить пароли. В связи с этим существует проблема потери и забывания информации, что может привести к утечке важных данных. В случае с биометрическими характеристиками пользователю не требуется дополнительная информация и документы, поиск объекта осуществляется по всей базе данных.

Разные виды статических биометрических характеристик обладают разными уровнями безопасности. Так, например, одной из самых распространенных методик является идентификация пользователя по отпечатку пальца. Несомненно, данная процедура проста в реализации и имеет широкое распространение в современном мире, но точность идентификации может быть снижена из-за повреждения пальца. Также высока вероятность репродуцирования. Последние несколько лет также активно внедряется распознавание по геометрии лица; плюс данной методики состоит в том, что не требуется дорогостоящее оборудование и не нужен физический контакт

с устройством. Но минусом данной процедуры является то, что если в базе данных сохранено лицо человека в молодости, то в старости распознавание производиться не будет, существует необходимость постоянного обновления базы данных. Также необходимо соблюдение особенных требований по освещённости в помещении или на улице и положению и выражению лица пользователей. Также существует высокая вероятность репродуцирования. Идентификацию пользователя, помимо этого, можно проводить по радужной оболочке глаза. В отличие от предыдущих методик, в данном случае отсутствует необходимость контакта с устройством, также отсутствуют временные изменения радужной оболочки глаза. Это приводит к низкой вероятности репродуцирования. Но для применения данной методики необходимо дорогостоящее оборудование, применение его повсеместно в данный момент времени не представляется возможным. Стоит заметить, что из-за хирургического вмешательства врачей возможны ошибки в идентификации пользователя [1].

Основные проблемы классической биометрии.

Идентификация пользователя осуществляется только на определённом этапе взаимодействия (вход в приложение, ввод информации, подтверждение транзакции).

Требует внедрения дополнительных устройств.

Основана на внешних (видимых) физиологических характеристиках.

Поведенческие алгоритмы. Анализ поведения пользователей и выявления аномалий в их поведении может стать отличной альтернативой классической биометрии. Нейросети способны отождествлять пользователя с конкретной личностью по множеству критериев сразу, что делает поведенческую биометрию мультимодальной.

К примеру [4]:

- По наличию сохранённых файлов Cookie;
- По тенденции к посещению значимых сайтов;
- По анализу динамики электронной подписи;

Принцип метода заключается в верификации динамики подписи. Происходит анализ того, как человек пишет своё имя или визирует документ. Анализ происходит не самой подписи (её можно подделать), а процесса её получения. В качестве измеряемых характеристик можно выделить: угол, под которым пользователь держит ручку, скорость написания, сила нажатия. Все эти показатели могут быть рассмотрены как уникальные поведенческие характеристики.

По анализу работы с клавиатурой и мышью (на ПК);

Методика заключается в анализе ритма печати. Но динамика работы с мышью и клавиатурой может меняться как в течение дня (пользователь отвлекается на работе), так и в течение всей жизни (развивается навык скоростного печатанья).

По клавиатурному почерку (на смартфонах);

У каждого человека индивидуальный подход к набору текста при помощи двух рук. Уникальные характеристики клавиатурного почерка выявляются по набору случайного текста и ключевой фразы. Данная поведенческая биометрическая характеристика описывает следующие аспекты: динамика ввода, скорость ввода, возникновение ошибок при наборе текста, особенности набора двух-трёх сочетаний символов подряд. Массив полученных данных обрабатывают специальные алгоритмы и сравнивают его с предыдущими взаимодействиями пользователя. Несомненными плюсами являются простота внедрения, возможность скрытой аутентификации, а также то, что не требуется дополнительных действий от пользователя. Помимо этого, существуют и минусы данной технологии, в частности всё зависит от конкретной раскладки клавиатуры. Также нужно учитывать состояние пользователя на момент ввода данных, так как настроение и психологическое состояние напрямую влияют на динамику набора текста [5].

По походке. Возможно пассивно верифицировать или идентифицировать человека, не привлекая его к дополнительным действиям. Плюсом является то, что для идентификации человека в данном случае не требуются изображения высокого разрешения.

Поведенческую биометрию также называют пассивной, поскольку пользователям не нужно совершать каких-либо дополнительных действий. Поведенческая биометрия позволяет выявляет нарушителей на ранних этапах атаки. Важным плюсом является то, что поведенческие характеристики не получится подделать [1].

Преимущества поведенческих алгоритмов.

Непрерывная идентификация;

Не требует установки дополнительных устройств;

Работает на всех платформах и устройствах;

Незаметна для пользователей;

Индивидуальный набор анализируемых характеристик;

Альтернатива для методов многофакторной аутентификации;

Высокая точность идентификации.

Сложность компрометации алгоритма со стороны злоумышленников.

Существующие экспериментальные исследования доказывают, что поведение человека моделируемо и прогнозируемо, и предлагают анализировать работу пользователя как с текстовыми данными, так и с устройствами

ввода-вывода, рассчитывая устойчивые паттерны работы по времени, активности и тематической направленности и анализируя отклонения от прогнозируемых величин. Данные методы поведенческой биометрии легко внедряемы, так как современные устройства работы в большинстве своём уже обладают необходимыми сенсорами и трекерами. Внедрение проанализированных методов позволит уменьшить усилия по обеспечению кибербезопасности и минимизировать затраты.

Идентификация по походке.

Рассмотрим аутентификацию пользователя методом анализа походки человека. Для распознавания походки никаких особых действий от объекта не требуется. Походка — это уникальная характеристика каждого человека. Она зависит от таких параметров как: вес, положения позвоночника, длина конечностей, осанка, характер, скорость, стиль движения. Все эти данные и создают неповторимую особенность поведения человека при ходьбе. Злоумышленнику будет сложнее имитировать стиль ходьбы в течение длительного периода времени, что приведет к тому, что сделать аутентификацию путем подделки модели поведения не представляется возможным. Применение такого подхода может уменьшить нагрузку на пользователя, пользователю не нужно помнить сложный пароль или идентификационную карту, либо служить дополнительной мерой по усилению защиты.

Если рассматривать походку, как совокупность поз и движений, можно выделить два наиболее распространенных способа регистрации такой информации: видеосъемка и регистрация с использованием датчиков, находящихся на теле человека.

В настоящее время мобильные телефоны, смартфоны, коммуникаторы, карманные персональные компьютеры и т.д., получили широкое распространение. Большинство из них оснащаются акселерометрами, которые и позволяют замерять необходимые параметры [6]. Именно с помощью данных, снятых с этих акселерометров, и будет производиться идентификация пользователей по походке.

Идентификация человека будет производиться путем соединения информации с акселерометра телефона и данных, полученных с видеокамеры.

Рассмотрим распознавание движения человека на видеосъемке.

Базовыми признаками походки являются [7]:

– Бинарные маски силуэта;

Это усредненные по одному циклу походки бинарные маски силуэта движущегося человека. В предположении, что движения человека во время ходьбы периодически повторяются, вычисляется пространственно-временное описание походки человека. Полученные изображения характеризуют частоты нахождения человека в той или иной позе во время движения.

– Изображение энергии походки;

Эти изображения представляют собой усредненные по одному циклу походки бинарные маски силуэта движущегося человека.

– Поза (скелет) человека.

Исследовать позу человека (положение ключевых точек фигуры – основных частей тела и суставов) в каждом полученном кадре.

Для того чтобы произвести анализ данных, полученных с камеры, необходимо разбить видеофайл на отдельные кадры, выделить силуэт движущегося человека. После чего необходимо произвести обработку и накопление данных.

Классификация выделения объекта на основе обработки изображения:

– Попиксельные алгоритмы;

– Попиксельные алгоритмы обрабатывают все точки изображения независимо. Обычно вначале они строят цветовую модель фона и во время работы оценивают, насколько текущий цвет пикселя ей соответствует.

– Поблочные алгоритмы;

– Поблочные алгоритмы обрабатывают независимо группы пикселей, объединенные в блоки.

– Алгоритмы, основанные на минимизации функционала энергии по всему изображению.

Алгоритмы позволяют использовать информацию со всего изображения в совокупности, включая информацию о градиенте яркости между соседними пикселями. Такой подход позволяет учесть и то, что граница объекта чаще разделяет пиксели, которые сильно различаются по цветам, чем те, что наоборот похожи по цвету.

В первую очередь необходимо подготовить изображение к выделению движущегося объекта. Во-первых, необходимо уменьшить размер кадра, что позволит существенно сократить объем информации, которую необходимо обрабатывать. Во-вторых, необходимо обнаружить объект на кадре. Это можно сделать путем применения алгоритмов, представленных выше. Чтобы обработать бинарные изображения с выделенной фигурой будем использовать фреймворк SimpleCV, написанный на языке программирования Python. После обнаружения человека внутри кадра, необходимо определить направление движения.

Для получения параметров движения, необходимо определить центр тяжести при ходьбе и вычислить изменение длины шага.

Рассмотрим данные, полученные с акселерометра телефона. Акселерометр — это прибор, который измеряет кажущееся ускорение. Он помогает понять смартфону о том, что он перемещается и в каком положении находится.

Рассмотрим параметры подвижности, которые можно получить через встроенное приложение на iPhone. Для того чтобы наиболее точно регистрировать измерения, необходимо нести телефон на уровне талии, например, в кармане.

Параметры ходьбы, которые можно получить с iPhone:

– Асимметрия при ходьбе;

Значение асимметрии при ходьбе выражается процентом времени, когда шаг одной ногой быстрее или медленнее, чем другой.

– Время двойной поддержки;

Процент времени при ходьбе, когда обе ноги стоят на земле.

– Длина шага;

Это расстояние при ходьбе между ногой, которая находится впереди, и ногой, которая находится позади.

– Скорость ходьбы.

Определяет, насколько быстро человек может идти по ровной поверхности.

Таким образом с помощью данных, полученных с камер видеонаблюдения и со встроенных датчиков смартфона можно определить уникальные характеристики походки человека.

Методика анализа данных. Задача состоит в том, чтобы выявить аномалии, то есть выделить необычные значения в выборке данных.

Этапы алгоритма.

– Сбор данных;

Собираются данные о центре тяжести при ходьбе и длины шага, также берется скорость движения при ходьбе.

– Создается модель пользователя;

В течение некоторого времени происходит накопление данных, после чего их можно использовать.

– Расчет схожести полученной выборке и идеальной;

Расчет расстояния между моделью пользователя и полученной выборкой. Расстояние рассчитывается с помощью расстояния Махаланобиса, можно определять сходство неизвестной и известной выборки.

Анализ полученных результатов.

Расчет вероятности того, что идентификация по походке корректна.

Таким образом была разработана методика для аутентификации пользователя методом анализа походки человека. Несомненно, данное направление является перспективным в дальнейшем исследовании.

Заключение. Применение данной технологии позволит предотвратить мошеннические платёжные транзакции. Поведенческая биометрия в ближайшее время придёт на смену традиционной биометрики, так как исследования показывают, что общепринятая система логин-пароль теряет свою надёжность в защите информации. Благодаря простоте и удобству внедрения методики, можно сделать финансовые услуги и цифровые сервисы более доступными для маломобильных пользователей и жителей отдалённых регионов, что приведёт к развитию всей банковской отрасли. Не менее важным является то, что применение данного метода сможет существенно снизить затраты на обеспечение безопасности конфиденциальных данных пользователей. Применение поведенческих алгоритмов позволит обеспечить более высокую безопасность.

СПИСОК ЛИТЕРАТУРЫ

1. Анисимов Р. Идентификация по нажатию клавиш: системы безопасности учатся анализировать поведение пользователей. [Электронный ресурс] // Журнал Forbes. АО «АС РУС МЕДИА», 04.05.2017. URL: https://www.forbes.ru/tehnologii/342733-identifikaciy (Дата обращения 07.05.2021).
2. ГОСТ Р 54411-2018/ISO/IEC TR 24722:2015. БИОМЕТРИЯ. Мультимодальные и другие мультибиометрические технологии. Information technology. Biometrics. Multimodal and other multibiometric fusion (2018). // НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. Москва: Стандартинформ, 2018.
3. Савинова В.М., Бесхмельницкий А.А., Бибина Е.С., Осадчая А.Д. Идентификация пользователей корпоративной системы с помощью поведенческого анализа с использованием модели искусственной нейронной сети [Электронный ресурс] // ТДР. 2017. №5. URL: https://cyberleninka.ru/article/n/identifikatsiya-pol (Дата обращения: 07.05.2021).
4. Юрасов Д.С., Зикратов И. А. Различение пользователей на основе их поведения в сети Интернет [Электронный ресурс] // Научно-технический вестник информационных технологий, механики и оптики. 2013. №6 (88). URL: https://cyberleninka.ru/article/n/razlichenie-polzova (Дата обращения: 08.05.2021).
5. Zanna K., King S., Neal T., Canavan S. Studying the Impact of Mood on Identifying Smartphone Users. [Электронный ресурс] // Department of Computer Science and Engineering University of South Florida, Tampa, FL USA. 27.07.2019. URL https://www.researchgate.net/publication/334129925_St. (Дата обращения 08.05.2021).
6. Казанцева А.Г., Лавров Д.Н. Распознавание личности по походке на основе wavlet-параметризации показаний акселерометров // Математические структуры и моделирование 2011, вып. 23, с. 31–37
7. Соколова А.И., Конушин А.С. Методы идентификации человека по походке в видео. Труды ИСП РАН, том 31, вып. 1, 2019 г., стр. 69-82.

ОГЛАВЛЕНИЕ

CONTENTS