САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
РЕГИОНАЛЬНАЯ ИНФОРМАТИКА

Сборник трудов

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Выпуск 3

Санкт-Петербург
2017

http://spoisu.ru

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
РЕГИОНАЛЬНАЯ ИНФОРМАТИКА

Сборник трудов

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Выпуск 3

Санкт-Петербург
2017

http://spoisu.ru

УДК (002:681):338.98

Р32

Региональная информатика и информационная безопасность.
Р32 Сборник трудов. Выпуск 3 / СПОИСУ. – СПб., 2017. – 346 с.
ISBN 978–5–906931–68–9

Сборник статей охватывает широкий круг направлений Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России» и Санкт-Петербургской международной конференции «Региональная информатика», проведенных при поддержке Правительства Санкт-Петербурга: Государственная политика в сфере информатизации и информационной безопасности; Телекоммуникационные сети и технологии; Безопасность информационных технологий; Современные средства защиты информации; Информационно-экономическая безопасность; Информационная безопасность и импортозамещение в критических инфраструктурах; Подготовка и переподготовка ИТ-специалистов; Подготовка и переподготовка ИТ-специалистов; Информационные технологии в социокомпьютинге; Информационные технологии управления объектами морской техники и морской инфраструктуры; Информационно-психологическая безопасность; Информационные технологии в экологии; Информационная безопасность киберфизических систем; Молодежные научные школы: Безопасные информационные технологии; Молодежные научные школы: Информационные технологии математического моделирования.

Предназначен для широкого круга руководителей и специалистов органов государственной власти и местного самоуправления, промышленности, науки, образования, бизнеса, аспирантов и студентов высших учебных заведений Санкт-Петербурга и других регионов, специализирующихся в вопросах информатизации, связи, информационной безопасности и защиты информации.

УДК (002:681):338.98

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

Публикуется в авторской редакции

Подписано в печать 20.10.2016. Формат 60x84⅛. Бумага офсетная.
Печать – трафаретная. Усл. печ. л. 30,7. Тираж 500 экз. Заказ № 1093
Отпечатано в ООО «Политехника-принт»
190005, Санкт-Петербург, Измайловский пр., 18-д

ISBN 978–5–906931–68–9

© Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления (СПОИСУ), 2017 г.
© Авторы, 2017 г.

ST. PETERSBURG INTERREGIONAL CONFERENCE
INFORMATION SECURITY OF RUSSIAN REGIONS

ST. PETERSBURG INTERNATONAL CONFERENCE
REGIONAL INFORMATICS

Proceedings

REGIONAL INFORMATICS AND INFORMATION SECURITY

The Issue No 3

St. Petersburg
2017

http://spoisu.ru

ГОСУДАРСТВЕННАЯ ПОЛИТИКА В СФЕРЕ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 323

ВЛИЯНИЕ СЕКЬЮРИТИЗАЦИИ НА ПОЛИТИКУ РОССИИ: ИНФОРМАЦИОННЫЙ АСПЕКТ

Баранов Николай Алексеевич
Санкт-Петербургский государственный университет,
Санкт-Петербург, ул. Смольного, д.1-3, 7-й подъезд
Северо-Западный институт управления – филиал РАНХиГС
199178, Санкт-Петербург, В.О., Средний пр. В.О., д. 57/43
email: nicbar@mail.ru

***Аннотация*:** Массовая информатизация общества способствует возникновению новых угроз безопасности, которые распространяются как на частную жизнь, так и на социальную, политическую, экономическую сферы. Секьюритизация предполагает приоритет экстремальной политики над установленными нормами и правилами решения аналогичных вопросов. Речь идет об экстренных мерах, предпринимаемых для снижения угрозы безопасности. В результате ценность безопасности начинает превалировать над всеми остальными политическими ценностями, детерминируя все сферы жизни. В сложившихся условиях высокую значимость приобретает деятельность государства в информационной сфере, которая может способствовать распространению процесса секьюритизации, подвергая опасности права и свободы человека.

Ключевые слова: *информатизация, секьюритизация, угрозы безопасности, экстремальная политика.*

INFLUENCE OF SECURITIZATION ON POLICY OF RUSSIA: INFORMATION ASPECT

Baranov Nikolai
St. Petersburg State University
Russia, St. Petersburg, Smolny St., 1-3, 7th entrance,
Northwest institute of management – RANEPA branch,
Russia, St. Petersburg, V.O., Sredny Ave. V.O., 57/43
email: nicbar@mail.ru

Abstract: Mass informatization of society promotes emergence of new threats to security which extend both to private life, and to social, political, economic spheres. Securitization assumes a priority of extreme policy over the established norms and rules of the solution of similar questions. It is about the emergency measures undertaken for decrease in threat to security. As a result the value of safety begins to prevail over all other political values, determining all spheres of life. At this conjuncture the high importance is gained by activity of the state in the information sphere which can promote securitization process distribution, endangering the right and freedom of the person.

Keywords: *informatization, securitization, threats to security, extreme policy.*

Введение. В современных обществах на первый план выходят проблемы безопасности, что вполне объяснимо с точки зрения социальных приоритетов. В соответствии с иерархией потребностей американского психолога А. Маслоу потребности безопасности и порядка у индивида возникают после реализации физических потребностей и предшествуют социальным контактам – потребностям в общении, дружбе и принадлежности к сообществу. Однако, как показывают реальное поведение людей и их мотивация, не существует жесткой, последовательной системы удовлетворения потребностей. В зависимости от смены ситуации, жизненных обстоятельств высшие потребности могут утратить доминирующее значение, а потребности более низкого порядка — приобрести для человека большую значимость.

В развитых обществах произошла именно такая трансформация потребностей: люди, стремящиеся к самореализации, для которых приоритетными стали постматериалистические ценности, вынуждены отказываться от части завоеванных свобод и возможностей в пользу безопасности, ввиду угрозы их стабильному существованию. Причиной такого выбора стали террористическая опасность, неконтролируемая миграция, рост преступности, распространение

экстремизма, национализма и неспособность государства адекватно отвечать на вызовы современности.

Проблематика безопасности распространяется в различных сферах жизни общества: в социально-экономической (экономическая, продовольственная, энергетическая безопасность); в сфере повседневности (безопасность жизнедеятельности); в области отношений человека с окружающим миром (экологическая, космическая безопасность). В конечном счете, она начинает определять политическую повестку дня: все вопросы внутренней и внешней политики начинают рассматриваться через призму проблем безопасности.

Включение проблематики безопасности в новые сферы жизни общества – экологическую, экономическую, культурную, информационную – способствует легитимации чрезвычайных мер, предпринимаемых государством, что сказывается на ограничениях демократических процедур. В результате ценность безопасности начинает превалировать над всеми остальными политическими ценностями, детерминируя все сферы жизни.

В академической среде появилась потребность обосновать новые тенденции политических изменений в мире. Так, в последнее десятилетие стала актуальной концепция секьюритизации, предложенная Б. Бузаном, О. Уивером и Я. Де Вилдом [1], связанная с восприятием новых угроз безопасности обществом. Исследователями Копенгагенской школы международных отношений была предложена новая структура в исследовании безопасности, предполагающая раскрытие механизма актуализации данного феномена: каким образом некий объект начинает рассматриваться в качестве угрозы, как он привносится в политический дискурс и утверждается в качестве угрозы, т. е. секьюритизируется.

Процесс, в ходе которого объект представляется в качестве проблемы безопасности и начинает рассматриваться как угроза, американский политолог Барри Бузан называет секьюритизацией [2]. В качестве объекта может выступать государство, национальный суверенитет, экономика, экологическая сфера, идентичность, биологические виды. Объект становится вопросом безопасности после принятия решения о его важности по сравнению с другими. В этом случае объекту придается статус чрезвычайного приоритета, что выводит его из области обычной политики. Такой статус может быть определен акторами, утверждающими, что объект находится под угрозой его существованию. В качестве акторов могут быть как государственные институты, так и гражданские, не относящиеся к сфере политики.

Барри Бузан выделяет пять основных секторов, в которых вопросы безопасности являются наиболее значимыми: военный; политический; экологический; экономический; социетальный.

Секюритизация предполагает, что «тот или иной случай представлен как существенная угроза (existential threat) и требует срочных экстраординарных мер, оправдывая выход за рамки нормальных политических процедур» [3, p. 25]. Угроза понимается как социально сконструированный феномен, а сам процесс секьюритизации того или иного случая имеет дискурсивную природу. Вопросы безопасности в меньшей мере относятся к физической реальности или к объективному положению дел, а скорее относятся к восприятию того или иного феномена как угрозы.

Процесс секьюритизации проходит в два этапа. Первоначально актор заявляет о наличии угрозы, затем аудитория убеждается в ее существовании и легитимизирует нарушение норм. Секьюритизация предполагает приоритет экстремальной политики над установленными нормами и правилами решения аналогичных вопросов. Таким образом, речь идет об экстренных мерах, предпринимаемых для снижения угрозы безопасности.

В безопасности в равной степени заинтересованы и государство, и общество, и человек. Если в прежние времена безопасность сводилась лишь к безопасности государства, то во второй половине XX века она стала распространяться и на общество, и на личность. Причем в деятельности Организации Объединенных Наций наблюдается тенденция в сфере определения угроз безопасности и мер противодействия им: приоритетом становятся интересы личности и гражданского общества. Логика такого приоритета заключается в том, что на основе обеспечения личной безопасности и возможности для ее гармоничного развития естественным образом возникает безопасность на государственном уровне, а также на международном и глобальном уровнях. Таким образом, возникает единый многоуровневый комплекс, включающий уровень безопасности личности, общества и государства. Такая трактовка безопасности появилась в Декларации тысячелетия Организации Объединенных Наций, утвержденной Генеральной Ассамблеей ООН 8 сентября 2000 г. [4]

В XXI веке международное сообщество столкнулось с рядом новых, нетрадиционных угроз и вызовов безопасности, которые в сочетании с традиционными переводят их в новое качество. Как справедливо считают современные исследователи, «необходимо учитывать возможности комбинирования разных видов угроз и необходимость срочного реагирования на наиболее угрожающие из этих возможных сочетаний» [5, с. 68]. Причинами возникновения новых вызовов и угроз является повышение неопределенности в современном мире, кризис традиционных ценностей, изменение глобальной политической культуры.

Массовая информатизация общества также способствует возникновению новых угроз безопасности, которые распространяются как на частную жизнь, так и на социальную, политическую,

экономическую сферы. В сложившихся условиях высокую значимость приобретает деятельность государства в информационной сфере, которая включает в себя совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, связанных с формированием и обработкой информации, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений [6].

Значимость любого произошедшего события зависит, в первую очередь, от его интерпретации в средствах массовой информации. А если эта информация имеет политический подтекст, выгодный одним и не выгодный другим акторам мирового политического процесса, то возникает потребность в соответствующем объяснении событий. Поэтому информационная политика «как особая сфера жизнедеятельности людей, связанная с распространением информации в интересах государства и гражданского общества» [7, с. 103] занимает особое место в современном обществе.

Потребность в критическом осмыслении информационной политики связана с распространением гибридных войн, понимаемых в НАТО как тактики, при которой не используется открытое применение обычных военных средств и включающих в себя пропаганду и дезинформацию, методы экономического давления, а также тайное использование сил специального назначения [8]. Цели гибридной войны – полная или частичная дезинтеграция государства, качественное изменение его внутри- или внешнеполитического курса, замена государственного руководства на лояльные режимы, установление над страной внешнего идеологического и финансово-экономического контроля, ее хаотизация и подчинение диктату со стороны других государств или ТНК.

В условиях жесткого информационного противодействия использование различных информационных каналов на формирование альтернативной Западу точки зрения является не только оправданной, но и необходимой формой защиты национальных интересов России. Поэтому важным направлением внешнеполитической деятельности Российской Федерации в соответствии с новыми руководящими документами, принятыми в последние годы, является доведение до мировой общественности объективной информации о позиции России по основным международным проблемам, ее внешнеполитических инициативах и действиях, процессах и планах социально-экономического развития Российской Федерации, достижениях российской культуры и науки. В частности, об укреплении «позиций российских средств массовой информации и массовых коммуникаций в глобальном информационном пространстве» говорится в Концепции внешней политики Российской Федерации, утвержденной 30 ноября 2016 г. Указом Президента России [9].

Информационное воздействие в XXI веке приобретает еще большую значимость, так как его направленность влияет на поведение большого количества людей, у которых под влиянием той или иной информации могут возникать потребности как конструктивного, так и деструктивного характера, что существенным образом влияет на политическую ситуацию в стране и в мировом пространстве в целом. Недаром средства информационного воздействия называют информационным оружием, так как по своим разрушительным силам оно сопоставимо с обычными средствами вооружения, а иногда по своим последствиям превосходит их. В современном научном дискурсе под информационным оружием понимается «совокупность информации, а также специальных методов, устройств и средств манипуляции ею для скрытого воздействия на информационный ресурс противника с целью достижения поставленных целей и решения задач информационной борьбы (войны)» [10, с. 53].

В целях предотвращения угрозы такого воздействия Россия предпринимает необходимые меры для обеспечения национальной и международной информационной безопасности, противодействия угрозам государственной, экономической и общественной безопасности, исходящим из информационного пространства, для борьбы с терроризмом и иными угрозами с применением информационно-коммуникационных технологий, добивается выработки под эгидой ООН универсальных правил ответственного поведения государств в информационной сфере, в том числе посредством интернационализации на справедливой основе управления информационно-коммуникационной сетью «Интернет».

Одной из причин зависимости России от ведущих западных стран в информационной сфере, по мнению профессора Дипломатической академии И.В. Сурмы, стала ошибочная политика в области инвестиций в информационно-коммуникационные технологии, нацеленная на внешних поставщиков без стратегического анализа возможностей развития производства современных вычислительных средств и информационных технологий на базе уже имеющихся производственных мощностей [11, с. 89].

В Стратегии национальной безопасности Российской Федерации высказывается озабоченность тем, что «все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории» [12]. В Стратегии отмечается, что появляются новые формы противоправной деятельности с использованием информационных коммуникационных и высоких технологий. В целях осуществления государственной и общественной безопасности совершенствуется система выявления

и анализа угроз в информационной сфере, противодействия им; принимаются меры для повышения защищенности граждан и общества от деструктивного информационного воздействия со стороны экстремистских и террористических организаций, иностранных спецслужб и пропагандистских структур.

В подтверждение опасений, высказанных в Стратегии, 23 ноября 2016 г. депутаты Европарламента одобрили резолюцию о противодействии антиевропейской пропаганде, которую, по их мнению, ведут Россия и исламистские террористические группировки. Для пропаганды, указывается в резолюции, «российское правительство использует широкий диапазон инструментов, включая ТВ-каналы, вещающие на разных языках (в том числе Russia Today), псевдоновостные агентства и мультимедийные сервисы (в том числе Sputnik), а также соцсети и интернет-троллей» [13]. Евросоюзу, подчеркивается в документе, необходимо более активно принимать меры по борьбе с дезинформации и пропагандой, опасаясь ситуации, при которой, по мнению А. Анненкова, «побежденное государство как бы встраивается в общий алгоритм функционирования победителя и начинает обеспечивать его национальные интересы» [14, с. 126].

Важнейшей задачей государства в рамках информационного противоборства является контроль информационного пространства, интегрированного в глобальное информационное пространство и являющегося его частью; создание специальных сил, в функции которых входит ведение информационного противоборства; разработка средств информационного воздействия; принятие нормативно-правовых актов, обосновывающих и определяющих информационную политику страны.

Агрессивная информационная политика, проводимая западными странами против России, вынуждает российское политическое руководство принимать адекватные меры, и прежде всего в концептуальном плане. 5 декабря 2016 г. Президентом России была утверждена Доктрина информационной безопасности Российской Федерации, представляющая собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере на основе анализа основных информационных угроз и оценки состояния информационной безопасности [6].

Таким образом, в условиях информационного противоборства государств, связанного с формированием нового мирового порядка, Россия добивается объективного восприятия ее в мире, развивает собственные эффективные средства информационного влияния на общественное мнение за рубежом, содействует усилению позиций российских и русскоязычных средств массовой информации в мировом информационном пространстве, предоставляя им необходимую для этого государственную поддержку, активно участвует в международном сотрудничестве в информационной сфере, принимает меры по противодействию угрозам своей информационной безопасности.

Большинство нормативно-правовых актов, принятых в последние годы в Российской Федерации, акцентируют внимание на предотвращении угроз и вызовов государству в информационной сфере, не акцентируя внимание на интересах гражданского общества. Информационную политику справедливо подразделяют на государственную и негосударственную. Если одной из основных задач государственной информационной политики является поддержание политической и социальной стабильности в стране, то негосударственная информационная политика может не совпадать с интересами государства, так как всегда существует часть общества, не разделяющая властные инициативы и требующая либерализации политического и информационного пространства.

Задача государства состоит в том, чтобы не только удовлетворить интересы большинства населения в информационной сфере, но и предоставить оппозиции возможность воспользоваться дополнительными информационными ресурсами, которые могут быть не востребованы остальными. Сужение информационного поля, как правило, осуществляется за счет ограничения деятельности тех средств информации, которые критично относятся к политическому курсу страны. В сложившихся условиях у государства возникает соблазн настроить против оппозиционеров большую часть населения, таким образом, объявив об опасности их деятельности для государства. Возникает повод для секьюритизации политики, направленной против «пятой колонны», «врагов государства» и т.д. Сужение сферы влияния негосударственной информационной политики способствует развитию авторитарных тенденций в стране. Следует согласиться с мнением А.А. Ковалева, полагающего результатом информационной политики – «синтез интересов государственного аппарата и гражданского общества, являющийся залогом всеобъемлющей безопасности страны» [15, с. 99].

В условиях тотального проникновения информационных технологий во все сферы жизни общества возникает потребность в создании соответствующей инфраструктуры в целях формирования общества знаний, в котором преобладающее значение для развития гражданина, экономики и государства имеют получение, сохранение, производство и распространение достоверной информации с учетом стратегических национальных приоритетов Российской Федерации. Такая цель перед государством поставлена в Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы, утвержденной Указом Президента России от 9 мая 2017 г., в которой определены задачи и меры по реализации внутренней и внешней политики страны «в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов» [16].

Технологии передачи информации с использованием сети «Интернет» все чаще используются для манипулирования общественным мнением. Происходит смещение акцентов в восприятии окружающего мира с научного, образовательного и культурного на развлекательно-справочный, что формирует новую модель восприятия - так называемое клиповое мышление, характерной особенностью которого является массовое поверхностное восприятие информации. Такая форма освоения информации упрощает влияние на взгляды и предпочтения людей, способствует формированию навязанных моделей поведения, что дает преимущество в достижении экономических и политических целей тем государствам и организациям, которым принадлежат технологии распространения информации.

В сложившихся условиях национальными интересами страны становятся развитие человеческого потенциала, обеспечение безопасности граждан и государства, повышение роли России в мировом гуманитарном и культурном пространстве, развитие свободного, устойчивого и безопасного взаимодействия граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления, повышение эффективности государственного управления, развитие экономики и социальной сферы, формирование цифровой экономики.

Заключение. Таким образом, в Российской Федерации произошла секьюритизация информационной сферы. В качестве акторов выступили как государство, так и часть гражданского общества, в основном патриотично настроенное, признавшее высокую значимость информационных технологий и их способность оказывать влияние на все стороны жизнедеятельности общества. Необходимость защиты от проникновения в частную сферу, служебную переписку, деятельность государственных и муниципальных учреждений было признано гражданами, обществом и государством, что привело к легитимации угрозы в информационной сфере. Поэтому принятые меры в виде вышеперечисленных государственных нормативно-правовых документов создали условия для экстремальной политики, логически завершив процесс секьюритизации.

Экспансия проблематики безопасности предполагает повышенный интерес экспертного сообщества к вопросам ограничения прав и свобод человека, демократических институтов и процедур. Следует согласиться с мнением А.А. Казанцева относительно актуальности результатов усиления административных рычагов воздействия на общество для России, как для страны, не имеющей старых демократических традиций, в связи с чем «экспансия проблематики безопасности может стать особенно опасной для демократических институтов» [5, с. 17]. Осуществлять контроль за государственными институтами в условиях процесса секьюритизации может только гражданское общество, акцентирующее внимание на опасности вторжения государства и общества в частную жизнь человека, ограничении его прав и свобод, всевластии органов безопасности. Убедительная гражданская экспертиза, свидетельствующая об опасности для общества тотального контроля со стороны государственных структур, может стать действенным механизмом на пути расширения секьюритизации в политической практике. Поэтому современные формы демократии, апеллирующие к мнению народа - делиберативная, согласительная, мониторинговая, представляются перспективными в вопросах ограничения запретительных мер в ответ на возможные угрозы.

Безопасность для человека всегда будет находиться на приоритетном месте. Этим пользуются в своих интересах государственные институты, расширяя контроль за деятельностью общества и конкретных индивидов. Поиск баланса между полномочиями специализированных органов по обеспечению безопасности личности, общества и государства и недопустимостью их вторжения в приватную сферу является актуальным для современных стран. В данном контексте актуально высказывание американского политического деятеля, одного из отцов-основателей США Бенджамина Франклина, который в 1755 году предупреждал об опасности отказа от свободы в обмен на безопасность: «Те, кто готовы пожертвовать насущной свободой ради малой толики временной безопасности, не достойны ни свободы, ни безопасности» [17]. Эти слова великого американца необходимо всегда вспоминать, когда безопасность становится приоритетом по сравнению с остальными ценностями.

СПИСОК ЛИТЕРАТУРЫ

1. Buzan B., Wæver O., de Wilde J. Security: A New Framework for Analysis. L.: Lynne Rienner Publishers, 1998. 239 p.
2. Агапеева К. Теория секьюритизации Барри Бузана // Информационно-аналитический портал «Геополитика». URL: https://www.geopolitica.ru/article/teoriya-sekyuritizacii-barri-buzana (дата обращения: 11.06.2017).
3. Buzan B., Waever O., Wilde J. de, Security: A New Framework for Analysis Boulder: Lynne Rienner Publishers, 1998. P.25.
4. Декларация тысячелетия Организации Объединенных Наций. URL: http://www.un.org/ru/documents/decl_conv/declarations/summitdecl.shtml (дата обращения: 12.06.2017).
5. Казанцев А.А. Расширение проблематики безопасности в политике России: секьюритизация, биополитика и новые административные практики. М.: Проспект, 2010. 200 с.
6. Доктрина информационной безопасности Российской Федерации. URL: http://kremlin.ru/acts/bank/41460 (дата обращения: 12.06.2017).
7. Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны. М.: Горячая линия – Телеком, 2012. 542 с.
8. НАТО приняла стратегию против гибридных войн. 2 декабря 2015 г. URL: https://newsland.com/user/4296735949/content/nato-priniala-strategiiu-protiv-quotgibridnykh-voinquot/4854888 (дата обращения: 11.06.2017).

9. Указ Президента Российской Федерации от 30 ноября 2016 г. №640 «Об утверждении Концепции внешней политики Российской Федерации». URL: http://www.kremlin.ru/acts/bank/41451/page/1 (дата обращения: 11.06.2017).
10. Новиков В.К. Информационное оружие – оружие современных и будущих войн. М.: Горячая линия-Телеком, 2011. 264 с.
11. Сурма И.В. Возможности и приоритеты4 России в мировом информационном пространстве // Россия и современный мир / Отв. ред. М.А. Неймарк. М.: «Канон+» РООИ «Реабилитация», 2016. С.71-94.
12. Стратегия национальной безопасности Российской Федерации // Официальный сайт Президента России. URL: http://kremlin.ru/acts/bank/40391 (дата обращения: 11.06.2017).
13. Европарламент принял резолюцию против российской пропаганды // Информационный портал Meduza. URL: https://meduza.io/news/2016/11/23/evroparlament-prinyal-rezolyutsiyu-o-protivodeystvii-rossiyskoy-propagande (дата обращения: 11.06.2017).
14. Анненков В. Информационно-психологическое противоборство: современные аспекты // Современный мир и геополитика / Отв. ред. М.А. Неймарк. М.: Издательство «Канон+» РООИ «Реабилитация», 2015. С.116-126.
15. Ковалев А.А. Информационная политика и военная безопасность России в эпоху противостояния цивилизаций: теоретико-методологические аспекты проблемы. СПб.: ИП Коновалов А.М., 2016. 194 с.
16. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы. URL: http://www.kremlin.ru/acts/bank/41919 (дата обращения: 11.06.2017).
17. Votes and Proceedings of the House of Representatives, 1755-1756 (Philadelphia, 1756). P.19-21.

УДК 004.67

РЕЗУЛЬТАТИВНОСТЬ ИНСТРУМЕНТОВ ЭЛЕКТРОННОГО УЧАСТИЯ В РОССИИ ПРИ ФОРМИРОВАНИИ ПОЛИТИЧЕСКИХ РЕШЕНИЙ

Видясова Людмила Александровна, Тенсина Ярослава Дмитриевна
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики
Санкт-Петербург, 199034, Биржевая линия В.О., 14
emails: bershadskaya.lyudmila@gmail.com, tensina.yaroslava@mail.ru

Аннотация: В статье анализируется результативность работы порталов электронного участия в России и оценивается их влияние на формирование политики. Для проведения сравнительного исследования методом кейс-стади были выбраны два портала петиций: Российская общественная инициатива и Change.org (русскоязычный сегмент). Для сбора и обработки данных использовалась система мониторинга порталов электронного участия, разработанная в Университет ИТМО. В результате исследования были получены выводы о необходимости учета как количественных, так и качественных параметров результативности порталов для получения достоверной оценки степени влияния работы инструментов электронного участия на принятие политических решений.

Ключевые слова: *электронное участие; управление; портал петиций; критерии эффективности*

EFFECTIVENESS OF E-PARTICIPATION TOOLS IN RUSSIA IN POLICY-MAKING

Vidiasova Lyudmila, Tensina Iaroslava
ITMO University,
Russia, St. Petersburg, 199034, V.O., Birzhevaya line, 14
emails: bershadskaya.lyudmila@gmail.com, tensina.yaroslava@mail.ru

Abstract: The article analyzes the effectiveness of e-participation portals in Russia and assesses their impact policy-making. To carry out the comparative case-study, two portals of petitions were chosen: Russian Public Initiative and Change.org (Russian-speaking segment). To collect and process data, a monitoring system for e-participation portals was developed at the ITMO University. As a result of the research, conclusions were received on the need to take into account both quantitative and qualitative parameters of portals' effectiveness in order to obtain a reliable estimate of e-participation tools on political decision-making.

Keywords*: e-participation; governance; e-petition portal; efficiency criteria*

Введение. В настоящее время в России появляется все больше новых механизмов электронного участия, которые включают в себя различные инструменты, методы и технологии взаимодействия власти и общества. Наибольшую популярность получили порталы электронных петиций, однако оценить результативность таких площадок и их возможность влиять на принятие политических решений является достаточно сложной задачей. В научной литературе имеются примеры исследований технологий электронного участия, но в то же время вопрос об оптимальных критериях оценки их результативности остается нерешенным. В нашем исследовании была предпринята попытка оценить результативность инструментов электронного участия в России и определить, приводит ли действие порталов электронных петиций в России к реальным изменениям в политике. На примере порталов электронных петиций «Российская общественная инициатива» и «Change.org» была проанализирована результативность сбора голосов за петиции и ход их дальнейшего рассмотрения.

В рамках исследования был проведен анализ методик оценки инструментов электронного участия. Р. Медаглиа при оценке сделал акцент на комплекс таких параметров, как действия, акторы, эффекты и контекстуальные факторы [1]. Другие исследователи подчеркивают большую роль

измерения влияния институциональных факторов [2]. Некоторые исследователи акцентируют внимание на влиянии форм правления [3] на развитие инструментов электронного участия. Существует также подход, основанный на подсчете параметров веб-присутствия: разнообразие мультимедиа, синхронные и асинхронные каналы связи и т.д. [4]. Макинтош и Уайт предложили систему оценки [5], состоящую из критериев демократичности (презентация, взаимодействие, прозрачность, поиск консенсуса, политическое равенство, общественный контроль), проектных параметров (привлечение более широкой аудитории, получение лучшего информированного мнения, экономическая эффективность, предоставление обратной связи гражданам) и социально-технических индикаторов (использование, польза, удобство). В нашем исследовании мы постарались обратиться к международной практике и национальному контексту и провести анализ порталов на основе комбинации факторов и критериев.

В качестве одного из объектов исследования был выбран портал «Российская общественная инициатива», созданный по инициативе Президента России. Портал появился в апреле 2013 года и получил такое название, поскольку он должен собирать инициативы граждан на федеральном, региональном и муниципальном уровнях. Основной целью создания «РОИ» являлось развитие и укрепление гражданского общества, защиты прав человека и гражданина, а также участия граждан в управлении делами государства. Чтобы проголосовать на портале необходимо быть гражданином России старше 18 лет, быть зарегистрированным на Едином портале государственных и муниципальных услуг и иметь сформулированную инициативу для того, чтобы предложить её власти. Сбор голосов в поддержку инициативы осуществляется в срок не более 1 года со дня размещения инициативы.

В качество второго объекта исследования был выбран международный портал «Change.org», который был создан в 2007 году и позиционируется как онлайн-платформа для размещения петиций. Данный портал предоставляет гражданам инструменты для продвижения гражданских инициатив и решения социальных проблем. Для того, чтобы оставить петицию на портале, достаточно авторизоваться через Facebook или пройти простую процедуру регистрации, после чего можно приступить к подробному описанию проблемы.

В ходе исследования была использована методология кейс-стади, в рамках которой были проанализированы количественные и качественные данные о работе порталов. Для количественного анализа данных была использована автоматизированная система мониторинга порталов электронного участия, разработанная в Университете ИТМО. Анализ был проведен по следующим параметрам:

— количество поданных инициатив;
— распространение инициатив по категориям;
— доля успешных инициатив.

Анализ количественных данных позволил нам рассмотреть масштаб публикации инициатив на каждом портале, распределение внимания граждан к различным сферам жизни, а также динамику сбора голосов в поддержку или против инициатив. Качественный анализ данных был проведен вручную при использовании данных о петициях, находящихся в открытом доступе на порталах «РОИ» и «Change.org». Анализ данных портала «РОИ» был осуществлен за период 2013-2017 гг., а для анализа портала «Change.org» были использованы данные за 2012-2017 гг.

За исследуемый система мониторинга собрала 9807 инициатив, опубликованных на портале «РОИ». Инициативы размещены по уровням в следующей пропорции: 86,4% относятся к федеральному уровню, 7,7% - региональному и 5,9% - муниципальному уровню. В ходе исследования был обнаружен высокий уровень заинтересованности граждан в самом начале работы портала, однако уже спустя пару месяцев интерес общественности к порталу значительно снизился. На рис. 1 продемонстрирована динамика распределения опубликованных петиций по годам.

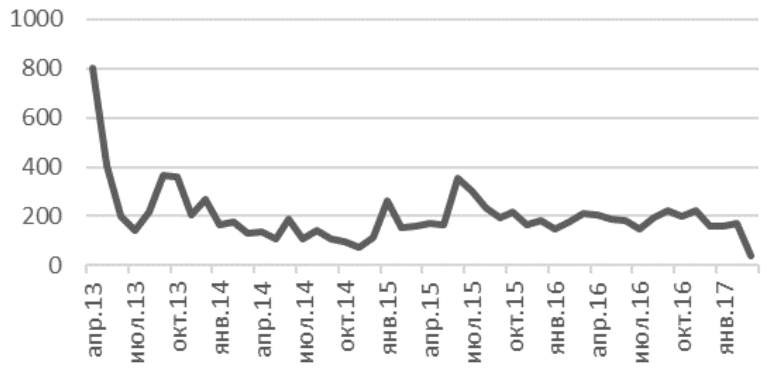


Рис.1. Динамика количества размещенных инициатив на портале «РОИ», 2013-2017 гг.

На портале «Change.org» на момент проведения исследования было опубликовано 139861 петиций. На рис. 2 можно наглядно проследить рост интереса граждан к порталу, начиная с 2015 года, однако в марте 2017 года количество публикуемых петиций все же значительно снизилось.

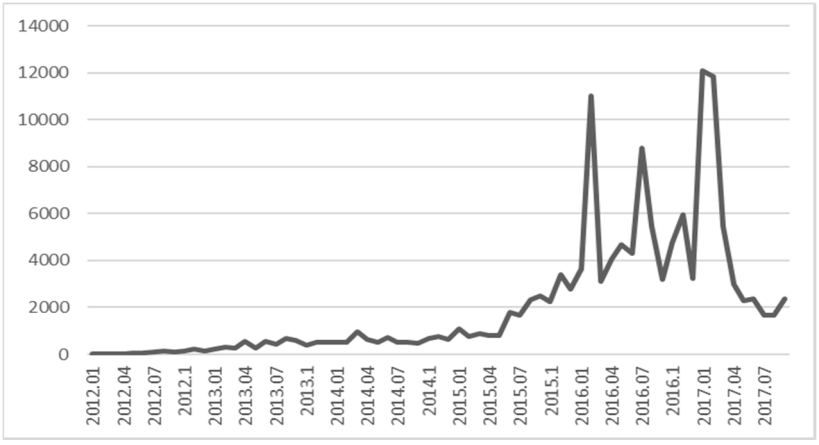


Рис. 2. Динамика количества размещенных инициатив на портале «Change.org», 2012-2017 гг.

Кроме того, стоит отметить, что с 2012 по 2016 год наблюдалась тенденция к росту количества петиций, по которым удалось добиться решения заявленных проблем. Однако, уже с ноября 2016 года количество успешных петиций заметно снизилось, что наглядно представлена на рис. 3.

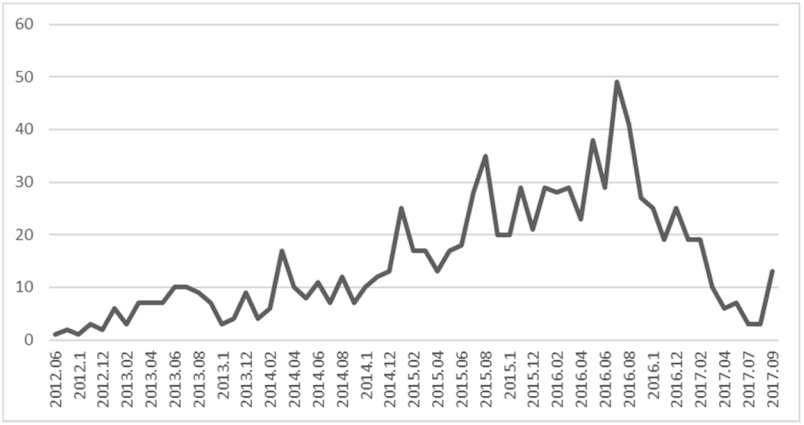


Рис.3. Динамика количества петиций со статусом «Победа», размещенных на портале «Change.org», 2012-2017 гг.

О снижении интереса граждан к порталу «Change.org» также свидетельствует отрицательная динамика количества голосов, которые граждане оставляют в поддержку петиций. На рис. 4 представлена динамика распределения голосов, что позволяет сделать вывод, о значительном снижении активности пользователей портала, начиная с мая 2017 года.

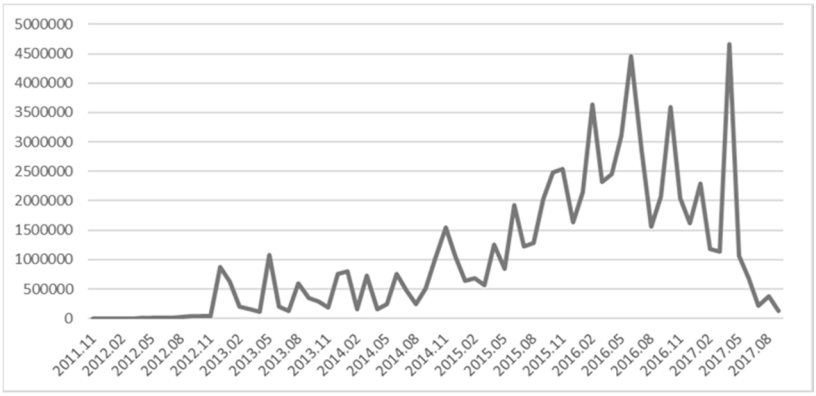


Рис.4. Динамика количества голосов, поданных за петиции на портале «Change.org», 2012-2017 гг.

Возможности автоматизированной системы мониторинга порталов электронного участия позволили нам проанализировать распределение голосов на портале «РОИ», которые были оставлены в поддержку или против опубликованных инициатив. На рис. 5 отображена динамика голосов граждан, которые были оставлены «за» и «против». Исследование выявило преобладание голосов в поддержку инициатив. Это означает, с одной стороны, определенную степень солидарности пользователей, а с

другой – определенную целесообразность публикуемых предложений. На графике отражены данные только с 2014 г., так как возможность оставлять голос против была введена на портале только в 2014 г. Стоит отметить, что голоса «против» не вычитаются из голосов «за», учитываются при принятии решений экспертными группами, созданными при органах государственной власти.

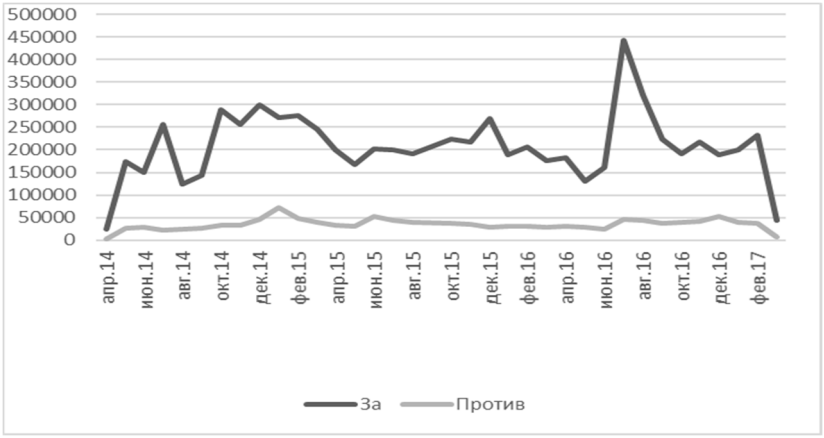


Рис.5. Распределение голос «за» и «против» на портале «РОИ», 2014-2017 гг.

Несмотря на то, что граждане больше склонны поддерживать публикуемые инициативы, на сегодняшний день среди 9799 инициатив, размещенных на портале «РОИ», только 23 инициативы набрали более 50% от необходимого количества голосов. Все инициативы были размещены на федеральном уровне. Таким образом, в среднем лишь 0,16% инициатив набирают более 50% голосов по тем категориям, которые лидируют по количеству размещенных инициатив. После запуска портала среди 9799 инициатив, размещенных на портале, решение было принято только по 25 инициативам (0,26%). Следует отметить, что 88% успешных инициатив принадлежало федеральному уровню, а остальные 12% - муниципальному уровню.

На платформе «Change.org» процент решенных проблем остается также весьма незначительным, так как положительное решение на текущий момент принято по 910 инициативам, что составляет 0,7% от числа всех инициатив на портале. Анализ успешных инициатив позволяет судить о том, что большинство решенных проблем не оказывают влияние как на формирование повестки дня, так и на принятие важных политических решений.

Выводы. Таким образом, проведенное исследование позволяет судить о целесообразности использования количественных и качественных параметров оценки порталов электронного участия. Выявленные количественные параметры работы порталов позволили нам определить снижение интереса и активности пользователей к публикациям петиций, независимо от того, был ли создан портал по инициативе органов власти, или по инициативе активистов. Кроме того, был выявлен низкий процент петиций, которым удалось повлиять на решение заявленной проблемы. Среди всех опубликованных петиций на портале «Change.org» и «РОИ» лишь менее 1% петиций смогли достичь поставленных целей. Можно предположить, что именно низкий процент решенных проблем ослабевает веру граждан в результативность петиций и снижает мотивацию к использованию порталов. Учитывая тенденцию к снижению активности пользователей порталов, а также малое количество петиций, по которым удалось решить волнующие граждан проблемы, можно судить о низкой результативности порталов электронных петиций в России и невысоком влиянии на формирование политических решений.

Работа выполнена в рамках проекта «Исследование социальной эффективности порталов электронного участия в России» при поддержке Российского фонда фундаментальных исследований (грант РФФИ 16-36-60035).

СПИСОК ЛИТЕРАТУРЫ

1. Medaglia R. eParticipation research: Moving characterization forward (2006-2011) // Government Information Quarterly. 2012. Vol. 29. P.346-360.
2. Jho W., Song K. Institutional and technological determinants of civil e-Participation: Solo or duet? // Government Information Quarterly. 2015. Vol. 32, P.488-495.
3. Zheng Y., Schachter H.L., Holzer M. The impact of government from e-participation: A study of New Jersey municipalities // Government Information Quarterly. 2014. Vol. 31. P. 653-659.
4. Ter'an L., Drobnjak A. An Evaluation Framework for eParticipation: The VAAs Case Study // International Scholary and Scientific Research and Innovation. 2013. Vol. 7(1). P. 77-85.
5. Macintosh A., Whyte A. Towards an evaluation framework for e-Participation// Transforming government: People, Process & Policy. 2008. Vol. 2 (1). P. 16-30.

УДК 35.078.42

ГОСУДАРСТВЕННАЯ ПОЛИТИКА В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕВЕРО-ЗАПАДНОМ ФЕДЕРАЛЬНОМ ОКРУГЕ

Кучерявый Михаил Михайлович, Вовенда Юлия Владимировна
Доктор политических наук, доцент,
Администрация Ленинградской области
Россия, Санкт-Петербург, Суворовский пр., д. 67
email: apparat@lenreg.ru, vovenda-yv@sziu.ru

Аннотация: В статье рассматривается деятельность органов государственной власти Северо-Западного федерального округа по обеспечению безопасности информации. Освещаются вопросы формирования и функционирования системы защиты информации в Северо-Западном федеральном округе. Особое внимание уделено государственным информационным системам, процессам регулирования и контроля обеспечения безопасности информации Управлением ФСТЭК по СЗФО.

Ключевые слова: Органы государственной власти, обеспечение информации, система защиты информации, государственные информационные системы, техническая защита информации.

STATE POLICY IN THE FIELD OF ENSURING INFORMATION SECURITY IN THE NORTH-WEST FEDERAL DISTRICT

Kucheryavyi Mikhail, Vovenda Julia
Doctor of political science, assistant professor,
Administration of the Leningrad Region
Russia, St. Petersburg, Suvorovsky pr., 67
email: apparat@lenreg.ru, vovenda-yv@sziu.ru

Abstract: The article is considered the activities of public authorities of the North-West Federal District to ensure information security. Highlightsthe issues of formation and functioning of the information security system in the North-West Federal District.The main attention is paid to the state information systems, control and monitoring of security information by the FSTEC Office for the North-West Federal District.

Keywords: *Public authorities, providing information, information security system, state information systems, technical protection of information.*

Сегодняшний мир, в котором мы живем – это мир, который характеризуется глобальным развитием, усовершенствованием информационно-коммуникационных технологий и сложившаяся к настоящему времени новая политическая реальность характеризуется трансформацией разрозненных и суверенных информационных систем в единое глобальное пространство.

Надёжная работа информационных ресурсов, систем управления и связи имеет исключительное значение для обороноспособности страны, для устойчивого развития экономики и социальной сферы, для защиты суверенитета России.

Доктриной информационной безопасности Российской Федерации [1] предусматривается повышение эффективности функционирования системы государственного управления, обеспечение информационного взаимодействия между органами власти при решении задач в области обороны и безопасности.

Определяя в качестве приоритетов построение в Российской Федерации информационного общества, государственная политика нацелена на усиление внимания к защите государственных информационных ресурсов.

Существующие современные угрозы в информационной сфере направлены, в первую очередь, против действующих органов государственной власти и управления всех регионов Российской Федерации.

В Северо-Западном федеральном округе проживает около четырнадцати миллионов человек. В состав округа входит одиннадцать субъектов Российской Федерации, более трех тысяч органов государственной власти субъектов Российской Федерации и около полутора тысяч органов местного самоуправления.

В государственных и муниципальных информационных системах органов власти субъектов Российской Федерации обрабатываются значительные массивы информации ограниченного доступа.

Зарегистрированных государственных информационных систем в округе около четырехсот, муниципальных более пятисот. В более чем четырех с половиной тысячах информационных систем персональных данных обрабатывается информация о населении округа. Такие данные очень привлекательны для технических разведок иностранных государств.

Большая часть объектов защиты, находящихся в пределах округа, доступны для средств космической, морской, наземной и воздушной разведок. Возможности разведок позволяют:

– непрерывно контролировать каналы сотовой связи;
– осуществлять перехват интернет трафика;

– осуществлять мониторинг органов государственного управления, военных объектов и объектов оборонно-промышленного комплекса.

При этом официально, в соответствии с «Договором по открытому небу» [2], осуществляется детальная фотосъемка объектов по маршруту полета.

Так же легально, в рамках международных научно-исследовательских программ, ведется разведка с использованием иностранных технических средств наблюдения и контроля, которые позволяют получать сведения об экономическом и военном потенциалах Северо-Западного региона. Такие средства размещены в Республике Коми, Мурманской и Ленинградской областях, в Санкт-Петербурге.

Технические средства более двадцати стран НАТО объединены в систему глобального контроля международных линий связи «Эшелон» [5,с. 165]. Часть пунктов сбора и обработки информации стран-участниц размещены вдоль внешней границы Северо-Западного федерального округа. Средствами системы «Эшелон» перехватывается и анализируется информация, передаваемая по линиям связи, а также с международных и национальных спутниковых систем. Возможности этой системы позволяют анализировать десятки миллионов сообщений в минуту.

Наибольшую угрозу для государственных информационных систем Северо-Западного федерального округа представляет техническая компьютерная разведка, реализованная в системе электронного наблюдения PRISM, созданной Агентством национальной безопасности США для сбора информации с крупнейших интернет-сервисов, включая электронную почту, поисковые запросы, разговоры в Skype, мобильные приложения, транзакции в системах Visa иMasterCard [6, с. 160].

Для обеспечения своевременной и адекватной реакции на возникающие и прогнозируемые угрозы утечки информации ограниченного доступа в округе сформирована и функционирует система защиты информации, которая охватывает все уровни и ветви органов власти Северо-Западного федерального округа.

Общее руководство деятельностью по защите информации в округе осуществляют полномочный представитель Президента Российской Федерации и Межведомственный совет по защите информации.

В субъектах Российской Федерации – главы высших органов исполнительных власти субъектов Российской Федерации и комиссии по защите информации. В органах власти и организациях ответственность за обеспечение защиты информации возлагается на их руководителей.

Управление ФСТЭК России по Северо-Западному федеральному округу осуществляет координацию деятельности по защите информации в пределах федерального округа, организует функционирование сформированной системы защиты информации.

Управление ФСТЭК России по Северо-Западному федеральному округу осуществляет реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

– обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, в том числе в функционирующих в составе критически важных объектов Российской Федерации информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям;

– противодействия иностранным техническим разведкам на территории Российской Федерации;

– обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носителей информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;

– защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

– осуществления экспортного контроля [3].

Управлением ФСТЭК России по Северо-Западному федеральному округу был рекомендован порядок действий для руководителей органов государственной власти, предприятий по обеспечению безопасности информации. Это, прежде всего:

– оценка угроз информационной безопасности;

– проведение организационно-технических мероприятий по их предотвращению;

– подготовка кадров в области информационной безопасности;

– обеспечение безопасности информации в ключевых системах информационной инфраструктуры;

– защита информации в государственных и муниципальных информационных системах;

– анализ и контроль.

Итоги контроля органов государственной власти Северо-Западного федерального округа показали, что не везде в полной мере выполняются рекомендации нормативных и методических документов ФСТЭК России, что приводит к серьезным нарушениям безопасности информации и к возможной вероятности раскрытия сведений, составляющих государственную тайну.

Характерными нарушениями, которые можно классифицировать как типовые, для всех проверенных органов власти являются следующие:

– недостаточное руководство системой информационной безопасности в регионах уполномоченными должностными лицами;

– назначение специалистов, не имеющих профильного высшего образования и не прошедших переподготовку и повышение квалификации;

– недостаточное финансирование для приобретения лицензионного и сертифицированного информационно-коммуникационного оборудования;

– назначение на должности специалистов по защите информации без соответствующего согласования с Управлением ФСТЭК России по Северо-Западному федеральному округу.

Сравнительная оценка результатов контроля свидетельствует об увеличении в три раза общего количества нарушений в области технической защиты информации.

В пять раз увеличилось число нарушений в общей организации работ, что говорит об ослаблении контроля со стороны руководства регионов, организаций и учреждений.

Не принимаются меры по устранению нарушений и недостатков, которые выявлялись в ходе предыдущих проверок.

Наибольшее количество нарушений связано с низкой организацией работ и недостаточной профессиональной подготовкой специалистов.

Система органов государственной власти и управления в Северо-Западном федеральном округе является центральным звеном обеспечения информационного противоборства в регионе.

Важное значение имеет обеспечение защиты информации в государственных информационных системах.

В информационных системах органов власти циркулирует информация, имеющая значение для деятельности государства и региона, в том числе в социальной сфере, здравоохранении и образовании, преждевременное раскрытие которой может привести к нежелательному, негативному общественному резонансу.

Безопасность информации в государственных информационных системах достигается путем проведения большого комплекса работ, в том числе по аттестованию ГИС и созданию систем по технической защите информации.

В органах власти субъектов Российской Федерации, по представленным данным, функционируют более шестнадцати тысяч информационных систем. При этом из восьми тысяч информационных систем, функционирующих в органах государственной власти, зарегистрировано порядка четырехсот государственных информационных систем, что составляет 6,5% от их общего количества.

В органах местного самоуправления из восьми с половиной тысяч информационных систем зарегистрировано около пятисот муниципальных информационных систем, что составляет 6%.

Работа по определению статуса информационных систем в органах власти находится на начальном этапе, в то время как решениями Межведомственного совета по защите информации в Северо-Западном федеральном округе руководителям органов власти рекомендовалось выполнить данные работы в 2014 году. При этом, необходимая правовая база, определяющая порядок и содержание работ по защите информации в государственных информационных системах, уже сформирована.

На сегодняшний день из зарегистрированных в округе государственных информационных систем, аттестовано по требованиям безопасности информации только двадцать пять, что составляет 7% от общего числа зарегистрированных систем.

Такая же ситуация складывается и с аттестацией информационных систем органов местного самоуправления, где аттестованных информационных систем около 3%.

Фактическое состояние работ по защите информации в государственных информационных системах органов государственной власти и органов местного самоуправления оценивается в ходе контроля, проводимого Управлением ФСТЭК России по СЗФО.

За последнее время проверены на соответствие требованиям законодательства Российской Федерации, нормативных и методических документов ФСТЭК России информационные системы органов государственной власти Санкт-Петербурга, Мурманской и Архангельской областей.

Результаты контроля показали, что основные организационные и технические требования приказа ФСТЭК России от 11 февраля 2013 г. № 17 [4] в полном объеме выполнены только в проверенных государственных информационных системах Санкт-Петербурга.

В информационных системах Архангельской и Мурманской областей требования к защите информации не выполняются или выполняются частично.

Уровень защищенности информационных систем в органах государственной власти не в полной мере соответствует существующим угрозам и масштабам информатизации.

Темпы совершенствования региональных систем защиты информации отстают от возрастания и усложнения требований в области информационной безопасности.

Без усиления внимания руководства к подбору, подготовке специалистов и необходимому финансированию работ, эффективность по обеспечению безопасности информации будет недостаточной.

СПИСОК ЛИТЕРАТУРЫ**:**

1 Доктрина информационной безопасности Российской Федерации. Новая редакция. [Электронный ресурс]. URL: http://infosystems.ru/assets/files/files/doktrina_IB.pdf

2 Договор по открытому небу. [Электронный ресурс] // Организация по безопасности сотрудничеству в Европе. URL: http://www.osce.org/ru/library/14131

3 Сведения о полномочиях ФСТЭК России; перечень нормативных правовых актов, определяющих эти полномочия. [Электронный ресурс] // ФСТЭК России. URL: http://fstec.ru/obshchaya-informatsiya/polnomochiya

4 Приказ Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электронный ресурс] // ФСТЭК России. URL: http://fstec.ru/normativnye-pravovye-akty-tzi/110-deyatelnost/tekushchaya/tekhnicheskaya-zashchita-informatsii/normativnye-pravovye-akty/prikazy/703-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17

5 Кучерявый М. М. Основные факторы влияния политики информационной безопасности на национальную безопасность современной России // Евразийская интеграция: экономика, право, политика.– Санкт-Петербург. 2013. № 14. С. 164-168.

6 Кучерявый М. М. Роль информационной составляющей в системе политики обеспечения национальной безопасности Российской Федерации // Известия Российского государственного педагогического университета им. А.И. Герцена. 2014. №164. С. 155-163.

7 Косов Ю.В. Кучерявый М.М. Статус России в мировом сообществе и обеспечение глобальной безопасности // Грядущий мировой порядок в оценках российских и американский экспертов: матер. XXII Ежегодного Российско-американского семинара в Санкт-Петербургском государственном университете, 15-21 мая 2013 года. СПб.: СПбГУ, 2013. С. 131-137.

УДК 332:331

ОБЕСПЕЧЕНИЕ КАДРОВОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ ВЫСОКОТЕХНОЛОГИЧНЫХ ОТРАСЛЕЙ

Советов Борис Яковлевич[1], Касаткин Виктор Викторович[2]
[1]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия, д. 39,
emails: bysovetov@mail.ru, v.v.kasatkin@iias.spb.su

Аннотация**:** Осуществление задач цифровой трансформации государственного управления и экономики страны, реализация приоритетных государственных программ требуют кардинальных изменений в проводимой государством политики в сфере высшего образования. В условиях санкций вектор направленности российского образования в значительной степени должен сместиться в сторону интересов промышленности, что будет способствовать предотвращению оттока кадров на запад и позволит обеспечить отечественную промышленность высококвалифицированными кадрами. Для этого необходимо устранить негативные факторы, которые проявились в процессе реформирования российского высшего образования и превращения его в многоуровневое образование западного образца, реализовать обсуждаемые в статье предложения, направленные на повышение качества подготовки кадров, сохранение и развитие кадрового потенциала промышленных предприятий, формирование кадрового резерва, обеспечение кадровой безопасности предприятий высокотехнологичных отраслей промышленности, в том числе за счет насыщения рынка труда ИТ-специалистами, подготовленными в рамках направления «Информационные системы и технологии».

Ключевые слова*: кадровая безопасность, высокотехнологичные отрасли промышленности, кадровый резерв, импортозамещение.*

ENSURING PERSONNEL SAFETY OF THE INDUSTRIAL ENTERPRISES OF HIGH-TECH INDUSTRIES

Boris Sovetov[1], Victor Kasatkin[2]
[1] The St. Petersburg State Electrotechnical University «LETI»,
Russia, St. Petersburg, Professor Popov str., 5,
[2] St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
Russia, St. Petersburg, 14 Line, 39,
emails: bysovetov@mail.ru, v.v.kasatkin@iias.spb.su,

Abstract: Implementation of problems of digital transformation of public administration and national economy, implementation of priority state programs demand cardinal changes in the policy pursued by the state in the sphere of the higher education. In the conditions of sanctions, the vector of orientation of Russian education substantially has to be displaced towards the interests of the industry that will promote prevention

of outflow of shots to the west and will allow to provide the domestic industry by highly qualified personnel. For this purpose it is necessary to eliminate negative factors which were shown in the course of reforming of the Russian higher education and his transformation into multilevel formation of the western sample, to realize the offers discussed in article directed to improvement of quality of training, preservation and development of personnel capacity of the industrial enterprises, formation of a personnel pool, ensuring personnel safety of the enterprises of high-tech industries of the industry including due to labor market saturation by the IT specialists trained within the "Information Systems and Technologies" direction.

***Keywords**: personnel safety, high-tech industries of the industry, personnel pool, import substitution.*

Осуществление масштабных планов цифровой трансформации государственного управления и экономики страны, поставленных Президентом Российской Федерации, реализация программы «Цифровая экономика Российской Федерации» и приоритетных проектов «Вузы как центры создания пространства инноваций», «Современная цифровая образовательная среда в Российской Федерации» требуют кардинальных изменений в проводимой государством политики в сфере высшего образования. В условиях санкций вектор направленности российского образования в значительной степени должен сместиться в сторону интересов промышленности, что будет способствовать предотвращению оттока кадров на запад и позволит обеспечить отечественную промышленность высококвалифицированными кадрами.

В основу идеологии развития российского образования должны быть положены интересы отечественного работодателя, инновационное развитие промышленного производства конкурентноспособной продукции с использованием собственной элементной базы и отечественных технологий на основе решения задач импортозамещения и обеспечения технологической независимости. Для этого необходимо исключить влияние негативных факторов, которые проявились в процессе реформирования российского высшего образования и превращения его в многоуровневую систему западного образца, и решить ряд неотложных задач, среди которых следует выделить:

– смещение вектора развития высшего образования в сторону нужд отечественной промышленности, повышение качества подготовки кадров при условии сохранения приоритета воспитания над обучением;

– введение в направления подготовки кадров, призванных обеспечивать основу роста валового продукта страны, специалитета, нацеленного на подготовку конструкторов, разработчиков новых технологий, приборов, систем, устройств наряду с сохранением подготовки бакалавров, обеспечивающих их эксплуатацию и работоспособность, и магистров (нацеленных на разработку инноваций в научно-исследовательской и педагогической деятельности);

– восстановление научно-педагогических школ как основы инновационного развития подготовки высококвалифицированных специалистов, востребованных промышленностью, формирования и обновления интеллектуальной научно-технической элиты;

– восстановление статуса аспирантуры как научной структуры, исторически являющейся организационной основой подготовки научно-педагогических кадров высшей квалификации, развития приоритетных направлений научных исследований, неотъемлемым элементом сохранения и развития научно-педагогических школ в высших учебных заведениях и научно-исследовательских институтах, с продолжительностью обучения от двух до четырех лет в зависимости от направления подготовки и представлением по окончании диссертационной работы;

– обеспечение студентов учебно-методической литературой, одобренной учебно-методическими объединениями и Минобрнауки России для унификации подготовки кадров по каждому направлению в разных образовательных организациях с включением в перечень рекомендованной литературы учебных изданий с соответствующим грифом;

– реализация содержательного контроля образовательного процесса с включением в состав экспертных комиссий, участвующих в проведении лицензирования и аккредитации вузов, высококвалифицированных представителей из профессорско-преподавательского состава вузов и учебно-методических советов по соответствующим направлениям подготовки;

– проведение содержательной оценки эффективности вуза, факультета, кафедры, преподавателя по конкретным результатам работы, исключение формальных показателей, ориентированных на западные стандарты;

– обеспечение реальной научно-исследовательской работы студентов в процессе реализации образовательного процесса подготовки бакалавров, магистров и специалистов за счет привлечения средств предприятий, заинтересованных в данном финансировании, и предоставления им налоговых льгот;

– совершенствование и внедрение инновационных форм интеграции образования, науки и промышленности, создане крупных научно-образовательных центров, как с российскими, так и зарубежными партнерами.

Особую актуальность рассмотренные предложения приобретают в условиях действия современных вызовов и санкций, когда со всей остротой проявляется необходимость принятия решительных мер по сохранению кадрового потенциала и воспроизводству

высококвалифицированных инженерных кадров для обеспечения технологической независимости и реализации стратегии импортозамещения, в первую очередь, в высокотехнологичных отраслях отечественной промышленности, включая ИТ-сферу.

Стратегическая цель обеспечения кадровой безопасности промышленных предприятий определяется возможностью сохранения и устойчивого развития их кадрового потенциала как ключевого экономического показателя, важнейшего производственного и интеллектуального ресурса. Реализация перечисленных предложений, направленных на повышение качества подготовки кадров, будет несомненно способствовать сохранению и развитию кадрового потенциала промышленных предприятий, формированию кадрового резерва и обеспечению кадровой безопасности предприятий высокотехнологичных отраслей промышленности, в том числе за счет насыщения рынка труда ИТ-специалистами, подготовленными в рамках направления «Информационные системы и технологии» – одного из наиболее динамично развивающихся в структуре укрупненной группы направлений и специальностей высшего образования 09.00.00 «Информатика и вычислительная техника».

СПИСОК ЛИТЕРАТУРЫ

1. Б.Я. Советов, В.В. Касаткин. Новые тенденции подготовки кадров в области информационных технологий (пленар. доклад) // Перспективные направления развития отечественных информационных технологий: материалы II межрегиональной научно-практическая конф. Севастополь, 13-17 сентября 2016 г. / Севастопольский государственный университет; науч. ред. Б.В. Соколов - Севастополь: СевГУ, 2016.
2. Советов Б.Я. Тенденции развития высшего образования и подготовки кадров в области информационных технологий. // 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. – 599 с.

ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И ТЕХНОЛОГИИ

УДК 621.391.28

СИСТЕМАТИЧЕСКАЯ ПРОЦЕДУРА ПРИМЕНЕНИЯ МЕТОДА ДВУХМОМЕНТНОЙ АППРОКСИМАЦИИ ДЛЯ ОПРЕДЕЛЕНИЯ ФУНКЦИИ РАСПРЕДЕЛЕНИЯ ВРЕМЕНИ РЕАЛИЗАЦИИ СТОХАСТИЧЕСКОЙ СЕТИ

Канаев Андрей Константинович, Карабанов Юрий Сергеевич, Привалов Андрей Андреевич
ФГБОУ ВО Петербургский государственный университет Путей сообщения императора Александра I
Россия, Санкт-Петербург, Московский пр., 9
emails: kanaevak@mail.ru, karabanov1994@yandex.ru, aprivalov@inbox.ru

***Аннотация**:* В статье рассматривается разработанная авторами процедура многократного применения метода двухмоментной аппроксимации при определении эквивалентной функции стохастической сети, что значительно упрощает задачу определения функции распределения времени реализации моделируемого процесса.

***Ключевые слова:** метод топологического преобразования стохастических сетей, уравнение Мейсона, эквивалентная функция, метод обращения, разложение Хевисайда, двух моментная аппроксимация, функция распределения, неполная гамма-функция.*

TWO-MOMENT APPROXIMATION METHOD APPLICATION SYSTEMATIC PROCEDURE FOR THE FUNCTION DETERMINATION OF STOCHASTIC NETWORK TIME DISTRIBUTION IMPLEMENTATION

Kanaev Andrey., Karabanov Yuriy., Privalov Andrey
Emperor Alexander I Saint-Peterburg State Transport University
Russia, Saint-Petersburg, Moskovsky pr., 9
emails: kanaevak@mail.ru, karabanov1994@yandex.ru, aprivalov@inbox.ru

Abstract: In this article, we consider the developed by the authors procedure for the repeated application of the moment approximation spirit method in determining the stochastic network equivalent function, which greatly simplifies the task of determining the implementation time distribution function for the simulated process.

***Keywords:** the topological transformation of stochastic networks, Mason equation, Equivalent function, treatment method, Heaviside decomposition, two-moment approximation, Distribution function, Incomplete gamma function.*

Введение**.** Современные системы поддержки принятия решений по управлению сложными организационно-техническими системами требуют включения в состав модуля информационно-расчетных задач таких расчетных моделей, которые позволяют получать достаточно точные результаты в масштабе времени, близком к реальному. При этом модели должны не только адекватно отображать функционирование системы в конкретных условиях, но и производить оценку качества (эффективности) по показателям, согласующимся с требованиями макросистемы.

Одним из методов моделирования, позволяющих разрабатывать модели, удовлетворяющие указанным выше требованиям, является метод топологического преобразования стохастических сетей (ТПСС) [1], известным также под названием GERT (Graphical Evaluation and Review Techique) [2,3].

Метод предполагает представление процесса функционирования системы в виде стохастической сети с последующим определением ее эквивалентной функции, математического ожидания и дисперсии времени успешной реализации моделируемого процесса, [4,].

В работах [1,5,6] были описаны способы получения функции распределения времени успешной реализации и спектральных характеристик моделируемого процесса из эквивалентной функции путем использования методов двух- и четырех - моментной аппроксимации, а также метода обращения, основанного на использовании разложения Хевисайда, [7].

Однако увеличение размерности стохастической сети приводит к значительному усложнению эквивалентной функции

$$Q(s) = \frac{\prod_{i=1}^{m} q_i(s)}{1 - \sum_{k=1}^{n} (-1)^k L_k(s)},$$

– где: $L_k(s)$ – эквивалентные функции петель k-го порядка; $\prod_{i=1}^{m} q_i(s)$ - эквивалентная функция последовательных ветвей, соединяющих входную и выходную вершины стохастической сети; $q_i(s)$ – преобразование Лапласа [7] плотности распределения вероятностей времени реализации i-й ветви.

Понятно, что это приводит к увеличению громоздкости получаемых формульных соотношений, а зачастую и к невозможности использования метода обращения, что обусловлено сложностью точного определения большого числа полюсов эквивалентной функции. Кроме того, использование для определения функции распределения методов двух– и четырех- моментной аппроксимации при моделировании процессов функционирования систем в условиях антагонистических конфликтов может привести к недопустимо большой погрешности получаемых результатов моделирования [8].

В настоящей статье, на примере модели процесса функционирования системы передачи информации в условиях конфликта с системой кибервоздействия нарушителя [8], предлагается систематическая процедура использования метода двухмоментной аппроксимации, значительно упрощающая получение функции распределения времени успешной реализации моделируемого процесса.

Постановка задачи. Пусть имеется система передачи информации (СПИ), под которой понимается совокупность технических средств, объединенных в единую технологическую цепочку, использующих общий физический принцип обработки и передачи сигналов, а также определенный порядок взаимодействия технических средств между собой, осуществляющая доставку потока данных пользователям. Указанная СПИ функционирует в условиях деструктивных кибервоздействий нарушителя, который за случайное время $t_{РП}$ с функцией распределения $R(t)$ обнаруживает факт передачи информации и реализует воздействие, не позволяющее осуществлять доставку достоверных данных пользователям.

Если деструктивное воздействие нарушителя на СПИ отсутствует, то она функционирует в условиях постоянно действующих случайных воздействий и обеспечивает успешную доставку данных за случайное время $t_{ПС}$ с функцией распределения $B(t)$. В противном случае, в течение времени передачи данных нарушителем будет реализовано деструктивное кибервоздействие, которое обнаруживается анализатором качества функционирования или оператором, и, после восстановления работоспособности, СПИ переключается в такой режим работы, который обеспечивает доставку пользователям достоверных данных в новых условиях. При этом время обнаружения факта деструктивного воздействия нарушителя и смены режима работы t_B является случайным с функцией распределения $D(t)$. В новом режиме работы СПИ обеспечивает успешную доставку данных за случайное время $t_{НР}$ с функцией распределения $A(t)$.

Функции распределения времени оказания нарушителем деструктивного кибервоздействия, успешной доставки данных в различных условиях, а также обнаружения факта деструктивного воздействия и смены режима работы, определяются с использованием моделей, описанных в [9,10,11].

Требуется определить функцию распределения и среднее время успешной доставки данных в СПИ.

Решение. Из постановки задачи следует, что стохастическая сеть должна содержать, по крайней мере, две цепи. Первая из них выбирается с вероятностью такого события, что за время доставки данных в условиях постоянно действующих случайных воздействий факт их передачи будет обнаружен системой компьютерной разведки, и нарушитель успеет реализовать кибервоздействие. Поэтому в стохастической сети первая ветвь этой цепи будет характеризоваться преобразованием Лапласа

$$\gamma(s+b) = \int_0^{\infty} \exp[-(s+b)t] r(t) dt, \qquad (1)$$

где: $r(t)$ – плотность распределения вероятностей времени успешной реализации нарушителем кибервоздействия; $b = \frac{1}{T_b}$; $T_b = \int_0^{\infty} t h_b(t) dt$, $h_b(t)$ - математическое ожидание и плотность распределения вероятностей времени успешной доставки данных в условиях случайных помех, соответственно.

В свою очередь, характеристикой первой ветви второй цепи стохастической сети является

$$1-\gamma(s+b)=1-\int_0^\infty \exp[-(s+b)t]r(t)dt\,.$$

Таким образом, укрупненная стохастическая сеть процесса функционирования СПИ в условиях конфликта с системой кибервоздействия нарушителя имеет вид, представленный на рис.1.

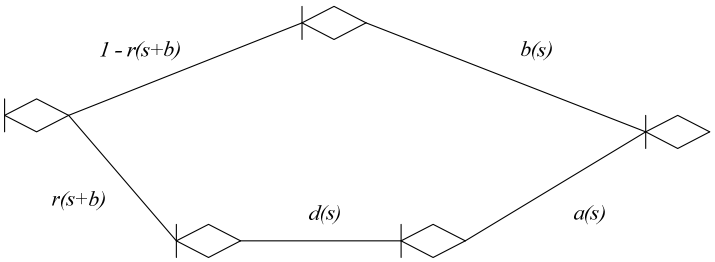


Рис. 1. Стохастическая сеть процесса функционирования СПИ в условиях конфликта с системой кибервоздействия нарушителя.

На рис.1 имеются следующие обозначения:

$$\gamma(s+b)=\int_0^\infty \exp[-(s+b)t]r(t)dt, \tag{1}$$

– преобразование Лапласа плотности распределения вероятностей времени – успешной реализации нарушителем кибервоздействия по параметру $(s+b)$;

$$b(s)=\int_0^\infty \exp(-st)h_b(t)dt, \tag{2}$$

– преобразование Лапласа плотности распределения вероятностей времени доставки данных в условиях случайных воздействий;

$$a(s)=\int_0^\infty \exp(-st)h_a(t)dt\,, \tag{3}$$

– преобразование Лапласа плотности распределения вероятностей времени доставки данных после смены режима работы;

$$d(s)=\int_0^\infty \exp(-st)d(t)dt\,, \tag{4}$$

– преобразование Лапласа функции распределения времени обнаружения факта кибервоздействия и смены режима работы.

Эквивалентная функция стохастической сети (рис.1) имеет следующий вид:

$$Q(s)=\left[1-r(s+b)\right]b(s)+r(s+b)d(s)a(s)\,. \tag{5}$$

После подстановки в (5) изображений по Лапласу (2), (3), (4) и результатов [9,10,11], получим:

$$Q(s)=\sum_{i=1}^{N}K_b(s_i)\frac{1}{s-s_i}-\left[\sum_{i=1}^{N}K_b(s_i)\frac{1}{s-s_i}\right]\cdot\left[\sum_{j=1}^{M}K_r(s_j)\frac{1}{s-s_j}\right]+\left[\sum_{k=1}^{K}K_d(s_k)\frac{1}{s-s_k}\right]\cdot\left[\sum_{j=1}^{M}K_r(s_j)\frac{1}{s-s_j}\right]\cdot\left[\sum_{i=1}^{N}K_a(s_i)\frac{1}{s-s_i}\right], \tag{6}$$

здесь $K_{b(a,r)}(s_{i(j,k)})$ - вычеты частных эквивалентных функций [9,10,11] в полюсах $s_{i(j,k)}$, $i=\overline{1,N};\ j=\overline{1,M};\ k=\overline{1,K}$, соответственно.

Очевидно, что нахождение оригинала функции *Q(s)* весьма трудоемко.

В тоже время, результаты [9,10,11] позволяют получить выражения для определения среднего и дисперсии времени реализации частных процессов:

– математическое ожидание и дисперсия времени успешной доставки данных в условиях случайных воздействий

$$T_b=\int_0^\infty t\cdot h_b(t)dt=\sum_{i=1}^{N}\frac{K_b(s_i)}{s_i^{\,2}}\,, \tag{7}$$

$$D_b=\int_0^\infty (t-T_b)^2\cdot h_b(t)dt=-2\cdot\sum_{i=1}^{N}\frac{K_b(s_i)}{s_i^{\,3}}-T_b^2\,; \tag{8}$$

– математическое ожидание и дисперсия времени успешной доставки данных после смены режима работы

$$T_a=\int_0^\infty t\cdot h_a(t)dt=\sum_{i=1}^{N}\frac{K_a(s_i)}{s_i^{\,2}}\,, \tag{9}$$

$$D_a = \int_0^{\infty} (t - T_a)^2 \cdot h_a(t)dt = -2 \cdot \sum_{i=1}^{N} \frac{K_a(s_i)}{s_i^3} - T_a^2, \quad (10)$$

– математическое ожидание и дисперсия времени обнаружения факта кибервоздействия и смены режима работы

$$T_d = \int_0^{\infty} t \cdot d(t)dt = \sum_{k=1}^{K} \frac{K_d(s_k)}{s_k^2}, \quad (11)$$

$$D_d = \int_0^{\infty} (t - T_d)^2 \cdot d(t)dt = -2 \cdot \sum_{k=1}^{K} \frac{K_d(s_k)}{s_k^3} - T_d^2, \quad (12)$$

– математическое ожидание и дисперсия времени успешной реализации нарушителем кибервоздействия

$$T_r = \int_0^{\infty} t \cdot r(t)dt = \sum_{j=1}^{M} \frac{K_r(s_j)}{s_j^2}, \quad (13)$$

$$D_r = \int_0^{\infty} (t - T_r)^2 \cdot r(t)dt = -2 \cdot \sum_{j=1}^{M} \frac{K_r(s_j)}{s_j^3} - T_r^2, \quad (14)$$

С использованием (7-14) определим параметры формы и масштаба неполной гамма-функции, аппроксимирующей плотности распределения вероятностей времени свершения частных процессов [12]:

$$\beta = \frac{T_b^2}{D_b}; \quad \mu_b = \frac{T_b}{D_b};, \quad (16)$$

$$\alpha = \frac{T_a^2}{D_a}; \quad \mu_a = \frac{T_a}{D_a};, \quad (17)$$

$$\eta = \frac{T_d^2}{D_d}; \quad \mu_d = \frac{T_d}{D_d};, \quad (18)$$

$$\rho = \frac{T_r^2}{D_r}; \quad \mu_r = \frac{T_r}{D_r}.., \quad (19)$$

Тогда выражение (6) с учетом (1) и свойств неполной гамма-функции [12] преобразуется к следующему виду:

$$\begin{aligned} Q(s) &= \left(\frac{\mu_b}{\mu_b + s}\right)^{\beta} - \left(\frac{\mu_b}{\mu_b + s}\right)^{\beta} \cdot \left(\frac{\mu_r}{\mu_r + \mu_b + s}\right)^{\rho} + \left(\frac{\mu_a}{\mu_a + s}\right)^{\beta} \cdot \left(\frac{\mu_d}{\mu_d + s}\right)^{\eta} \cdot \left(\frac{\mu_r}{\mu_r + \mu_b + s}\right)^{\rho} = \\ &= \left(\frac{\mu_b}{\mu_b + s}\right)^{\beta} - \left(\frac{\mu_r}{\mu_r + \mu_b}\right)^{\rho} \cdot \left(\frac{\psi}{\psi + s}\right)^{\varphi} + \left(\frac{\mu_r}{\mu_r + \mu_b}\right)^{\rho} \cdot \left(\frac{\vartheta}{\vartheta + s}\right)^{\xi}, \end{aligned} \quad (20)$$

где: $\psi = \frac{T_{rr} + T_b}{D_{rr} + D_b}; \quad \varphi = \frac{(T_{rr} + T_b)^2}{D_{rr} + D_b}; \quad \vartheta = \frac{T_{rr} + T_d + T_a}{D_{rr} + D_a + D_d};$

$\xi = \frac{(T_{rr} + T_d + T_a)^2}{D_{rr} + D_a + D_d}; \quad T_{rr} = \frac{\rho}{\mu_r + \mu_b}; \quad D_{rr} = \frac{\rho}{(\mu_{rr} + \mu_b)^2}.$

Результат (20) позволяет достаточно просто определить функцию распределения времени успешной доставки данных СПИ путем почленного перехода в пространство оригиналов и интегрирования полученного результата с переменным верхним пределом:

$$F(t) = \frac{\mu_b}{\Gamma(\beta)} \int_0^t t^{\beta-1} e^{-\mu_\beta t} dt - \frac{\psi}{\Gamma(\varphi)} \left(\frac{\mu_b}{\mu_b + s}\right)^{\beta} \int_0^t t^{\varphi-1} e^{-\varphi t} dt + \frac{\vartheta}{\Gamma(\xi)} \left(\frac{\mu_b}{\mu_b + s}\right)^{\beta} \int_0^t t^{\xi-1} e^{-\vartheta t} dt. \quad (21)$$

Не сложно видеть, что математическое ожидание времени успешной доставки данных СПИ равно

$$T_{дост} = \frac{\beta}{\mu_b} + \left(\frac{\mu_r}{\mu_b + \mu_r}\right)^{\rho} \left(\frac{\beta}{\mu_b} - \frac{\eta}{\mu_d} - \frac{\alpha}{\mu_a}\right), \quad (22)$$

Таким образом, поставленная задача решена.

Порядок решения задачи соответствует предлагаемой авторами систематической процедуре, которая заключается в реализации следующей последовательности:

– Шаг 1. Составление стохастической сети моделируемого процесса, в т.ч. и с использованием подхода, изложенного в [13];

– Шаг 2. Укрупнение стохастической сети, таким образом, чтобы ветви соответствовали отдельным, самостоятельно реализуемым композиционным подпроцессам;

– Шаг 3. Для ветвей, отображающих композиционные процессы, с использованием уравнения Мейсона для замкнутых графов определяются их (частные) эквивалентные функции;

– Шаг 4. Из каждой частной эквивалентной функции определяются первый начальный и второй центральный моменты случайного времени их реализации;

– Шаг 5. Определяются параметры формы и масштаба неполной гамма-функции по формулам (16…19);

– Шаг 6. Составляется эквивалентная функция укрупненной стохастической сети, элементами которой являются изображения по Лапласу неполных гамма функций с параметрами, определенными на шаге 5;

– Шаг 7. Для фрагментов эквивалентной функции, представляющих собой произведение изображений по Лапласу ставится в соответствие изображение неполной гамма-функции с математическим ожиданием, равным сумме математических ожиданий и дисперсией, равной сумме дисперсий, как это сделано при проведении преобразований в (20). Таким образом, получается выражение, представляющее алгебраическую сумму изображений неполных гамма-функций;

– Шаг 8. Осуществление по членного перехода в пространство оригиналов и получение плотности распределения вероятностей времени реализации моделируемого процесса;

– Шаг 9. Интегрирование полученного на шаге 8 результата с переменным верхним пределом и определение искомой функции распределения.

Завершение процедуры.

По (21) произведены расчеты, результаты которых представлены на рис.2. При расчетах предполагалось, что среднее время реализации частных процессов составляло: $T_b = 3,3$ мин., $T_a = 10$ мин., $T_d = 14$ мин., $T_r = 3$ мин. Дисперсия времени их реализации полагалась равной: $D_b = 11 мин^2$, $D_a = 100 мин^2$, $D_d = 196 мин^2$, $D_r = 9 мин^2$. На рисунке обозначено: 1 – функция распределения времени доставки данных в условиях случайных воздействий; 2 – функция распределения времени доставки данных в условиях реализованного кибервоздействия после смены режима работы; 3 – функция распределения времени успешной доставки данных в условиях конфликта с системой кибервоздействия нарушителя, полученная в результате строгого решения задачи, описанного в [8]; 4 – тоже, при решении с использованием предлагаемой систематической процедуры; 5 – тоже, при ее аппроксимации неполной гамма-функцией, т.е. в этом случае параметры распределения определялись в соответствии с [12,14,15]:

$$\mu_G = \frac{T_{дост}}{D_{дост}}; \quad \alpha_G = \frac{T_{дост}^{\ 2}}{D_{дост}}; \quad T_{дост} = -\frac{\partial}{\partial s}\left[\frac{Q(s)}{Q(0)}\right]_{s=0}; \; D_{дост} = \frac{\partial^2}{\partial s^2}\left[\frac{Q(s)}{Q(0)}\right]_{s=0} - T_{дост}^2 .$$

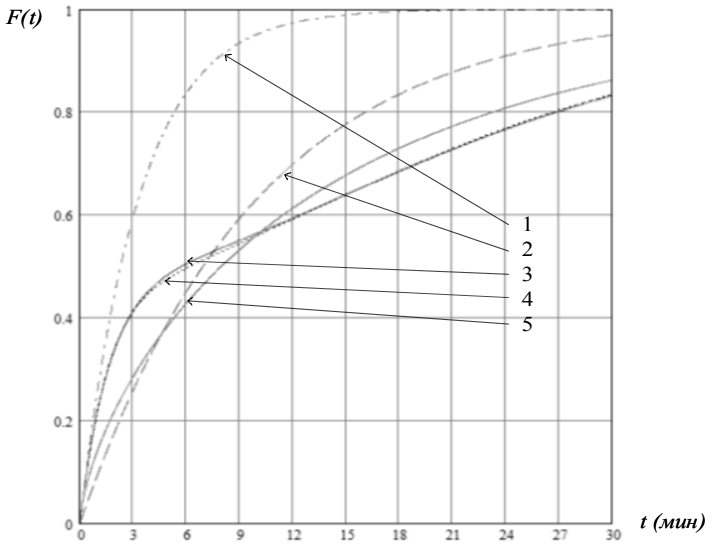


Рисунок 2. Вид функций распределения времени доставки данных, полученных при различных способах решения задачи.

Анализ полученных результатов показывает, что систематическая процедура применения метода двухмоментной аппроксимации имеет погрешность при определении функции распределения времени свершения процесса, представленного в виде стохастической сети, не превышающую 2% относительно строго полученного результата (кривые 3 и 4). При этом аппроксимация реальной функции распределения по двум моментам случайного времени приводит к погрешности получаемых результатов до 30% (кривые 4 и 5). Сопоставление выражений (6) и (20) показывает, что (20) является менее громоздкой и не чувствительной к кратности полюсов эквивалентной функции, что значительно упрощает процедуру перехода в пространство оригиналов и определения функции распределения

времени успешной реализации моделируемого процесса. Это свидетельствует о целесообразности использования предложенной процедуры для упрощения задачи определения функции распределения с достаточной для инженерных расчетов точностью.

Заключение. Таким образом, в настоящей статье рассмотрено новое решение известной задачи, для которого авторами предложена систематическая процедура применения метода двух моментной аппроксимации при определении функции распределения времени реализации случайного процесса, представленного в виде стохастической сети. Использование в методе двух моментной аппроксимации неполной гамма-функции не является обязательным условием для реализации процедуры и закон распределения времени свершения композиционных ветвей в укрупненной стохастической сети может быть выбран любым другим. Порядок проведения преобразований при этом не изменяется.

Предложенная систематическая процедура позволяет получать результаты, имеющие погрешность, не превышающую 2 %, что является достаточным для большинства инженерных расчетов.

СПИСОК ЛИТЕРАТУРЫ

1. Привалов А.А. Метод топологического преобразования стохастических сетей и его использование для анализа систем связи ВМФ. // СПб, ВМА, 2000 г. – 166 с.
2. Pristker A.A.B., Happ W.W. GERT: Graphical Evaluation and Review Technique, Part I, Fundamentals. // The Journal of Industrial Engineering (May, 1966).
3. Pristker A.A.B., Whitehouse G.E. GERT: Graphical Evaluation and Review Technique, Part II. // The Journal of Industrial Engineering (June, 1966).
4. Филлипс Д., Гарсиа-Диас А. Методы анализа сетей: Пер. с англ. // Мир: 1984. – 496 с.
5. Привалов А.А., Симонов М.В. Метод поиска функций распределения времени доставки кадров данных в сетях передачи данных.// Техника средств связи./ Сборник научных статей НПК «Красная Заря». Серия: Техника проводной связи. Выпуск 4. – СПб: «Политехника», 1992 г. - С. 56-61.
6. Бекбаев Г.А., Вандич А.П., Привалов А.А., Привалов Ал.А., Ясинский С.А. Динамическая модель процесса функционирования телекоммуникационной сети ОАО «РЖД» в нестационарных условиях. // Информация и космос. 2015г., № 4. – С. 13-17.
7. Дёч Г. Руководство к практическому применению преобразований Лапласа: Пер. с нем. // М.: «Государственное издательство физико-математической литературы», 1960г. – 208 с.
8. Куделя В.Н., Привалов А.А., Петриева О.В, Чемиренко В.П. Методы математического моделирования систем и процессов связи. // По общ. ред. Чемиренко В.П. – СПб: Изд-во Политехн. ун-та, 2009 г. – 368с.
9. Вандич А.П., Кудряшов В.А., Привалов А.А. Моделирование процесса работы в ECMA. // Автоматика, связь, информатика. 2012г. , № 6. - С. 24-26.
10. Вандич А.П., Евглевская Н.В., Привалов А.А., Привалов Ал.А. Комплексная модель воздействия злоумышленника на автоматизированные системы управления технологическими процессами. // «Актуальные проблемы инфотелекоммуникаций в науке и образовании». Сборник трудов II Международной научно-технической и научно-методической конференции. 2013. - С. 118-122.
11. Евглевская Н.В., Привалов А.А. Модель информационного воздействия на объекты телекоммуникационной сети. // Известия Петербургского университета путей сообщения. 2015. № 1 (42). - С. 72-77.
12. Мартин Дж. Системный анализ передачи данных. Том 2. // Пер. с англ. – М.: Мир, 1975г. – 434с.
13. Рытов М.Ю., Мегаев К.А. Алгоритм управления трафиком в среде корпоративного портала. /Вестник Брянского государственного технического университета. 2014. - № 1(41). – С. 87-93
14. Еременко, В.Т. Анализ моделей управления трафиком в сетях АСУП на основе технологии MPLS / В.Т. Еременко, С.В. Еременко, Д.В. Анисимов, С.А. Черепков, А.А. Лякишев // Информационные системы и технологии. –2013. – № 1. – С. 106-112.
15. Андрющенко В.А., Скалозуб В.В. Метод структурного преобразования стохастических сетей для ГЕРТ-моделирования технологических и экономических процессов/ Наука и прогресс транспорта. Вестник Днепропетровского университета железнодорожного транспорта им. акад. В. Лазаряна. – Д.: Изд-во ДНУЖТ, 2008. – С. 167-180

УДК 004.9, 004.056

ПРИМЕНЕНИЕ РОЛЕВОЙ МОДЕЛИ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ В МЕЖМАШИННЫХ СЕТЯХ ДИНАМИЧЕСКОЙ ТОПОЛОГИИ

Калинин Максим Олегович, Резединова Евгения Юрьевна
Санкт-Петербургский политехнический университет Петра Великого
Россия, Санкт-Петербург, ул. Политехническая, д. 29,
emails: max@ibks.spbstu.ru, er@ibks.spbstu.ru

***Аннотация*:** В статье рассмотрены особенности сетей транспортных средств, сценарии взаимодействия узлов, а также возможность адаптации ролевой модели контроля и управления доступа к особенностям VANET.

***Ключевые слова**: ролевая модель; управление доступом, сети транспортных средств; безопасность.*

APPLICATION OF ROLE-BASED ACCESS CONTROL IN MACHINE-TO-MACHINE NETWORKS WITH DYNAMIC TOPOLOGY

Kalinin Maxim, Evgenia Rezedinova
Peter the Great St. Petersburg Polytechnic University,
Russia, St. Petersburg, Polytechnicheskaya street, 29
emails: max@ibks.spbstu.ru, er@ibks.spbstu.ru

Abstract: The paper discusses features of vehicular and mobile devices networks, interaction scenarios of nodes, and also examines the access control model for role-based security control in VANET/MANET.

Keywords: *RBAC; access control; vehicular networks; security***.**

При финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП "Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы" (Соглашение №14.578.21.0224, от 03.10.2016, уникальный идентификатор Соглашения RFMEFI57816X0224).

Введение. Современные сети транспортных средств являются быстро развивающейся технологической сферой, в которой формируются новые общественные потребности, ориентированные на поддержание непрерывных, защищенных и надежных служебных, личных и сервисных коммуникаций.

В настоящее время активно расширяется рынок особых информационных систем – интеллектуальных транспортных систем, включающих сервисы и услуги транспортной направленности. Такого рода сервисы интегрируют транспортные средства, системы и решения, направленные на реализацию функций управления дорожным движением, предупреждения чрезвычайных ситуаций, информирования водителей, автоматизации транспортной логистики, оптимизации транспортной и околотранспортной экономики, анализа, обработки и визуализации «больших данных» о событиях в транспортной сфере и т.п.

Актуальной научной задачей является построение моделей контроля и управления доступа для сетей транспортных средств, поскольку такие сети обладают динамической топологий, могут быстро изменяться, им свойственно постоянное и непрерывное изменение состояний узлов. Поэтому особенно важным является возможность актуализации модели путем внесения в нее изменений в любой момент времени.

Известные методы и модели контроля доступа (DAC, MAC) в случае их применения к сетям транспортных средств нуждаются в серьезной адаптации [1]-[4].

Применительно к сетям транспортных средств основополагающим является развитие моделей разграничения прав доступа, приближающихся к реальным ситуациям и учитывающих сложные межмашинные связи и динамику топологии.

Проанализировав существующие подходы [5]-[12] к обеспечению безопасности и конфиденциальности для динамических сетях были сделаны следующие выводы.

1. Традиционные методы контроля доступа, такие как ABAC или RBAC могут быть использованы для сложных динамических систем (Интернет Вещей, сети транспортных средств) при условии их уточнения и дополнения;

2. Для определения и назначения прав доступа в сложных случаях (при контекстно-зависимых или основанных на доверии условиях) вычислительная мощность устройств Интернета Вещей является заведомо недостаточной в связи, с чем предпочтительным здесь является централизованный подход, при котором принятие решений будет производить отдельный мощный узел или ПКС. Под контролем и управлением доступом на основе ролей понимают развитие дискреционной модели управления доступом, при которой права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли.

Иными словами определяющей особенностью ролевой модели является предоставление доступа к информационным сервисам исключительно через роли.

Появление идеи предоставления доступа на основе ролей обусловлено необходимостью сгруппировать наборы прав пользователей таким образом, чтобы было понятно, какой доступ есть у того или иного пользователя, и как он изменяется в случае смены положения этого пользователя.

В классической статье Феррайоло и Куна [13], опубликованной в 1992 году, было предложено формально описание модели RBAC. Ролевой доступ предлагается осуществлять только через механизм ролей, также предложены механизмы наследования, сессии и описаны возможные ограничения. В 2000 году выходит статья Санди, Феррайоло и Куна, закрепляющая стандарт RBAC [14].

В настоящее время действует стандарт ANSI Standart RBAC от 2004 года [15]. Этот стандарт представляет собой полное описание возможностей RBAC.

Анализируя стандарт, можно прийти к выводу, что ключевые возможности RBAC удобно применить к контролю доступа в сетях VANET следующим образом:

1. Ролевая модель позволяет избежать конфликтов интересов, если заранее определить, что пользователь не может брать роли с противоречащими друг другу возможностями.

2. Механизм сессии также может быть эффективно внедрен и применен при управлении доступом в сетях транспортных средств. Пользователь может работать с ролью только в определённой ситуации, строго определенное время. После закрытия сессии пользователь больше не может применять роль. В сетях транспортных средств такой механизм может быть полезен при возникновении каких-либо особых нестандартных ситуаций.

3. В случае динамических систем время на произведение операций имеет существенное значение. Механизм наследования удобен тем, что позволяет быстро изменять права пользователям.

4. Ролевой доступ может быть расширен введением широкого множества атрибутов. Это решение, повышающее гибкость, что особенно важно, если следует динамически переназначать полномочия и роли.

Сопоставление модели RBAC с другими существующими моделями контроля доступа относительно применения в межмашинных коммуникационных сетях представлено в таблице 1.

Таблица 1

Сравнение RBAC с другими моделями контроля доступа

Сравнительные характеристики	Модели контроля доступа		
	DAC	MAC	RBAC
Разделение по уровням доступа	нет	да	нет
Экономия трудозатрат [16]	нет	да	да
Гибкость управления [17]	да	нет	да
Управление правами без участия администратора	да	нет	да
Невысокая стоимость реализации [16]	да	да	нет
Поддержка ACL [18]	да	нет	да
Высокая производительность	да	нет	нет
Механизм наследования	нет	нет	да
Сеансовый механизм	нет	нет	да
Применение в сложных распределенных системах	да	нет	да
Поддержка механизма запретов	нет	да	нет
Расширение широким множеством атрибутов	да	нет	да

Ролевые модели, как правило, разрабатываются на основе следующих подходов [12].

1. Должностная ролевая модель – выделение ролей на базе должностных обязанностей сотрудников. Используя аналогичный подход к сетям транспортных средств представляется возможным выделение ролей в зависимости от назначения транспортного средства: обычный подключенный автомобиль, автомобиль скорой помощи, автомобиль дорожной службы, полицейский автомобиль и т.д. Если в сети транспортных средств существует строго ограниченный перечень участников, и каждый из них должен следовать определенным правилам поведения в рамках системы, то наиболее подходящим будет использование аналог должностной ролевой модели.

2. Функциональная ролевая модель – выделение ролей на базе функциональных задач. Метод наиболее оптимален с точки зрения соотношения результатов и затраченных усилий. Применительно к сети транспортных средств выделяются следующие функциональные роли: автомобили (узлы) служб помощи, поддержки, безопасности, автомобили (узлы) предоставляющие развлечения, доступ к Интернет, также другие основные и вспомогательные роли в зависимости от степени развитости технических и информационных возможностей СТС.

3. Гибридная модель – это модель, совмещающая подходы должностной и функциональной ролевой модели. В сети транспортных средств гибридную модель можно представить следующим образом. Базовые участники движения: «подключенный автомобиль», «помощь на дороге», «полицейский автомобиль», «служба развлечений».

При разработке ролевой модели для сети транспортных средств оптимальным представляется применение функциональной в силу простоты и удобства выделения сущностей.

Основными преимуществами использования ролевой модели контроля и управления доступом являются: адаптируемость к изменениям в процессе развития сложной транспортной системы и относительная простота проецирования типов узлов, объектов и полномочий на систему ролей за счет эквивалентности множеств, на которых в системе определяются полномочия и множеств, вводимых моделью.

Ролевым моделям контроля и управления доступом присущи следующие недостатки: механизмы управления информационными потоками между сущностями системы не являются достаточно гибкими. Ролевая модель позволяет ограничить потоки между сущностями системы только путем запрета взаимодействия между разными ролями и предоставления доступа ролям на непересекающиеся множества объектов; назначение наборов типовых прав роли при использовании в сложных системах может приводить к значительному росту числа ролей (в пределе — индивидуальная роль для каждого пользователя). Это связано с наличием большого количества типов объектов, схем доступа к ним, типов операций, которые необходимо учитывать при назначении прав.

В тоже время названные недостатки не являются существенными при применении ролевой модели в качестве основы контроля и управления доступом к информационным сервисам в сетях транспортных средств. Более того, преимущества данной модели позволяют эффективно организовать контроль и управление доступом к информационным сервисам.

Учитывая специфику сетей транспортных средств предъявляются следующие требования к ролевой модели управления:

1. За основу системы контроля и управления доступов в сети транспортных средств принимается классическая ролевая модель контроля доступа, модифицированная с учетом иерархии объектов и иерархии ролей.

2. Модель должна легко адаптироваться к изменениям, обусловленным динамической топологией сети транспортных средств, также должна учитывать межмашинные связи.

3. Права доступа зависят от статуса узла в сети и его функционального назначения.

4. Модель должна учитывать между объектами: структурные связи (агрегацию) и функциональные связи (объекты могут участвовать в выполнении одной или нескольких различных функций, изменение статуса (состояния) в силу выполнения (завершения выполнения) им какой-либо функции приводит к изменению статуса объекта, связанного с ним).

5. Политика безопасности состоит из набора правил следующего вида: когда триггер события и некоторое условие выполняются, то только тогда возможно выполнение заданного действия. Событие – это изменение состояния какого-либо физического (виртуального) объекта.

6. Для динамического переназначения ролей необходимо расширить ролевую модель атрибутами. Например, применение атрибутов "геозона", "дата/время", "текущие сервисы" дадут возможность переназначать роли в зависимости от внешних условий (обстоятельств) в сети транспортных средств.

Для модификации ролевой модели с учетом иерархии объектов предлагается исходить из следующего. Все объекты системы вложены друг в друга. Каждый объект помимо единственного корневого объекта имеет один родительский объект и неограниченное количество дочерних. Пользователю может быть назначена роль для любого объекта.

Определим следующие понятия:

1. Пользователь (U): множество узлов транспортной сети, получающих доступ к сервису. Пользователь: человек, автомобиль, бортовой компьютер, робот и т.д. Каждый пользователь имеет уникальный идентификатор в системе.

$$U_i = \{u_1, u_2, \ldots, u_{n-1}, u_1\},\ (n \in N)\ (i, j, \text{если } i \neq j, \text{то } u_i \neq u_j) \quad (1)$$

2. Роль (R): в системе роль – это категория пользователей, выполняющих однотипные действия или получающих доступ к одинаковому функционалу системы.

$$r_i = \{u_{i1}, u_{i2}, \ldots, u_{ik-1}, u_k\},\ (k \in N) \quad (2)$$

$$R_i = \{r_1, r_2, \ldots, r_{m-1}, r_m\},\ (m \in N) \quad (3)$$

3. Сервис (SERV): сервис – это основной функционал системы, возможности, которые предоставляет система своим пользователям. Услуга предоставляется по запросу от пользователя. Перед исполнением запроса, система должна проверить, что данный пользователь имеет права на получение этой услуги. Сервис может быть представлен как множество других сервисов или услуг.

$$SERV = \{serv_1, \ldots, serv_t\},\ (t \in N)\ (i, j, \text{если } i \neq j, \text{то } serv_i \neq serv_j) \quad (4)$$

4. Назначение пользователя: чтобы использовать сервис, пользователь должен быть соотнесен с ролью. Один и тот же пользователь может использовать разные роли для доступа к разным сервисам.

$$UA \subseteq U \times R \quad (5)$$

5. Иерархия ролей: отношения между ролями, которые могут быть представлены, например, наследованием. Математически иерархия ролей описывается отношением частичного порядка.

$$RH \subseteq R \times R \quad (6)$$

6. Иерархия полномочий: (аналогично с иерархией ролей) используется для повышения гибкости ролевой модели.

$$PH \subseteq P \times P \quad (7)$$

7. Назначение полномочий: отношение «многие-ко-многим» между полномочиями и ролями. Каждой роли назначаются определенные полномочия на доступ к ресурсам.

$$PA \subseteq P \times R \quad (8)$$

8. Сессия: взаимодействие между объектом и субъектом. Сессия создается каждый раз, когда пользователь активирует ту или иную роль и получает доступа к сервису. Каждая сессия связана только с одним пользователем, каждый пользователь может начать несколько сессий.

Метамодель системы ролевого контроля доступа применительно к сети транспортных средств представлена на рис. 1.

Далее подробно рассмотрим сервисы, субъекты, объекты, роли, полномочия в сети транспортных средств.

Под сервисами будем понимать услуги, предоставляемые сетью транспортных средств участникам. Набор сервисов и их краткое название: удаленная диагностика и техническое обслуживание программного обеспечения автомобиля, помощь при авариях, ДТП, развлекательные сервисы; оптимизация трафика и навигация, взаимодействие с системами умный дом.

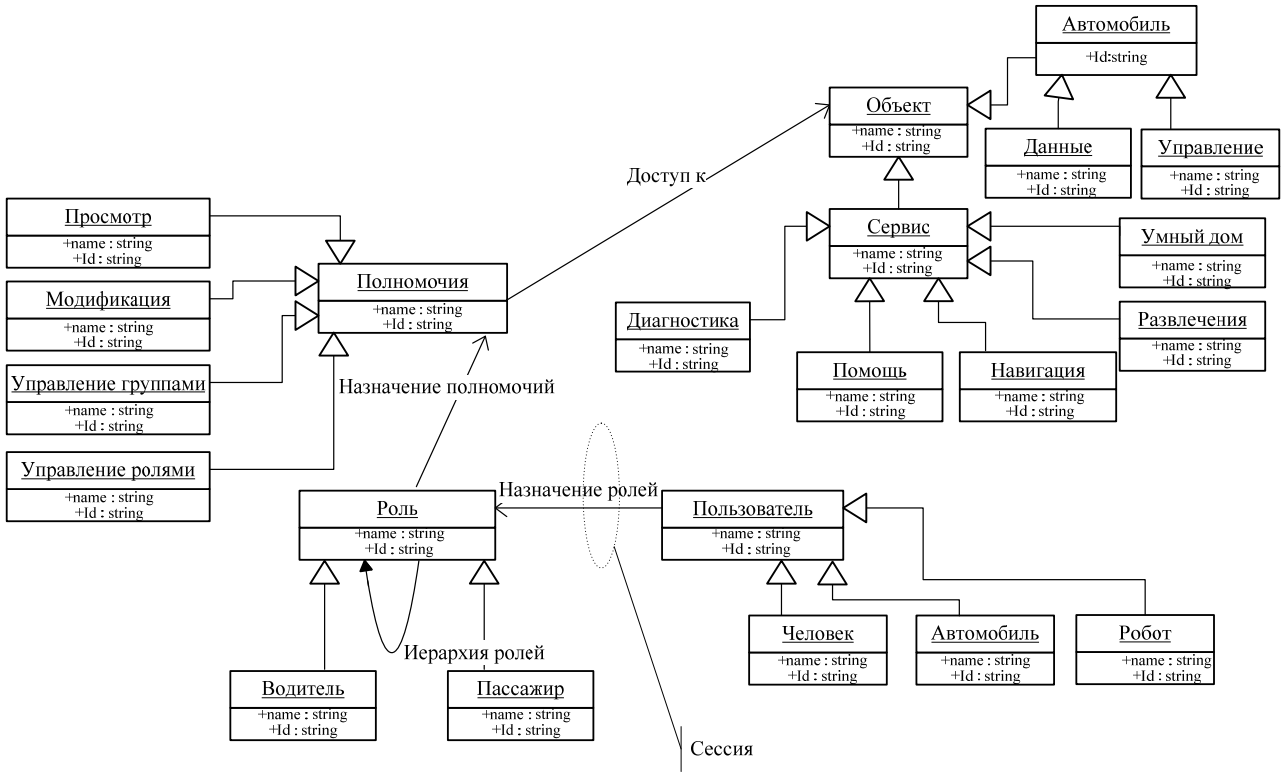


Рис. 1. Метамодель системы ролевого контроля доступа

Субъекты – пользователь системы (человек или автоматизированный агент), обладающий определенными обязанностями и полномочиями: например, водитель со стандартными полномочиями, водитель с расширенными полномочиями, водитель с повышенными полномочиями, т.е. с возможностью управления настройками сети, администрирования и т.д. Также субъектами могут быть пассажир со стандартными полномочиями; пассажир с расширенными полномочиями; пассажир с повышенными полномочиями, возможностью управления настройками сети, администрирования.

Объекты – ресурсы, к которым предоставляется доступ: автомобили с бортовым компьютером – перемещающиеся узлы, управляющие придорожные станции RSU – управляющие стационарные узлы, умный дом, сеть.

Роль – рабочая функция или ее название, которое определяется на уровне авторизации: водитель обычного автомобиля, водитель автомобиля службы 112 водитель автомобиля службы дорожной помощи; пассажир.

Полномочия – разрешенные для роли действия: запрос, просмотр информации (аналог действия «чтение»), модификация информации (аналог действия «запись»), управление настройками системы, управление ролями (добавление, отзыв роли, добавление новых полномочий, полномочий роли), управление группами ролей, создание новой групповой роли, добавление членов в группу, удаление членов из группы, модификация полномочий уже существующей группы, создание новых настроек.

Полнота операций обоснована следующими положениями:

1. Были проанализированы возможные реальные ситуации, возникающие в сети транспортных средств. Анализ показал, что объекты (перемещающиеся и стационарные узлы) – это физические объекты, состоящие из программно-управляемых частей (автомобиль состоит из бортового компьютера, электронного блока управления, умный дом состоит из сети датчиков). Таким образом, объекты и операции над ними могут быть смоделированы по аналогии с компьютерными системами, так программным обеспечение и данными можно управлять только через чтение, запись (в данной работе операции «view» и «modify»).

2. Помимо операций с единичными объектами были рассмотрены групповые операции, так как узлы могут взаимодействовать вместе в рамках какой-то задачи.

3. Включены также операции, отвечающие за управление роля и полномочиями.

4. Были учтены все типы управляющих воздействий на систему: воздействие может отсутствовать, быть исходящим или входящим.

Возможные сценарии взаимодействия сетях транспортных средств соответствуют сценариями взаимодействия в VANET сети и представлены следующим образом: V2V – автомобиль-автомобиль, V2I – автомобиль-инфраструктура, V2H – автомобиль-дом, V2G – автомобиль-сеть.

Рассмотрим детальнее возможные сценарии.

1. Сценарии V2V. При взаимодействии V2V происходит общение между двумя равноправными узлами. Можно рассматривать несколько сценариев внутри: позитивный (дорожная ситуация нормальная, не произошло аварий и ДТП) и негативный (авария, ДТП).

При позитивном сценарии все участники дорожного движения могут получать информацию (в том числе друг от друга) о дорожной ситуации, обмениваться информацией о наличии и отсутствии пробок, помогать друг другу в выборе оптимального маршрута, общаться друг с другом, делиться развлекательным контентом.

При негативном сценарии, например, в случае аварии или ДТП, водитель автомобиля, должен, прежде всего, обратиться за медицинской помощью, если есть пострадавшие, затем вызвать полицию и при необходимости воспользоваться службой помощи на дорогах. В таком случае водитель должен передать всю необходимую информацию: число пострадавших, виды их травм, свое точное местоположение. От полноты информации будет зависеть количество автомобилей скорой помощи и полицейских, а также скорость реагирования на весь инцидент.

2. Сценарии V2I. При взаимодействии V2I в процессе участвуют перемещающиеся узлы (автомобили) и дорожная инфраструктура (стационарные управляющие узлы). Автомобили могут запрашивать и получать необходимую информацию. Через стационарный управляющий узел можно получить информацию о текущей дорожной обстановке, получить информацию по выбору оптимального маршрута. Дорожный узел может также получать и аккумулировать информацию от полицейских автомобилей, карет скорой помощи, автомобилей дорожной помощи, находящихся географически близко к управляющему узлу о том, как изменилась дорожная ситуация.

3. Сценарии V2H. При взаимодействии V2H происходит общение между автомобилем и умным домом. В данном случае, возможно два сценария: у одного автовладельца может быть несколько домов, тогда автомобиль должен иметь доступ к управлению всеми домами; в одном доме может проживать несколько автовладельцев, тогда каждый автовладелец должен иметь право на управление домом.

4. Сценарии V2G. При взаимодействии V2G общаются узел и сеть. В данном случае, будем считать, что рядовые узлы не могут менять настройки, конфигурации сети. Изменять настройки сети может только водитель, обладающий максимальными полномочиями.

Заключение. Исходя из вышеизложенного, ролевая модель позволяет решить ряд проблем контроля и управления доступом в условиях большого числа динамически меняющихся групп пользователей. Также, в части контроля и управления доступом в сетях транспортных средств ролевая модель может быть реализована в сети с изоляцией сетевого трафика. Под изоляцией сетевого трафика понимается группирование нескольких потоков данных с различными характеристиками в рамках одной логической сети (сегментация сети на основе потоков), которая может разделять единую физическую сеть с другими логическими сетями или сетевыми срезами (network slices).

СПИСОК ЛИТЕРАТУРЫ

1. Щеглов А.Ю. Модели, методы и средства контроля доступа к ресурсам вычислительных систем. Учебное пособие.– СПб: Университет ИТМО, 2014. – 95с.
2. Хруслова Д. В. Обзор методов разграничения прав доступа // Новые информационные технологии в автоматизированных системах. 2010. №13.
3. Подходы к контролю доступа: RBAC vs. ABAC [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/company/custis/blog/248649
4. Гусев К. В., Сумкин К. С. Управление правами и потоками в компьютерных сетях // Спецтехника и связь. 2011. №6.
5. SecKit: A Model-based Security Toolkit for the Internet of Things. Ricardo Neisse,Gary Steri,Igor Nai Fovino,Gianmarco Baldini. Computers & Security. Elsevier. October 2015http://www.sciencedirect.com/science/article/pii/S0167404815000887
6. Access Control Models for Cloud-Enabled Internet of Things: A Proposed Architecture and Research Agenda. Ravi Sandhu. http://profsandhu.com/confrnc/misconf/picsoc16-asma-slides.pdf
7. Activity-Based Access Control for IoT. Lyes Touati, Yacine Challal. Workshop on experiences with the design and implementation of smart objects, Sep 2015, Paris, Francehttps://hal.archives-ouvertes.fr/hal-01226167
8. Hernández-Ramos J. L. et al. Distributed capability-based access control for the internet of things //Journal of Internet Services and Information Security (JISIS). – 2013. – Т. 3. – №. 3/4. – С. 1-16.
9. S. Paul, J. Pan, R. Jain. Architectures for the future networks and the next generation internet: a survey. Comput Commun, 34 (1) (2011), pp. 2–42 http://dx.doi.org/10.1016/j.comcom.2010.08.001
10. S. Gusmeroli, S. Piccione, D. Rotondi.A capability-based security approach to manage access control in the internet of things. Math Comput Model, 58 (5) (2013), pp. 1189–1205
11. J.L. Hernandez-Ramos, A.J. Jara, L. Marn, A.F. Skarmeta. Distributed capability-based access control for the internet of things. J Internet Serv Inf Secur (JISIS), 3 (3/4) (2013), pp. 1–16
12. Разработка ролевой модели прав доступа http://www.jetinfo.ru/stati/razrabotka-rolevoj-modeli-prav-dostupa
13. Ferraiolo D. F., Kuhn D. R. (October 1992). "Role Based Access Control". 15th National Computer Security Conference: 554—563.
14. R. Sandhu, D. F. Ferraiolo, and D. R. Kuhn, "The NIST Model for Role Based Access Control: Towards a Unified Standard," In 5th ACM Workshop on Role Based Access Control, Berlin, Germany, 2000, pp. 47-63.
15. American National Standard for Information Technology – Role Based Access Control http://profsandhu.com/journals/tissec/ANSI+INCITS+359-2004.pdf
16. SWOT Analysis of Access Control Models Ennahbaoui Mohammed1 and El Hajji Said. International Journal of Security and Its Applications Vol.8, No.3 (2014), pp. 407-424 http://dx.doi.org/10.14257/ijsia.2014.8.3.39
17. Difference Between MAC and DAC http://www.differencebetween.net/technology/software-technology/difference-between-mac-and-dac/
18. Role Based Access Control (RBAC) vs. Access Control Lists (ACLs) http://www.manasclerk.com/blog/2003/09/30/role-based-access-control-vs-acls/

УДК 621.391.28

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ ИНФОРАСТРУКТУРЫ РФ ОТ КИБЕРАТАК

Мошак Николай Николаевич, Евсейко Константин Владиславович,
Логинцев Александр Владимирович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Россия, Санкт-Петербург, пр.Большевиков, 22
emails: nnmoshak49@mail.ru, kevseiko@gmail.com, logincev_a.v@bk.ru

Аннотация: В статье рассматриваются современные проблемы построения систем мониторинга информационной безопасности в киберпространстве РФ в условиях информационного противоборства.

Ключевые слова: *информационное противоборство, киберпространство, модель угроз, политика информационной безопасности, мониторинг информационной безопасности*

PROBLEMS OF PROTECTION OF INFORMATION AND TELECOMMUNICATION INFORASTRUKTURA OF THE RUSSIAN FEDERATION AGAINST CYBER ATTACKS

Moshak Nikolay Nikolaevich, Evseiko Konstantin Vladyslavovich
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
Russia, St. Petersburg, Bolshevikov pr.,22
emails: nnmoshak49@mail.ru, kevseiko@gmail.com, logincev_a.v@bk.ru

Abstract: In article modern problems of creation of systems of monitoring of information security in a cyberspace of the Russian Federation in the conditions of information confrontation are considered.

Keywords: *information confrontation, cyberspace, model of threats, politician of information security, monitoring of information security*

Введение. В настоящее время очевидным является тот факт, что информационное противоборство (ИП) в киберпространстве становится неотъемлемой частью внешней политики развитых государств. Причем, его масштабы в современных условиях растут непрерывно и уже требуют рассмотрения ИП как самостоятельной формы межгосударственного противостояния. Первоочередными объектами кибератак становятся элементы информационно-телекоммуникационной инфраструктуры (ИТКИ) РФ: информационно-телекоммуникационные сети специального назначения и их автоматизированные системы управления (АСУ) - АСУ связью, АСУ объектами критической информационной инфраструктуры РФ (электросети, системы управления транспортом и т. п.). В этих условиях проблема обеспечения информационной безопасности киберпространства РФ становиться одной из ключевых, т.к. невыполнение требований по его гарантированной защите от киберугроз создает реальные предпосылки срыва или перехвата военного и/или государственного управления. Растущая степень информатизации критически важных объектов, развитие и конвергенция информационных и телекоммуникационных технологий, а также растущие возможности сил и средств вероятного противника в области ИП в киберпространстве РФ, требует тщательного концептуального обоснования и построения его политики информационной безопасности (ИБ). В этой связи становиться актуальным рассмотрение и учет основных проблем безопасности в информационно-телекоммуникационной инфраструктуре РФ на современном этапе развития информационного общества, а также обоснование выбора решений в области мониторинга ИБ на основе разрабатываемых российских специализированных систем.

Основные этапы построения политики ИБ любого элемента информационно-телекоммуникационной инфраструктуры РФ включают в себя [1]:

— описание объекта защиты;

— определение основных приоритетов информационной безопасности;

— оценка рисков с учетом ранжирования активов по уровню важности;

— определение модели нарушителя;

— определение модели угроз информационной безопасности, с учетом нарушения активов базовых услуг безопасности: конфиденциальность и целостность и доступность;

— определение перечня требований ИБ элемента ИТКИ РФ;

— разработка комплекса организационно-технических мер по реализации требований и построению системы защиты;

— разработка организационно-технической схемы контроля состояния ИБ элемента информационно-телекоммуникационной инфраструктуры РФ.

Структурная схема процесса разработки политики ИБ элемента информационно-телекоммуникационной инфраструктуры РФ показана на рис.1.

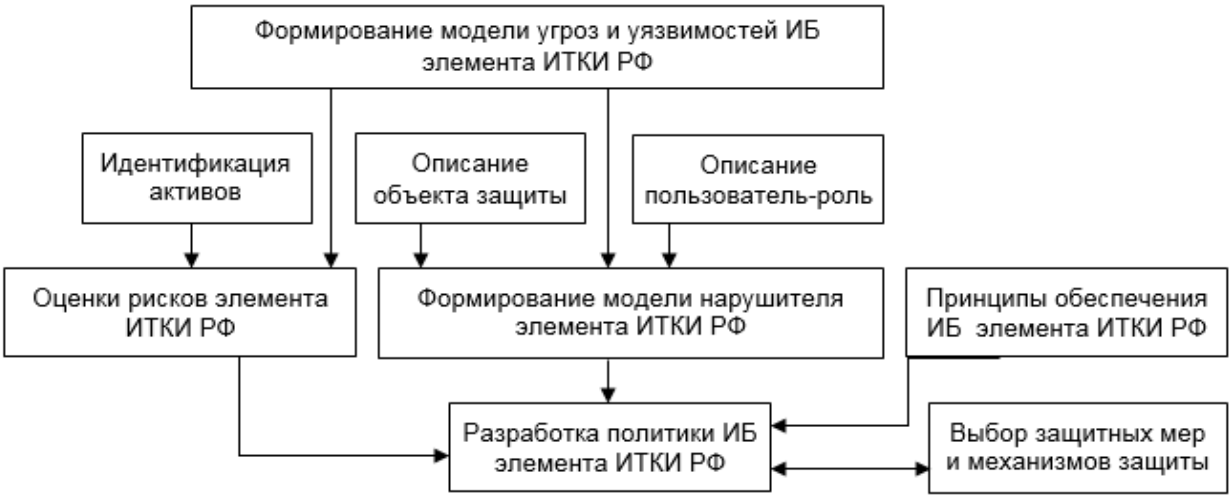


Рис.1. – Структурная схема процесса разработки политики ИБ элемента информационно-телекоммуникационной инфраструктуры РФ

К объектам защиты киберпространства РФ относятся: информационные ресурсы, содержащие информацию, составляющую государственную, коммерческую тайну и другие конфиденциальные данные, а также открытую информацию; системы формирования, хранения, передачи и использования информационных ресурсов (информационные системы, библиотеки, архивы, базы и банки данных, информационные технологии, различные регламенты, обслуживающий персонал); информационная структура, включающая центры обработки и анализа информации; комплексы средств автоматизации (КСА), каналы связи и оборудование телекоммуникационной инфраструктуры (концентраторы, коммутаторы, маршрутизаторы, мультиплексоры, межсетевые экраны и т. д.), а также механизмы, обеспечивающие их функционирование, в том числе системы и средства защиты информации.

В основе разработки требований политики ИБ информационно-телекоммуникационной инфраструктуры РФ и ее элементов лежат приоритеты безопасности (защиты) их ресурсов (активов): доступность; целостность; конфиденциальность. В современном киберпространстве существенно возрастает важность угроз нарушения доступности и целостности ресурсов. Киберугрозы включают не только три базовых типа угроз перечисленным выше услугам безопасности, но и формируют четвертый тип угроз - нарушение функционирования инфраструктурных объектов, которое может проявляться как в отказе обслуживания, так и в изменении алгоритмов управления кибернетическими элементами (перехват управления), например, за счет несанкционированной активизации внедренного вредоносного программного обеспечения (ПО). Особенно это касается специализированного комплексного вредоносного ПО (например, вирусов типа Stuxnet и Flame), ориентированного на решение специальных задач по компрометации конкретных систем и ресурсов с разведывательными, деструктивными, диверсионными и другими целями. Сущность нарушения устойчивости функционирования информационно-телекоммуникационной инфраструктуры РФ в условиях компьютерных атак заключается в том, что несвоевременно выполняется технологические циклы управления ее компонентами или инфраструктурными объектами (вводится искусственное замедление).

Направленные воздействия на инфраструктурные объекты с целью нарушения их функционирования возможно осуществить через следующие элементы:

– сетевые и коммуникационные каналы;

– порты тестирования микросхем (Test Access Port - TAP). Широко распространенным стандартным портом тестирования является Boundary Scan (JTAG) IEEE 1149.1-2001 и IEEE 1149.6-2003 порт;

– ПЗУ начальной загрузки (обновлении программы BIOS);

– периферийные интерфейсы, такие как SATA, USB и др.;

– встроенные на этапе изготовления микросхем, модулей и ЭВМ аппаратные «закладки», исполнительные механизмы которых могут иметь различную целевую направленность по реализации нанесения потенциального ущерба функциям информационно-телекоммуникационной инфраструктуры РФ, в том числе полное ее блокирование.

Следует отметить, что отсутствие выхода отдельных инфраструктурных элементов киберпространства РФ в глобальную сеть Интернет не гарантирует защиту от проникновения вредоносного программного обеспечения типа Stuxnet и Flame, которое может быть внесено внутренним легальным нарушителем через USB-интерфейс вычислительных средств. На настоящий момент минимизация остаточных рисков наличия вредоносного кода в программных изделиях КСА специального назначения элементов информационно-телекоммуникационной инфраструктуры РФ

обеспечивается проведением сертификационных испытаний (тематических исследований) в различных государственных системах сертификации, например, ФСТЭК России и др.

Внедрение технологий третьей платформы информатизации (ТПИ) одновременно с предоставлением многих недоступных ранее информационных услуг создает и угрозы нового типа[2]. Это обстоятельство стало одной из основных предпосылок создания новой доктрины информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. №646. Анализ приведенного в новой доктрины ИБ Российской Федерации перечня блоков угроз показывает, что эффективность защиты информационных интересов РФ напрямую зависит от внедрения технологий ТПИ, элементами которой являются (рис. 2):

– облачные вычисления, безопасность которых связана с виртуализацией логически разделяемых вычислительных процессов и физических вычислительных ресурсов;

– интернет вещей, ставших частью киберпространства, безопасность которых связана с соединением физических вещей с цифровыми сенсорами, с объединением аналогового мира и его цифрового описания, что заставляет обеспечивать информационно-энергетическую, информационно-транспортную, информационно-производственную и, в целом, информационно-экономическую безопасность;

– большие данные, безопасность которых связана с возможностью путем их обработки, в том числе и с деструктивными целями, делать достаточно точные статистические оценки о состоянии дел во всех областях деятельности государств, а также силовых министерств и ведомств РФ;

– мобильный широкополосный доступ, безопасность которого связана с отсутствием границы сети, на которой можно было бы блокировать атаки;

– наложенные сервисы, безопасность которых связана, помимо традиционных угроз (Web-атаки, фишинг и др.), с появлением рисков и угроз при обезличивании пользователей в социальной сети и необходимо учитывать, что процессы и тематика общения в социальных сетях могут быть намеренно организованы противником, использующим средства социальной инженерии.

Услуги третьей платформы информатизации	Угрозы нового типа
Облачные вычисления	Угрозы, связанные с виртуализацией логически разделяемых вычислительных процессов и физических вычислительных ресурсов
Интернет-вещи	Угрозы, связанные с соединением физических вещей с цифровыми сенсорами, с объединением аналогового мира и его цифрового описания
Большие данные	Угрозы, связанные с обработкой больших данных в деструктивных целях
Мобильный широкополосный доступ	Угрозы, связанные с отсутствием границы сети, на которой можно было бы блокировать атаки
Наложенные сервисы	Угрозы, связанные с обезличиванием пользователей в социальной сети

Рис.2 - Услуги третьей платформы информатизации и угрозы нового типа

Рассмотренные проблемы безопасности в киберпространстве РФ ставят на повестку дня ускоренное внедрение технических и организационно-технических систем мониторинга ИБ киберпространства РФ, которые выступают в статусе вспомогательных («индикативно-сенсорных») по отношению к базовым системам защиты и являются одним из компонентов систем контроля защищенности информационно-телекоммуникационной инфраструктуры РФ. Указанные системы позволяют нейтрализовать потенциальные киберугрозы путем оперативного устранения ее уязвимостей. В этой связи мы приходим к выводу о необходимости внедрения в киберпространство РФ независимых средств или так называемых доверенных средств мониторинга ИБ [1,3]. Система независимого мониторинга ИБ представляет собой специально разработанные программные средства, основу которых составляют программные агенты (сенсоры), функционирующие на уровне драйверов соответствующих операционных систем. Необходимо отметить, что независимый мониторинг часто является единственным инструментом контроля так называемых легальных привилегированных пользователей информационно-телекоммуникационной инфраструктуры и ее элементов, а именно, в тех случаях, когда невозможно ограничить выполнение ими несанкционированных/деструктивных действий не лишив их при этом необходимой административной функциональности.

Учитывая значительный объем данных аудита, поступающих от различных контролируемых элементов информационно-телекоммуникационной инфраструктуры, а также многообразие требований политик ИБ, которые должны быть отслежены через эти данные, становится очевидной необходимость автоматизации процесса их анализа. При этом службу ИБ интересуют ответы хотя бы на три вопроса, связанные с этим же инцидентом:

— «Какие свойства безопасности информационных активов были нарушены?»;

— «Какой ущерб нанесен и его величина?»;

— «Не является ли произошедший инцидент следствием злоумышленной активности?».

Для ответа на эти вопросы требуется углубленный анализ предшествующих и последующих событий с целью поиска причинно-следственных связей между ними. Также необходимы подробные сведения о затронутых активах и операциях с ними, причастном персонале и т. п., то есть обо всем, что образует контекст события-инцидента.

Продукты для автоматизации сбора и анализа событий безопасности, с помощью которых администраторы информационной безопасности (АИБ) могут получить на консоли управления осмысленную информацию, выделяют в класс решений управления информацией безопасности (Securite Information Management, SIM) - обеспечивает сбор, хранение и анализ данных (взятых из журналов), подготовка отчетов по соответствию нормативным требованиям или (Securite Information and Event Managemen, SIEM) - обеспечивает в реальном времени мониторинг событий безопасности, выявление и реагирование на инциденты безопасности. Они решают проблему обработки больших объемов данных, генерируемых различными платформами, системами и приложениями безопасности. Системы SIM (SIEM) агрерируют и приоретизируют данные, получаемые с различных устройств и программных систем (межсетевых экранов, систем обнаружения вторжений, антивирусов, коммутаторов, маршрутизаторов и проч.), обрабатывают разнородную информацию, используют правила корреляции (позволяющие выделить взаимосвязанные процессы во всей системе), производят анализ и визуализацию. Результат их работы - информация, на основе которой можно принимать те или иные решения, управлять событиями или расследовать инциденты. АИБ получают возможность визуализировать операции в сети, определить степень уязвимости ресурсов и выводить отчеты по аудиту безопасности.

На российском рынке предлагаются ряд систем указанного класса (Symantec Security Information Manager (SSIM) компании Symantec; Netforensics Security Information & Event Management Solotion (nFX SIM One) компании net Fore nsics; Intelli tactics SAFE компании Intell I tactics; RSA enVision компании RSA Security; Check Point Eventia Analyzer компании Check Point; IBM Tivoli Security Operation Manager компании IBM; ArcSight Logger компании ArcSight ; ArcSight Express компании ArcSight и др.). Между тем, несмотря на необходимость регулярного мониторинга рисков элементов киберпространства, вряд ли продукты SIM (SIEM) позволят в ближайшее время преодолеть такие проблемы, как отсутствие комплексного подхода к обеспечению ИБ, избыточность одних функций защиты и недостаточность других, поддержка из разных источников. Кроме того, использование решений SIM (SIEM) в нашей стране связано с некоторыми ограничениями. Непростую задачу представляет и сопровождение таких систем. Это требует обучения специалистов заказчика или аутсорсинга сопровождения SIM (SIEM). В некоторых случаях необходима также увязка SIM (SIEM) с продуктами отечественных разработчиков.

В свете государственной политики импортозамещения в различных сферах народнохозяйственной деятельности ниже рассматриваются причины, препятствующие созданию решений в области ИБ на основе стандартных иностранных продуктов, в частности, обоснование выбора для целей контроля действий администраторов и пользователей решений на основе разрабатываемых российских специализированных систем в противовес решениям на базе стандартных продуктов ведущих иностранных производителей. При этом рассматривается только техническая сторона вопроса, хотя можно предположить, что экономическая сторона вопроса, при попытке решить проблему доработки стандартного импортного продукта, также окажется существенным фактором.

1. Необходимость получения событий мониторинга ИБ от новых источников данных или применения новых способов сбора (доставки) информации о событиях (специализированных интерфейсов, нетиповых протоколов).

В специализированных средствах разрабатываемых российских систем на возможность подключения новых источников данных решается в рамках функционального развития этих систем после согласования Заказчиком предлагаемых решений.

Реализовать подобные решения в стандартных импортных продуктах возможно силами подрядных организаций за счет создания ПО так называемых «адаптеров», выполняющих функции конвертирования событий мониторинга ИБ из журналов ИАС/АСУ (т.е. новых источников) во внутренний формат продукта. Как правило, стандартные импортные продукты предоставляют возможности написания адаптеров, публикуя для этого API, однако, при создании адаптера для журналов конкретной системы предоставленных возможностей может оказаться недостаточно, и возникнет необходимость привлечения производителя продукта. Однако в силу разных причин создать новые адаптеры невозможно.

Проблема получения информации от новых источников в условиях России, когда используется покупное ПО, разработанное с учетом западных стандартов, весьма актуальна. И особенно это актуально для продуктов, применяемых в области ИБ, поскольку по Российскому законодательству в некоторых областях, например, связанных с криптографией, использовать зарубежные аппаратные средства и ПО просто нельзя. В стандартных продуктах не предусмотрена возможность импорта и анализа регистрационных журналов от российских средств ИБ.

2 . Необходимость получения дополнительной информации об условиях и ситуации, связанной с возникновением событий (установления контекста событий), вызванная спецификой анализа и оценки событий ИБ, а также адекватной их интерпретацией.

Для установления контекста событий ИБ чаще всего требуется сбор дополнительных событий мониторинга, связанных с этим контекстом. Возможности сбора дополнительных событий мониторинга ИБ, как правило, в принципе не могут быть решены для стандартных импортных продуктов написанием адаптеров, поскольку требуют специальных возможностей, например, перехвата системных вызовов в ОС.

Адаптеры стандартных продуктов предназначены только для изменения формата представления события мониторинга ИБ из штатных журналов приложений ИАС, но никак не могут заменить формирование новых событий и при необходимости взять дополнительную информацию, необходимую для контроля и анализа, путем перехвата системных вызовов.

Проблема установления контекста возникает из-за неопределенностей и неоднозначности информации, связанной с событиями, регистрируемыми в штатных журналах регистрации платформ и приложений. А именно, события с одним и тем же кодом генерируются по разным ситуациям, возникшим в системе, программе, приложении. При этом предполагается, что этой информации достаточно, поскольку основным назначением такой записи в журнале регистрации является просто сигнал о нештатной (или штатной) ситуации. Если необходимо в этой ситуации разобраться подробнее, например, чтобы найти ошибку или другую причину ее возникновения, то ситуация должна быть повторена, а программное обеспечение при этом должно быть переведено в специальный отладочный режим с подробным протоколированием промежуточных данных, трассировкой исполнения программы или системных вызовов и т. п. Затем отладочная информация (фактически контекст события) анализируется специалистами разработчика ПО на стендах. Таким образом, контекст события при необходимости формируется и анализируется в «лабораторных» условиях.

Но эта схема не подходит для целей безопасности, потому, например, что ситуацию, специально созданную злоумышленником, возможно, с применением какого-то уникального инструментария, повторить невозможно. Она возникает один раз во время проведения атаки. Весьма примечательно, что цели безопасности не учитываются разработчиками ПО даже в тех случаях, когда дополнительная информация о событии могла бы быть включена без особых затрат.

3. Необходимость контроля работы приложений, не формирующих собственный журнал регистрации событий.

Если по условиям вновь утвержденной или введенной в действие политики ИБ, возникает потребность контроля приложений ИАС/АСУ, не формирующих собственного журнала регистрации событий, то такая ситуация принципиально неразрешима с использованием стандартных импортных продуктов, поскольку приводит к необходимости формирования нужных для контроля событий средствами этого продукта. Здесь единственной возможностью для получения событий мониторинга ИБ является перехват системных вызовов.

Возможность доработки стандартных импортных продуктов в части формирования новых событий, не генерируемых штатными средствами регистрации ОС и приложений, ограничена. Кроме того, в подавляющем большинстве случаев, при необходимости контроля приложений ИАС, не формирующих собственных регистрационных журналов, требуется участие разработчиков стандартного продукта.

4. Необходимость в специализированных средствах анализа и генерации отчетов, потребности по их доработке, переработке и оптимизации.

В случае специализированных средств разрабатываемых российских систем мониторинга ИБ такая оптимизация или доработки предусматриваются в рамках сопровождения или функционального развития. Возможности анализа и отчетности в стандартных продуктах хоть и разнообразны, но также ограничены. Доработка или адаптация видов отчетности по пожеланиям Заказчика требуют участия разработчиков и вряд ли возможны.

5. Необходимость защиты данных мониторинга от таких угроз как:

— действия администраторов по отключению процессов, осуществляющих сбор данных о событиях мониторинга ИБ;

— модификация, уничтожение данных о событиях мониторинга ИБ;

— подмена актуальных данных данными, сформированными ранее.

В системах мониторинга ИБ отечественной разработки возможна реализация комплекса мер противодействия данным угрозам.

Заключение. Рассмотренные проблемы безопасности и новые типы угроз в киберпространстве РФ на современном этапе развития информационного общества должны быть учтены в типовых моделях нарушителей и угроз при построении политики ИБ информационно-телекоммуникационной инфраструктуры страны [4]. При этом выбор решений в области мониторинга ИБ должен базироваться на основе разрабатываемых российских специализированных систем в противовес решениям на базе стандартных продуктов ведущих иностранных производителей.

СПИСОК ЛИТЕРАТУРЫ

1. Мошак Н.Н., Тимофеев Е.А. Особенности построения политики информационной безопасности в инфокоммуникационной сети // «Электросвязь», №9, 2005.
2. Колбанёв А.М., Колбанёв М.О., Цехановский В.В. Проектирование корпоративных информационных систем. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2016. - с.192
3. Мошак Н.Н., Тимофеев Е.А. Модели и методы анализа данных мониторинга автоматизированных систем. «Электросвязь», №4, 2008
4. Мошак Н.Н., Яшин А.И., Иванов В.И. Модели нарушителя и угроз в автоматизированных информационных системах специального назначения на технологии «клиент-сервер». «Телекоммуникационные технологии». Вып. 2(142) – СПб.: ОАО «НИИ «Рубин», 2014, инв.№в-760с – с. 50-65.

УДК 621.391.28

МЕТОДЫ РАСЧЕТА КВАНТИЛЕЙ РАСПРЕДЕЛЕНИЯ СЛУЧАЙНОЙ СЕТЕВОЙ ЗАДЕРЖКИ ПАКЕТОВ ИЗОХРОННОГО ТРАФИКА В ЗАДАЧЕ АНАЛИЗА ИНФОКОММУНИКАЦИОННЫХ ТРАНСПОРТНЫХ СИСТЕМ

Мошак Николай Николаевич, Логинцев Александр Владимирович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Россия, Санкт-Петербург, пр.Большевиков, 22
emails: nnmoshak49@mail.ru, logincev_a.v@bk.ru

Аннотация: В статье формулируется и обосновывается «квантильный» подход к качеству обслуживания изохронного трафика в пакетной мультисервисной сети в режиме сессии. Предложены методы расчета квантилей распределения случайной сетевой задержки пакетов речевого трафика, используемые при расчете вероятности непревышения требуемого времени доставки пакетов указанного класса в инфотелекоммуникационной транспортной системе, которая гарантирует необходимую изохронность передачи.

Ключевые слова: *мультисервисная сеть, инфокоммуникационная транспортная система, квантиль распределения случайной величины, методы расчета квантилей распределения случайной величины*

METHODS OF CALCULATION OF QUANTILES OF DISTRIBUTION OF THE CASUAL NETWORK DELAY OF PACKAGES OF ISOCHRONOUS TRAFFIC IN THE TASK OF THE ANALYSIS OF THE INFOCOMMUNICATION TRANSPORT SYSTEMS

Moshak Nikolay Nikolaevich, Logincev Aleksander Vladimirovich
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
Russia, St. Petersburg, Bolshevikov pr.,22
emails: nnmoshak49@mail.ru, logincev_a.v@bk.ru

Abstract: In article "quantile" approach to quality of service of an isochronous traffic on a package multiservice network in the session mode is formulated and justified. The methods of calculation of quantiles of distribution of accidental cross-network delay of packets of the voice traffic used when calculating probability of not exceeding of the required time of delivery of packets of the specified class in the infotelekommunikation transport system which guarantees necessary isochronism of transmission are offered..

Keywords: *multiservice network, infocommunication transport system, quantile of distribution of a random variable, methods of calculation of quantiles of distribution of a random variable*

Введение. В качестве базовой структурно-сетевой задачи, как правило, выступает задача оптимизации структуры, которая включает в свой состав как минимум три частные задачи (рис.1) [1]:

— выбор топологии графа, заключающийся в определении оптимального числа вершин и ребер, соединяющих вершины;

— распределение приоритетных потоков (РПП), сводящееся к поиску оптимальных маршрутов передачи потоков информации и расчету интенсивностей потоков в отдельных линейно-цифровых трактах (ЛЦТ). При этом задача РПП может включать в себя задачу ограничения порогов нагрузки по внешнему трафику каждого класса;

— выбор пропускных способностей (ВПС) ЛЦТ сети из заданного дискретного ряда.

Задача анализа инфотелекоммуникационной транспортной системы (ИТС) мультисервисной сети [2-6] по сути является задачей распределения многопродуктовых приоритетных потоков и имеет два прикладных аспекта: расчет удельной загрузки ЛЦТ трафиком различной природы ρ_{ij}^{k} и оценку вероятностно-временных характеристик (ВВХ) ИТС. Оптимизация сети одновременно по потокам и пропускной способности V_{ij} есть задача ВПС. В статье рассмотрены методы расчета квантилей распределения случайной сетевой задержки пакетов в ИТС, которые могут быть использованы при решении задачи ее анализа.

Аналитическое описание показателей качества обслуживания изохронного трафика в пакетной мультисервисной сети

Состав показателей качества обслуживания QoS, ограничения на значения которых должны учитываться в процессе создания ИКС, подробно рассмотрены в [2-5]. В роли ограничений на значения показателей качества обслуживания изохронного трафика в сессии в существующих моделях ИТС выступает заданная вероятность d^B непревышения требуемого времени Θ^B доставки пакета указанного класса в сети $\Pr\{t \geq \Theta^B\} \leq d^B$,которая гарантирует необходимую изохронность передачи. Если обозначить $T^B_{st,m}$ случайную задержку речевого пакета в m–ом виртуальном канале тракта $st \in S^B$ с вероятностью $p^B_{st,m}$множества последовательно-параллельной схемы виртуальных соединений L^B_{st} дерева путей R_{st}, T^B_{st}- случайную величину вида $T^B_{st} = \sum_{m=1}^{M^B_{st}} p^B_{st,m}\, T^B_{st,m}$, а соответствующие им функции распределения $F^B_{st,m}(t) = \Pr\{T^B_{st,m} \leq t\}$ и $F^B_{st}(t) = \Pr\{T^B_{st} \leq t\}$, то в силу эквивалентности дерева путей R_{st} тракта и последовательно-параллельной схемы виртуальных соединений L_{st} [2] $F^B_{st}(t) = \sum_{m=1}^{M^B_{st}} p^B_{st,m} F^B_{st,m}(t)$. Соответствующая плотность распределения равна $f^B_{st}(t) = \sum_{m=1}^{M^B_{st}} p^B_{st,m} f^B_{st,m}(t)$,где $f^B_{st,m}(t) = \frac{dF^B_{st,m}(t)}{dt}$. Искомая вероятность превышения задержки вычисляется по следующей формуле: $\Pr_{st}\{t \geq \theta^B_{st}\} = \sum_{m=1}^{M^B_{st}} p^B_{st,m} \int_{\theta^B_{st}}^{\infty} f^B_{st,m}(t)\, dt$. Интегрируя и подставляя пределы интегрирования, получим $\Pr_{st}\{t \geq \theta^B_{st}\} = \sum_{m=1}^{M^B_{st}} p^B_{st,m}(1 - F^B_{st,m}(\theta^B_{st}))$, $\forall st \in S^B$: $a^{B,a}_{st} \neq 0$. Квантили $F^B_{st,m}(\theta^B_{st})$ легко вычисляются при принятых предположениях. Пусть функция распределения вероятностей времени пребывания пакета класса В $F^B_{ij}(t)$ в канале ij имеет экспоненциальный характер. В этом случае ребрам m-го пути $l_{st,m}\{si_1, i_1 i_2, \dots, i_{p-1} t\}$ тракта $st \in S^B$соответствуют параметры экспоненциального распределения времени задержки пакетов $\mathrm{l_{st,m}}\{\mu^{\mathrm{B}}_{\mathrm{si_1}}(1-\rho^{\mathrm{B}}_{\mathrm{si_1}}), \mu^{\mathrm{B}}_{\mathrm{i_1 i_2}}(1-\rho^{\mathrm{B}}_{\mathrm{i_1 i_2}}), \dots, \mu^{\mathrm{B}}_{\mathrm{i_{p-1} t}}(1-\rho^{\mathrm{B}}_{\mathrm{i_{p-1} t}})\}$. Дифференциальная функция распределения имеет вид: $\mathrm{f^B_{ij}(t) = \mu^B_{ij}(1-\rho^B_{ij}) e^{-\mu^B_{ij}(1-\rho^B_{ij})t}}$, где $\mu^{\mathrm{B}}_{\mathrm{ij}} = \frac{\mathrm{V_{ij}}}{\mathrm{L^B + H_{NA}}}$ – величина, обратная средней длительности обслуживания речевого пакета в каждой отдельной СМО типа M/M/1 тракта $st \in S^B$. Одностороннее преобразование Лапласа-Стилтьеса дифференциальной функции распределения: $\mathrm{f^{*B}_{ij}(s) = \int_0^\infty e^{-st}\, dF^B_{st,m}(t) = \frac{\mu^B_{ij}(1-\rho^B_{ij})}{s+\mu^B_{ij}(1-\rho^B_{ij})}}$. Поскольку случайные величины $\mathrm{t_{ij}}$ $(\mathrm{ij} \in \mathrm{l^B_{st,m}})$ времени задержки пакета класса B в отдельных ЛЦТ пути $\mathrm{l^B_{st,m}}$ определены на одном вероятностном пространстве и в силу предполагаемой независимости задержек в отдельных ЛЦТ пути $\mathrm{l^B_{st,m}}$ и учетом предположений относительно распределения времени задержек пакетов в отдельных ребрах пути $\mathrm{l^B_{st,m}}$, дифференциальная функция распределения времени задержки пакета класса В в -ом виртуальном пути имеет вид: $\mathrm{f^B_{st,m}(t) = f^B_{st,m}\left(\sum_{ij \in l^B_{st,m}} t_{ij}\right) = \mathcal{L}^{-1}\{f^{*B}_{st,m}(s)\}}$

$$f^{*B}_{st,m}(s) = \prod_{ij \in l^B_{st,m}} \frac{\mu^B_{ij}(1-\rho^B_{ij})}{s+\mu^B_{ij}(1-\rho^B_{ij})}. \quad (1)$$

Обращение этого преобразования дает плотность вероятности $f^B_{st,m}$ сквозного времени пребывания θ^B речевого пакета в тракте $st \in S^B$ двухполюсной сети, представляющую собой i кратную свертку в виде произведения дробно-рациональных функций. В общем виде $f^B_{st,m}(t) = \mathcal{L}^{-1}\left\{\prod_{ij \in l^B_{st,m}} \frac{\mu^B_{ij}(1-\rho^B_{ij})}{s+\mu^B_{ij}(1-\rho^B_{ij})}\right\}$, $\mathcal{L}^{-1}$ обратное преобразование Лапласа. К результатам свертки распределений времени передачи пакета прибавляется среднее время обработки пакета на УК, время, затраченное на предоставления механизмов защиты [3] и т.п. Суммарное время есть время передачи и обработки пакета (сообщения), фиксирующее заданный квантиль. Для каждой корреспондирующей пары при вычислении ограничений количество свертываемых функций определяется длиной пути $\mathrm{l_{st,m}}$. Отметим, что свертка плотностей функций распределения времени пребывания пакета в канале вычисляется с использованием преобразования Лапласа и ее изображение предоставляет собой дробно-рациональную функцию.

Методы вычисления плотности вероятности распределения времени задержки изохронных пакетов в сети

Для обращения $f^k_{st}(s)$ можно применить как прямой метод получения плотности вероятности распределения времени задержки в тракте $st \in S^B$, связанный с вычислением в явном виде указанных распределений для заданной конфигурации корней так и итерационный метод, основанный на численном взятии неопределённых интегралов, возникающих при вычислении свёрток экспоненциальных распределений. Первый вариант является более точным и быстродействующим, однако требует для своей реализации большой предварительной аналитической работы. Другой метод с вычислительной точки зрения является более медленным, но не имеет ограничений на длину пути.

Основную трудность для получения вероятности превышения заданного уровня задержки в тракте передачи $st \in S^B$составляет машинная обработка преобразования $f^{*B}_{st,m}(s)$. Для выполнения

обратного преобразования применим метод разложения на простые дроби. Пусть $a_{ij}^{B} = \mu_{ij}^{B}(1-\rho_{ij}^{B})$. Выражение

$$R(s) = \prod_{ij \in l_{st,m}^{B}} \frac{a_{ij}}{s + a_{ij}}$$

представляет собой правильную рациональную дробь, которая может быть представлена в виде суммы простейших дробей

а) для случая $a_{si_1} \neq a_{i_1 i_2} \neq \cdots \neq a_{i_{p-1}t}$

$$R(s) = \frac{A_{si_1}}{(s + a_{si_1})} + \frac{A_{i_1 i_2}}{(s + a_{i_1 i_2})} + \cdots + \frac{A_{i_{p-1}t}}{(s + a_{i_{p-1}t})}.$$

б) для случая когда заменатель дроби $R(s)$ может быть представлен в виде $(s + a_{i_n i_{n+1}})^b (s + a_{i_m i_{m+1}})^c \ldots (s + a_{i_r i_{r+1}})^d$ (число множителей вида $(s + a_{ij})^n \leq$ числа последовательно включенных СМО типа M/M/1, составляющих -ый виртуальный путь)

$$R(s) = \frac{A_{si_1}}{(s + a_{i_n i_{n+1}})^b} + \frac{A_{i_1 i_2}}{(s + a_{i_n i_{n+1}})^{b-1}} + \cdots + \frac{A_{i_n i_{n+1}}}{(s + a_{i_n i_{n+1}})} + \frac{A_{i_{n+1} i_{n+2}}}{(s + a_{i_m i_{m+1}})^c} + \cdots + \frac{A_{i_m i_{m+1}}}{(s + a_{i_m i_{m+1}})} + \cdots + \frac{A_{i_r i_{r+1}}}{(s + a_{i_r i_{r+1}})^d} + \cdots + \frac{A_{i_{p-2} i_{p-1}}}{(s + a_{i_r i_{r+1}})^2} + \frac{A_{i_{p-1}t}}{(s + a_{i_r i_{r+1}})},$$

где A_{ij} $(ij \in l_{st,m}^{B})$ - неизвестные коэффициенты, которые находятся путем приведения суммы справа к общему знаменателю и последующего приравнивания полученного числителя к числителю $R(s)$ (число неизвестных коэффициентов равно числу последовательно включенных СМО типа M/M/1, составляющих -ый виртуальный путь).

В результате получаем равенство

$$\begin{aligned}
&A_{si_1}(s + a_{i_m i_{m+1}})^c \ldots (s + a_{i_r i_{r+1}})^d + A_{i_1 i_2}(s + a_{i_n i_{n+1}})(s + a_{i_m i_{m+1}})^c \ldots (s + a_{i_r i_{r+1}})^d + \cdots \\
&+ A_{i_n i_{n+1}}(s + a_{i_n i_{n+1}})^{b-1}(s + a_{i_m i_{m+1}})^c \ldots (s + a_{i_r i_{r+1}})^d \\
&+ A_{i_{n+1} i_{n+2}}(s + a_{i_n i_{n+1}})^b \ldots (s + a_{i_r i_{r+1}})^d + \cdots \\
&+ A_{i_m i_{m+1}}(s + a_{i_n i_{n+1}})^b (s + a_{i_m i_{m+1}})^{c-1} \ldots (s + a_{i_r i_{r+1}})^d + \cdots \\
&+ A_{i_r i_{r+1}}(s + a_{i_n i_{n+1}})^b \ldots (s + a_{i_m i_{m+1}})^c + \cdots \\
&+ A_{i_{p-2} i_{p-1}}(s + a_{i_n i_{n+1}})^b (s + a_{i_m i_{m+1}})^c \ldots (s + a_{i_r i_{r+1}})^{d-2} \\
&+ A_{i_{p-1}t}(s + a_{i_n i_{n+1}})^b (s + a_{i_m i_{m+1}})^c \ldots (s + a_{i_r i_{r+1}})^{d-1} = \prod_{ij \in l_{st,m}^{B}} a_{ij}
\end{aligned}$$

Раскрывая скобки и приравнивая выражения получаем систему линейных уравнений относительно неизвестных коэффициентов:

$$\begin{cases}
x_{11}A_{si_1} + x_{12}A_{i_1 i_2} + \cdots + x_{1n}A_{i_{p-1}t} = \prod_{ij \in l_{st,m}^{B}} a_{ij} \\
x_{21}A_{si_1} + x_{22}A_{i_1 i_2} + \cdots + x_{2n}A_{i_{p-1}t} = 0 \\
\cdots \cdots \cdots \\
x_{k1}A_{si_1} + x_{k2}A_{i_1 i_2} + \cdots + x_{kn}A_{i_{p-1}t} = 0
\end{cases},$$

где x_{kn} – коэффициенты при искомых аргументах A_{ij}. Число линейных уравнений k равно числу неизвестных коэффициентов или числу последовательно включенных СМО типа M/M/1, составляющих -ый виртуальный путь. Для решения данной системы уравнений можно воспользоваться методом Гаусса.

Метод Гаусса состоит из 2 этапов:

1. Составление расширенной матрицы, состоящей из коэффициентов при неизвестных и свободных коэффициентов:

$$\begin{bmatrix}
x_{11} & x_{12} & \ldots & x_{1n} & b_1 \\
x_{21} & x_{22} & \ldots & x_{21} & b_2 \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
x_{k1} & x_{k2} & \ldots & x_{kn} & b_k
\end{bmatrix}$$

Приведение расширенной матрицы с помощью элементарных преобразований:

– Перестановка строк и столбцов;
– Умножение строки/столбца на число отличное от нуля;
– Прибавление к одной строке/столбцу другой строки/столбца к диагональной матрице вида:

$$\begin{bmatrix} 1 & 0 & \dots & 0 & A_{si_1} \\ 0 & 1 & \dots & 0 & A_{i_1 i_2} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & A_{i_{p-1} t} \end{bmatrix},$$

где $A_{ij}\left(ij \in l_{st,m}^{B}\right)$ – решение системы линейных уравнений.

Рассчитать коэффициенты при неизвестных в расширенной матрице можно по следующей итерационной схеме. Пусть d^{max}- число множителей вида $(s+a_m)$ в знаменателе простейшей дроби, которой соотвествует коэффициент A_n (n – номер столбца в расширенной матрице), $m = 1 \dots d^{max}$. x_{iA_n}- вектор коэффициентов, соответствующий столбцу A_n расширенной матрицы.

Перед началом задаем $x_{1A_n} = 1, m = 1$.

1. Задаем границы подцикла $i_{max} = m+1, i = 1$.
2. Если $i = 1$, то $x_{iA_n} = x_{iA_n} * a_m$;
3. Если $i = m$ (при условии что $i \neq 1$), то $x_{iA_n} = x_{i-1,A_n} + a_m$;
4. Если $i = m+1$, то $x_{iA_n} = 1$;
5. В других случаях $x_{iA_n} = x_{iA_n} * a_m + x_{i-1,A_n}$.
6. Увеличиваем i на 1 и, если $i \leq i_{max}$, возвращаемся на шаг 2, иначе переходим на шаг 4.
7. Увеличиваем m на 1 и , если $m \leq d^{max}$, вовращаемся на шаг 1, иначе “конец”.

Данную итерационную схему можно получить рассматривая результат пошагового умножение множителей вида $(s+a_m)$. Из всего выше сказанного получаем:

$$f_{st,m}^{*B}(s) = \sum_{ij \in l_{st,m}^{B}} \frac{A_{ij}}{\left(s + \mu_{ij}^{B}\left(1-\rho_{ij}^{B}\right)\right)^{n}}, \text{ где } n - \text{степень знаменателя простейшей дроби}$$

$$f_{st,m}^{B}(t) = \sum_{ij \in l_{st,m}^{B}} A_{ij}\, \mathcal{L}^{-1}\{\frac{1}{(s+\mu_{ij}^{B}\left(1-\rho_{ij}^{B}\right))^{n}}\}$$

$$\mathcal{L}^{-1}\left\{\frac{1}{\left(s+\mu_{ij}^{B}\left(1-\rho_{ij}^{B}\right)\right)^{n}}\right\} = \frac{t^{n-1}}{(n-1)!} e^{-\mu_{ij}^{B}\left(1-\rho_{ij}^{B}\right)t}$$

$$F_{st,m}^{B}(\theta^{*B}) = \sum_{ij \in l_{st,m}^{B}} \frac{A_{ij}}{(n-1)!} \int_{0}^{\theta^{*B}} t^{n-1} e^{-\mu_{ij}^{B}\left(1-\rho_{ij}^{B}\right)t}$$

Интегрируя $\int_0^{\theta^{*B}} t^{n-1} e^{-\mu_{ij}^{B}\left(1-\rho_{ij}^{B}\right)t}$ по частям получаем следующее рекурсивное выражение для расчета: $I = \int_0^{\theta^{*B}} t^{n-1} e^{-\mu_{ij}^{B}\left(1-\rho_{ij}^{B}\right)t} = \frac{-t^{n-1} e^{-\mu_{ij}^{B}\left(1-\rho_{ij}^{B}\right)t}}{a} - \frac{n-1}{a} \int_0^{\theta^{*B}} t^{n-2} e^{-\mu_{ij}^{B}\left(1-\rho_{ij}^{B}\right)t}$

$I^k = U^k - \frac{k}{\mu_{ij}^{B}\left(1-\rho_{ij}^{B}\right)} I^{k-1}$, где $U^k = \frac{-t^k e^{-\mu_{ij}^{B}\left(1-\rho_{ij}^{B}\right)\theta^{*B}}}{\mu_{ij}^{B}\left(1-\rho_{ij}^{B}\right)}$.

В итоге, задача расчета квантилей сетевых задержек разбивается на 2 подзадачи, которые решаются с помощью описанных выше алгоритмов:

1. Поиск методом Гаусса коэффициентов A_{ij}.
2. Вычисление интеграла.

В итоге, задача расчета квантилей сетевых задержек разбивается на 2 подзадачи, которые решаются с помощью описанных выше алгоритмов:

1. Поиск методом Гаусса коэффициентов A_{ij}.
2. Вычисление интеграла.

Получение обратного преобразования затрудняется из-за возможности присутствия в выражении $f_{st,m}^{B}$ кратных корней знаменателя, так как может оказаться, что в составном пути часть каналов или все каналы имеют одинаковую величину (физически кратный корень в знаменателе указывает на присутствие в тракте $st \in S^B$ каналов с одинаковыми членами $\mu_{ij}^{B}(1-\rho_{ij}^{B})$). Значения кратных корней, их число и количество свертываемых функций являются параметрами, по которым вычисляются

неопределенные коэффициенты разложения на простые дроби. Для этого вычисляются производные всех порядков до $l^B_{st,m}$ от полученной дробно-рациональной функции в точках, где она имеет полюса. Эти производные и используются для вычисления неопределенных коэффициентов и оригинала свертки. Ее интегрирование дает искомый квантиль распределения времени передачи по m-ом пути.

Выполнение этой процедуры требует следующей подготовки. Для каждого значения $l^B_{st,m}$ и возможных значений кратности корней должны быть получены явные выражения квантиля распределения времени передачи по m-ом пути, которые следует оформить в виде отдельных процедур. Кроме того, должна быть разработана специальная процедура-переключатель, которая выполняет следующие действия: для каждого ребра $ij \in l^B_{st,m}$ вычисляется величина $a^B_{ij} = \mu^B_{ij}(1-\rho^B_{ij})$. Величины a^B_{ij} сравниваются между собой и при их совпадении с заданной точностью подсчитывается кратность каждого a^B_{ij}. Определяется количество разных корней и кратность каждого. Для удобства корни упорядочиваются по убыванию кратности. Комбинация длины пути, числа разных корней и максимальной кратности однозначно определяет процедуру вычисления квантиля. Выполнение процедуры для $l^B_{st,m} \le 6$ вполне удовлетворяет практическим потребностям проектировщика.

Другой метод вычисления сверток базируется на следующих рекуррентных соотношениях, если

$\varphi^k_{m,0}(t) = 1$;

$$\varphi^k_{m,1}(t) = \int_0^t \varphi^k_{m,0}(x) e^{-(a^k_{m,1}-a^k_{m,2})x} dx;$$

$$\varphi^k_{m,2}(t) = \int_0^t \varphi^k_{m,1}(x) e^{-(a^k_{m,2}-a^k_{m,3})x} dx;$$

$$\varphi^k_{m,3}(t) = \int_0^t \varphi^k_{m,2}(x) e^{-(a^k_{m,3}-a^k_{m,4})x} dx;$$

……

$$\varphi^k_{m,p-1}(t) = \int_0^t \varphi^k_{m,p-2}(x) e^{-(a^k_{m,p-1}-a^k_{m,p})x} dx$$

, то

$$f^k_{m,p}(t) \equiv a^k_{m,1} e^{-a^k_{m,1}t} * a^k_{m,2} e^{-a^k_{m,2}t} * \ldots * a^k_{m,p} e^{-a^k_{m,p}t} = \left(\prod_{i=1}^{p} a^k_{m,i}\right) e^{-a^k_{m,p}t} \varphi^k_{m,p-1}(t). \quad (2)$$

Если $t = nh$, $n = 0,1,2,...,N$, h – шаг интегрирования, то вычисление интегралов в (2) можно проводить по интерполяционной формуле

$$\varphi^k_{m,i}((n+1)h) = \varphi^k_{m,i}(nh) + \int_{Nh}^{(N+1)h} \varphi^k_{m,i-1}(x) e^{-(a^k_{m,i}-a^k_{m,i+1})x} dx,$$ где $i = \overline{1, p-1}$, N – число точек разверстки (например, N =2000).

Пусть $g^k_{m,i-1}(x) \equiv \varphi^k_{m,i-1}(x) e^{-(a^K_i - a^k_{i+1})x}$, тогда

$$\int_{nh}^{(n+1)h} g^k_{m,i-1}(x)dx \approx h\left[\frac{g^k_{m,i-1}(nh) + g^k_{m,i-1}((n+1)h)}{2} - \frac{1}{12}\frac{\Delta^2 g^k_{m,i-1}((n-1)h) + \Delta^2 g^k_{m,i-1}(nh)}{2} + \right.$$
$$\left. + \frac{11}{720} \cdot \frac{\Delta^4 g^k_{m,i-1}((n-2)h) + \Delta^4 g^k_{m,i-1}((n-1)h)}{2}\right], n = \overline{2, N-2};$$

$$\int_0^h g^k_{m,i-1}(x)dx \approx h\left[\frac{g^k_{m,i-1}(0) + g^k_{m,i-1}(h)}{2} - \frac{1}{12}\cdot\Delta^2 g^k_{m,i-1}(0) + \frac{1}{24}\Delta^3 g^k_{m,i-1}(0) - \frac{19}{720}\Delta^4 g^k_{m,i-1}(0)\right];$$

$$\int_0^{2h} g^k_{m,i-1}(x)dx \approx h\left[\frac{g^k_{m,i-1}(h)+g^k_{m,i-1}(2h)}{2}-\frac{1}{12}\cdot\frac{\Delta^2 g^k_{m,i-1}(0)+\Delta^2 g^k_{m,i-1}(h)}{2}+\frac{11}{720}\Delta^4 g^k_{m,i-1}(0)\right];$$

$$\int_{(N-1)h}^{Nh} g^k_{m,i-1}(x)dx \approx h\left[\frac{g^k_{m,i-1}(Nh)+g^k_{m,i-1}((N-1)h)}{2}-\frac{1}{12}\cdot\Delta^2 g^k_{m,i-1}(N-2)-\frac{1}{24}\Delta^3 g^k_{m,i-1}(N-3)-\right.$$
$$\left.-\frac{19}{720}\Delta^4 g^k_{m,i-1}(N-4)\right];$$

$$\int_{(N-2)h}^{(N-1)h} g^k_{m,i-1}(x)dx \approx h\left[\frac{g^k_{m,i-1}((N-2)h)+g^k_{m,i-1}((N-1)h)}{2}-\frac{1}{12}\cdot\frac{\Delta^2 g^k_{m,i-1}(N-2)+\Delta^3 g^k_{m,i-1}(N-3)}{2}+\right.$$
$$\left.+\frac{11}{720}\Delta^4 g^k_{m,i-1}(N-4)\right];$$

$$\Delta\, g^k_{m,i-1}(nh) = g^k_{m,i-1}((n+1)h) - g^k_{m,i-1}(nh)$$
$$\Delta^2\, g^k_{m,i-1}(nh) = \Delta\, g^k_{m,i-1}((n+1)h) - \Delta\, g^k_{m,i-1}(nh)$$
$$\Delta^3\, g^k_{m,i-1}(nh) = \Delta^2\, g^k_{m,i-1}((n+1)h) - \Delta^2\, g^k_{m,i-1}(nh)$$
$$\Delta^4\, g^k_{m,i-1}(nh) = \Delta^3\, g^k_{m,i-1}((n+1)h) - \Delta^3\, g^k_{m,i-1}(nh).$$

Шаг интегрирования $h=\dfrac{12}{a^k_{m,p}N}$ и является единым для данного тракта $st \in S^B$. Расчет выполняется по следующей схеме.

$i\ t_{\backslash}$	0	h	2h	3 h	…	$(N-2)$h	$(N-1)$h	h
0	0	1	1	1	…	1	1	1
1	φ^k_1 (0)	φ^k_1 (h)	φ^k_1 (2h)	φ^k_1 (3 h)	…	φ^k_1 (($N-2$)h)	φ^k_1 (($N-1$)h)	φ^k_1 (N h)
2	φ^k_2 (0)	φ^k_2 (h)	φ^k_2 (2h)	φ^k_2 (3 h)	…	φ^k_2 (($N-2$)h)	φ^k_2 (($N-1$)h)	φ^k_2 (N h)
⋮	⋮	⋮	⋮	⋮	…	⋮	⋮	⋮
$p-1$	$\varphi^k_{p-1`}$ (0)	$\varphi^k_{p-1`}$ (h)	$\varphi^k_{p-1`}$ (2h)	$\varphi^k_{p-1`}$ (3 h)	…	$\varphi^k_{p-1`}$ (($N-2$)h)	$\varphi^k_{p-1`}$ (($N-1$)h)	$\varphi^k_{p-1`}$ (N h)
p	$\varphi^k_{p`}$ (0)	$\varphi^k_{p`}$ (h)	φ^k_p (2h)	φ^k_p (3 h)	…	φ^k_p (($N-2$)h)	φ^k_p (($N-1$)h)	φ^k_p (N h)

Например, для получения φ^k_2 (2h) используются значения φ^k_1 (h), φ^k_1 (2h), φ^k_2 (h), которые, в свою очередь, используют φ^k_1 (0), φ^k_1 (h), φ^k_1 (2h), φ^k_1 (3 h); для получения $\varphi^k_{p`}$ ( h) используются значения $\varphi^k_{p-1`}$ (0), $\varphi^k_{p-1`}$ ( h), $\varphi^k_{p`}$ (0), которые используют $\varphi^k_{p-1`}$ (0) $\varphi^k_{p-1`}$ (h) $\varphi^k_{p-1`}$(2h), а для получения $\varphi^k_p$ ($N$ h) используются значения $\varphi^k_{p-1`}$(($N-1$)h), $\varphi^k_{p-1`}$(N h) и т. д. Для увеличения точности вычисления интегралов число точек развёртки должно быть достаточно большим. Так, например, для M = 2000 точность достигает величины 1%, а время счёта для одного маршрута 5–7 секунд. Для точности порядка 0,1% число точек развёртки требуется увеличить в 5–10 раз, что существенно увеличивает время счёта.

Заключение. В статье сформулирован и обоснован «квантильный» подхода к качеству обслуживания изохронного трафика в пакетной мультисервисной сети в режиме сессии. Предложены методы расчета квантилей распределения случайной задержки, которые могут быть применены при вычислении ограничений в задаче анализа пакетной инфотелекоммуникационной транспортной системы мультисервисной сети.

СПИСОК ЛИТЕРАТУРЫ

1. Лохмотко, В.В. Анализ и оптимизация цифровых сетей для интегрального обслуживания / В.В. Лохмотко, Пирогов К.И. Мн.: Наука и техника, 1991. 192 с.

2. Мошак Н.Н. Теория проектирования транспортной системы инфокоммуникационной сети.: Учебное пособие для ВУЗов, «Энергомашиностроение», СПб, 2006, 159с.
3. Н. Н. Мошак. Защищенные инфотелекоммуникации. Анализ и синтез: монография / СПб.: ГУАП, 2014. 193 с.: ил.
4. ISBN 978-5-8088-0920-8
5. А.И.Яшин, Н.Н.Мошак, Е.В.Давыдова. Параметрический и структурный синтезпакетных мультисервисных сетей NGN. Техника средств связи: научно-технический сборник. Вып. 3 (142). – СПб. : Изд-во Политехн. ун-та. 2014, с. 36-47.
6. Мошак Н.Н., Яшин А.И., Давыдова Е.В. Методология моделирования и анализа процессов функционирования пакетных мультисервисных сетей. «Электросвязь». №4, 2015. – с. – С. 35-39

УДК 621.391

ВАРИАНТ ФОРМИРОВАНИЯ АНСАМБЛЯ ДИСКРЕТНЫХ ОРТОГОНАЛЬНЫХ СИГНАЛОВ С ТРЕБУЕМЫМИ ПАРАМЕТРАМИ СТРУКТУРНОЙ СКРЫТНОСТИ

Сазонов Виктор Викторович, Беззубов Олег Владимирович,Мосягин Дмитрий Евгеньевич
Военная академия связи им. Маршала Советского Союза им. С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр. 3
emails: vmktor-sazonov@yandex.ru,bov774@mail.ru, mitya.mosyagin@mail.ru

Аннотация: В статье раскрывается математический аппарат формирования ансамблей дискретных ортогональных сигналов с изменяющейся структурой, на основе свойств собственных векторов бидиогональных эрмитовых матриц. Количество формируемых структур напрямую зависит от размерности и числа состояний коэффициентов бидиагональных эрмитовых матриц.

Ключевые слова: *дискретный сигнал определяемый вектором в многомерном пространстве, амплитуды и фазы единичных элементов формируемых сигналов, модули и аргументы коэффициентов бидиагональных эрмитовых матриц.*

OPTION FOR THE FORMATION OF THE ENSEMBLE OF DISCRETE ORTHOGONAL SIGNALS WITH THE REQUIRED PARAMETERS OF STRUCTURAL HIDDEN

Sazonov Viktor, Bezubov Oleg, Mosyagin Dmitry
Military Academy of Communications. Marshal of the Soviet Union. CM. Budyonny
Russia, St. Petersburg, Tikhoretsky Ave 3
emails: vmktor-sazonov@yandex.ru,bov774@mail.ru, mitya.mosyagin@mail.ru

Annotation: The article reveals the mathematical apparatus for the formation of ensembles of discrete orthogonal signals with a variable structure, on the basis of the properties of the eigenvectors of bidiolagonal Hermitian matrices. The number of structures formed directly depends *on the dimension and the number of states of the coefficients of bidiagonal Hermitian matrices.*

Keywords:*a discrete signal determined by a vector in a multidimensional space, the amplitudes and phases of the unit elements of the generated signals, the moduli and the arguments of the coefficients of bidiagonal Hermitian matrices.*

Известно [1, 2], что структурная скрытность характеризует способность противостоять мерам радиотехнической разведки, направленным на раскрытие структуры сигнала. Это означает, что распознавание формы сигнала, определяемой способами его кодирования и модуляции, осуществляется посредством отождествления обнаруженного сигнала с одним из множества априорно известных. Следовательно, для увеличения структурной скрытности необходимо иметь по возможности больший ансамбль используемых сигналов и достаточно часто изменять форму сигналов. Наиболее сложно, часто изменять форму сигналов в системах связи использующих ортогональные сигналы. Данную задачу можно решить посредством модификации способа защиты информации со стохастическим применением ансамблей дискретных ортогональных сигналов (АДОС) построенных на основе свойств собственных векторов бидиагональных эрмитовых матриц (БЭМ) вида[3÷5]:

$$Q=\begin{vmatrix} 0 & q_{1,2}e^{j\psi_{1,2}} & 0 & . & 0 & 0 \\ q_{2,1}e^{j\psi_{2,1}} & 0 & q_{2,3}e^{j\psi_{2,3}} & . & 0 & 0 \\ . & . & . & . & . & . \\ 0 & 0 & 0 & . & 0 & q_{k-1,k}e^{j\psi_{k-1,k}} \\ 0 & 0 & 0 & . & q_{k,k-1}e^{j\psi_{k,k-1}} & 0 \end{vmatrix}, \quad (1)$$

где $q_{k-1,k}=q_{k,k-1}$ -модули, а $\psi_{k-1,k}=\psi^{*}_{k,k-1}$ - аргументы коэффициентов.

Поскольку известно [4], что для всякого ортогонального базиса конечномерного комплексного пространства существует БЭМ самосопряженного оператора, собственные векторы которой составляют данный базис. Координаты собственных векторов БЭМ

в общем случае являются комплексными числами, при этом выполняются условия ортогональности, представленным для дискретных аналитических комплексно-сопряжённых сигналов $\dot{x}_1(t)$ и $\dot{x}_2^*(t)$:

$$\int_0^T \dot{x}_1(t)\cdot \dot{x}_2^*(t)dt = 0,$$

где $\dot{x}_1(t) = a_1(t)\cdot e^{j\varphi_1(t)}, \dot{x}_2^* = a_2(t)\cdot e^{j\varphi_2^*(t)}, a_1(t)$ и $a_2(t)$ - амплитуды первого и второго сигналов, $\varphi_1(t)$ и $\varphi_2^*(t)$ - фазы соответствующих сигналов.

Рассмотрим дискретный сигнал $\dot{x}_1(t)$ (рис. 1), однозначно определяемый вектором в N - мерном пространстве:

$$\dot{x}_1(t) = \left\{a_{1,1}e^{j\varphi_{1,1}},\ a_{1,2}e^{j\varphi_{1,2}},\ a_{1,3}e^{j\varphi_{1,3}},\ \ldots a_{1,\mathrm{m}}e^{j\varphi_{1,m}}\right\},$$

где $a_{1,k}$ - амплитуда единичного элемента первого сигнала, $\varphi_{1,k}$ - фаза единичного элемента первого сигнала.

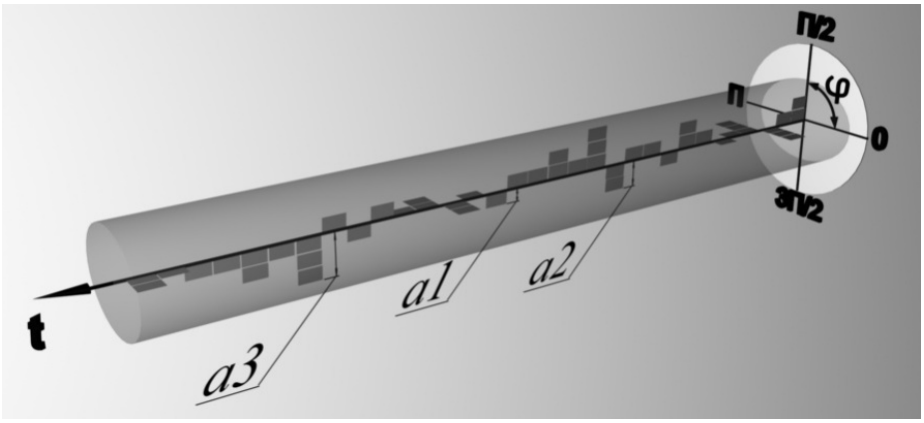


Рис. 1. Пространственное представление дискретного сигнала

Количество C_N формируемых структур АДОС будет напрямую зависеть от значений α и β, состояний диагональных коэффициентов исходной БЭМ Q и её размерности N и будет определяться выражением вида:

$$C_N = (\alpha\cdot\beta)^{N-1} \quad (3)$$

Графическое представление зависимости C_N, при различных значениях α и β, от размерности N представлено на рис. 2. Из анализа рис. 2 следует, что при росте размерности N исходной БЭМ Q, количество C_N возможных формируемых структур АДОС (базисов) возрастает по экспоненциальному закону, при этом скорость возрастания напрямую зависит от числа $\alpha\cup\beta$ возможных состояний диагональных коэффициентов $q_{k-1,k}$ и $\psi_{k-1,k}$, что, в свою очередь, способствует увеличению структурной скрытности системы связи.

При этом возможны три варианта формирования структуры АДОС:

1. С различными амплитудными $a_{1,k}$ параметрами единичных элементов, при изменении модулей коэффициентов $q_{k-1,k}$, принимающих α возможных состояний и $\beta = const$;

2. С различными фазовыми $\varphi_{1,k}$ параметрами единичных элементов, при изменении аргументов коэффициентов $\psi_{k-1,k}$, принимающих β возможных состояний и $\alpha = const$;

3. С различными амплитудными $a_{1,k}$ и фазовыми $\varphi_{1,k}$ параметрами единичных элементов, при изменении модулей $q_{k-1,k}$ и аргументов $\psi_{k-1,k}$ коэффициентов, принимающих α и β возможных значений.

Отметим, что по количеству базисов C_N первый и второй варианты равнозначны при условии $\alpha = \beta$, а третий вариант будет совпадать лишь при выполнении условия $(\alpha\cdot\beta) = \alpha\cup\beta$ первого и второго варианта.

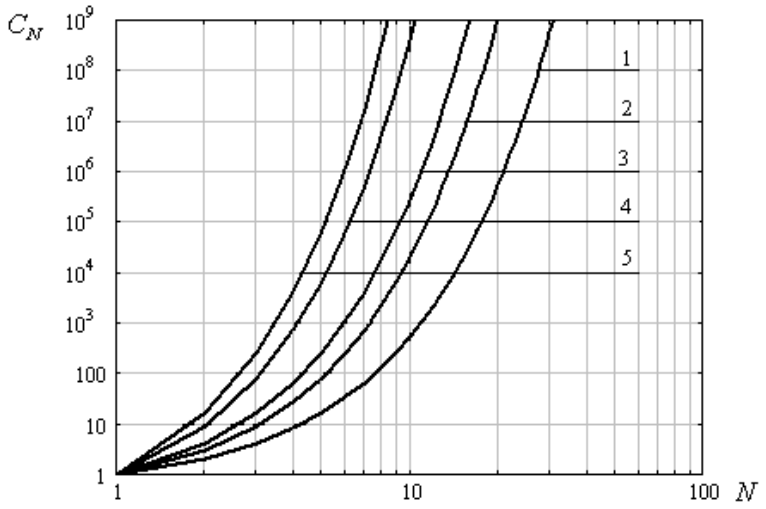


Рис.2. Зависимость C_N от N при $\alpha \cup \beta = 2$ (кривая 1), $\alpha \cup \beta = 3$ (кривая 2), $\alpha \cup \beta = 4$ (кривая 3), $\alpha \cap \beta = 3$ (кривая 4), $\alpha \cap \beta = 4$ (кривая 5)

Например, для систем с кодовым разделением каналов применяют последовательности сформированные на основе АДОС Уолша размерностью $N = 64$, с равными значениями амплитуд $a_1 = a_2 = \ldots = a_k$ единичных элементов сигналов в ансамбле и изменяющимися значениями фазы $\varphi_{k-1,k}$ имеющих два значения 0 и π. Для выполнения данного условия модули коэффициентов БАМ вида (1) устремляются $q_{1,2}, \ldots q_{k-1,k} \to \lambda$ (λ - собственные значения БЭМ), а $q_{2,3}, \ldots, q_{k-2,k-1} \to 0$, а аргументы $\psi_{1,2}, \ldots \psi_{k-1,k}$ принимают значения 0 и π. Следовательно, количество формируемых структур АДОС (3) при $\alpha = 1$ и $\beta = 2$ будет

$$C_{64} = (1 \cdot 2)^{64-1} = 9{,}223 \cdot 10^{18}.$$

Использование такого количества сформированных АДОС в системах с кодовым разделением каналов позволит значительно повысить её структурную скрытность.

Подводя итог вышеизложенному, можно сказать что случайно сформированные АДОС для каждого этапа передачи информации, на основе изменения исходных коэффициентовБЭМ по одному из трёх вариантов, позволит решить задачу повышения структурной скрытности системы связи.

СПИСОК ЛИТЕРАТУРЫ

1. Помехозащищённость радиосистем со сложными сигналами // Г.И.Тузов, В.А. Сивов, В.И. Прытков, и др.; Под ред. Г.И.Тузова. –М.: Радио и связь, 1985. -264 с.

2. Жук А.П., Галкин И.В., Сазонов В.В., Черняк З.В., Топкин Е.В. Оценка структурной скрытности сигналов в системе передачи информации с ортогональными последовательностями / Известия ЮФУ. Технические науки. 2007. № 4 (76). С. 167-171.

3. Жук А.П., Сазонов В.В. Влияние коэффициентов второй диагонали эрмитовой матрицы на корреляционные и спектральные свойства определяемых ею ортогональных в усиленном смысле сигналов / Физика волновых процессов и радиотехнические системы. / Периодический теоретический и научно-практический журнал Том 10, № 6– Самара.:, 2007. 52-55.

4. Пашинцев В. П., Малофей О. П., Жук А. П. и др. Развитие теории синтеза и методов формирования ансамблей дискретных сигналов для перспективных систем радиосвязи различных диапазонов радиоволн. М.: Физматлит, 2010. 264 с.

5. Мосягин Д.Е., Пантюхин О.И., Сазонов В.В., Титов В.С.Вариант помехозащищённой системы передачи информации /Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017) VI Международная научно-техническая и научно-методическая конференция : сборник научных статей : в 4 т.. 2017. С. 493-498.

УДК 004.49

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ

Пиюков Олег Юрьевич, Гвоздков Игорь Вячеславович
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М. А. Бонч-Бруевича
Россия, Санкт-Петербург, просп. Большевиков, 22 к1
emails: oleg9609@mail.ru, gvozdkov@rambler.ru

Аннотация: Обеспечение безопасности информационных ресурсов – крупная и разноплановая проблема, которая требует серьезного и комплексного анализа для предотвращения несанкционированного доступа к конфиденциальным данным. В понятие безопасности информационных ресурсов входит не только информационная безопасность, но и компьютерная, сетевая.

Ключевые слова: *информационная безопасность, информационные ресурсы, угрозы информационным ресурсам образовательных учреждений, аппаратная и программная защита.*

SECURITY OF INFORMATION RESOURCES OF EDUCATIONAL INSTITUTIONS

Piyukov Oleg Yrievich., Gvozdkov Igor Vyacheslavovich
St. Petersburg State University of Telecommunications. prof. M. A. Bonch-Bruevicha
Russia, St. Petersburg, prosp. Bolsheviks, 22k1
emails: oleg9609@mail.ru, gvozdkov@rambler.ru

Abstract*:* Ensuring the security of information resources is a large and diverse problem that requires a serious and comprehensive analysis to prevent unauthorized access to confidential data. In the notion of security of information resources is not only information security, but also computer, network.

Keywords: *information security, information resources, threats to information resources of educational institutions, hardware and software protection.*

Анализ и реализация безопасности информационных ресурсов будет осуществляться на основе существующих угроз. В настоящий момент теория общей защиты информации имеет несколько классов информационных рисков и угроз защиты информации. Сейчас являются двумя самыми большими классами угроз по определению местоположения злоумышленника - внешние и внутренние угрозы. Внедрение вредоносного программного обеспечения, изменение или уничтожение установленного программного обеспечения, использование уязвимостей открытых информационных ресурсов, нарушение работы пользователей вредоносным программами. Это относится к внешним угрозам безопасности информационных ресурсов. Также большая часть случаев утечки информации, кражи коммерческой тайны и персональных данных происходят по причине внутренних угроз. К примеру, сотрудники инсайдеры, которые часто являются членами преступных групп и могут иметь доступ к конфиденциальной информации, также сотрудники, которые не имеют достаточно знаний и опыта работы с важной информацией (забытые распечатанные страницы в лотке принтера, использование зараженных USB-накопителей и др.). В итоге получается, что опасность для информационных ресурсов поступает с разных сторон. Чаще всего инциденты утечки информации происходят в связи с безграмотностью работников и неумышленными действиями (передача данных по открытым каналам связи, загрузки вредоносных вирусов).

Информационные ресурсы образовательного учреждения основываются на электронных хранилищах разной информации. Такими средствами хранения и обработки информации являются файловые сервера, сервера для обработки специализированной информации (Электронный дневник, заказ питания, параграф), сайт. Для правильной работы всей структуры информация должна быть распределена между всеми ресурсами, а защита этой информации – комплексной.

В качестве программно-аппаратной защиты от внешних угроз используются антивирусы, межсетевые экраны, различные системы предотвращения вторжений, песочница. После правильной настройки всех элементов защиты, вероятность проникновения в сеть образовательного учреждения сводится к минимум. Для общеобразовательных учреждений Санкт-Петербурга поставляется антивирусное программное обеспечение Dr.Web, которое защищает от многих типов вредоносных программ и препятствует их автоматической установки. В качестве аппаратной защиты во многих учреждениях используются межсетевые экраны, к примеру, Altell Neo – это российский межсетевой экран, имеющий сертификат ФСТЭК. Одна из главных особенностей этого устройства – фильтрация трафика с возможностью защиты канала связи VPN, обнаружение и предотвращение вторжений (IDS/IPS), а также фильтрация контента (антивирусы, приложения, спам).

Защита от внутренних угроз должна основываться на политике информационной безопасности образовательного учреждения. Высокая степень мониторинга и контроля действий пользователя. А также ограничение на копирование файлов и данных на внешние накопители. Разграничение и администрирование прав доступа пользователей к информации. Чтобы получить доступ к определенной информации каждый пользователь имеет учётную запись, которая состоит из имени пользователя и пароля, а также некоторые данные о нем. Все данные для авторизации хранятся в зашифрованном виде. Каждый пользователь имеет доступ к информации, которая положена только для данного пользователя с данными правами, к примеру ограничение доступа к файлам и папкам, ограничение на запуск исполняемых файлов и др.

Для комплексной защиты от утечки данных с информационных ресурсов образовательных учреждений необходимо выполнять строгий контроль и мониторинг всех действий пользователей с конфиденциальной информацией с помощью программно-аппаратной защиты от внешних и внутренних угроз. Необходимо соблюдать внутреннюю политику безопасности, устанавливать антивирусное программное обеспечение, правильно разграничивать действия для пользователей, установку межсетевого экрана, а также другого лицензионного программного обеспечения, которое может помочь сохранить информационные ресурсы в безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. А. В. Башаш, Е. К. Баранова, Д. А. Ларин. Информационная безопасность. История защиты информации в России, 2015.
2. С. А. Будников, Паршин Н. В. Информационная безопасность иавтоматизированных систем, 2011.
3. Г. А. Бузов. Защита от утечки информации по техническим каналам, 2005, 416 с.

УДК 004.49

ВОПРОСЫ ВНЕДРЕНИЯ ТЕХНОЛОГИИ ЦИФРОВОГО ВИДЕО В ДЕЯТЕЛЬНОСТЬ ПОЛИЦИИ

Шалагинова Ольга Борисовна
Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, ул. Летчика Пилютова, д. 1,
email: shalaginova1337@yandex.ru

***Аннотация*:** В статье рассмотрены проблемы внедрения и эффективного использования в работе полиции современных видеотехнологий, критерии отбора техники в условиях большого разнообразия устройств цифрового видео. Решение задач видеомониторинга в целях обеспечения правопорядка в различных районах города. Изучение и применение позитивного зарубежного опыта использования видеонаблюдения для обеспечения общественной безопасности расследования преступлений.

***Ключевые слова**: видеофиксация; видеосъёмка; видеотехника; видеобанки; видеотеки.*

THE ISSUES OF INTRODUCTION OF DIGITAL VIDEO TECHNOLOGY IN POLICING

Shalaginova Olga Borisovna
Saint-Petersburg University of MIA of Russia,
Russia, St.-Petersburg, street Pilot, Pilyutova, 1,
shalaginova1337@yandex.ru

Abstract: The article presents problems of implementation and effective use in police work of modern video technology, selection criteria equipment in the conditions of various devices of digital video. The task of monitoring in order to ensure law and order in various parts of the city. The study and application of positive foreign experience in the use of CCTV for public safety crime investigation.

***Keywords:** video recording; videography; video equipment; videobank; video library.*

Введение. Перестройка и реформирование ОВД в России, активно осуществляемые государством в последние годы, нацелены на смещение акцента в деятельности полиции в сторону защиты прав и свобод граждан, а также повышения эффективности раскрытия и расследования преступлений, предупреждения и профилактики правонарушений. В федеральном законе «О полиции» [1] подчёркивается: «полиция оказывает поддержку развития гражданских инициатив в сфере предупреждения правонарушений и обеспечения правопорядка» (п. 3 ст. 10); «полиция использует технические средства, включая средства аудио-, фото- и видеофиксации, при документировании обстоятельств совершения преступлений, административных правонарушений, обстоятельств происшествий» (п. 3 ст. 11). При этом в качестве законных прав полиции указываются следующие права. Право «производить видеосъёмку лиц, задержанных по подозрению в совершении преступления, заключённых под стражу, обвиняемых в совершении преступления, подвергнутых административному наказанию в виде административного ареста, иных задержанных лиц, если в течение установленного срока задержания достоверно установить их личность не представилось возможным» (п. 19 ст. 13). Право формирования банков данных о лицах, состоящих на профилактическом учёте (п. 16 ст. 17); право «использовать в деятельности … видеотехнику …, вести видеобанки и видеотеки лиц, проходивших (проходящих) по делам и материалам проверок полиции» (п. 33 ст.13). К обязанностям полиции отнесены: обязанность «выявлять лиц, имеющих намерение совершить преступление, и проводить с ними индивидуальную профилактическую работу» (п.4 ст. 12).

Для полноценной реализации полицией обсуждаемых прав и обязанностей, внедрения и эффективного использования в работе подразделений и сотрудников полиции современных видеотехнологий необходимо предусмотреть систему мероприятий, включающую в себя: мероприятия по дальнейшему правовому регулированию вопросов использования технологий цифрового видео в деятельности ОВД; организационно-управленческие мероприятия по выработке служебного регламента использования видеотехнологий и контролю его эффективности; мероприятия по кадровому, финансовому и программно-техническому обеспечению соответствующей деятельности [2]. Остановимся на последней группе мер более подробно.

Кадровое обеспечение внедрения технологий цифрового видео в деятельность ОВД потребует расширения штата аттестованных инженерно-технических работников. Первый шаг в этом направлении уже сделан. Как известно, в структуре МВД учрежден Департамент информационных технологий, связей и защиты информации. Департамент обеспечивает и осуществляет функции по выработке и реализации государственной политики, нормативному правовому регулированию в

области совершенствования информационных и телекоммуникационных технологий, автоматизированных информационных систем, систем и средств связи, формирования и ведения информационных ресурсов, межведомственного информационного взаимодействия, реализации государственных и ведомственных программ в области информатизации навигационно-мониторинговых систем ОВД.

Финансовое обеспечение дальнейшего введения видеотехнологий в деятельность полиции требует существенных инвестиций в масштабах всей страны. Одним из возможных вариантов экономии средств на этом пути может стать включение в единую сеть видео-мониторинга пунктов видеонаблюдения частных, охранных и детективных агенств с необходимым разграничением доступа (для решения задач частной охраны и частного сыска обеспечивается доступ только в заранее определенным для них накопителям видеоданных).

Техническое обеспечение видеотехнологий, как правило, включает в себя следующие устройства. Цифровые видеокамеры (встроенные, корпусные, купольные, уличные, стационарные, управляемые, гиростабилизированные, проводные, беспроводные и др.). Цифровые устройства записи видеоинформации (компьютерные видеосервисы, некомпьютерные видеорегистраторы и др.). Программные и технические средства обработки видеоизображения (матричные видеокоммутаторы и др.) [3]. В условиях большого разнообразия устройств, представленных на рынке цифрового видео, вопрос о критериях отбора техники для ОВД является далеко не праздным.

Изучение и внедрение позитивного зарубежного опыта использования видеонаблюдения для обеспечения общественной безопасности расследования преступлений является одним из резервов повышения эффективности работы российской полиции. Признанным мировым лидером в этой области является Великобритания, которая имеет многолетний опыт применения технологий видеонаблюдения в антитеррористической деятельности. В этой стране систем видеонаблюдения установлено больше, чем в любой другой стране мира, причем значительная часть из них является частной собственностью.

Примером согласованного и взвешенного программно-технологического решения проблемы видеонаблюдения является хорошо известная и уже доказавшая свою эффективность отечественная система «Безопасный город». Эта система предназначена для решения задач видеомониторинга в целях обеспечения правопорядка, безопасности граждан и охраны собственности в различных районах города. В стандартный перечень функций входят: централизованная сеть видеонаблюдения (на автомобильных дорогах, в аэропортах и на вокзалах, в детских садах и школах, в точках работы коммунальных служб, на чердаках и в подвалах); архив видеозаписей; пункты экстренной связи с правоохранительными органами [3].

Заключение. С нашей точки зрения, было бы разумно создать под патронатом МВД научно-производительный кластер, который бы по централизованному госзаказу производил видеотехнику для ее использования во всех регионах. К тому же при определении единой программно-технической политики следует иметь в виду необходимость международного сотрудничества подразделений полиции в рамках Интерпола по обмену значимой для раскрытия, расследования и профилактики транснациональных преступлений цифровой информацией. Одинаковые или родственные стандарты видеоданных значительно ускорят удовлетворение участниками-партнерами взаимных поисковых запросов.

СПИСОК ЛИТЕРАТУРЫ

1. ФЗ N 3 от 07.02.2011 «О полиции» с изменениями от 10.08.2017.
2. Молотков А. С. Проблематика развития и внедрения и внедрения современных информационных технологий в системе МВД России. // Мировой судья. -2012. - № 5. - С. 13 – 16.
3. Ржавский К. В. Информационная безопасность: практическая защита информационных технологий и телекоммуникационных систем: Учебное пособие. - Волгоград: Изд-во ВолГУ, 2012 — 120 с.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

УДК 681.518.5:004.052.32

ДВУХМОДУЛЬНЫЕ КОДЫ С СУММИРОВАНИЕМ В ЭКСПЕРИМЕНТЕ ПО АНАЛИЗУ СТРУКТУРНОЙ ИЗБЫТОЧНОСТИ СИСТЕМ ФУНКЦИОНАЛЬНОГО КОНТРОЛЯ

Ефанов Дмитрий Викторович, Щагина Владислава Александровна
Петербургский государственный университет путей сообщения Императора Александра I,
Россия, Санкт-Петербург, Московский пр., д.9,
emails: TrES-4b@yandex.ru, vladislava1997@inbox.ru

Аннотация. В статье рассматривается семейство двухмодульных кодов с суммированием. Приведен обобщенный алгоритм построения двухмодульных кодов с суммированием. Произведен сравнительный анализ структурной избыточности систем функционального контроля на основе двухмодульных кодов и систем функционального контроля на основе классических и модифицированных кодов с суммированием единичных информационных разрядов. Приведены результаты экспериментов с контрольными комбинационными схемами из набора MCNC Benchmarks. Установлены некоторые закономерности увеличения сложности технической реализации систем функционального контроля в зависимости от выделения подмножеств разрядов при построении двухмодульного кода.

Ключевые слова: *техническая диагностика, система функционального контроля, код с суммированием, код Бергера, модифицированный код с суммированием, двухмодульный код с суммированием, сложность технической реализации, структурная избыточность.*

TWO-MODULO CODES WITH SUMMATION IN EXPERIMENT ON THE ANALYSIS OF STRUCTURAL REDUNDANCY OF CONCURRENT ERROR DETECTION SYSTEMS

Efanov Dmitry, Schagina Vladislava
The Emperor Alexander I St. Petersburg State Transport University,
Russia, St. Petersburg, Moscow ave., 9
emails: TrES-4b@yandex.ru, vladislava1997@inbox.ru

Abstract. The family of two-modulo codes with summation is considered in the article. A generalized algorithm for constructing two-modulo codes with summation is given. A comparative analysis of structural redundancy of concurrent error detection systems based on two-modulo codes and on classical and modified codes with summation of data on-bits is made. The results of experiments with test combination circuits from the MCNC Benchmarks set are presented. Certain regularities of increasing the complexity of the technical implementation of concurrent error detection systems are established depending on the allocation of subsets of bits in the construction of a two-modulo code.

Keywords: *technical diagnostics, concurrent error detection system, code with summation, Berger code, modified code with summation, two-modulo code with summation, complexity of technical implementation, structural redundancy.*

Введение. Для организации тестирования комбинационных логических схем в процессе выполнения ими своих функций используются системы функционального контроля [1 – 5]. Такие системы строятся при использовании помехоустойчивых кодов. Часто для построения систем функционального контроля используются классические и модифицированные коды с суммированием [6 – 11].

Классический код с суммированием (код Бергера) [12], обозначаемый как S(m,k)-код (m и k – количество информационных и контрольных разрядов кода), строится путем записи в его контрольный вектор двоичного эквивалента веса информационного вектора r (количества единичных разрядов). Код Бергера имеет свойство обнаружения всех монотонных ошибок в информационных векторах, однако из-за неравномерного распределения информационных векторов между всеми контрольными векторами, имеет достаточно большое общее количество не обнаруживаемых ошибок в информационных векторах [13]. Кроме того, сложность технической реализации систем функционального контроля, построенных на основе кода Бергера, зачастую можно уменьшить при использовании различных их модификаций [14, 15].

Для улучшения свойств кода Бергера используются его различные модификации. Так, например, известным способом улучшения характеристик S(m,k)-кодов является взвешивание разрядов заранее выбранными натуральными числами и подсчет суммарного веса единичных информационных разрядов [16]. Другим способом построения кода с суммированием является формирование веса информационного вектора по формуле $W = r(\mathrm{mod}\, M) + \alpha M$, где $r(\mathrm{mod}\, M)$ – наименьший неотрицательный вычет веса по модулю $M = 2^{\lceil \log_2 (m+1) \rceil}$, а α – специальный поправочный коэффициент, вычисляемый как сумма по модулю два значений заранее выбранных информационных разрядов (далее обозначим этот модифицированный код Бергера как RS(m,k)-код) [17]. Еще одним подходом к построению кода является разбиение разрядов информационного вектора на подмножества и формирование отдельных контрольных частей для каждого подмножества. В [18] описывается такой код с учетом разбиения разрядов вектора на два подмножества и контроля каждого, вновь получаемого, информационного вектора по модулю M=4 (так называемый двухмодульный код, или TM(m,k)-код).

Последний подход к модификации кода из перечисленных подходов является перспективным в задачах технической диагностики. Ранее уже была рассмотрена такая модификация с половинным разбиением информационного вектора и контроля каждого по модулю 4 [19 – 21], однако такой код является всего лишь частным случаем. Поэтому целью данной статьи является изложение результатов исследования всего многообразия двухмодульных кодов с определением наименьшего неотрицательного вычета по модулю M=4. При этом материал данной работы сконцентрирован на изложении результатов анализа сложности технической реализации систем функционального контроля, построенных на основе TM(m,k)-кодов.

1. Принципы построения двухмодульных кодов с суммированием. Рассмотрим построение кода с улучшенными характеристиками, алгоритм построения которого основан на разбиении информационных векторов на два подвектора и отдельного контроля каждого из них по модулю M=4.

1. Алгоритм построения двухмодульного кода с суммированием:
2. Выбираются значения модулей: M_1 =4, M_2=4.
3. Из полного множества разрядов информационного вектора {Q} выделяется два подмножества разрядов $\{D_1\}$ и $\{D_2\}$ такие, что $\{D_1\} \cap \{D_2\} = \{Q\}$.
4. Разряды из полученных подмножеств$\{D_1\}$ и $\{D_2\}$ объединяются, образуя два вектора $\langle V_1 \rangle$ и $\langle V_2 \rangle$ длинами $m_1 \in [2; m]$ и $m_2 \in [2; m]$ соответственно.
5. Определяются веса векторов $\langle V_1 \rangle$ и $\langle V_2 \rangle$: W_1 и W_2 соответственно.
6. Определяются наименьшие неотрицательные вычеты чисел W_1 и W_2: $W_1(\mathrm{mod}\ M_1)$ и $W_2(\mathrm{mod}\ M_2)$.
7. Числа $W_1(\mathrm{mod}\ M_1)$ и $W_2(\mathrm{mod}\ M_2)$ представляются в двоичном виде и записываются в разряды контрольного вектора.

На рис. 1 показан пример получения контрольного вектора при длине информационного вектора *m*=9.

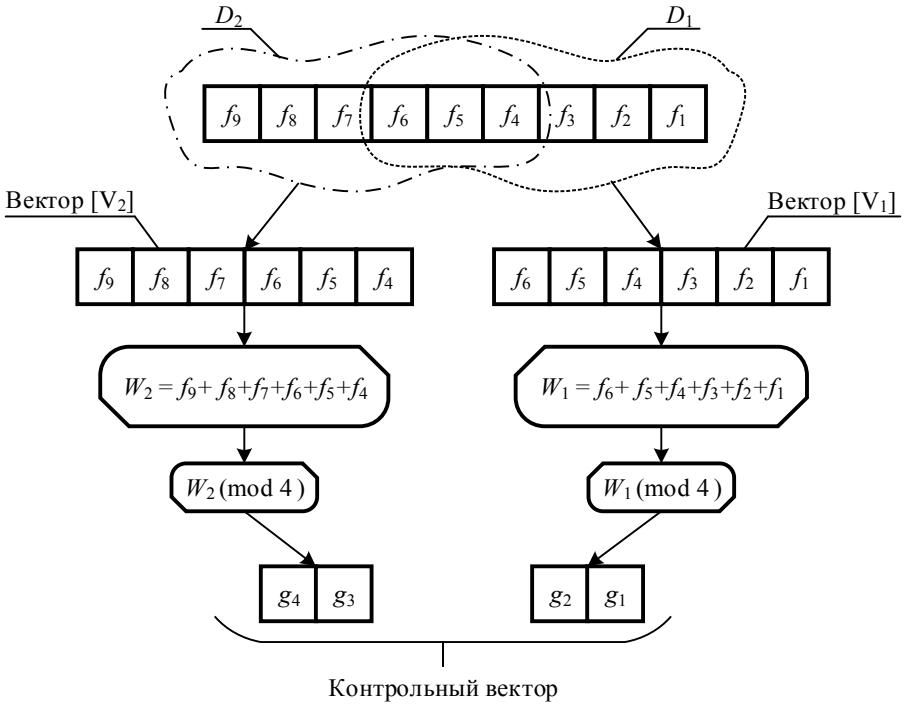
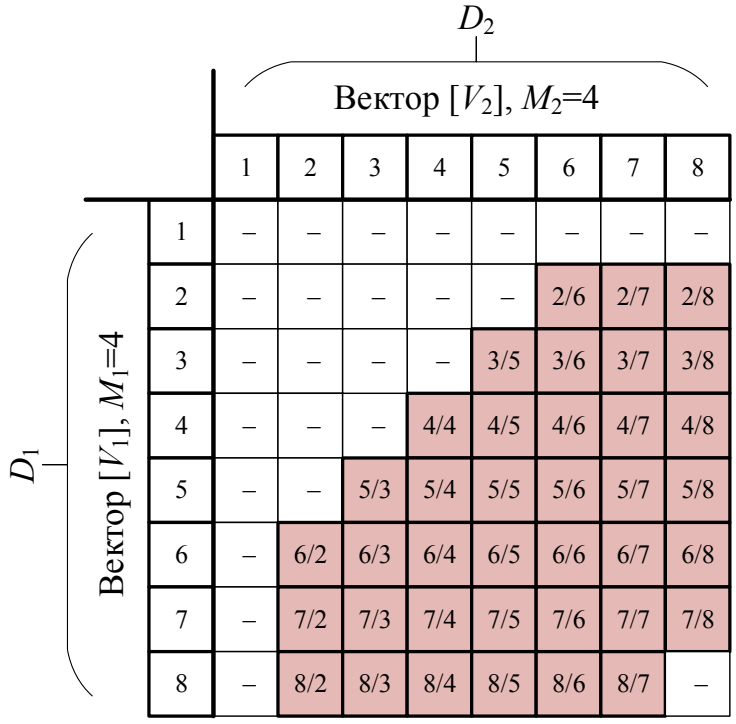


Рис. 1. Построение контрольного вектора для TM (9,4)-кода

Код, контрольные векторы которого получены при использовании выше представленного алгоритма, будем обозначать как TM(m,k,D1/D2)-код, где запись D1/D2 обозначает количество разрядов информационного вектора в первом и во втором подмножествах.

В зависимости от выделения разрядов информационного вектора на подвекторы образуется целое семейство двухмодульных кодов, которые обладают как общими свойствами, так и уникальными для каждого варианта разбиения.

Например, для информационного вектора с длиной m=8 возможно 39 вариантов построения двухмодульного кода. На рис. 2 представлена матрица, в которой на пересечении строки и столбца, соответствующих количеству разрядов в каждом из подмножеств разрядов, указан конкретный двухмодульный код.



	1	2	3	4	5	6	7	8
1	–	–	–	–	–	–	–	–
2	–	–	–	–	–	2/6	2/7	2/8
3	–	–	–	–	3/5	3/6	3/7	3/8
4	–	–	–	4/4	4/5	4/6	4/7	4/8
5	–	–	5/3	5/4	5/5	5/6	5/7	5/8
6	–	6/2	6/3	6/4	6/5	6/6	6/7	6/8
7	–	7/2	7/3	7/4	7/5	7/6	7/7	7/8
8	–	8/2	8/3	8/4	8/5	8/6	8/7	–

Рис. 2. Матрица для *TM* (8,4)-кода

Клетки в матрице обозначенные как «–» не удовлетворяют условию алгоритма построения (пересечение подмножеств разрядов не образует полного множества разрядов), и поэтому не являются помехоустойчивыми. Так же клетки на пересечении 8 строки и 1 столбца, 1 столбца и 8 строки матрицы не имеет смысла рассматривать в виду равнозначности разрядов. Стоит отдельно отметить, что код на пересечении 8 строки и 8 столбца матрицы также не имеет смысла рассматривать в виду его двойной избыточности. Все остальные клетки соответствуют кодам, удовлетворяющим алгоритму, так как при пересечении подмножеств D_1 и D_2 образуется полное множество разрядов Q, поэтому в дальнейшем они могут быть применены для синтеза систем функционального контроля.

В [19 – 21] рассмотрен частный случай двухмодульного *TM*(8,4,4/4)-кода, где исследованы его свойства, и доказано что в сравнении с -*S*, -*RS*(*m*,*k*)-кодами он является более эффективным при организации систем функционального контроля в диапазоне длин информационных векторов *m*=8÷15.

Стоит отметить, что при построении двухмодульных кодов в виду равнозначности разрядов, не важно, какие разряды входят в подмножество, так, например, TM(8,4,2/6), TM(8,4,6/2)-коды, будут иметь одинаковые свойства, поэтому важными факторами являются количество разрядов в подмножестве, а также всевозможные пересечения двух подмножеств.

Однако на практике, в реальных схемах, не формируется полное множество информационных разрядов 2m, в виду чего это влияет на конкретные разряды, поэтому, например, коды TM(10,4,7/5) и TM(8,4,5/7) будут иметь одинаковые свойства в общем случае, но в системах функционального контроля могут проявляться иначе показатели сложности технической реализации.

2. Результаты экспериментов по анализу характеристик структурной избыточности систем функционального контроля. Основными характеристиками систем функционального контроля являются обнаруживающая способность и структурная избыточность. В [18] показано, что двухмодульные коды гораздо эффективнее обнаруживают ошибки в информационных векторах, чем сравниваемые с ними коды. Рассмотрим характеристики сложности.

Для сравнения сложности технической реализации систем функционального контроля, построенных на основе TM(m,k,D1/D2)-кодов, с системами функционального контроля, построенными на основе -S, -RS (m,k)-кодов, были выбраны 15 контрольных комбинационных схем из базы MCNC с количеством выходов m=8÷15 [22]. Именно при данных длинах код -S, -RS (m,k) и TM-(m,k) коды могут быть сравнимы, так как имеют одинаковое количество контрольных разрядов. RS(m,k)-коды при каждом конкретном способе вычисления поправочного коэффициента α имеют свои уникальные характеристики [23]. В дальнейшем рассматриваются RS(m,k)-коды, для которых поправочный коэффициент α вычисляется как сумма $^{m}/_{2}$ различных информационных разрядов при четном

значении m и $(m \pm 1)/2$ различных информационных разрядов при нечетном значении m (такой код обладает наилучшими характеристиками обнаружения ошибок).

Все выбранные контрольные комбинационные схемы заданы в формате *.pla, который в виде таблицы истинности задает логику ее работы. Для получения файлов описания блоков систем функционального контроля в формате *.pla использовался комплекс программ «Coding», разработанный на кафедре «Автоматика и телемеханика на железных дорогах» Петербургского государственного университете путей сообщения Императора Александра I. С помощью интерпретатора SIS и библиотеки функциональных элементов stdcell2_2.genlib были рассчитаны площади [24], занимаемые устройством на кристалле в условных единицах, которые фактически являются показателями сложности технической реализации систем функционального контроля.

Для представления результатов была выбрана контрольная логическая схема «br1», имеющая количество выходов m=8. В табл. 1 приведены результаты, где для удобства сравнения показателей сложности технической реализации был введен коэффициент ε, показывающий отношение площади схемы функционального контроля, построенной по TM(m,k,D1/D2)-коду к площади схемы функционального контроля, построенной по -S,-RS(m,k)-коду, а также к площади схемы дублирования.

Из 22 различных вариантов выделения подмножеств D1/D2 почти для 80% коэффициент ε получился меньше 100% как для дублирования, так и для S(m,k)- кода. Это свидетельствует о том, что, системы функционального контроля, построенные по двухмодульным кодам имеют меньшую сложность технической реализации, чем системы функционального контроля, построенные на основе схемы дублирования и кода Бергера. Однако при сравнении с RS(m,k)-кодом этот процент разбиения сократился почти вдвое. Можно заметить, что некоторые виды разбиения показывают стабильные результаты, например: 4/4, 5/3, 5/3, 6/4, 6/3, 7/2 и т.д.

Из результатов, приведенных в табл. 1, следует, что системы функционального контроля, построенные на основе двухмодульных кодов, имеют меньшую структурную избыточность, но не для всех видов разбиения.

Для наглядности значения коэффициентов из табл. 1 также представлены в графической форме на рис. 3.

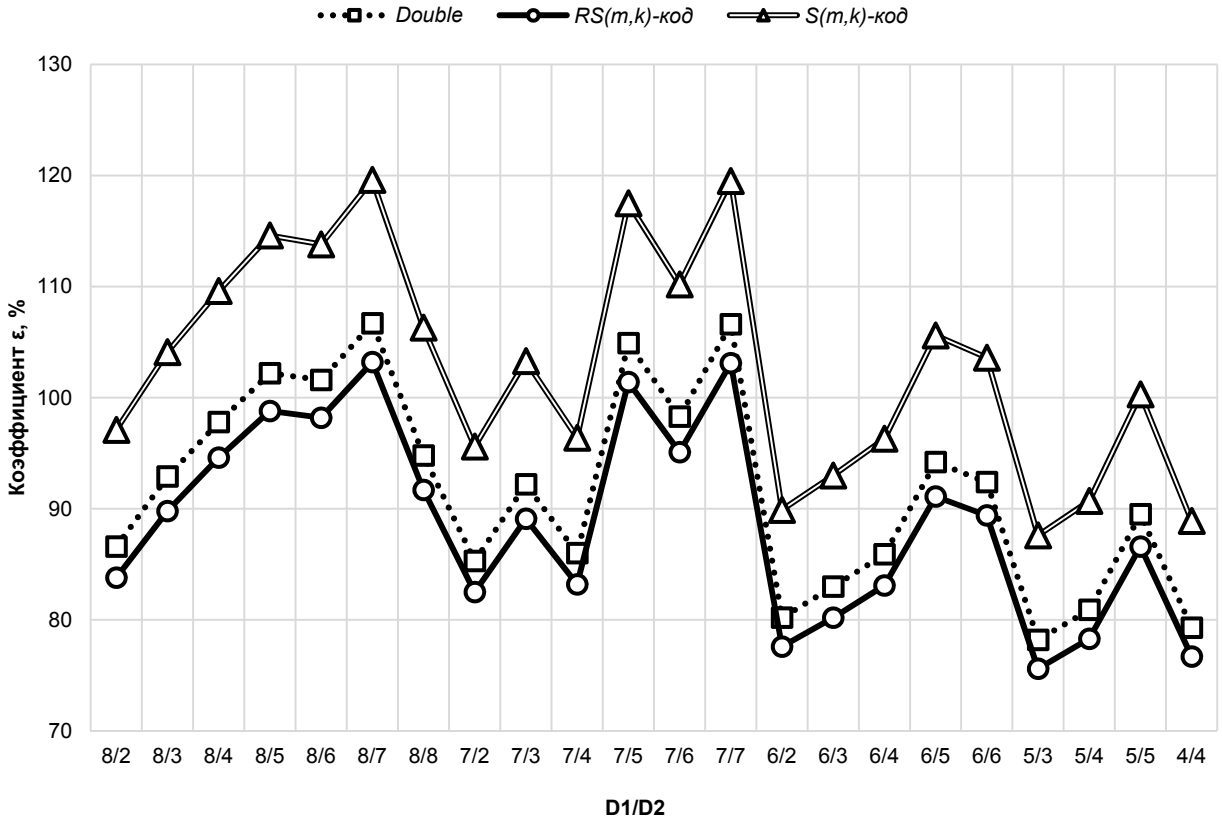


Рис. 3. Зависимость увеличения показателей сложности технической реализации от выделения подмножеств $TM(8,4,D_1/D_2)$-кода

По графикам на рис. 3 прослеживается некоторая зависимость показателей сложности технической реализации от способа выделения подмножеств D_1/D_2. Чтобы показать данную зависимость, были выбраны некоторые комбинационные схемы: «b10», «gary», «in0», имеющие количество выходов m=11. Для них были подсчитаны коэффициенты ε, показывающие отношение

площади системы функционального контроля, основанной на $TM(11,4,D_1/D_2)$-коде, к площади схемы дублирования. На рис. 4 приведен график значений этих величин.

Из графиков видно, что зависимость показателей сложности технической реализации сохраняется, то есть, при фиксированном первом подмножестве разрядов с увеличением количества разрядов во втором подмножестве возрастает сложность реализации. Также стоит отметить, что для 90% видов двухмодульных кодов, значение коэффициента ε не превышает 100%, что свидетельствует о меньшей структурной избыточности систем функционального контроля, построенной на основе двухмодульных кодов.

Таблица 1

Показатели сложности технической реализации

№ п/п	TM (8,4,D_1/D_2)- code	L^{Double}, усл. ед.	$L^{S\text{-}code}$, усл. ед.	$L^{RS\text{-}code}$, усл. ед.	$L^{TM-code}$, усл. ед.	ε^{Double}, %	$\varepsilon^{S\text{-}code}$, %	$\varepsilon^{RS\text{-}code}$, %
1	8/2	8688	8984	7752	7528	86,6	83,8	97,1
2	8/3				8072	92,9	89,8	104,1
3	8/4				8496	97,8	94,6	109,6
4	8/5				8880	102,2	98,8	114,6
5	8/6				8824	101,6	98,2	113,8
6	8/7				9272	106,7	103,2	119,6
7	8/8				8240	94,8	91,7	106,3
8	7/2				7408	85,3	82,5	95,6
9	7/3				8008	92,2	89,1	103,3
10	7/4				7472	86	83,2	96,4
11	7/5				9112	104,9	101,4	117,5
12	7/6				8544	98,3	95,1	110,2
13	7/7				9264	106,6	103,1	119,5
14	6/2				6968	80,2	77,6	89,9
15	6/3				7208	83	80,2	93
16	6/4				7464	85,9	83,1	96,3
17	6/5				8184	94,2	91,1	105,6
18	6/6				8032	92,4	89,4	103,6
19	5/3				6792	78,2	75,6	87,6
20	5/4				7032	80,9	78,3	90,7
21	5/5				7776	89,5	86,6	100,3
22	4/4				6888	79,3	76,7	88,9
Средние значения						91,796	88,777	102,886

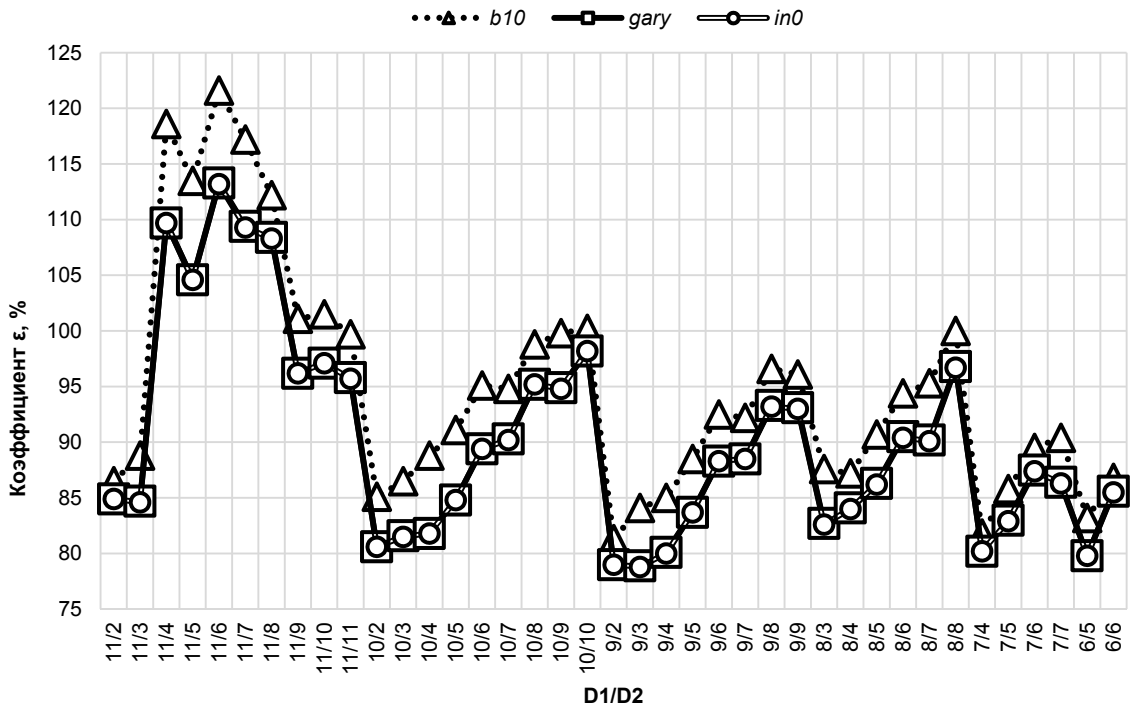


Рис. 4. Зависимость увеличения показателей сложности технической реализации от выделения подмножеств $TM(11,4,D_1/D_2)$-кода

Заключени***е.*** В ходе исследования свойств двухмодульных кодов можно сделать вывод о том, что некоторые из них позволяют строить системы функционального контроля с уменьшенной по сравнению с дублированием и использованием $-S$ и $-RS(m,k)$-кодов структурной избыточностью. Прослеживаются некоторые зависимости увеличения сложности технической реализации систем функционального контроля от выделения подмножеств разрядов при построении двухмодульного кода. Это дает возможность выбрать такие двухмодульные коды, структурная избыточность систем функционального контроля при использовании которых будет наименьшей.

Предложенный способ образования контрольных векторов, путем записи наименьшего неотрицательного вычета веса подвекторов $<V_1>$ и $<V_2>$ в двоичном виде в контрольный вектор не является единственным. В дальнейшем в качестве основы образования контрольных векторов может быть использование не только подсчета веса подвекторов $<V_1>$ и $<V_2>$, но и подсчет весов подвекторов с учетом весового коэффициента разрядов, а также переходов между разрядами. Таким образом, открывается целый класс двухмодульных кодов, каждый из которых обладает своими уникальными характеристиками, а дальнейшее исследование их свойств является важным для учета при решении задач технической диагностики.

СПИСОК ЛИТЕРАТУРЫ

1. Слабаков Е.В., Согомонян Е.С. Самопроверяемые вычислительные устройства и системы (обзор) // Автоматика и телемеханика. – 1981. – №11. – С. 147-167.
2. Nicolaidis M., Zorian Y. On-Line Testing for VLSI – A Compendium of Approaches // Journal of Electronic Testing: Theory and Applications. – 1998. – Vol. 12, issue 1-2. – Pp. 7-20.
3. Goessel M., Graf S. Error Detection Circuits. – London: McGraw-Hill, 1994, 261 p.
4. Mitra S., McCluskey E.J. Which Concurrent Error Detection Scheme to Choose? // Proceedings of International Test Conference, 2000, Atlantic City, USA, 03-05 October 2000. – Pp. 985-994. – DOI: 10.1109/TEST.2000.894311.
5. Göessel M., Ocheretny V., Sogomonyan E., Marienfeld D. New Methods of Concurrent Checking: Edition 1. – Dordrecht: Springer Science+Business Media B.V., 2008, 184 p.
6. Busaba F.Y., Lala P.K. Self-Checking Combinational Circuit Design for Single and Unidirectional Multibit Errors // Journal of Electronic Testing: Theory and Applications. – 1994. – Issue 1. – Pp. 19-28. – DOI: 10.1007/BF00971960.
7. Piestrak S.J. Design of Self-Testing Checkers for Unidirectional Error Detecting Codes. – Wrocław: Oficyna Wydawnicza Politechniki Wrocławskiej, 1995. – 111 p.
8. Morosow A, Saposhnikov V.V., Saposhnikov Vl.V., Goessel M. Self-Checking Combinational Circuits with Unidirectionally Independent Outputs // VLSI Design. – 1998. – Vol. 5, Issue 4. – Pp. 333-345.
9. Matrosova A.Yu., Levin I., Ostanin S.A. Self-Checking Synchronous FSM Network Design with Low Overhead // VLSI Design. – 2000. – Vol. 11. – Issue 1. – Pp. 47-58.
10. Das D., Touba N.A., Seuring M., Gossel M. Low Cost Concurrent Error Detection Based on Modulo Weight-Based Codes // Proceedings of IEEE 6th International On-Line Testing Workshop (IOLTW), Spain, Palma de Mallorca, July 3-5, 2000, pp. 171-176.
11. Мехов В.Б., Сапожников В.В., Сапожников Вл.В.Контроль комбинационных схем на основе модифицированных кодов с суммированием // Автоматика и телемеханика. – 2008. – №8. – С. 153-165.
12. Berger J.M. A Note on Error Detection Codes for Asymmetric Channels // Information and Control. – 1961. – Vol. 4. – Issue 1. – Pp. 68-73. – DOI: 10.1016/S0019-9958(61)80037-5.
13. Ефанов Д.В., Сапожников В.В., Сапожников Вл.В. О свойствах кода с суммированием в схемах функционального контроля // Автоматика и телемеханика. – 2010. – №6. – С. 155-162.
14. Das D., Touba N.A. Synthesis of Circuits with Low-Cost Concurrent Error Detection Based on Bose-Lin Codes // Journal of Electronic Testing: Theory and Applications. – 1999. – Vol. 15. – Issue 1-2. – Pp. 145-155. – DOI: 10.1023/A:1008344603814.
15. Сапожников В.В., Сапожников Вл.В., Ефанов Д.В., Дмитриев В.В. Новые структуры систем функционального контроля логических схем // Автоматика и телемеханика. – 2017. – №2. – С. 127-143.
16. Das D., Touba N.A. Weight-Based Codes and Their Application to Concurrent Error Detection of Multilevel Circuits // Proceedings of 17th IEEE Test Symposium, USA, California, 1999, pp. 370-376.
17. Блюдов А.А., Ефанов Д.В., Сапожников В.В., Сапожников Вл.В. Построение модифицированного кода Бергера с минимальным числом необнаруживаемых ошибок информационных разрядов // Электронное моделирование. – 2012. – Том 34. – №6. – С. 17-29.
18. Efanov D., Sapozhnikov V., Sapozhnikov Vl. Generic Two-Modulus Sum Codes for Technical Diagnostics of Discrete Systems Problems // Proceedings of 14th IEEE East-West Design & Test Symposium (EWDTS`2016), Yerevan, Armenia, October 14-17, 2016, pp. 256-260, doi: 10.1109/EWDTS.2016.7807713.
19. Ефанов Д. В., Щагина В. А. Код с суммированием единичных разрядов на основе принципа выделения групп разрядов и их контроля по модулю 4 // Материалы Юбилейной XV Санкт-Петербургской международная конференция «Региональная информатика – 2016», Санкт-Петербург, 26 – 28 октября 2016 г., СПОИСУ, СПб, 2016, с. 295-296.
20. Ефанов Д.В., Щагина В.А. Анализ сложности технической реализации систем функционального контроля организованных на основе двухмодульных кодов с суммированием по модулю 4 // Транспортные интеллектуальные системы: сборник материалов I международной научно-практической конференции «Транспортные интеллектуальные системы – 2017» (TIS-2017), Санкт-Петербург, 16-17 февраля 2017 г.; под. ред. Вал. В. Сапожникова, Д. В. Ефанова. – СПб: ФГБОУ ВО ПГУПС, 2017, с. 19-31.
21. Efanov D., Sapozhnikov V., Sapozhnikov Vl., Schagina V. The Analysis of Two-Modulus Codes Detection Ability with Summation of Unit Data Bits Compared to Classical and Modified Berger Codes // Proceedings of 15th IEEE East-West Design & Test Symposium (EWDTS`2017), Novi Sad, Serbia, September 29 – October 2, 2017.
22. Collection of Digital Design Benchmarks [Режим доступа: http://ddd.fit.cvut.cz/prj/Benchmarks/].
23. Efanov D., Sapozhnikov V., Sapozhnikov Vl., Blyudov A. On the Problem of Selection of Code with Summation for Combinational Circuit Test Organization // Proceedings of 11th IEEE East-West Design & Test Symposium (EWDTS`2013), Rostov-on-Don, Russia, September 27-30, 2013, pp. 261-266, doi: 10.1109/EWDTS.2013.6673133.
24. SIS: A System for Sequential Circuit Synthesis / E. M. Sentovich, K. J. Singh, L. Lavagno, C. Moon, R. Murgai, A. Saldanha, H. Savoj, P. R. Stephan, R. K. Brayton, A. Sangiovanni-Vincentelli // Electronics Research Laboratory, Department of Electrical Engineering and Computer Science, University of California, Berkeley, 4 May 1992, 45 p.

УДК 004.056.5

ЗАЩИТА ИНФОРМАЦИИ И ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Карташов Павел Николаевич
Санкт-Петербургский государственный экономический университет, кафедра информационных систем и технологий (ИСИТ),
Россия, 191023, Санкт-Петербург, улица Садовая, дом 21.
Вход в университет с набережной канала Грибоедова, дом 30/32.
email: torgul@bk.ru

***Аннотация*:** С каждым годом всё большее количество информации сохраняется и обрабатывается в цифровом виде. Разнообразные «девайсы» и «гаджеты» стали неотъемлемой частью жизни большинства людей. Помимо рабочей или финансовой информации устройства стали нести в себе и огромное количество личных, конфиденциальных данных. В связи с этим активно развиваются различные программные и аппаратные средства защиты информации. А потому в системе человек-компьютер всё более уязвимым звеном становится не машина, а сам человек. В статье рассмотрены проблемы защиты информации, связанные именно с человеческим фактором.

***Ключевые слова**: защита информации; безопасность; социальная инженерия; человеческий фактор.*

DATA PROTECTION AND THE HUMAN FACTOR

Kartashov Pavel
The St. Petersburg State Economical University
Russia, St. Petersburg, Sadovaya str. 21,
email: torgul@bk.ru

Abstract: From year to year more and more information is stored and processed in digital forms. A variety of "devices" and "gadgets" have become an integral part of most people's lives. Besides working or financial data, the devices now carry a huge amount of personal, confidential information. For that matter various software and hardware methods of information protection are actively developing. Therefore, in the human-computer system, the increasingly vulnerable component is not the machine, but the person himself. The article deals with the problems of data protection, in the context of the human factor.

***Keywords:** data protection; security; social engineering, human factor.*

Все мы с детства помним сказку «Волк и семеро козлят». На её примере детям просто и доступно доводили мысль о том, что нельзя открывать двери незнакомцам. Поразмыслив о сути этой сказки, можно сказать о том, что волк попытался попасть в защищенную систему (дом), подслушав песенку мамы-козы и используя её, как ключ доступа. Однако не смог «пройти авторизацию» из-за хриплого голоса и вынужден был «подкорректировать» его, после чего дверь ему открыли. Отдельно стоит отметить тот факт, что во всех версиях сказки на несоответствие голоса ему указали сами козлята. История закончилась для них не лучшим образом.

К сожалению, в жизни мы всё чаще сталкиваемся с тем, что с возрастом люди забывают эту поучительную сказку и, став взрослыми, сами открывают незнакомцам двери, впуская к себе кого угодно: от торговых представителей и сектантов, до откровенных мошенников или грабителей. С такой же лёгкостью они сообщают посторонним информацию, которая может быть использована против них самих. Количество и разнообразие мошеннических схем по выманиванию каких-либо сведений (чаще всего пригодных для финансовых махинаций) растёт день ото дня. Под ударом могут оказаться как организации, так и обычные граждане.

В современном мире информация является одним из ценнейших ресурсов. Утечка данных может привести к весьма печальным последствиям, начиная от крупных финансовых потерь и заканчивая человеческими жертвами. Согласно ISO/IEC 2382:2015 информационная система представляет собой систему, предназначенную для хранения, поиска и обработки информации, к которой также относятся организационные ресурсы (человеческие, технические, финансовые и т.д.), которые обеспечивают и распространяют информацию. Именно уязвимость человеческих ресурсов мы рассмотрим в данной статье.

По мере развития технологий всё больше информации хранится и обрабатывается именно в электронном виде. Разнообразные «девайсы» и «гаджеты» могут иногда поведать о человеке больше, чем его окружение. Столь привычные и уже незаменимые в обычной жизни устройства сохраняют в себе фотографии, видеозаписи, переписки, рабочие документы, различную финансовую и прочую конфиденциальную информацию. Они как будто «впитывают» и несут в себе часть жизни своего владельца. А потому неудивительно, что эту оцифрованную информацию человек стремится защитить максимально надёжно. И со временем пользователю начинает казаться, что если он надежно защитит свой компьютер (планшет, телефон, локальную сеть – неважно), то его информация будет в

безопасности. Однако не стоит забывать, что в системе человек-компьютер уязвимым звеном всегда будет оставаться не машина, а сам человек.

Ещё в 1930 году советский учёный Н.М. Добротворский поднимал вопросы взаимодействия человека и машины, выделив то, что впоследствии назовут «человеческий фактор». Согласно Большой Советской Энциклопедии, учёт человеческих факторов являются неотъемлемой частью проектирования, создания и эксплуатации машин и технических систем, необходимым условием повышения производительности труда и качества продукции. Наиболее полно такой учёт осуществляется при проектировании деятельности человека в системах «человек - машина».

Таким образом, мы в очередной раз убеждаемся в том, что ещё при подготовке и обучении специалистов в информационной сфере, особое внимание надо уделять человеческому фактору и его роли в информационных системах. Так, предлагая своим студентам подготовить выступления по темам «угрозы информационной безопасности» и «методы защиты информации», я неоднократно сталкивался с тем, что наиболее подробно они рассматривали всю техническую сторону вопроса: системы контроля доступа, персональную идентификацию, ключи и шифрование данных, защиту сетей, программно-технические методы и т.д. Дыры в безопасности, связанные с человеческим фактором, обычно комментировались дежурной фразой «применять организационные методы защиты». Примеры подобных уязвимостей обычно приводились с трудом, не хватало понимания того, как через слабости человека пробивается брешь в информационной безопасности.

Если провести анализ известных случаев взломов и проникновений в защищённые информационные системы, то вы увидите, что большинство из них были связаны именно с человеческим фактором. Случаи умышленной кражи, порчи или уничтожения информации сотрудниками внутри своей организации мы сейчас рассматривать не будем. Такие проблемы чаще всего решаются на уровне подбора кадров и жёсткого разграничения доступа. Последствия же разбираются постфактум с привлечением ответственных за безопасность внутри организации, а также соответствующих служб органов внутренних дел.

Для нас интерес представляют ситуации, когда человек неумышленно оставляет «открытые двери» в информационной безопасности и не придаёт должного значения произошедшему с целью минимизации последствий. Как примеры можно упомянуть потерю рабочего пропуска или банковской карты без дальнейшей их блокировки, удаление или изменение какой-либо информации по неосторожности, оставление в доступных местах записанных паролей, ключей доступа, конфиденциальной информации и т.п.

В подобных случаях сотрудникам должна изначально по всем ключевым моментам разъясняться ситуация с личной ответственностью за информацию, с которой они работают. Должны быть составлены соответствующие инструкции. Необходимо проводить беседы и разъяснять порядок действий в той или иной ситуации для минимизации негативных последствий. Неоднократно за собственную рабочую практику я наблюдал ситуации, когда система контроля доступа нарушалась простым «придержите дверь, пожалуйста», когда ключи ЭЦП с правом подписи контрактов оставлялись в ящике стола, логины и пароли для доступа к компьютеру обнаруживались на бумажке под клавиатурой или в рабочем блокноте на столе. Такие случаи необходимо отрабатывать сразу же, проводить повторные инструктажи сотрудников, напоминать о недопустимости подобных деяний.

Отдельным пунктом стоит упомянуть случаи, когда злоумышленники проникают внутрь защищенной информационной системы, пользуясь обычными слабостями человеческого характера. Чаще всего это связано с тем, что на многие события люди реагируют автоматически, привычным для них способом. Об этом писал в своей книге «Психология влияния» Роберт Чалдини. Серьезно и аналитически человек реагирует только на ту информацию, на которую у него есть время и желание, в остальных случаях реакция обычно идёт по типу «щёлк, зажужжало». Также у сотрудников, чья работа однообразна, утомительна и предполагает обработку большого количества информации, часто срабатывает рефлекс: позвонили и сказали, что надо сделать - делаем. В качестве примера подобных действий Роберт Чалдини упоминает эксперимент, проводившийся психологами, которые обзванивали медсестёр в больницах и, представившись врачом, давали распоряжение ввести смертельную дозу препарата пациенту. Медсёстры понимали, что делают, но в силу загруженности по работе и давления авторитета позвонившего, шли выполнять поставленную задачу. Останавливали их уже на входе в палату. Подобные методы воздействия получили название социальная инженерия.

Одним из родоначальников социальной инженерии был Кевин Митник, который в своей книге «Искусство обмана» прямым текстом говорит о том, что намного проще получить доступ, воздействуя на людей, чем пытаться взломать систему.

Задача с проникновением в чужую информационную систему намного упрощается, если провести предварительную разведку и запастись сведениями, находящимися в открытом доступе: имена сотрудников или знакомых (особенно руководства, друзей, родственников), номера телефонов, род занятий, увлечения и т.д. Всё это может быть использовано как для проникновения на объект, так и для последующего воздействия через телефон, смс, электронную почту и т.д.

Выбрав «жертву», злоумышленник попытается втереться в доверие, ссылаясь на доступную ему информацию. После чего он может уговорить или сообщить ему что-то, или же выполнить какие-то

действия. Подобным образом сейчас работают мошенники, действующие через социальные сети или телефон, выманивая у доверчивых людей деньги.

Для проникновения в организации чаще всего используются рядовые сотрудники, которые хоть и не обладают высоким уровнем допуска, но могут открыть доступ к «следующей ступени». Полученные сведения собираются, анализируются и используются для воздействия на сотрудника более высокого ранга.

Такой способ получил название претекстинг, то есть работа по заранее составленному сценарию. Для атаки использоваться может как телефонный звонок, так и переписка. Мошенник может, например, сделать заказ, сославшись на какого-то доверенного клиента и не оплатить его. Другой распространённый вариант – представиться сотрудником техподдержки. Как показывает практика, доверчивые люди запросто могут называть свои пароли или же выполнять какие-то указания, полученные от мнимого сотрудника. Потребовать какой-то достоверной «авторизации» догадываются, увы, далеко не все.

Другой способ основывается на закидывании «приманки» - фишинг (от англ. «рыбалка»). Это может быть электронное письмо со ссылкой на поддельную страницу, оформленную в подражание какому-нибудь известному сайту. Как только человек вводит туда логин и пароль, он передаёт их мошенникам. Другой вариант - смс, подписанное, например, банком с настораживающим текстом вроде «Ваша карта заблокирована, с вами свяжется сотрудник службы безопасности банка». А следом звонок от мошенника, который попросит сообщить ему сведения о банковской карте.

Ещё один вариант атаки - троянский конь. Главная задача - заинтересовать потенциальную жертву. И не так важно чем - «вы выиграли в лотерею» или «смотри, тут твои фото выложили с корпоратива»… А дальше любопытство или алчность сделают своё дело. Вариант «дорожное яблоко» отличается лишь тем, что используются подкинутые флешки, диски и т.д. А на них уже будет находиться вредоносное ПО. И чем более «аппетитно» будет выглядеть это яблоко, тем больше шансов, что его «надкусят». Варианты – надписи о секретности или конфиденциальности содержимого, стилизация под установщик игры или программы и т.п.

Квид про кво (услуга за услугу) – вариант, в котором давление идёт на естественное желание отблагодарить за оказанную услугу. Например, вам звонят и спрашивют, есть ли у вас такая-то проблема, а затем решают её. Взамен просят осуществить какие-то действия, или просто подсказать по какому-то вопросу. Проникшийся доверием к «помощнику» человек способен в разговоре сказать очень много лишнего.

Для противодействия подобным мошенническим действиям необходимо регулярно проводить инструктажи сотрудников. Стоит разъяснить им, что информация, которую легко найти в открытом доступе, не может служить для авторизации.

Также стоит сказать о том, что при любых подозрительных просьбах необходимо проверить информацию по внутренним источникам прежде, чем что-либо делать. Сплошь и рядом встречаются истории о том, как пожилые люди бегут класть деньги на незнакомый номер только потому, что с него пришло сообщение вида: «Мама, я попал в аварию, срочно положи … рублей на этот номер». Или же подобная информация озвучивается по телефону от третьих лиц («ваш сын/дочь попали в аварию…»). В таких случаях жертвы далеко не всегда догадываются хотя бы позвонить человеку, о котором идёт речь.

Подводя итоги, хочется сказать о том, что разрабатывая «организационные методы защиты информации», необходимо понимать, что, даже обнаружив какую-то угрозу и проинструктировав о ней сотрудников или просто близких вам людей, нельзя быть до конца уверенным, что эта информация останется навсегда усвоенной. Регулярные инструктажи по защите информации должны быть частью вашей системы безопасности наравне с программно-техническими методами.

Не будет лишним напомнить даже взрослому человеку, что нельзя открывать дверь кому попало - за ней могут оказаться волки.

СПИСОК ЛИТЕРАТУРЫ

1. Верзун Н.А., Колбанев М.О., Татарникова Т.М. Аспекты безопасности информационно-экономической деятельности // Технологии информационно-экономической безопасности: сб. статей сотр. каф. ИС и Т. – СПб.: Изд-во СПбГЭУ, 2016. – С.52–56.
2. Митник К. Д., Саймон В. Л. Искусство обмана. М.: Компания АйТи, 2004. 359 с.
3. Чалдини Р, Психология влияния. СПб: Питер, 2011. 304 с.

УДК 811.116.1

ИНФОРМАЦИОННО-КОММУНИКАТИВНЫЕ ТЕХНОЛОГИИ КАК ИНСТРУМЕНТАЛЬНАЯ СРЕДА ПОДДЕРЖКИ УЧЕБНОГО ПРОЦЕССА

Колоколова Лидия Петровна
Стерлитамакский филиал Башкирского государственного университета
Россия, Республика Башкортостан, Стерлитамак, пр. Ленина, д. 49
emails: 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.*

INFORMATION AND COMMUNICATION TECHNOLOGY AS AN INSTRUMENTAL ENVIRONMENT SUPPORT OF EDUCATIONAL PROCESS

Lidia Kolokolova
Sterlitamak Branch of Bashkir state university
Russia, Republic of Bashkortostan, Sterlitamak, Lenin Prospect, 49
emails: kollidia@rambler.ru

Abstract. The article presents information and communication technologies, actively used in the educational activity in describing new material, at the stage of consolidation of the material, at controls and examination, as well as independent work. Process technologizing accelerate the transfer of knowledge and learning, promotes formation of a language picture of the world, provides interaction the teacher and the student in modern systems of open and distance education.

Keywords*: Information and communication technologies; computer education; interactive whiteboard; software.*

Введение. Время не стоит на месте. Изменяется и развивается общество, а вместе с ним изменяется система образования. Создаются новые средства обучения и устанавливаются требования к уже используемым средствам обучения. В результате стремительного роста научно-технического прогресса каждые десять лет в мире происходит удвоение объёма научных знаний. Данный фактор вызывает существенное увеличение количества информации, используемой в сфере обучения, и её усложнение. В российской системе образования наблюдается устойчивый интерес исследователей к привлечению информационно-коммуникативных технологий в преподавание лингвистических дисциплин. 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.

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 «Фонетическая система современного русского литературного языка» ключевым понятием является фонетическая транскрипция, представляющая собой передачу на письме графемами-буквами и специальными дополнительными знаками звучания различных по величине отрезков живой речи. Потребность в транскрипции была обусловлена зарождением сравнительно-исторического языкознания и развитием фонетики как науки. В специальных лингвистических трудах обычно применяется транскрипция Международной фонетической ассоциации, основанная на латинской графической системе. Бесспорно, используя интерактивные технические средства, можно детально представить фонетическое письмо и познакомить студентов с системой важных знаков транскрипции. Кроме того, интерактивная доска может быть использована при изучении артикуляционно-акустической системы современного русского литературного языка. Например, артикуляционная характеристика системы консонантизма предполагает следующие артикуляционные признаки:

1) характеристика согласных звуков по участию голоса и шума (сонорные и шумные);

2) характеристика согласных звуков по участию голосовых связок (шумные звонкие и шумные глухие: [б] - [п], [в] - [ф], [г] - [к], [з] – [с] и т.п);

3) характеристика согласных звуков по способу образования шума в полости рта (щелевые, смычные, аффрикаты (смычно-щелевые));

4) характеристика согласных звуков по месту образования шума в полости рта (переднеязычные (зубные, нёбные), среднеязычные, заднеязычные);

5) характеристика согласных звуков по наличию/отсутствию палатализации (мягкие и твердые: [б] - [б’], [в] - [в’], [г] - [г’], [д] - [д’] и т.п.).

Таким образом, предложенная информация на занятиях по «Фонетике» современного русского литературного языка будет способствовать образному, зрительному восприятию учебного материала.

При изучении лексической системы современного русского литературного языка информационно-технические средства могут быть использованы при знакомстве с терминологическим аппаратом. В ходе занятий по разделу «Лексикология» студент должен овладеть определенным запасом довольно сложных лингвистических терминов, уметь профессионально квалифицировать языковые факты, формировать лингвистическое чутьё. Терминологический словарь составляет теоретическую основу изучаемой дисциплины, включает в себя словарные статьи по наиболее частотным терминам с дефинициями по теме «Лексикология. Фразеология. Лексикография», встречающимся в вузовских учебниках лингвистического цикла, лекционных курсах, на практических и семинарских занятиях, при изучении студентами курса сравнительной лексикологии и в школьной практике, при чтении периодических изданий не только популярных, но и академического типа. Помимо толкования терминов в терминологическом словаре приводятся примеры из ряда языков, особенно из

истории развития русского языка, в его литературном варианте, просторечии и диалектах. Особенностью данного словаря является то, что он многофункционален (перевод терминов на изучаемые языки предваряется этимологическими сведениями). Например, в словарной статье «основные признаки слова (по теории А.И. Смирницкого)» представлены фонетические, лексико-грамматические и лексико-семантические признаки слова. В свою очередь, к фонетическим признакам слова относятся следующие особенности слова: 1) цельность и единооформленность, 2) фонетическая оформленность, 3) недвуударность, 4) непроницаемость, 5) постоянство звучания и значения. Лексико-грамматическим признакам слова включают такие свойства слова, как 1) изолируемость, 2) цельность и единооформленность, 3) лексико-грамматическая отнесенность. К лексико-семантическим признакам относят 1) фразеологичность, 2) номинативность, 3) воспроизводимость, 4) семантическая валентность.

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.

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» и т.д.

Но не стоит забывать, что главным источником получения информации на занятиях остается слово педагога. И только при методически грамотном использовании слова педагога и технических средств обучения, возможно успешное усвоение материала.

Совершенно очевидно, эффективность обучения может быть значительно повышена с помощью ИКТ, применяемых в различных оптимальных для данных занятий сочетаниях с другими средствами обучения.

СПИСОК ЛИТЕРАТУРЫ

1. Колоколова Л.П. Современный русский 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 004.056

ФОРМИРОВАНИЕ ЭКЗЕМПЛЯРОВ ОНТОЛОГИЧЕСКИХ КЛАССОВ ПРИ ОБРАБОТКЕ НЕСТРУКТУРИРОВАННЫХ ДАННЫХ В РЕШЕНИИ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Полтавцева Мария Анатольевна, Печенкин Александр Игоревич
Санкт-Петербургский политехнический университет Петра Великого,
Россия, Санкт-Петербург, ул. Политехническая, д. 29,
emails: poltavtseva@ibks.spbstu.ru, pechenkin@ibks.spbstu.ru;

***Аннотация*:** В статье рассмотрены вопросы работы с неструктурированными данными при решении задач информационной безопасности. Приводится специфика и классификация данных с точки зрения автоматизированной обработки. Рассматривается вопросы соотнесения данных с классами онтологии предметной области и формирования экземпляров. Вводятся понятия дискретности и полноты онтологических концептов и определяются необходимые структуры метаданных.

***Ключевые слова**: неструктурированные данные; анализ; онтологии; информационная безопасность*

THE ONTOLOGICAL CLASSES INSTANCES GENERATION WHEN PROCESSING SEMISTRUCTURED DATA IN SOLVING INFORMATION SECURITY CHALLENGES

Poltavtseva Maria Anatolevna, Pechenkin Alexander Igorevich
The St. Petersburg State Polytecnical University Petra Velikogo,
Russia, St. Petersburg, Politechnicheskaya str. 29,
emails: poltavtseva@ibks.spbstu.ru, pechenkin@ibks.spbstu.ru;

Abstract: The article presents working with semistructured data due to the solution of information security problems. Given the specificity and classification of these data automated processing. The novelty of the paper is in the questions of data and ontology classes (domains) correlation. We introduce the concepts of discreteness and completeness of the ontological concepts and define the required metadata structure.

***Keywords**: semistructured data; data analysis; ontology; information security*

Введение. Развитие автоматизации и методов машинной обработки данных, а также рост распространенности и сложности автоматизированных систем приводит к необходимости применения автоматизированных методов не только к процессам обработки данных, но и к решению задач обеспечения их безопасности. В этом направлении необходимо отметить применение методов Data Mining и машинного обучения в области обнаружения вторжений [1] и [2], управления рисками ИБ [3], построения SIEM – систем [4]. Можно выделить комплексные работы, например, [5], также выделяющие вопросы обнаружения аномалий и сканирования, профилирования трафика, проблемы конфиденциальности. В целом, необходимо отметить, что все эти решения сконцентрированы на интеллектуальном анализе определенных структурированных наборов данных (дампов сетевого трафика, логов информационных систем и систем безопасности, структурированной информации автоматизированных систем.

Развитие и расширение применения информационных технологий приводит не только к их проникновению во все сферы жизни, включая здравоохранение, образование и бытовое общение, но и эволюцию атак на личность, информационные и физические объекты с использованием компьютерных технологий. Одной из основных тенденций является использование методов социальной инженерии и фишинга, причем в том числе, в атаках на промышленные объекты[7]. Самыми распространенными атаками в банковской сфере за период с 01 июня 2015 г. по 31 мая 2016 г. ЦБ РФ признает рассылки электронных сообщений, содержащих вредоносное ПО[8]. Аналогичные тенденции отмечают и другие исследователи [9]. Таким образом, на сегодняшний день особенностью информационной безопасности частных, корпоративных и даже промышленных объектов является обеспечение не только сетевой и технической безопасности, но и безопасности относительно применения злоумышленниками социально-культурных методов.

В то же время, распределенность современных организаций, высокая численность сотрудников, обилие социальных сетей и медиа, электронных профилей и тому подобных решений не позволяет провести какой-либо комплексный анализ безопасности, включающий их как информационно – телекоммуникационный, так и социальный профиль (включая сайт, порталы партнеров и т.д.). Таким образом, возникает задача автоматизированного анализа не только структурированных (компьютерных) данных узкой предметной области, но широко спектра неструктурированных данных для решения различных задач информационной безопасности. Таких, как оценка защищенности, выявление угроз, проведение расследований, тестирование на проникновение и других.

Неструктурированные данные в области информационной безопасности.

Исторически неструктурированными данными назывались простые типы данных, не имеющие какой-либо внутренней структуры [10] (символы, числа и т.д.). Однако, со временем в этот термин стал вкладываться совсем другой смысл, присущий ему и на сегодняшний день. До сих пор нет четкого определения неструктурированных данных. Как правило, к информации такого рода относят [11] файлы документов, электронные сообщения, видеофайлы, изображения и т.д. Несмотря на то, что все эти сведения имеют определенную внутреннюю структуру, в том числе, связанную с семантикой данных (например, заголовок электронного сообщения), обычно форма их хранения не позволяет простого применения методов анализа (например, методов классификации или кластеризации информации).

Мы можем сказать, что к неструктурированным данным на сегодняшний день относят информацию, в явном виде, без предварительной обработки, не пригодную для выполнения задач анализа. Когда говорят о неструктурированных данных в современных информационных системах, выделяют следующие признаки [12]:

Разнообразие. Речь идет о многообразии представлений данных. Сюда входят как форматы данных (видео, изображения, текст), так и особенности самого формата. Например, текстовые данные (которые часто отождествляются с неструктурированными данными) могут быть представлены в виде плоского текста, сообщений (e-mail, социальных сетей и других), комментариев, статей СМИ и так далее.

Неоднозначность. Один и тот же набор данных может иметь разный смысл, в зависимости от контекста, языковых и культурных особенностей (как создателя, так и потребителя информации). Сюда же можно отнести субъективность и эмоциональную окрашенность большого количества неструктурированных данных, особенно представленных в естественно – языковой форме (например, публикации в СМИ и блогах).

Динамичность. Со временем может меняться как структура такого рода сведений, так и их значение.

На сегодняшний день анализ данных с такими характеристиками является динамично развивающейся областью. Существуют общие подходы к обработке неструктурированных данных, выделяемые специалистами [12], такие как:

1. Разработка онтологии – семантического описания предметной области, позволяющего систематизировать и установить связи между понятиями в ней. Онтология, представленная в том или ином виде, включает понятия, извлеченные из данных и связи между ними. В ряде задач по обработке неструктурированной информации онтология может использоваться в неявном виде.
2. Поиск упоминаний, категоризация и извлечение фактов. Найденные понятия и факты могут быть сопоставлены с онтологией для определения их смыслового места в описании предметной области, фиксации связей между ними.
3. Выделение закономерностей. На основании оцененных фактов, онтологических сущностей, их свойств и взаимосвязей определяются общие характеристики между данными, заимствования, устанавливаются существующие тенденции. Выделение эмоциональной окраски, оценка интереса и отношения к выделенным фактам. Это процедура более глубокого анализа извлеченных фактов на основе антологии.

Можно обобщить данный перечень, выделив основные действия, производимые при обработке неструктурированных сведений в различных областях. При таком подходе можно обозначить несколько этапов. В зависимости от области применения задачи они могут присутствовать все или частично в процедуре обработки информации.

1. Предварительная обработка.
2. Извлечение понятий (категорий, фактов и т.д.).
3. Проведение анализа извлеченных сведений.

Такой порядок обработки будет применим к неструктурированным данным любого вида: текстовой информации, изображениям, видео и аудио фрагментам.

В общем случае неструктурированные данные в области информационной безопасности можно представить двумя категориями.

Формализованная информация.

Сюда относятся данные, полученные от технических устройств, результаты сканирований, журналы аудита, результаты работы автоматизированных систем. Эти данные имеют четкую структуру

(хотя и отличающуюся между собой), ясный источник, и, зачастую, этого набора сведений достаточно чтобы говорить об их семантическом наполнении. То есть, получая результат работы конкретного сканера мы можем с уверенностью сказать, что в заданном поле находятся сведения о найденной операционной системе, а не что-либо иное. Эта информаций относится к хорошо обобщаемым данным, хорошо поддающимся автоматизированной обработке. Основной сложностью по работе с ними является их разнообразие и, как следствие, необходимость сведения их из гетерогенных источников в общее представление об анализируемой системе.

Неформализованная информация.

К этой категории отнесем данные, касающиеся не технической сферы, хотя, конечно, они должны быть получены также с помощью автоматизированных средств, учитывая объемы информации. Сюда входят страницы сайтов сети Интернет (самой организации, ее партнеров, мероприятий, личные страницы сотрудников и т.д.), страницы социальных сетей, блоги другие слабо формализуемые источники данных. Их особенностью является невозможность зачастую точного установления семантической значимости сведений. Например, невозможно достоверно утверждать, что некто является сотрудником компании если его имя встретилось на ее сайте, также, как и предсказать семантические разделы страницы сайта. Упоминание организации в профиле социальной сети также не может гарантировать, что владелец профиля связан с компанией: он мог там учиться, сотрудничать или поместить у себя чужое сообщение. Таким образом, сразу установить семантическое наполнение неформализованных сведений не представляется возможным.

Применение онтологии для нормализации данных из гетерогенных источников.

Для нормализации, или приведения к единому представлению и унифицированному семантическому значению, данных на сегодняшний день применяется механизм онтологий [13] в том числе, в научной сфере [14]. Созданная на базе предметной области онтология представляет собой ее семантическое описание. Ассоциирование данных с экземплярами классов онтологий позволяет установить их семантическое значение, связи с другими понятиями и место в общей системе. В области информационной безопасности также ведется разработка онтологических представлений (см., например, [15]).

При анализе формализованных данных, возможно сразу автоматизированными средствами установить значимые метаданные [16], такие как источник информации, семантическое значение информационного поля. Таким образом, в большинстве случаев возможно однозначно соотнести формализованные данные с экземпляром конкретного класса онтологии.

При этом отдельной задачей становится установление связей между объектами. Наличие связи между классами онтологии показывает наличие связи между их экземплярами, однако при подобном анализе в большом числе случаев нельзя однозначно сопоставить экземпляры классов онтологии друг другу. То есть, если на определенной онтологии O^{cl} заданы классы $o_s^{cl} \in O^{cl}$ и $o_e^{cl} \in O^{cl}$, связанные отношением g ($o_s^{cl} g\, o_k^{cl}$) тогда, при наличии экземпляра $e_j \in O, e_j\, r\, o_s^{cl}$ где r – отношение принадлежности экземпляра к классу, и экземпляров $E = \{e_k \mid e_k \in O, e_k\, r\, o_e^{cl}\}$ то необходимо определить, существует ли отношение $e_j g\, e_k, e_k \in E$. В противном случае, если отношение имеет модальность «должен», подобная ситуация подразумевает наличие неопределенного объекта $e_k^{'} \in E$, данные которого не установлены.

В большинстве случаев неформализованные данные могут быть единообразно представлены для предварительной обработки в виде плоского текста. При анализе неформализованных данных установление принадлежности к онтологии становится более сложной задачей, так как, зачастую, по имеющимся данным сложно идентифицировать объект и практически невозможно – его связи.

Для решения этой задачи онтологическому классу ставится в соответствие формат данных класса (если его можно выделить – например, множество форматов телефонных номеров или электронной почты) и модуль извлечения понятий из данных. Последний, базируясь на известных методах извлечения понятий и именованных сущностей [17], позволит достаточно точно определять сами сущности, хотя применение методов выявления семантических связей в исходном тексте, таких как описанные в [18] и [19], не дает достаточно хорошего результата. Подобные семантические графы позволяют скорее говорить о наличии связи между концептами, а не о семантическом наполнении этой связи. Таким образом, возникает оценка $r_{i,j} = \max(t_k)$- степень достоверности принадлежности i-го экземпляра к j-му классу, где t_k - нормированная степень достоверности k-го критерия принадлежности. Критерии принадлежности – оценки, позволяющие сделать вывод о принадлежности экземпляра классу (например, соответствие формату представления). Однако, не смотря на разную степень значимости, сами по себе эти оценки почти никогда не являются точными (t_k=1).

Также необходимо учесть дискретность большого числа данных. Под дискретностью в данном случае понимается различная степень полноты данных, начиная от самого общего представления и заканчивая детализированным. Например, телефон +7(812)XXXXXX говорит о стране (+7 – Россия) и городе (812-Санкт - Петербург), но не позволяет сделать вывод о самом номере, цифры которого неизвестны. Аналогично в случае программного обеспечения автоматизированные сканеры могут предоставлять сведения различной полноты.

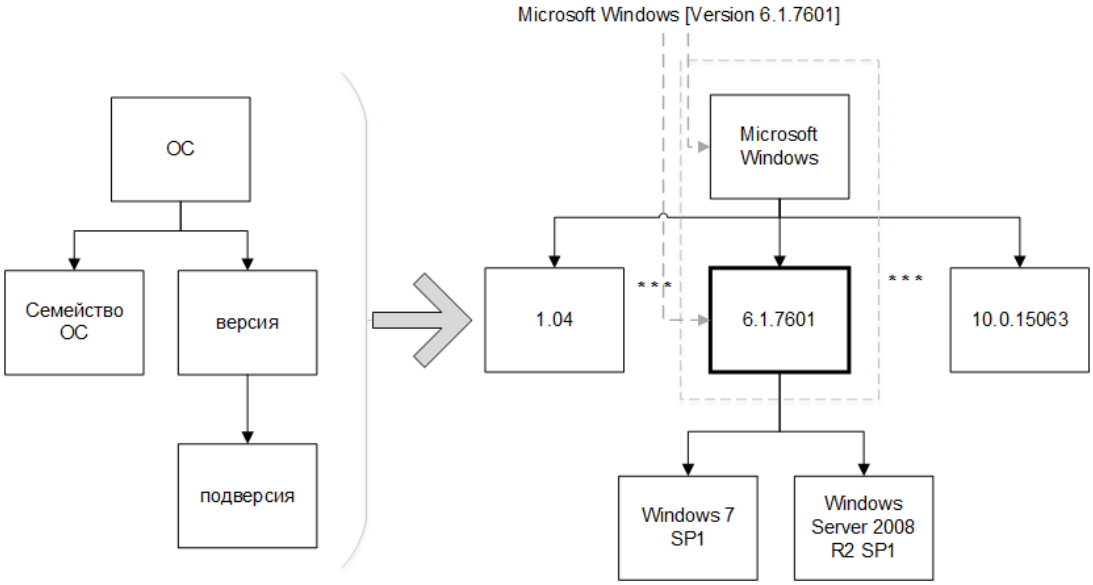


Рис. 1. Дискретное представление данных. Версия операционной системы.

На рисунке 1 приведен пример строки версии операционной системы и полного дерева версий. Соотнесение строки с узлами дерева на двух уровнях (Microsoft Windows и 6.1.7601) позволяет сделать вывод о семействе ОС, о ее версии, но не позволяет установить, что именно установлено (Windows 7 SP1 или Windows Server 2008 R2 SP1) так как, в данном случае, оба варианта возможны.

Таким образом, возникает понятие полноты или точности концепта, показывающего, на каком уровне детализации он представлен. Это дискретная оценка, которую можно представить как: $p_i = \frac{l}{n}$, где l – уровень дерева концепта, на котором (или до которого, считая от вершины) концепт определен, n – общее число узлов дерева. Для полностью определенного концепта p=1.

Для оценки полноты контекстов и учета описанной дискретной природы данных, с каждым классом онтологии оказывается связан признак дискретности $Discreetne\ \ ss \in \{0,1\}$ и, при Discreetness=1, иерархия полноты концепта H. Иерархия H позволяет выделить смысловые составляющие концепта, которые могут быть определены отдельно друг от друга. Таким образом, каждый концепт может рассматриваться на нескольких уровнях полноты. Для сопоставления концептов могут использоваться переходы на более высокие уровни полноты по PCR (Parent Child Relation [20]) связям.

Таким образом, метаданные, связанные с концептом онтологии информационной безопасности, для обработки неструктурированных данных, представляют собой кортеж <Discreetness, H>, где Discreetness - признак дискретности структуры данных в рассмотренном понимании, H – иерархия концепта при его дискретности. С каждым уровнем иерархии также может быть связан Format – формат данных, если он может быть определен.

Заключение. В работе рассмотрена проблема обработки неструктурированных данных при решении задач в области информационной безопасности. Выделены основные свойства неструктурированных данных (разнообразие, неоднозначность и динамичность) и определены специфические данные такого рода, характерные для области информационной безопасности. Дано понятие формализованных и неформализованных данных в рассматриваемом контексте.

Для определения семантики неструктурированных данных предлагается использовать онтологию информационной безопасности, как предметной области, по аналогии с задачами интеграции данных из гетерогенных источников. Рассмотрены специфические вопросы определения семантики данных и их соотнесения с классами онтологии. Определены необходимые метаданные для корректного соотнесения данных и экземпляров онтологических классов. Введены понятия дискретности и полноты концептов.

В работе почти не затронуты вопросы формирования онтологических связей. Показана неоднозначность формирования связи даже при корректном соотнесении с классами участвующих в связи единиц данных. Выявление и корректное формирование связей между экземплярами классов

онтологии является отдельной задачей, в целом, выходящей за рамки этой работы и относящейся к направлениям дальнейших исследований.

СПИСОК ЛИТЕРАТУРЫ

1. Lee, W., Stolfo, S.J. & Mok, K.W. Adaptive Intrusion Detection: A Data Mining Approach // Artificial Intelligence Review (2000) December 2000, Volume 14, Issue 6, pp 533–567. doi:10.1023/A:1006624031083
2. Miller S.T., Busby-Earle, C. Multi-perspective machine learning a classifier ensemble method for intrusion detection (Conference Paper) // ACM International Conference on Machine Learning and Soft Computing, ICMLSC 2017; Ho Chi Minh City; Viet Nam; January 2017, Pages 7-12
3. Alsadhan T., Park, J.S. Enhancing risk-based decisions by leveraging cyber security automation (Conference Paper) // 7th European Intelligence and Security Informatics Conference, EISIC 2016 Uppsala; Sweden; 17 August 2016 Pages 164-167
4. Lavrova, D., Pechenkin, A., Gluhov, V. Applying correlation analysis methods to control flow violation detection in the internet of things //Automatic Control and Computer Sciences , (8) , 2015 p. 735-740
5. Dua S., Du X. Data Mining and Machine Learning in Cybersecurity / Taylor and Francis Group, LLC 2011 248p.
6. Zegzhda, D.P. Sustainability as a criterion for information security in cyber-physical systems // Automatic Control and Computer Sciences Volume 50, Issue 8, 2016, Pages 813-819
7. Кибербезопасность 2016-2017: от итогов к прогнозам // https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2016-2017-rus.pdf
8. Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России // http://www.cbr.ru/credit/Gubzi_docs/fincert_survey.pdf
9. Угрозы и тенденции рынка информационной безопасности. Защита от атак «нулевого» дня // Jet Infosystems VII ежегодная конференция Центра информационной безопасности компании «Инфосистемы Джет» «Pro безопасность» 06.2016г.
10. Могилев А.В., Пак Н.И., Хённер Е.К. Информатика. М.: Академия, 2004 г. — 848 с
11. Роберт Д. Кугель Управление неструктурированной информацией Intelligent Enterprise №2 (91), 2004
12. Артем Гришковский Интегрированная обработка неструктурированных данных «Открытые системы», № 06, 2013
13. Бова В. В. Онтологическая модель интеграции данных и знаний в интеллектуальных информационных системах // Известия ЮФУ. Технические науки. 2015. №4 (165).
14. Кузнецов О.П., Суховеров В.С., Шипилина Л.Б. Онтология как систематизация научных знаний: структура, семантика, задачи // Труды конференции «Технические и программные средства систем управления, контроля и измерения» М., октябрь 2010г.
15. Stepanova T., Pechenkin A., and Lavrova D. Ontology-based big data approach to automated penetration testing of large-scale heterogeneous systems. In Proceedings of the 8th International Conference on Security of Information and Networks (SIN '15). ACM, New York, NY, USA, 142-149. 2015. DOI: http://dx.doi.org/10.1145/2799979.2799995
16. Когаловский М.Р. Метаданные, их свойства, функции, классификация и средства представления // Труды 14-й Всероссийской научной конференции «Электронные библиотеки: перспективные методы и технологии, электронные коллекции» — RCDL-2012, Переславль-Залесский, Россия, 15-18 октября 2012 г.
17. Grishman R. Information extraction: Techniques and challenges. // Information Extraction. Springer-Verlag, Lecture Notes in Artificial Intelligence, Rome, 1997.
18. Палагин А. В., Кривой С. Л., Петренко Н. Г. Концептуальные графы и семантические сети в системах обработки естественно-языковой информации // Математические машины и системы. 2009. №3(т.1)
19. Белоусов К.И. Деятельностно-онтологическая концепция формообразования текста [Текст]: дис. докт. филол. наук / К.И. Белоусов. – Оренбург, 2005. – 374.
20. Полтавцева М.А., Полтавцев А.А. Математические модели баз данных. Учебное пособие / А.А. Полтавцев, М.А. Полтавцева СПб. Изд-во Политехнического университета, 2017. – 236с.

УДК 004.042

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СЕТИ ИНТЕРНЕТА ВЕЩЕЙ СРЕДСТВАМИ НИЗКОРЕСУРСНОЙ КРИПТОГРАФИИ

Супрун Александр Федорович, Царьков Игорь **Сергеевич**
Санкт-Петербургский политехнический университет Петра Великого
Россия, Санкт-Петербург, Политехническая ул., д. 29
emails: afs54@inbox.ru, sator_nr@mail.ru.

***Аннотация*:** В статье рассмотрен безопасный протокол взаимодействия между узлами Интернета вещей.

***Ключевые слова**: Интернет Вещей; взаимодействие; протокол.*

THE NETWORK SECURITY OF THE INTERNET OF THINGS MEANS OF LOW-RESOURCE CRYPTOGRAPHY

Suprun Aleksandr, Tsarkov Igor
Peter the Great St.Petersburg Polytechnic University “SPbPU”
Russia, St. Petersburg, Polytechnicheskaya str, 29
emails: afs54@inbox.ru, sator_nr@mail.ru.

Abstract: In article the safe protocol of interaction between nodes of the Internet of things is considered.

***Keywords**: Internet of Things; interaction; protocol*

Введение. IoT (internet of Things, далее – Интернет вещей) представляет собой распределенную мультиагентную сеть, осуществляющую автономный сбор и обработку данных об окружающей среде. Интернет Вещей имеет представление как в реальном, так и в виртуальном пространстве.

В последнее десятилетие наблюдается лавинообразный рост числа агентов ИВ: на февраль 2017 года числа упомянутых агентов составило порядка 10 миллиардов устройств. По прогнозам

экспертов, к 2020 году количество агентов ИВ по всему миру может достигнуть 50 миллиардов устройств, а по самым оптимистичным прогнозам развития отрасли – 80 миллиардов. Подобный массив устройств, несмотря на малую среднюю мощность, нельзя оставлять беззащитным: примером последствий пренебрежения безопасностью ИВ являются нашумевшие в СМИ атаки ботнетов BrickerBot, Amnesia и Mirai, объединившие под собой сотни тысяч устройств, которые в последствии были использованы для проведения массированных DDOS атак.

Взаимодействие между узлами Интернета Вещей отличаются требованиями низкой нагрузки на узлы сети, малого объема пересылаемых данных и ограничениями энергопотребления узлов. В рамках исследования создан протокол, отвечающий данным требованиям, предоставляющий возможность построения защищенных каналов общения между узлами сети Интернета вещей.

Структура исследуемой модели, представленная на рисунке 1, была задействована для создания данного протокола. Под внешним контроллером подразумевается любой контроллер, выполняющий роль концентратора для датчиков, выполняющий промежуточные вычисления, либо объединение данных для последующей отправки на базовую станцию. В роли агентов выступают маломощные контроллеры датчиков. Далее под внешними контроллерами подразумеваются все элементы сети, кроме базовой станции.

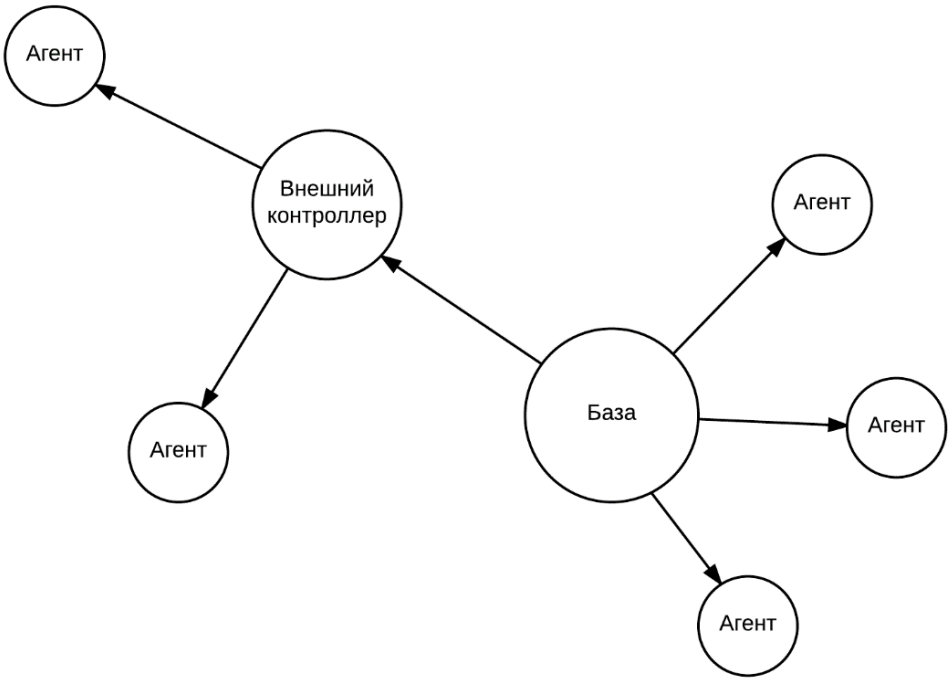


Рис. 1. Структура исследуемой модели

Рассматривались следующие нарушения безопасности системы:
– атаки на отказ в обслуживании внешних датчиков;
– атаки на отказ в обслуживании базовой станции;
– перехват данных канала «базовая станция ←→ внешний контроллер»;
– подделка данных канала «базовая станция ←→ внешний контроллер».

Следующие модели нарушителя рассматривались в рамках данной работы:
– внешний нарушитель (отсутствие доступа в сеть);
– внутренний нарушитель (наличие доступа в сеть);
– внутренний нарушитель (контроль агента сети);
– внутренний нарушитель (подделка агента сети).

Идентификация устройства производилась в соответствии с Блок-схемой алгоритма идентификации, представленой на рисунке 2.

Алгоритм представлен следующими действиями:

1) Базовая станция отправляет запрос новому устройству. В случае, если устройств подключается несколько – запросы обрабатываются в порядке достижения базовой станции.

2) Если запрос верен – на основе R/O метки устройства происходит генерация основной метки и её установка на базовой станции.

3) Метка пересылается устройству и устанавливается.

Делегация прав базовой станции возможно. Внешний контроллер может исполнять роль базовой станции, собирая информацию с подчиненных ему агентов. В рамках экспериментов были рассмотрены следующие варианты делегирования:

1) Внешний контроллер получает собственную таблицу ключей и осуществляет взаимодействие с подчиненными агентами аналогично базовой станции, отправляя на неё итоговый данные. Базовая станция не хранит метки подчиненных внешнему контроллеру устройств.

2) Внешний контроллер получает права базовой станции аналогично первому пункту, но не имеет права инициировать замену ключей. Замена производится путем последовательных запросов к базовой станции, при этом базовая станция хранит полный набор меток.

3) Внешний контроллер запрашивает данные с базовой станции при каждом опросе подчиненных агентов.

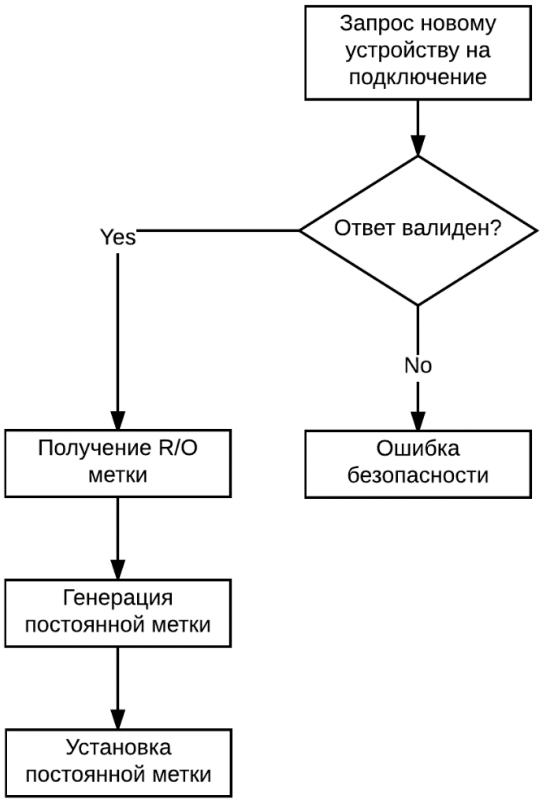


Рис. 2. Блок-схема алгоритма идентификации

Текущий протокол использует второй вариант. Таким образом, удалось избежать падения работоспособности внешнего контроллера с увеличением числа его агентов.

Обмен данными. Обмен данными осуществляется посредством пакетов, длиной 312 бит. Структура пакета представлена в таблице 1.

Таблица 1

Заголовок пакета

Заголовок [8 бит]	Флаги [8 бит]	Данные [264 бита]	Магическое число [16 бит]	Метка [16 бит]

Заголовок позволяет устройству идентифицировать пакет и тип устройства, от которого пришло сообщение. Тип устройства применяется для подтверждения корректности пакета. Поле флагов позволяет точно идентифицировать содержимое пакета и набор процедур, необходимый для его декодирования. Данные, в зависимости от набора флагов могут содержать либо ключ, либо данные с датчика, либо команду контроллеру. 264 бита информации позволяют, с одной стороны, достаточны для передачи ключа LW-алгоритма, а с другой – позволяют закодировать и передать данные или команду без фрагментации.

Структура поля данных представлена в таблице 2.

Таблица 2

Представление поля данных

Длина данных [8 бит]	Данные	Дополнение

Дополнение случайно генерируется отправителем (если поле не занято целиком) и занимает пустое пространство поля данных. Магическое число используется для подтверждения сеанса

общения между внешним контроллером и базовой станцией. Ответное магическое число вычисляется по формуле:

$$Magic_{answ} = Magic + Int(addition)_8 \ mod \ 2^{16}$$

$Magic_{answ}$– ответное магическое число

$Magic$ – полученное магическое число

$Int(addition)_8$ – целочисленное представление последних 8 бит поля данных.

Метка позволяет идентифицировать устройство, с которым происходит общение. Шифрованию в рамках общения подвергаются поля флагов, данных и магического числа. Инициализатором общения может являться как базовая станция, так и внешний контроллер.

Блок-схема алгоритма обработки пакета представлена на рисунке 3.

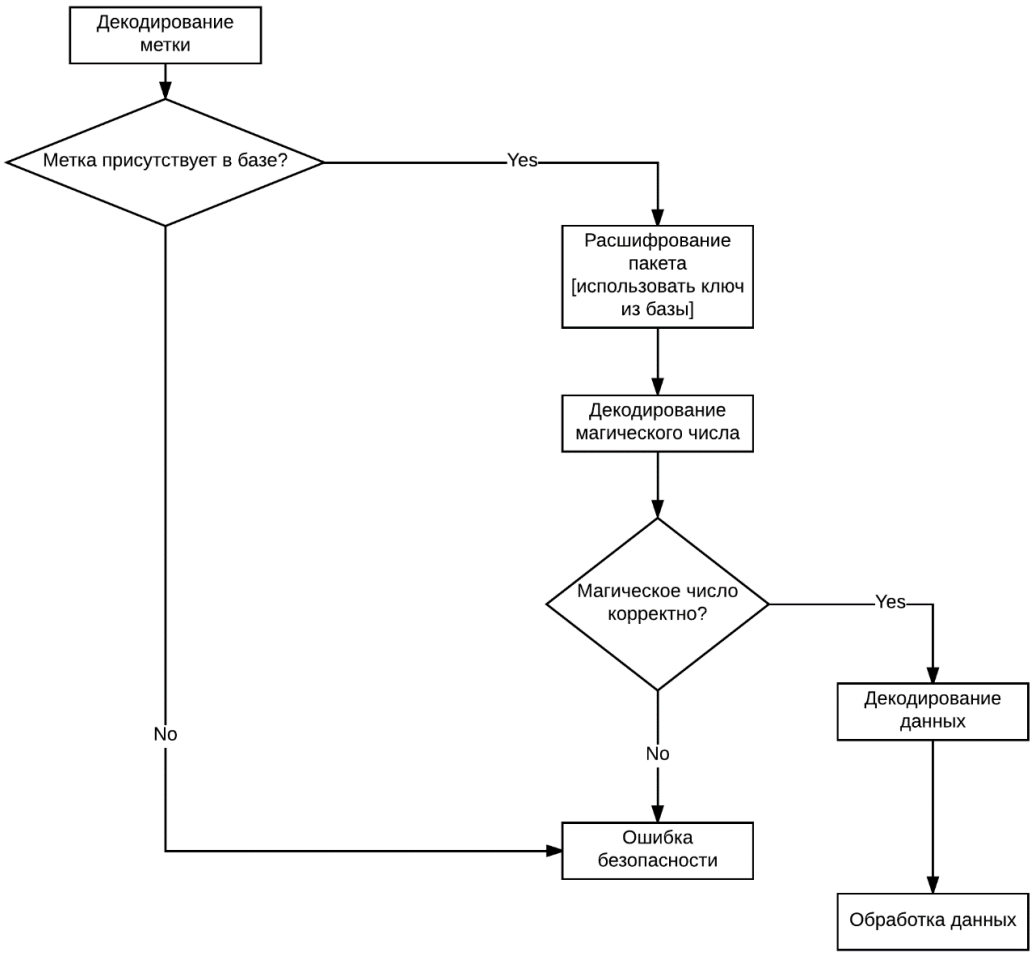


Рис. 3. Блок-схема алгоритма обработки пакета

Обновление ключа устройства. Инициатором обмена является базовая станция. Оптимальным решением для использования в рамках данного протокола является криптография на эллиптических кривых, за счет относительно высокой скорости работы, а также малого размера данных для обмена. Наиболее перспективным вариантом является применение схемы ECDH для обмена сеансовыми ключами. Параметры кривой, поставляемой на неинициализированном контроллере должны храниться в памяти базовой станции без возможности их изменить.

Заключение. В результате проведенного исследования был разработан протокол, позволяющий устанавливать соединения и обмениваться данными внутри защищенного канала между узлами сети ИВ. Разработанный протокол обладает следующими преимуществами:

- возможность однозначно идентифицировать устройство;
- многоуровневое подтверждение валидности сообщения;
- простота реализации;
- низкие требования к вычислительной мощности компонентов сети;
- низкие требования к пропускной способности канала сети.

СПИСОК ЛИТЕРАТУРЫ

1. Hannes Gross, Marko Holbl, Daniel Slamanig, and Raphael Spreitzer Privacy-Aware Authentication in the Internet of Things. [Электронный ресурс] / IACR Cryptology ePrint Archive. 2015. – Режим доступа: https://eprint.iacr.org/2015/1110.pdf свободный (дата обращения: 21.05.2017). – Загл. с экрана. – Яз. англ.

2. Hannes Gross, Marko Holbl, Daniel Slamanig, and Raphael Spreitzer Privacy-Aware Authentication in the Internet of Things. [Электронный ресурс] / IACR Cryptology ePrint Archive. 2015. – Режим доступа: https://eprint.iacr.org/2015/1110.pdf свободный (дата обращения: 21.05.2017). – Загл. с экрана. – Яз. англ.
3. Elias Yarrkov Cryptoanalysis of XXTEA. [Электронный ресурс] / IACR Cryptology ePrint Archive. 2010. – Режим доступа: https://eprint.iacr.org/2010/254.pdf, свободный (дата обращения: 21.05.2017). – Загл. с экрана. – Яз. англ.
4. Zheng Gong, Svetla Nikova, and Yee Wei Law KLEIN: A New Family of Lightweight Block Ciphers. [Электронный ресурс] / School of Computer Science, South China Normal University, China, Faculty of EWI, University of Twente, The Netherlands, Dept. ESAT/SCD-COSIC, Katholieke Universiteit Leuven, Belgium, Department of EEE, The University of Melbourne, Australia. 2012. – Режим доступа: http://www.smartsantander.eu/downloads/Presentations/gong12klein.pdf, свободный (дата обращения: 29.05.2017). – Загл. с экрана. – Яз. агл.
5. Wenling Wu and Lei Zhang LBlock: A Lightweight Block Cipher. [Электронный ресурс] / IACR Cryptology ePrint Archive. 2011. – Режим доступа: https://eprint.iacr.org/2011/345.pdf, свободный (дата обращения: 29.05.2017). – Загл. с экрана. – Яз. англ.
6. HIGHT Algorithm Specification. [Электронный ресурс] / Korea Internet & Security Agency. 2009. – Режим доступа: h ttps://seed.kisa.or.kr/html/egovframework/iwt/ds/ko/ref/01.+HIGHT+Algorithm+Specification.pdf, свободный (дата обращения: 29.05.2017). – Загл. с экрана. – Яз. англ.
7. Christophe De Canniere and Orr Dunkelman, Miroslav Knezevic KATAN & KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers. [Электронный ресурс] / Katholieke Universiteit Leuven, Department of Electrical Engineering ESAT/SCD-COSIC and Interdisciplinary Center for Broad Band Technologies Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium, Ecole Normale Sup´erieure ´ D´epartement d'Informatique. 2010. – Режим доступа: h ttps://pdfs.semanticscholar.org/2686/044f8a972325e1b23824430dea731d8e2817.pdf, свободный (дата обращения: 1.06.2017). – Загл. с экрана. – Яз. англ.
8. Ari Keränen, Carsten Bormann Интернет вещей: Стандарты и рекомендации. [Электронный ресурс] / Информационный сборник «Интернет изнутри». 2017 – Режим доступа: http://internetinside.ru/internet-veshhey-standarty-i-rekomenda, свободный (дата обращения: 5.06.2017). – Загл. с экрана. – Яз. рус.

УДК 371.39

ПЕДАГОГИЧЕСКИЕ И ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОГО ТЕСТИРОВАНИЯ НА РАЗНЫХ СТАДИЯХ ОБУЧЕНИЯ ДИСЦИПЛИНЕ

Титова Юлияна Францевна
Смольный институт Российской академии образования
Кафедра информационных систем, зав.кафедрой, к.пед.наук, доцент
Россия, Санкт-Петербург, Полюстровский пр., д.59
email: titova-stud@yandex.ru

Аннотация: В статье рассмотрены педагогические и технологические аспекты использования компьютерного тестирования на разных стадиях обучения дисциплине. Дана типология тестовых вопросов. Рассмотрен малоиспользуемый, но перспективный вид тестовых вопросов «вычисляемый». Описаны возможности использования компьютерных тестов, как на стадии обучения, так и на стадии контроля. Рассмотрены особенности настройки компьютерного теста в LMS Moodle в зависимости от педагогических целей.

Ключевые слова: *LMS-система; Moodle; методика; электронное обучение; тестовый вопрос; вычисляемый вопрос; тест, типология компьютерных тестов.*

PEDAGOGICAL AND TECHNOLOGICAL ASPECTS OF THE USE OF COMPUTER-BASED TESTING AT DIFFERENT STAGES OF LEARNING THE DISCIPLINE

Titova Yuliayna Frantsevna
Smolny Institute of the Russian Academy of education
Department of information systems, head of department, Associate Professor
Russia, Sankt-Peterburg, Polyustrovskiy PR., d. 59
email: titova-stud@yandex.ru

Abstract: the article deals with pedagogical and technological aspects of the use of computer-based testing at different stages of learning the discipline. Given typology test questions. Considered under-utilized, but promising form of test questions "calculated". The possibilities of using computer tests, during learning and during supervision. The features of the settings of the computer test in LMS Moodle, depending on pedagogical purposes.

Keywords: *LMS; Moodle; methodology; e-learning; the test question; a numerical question given test, types of computer tests.*

Все большее количество вузов внедряет системы управления образовательным контентом (LMS-системы) в учебный процесс. Одна из них - свободно распространяемая среда LMS Moodle - предоставляет богатые возможности организации электронного обучения: элементы для представления учебных материалов в виде файлов (текстовых, презентаций, видео и пр.), интерактивные элементы (рабочие тетради, форумы, чаты, опросы, задания), средства для создания контрольно-измерительных материалов (базы тестовых вопросов), средства анализа результатов обучения с использованием шкал. Как правило, среду с успехом используют наиболее передовые преподаватели, которые довольно хорошо владеют информационными технологиями, имеют интерес

к электронным формам обучения и способны самостоятельно освоить технологии работы в среде LMS. Хуже ситуация с основным контингентом преподавателей со слабой компьютерной подготовкой и отсутствием мотивации создания и применения электронных средств обучения [1]. Если государство и администрация вузов найдут формы повышения такой мотивации, то тогда на повестку дня встанут вопросы разработки педагогических методик использования возможностей LMS-систем в обучении. На сегодняшний день можно констатировать факт, что до сих пор отсутствует педагогическое обоснование правомочности, эффективности использования разнообразных возможностей LMS при обучении. Поэтому преподаватели используют элементы электронного обучения так, как умеют, и насколько хватает их знаний об используемой среде LMS. Однако при неумелом использовании возможностей среды можно получить отрицательный педагогический результат. Одним их таких отрицательных примеров является использование в тестах вопросов типа «множественный выбор», когда испытуемому задают вопрос и на выбор предлагаются варианты ответов. Даже при отсутствии знаний по дисциплине путем угадывания можно получить зачетный результат. В связи с этим от вопросов такого типа уже стали отказываться и на уровне государственного тестирования, а именно в тестах ЕГЭ по естественнонаучным дисциплинам. Для педагогически правильного использования тестирования в учебном процессе необходимо не только объяснять технологические возможности использования отдельных элементов среды, но и давать педагогическое обоснование, на какой стадии учебного процесса и в каком виде их применять. При этом надо учесть тот факт, что для большинства преподавателей в силу многих причин освоение среды LMS представляет большие трудности, и поэтому курсы по технологии работы в среде и педагогическим методикам использования среды надо проводить от простого к сложному.

В учебном процессе, как известно, выделяется учебная стадия и контролирующая стадия. С точки зрения электронного обучения предполагается, что студенту будут представлены учебные материалы в электронной форме. В самом простом случае это файл с конспектом лекции и файлы с примерами выполнения практических заданий. Такие ресурсы, по сути, являются заменой бумажных учебников. Но как проконтролировать, насколько правильно усвоил материал студент? Для этого среда LMS предоставляет возможность проверки знаний в форме тестирования.

Для организации компьютерного тестирования в современных LMS необходимо организовать базу вопросов и разработать тесты. Будем называть тестом совокупность вопросов, специальным образом отобранную из базы, на которые должен ответить обучающийся в соответствии с поставленной педагогом целью обучения. Здесь кроется первая проблема – многие преподаватели не видят разницы между тестом и тестовыми вопросами. В печатных учебных изданиях последнее время довольно часто стали встречаться тесты как формы проверки знаний. Эти тесты располагаются после параграфа или главы, и основной их целью является проверка знаний конкретно по данной теме. И вот по аналогии с таким «бумажным» тестом - преподаватели не отделяют тестовый вопрос как самостоятельную единицу. Это на бумаге тестовый вопрос встретится только один раз в одном тесте. Но когда речь идет об электронной среде и базе тестовых вопросов, их функция существенно расширяется. Как сказано выше, из тестовых вопросов можно составлять разные тесты, например, для проверки знаний по теме одной лекции, тест проверки знаний по теме программы, тесты для рубежного контроля и для итогового контроля. Электронный вопрос может присутствовать во всех этих тестах.

В LMS Moodle предлагается несколько типов вопросов, разной трудоемкости и технологической сложности. Наиболее простыми и в том, и в другом плане являются вопросы со множественным выбором, о которых говорилось выше. Большинство преподавателей и методистов знают только такую форму тестового вопроса, и поэтому она является самой распространенной в вузовской среде. Даже ФОСы требуют создавать, используя только эту форму вопроса. По этим причинам они наиболее часто используются преподавателями. Основная трудоемкость создания таких вопросов заключается в подборе неправильных ответов, которые бы «выглядели» как правильные. Негативной стороной является возможность подбора ответа студентом, т.к. зачастую довольно просто «отсечь» неправильные ответы. Именно поэтому такие вопросы должны иметь ограниченную применимость. Например, в тех случаях, когда вопросы заранее студенту не известны, что имеет место при официальном тестировании. Тем не менее, совсем отказываться от них не разумно. Вопросы такого типа можно успешно использовать для контроля усвоения терминологии курса, для проверки знания дат, фамилий, названий чего-либо. Для проверки терминологии общая структура вопроса может выглядеть следующим образом. В теле вопроса дается формулировка определения термина и ставится вопрос «О каком термине идет речь?». В ответе в качестве множественного выбора приводятся термины курса, из которых надо выбрать один. Ответов на выбор надо предложить достаточное количество (желательно более 6), чтобы уменьшить вероятность выбора правильного ответа случайным образом. В этом случае не надо придумывать неправильные ответы, и решается педагогическая задача усвоения терминологии.

Другой, более глубокий уровень тестовых вопросов представляют вопросы с коротким ответом. Технология создания таких вопросов не очень сложна и хорошо описана – надо составить формулировку вопроса, на который студенты должны ввести в качестве ответа короткую фразу произвольным образом, обычно 1-3 слова. Трудоемкость разработки такого вопроса заключается в

подборе формулировок правильных ответов и описании их. Значительную помощь в составлении вопроса оказывает использование технологии подстановочных знаков, что позволяет отбросить возможные окончания слов. Возможные варианты ответов можно определить в ходе анализа ответов студентов на вопрос и тем самым при необходимости откорректировать его. Педагогическая ценность таких вопросов гораздо выше, потому что студент должен понять, о чем речь, найти и прочитать нужное место в учебнике, а также сформулировать кратко ответ. Кроме этого решается задача правильного написания слов (в т.ч. и терминов). Здесь уже нет готовых ответов, чтобы методом подбора найти правильный. Однако надо констатировать факт, что в учебном процессе эти вопросы используются очень мало, особенно преподавателями некомпьютерных дисциплин.

В современных LMS также присутствует форма тестового вопроса «на сравнение». В таких тестах испытуемому предлагается к заданным формулировкам (вопросам) подобрать правильные ответы и ограниченного набора. Количество вопросов и ответов может не совпадать. На разные вопросы может быть один и тот же ответ. В какой-то мере этот тип вопроса поход на вопрос со множественным выбором, но у него больше аспектов использования. Например, с помощью таких вопросов можно попросить установить правильную последовательность расположения чего-либо (дат, исторических событий, действий в алгоритме и пр.). Технология создания такого теста очень проста – надо описать все формулировки и указать правильный ответ к каждой. Неправильные ответы тоже гораздо проще придумать.

И, наконец, хочется остановиться на вычисляемых вопросах. Это на настоящий момент практически неиспользуемая форма тестовых вопросов. По своей сути такой вопрос позволяет организовать решение некой вычислительной задачи, в которой традиционно заданы исходные данные и требуется получить результат с использованием одной или нескольких формул. Вычисляемые задачи используются при обучении экономическим, естественнонаучным, в том числе и компьютерным, дисциплинам. В традиционной вычисляемой задаче формулировка включает описание ситуации, набор известных исходных данных и вопрос, что требуется найти. Задача решается в одно или несколько действий. На каждом этапе вычислений применяется формула, связывающая известные и неизвестные величины. В большинстве случаев набор исходных данных является минимально необходимым, т.е. все исходные данные при решении так или иначе должны быть использованы. В любой дисциплине можно выделить типовые задачи, выстроить их в методической последовательности освоения. И самая большая проблема – это научить студентов видеть в формулировке некой конкретной задачи целую категорию, и применять типовой для этой категории метод. Решить эту проблему можно в том числе и многократным решением типовых задач, что не позволяет делать современный процесс обучения. Электронный вычисляемый вопрос позволяет на основе одной формулировки сгенерировать целую категорию типовых задач. Во время тестирования к типовой формулировке добавляется случайный набор исходных данных, что делает конкретную задачу уникальной для каждого тестируемого, чем обеспечивается индивидуализация тестирования и невозможность механического запоминания ответа. Наличие электронных вычисляемых вопросов позволит студенту самостоятельно тренироваться решать задачи в том объеме, пока он уверенно не освоит категории типовых задач. И степень его умений будет зависеть только от его прилежности, способностей и упорства.

Создание вычисляемого вопроса включает описание типовой формулировки задачи, программирование формулы правильного ответа и создание наборов исходных данных. Сама формулировка – это, по сути, обобщенное описание некоторого класса однотипных задач, наборы исходных данных позволяют сформировать множество задач с одинаковыми формулировками и с разными исходными данными. Для создания наборов данных в LMS-среде предусмотрена технология автоматической генерации чисел в заданном диапазоне с заданной погрешностью, что снижает трудоемкость создания вопросов, что избавляет преподавателя от придумывания наборов данных.

Проблемы использования вычисляемых вопросов заключаются в том, что, во-первых, не понятно, как преподаватели узнают о том, что такая форма вопросов есть, во-вторых, кто их научит создавать такие вопросы, и в-третьих, что технология их создания предполагает, хоть и несложное, но программирование формулы. Администраторы системы во многих вузах ограничиваются чисто администраторскими функциями, а именно создание учетных записей, ведение списка групп, общая настройка системы. В их функции не входит исследование возможностей системы и обучение преподавателей, а также методическое обоснование использования элементов системы в учебном процессе. Именно поэтому при организации системы электронного обучения должен быть предусмотрен методист, решающий именно такие методические задачи. Проблема программирования формул решается тем, что если в дисциплине есть вычислительные задачи, которые предполагают какой-никакой алгоритм решения, значит, и преподаватель способен освоить несложные элементы программирования.

У электронных вычисляемых вопросов есть и более важная функция, чем просто организация решения традиционной вычислительной задачи. Повысить обучающий эффект можно также за счет использования разработки так называемых комплексных задач. В данном контексте под комплексной задачей понимается описание в тестовом вопросе ситуации, по которой можно задать несколько

вопросов, использующих для ответа разные формулы. Для такой ситуации задается набор исходных данных, необходимый для ответа на все вопросы. С точки зрения одного конкретного вопроса к ситуации этот набор данных будет избыточным. Такой подход позволяет получить вместо одного вопроса несколько тестовых вопросов с использованием одного и того же набора данных. Кроме этого, в среде есть также возможность отображения в теле вопроса исходных данных, которые сами получены по некоторой формуле, что позволяет использовать тот же набор данных для формулировки обратных задач и тем самым еще большего расширения круга вопросов по описанной ситуации. Допустим, у нас есть 3 исходных величины (*a, b, c*), по которым можно вычислить 2 других величины по некоторым формулам, например, *d(a, b)* и *f(b, c)*. По заданному набору данных (*a, b, c*) можно создать вопросы с такими формулировками (неполный перечень):

— дано *a, b, c* найти *d*; - это прямая задача с одним действием
— дано *a, b, c* найти *f*; - это прямая задача с одним действием
— дано *b, c*, *d* найти *a*; - это обратная задача с одним действием
— дано *f, c*, *d* найти *a*; - это обратная задача с двумя действиями
— дано *f, b*, *d* найти *a*; - это обратная задача с одним действием
— дано *f, b*, *d* найти *c*; - это обратная задача с одним действием и т.д.

Понятно, что увеличение количества исходных данных в геометрической прогрессии расширяет круг вопросов, которые можно задать. Использование комплексных ситуаций в тестовых вычислительных задачах формирует у студента интегрированные знания по курсу. Такие комплексные задачи намного ближе к реальным ситуациям. Ведь в жизни и профессиональной деятельности именно человек из множества величин должен понять, какие нужны для ответа на тот или иной вопрос.

Ниже приводится пример комплексной ситуации в курсе «Имитационное моделирование». На рисунке приводится описание ситуации по простейшей модели системы массового обслуживания с очередью и 1-м узлом обслуживания из n каналов, построенной в среде AnyLogic. Вместо чисел, отображаемых при проигрывании модели, указаны параметры. При создании тестового вопроса часть этих параметров задаются в наборе данных, другие вычисляются по формулам, которые скрыты от студентов.

Обобщенная формулировка ситуации: На рисунке (рис. 1) представлена функциональная модель системы массового обслуживания (СМО) в некий текущий момент времени. Известно, что за единицу времени в СМО поступает в среднем {x} заявок. Каждая заявка обслуживается каналом обслуживания в среднем {y} единиц времени. Считаем, что поток заявок и поток обслуживания являются простейшими.

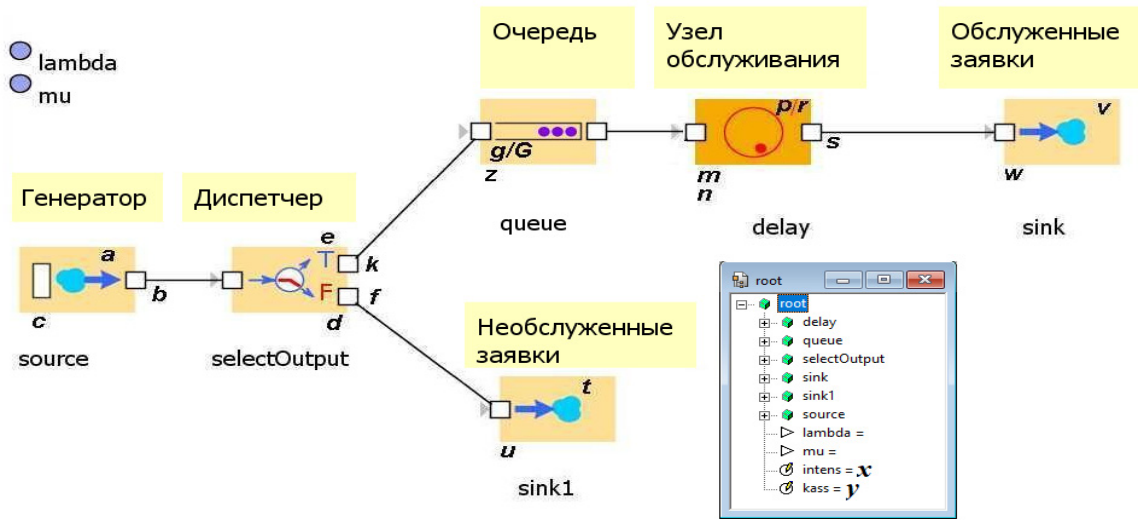


Рис. 1. Система массового обслуживания в среде Anylogic 5

По описанной ситуации можно задать порядка 80 разнообразных вопросов. В простейших вопросах проверяется, понимают ли студенты, какие показатели отражаются на модели. В более сложных вопросах студенты должны вычислить другие показатели СМО, не отраженные в модели.

Как известно, решение задач – это один из основных методов усвоения теории. Зачастую аудиторного учебного времени не хватает, для прорешивания всевозможных вариантов постановки задач. Поэтому использование вычисляемых вопросов позволяет продолжить обучение в режиме самостоятельной работы. По мнению автора, вычисляемые вопросы должны составлять основную часть фонда оценочных средств. Это согласуется с современной концепцией образования, направленной на формирование у студентов бакалавриата прикладных навыков. Поэтому необходимо организовать обучение преподавателей, в первую очередь экономических дисциплин, технологии создания таких вопросов в рамках курсов повышения квалификации. При обучении надо обязательно

касаться и технологической и педагогической составляющих, что могли бы сделать в большей степени преподаватели компьютерных технологий, а не системные администраторы.

Коснемся далее типологии тестов, которые можно использовать с учебном процессе. Следует заметить, что создание тестов с разными настройками на основе одной и той же базы вопросов позволяет решить различные педагогические задачи в процессе обучения.

Так можно предложить следующие типы тестов:

— тест входного контроля – предполагает проверку остаточных знаний по изученным ранее дисциплинам. Такой тест должен использовать вопросы из изученных ранее дисциплин. В LMS это достигается экспортом/импортом вопросов из одной дисциплины в другую.

— тест для самостоятельного тестирования по теме (для самоподготовки, для самопроверки) – включает вопросы одной из тем курса, предназначен для подготовки к контрольному тестированию.

— контрольный тест по теме – обеспечивает контроль усвоения знаний по одной из тем курса.

— рубежный тест – содержит вопросы по нескольким последовательным темам и проводится 1-2 раза в семестр в зависимости от объема изучаемой дисциплины.

— пробный тест итогового контроля – включает вопросы по всем темам и предназначен для подготовки к итоговому тестированию по дисциплине.

— итоговый тест по дисциплине – для итоговой проверки знаний.

Использование этих видов тестов не вызывает сомнения. Дополним этот перечень рядом других типов, которые также можно использовать в учебном процессе.

Как промежуточный этап в процессе усвоения теоретических знаний по отдельной теме можно использовать тест, названный автором «Работа с учебником». В этот тест вопросы включаются в логической последовательности предъявления учебного материала. При этом порядок вопросов не меняется. Для прохождения этого теста достаточно 1-й попытки (не более 3-х), и студенту рекомендуется проходить этот тест вместе с чтением конспекта. Такая форма учебной работы обеспечивает и последовательное прочтение учебного материала, а не хаотичный поиск по учебнику ответа на тестовый вопрос, если вопросы включены в тест случайным образом, и первичное ознакомление с базой вопросов. При выстраивании траектории обучения надо обеспечить переход к тестам для самостоятельного тестирования только после прохождения теста «Работа с учебником».

Другой тип тестов можно назвать «Учебный тест». Он некоторым образом моделирует процесс проведения практического занятия, на котором преподаватель со студентами рассматривает примеры решения задач по теме. Как правило, на занятии преподаватель предлагает методически подобранную систему задач, ориентированных на применение определенного вычислительного аппарата и на получение представления о типологии задач по данной теме. Преподаватель руководит процессом решения задач, показывает примеры решения и пр. Отталкиваясь от этой технологии можно сформулировать основные принципы построения учебного теста.

1. Тест должен содержать вопросы в основном вычисляемого типа.
2. Вопросы в тесте располагаются в строго логическом неизменяемом порядке.
3. Тест содержит вопросы-примеры и вопросы-задачи. В вопросах-примерах дается формулировка задачи, приводится пример решения аналогичной задачи с другими исходными данными. Студенту предлагается применить методику к новому набору исходных данных. Вопросы-задачи следуют стразу за вопросами примерами, имеют аналогичную или близкую формулировку, но пример решения уже не приводится. Во время тестирования студент при необходимости всегда может вернуться к вопросу-примеру.

Учебные тесты особенно важны при использовании на заочном обучении, где аудиторных часов очень мало, а центр тяжести в обучении переносится на самостоятельную работу.

Очень важную роль при организации тестирования играет правильная настройка параметров теста. Необходимо добиться такой ситуации, при которой студент должен подходить к тестированию подготовленным. Тест ни в коем случае не должен заменить собой чтение учебного материала. Анализ многих тестов, представленных в ЭОС, показывает, что часто преподаватели используют настройки, заданные по умолчанию при создании теста, видимо предполагая, что они самые оптимальные [2]. Хотя, во-первых, это не так, и, во-вторых, настройки должны быть разными для разных типов тестов и разных форм обучения. Вот некоторые негативные последствия определенных настроек теста.

При определенных параметрах теста студент сразу же после первой попытки может увидеть, как правильно отвечать на вопросы, и чтение учебников становится не нужным. При использовании адаптивного режима, студент может за одну попытку многократно вводить ответ и таким образом подбирать правильный, что, в общем, методически неверно. При использовании неограниченного количества попыток прохождения теста студент вместо чтения конспекта может «натаскивать себя» путем многократного прохождения теста и подбора правильных ответов таким образом. Надо заметить, что студенты никогда не скажут, что тесты настроены неправильно, потому что они думают, что так и надо. Но какое мнение сложится у студента о преподавателе, если тест настроен так, чтобы все могли на него ответить. Значит, идет борьба не за качество обучения, а за процент положительных оценок. А это, согласитесь, разные цели.

При настройке теста задаются следующие параметры (рис. 2 и 3):

1. дата и время начала и окончания теста;
2. ограничение времени ответа на вопросы;
3. количество попыток;
4. метод оценивания;
5. порядок расположения вопросов в тесте;
6. отображение вопросов на экране во время тестирования;
7. случайный (или нет) порядок ответов в вопросах с выбором ответа;
8. обучающий режим (да/нет);
9. начислять штрафы (да/нет);
10. настройки просмотра результатов теста студентом;
11. пароль для доступа к тесту.

Другие настройки пока рассматривать не будем.

Каждый вид настройки в тесте должен быть обоснован.

Опыт использования тестов позволяет сформулировать следующие рекомендации.

Указание времени начала и окончания теста (1) оправдано в очень ограниченных ситуациях:

— на очном обучении, если курс используется для 1-й группы;

— для контрольных тестов – дата и время окончания теста указывается непосредственно перед прохождением теста; при этом начало можно не указывать.

Если тестом пользуются студенты нескольких групп, и особенно студенты всех форм заочного обучения, разные преподаватели, задавать начало и окончание тестирования не рекомендуется.

Говоря об ограничении времени прохождения теста (2), надо иметь в виду, что все виды промежуточного внутрикурсового тестирования так или иначе нацелены на итоговый тест, который всегда имеет ограничение по времени. Поэтому и все промежуточные тесты должны иметь ограничение по времени. Но эта общая рекомендация имеет свои разновидности. Так для студентов очного и заочного обучения длительность ограничения должны быть разной. Тест «Работа с учебником» должен иметь длительность, достаточную и для спокойного прочтения учебника и для поиска ответа на вопросы. В этом случае возможно не стоит устанавливать ограничение по времени. Здесь также можно использовать адаптивный режим с возможностью нескольких попыток ответа на вопрос во время прохождения теста. Учебные тесты, моделирующие практическое занятие по решению задач, могут иметь ограничение равное длине реального практического занятия. В этих тестах можно и не задавать ограничение. В целом ограничение теста по времени организует студента, заставляет его подготовиться определенным образом к тесту, а также и анализировать свою подготовку и по временному фактору.

Количество попыток (3) надо ограничивать, что заставит студента «дорожить» попытками и не разбрасываться ими понапрасну. Очень интересна методика использования метода оценивания (4) «Средняя оценка» в сочетании с ограничением количества попыток. Студенту предлагается при самостоятельном тестировании обязательно пройти, например, 5 попыток, и при этом система будет выставлять среднюю оценку. Итоговая оценка, выставленная системой, нормируется на количество попыток, т.е. если студент прошел вместо 5-ти попыток только 3, то окончательная оценка за тест будет составлять 3/5 от итоговой. Такой подход «заставляет» студента использовать все попытки, что в свою очередь позволяет познакомиться с большим количеством вопросов из базы, а значит, качество обучения будет выше. Правда использование этой методики пока приходится проводить в полуавтоматическом режиме, т.к. система пока не позволяет сформировать отчет о количестве пройденных попыток студентами в группе, хотя настройку такого отчета можно было бы сделать системным администраторам.

Порядок вопросов в тесте (5) «как показано на экране редактирования» отображает тестовые вопросы в той последовательности, как их внес преподаватель в тест. Надо иметь в виду, что в этом случае в тест все вопросы включаются только при создании теста и далее он имеет статичную структуру, т.е. количество вопросов и порядок их следования не меняется при многократном прохождении теста. При дальнейшем расширении базы вопросов в тест с такими настройками невозможно будет добавить новые вопросы. Придется только создавать тест заново. Это недостатки такой настройки. Тем не менее, такую настройку рекомендуется использовать в тестах типа «Работа с учебником» и «Учебный тест», рассмотренных выше. Для других типов тестов порядок должен быть задан случайным. При случайной выборке вопросов из базы каждая новая попытка теста будет отличаться от предыдущей, что делает тест динамичным. При добавлении вопросов в базу они также будут включаться случайным образом в тест.

Рекомендуется также устанавливать отображение на экране вопросов (6) «по одному вопросу на каждой странице теста». Это позволяет студенту сосредоточиться на одном вопросе. Эта установка также важна при проведении итогового тестирования. Коснемся методики проведения итогового тестирования. Первая проблема заключается в том, какие вопросы и сколько включать в тест итогового контроля. Если база тестовых вопросов мала, то возможно надо включить все вопросы. А если база вопрос достаточно большая, то тест должен обеспечить проверку знаний по всем темам, вопросы для разных студентов должны быть одинакового уровня сложности, и тест должен иметь ограниченную

длительность порядка 30-45 минут. Оптимальным здесь видится тест с одинаковыми вопросами для всех студентов. Так проводят тесты ЕГЭ и другие тесты централизованного массового тестирования. Тесты с одинаковыми вопросами повышают объективность оценки и позволяют преподавателю анализировать уровень сложности теста. Отображение на экране только одного вопроса и случайный порядок их отображения в тесте не позволяет студенту сравнивать свои вопросы с теми, которые попались другому студенту. В таком тесте для обеспечения индивидуальной работы каждого тестируемого также можно установить настройку «последовательное прохождение теста», которая не позволит вернуться к предыдущим вопросам и изменить ответ.

О негативных сторонах обучающего режима (8) было сказано выше.

В режиме просмотра результатов теста ответы (10) во всех видах теста рекомендуется установить настройку отображения ответов студента («Свои ответы»), и не отображать правильные ответы теста («Ответы»), чтобы студент сам анализировал свои ошибки, а не получал ответы в готовом виде. При контрольном тестировании следует снять, в том числе, и флажок «Свои ответы», оставить только «Отзыв» и «Баллы».

Если вы проводите контрольное тестирование в присутствии преподавателя, то рекомендуется установить пароль доступа к тесту (11). Пароль вводит преподаватель перед началом тестирования. Если в компьютерном классе установлена программа подключения к столам студентов, например, NetOpSchool, то это можно сделать прямо с рабочего места преподавателя. Ввод пароля гарантирует, что тестирование проходит именно тот студент, который сейчас сидит в классе, а не кто-то удаленный за студента. При других вариантах доступа к тесту это в принципе возможно.

В заключении хочется дать общую рекомендацию администрации вузов. Использованием LMS-систем в учебном процессе и, в частности, применением тестирования, следует управлять, не пуская этот процесс на самотек, потому что от того как построен процесс тестирования во многом зависит и успешность обучения, и мнение студентов о конкретном преподавателе и о вузе вообще [3]. Рассмотренные в статье вопросы могут показаться очевидными опытному пользователю, владеющему компьютерными технологиями и хорошо знакомому с LMS Moodle. Однако в целях дальнейшего повышения качества использования системы в учебном процессе необходимо обучать преподавателей некомпьютерных дисциплин педагогически и технологически правильному использованию возможностей тестирования с помощью курсов повышения квалификации, что в настоящий момент еще далеко от совершенства.

СПИСОК ЛИТЕРАТУРЫ

1. Титова Ю.Ф. Задачи и проблемы организации электронного обучения и применения дистанционных образовательных технологий // Академия профессионального образования. - 2015 - №6
2. Барабаш П.А., Воробьев С.П., Курносов В.И., Советов Б.Я. Инфокоммуникационные технологии в Глобальной информационной инфраструктуре – Санкт-Петербург,: Наука, 2008, 552 с.
3. Титова Ю.Ф. Об особенностях труда педагогических работников при использовании электронного обучения.// IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2017)» / Материалы конференциию - СПОИСУ. – СПб, 2016.

УДК 51.74

МОДЕЛИРОВАНИЕ УЯЗВИМОСТЕЙ В СИСТЕМЕ БЕЗОПАСНОСТИ

Шипилева Алла Владимировна
Волгоградский государственный университет,
Россия, Волгоград, Университетский проспект, д. 100,
email: ashipileva@mail.ru

***Аннотация*:** В статье представлена модель динамики уязвимостей в системе безопасности, используя предельное поведение ветвящегося процесса с непрерывным временем можно показать, как в многоуровневой системе безопасности можно вычислять потенциал атаки.

Ключевые слова: *безопасность; уязвимости; ветвящиеся процессы.*

MODELING OF FLAWS WITHIN A SECURITY SYSTEM

Shipileva Alla
Volgograd State University,
Russia, Volgograd, University prospect, 100,
email: ashipileva@mail.ru

Abstract: The article presents a model of the dynamics of vulnerabilities in the security system, using the limiting behavior of a branching process with continuous time can show how in a multi-level security system it is possible to calculate the attack potential.

Keywords*: security; flaws; branching processes.*

Введение. В настоящее время существует много работ, раскрывающих различные подходы к анализу уязвимостей систем безопасности [1, 2]. В отличие от других программных элементов системы безопасности являются многоуровневыми. Предполагаемый эффект каждого уровня заключается в том, чтобы значительно увеличить объем информации и усилий, необходимых атакующим для преодоления и проникновения в этот барьер. Поэтому все защитные барьеры должны быть преодолены злоумышленниками, чтобы они могли получить неограниченный доступ.

В настоящее время существует ряд моделей, позволяющих с разной степенью детализации описать процесс сетевой атаки. Модели используют разную математическую базу, но большинство из них основаны на конечных автоматах и представляют атаку как последовательность состояний автомата. Модели, которые получили широкое распространение – это деревья и графы атак. Деревья атак предложил использовать в 1999 г. Б. Шнайдер. Они представляют собой концептуальные диаграммы, которые описывают угрозы системе и возможные атаки, направленные на их реализацию. Модель пригодна для описания атак на любые системы информационного или физического характера. Модель предоставляет возможность для введения оценок каждого шага по некоторым критериям: по времени выполнения, числу операций, оценочной стоимости и другим. При этом последовательность шагов может быть оценена на основании критериев для каждого шага. Однако эта модель не может быть использована для моделирования атаки, поскольку не обеспечивает средств динамического моделирования, не учитывает решений с различной вероятностью. Модель графов атак предложил коллектив авторов в работе [6] в 2002 г. Графы атак являются специализированным средством для описания сетевых атак, узлы графа представляют не концептуальные действия, а узлы сети, процессы, программы, конфигурационные файлы, участки кода, переменные и т. д. Моделирование систем с использованием графов атак основано на конечных автоматах. Переходы между узлами осуществляются на основе применения детерминированных правил, при этом могут учитываться текущие значения некоторых параметров системы, переменных. Целью является достижение необходимой вершины. Модель предусматривает анализ условий, необходимых для достижения цели атаки, поэтому ее можно использовать для оценки безопасности программной системы или компьютерной сети. Модель была реализована в инструментальных средствах - Lockheed Martin ANGI. Однако эта модель является средством оценки сложности нарушения безопасности информационной системы, а не моделирования и исследования атак.

В этой статье представлен подход, основанный на предельном поведении ветвящихся процессов с непрерывным временем [5], который обеспечивает построение динамической модели представления атаки на систему безопасности.

Пусть случайные величины ξ0, ξ1, ξ 2, … - число уязвимостей в нулевом, первом, втором, и т.д. уровнях защиты системы соответствует числу вершин (состояний) корневого ориентированного дерева уязвимостей (дерева угроз). На рис.1 представлен пример дерева уязвимостей. Дугам дерева уязвимостей приписаны вероятности pi перехода из состояния i – го уровня защиты в состояние i+1 – го уровня. Длительность пребывания в каждом состоянии нулевого, первого, и т.д. уровнях защиты равна соответственно t0, t1, t2, … и не является случайной величиной.

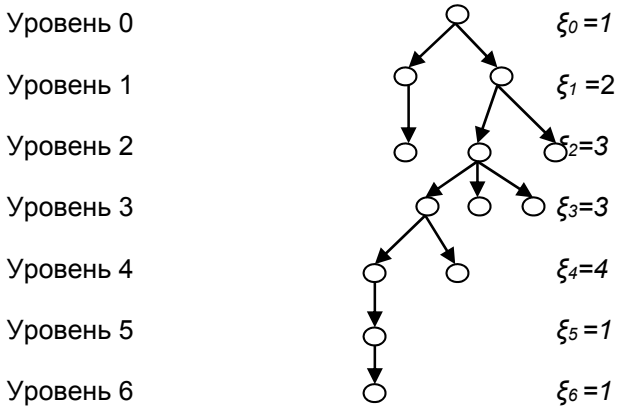


Рис. 1. Пример дерева уязвимостей с 7 уровнями.

При определении вероятности p_i того, что злоумышленник не сможет использовать уязвимости в *i* – узле дерева уязвимости для проведения атак за заданное время, необходимо учитывать тип дерева уязвимостей.

Пусть дерево уязвимостей системы защиты является *m* – арным деревом, тогда злоумышленник в каждом узле выбирает для осуществления атаки уязвимости с вероятностями $p_1=b_1, p_2=b_2, \ldots, p_m=b_m, m\geq 3$ с учетом выполнения следующих неравенств [4]:

$$0 < b_1 < 1$$

$$\frac{1}{2}b_1(1-b_1) < b_2 \leq b_1(1-b_1)$$

$$max\{0,(n+1)\beta_n-\alpha_n\}\le\nu_n\le\beta_n$$
$$\alpha_2=b_1(1-\lambda),\beta_2=b_1(1-\sigma)$$
$$\alpha_n=\alpha_2-\sum_{k=2}^{n-1}k\nu_k,\beta_n=\beta_2-\sum_{k=2}^{n-1}\nu_k,\text{ при } n=3,\dots,m,$$

где значения величин σ и λ вычисляются по формулам:

$$\sigma=\frac{b_1}{(b_1^2+2b_2)}$$
$$\boldsymbol{\lambda=b_1\sigma.}$$

Вероятности bk находятся из рекуррентных равенств:

$$\boldsymbol{\nu_k=(k-\lambda)b_k-(k+1)\sigma b_{k+1}-\frac{1}{b_{k+1}}\sum_{n=2}^{k-1}(k-n+1)\,\nu_n b_{k-n+1}}$$

Автором реализована программа динамического моделирования деревьев уязвимостей многоуровневой системы безопасности в Microsoft Visual Studio.NET на языке C#. На рис 2. представлен пользовательский интерфейс программы. Основные результаты компьютерного моделирования следующие:

– максимальная вероятность достижения злоумышленником цели за заданное время;
– время, затраченное злоумышленником на достижение цели.

Расчет проникновения барьеров в многоуровневой системе безопасности при атаке злоумышленников позволяет определить наиболее уязвимые места и определить перечень необходимых дополнительных мер защиты узлов.

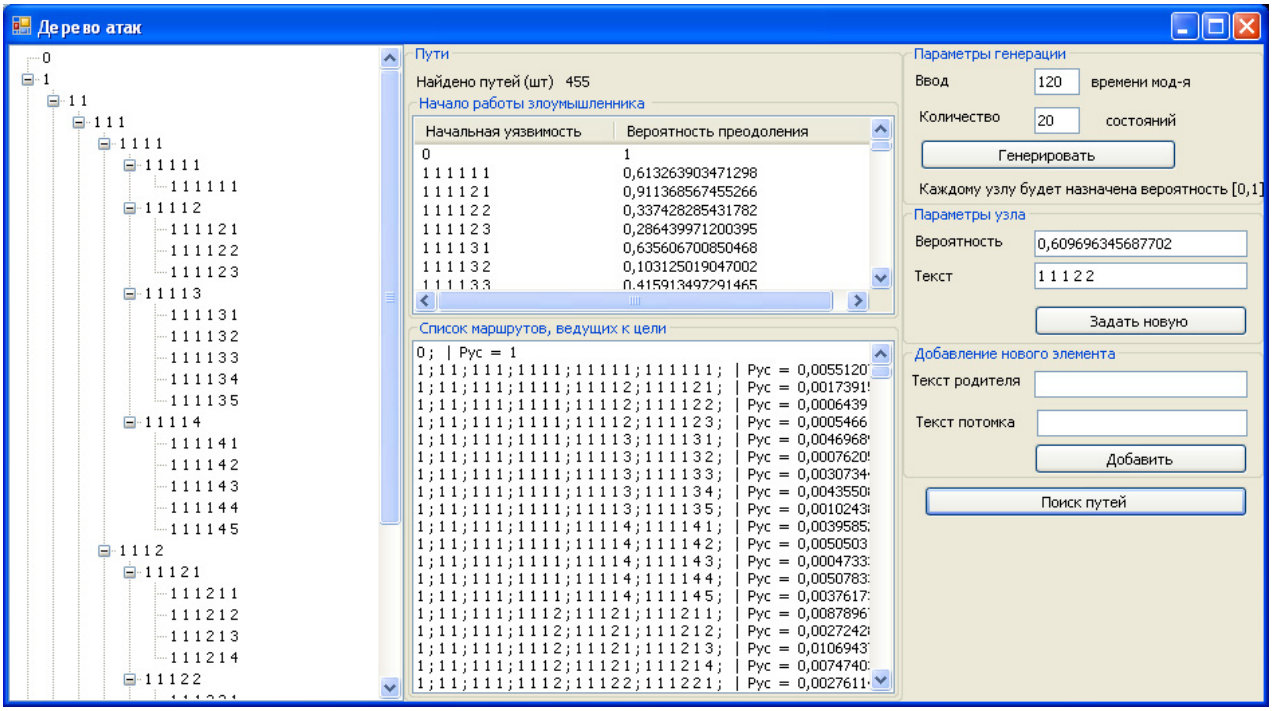


Рис. 2. Пользовательский интерфейс программы.

Заключение. Предложенная динамическая модель атаки на систему безопасности не зависит от топологии сети, а определяется вероятностями преодоления уязвимостей и может быть использована для вычисления потенциала атаки [5].

СПИСОК ЛИТЕРАТУРЫ

1. Абрамов Е. С., Андреев А. В., Мордвин Д. В. Применение графов атак для моделирования вредоносных сетевых воздействий // Известия Южного федерального университета. Технические науки. 2012.Том 26. Вып.1. С.165 -173.
2. Котенко И. В., Степашин М.В., Богданов В.С. Оценка безопасности компьютерных сетей на основе графов атак и качественных метрик защищенности // Труды СПИИРАН.2006. Вып.3. С.30-39.
3. Котенко И. В., Дойникова Е. В., Чечулин А.А. Динамический перерасчет показателей защищенности на примере определения потенциала атаки // Труды СПИИРАН. 2013. Вып.7. С.26-39.
4. Цыбулин А.М., Шипилева А.В. Математическая модель злоумышленника в корпоративной сети // Сборник трудов. Управление большими системами ИПУ им. В.А.Трапезникова РАН.2007. Вып.19. С.127-133.
5. Харрис Т. Теория случайных ветвящихся процессов. — М: Мир, 1966 — 356с.
6. Sheyner O. Automated generation and analysis of attack graphs // Proceedings of the IEEE Symposium on Security and Privacy. - Oakland, CA, USA - 2002. - P.273 – 284.

СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.451

ПРИМЕНЕНИЕ ПСЕВДОВЕРОЯТНОСТНОГО ЗАЩИТНОГО ПРЕОБРАЗОВАНИЯ В ТЕХНОЛОГИИ ТАЙНОГО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

Вайчикаускас Мария Александровна, Татчина Яна Александровна, Синев Валерий Евгеньевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
email: sovizo@mail.ru; mondikovay@gmail.com; vesinev@mail.ru

Аннотация: В статье рассматривается применение протокола псевдовероятностного защитного преобразования для обеспечения защиты технологии тайного электронного голосования от автоматизированной скупки голосов. Предлагаемый протокол основывается на криптосхеме Рабина и по криптограмме неотличим от алгоритма вероятностного шифрования.

Ключевые слова: *криптография; электронное голосование; отрицаемое шифрование; открытое шифрование; вероятностное шифрование.*

THE APPLICATION OF THE PSEUDOPROBABILISTIC PROTECTING DATA CONVERSION IN THE ELECTRONIC ELECTION TECHNOLOGY

Vaichikauskas Maria, Tatchina Yana, Sinev Valery
The St. Petersburg State Electrotechnical University "LETI",
email: sovizo@mail.ru; mondikovay@gmail.com; vesinev@mail.ru

Abstract: The article describes application of the pseudoprobabilistic protecting data conversion protocol to protect electronic voting system against automated bying of the votes. Proposed protocol is based on Rabin cryptosystem and provides the same cyphertext as the probabilistic encryption algorithm.

Keywords*: cryptography; electronic voting; deniable encryption; open key encryption; probabilistic encryption.*

Практическое внедрение систем тайного голосования через Интернет является весьма значимым направлением приложения информационных технологий. Таким образом, важное практическое значение имеет применение алгоритмов псевдовероятностного защитного преобразования, также известного как отрицаемое шифрование, для реализации на их основе механизмов защиты от скупки голосов избирателей в случае использования технологии тайного электронного голосования через Интернет. В реализации таких механизмов бюллетени избирателей подаются в избирком в зашифрованном виде: перед подачей заявленного бюллетеня избиратель должен зашифровать его, используя открытый ключ избиркома. Полученная криптограмма отправляется в избирком. Избирком расшифровывает криптограмму, содержащую серийный номер бюллетеня и решение избирателя. Для зашифрования используется алгоритм отрицаемого шифрования по открытому ключу избиркома, в результате чего направляемая в избирком криптограмма может быть также получена путем выполнения процедуры зашифрования бюллетеня с другим серийным номером в пользу другого решения, т.е. некоторого фиктивного бюллетеня.

При этом вычислительно невозможно доказать, что криптограмма содержит более одного бюллетеня. Таким образом, в случае появления скупщика голосов, который объявляет вознаграждение за выбор определенной кандидатуры, избиратель может получить данное вознаграждение, указав в фиктивном бюллетене запрашиваемое скупщиком решение. При этом бюллетень, получаемый избиркомом из криптограммы избирателя, может содержать голос в пользу другой кандидатуры, выбираемой избирателем произвольно. Доказать наличие другого бюллетеня в криптограмме может только тот, кому известен секретный ключ избиркома, связанный с его открытым ключом. Поскольку по открытому ключу вычислительно невозможно вычислить секретный ключ, то скупщик голосов не имеет никакой возможности узнать, что его обманывают.

Такая возможность обмана скупщика избирателем делает скупку голосов нерациональной, что обеспечивает защиту технологии тайного электронного голосования от скупки голосов избирателей.

Для применения алгоритма ОШ, предложенного в [1], в системах тайного электронного голосования необходимо снять ограничения на размер шифруемых сообщений, а именно обеспечить возможность стойкого шифрования коротких сообщений. Для обеспечения возможности

зашифрования коротких сообщений целесообразно применить предварительное преобразование бюллетеня *T* (преобразование значения *T* в значение *R*) по формуле:

$$R = (n - T)2 \bmod n.$$

Также для реализации такой возможности по отношению к фиктивному бюллетеню M второй предполагаемый корень соотношения:

$$x^2 - Ax + B \equiv 0 \bmod n,$$

целесообразно задать в виде:

$$Z = (R - M) \bmod n.$$

В результате такого усовершенствования получается следующий протокол отрицаемого шифрования по открытому ключу получателя сообщений *T* и *M* (избиркома) *n*:

1. Избиратель вычисляет псевдослучайное значение

$$R = (n - T)^2 \bmod n.$$

2. Далее он формирует фиктивный бюллетень M.

3. Вычисляет значение коэффициента

$$A = (2R - M) \bmod n.$$

4. Вычисляет значение коэффициента

$$B = R(R - M) \bmod n.$$

5. Затем он выполняет процедуру слепого подписывания избиркомом криптограммы C = (A, B).

6. Получив слепую подпись к C, избиратель вычисляет истинную цифровую подпись избиркома к своей криптограмме и направляет ее вместе с подписью в избирком.

7. Избирком проверяет подлинность подписи к криптограмме и, используя свой секретный ключ, расшифровывает ее, получая два бюллетеня, из которых учитывает в подсчете голосов бюллетень T, имеющий больший серийный номер, но публикует в результатах голосования оба бюллетеня.

Для расшифрования выполняются следующие шаги:

1. Избирком, используя пару простых чисел (p, q), вычисляет четыре корня X1, X2, X3, и X4 сравнения

$$x2 - Ax + B = 0 \bmod n.$$

2. Затем он вычисляет значения M1, M2, M3, и M4, используя формулу $Mi = (2Xi - A) \bmod n$ где (i = 1, 2, 3, 4).

3. Отбрасывает три случайных значения из набора {M1, M2, M3, M4} и выбирает одно осмысленное сообщение в качестве бюллетеня M.

4. Затем избирком вычисляет значение

$$R = (M + A)/2 \bmod n,$$

и, используя секретный ключ (p, q), находит четыре квадратных корня S1, S2, S3 и S4 из числа R по модулю n.

5. Далее избирком вычисляет значения

$$Ti = (n - Si) \bmod n, \text{ (где } i = 1, 2, 3, 4).$$

Если все эти значения случайные, то он учитывает бюллетень M, как истинный бюллетень избирателя. Если одно из значений Ti (обозначим его как T) представляет собой еще один бюллетень, то он сравнивает серийные номера бюллетеней T и M и если серийный номер первого больше серийного номера второго бюллетеня, то он учитывает бюллетень T в подсчете голосов.

Распознать то, что в приведенном алгоритме псевдослучайное значение R на самом деле не является случайным, является вычислительно трудной задачей без знания секретного ключа, связанного с открытым ключом избиркома. Поэтому избиратель может уверенно утверждать, что он использовал для шифрования фиктивного бюллетеня M вероятностный алгоритм открытого шифрования, рекомендованный в рамках системы тайного электронного голосования, который описывается следующими шагами:

1. Сгенерировать случайное значение $R' < n$.

2. Вычислить значение $A = (2R - M) \bmod n$.

3. Вычислить значение $B = R(R - M) \bmod n$.

Этот алгоритм вероятностного шифрования вырабатывает ту же криптограмму C = (A, B), что и алгоритм ОШ, если R′ = R. Поскольку значение R в протоколе ОШ вычисляется как квадрат числа n – T по модулю n, то оно неотличимо от случайного значения без использования делителей модуля n, которые являются секретными и известны только избиркому. Поэтому избиратель может декларировать скупщику голосов, что в криптограмме C = (A, B) содержится только один бюллетень M и ему причитается объявленное вознаграждение за свой голос. Скупщик не может распознать случаи обмана, поэтому плата за голоса становится для него нерациональной.

СПИСОК ЛИТЕРАТУРЫ

1. Молдовян Н.А., Вайчикаускас М.А. Расширение криптосхемы Рабина: алгоритм отрицаемого шифрования по открытому ключу // Вопросы защиты информации. 2014. № 2. С. 12-16.
2. Moldovyan N.A. Blind Collective Signature Protocol // Computer Science Journal of Moldova. 2011. Vol. 1. P. 80-91
3. Rabin M.O. Digitalized signatures and public key functions as intractable as factorization. – Technical report MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979.

УДК 004.5

КОНТРОЛЬ ФУНКЦИОНАЛЬНОГО СОСТОЯНИЯ ЧЕЛОВЕКА-ОПЕРАТОРА И ЕГО КОРРЕКЦИЯ КАК МЕТОД ПОВЫШЕНИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ НА РАБОЧЕМ МЕСТЕ

Колмаков Сергей Александрович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
emails: s.kolmakov1992@gmail.com

***Аннотация*:** В данной статье рассматривается проблема контроля и управления функциональным состоянием человека на основе его типологических особенностей. Рассматриваются методики контроля функционального состояния с учетом физиологических характеристик человека, его психологии и показателей эффективности труда. На основе рассмотренных в статье материалов предложена модель управления функциональным состоянием человека, на основе его типологических особенностей.

***Ключевые слова**: функциональное состояние; психологическая безопасность; работоспособность; типологические особенности.*

MONITORING OF THE FUNCTIONAL STATE OF THE HUMAN OPERATOR AND ITS CORRECTION AS A METHOD OF INCREASING THE INFORMATION-PSYCHOLOGICAL SAFETY IN THE WORKPLACE

Kolmakov Sergey
The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
emails: s.kolmakov1992@gmail.com

Abstract: This paper considers information about problems of monitoring and control of the functional state of a human-operator based on typological features. Paper discus methods control of functional state, taking into account the physiological characteristics of man, his psychological features and indicators of the labor efficiency. At the end of the paper, a model to control the functional state of the person, on the basis of its typological features is proposed.

***Keywords:** functional state;psychological safety; working capacity; typological features*.

Введение. Психологическая безопасность – одно из ключевых и наиболее важных направлений в исследованиях трудовых психологов, инженерных психологов и эргономистов по всему миру. Это связанно с многократно возросшей информатизацией не только труда, но и всей деятельности человека в целом. Помимо этого так же растет и сама цена ошибки оператора в трудовом процессе, низкий уровень информационно-психологической безопасности может повлечь за собой повышение числа ошибок по вине человеческого фактора.

Если понимать информационно-психологическую безопасность человека как состояние защищенности личности, обеспечивающее ее целостность как активного социального субъекта и возможности развития в условиях информационного взаимодействия с окружающей средой [1]. То мы можем утверждать, что информационно-психологическая безопасность человека тесно связана с его функциональным состоянием.

В современном научном сообществе понятие функционального состояния (ФС) рассматривают с различных сторон:

– С точки зрения психофизиологии функциональное состояние рассматривают как фоновую активность нервной системы человека.

– С точки зрения эргономики и инженерной психологии функциональное состояние рассматривают в рамках деятельностного подхода, т.е. оценки эффективности труда в конкретной деятельности человека.

В первом случае необходимо понимать функциональное состояние как некий набор физиологических и психофизиологических характеристик человека, например: частоту сердечных сокращений (ЧСС); топографическую активность головного мозга, ЭЭГ, ЭКГ, КГР, РД, ФПГ и т.д.

При этом в последнем случае, важно понимать, что нельзя рассматривать определенные показатели эффективности труда одной деятельности наряду с показателями эффективности труда иной работы. Другими словами, у каждой из работ будет разный коэффициент надежности и ошибок. [2].

Ввиду отсутствия единого подхода к пониманию ФС, следует рассматривать его как набор характеристик разных направлений, включающих в себе сразу несколько основ: физиологическую, деятельностную и психологическое само восприятие субъекта. Соответственно ФС человека можно представить следующим кортежем:

$$\mathrm{X} =< A, B, C >=< a_1 \dots a_n >< b_1 \dots b_n >< c_1 \dots c_n > \quad (1)$$

Где X – интегральная оценка функционального состояния человека-оператора, A–интегральная оценка физиологических характеристик ФС, B – интегральная оценка деятельностных характеристик ФС, C – интегральная характеристика психологического самоощущения ФС человека; a – конкретная физиологическая численная характеристика, отражающая ФС, b–конкретная численная характеристика, отражающая показатель эффективности труда или надежности, c – конкретный численный показатель, отражающий само восприятие своего функционального состояния (выражается в виде бальной оценки на основе методики оценки функционального состояния).

При этом следует учитывать, что интегральные оценки функциональных состояний не должны выходить за рамки установленных норм для конкретной деятельности, т.е. реализовывать методы адаптивного анализа отклонения показателей от нормы [3].

Обобщая все отмеченное выше, получаем, что оценка ФС должна вестись не только используя лишь один вид параметров, но комплексно использовать параметры различных видов: физиологические (ЧСС, ЭКГ); показатели эффективности деятельности (количество ошибок в период времени); психологические (оценка самоощущения человека на основе опросников, отображающих уровень утомления).

Однако при возможности оценки ФС человека не менее важным для информационно-психологической безопасности индивида стоит вопрос о возможности управления этим состоянием, т.е. о возможности коррекции данного состояния.

Если обратиться к диаграмме работоспособности человека-оператора (Ч-О), изображенной на рисунке 1, то можно увидеть, что работоспособность оператора имеет несколько ярко выраженных периодов. Первый из них этап врабатываемости, который характеризуется мобилизацией внутренних ресурсов организма, второй период – оптимальная работоспособность, характеризуется минимальным количеством ошибок, третий период – фаза утомления, характеризующаяся ростом ошибок.

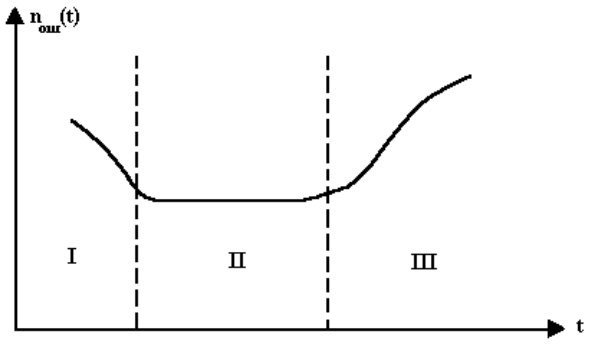


Рис. 1. Динамика работоспособности человека-оператора

Опираясь на сказанное выше, с точки зрения оптимизации функционального состояния мы имеем три вида решаемых задач:

1. Задача мобилизации, которая решается повышением активности нервной системы, увеличением концентрации человека.

2. Задача поддержания всех параметров, характеризующих функциональное состояние в оптимальных значениях.

3. Задача обеспечения условий для максимально быстрого восстановления ресурсов организма.

Каждая из приведенных задач имеет свой ряд особенностей, и решение коррекции функционального состояния человека-оператора будет отличаться на каждой из фаз. Однако каждая из фаз будет связана с необходимостью активации или же торможения определенных процессов внутри организма или же нервной системы в целом [4].

С точки зрения воздействий и контроля функционального состояния современные исследователи выделяют множество способов:

– методы профессионального отбора;
– оптимизация и совершенствование условий труда;
– приемы прямого воздействия на человека.

Последняя группа методов является непосредственным влиянием на человека-оператора психогенными, фармакологическими или же иными способами, к примеру, сигналами различной модальности (звуками, визуальными образами, запахами и т.д.) для повышения его работоспособности. В целом можно выделить следующие способы воздействия:

1) Ароматерапия.
2) Музыкотерапия.
3) Электростимуляция тканей.
4) Цветотерапия.
5) Мультимедийные воздействия.

6) Вибростимуляция.

Стоит отметить, что каждый из видов приведенных воздействий человек воспринимает всецело индивидуально. К примеру, воспринимая красный цвет, каждый человек испытывает функциональное возбуждение нервной системы, однако степень этого возбуждения варьируется от временного повышения работоспособности, до ее снижения из-за высокого перевозбуждения нервной системы [5].

Соответственно, каждый из методов работает с разной эффективностью. Ответ на вопрос «почему?» стоит искать в области дифференциации психологического и психофизиологического строения человека. Соответственно, при нормализации функционального состояния человека-оператора необходимо учитывать индивидуальные особенности строения его нервной системы. Однако данный вопрос почти не освещен современной наукой.

Если рассматривать типологические особенности индивида, влияющие на восприятие сигналов различной модальности, а так же на фоновые показатели его функциональной активности, то можно выделить довольно большой список подобных характеристик. Однако здесь следует выделить именно первичные факторы, т.е. врожденные характеристики.

Одной из таковых является психофизиологический тип человека, который представляет собой динамичную, относительно устойчивую целостную систему стандартных интеллектуальных, социально-культурных, морально-волевых ценностей, потребностей и поведенческих норм, присущих индивиду, а так же тип нервной системы. Одной из наиболее популярных типологий психологического типа является типология Майерс-Бриггс, основанная на работах Карала-Гюстава Юнга [6].

Таблица 1

Психологические типы по типологии Майерс-Бриггс

		Сенсорные		Интуитивные			
		Мысли	Чувства	Чувства	Мысли		
Интроверсия	Решение	ISTJ	ISFJ	INFJ	INTJ	Решение	Интроверты
	Восприятие	ISTP	ISFP	INFP	INTP	Восприятие	
Экстраверсия	Восприятие	ESTP	ESFP	ENFP	ENTP	Восприятие	Экстраверты
	Решение	ESTJ	ESFJ	ENFJ	ENTJ	Решение	

Так же одним из влияющих факторов при выборе способа коррекции функционального состояния человека является функциональная асимметрия, которая наряду с рядом вышеперечисленных факторов определяет процесс адаптации к изменениям окружающей среды, склонность к заболеваниям, соотношение объективных и субъективных показателей здоровья, организации эффективной трудовой и учебной деятельности. Исследования взаимосвязи межполушарной специализации с эмоциональными состояниями показали, что оба полушария вносят свой вклад в эмоциональные переживания [7].

Третьей врожденной характеристикой человека является его соматотип или же конституциональный тип человека, на данный момент имеется ряд исследований подтверждающих взаимосвязь соматотипа с коррекцией функционального состояния [8]. При этом все вышеуказанные характеристики коррелируют с типом строения нервной системы человека [9]. Соответственно состояние нервной системы так же связано с интегральным ФС.

Таким образом, мы можем выдвинуть следующую гипотезу, что все сигналы, воздействующие на Ч-О, можно разделить на две категории – активизирующие и релаксирующие. Активизирующие сигналы можно пометить знаком «+», они отвечают за мобилизацию резервов организма, а так же повышают количественные показатели характеристик отображающих ФС. Релаксирующие сигналы можно пометить знаком «-», они отвечают за снижение активности и количественное уменьшение показателей отображающих ФС. Соответственно, мы можем представить само оптимальное ФС человека как некий коридор из допустимых значений входящих в кортеж (1). При выходе из коридора допустимых значений необходимо применять методы коррекции.

Так же, как было сказано выше, типологические особенности человека-оператора важны при определении и выборе программы воздействия на индивида, однако данный момент современной наукой мало изучен. Отсутствуют единые алгоритмы для составления программ воздействия, а так же мало изучено влияние типологических характеристик человека-оператора и различных параметров сигналов отличных модальностей на функциональное состояние человека-оператора. Однако, воздействие на человека можно было бы представить в виде двух иерархических структур, приведенных на рисунке 2 и 3 соответственно.

В приведенных моделях: $F_1…F_n$, $G_1…G_n$, $M_1…M_n$,$Z_1…Z_n$–характеристики сигналов различной модальности. $L_1…L_n$ – типологические особенности человека-оператора. Коэффициенты вида f_n, g_n, m_n, z_n– весовые коэффициенты, отображающие зависимость характеристики того или иного сигнала на количественные значения характеристик ФС. Коэффициенты вида lf_{11} – весовые коэффициенты, отображающие зависимость той или иной типологической особенности человека-оператора, на ту или

иную характеристику сигнала. Соответственно исходя из приведенной выше модели описать воздействие на человека-оператора можно при помощи нескольких кортежей, содержащих как характеристические данные по сигналам, так и весовые коэффициенты зависимостей.

Однако, данная модель имеет ряд сложностей, которые еще предстоит решить. Одной из основных сложностей является отсутствие в достаточном количестве проведенных исследований, а соответственно, необходимость разработать методологию исследования искомых зависимостей. Так же из задач, которые будет необходимо решить – подбор характеристик сигналов, которые могли бы выражаться в количественном эквиваленте, а не в качественном [10].

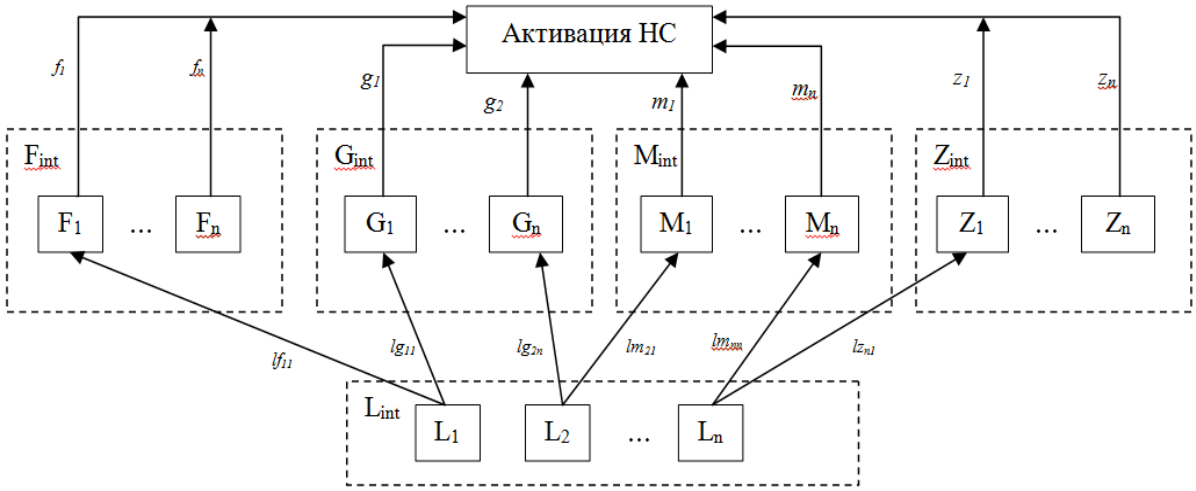


Рис. 2. Модель активации функционального состояния Ч-О

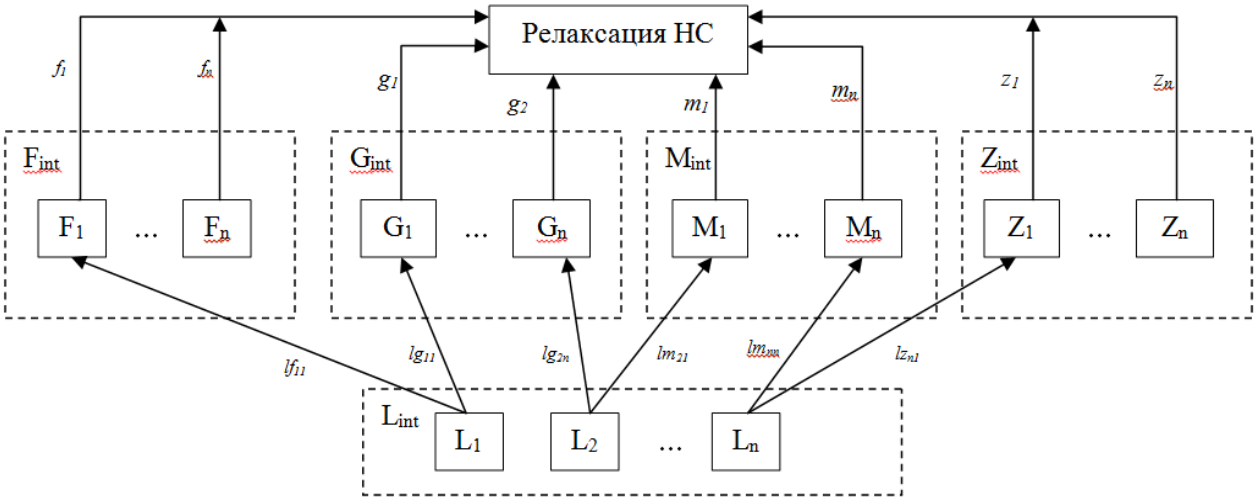


Рис. 3. Модель релаксации функционального состояния Ч-О

Заключение. Несмотря на то, что в области коррекции функционального состояния человека методами прямого воздействия имеется множество вопросов, на которые до сих пор не найдены ответы, данное направление является крайне перспективным. Оно открывает огромные возможности для создания методов повышения работоспособности человека, разработок методологии для снятия психологических нагрузок, стрессов и депрессий, что в конечном итоге будет способствовать повышению информационно-психологической безопасности личности. В данной работе приведены иерархические модели коррекции функционального состояния человека-оператора, а так же отмечены имеющиеся проблемы в реализации данных моделей, которые и являются следующими этапами для изучения проблемной области.

СПИСОК ЛИТЕРАТУРЫ

1. Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты – М.: Изд-во РАГС, 1998 - 125 с.
2. Леонова А.Б., Психодиагностика функциональных состояний человека, изд. МГУ, 1984г.
3. Ушаков И.Б., Богомолов А.В. Паттерны функциональных состояний оператора – М.: Наука, 2010. – 390 с.
4. Данилова Н.Н., Крылова А.Л. Физиология высшей нервной деятельности. М.:изд. Моск. ун-та, 1989, 231 с.
5. Колмаков С.А. Методы коррекции функционального состояния человека-оператора и его типологические особенности// Человеческий фактор в сложных технических системах и средах, труды Второй Международной научно-практической

конференции. 2016, Издательство: Межрегиональная эргономическая ассоциация, С. – 325 – 331.
6. Богомаз С.А. Психологические типы К.Г.Юнга, психофизиологические типы и интертипные отношения. – Т.: Издательский дом ТГУ, 2000, 712 с.
7. Антропова Л .К. Функциональная асимметрия мозга и индивидуальные психофизиологические особенности человека// Медицина и образование в Сибири. – 2011. – №3. – С. 81 – 93.
8. Шутова С.В. Влияние обонятельного сенсорного притока на время и точность сенсомотрных реакций у юношей разных конституциональных типов // Вестник ТГУ – 2001. – Вып. 1 – С. 69 – 71.
9. Психологические основы профессиональной деятельности: хрестоматия / Сост. В.А. Бодров. – М.: ПЕР СЭ; Логос, 2007, 511 с.
10. Леонова А.Б. Психологические технологии управления состоянием человека – М.: Изд-во Моск. ун-та, 2007. – 380 с.

УДК 004.5

БЕЗОПАСНОСТЬ И ЮЗАБИЛИТИ СОВРЕМЕННЫХ ПОЛЬЗОВАТЕЛЬСКИХ ИНТЕРФЕЙСОВ

Леонов Антон Викторович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
emails: anton.leonov18@gmail.com

Аннотация: Обеспечение безопасности сложных технических систем - важная проблема современного общества. С развитием Интернета все большее и большее количество конфиденциальной информации, персональных данных, которое необходимо защищать, используется в технических системах. Более того, необходимо обеспечивать безопасность самой системы от риска принятия неправильных решений конечным пользователем. Взаимодействие с системой происходит при помощи пользовательского интерфейса, тем самым возникает необходимость нахождения компромисса между требованиями безопасности и удобством работы с системой. В данной работе приведен обзор существующей литературы, целью которой является нахождение баланса между безопасностью и юзабилити пользовательских интерфейсов.

Ключевые слова*: пользовательские интерфейсы; безопасность; юзабилити.*

SECURITY AND USABILITY OF MODERN USER INTERFACES

Leonov Anton
The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
emails: anton.leonov18@gmail.com

Abstract: Providing the security of complex technical systems is an important problem for modern society. With the progress of the Internet, more and more confidential information, personal data that must be protected, is used in technical systems. Moreover, it is necessary to ensure the security of the system itself from the risk of making the wrong decisions by the end-user. Interaction with the system takes place through the user interface, thus there is a need to find a compromise between the security requirements and the convenience of working with the system. In this paper the existing literature review is done, which dedicates to find a balance between security and usability of user interfaces.

Keywords: *user interfaces; security; usability****.***

Введение. В данной работе делается попытка оценить применение методов обеспечения безопасности в пользовательских интерфейсах (ПИ) технических систем (например, файерволы, протоколы безопасности, механизмы аутентификации). В контексте обеспечения безопасности рассматривается удобство использования системами с точки зрения достижения конкретных целей пользователя (выполнения им определенных задач) [1]. С другой стороны, удобство использования интерфейса – это одно из требований к его безопасности, поскольку данный компонент является основной платформой для взаимодействия с системой [2]. Одними из главных проблем проектирования ПИ являются нахождение баланса между юзабилити и безопасностью, критериями, используемыми для оценки удобства использования системы, связью между критериями безопасности и критериями удобства использования [3].

Был проведен тематический литературный обзор. В литературе, посвященной безопасности и пользовательским интерфейсам, существует два способа взглянуть на проблему нахождения баланса между юзабилити и безопасностью ПИ. Во-первых, с точки зрения безопасности (такие методы как использование паролей, пин-кодов и т.д.).Во-вторых, с точки зрения юзабилити, которая описывается как «эффективность и удовлетворенность, с которой указанные пользователи могут достичь определенных целей в заданной среде» [1].

В 1994 году Норманном [3] были сформулированы основные принципы юзабилити. Если пользователь испытывает какой-либо дискомфорт при использовании интерфейса, то встает вопрос об удобстве использования этой системы. Термин «юзабилити» может быть описан как «способ разработки и проверки систем с использованием экспериментальных методов для достижения эффективности и удовлетворенности конкретных пользователей, которые выполняют определенную

задачу в определенной среде [4]. Цель юзабилити состоит в том, чтобы установить компромиссы между удовлетворением пользователя и его эффективностью.

Проектирование системы безопасности не ограничивается просто созданием безопасного программного обеспечения. Это предполагает правильную интеграцию действий и политик безопасности в процесс разработки программного обеспечения. Подходы, основанные на оценке только юзабилити ПИ, не вполне подходят для оценки систем, которые сосредоточены на безопасности [3]. Как отметил Михайлов и др. [5], во многих исследованиях отсутствует анализ реакции и поведения пользователей на нарушения в системе безопасности (например, вредоносные события или сообщения о мошенничестве). Рассмотрение таких вариантов использования поможет лучше разработать безопасный интерфейс. Согласно Меллеру и др. [1], причина, по которой пользователи не могут эффективно использовать защищенные системы, заключается в том, что такие системы не учитывают принципы юзабилити в своем дизайне. Если система безопасности не учитывает принципы юзабилити, то вред может быть нанесен не только пользователю системы, но самой системе в целом. В качестве примера можно привести графические формы для ввода пароля (рис. 1) и требования, которые система безопасности предъявляет к паролям. Система безопасности, например, требует ввода старого пароля, который ни разу не использовался для системы, а также повтора нового пароля, тем самым возникает конфликт между памятью человека и требованиями безопасности.

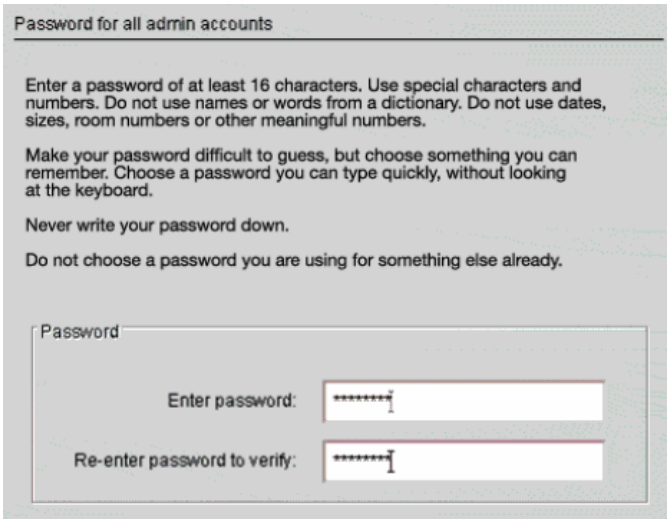


Рис. 1. Пример формы ввода пароля с требованиями системы к нему

Аналогичная ситуация возникает с всплывающими диалоговыми окнами (рис. 2), которые прерывают нормальный процесс взаимодействия с системой из-за политик безопасности. Слишком частое появление таких окон раздражает пользователя, и он стремится их отключить или избежать в дальнейшем.

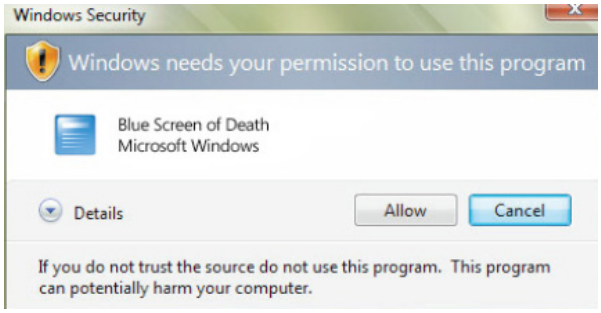


Рис. 2. Пример всплывающего окна системы безопасности MicrosoftWindows

Для оценки возможности интеграции юзабилити в систему безопасности был проведен эксперимент, выполненный Gunsonи др. [6] на основе системы автоматизированного телефонного банкинга. Восприятие безопасности было усилено путем добавления процедуры расширенной аутентификации за счет удобства использования системы. При проведении эксперимента было обнаружено, что 90% пользователей успешно входили в систему, когда процессу аутентификации требовался только один шаг, но при использовании двухфакторной аутентификации (ввод секретного номера и кода доступа) количество пользователей, успешно выполнивших задание, снижалось. Результат эксперимента показывает компромисс между удобством использования и безопасностью. Еще одно исследование, проведенное Михайловым и др. [7], использовало подход количественной оценки характеристик безопасности и удобства использования систем. На их основе определялся

критерий качества как линейная зависимость между критериями качества безопасности и удобства использования. Другое исследование, проведенное Chiassonи др. [8], было посвящено аспекту безопасности пользовательского интерфейса, рассматривая графические пароли. Было установлено, что пользователи имели тенденцию выбирать предсказуемые пароли и повторно их использовать для разных учетных записей.

Проблемы нахождения компромисса между безопасностью и юзабилити требуют проведения дальнейших исследований. На основе обзора литературы, сформулированы основные вопросы по проблеме безопасности и юзабилити ПИ, а также приведены основные результаты проведенных исследований.

Во-первых, какие критерии могут быть использованы для оценки юзабилити ПИ [3]? Рассматривая юзабилити, необходимо принять во внимание систему безопасности с точки зрения пользователя [3]:

1) удобство – безопасность системы не должна быть заметной, поскольку это вызовет неудобства для пользователя (например, простое отключение данной функции, если это предусмотрено системой) [9];

2) понятность – способность пользователей системы понять возможности безопасности, показывает степень удобства использования этой системы [9]. Например, количество времени, которое пользователь тратит на получение пароля и последующего прохождения аутентификации [4]. Одним из основных принципов проектирования ПИ является принцип, по которому пользователь должен уметь распознавать, а не вспоминать свойство конкретной функции системы;

3) инклюзивность – идея состоит в том, что каждый пользователь, независимо от уровня познавательных способностей, может использовать систему с функциями безопасности (то есть пользователю в любой момент времени понятно, что от него требует система безопасности);

4) системные требования – системные требования определяют свойства, необходимые для аппаратной, технической и программной поддержки функций безопасности системы [3].

Вторая проблема, которая возникает – это какие критерии можно использовать для оценки безопасности системы? [3]

По мнению Михайлова и др. [4] критерии безопасности системы основаны на стандартах качества измерения безопасности. Критерии безопасности следующие:

1) откровение (англ. revelation) – рассматривает уровень доступа пароля аутентификации с точки зрения пользователя и системы [3]. Существуют определенные способы, которыми пользователь системы может открыть свой ключ аутентификации. Один из этих способов – частые предупреждения всплывающих окон; чтобы избавиться от таких уведомлений, пользователь может согласиться на разглашение конфиденциальной информации [10];

2) секретность – возможность прогнозирования пароля пользователя;

3) конфиденциальность – относится к числу зарезервированных данных, необходимых для части аутентификации системы [11];

4) возможность взлома (англ. breakability) – это относится к усилиям, предпринимаемым злоумышленником для навигации по защищенной части системы и доступа к системе паролей. На основе того, как система построена, злоумышленник может использовать любой из следующих методов для определения ключа пользователя: кейлоггера, грубой силы, исследования и перебора по словарю [12];

5) множество паролей – этот критерий вычисляет пространство паролей аутентификации или, другими словами, набор возможных паролей, которые могут быть использованы для генерации[3].

В-третьих, какова связь между критериями безопасности и критериями удобства использования и их влияние на качество системы? [3]

Из вопросов исследований, которые были упомянуты выше, главный вопрос заключается в необходимости компромисса между юзабилити и безопасностью. Распространенное мнение заключается в том, что критерии удобства использования не должны рассматриваться для достижения значимых критериев безопасности и наоборот [3].С другой стороны, Угочи и др. в [3] утверждают, что существует возможность достижения удобства использования ПИ при необходимом уровне безопасности системы. Данное утверждение подтверждается работами Михайлова и др. [5, 7], а также Виера и др. [4].В двух работах [5, 7] Михайлова и др.провели обширное исследование механизмов аутентификации, попытались количественно оценить их, разработали базовую структуру для создания компромисса между юзабилити и безопасностью (например, использование «умных» дефолтных значений, чтобы пользователь не тратил большое количество времени на их осознание, но в тоже время мог ими управлять).

Выводы. Очевидно, что критерии качества юзабилити и безопасности нельзя обсуждать отдельно друг от друга. Данные критерии необходимо рассматривать совместно на протяжении всех этапов разработки ПИ. Безопасный дизайн интерфейса пользователя – одна из основных проблем современных систем. На основе проведенного литературного обзора была показана возможность совмещения критериев юзабилити и безопасности. Грамотное проектирование ПИ с учетом обоих видов критериев позволяет максимально снизить риск дорогостоящей ошибки.

СПИСОК ЛИТЕРАТУРЫ

1. Moller S., Ben-Asher N., Engelbrecht K.-P., Englert R., Meyer J. Modeling the behavior of users who are confronted with security mechanisms // Computers & Security, 2011, № 30, P. 242-256.
2. Cranor L. F., Buchler N. Better together: Usability and security go hand in hand // IEEE Security & Privacy, 2014, P. 89-93.
3. Ugochi O. N., Beverly A. O., Babak B. R. Usability and Security in User Interface Design: A Systematic Literature Review // I.J. Information Technology and Computer Science, 2016, № 5, P. 72-80.
4. Weir C. S., Douglas G., Carruthers M., Jack M. User perceptions of security, convenience and usability for ebanking authentication tokens // Computers & Security, 2009,№ 28, P. 47-62.
5. Mihajlov M., Blažič B. J., Josimovski S. Quantifying Usability and Security in Authentication,2011,P. 626-629.
6. Gunson N., Marshall D., Morton H., Jack M. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking // Computers & Security, 2011, № 30, P. 208-220.
7. Mihajlov M., Jerman-Blazic B., Josimovski S.A conceptual framework for evaluating usable security in authentication mechanisms-usability perspectives, 2011,P. 332-336.
8. Chiasson S., Forget A., Biddle R., Van Oorschot P. C. User interface design affects security: Patterns in click-based graphical passwords // International Journal of Information Security, 2009, № 8, P. 387-398.
9. Furnell S. Usability versus complexity–striking the balance in end-user security // Network Security, 2010, № 2010, с. 13-17.
10. Dhamija R., Dusseault L. The seven flaws of identity management: Usability and security challenges// Security & Privacy, IEEE, 2008, № 6, P. 24-29.
11. Habiba U., Masood R., Shibli M. A., Niazi M. A. Cloud identity management security issues & solutions: a taxonomy// Complex Adaptive Systems Modeling, 2014, № 2, P. 1-37.
12. Renaud K. Evaluating authentication mechanisms // Security and Usability: Designing Secure Systems That People Can Use, 2005, P. 103-128.

УДК 004.056

ПОДХОД К ФОРМИРОВАНИЮ МОТИВОВ ПЕРЕМЕЩЕНИЙ СОТРУДНИКОВ ВНУТРИ ОРГАНИЗАЦИИ

Новикова Евгения Сергеевна[1,2], Бекенева Яна Андреевна[1]
[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия, д. 39,
emails: novikova.evgenia123@gmail.com, yana.barc@mail.ru

***Аннотация*:** В статье рассматривается основанный на мотивах подход к анализу перемещения сотрудников с целью выявления аномалий. Подробно рассмотрены характеристики мотивов и атрибуты маршрутов. Представленный подход помогает снизить объем обрабатываемых данных, получаемых из логов журналов перемещений, а также автоматически выявлять отклонения в траекториях сотрудников.

***Ключевые слова**: перемещения сотрудников; мотивы; атрибуты маршрутов; аномалии перемещений.*

APPROACH TO THE EXTRACTION OF THE MOTIVES IN EMPLOYEES MOVEMENT WITHIN ORGANIZATION

Novikova Evgenia[1,2], Bekeneva Yana[1]
[1] The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
[2] St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
Russia, St. Petersburg, 14 Line, 39,
emails: novikova.evgenia123@gmail.com, yana.barc@mail.ru

Abstract: The article deals with the motif-based approach to employees' movement analysis for anomalies detection. Motives features and routes attributes are considered in details. The presented approach helps to reduce the amount of data processed from the logs, as well as automatically detect deviations in employee trajectories.

***Keywords**: employees' movement; motives; route attributes; movement anomalies.*

Введение. В настоящее время всё чаще возникает задача анализа данных, описывающих движение различных объектов. Анализ этих данных позволяет решить достаточно широкий спектр практических задач, таких как определение типичных маршрутов, наиболее посещаемых мест, выявление существующих в изучаемой среде ограничений или правил. Одной из частных задач является исследование данных о перемещениях сотрудников внутри организации. Анализ перемещений сотрудников необходим для определения типичных маршрутов, а также выявления различных аномалий в их поведении. Решение этих задач обеспечивает контроль выполнения установленных политик безопасности и способствует выявлению внутреннего нарушителя информационной безопасности [1].

Основная идея предлагаемого в данной работе подхода заключается в том, что сотрудники осуществляют перемещения внутри организации из-за некоторых профессиональных обязанностей, таких как приход на рабочее место, посещение еженедельных совещаний или некоторые индивидуальные потребности, такие как поход на обед кафе или перерыв в течение рабочего дня. Таким образом, каждый шаг сотрудника можно объяснить с помощью какого-либо мотива, который описывается комбинацией временных и пространственных атрибутов каждого перемещения. В том числе это касается специфических особенностей посещаемого помещения, например, конференц-залов, офисов, уборных и др. Использование мотивов помогает преобразовать пространственно-временную информацию о перемещениях работников в последовательность более высоких уровней абстракции деятельности, что позволяет осуществлять эффективный и семантически значимый анализ. Ходы, которые не могут быть распознаны как перемещение на основе какого-либо из мотивов, считываются аномальными. В рамках предложенного подхода мотивы перемещений работника извлекаются из журналов бесконтактных датчиков контроля доступа и атрибутов контролируемой зоны.

Когда аналитик не обладает маркированными данными, описывающими нормальное и ненормальное поведение, единственно возможным решением является применение методов кластеризации на основе исследования траектории. Полученные кластеры затем используется для описания нормального поведения движущихся объектов, в то время как выбросы могут быть использованы для обнаружения аномалий. Кластеры могут быть найдены с помощью центроида на основе подходов, иерархических моделей или подходов на основе плотности [2, 3].

В этой статье предлагается подход, основанный на принципах, аналогичных принципам, предложенным в [4, 5]. Тем не менее, [4, 5] разработаны для анализа траекторий морских судов, и, таким образом, предметная область существенно отличается от исследуемой в данной работе, а потому требует другой разработки концепции мотива. В работе [6] рассматривается подобный вопрос, однако, модель поведения создается с точки зрения посещаемых зон, в то время как предлагаемый подход позволяет абстрагироваться от этих данных низкого уровня и представить модель поведения с точки зрения мотива на основе мероприятий высокого уровня, такие как встречи с коллегами, работа в офисе и перерыв на обед.

Описание подхода. В общем случае движение может быть представлено в виде набора пространственно-временных характеристик, указывающих на местоположение объекта, время его появления и продолжительность его пребывания в конкретной точке пространства. В предложенном подходе в качестве источника исходных данных используются журналы, формируемые считывателями контролируемых зон. Они содержат информацию только о времени посещения контролируемой зоны конкретным сотрудником. Эти сведения дополнены данными о должностях сотрудников организации, а также картой здания с указанием расположения офисов, кафе, лестниц, конференц-залов внутри контролируемой зоны.

В предлагаемом подходе мотив представляет собой комбинацию пространственных и временных атрибутов движения, выполняемых атрибутами посещенной контролируемой зоны.

Пространственные атрибуты мотива построены на основе контролируемых зон, посещенных сотрудником, и их атрибутами. План контролируемых зон позволяет построить график соседних зон. Предполагается, что маршрут сотрудника между двумя несмежными контролируемыми зонами будет состоять из зон, которые составляют самый короткий путь между выбранными зонами, в случае, если нерегулярный визит зоны, не включенной в кратчайший путь, можно считать ненормальным.

Для определения мотива анализируется следующие атрибуты маршрутов сотрудников: свойства зон, входящих в последовательность, время и длительность их прохождения и длительность нахождения в конечной точке последовательности. Также необходимо учитывать, в каком отделе работает сотрудник и где находится его рабочее место. Например, в одной зоне могут находиться кафетерий, санитарные комнаты, конференц-залы и офисы коллег конкретного сотрудника. Если данная зона является конечной в последовательности, то по времени суток и длительности нахождения в ней, можно сделать предположения о том, куда пришел сотрудник. Таким образом, если длительность нахождения сотрудника в зоне, в которой находится столовая или кафе около 30-60 минут в середине рабочего дня можно определить мотив «обеденный перерыв».

При анализе маршрутов передвижения считается, что сотрудник выбирает кратчайший путь до конечной контролируемой зоны. В случае если сотрудник выбирает иной путь, маршрут определяется как аномальный, и данные о нем передаются аналитикам для дальнейшего его анализа.

Этот подход позволяет при анализе исторических данных выявить перемещения сотрудника, являющиеся нормальными для него (например, проход на рабочее место, зон отдыха, посещение совещаний) и обнаружить возможные аномалии, требующие более тщательного изучения. Также этот подход позволяет описать типичные шаблоны поведения сотрудников относительно контролируемых зон.

Можно описать мотив следующим образом:

$$Motif = \left\{ f_i, dep_id, \left\{ wd_j, offset_j, t_dur_j \right\}_{j=1}^{n} \right\}, \quad (1)$$

где fi – атрибут зоны, dep_id – отдел сотрудника, wdj – день недели, time_offsetj - смещение времени с начала дня в секундах, t_durj – продолжительность пребывания в зоне с атрибутом fi. Поскольку предполагается, что мотив может иметь временную периодичность, следует определить набор временных ограничений, описывающих, когда имеет место данный мотив. Например, работник может посещать собрания, проводимые в его/ее отделе, каждый понедельник и среду утром в 10.30. Пусть продолжительность встречи будет около полутора часов и находиться в контролируемой зоне с офисами, то такие визиты, зарегистрированные датчиками приближения, могут быть объяснены мотивом «встречи с коллегами». Ежедневный визит в зону, в которой находится столовая или кафе с продолжительностью пребывания около 45 минут в середине рабочего дня, можно объяснить мотивом «обеденный перерыв».

Очевидно, что сотрудники совершают даже запланированные перемещения в разное время, например, они могут приступить к работе в 7.55 утра, в 7.58 утра или даже 7.43. Они могут пообедать в течение 30 минут или 47 минут. При извлечении шаблонов необходимо учитывать возможные вариации временных атрибутов маршрутов для получения более обобщенного описания их мотивов. Возможное решение проблемы состоит в том, чтобы сгруппировать необработанные функции траекторий сотрудников и извлечь функции более высокого уровня. Центрифуги недавно найденных кластеров можно рассматривать как описание мотива, которое может быть применено далее для классификации журналов датчиков приближения в качестве мотивов.

После преобразования необработанных журналов они сгруппированы по отделам сотрудников. Это делается, потому что предполагается, что мотивы могут варьироваться от отдела к отделу. Затем каждой зоне назначаются атрибуты и группы, преобразованные в журнал, в соответствии с атрибутами зоны независимо от идентификатора зоны. Это позволяет извлекать кластеры из набора журналов, создаваемых датчиками близости зон с аналогичными характеристиками для сотрудников одного отдела.

Использование мотивов позволяет осуществлять преобразование необработанных логов с датчиков приближения, содержащих только идентификаторы контролируемых зон в семантически значимый список видов деятельности. Это делается путем маркировки необработанных данных с помощью извлеченных мотивов. Логи с одинаковыми мотивами объединяются в один лог, сохраняя метку времени первого лог с заданным мотивом.

Трансформированные логи с датчиков приближения, оснащенных ярлыками мотивов, могут использоваться для моделирования поведения сотрудников одного отдела. Для формирования сети Петри N, описывающей модель поведения сотрудников, можно использовать алгоритм Alpha. Он определяется следующим образом $N = \{P, T, F\}$, где P - множество положений, T - множество переходов (мотивов), F - множество дуг, соединяющих положения и переходы. На рисунке 1 представлена сеть Петри, построенная для необработанных логов из датчиков приближения, а на рисунке 2 – сеть Петри, построенная для трансформированных логов, отмеченных метками мотивов. Ясно видно, что вторая сеть Петри более очевидна, и ее довольно легко понять аналитику, особенно в том случае, когда профиль ролей сотрудников неясен.

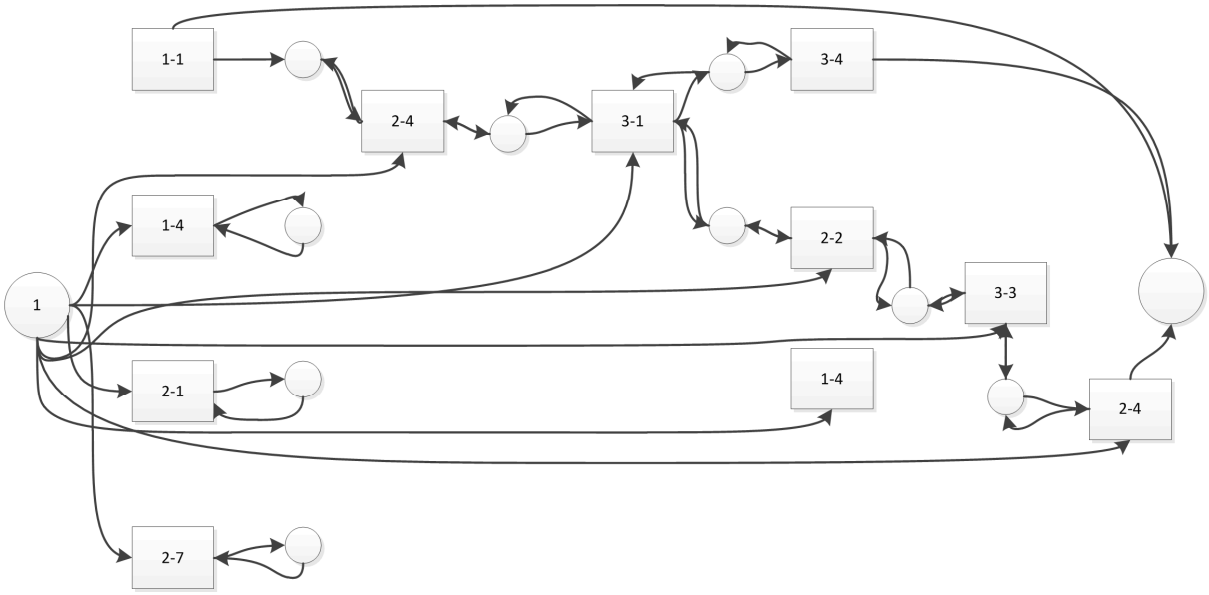


Рис. 1. Сеть Петри, построенная на основе необработанных логов

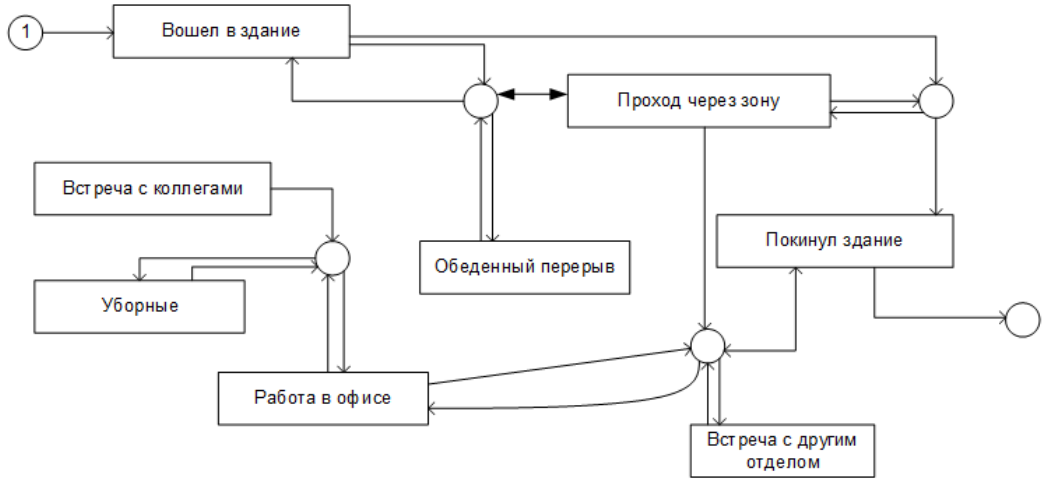


Рис. 2. Сеть Петри, построенная на основе трансформированных логов

Заключение. В статье предложен основанный на мотивах подход к обнаружению пространственно-временных моделей и аномалий в движении сотрудников. Представленный подход к анализу движений критической инфраструктуры, в отличие от известных, объединяет данные траектории, атрибуты контролируемых зон и положение сотрудников в организации. Используя мотивы, можно трансформировать пространственно-временные данные о траекториях сотрудников в последовательность действий более высокого уровня абстракции. Перемещение, которое не может быть признано основанным на мотивах, считается аномальным. В предлагаемом подходе мотивы движения сотрудников извлекаются из журналов датчиков приближения контроля доступа и атрибутов контролируемой зоны.

СПИСОК ЛИТЕРАТУРЫ

1. Pan X., Han C., Dauber K., Law K. A multi-agent based framework for the simulation of human and social behaviors during emergency evacuations //Ai & Society. – 2007. – Т. 22. – №. 2. – С. 113-132.
2. Kisilevich S., Mansmann F., Nanni M., Rinzivillo S. Spatio-temporal clustering //Data mining and knowledge discovery handbook. – Springer US, 2009. – С. 855-874.
3. Zendulka J., Pesek M. Mining moving object data //Open Computer Science. – 2012. – Т. 2. – №. 3. – С. 183-193.
4. Li X., Han J., Kim S. Motion-alert: automatic anomaly detection in massive moving objects //International Conference on Intelligence and Security Informatics. – Springer, Berlin, Heidelberg, 2006. – С. 166-177.
5. Li X., Han J., Kim S., Gonzalez H. ROAM: Rule-and motif-based anomaly detection in massive moving object data sets //Proceedings of the 2007 SIAM International Conference on Data Mining. – Society for Industrial and Applied Mathematics, 2007. – С. 273-284.
6. Novikova E. S., Murenin I. N., Shorov A. V. Visualizing anomalous activity in the movement of critical infrastructure employees //Young Researchers in Electrical and Electronic Engineering (EIConRus), 2017 IEEE Conference of Russian. – IEEE, 2017. – С. 504-509.

МЕТОД РАНДОМИЗИРОВАННЫХ СВОДНЫХ ПОКАЗАТЕЛЕЙ ДЛЯ ЭКСПЕРТНОЙ ОЦЕНКИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Попова Елена Владимировна
Смольный институт РАО,
Россия, Санкт-Петербург, Полюстровский проспект, 59.
emails: serana5@inbox.ru

***Аннотация*:** В статье анализируются методы многокритериальной оптимизации для подбора наилучшего варианта системы защиты информации. Делается вывод о методе рандомизированных сводных показателей, как наиболее подходящем, нуждающемся в дальнейшей модификации .

***Ключевые слова**: многокритериальная оптимизация, сводный показатель; система защиты информации.*

METHOD OF RANDOMIZED CONSOLIDATED INDICATORS FOR EXPERT EVALUATION OF INFORMATION PROTECTION SYSTEMS

Popova Elena
Smol'nyj Institut RAO,
Rossija, Sankt-Peterburg, Poljustrovskij prospekt, 59.
emails: serana5@inbox.ru

Abstract: The article analyzes the methods of multicriteria optimization for the selection of the best variant of the information security system. The conclusion is made about the method of randomized aggregates as the most appropriate in need of further modification.

***Keywords**: multi-criteria optimization, summary indicator; information security system.*

Введение. Методы многокритериальной оптимизации более полно отражают задачи, ставящиеся перед реальными многосвязными системами, которыми являются системы защиты информации (СЗИ). Перед лицом, принимающим решение, появляется проблема выбора наиболее подходящего метода многокритериальной оптимизации, и, как следствие, принятие допущений, условностей, границ теоретических аналогов реальных объектов. Ставится задача выбора оптимального варианта СЗИ, который спроектирован для конкретного предприятия. Оптимизация проводится по нескольким критериям: равнозначным, независимым, наиболее полно отражающим объекты выбора.

Рассмотрим различные способы выбора оптимизационного варианта. На основе проведённого анализа выберем метод, соответствующий поставленной задаче и имеющий минимальные недостатки. При построении траектории выбора наилучшего варианта есть соблазн сократить количество вариантов, например, до множества Парето, убрав заведомо худшие. Согласно принципу Эджворта-Парето [1], при многокритериальном выборе один вариант лучше другого, если по одному частному критерию он лучше другого, а по остальным не хуже. Сформированное множество Парето не больше первоначального количества вариантов, и задача нахождения наилучшего варианта, как кажется, упрощается. Но наилучшие решения могут лежать за пределами множества Парето, если не выполняются определённые условия использования принципа, например, аксиома транзитивности, в которой говорится, что отношение предпочтения должно быть транзитивным бинарным отношением.

Ещё один путь упрощения задачи – сокращение количества критериев. Метод главного критерия уменьшает множество критериев до одного [2]. Один критерий объявляется главным, по нему ищется экстремум, а остальные критерии формируют ограничения. Один из главных недостатков метода – это допустимая область решения может оказаться пустым множеством.

Метод уступок [2] преодолевает недостаток предыдущего метода. Критерии оцениваются по значимости и используются в порядке возрастания. Выбирается первый критерий и решается однокритериальная задача. Затем находят величину возможного отклонения. Не выходя за размеры фиксированных отклонений, итерационно находятся следующие экстремальные задачи. В конце используют последний критерий, и решается задача, аналогичная задаче с главным критерием. При достижении граничных условий решение может быть слабо эффективным.

Метод свёртки применяют при агрегировании всех критериев в скалярную величину, и на основании этой величины происходит оценивание объекта [3]. Свёртка имеет аддитивный или мультипликативный вид. Мультипликативная запись зависит от уменьшения значений отдельных критериев и может стремиться к нулю. При аддитивной свёртке уменьшение значений некоторых критериев компенсируется увеличением других, имеющих большую «весомость». Мультипликативную свёртку можно перевести в аддитивную, логарифмируя произведение.

Немаловажным этапом метода свёртки является задача выбора весовых коэффициентов, которая допускает различные решения. Метод логического анализа основан на прямом экспертном присвоении конкретных значений критериям. Эксперты присваивают значения критериям в диапазоне натурального ряда от единицы до величины количества критериев [4]. Весовые коэффициенты считаются как отношение суммы присвоенных значений разными экспертами одному критерию к общей сумме по всем критериям и по всем экспертам. В случае разной компетентности экспертов, им присваиваются экспертные коэффициенты, которые включаются в формулы. В этом методе важны не только правильно подсчитанные экспертные коэффициенты, но и достаточное количество экспертов.

Метод анализа иерархий [4] основан на построении матриц парных сравнений различных критериев. Матрица должна быть квадратная, обратно-симметричная и согласованная. Оценивается критерий натуральными числами от 1 до 9. Диагональные элементы после нормализации и образуют весовые коэффициенты. При построении первоначальной матрицы, если критерий менее важен его значение оценивается обратным числом. Таким образом, важный критерий с оценкой n и менее важный с оценкой $\frac{1}{n}$, симметрично расположенные относительно диагонали, отличаются в n^2 раз, где $n\epsilon\{1,\dots,9\}$, что является грубым приближением.

Формулы Фишберна [4] дают аналитическую запись весовых коэффициентов. Если критерии упорядочены в порядке убывания, то предлагается применить арифметическую или геометрическую убывающую прогрессию. Весовые коэффициенты, полученные с помощью простых формул, кажутся очень привлекательными, но, во-первых, не во всех задачах критерии подчинены отношению порядка, и, во-вторых, встаёт вопрос обоснования применения формул прогрессий.

К методу свёртки относится метод сводных показателей (МСП). Существует вектор исходных характеристик исследуемого объекта $\boldsymbol{x} = (x_1, \dots, x_m)$. $q_i(x_i)$ – отдельные показатели объекта. $\boldsymbol{w} = (w_1, \dots, w_m)$ - вектор весовых коэффициентов. $Q(q_1, \dots, q_m; \boldsymbol{w})$- сводный показатель исследуемого объекта. В методе рандомизированных сводных показателей (МРСП) неопределённость задания весовых коэффициентов компенсируется их рандомизацией [5,6]. Весовые коэффициенты имеют совместное равномерное распределение на области допустимых значений. Рандомизированный сводный показатель представляет собой случайную величину, у которой можно подсчитать математическое ожидание $\bar{Q}^{(j)} = M\tilde{Q}^{(j)}$, стандартное отклонение $S^{(j)} = \sqrt{D\tilde{Q}^{(j)}}$ и достоверность

доминирования $P(\{\tilde{Q}^{(m)} > \tilde{Q}^{(l)}\}) > \alpha$.. Для увеличения точности и достоверности оценок применяют дополнительную нечисловую, неполную и неточную информацию, то есть *ннн*-информацию (I).

Рассмотрим различные модификации МРСП. Из перечисленных методов наиболее подходящим к решению задачи выбора наилучшего варианта СЗИ по равнозначным независимым критериям является метод свёртки с рандомизированными весовыми коэффициентами, то есть МРСП.

МРСП подвергается изменениям при решении специфических задач. Одним из способов модификации МРСП является применение модели с иерархической системой критериев [7], где на каждом уровне решаются локальные задачи, а итоговые результаты объединяются на самом высоком уровне. На нулевом уровне строятся несколько сводных показателей, которые делят критерии на подзадачи. Сводные показатели следующего уровня формируются на основе показателей предыдущего уровня. Происходит декомпозиция сложной задачи на более простые подзадачи. Недостатком данной модификации является потенциальная сложность разбивки на подзадачи. Используется принцип сильных и слабых связей. То есть связи между сводными показателями, формирующими показатель более высокого уровня должны быть сильнее, чем с другими показателями «своего» уровня. Также происходит увеличение дисперсии с переходом на следующий иерархический уровень. При формировании сводных показателей на всех иерархических уровнях для повышения точности оценок формируется экспертами дополнительная *ннн*-информация. Но эксперту психологически трудно оценить сводные показатели на разных уровнях, имеющие сложные связи.

В другой работе [8] формируются два различных набора оценок объектов в определённые промежутки времени, сформированные двумя экспертными группами. Итоговые результаты (более высокий иерархический уровень) получают как усреднение предыдущих результатов. Для этого метода необходимо двойное количество экспертов с одинаковыми оценками компетентности, и расчёт допустимых границ согласованности действий экспертов как внутри группы, так и между группами.

Во всех работах, с описанием практических расчётов применения МРСП, в основе вычислений использовались точные данные об исследуемых объектах, полученные из печатных источников, котировок, электронных документов [9,10]. Количественные оценки разных свойств одного объекта затем подвергались нормировке и подстановке в формулы метода. При исследовании СЗИ, спроектированной для конкретного предприятия точные данные, характеризующие её показатели по критериям, например, конфиденциальности, целостности, доступности информации невозможно найти в каких-либо источниках. Поэтому необходима новая модификация МРСП, подходящая для выбора наилучшего варианта СЗИ с учётом возможности использования точного результата в критериальных формулах.

Заключение. МРСП выбран как наиболее подходящий для решения поставленной задачи нахождения наилучшего варианта СЗИ. Подбирая подходящую модификацию данного метода, можно добиться количественного обоснования полученных результатов по критериям, коррелирующим с показателями бизнес-процессов предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Ногин В. Д. Обобщённый принцип Зджворта-Парето и границы его применимости // Экономика и математические методы, «Издательство Наука», М. 2005. С. 128-134.
2. Городецкий С. Ю. ННГУ. Учебный курс «Модели и методы конечномерной оптимизации». Часть 2. Нелинейное программирование и многоэкстремальная оптимизация. // Учебно-исследовательская лаборатория "Математические и программные технологии для современных компьютерных систем (Информационные технологии)". 2003. 157 с.
3. Герасимова Л.В., Погожев И.Б. Комплексная оценка качества проектов и выбор оптимального варианта по методу академика А.Н. Крылова // Стандарты и качество. 1972. №8. С.37-39.
4. Постников В. М. Спиридонов С. Б. Методы выбора весовых коэффициентов локальных критериев // Наука и Образование. МГТУ им. Н. Э. Баумана, Электрон. журн. 2015. № 06. С. 267-287.
5. Хованов Н.В., Федотов Ю.В. Модели учета неопределенности при построении сводных показателей эффективности деятельности сложных производственных систем // Научные доклады НИИ менеджмента СПбГУ. 2006. № 28. 37 с.
6. Hovanov N., Yudaeva M., Hovanov K. “Multicriteria estimation of probabilities on basis of expert non-numeric, non-exact and non-complete knowledge // Abstracts of 18-th International Conference on Multiple Criteria Decision Making”. Chania (Greece), June 19-23, 2006. P.102.
7. Михайлов М. В. Модель оценки качества институтов высшего профессионального образования // Вестник Санкт-Петербургского университета. Сер. 5. Вып. 4. 2006. С. 74-82.
8. Жук С.Н. Оценка эффективности функционирования сложных систем по иерархической системе показателей // Труды СПИИРАН. 2013. Вып. 26. С. 194-203.
9. Корников В. В., Серегин И. А., Хованов Н. В. Многокритериальное оценивание финансовых рисков в условиях неопределённости: Учеб. Пособие. СПб.: Изд-во С.-Петерб. Ун-та, 2002. 96 с.
10. Хованов Н. В., Федотов Ю. В. Модели учёта неопределённости при построении сводных показателей эффективности деятельности сложных производственных систем // Научные доклады № 28(R)-2006. СПб.: НИИ Менеджмента СПбГУ, 2006. 31 с.

УДК 004.056.53

ОРГАНИЗАЦИЯ ДРЕВОВИДНЫХ ХРАНИЛИЩ ДАННЫХ С УЧЁТОМ РАЗМЕЩЕНИЯ В НИХ ЭЛЕКТРОННЫХ ПОДПИСЕЙ

Романова Юлия Николаевна, Янюшкин Константин Александрович
Государственный университет морского и речного флота им. адм. С.О. Макарова,
Россия, г. Санкт-Петербург, ул. Двинская 5/7,
emails: romanovaiuli@gmail.com, kayahidden@gmail.com

Аннотация: В статье рассматривается задача формирования блоков данных для вычисления дайджеста структурированных хранилищ информации большого размера, а также размещения сформированных электронных подписей в этих хранилищах. Описаны свойства предложенного подхода, который позволяет хранить подписи в виде древовидной структуры (с учетом порядка их формирования), которая позволяет последующее добавление данных и электронных подписей в хранилище.

Ключевые слова: *электронная подпись; структурированное хранилище; сплошное файловое хранилище; crypto api; потоки данных; дайджест; хэширование данных.*

DESIGN OF TREE-BASED SERIAL DATA STORAGES WITH INCLUDED DIGITAL SIGNATURES

Romanova Yuliya Nikolaevna, Yanyushkin Konstantin Aleksandrovich
Admiral Makarov State University of Maritime and Inland Shipping,
Russia, St. Petersburg, Dvinskaya str. 5/7,
emails: romanovaiuli@gmail.com, kayahidden@gmail.com

Abstract: This paper provides one of possible ways of forming data blob from big data storage with serial access for hashing function to form digital signature. Also, we describe the way of storing digital signatures of data parts inside of these storages, which allow to keep tree structure of signatures sequences and add subsequent data to storage.

Keywords: *digital signature; structured storage; big data storage; crypto api; data stream; data hashing.*

Введение. На современных предприятиях водного транспорта вся циркулирующая в них информация представлена в виде документов. На сегодняшний день практически все документы создаются изначально в электронном виде и, несмотря на то, что многие из них попадают на печать и подпись, продолжая свою жизнь в бумажном виде, всё больше документов остаются и хранятся исключительно в электронном виде, сохраняя при этом свою юридическую силу [1]. Согласно российскому законодательству, электронные документы, при соблюдении определённых законодательных норм, могут использоваться как для сообщения юридических и физических лиц с государственными органами, так и между собой. Ведение архива последовательности обмена данными, подписанными электронными подписями в сложных конфигурациях согласования документов в современной бизнес-логике, является не очевидной задачей с ростом скорости обработки и числа обрабатываемых документов [2]-[5]. Архив может быть представлен как последовательный поток данных (возможно, только с последовательным доступом), который разворачивается в древовидную структуру, похожую на структуру каталогов современных файловых систем [2].

Для внедрения подписи в последовательное хранилище рассмотрим его структуру. Структура хранилища с подписью имеет вид непрерывной битовой последовательности, хранящейся на физическом носителе [6], [7]. Корневое хранилище состоит из суб-хранилищ, и потоков данных. Каждое суб-хранилище имеет имя и свойства, а также, в свою очередь, само является хранилищем, тем самым обеспечивая древовидную структуру данных. Поток имеет имя и свойства и хранит в себе последовательность неформатированных данных. К имеющимся суб-хранилищам в корневое хранилище добавляется ещё одно, с зарезервированным именем DigitalSignatures, которое содержит потоки с подписями с именами signature_N, где N номер подписи. Потоки с подписями хранятся в той последовательности, в которой они были созданы. Подписываемые данные для хэширования собираются следующим образом:

1. Выбирается первый поток или первое хранилище (исключается хранилище с именем DigitalSignatures), который/которое содержится в корневом хранилище, к хэшируемым данным добавляется его имя;
2. Затем, если это хранилище, таким же образом рекурсивно обходится всё содержимое (потоки и субхранилища) этого хранилища;
3. Если это поток, то содержимое потока целиком добавляется к хэшируемым данным;
4. После обхода найденных потоков/хранилищ открывается хранилище DigitalSignatures, если оно существует. К хэшируемым данным добавляются все содержащиеся в нём потоки с контейнерами подписей в порядке следования без учёта имён этих потоков;

5. Собранный blob данных хэшируется, используя, например, реализованные отечественным ПО Крипто ПРО CSP (для *nix и Windows платформ) интерфейсные функции MS Crypto API, позволяющие частичную последовательную загрузку хэшируемых данных в оперативную память ЭВМ.

Процесс формирования подписи будет производится с использованием сертификата, который содержит открытый ключ электронной подписи, а также сведения о владельце сертификата и удостоверяющем центре, который его изготовил. Сертификат, используемый для подписания документа, должен быть установлен в локальное хранилище сертификатов или находится на съёмном защищённом носителе, откуда его может извлечь только используемый криптопровайдер. Оператору системы предлагается выбрать один из сертификатов хранилища. Выбранный сертификат открывается соответствующим ему криптопровайдером (если такого нет, то выдаётся ошибка). Сертификат проверяется на валидность, после чего, если он валиден, осуществляется попытка открыть по ссылке из сертификата контейнер с закрытым ключом, который должен соответствовать открытому ключу из сертификата. Оператор должен ввести PIN-код для контейнера, если это потребуется.

При проверке валидности сертификата происходит попытка построить цепочку доверия (цепочку подписанных сертификатов вплоть до корневого доверенного сертификата), в том числе с использованием загрузки из сети по указанному в сертификате адресу. В это же время происходит загрузка из сети списка отозванных сертификатов по адресу из сертификата, а также сверка с этим списком. Таймаут на эти операции установлен в зависимости от технических условий, а также требованиями регуляторов к обязательности проверки списков отозванных сертификатов. Помимо сформированной подписи в контейнер с подписью добавляются все сертификаты цепочки доверия. Структура контейнера закодирована в формате ASN.1, сертификаты и подпись в него входящие — согласно CAdES — RFC5126. Этот контейнер и записывается в поток Signature_N. Процесс формирования подписи и содержимое контейнера (Signed Message в терминах PKCS#7) представлен на рис. 1.

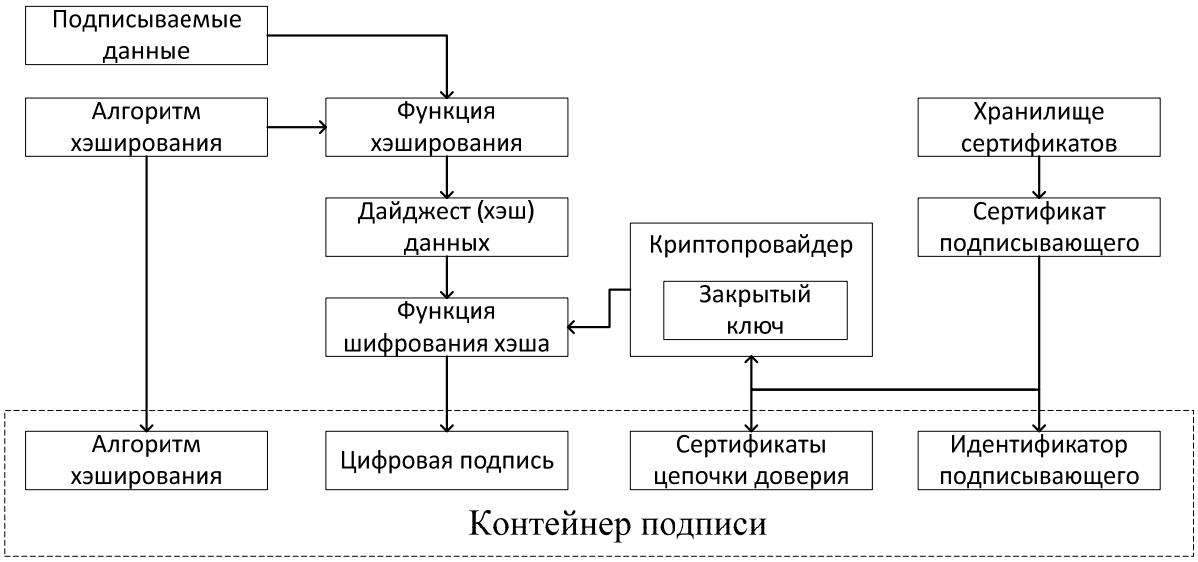


Рис. 1. Блок-схема процесса формирования подписи хранилища

В процессе проверки подписи для формирования цепочки доверия используются только сертификаты из контейнера подписи и локальных хранилищ. Никаких загрузок сертификатов и списков отзыва сертификатов не происходит, если иного не предусматривают особые требования законодательства к сфере применения метода.

Результатом проверки может быть три состояния:

1. Подпись верна, цепочка доверия построена и её корневой сертификат является доверенным;
2. Подпись верна, но нет доверия к сертификату. В этом случае отображаются подробности ошибок проверки;
3. Подпись не верна, сертификат в таком случае не проверяется. Отображаются подробности ошибок проверки.

Рассмотрим возможные преднамеренные или случайные изменения данных, расположенных в подписанном хранилище, а также последствия таких изменений [7]-[11]:

1. Смена порядка следования потоков/хранилищ приведёт к нарушению подписей документа;
2. Изменение содержимого любого потока приведёт к нарушению подписей документа;
3. Изменение имён потоков/хранилищ приведёт к нарушению подписей документа (кроме потоков хранилища DigitalSignatures, их имена не учитываются при подписании и могут быть изменены, это не повлияет ни на данные, ни на сами подписи);

4. Добавление любого нового потока/хранилища приведёт к нарушению подписей документа (кроме добавления нового, последующего потока в хранилище DigitalSignatures, он будет восприниматься как новая подпись);

5. Смена порядка следования потоков в хранилище DigitalSignatures приведёт к нарушению всех тех подписей, которые следуют за первым изменённым потоком, включая его;

6. Изменение любого потока в хранилище DigitalSignatures сделает соответствующую ему, а также все последующие подписи невалидными;

7. Удаление одного или нескольких последних потоков из хранилища DigitalSignatures не повлияет на работу, но все соответствующие потокам подписи документа будут удалены. Такое удаление будет невозможно отследить.

Заключение. Предложенная схема позволяет работать с последовательными хранилищами очень больших объёмов, содержащими древовидную структуру данных, которые могут быть подписаны последовательностью электронных подписей по мере заполнения.

СПИСОК ЛИТЕРАТУРЫ

1. Нырков А.П. Автоматизированное управление транспортными системами / А. П. Нырков, С. С. Соколов, А. А. Шнуренко // СПб.: ГУМРФ имени адмирала С.О. Макарова, 2013. – 325 с.
2. Черняков А.В. Алгоритмы резервного копирования / Черняков А.В., Нырков А.П. // Материалы работы III научно–исследовательской конференции студентов и аспирантов факультета информационных технологий. «IT: ВЧЕРА, СЕГОДНЯ, ЗАВТРА – 2014» 19 декабря 2014 г. – СПб.: ГУМРФ имени адмирала С.О. Макарова, 2015. – С. 129–133.
3. Сабанов А. Г. Скиба В. Ю., Некоторые аспекты защиты электронного документооборота [Журнал] // Проблемы информационной безопасности. Компьютерные системы. - 2012 г. №2 стр. 42-45.
4. Bukharmetov M.R. Robust Method for Protecting Electronic Document on Waterway Transport with Steganographic Means by Embedding Digital Watermarks into Images / M. R. Bukharmetov, A. P. Nyrkov, S. S. Sokolov, S. G. Chernyi, V. N. Kuznetsov, D. G. Mamunts // Proceedings of the 16-th Conference on Reliability and Statistics in Transportation and Communication, RelStat'2016, 19-22 October, Procedia Engineering 178, 2017. – С. 507 – 514. DOI: 10.1016/j.proeng.2017.01.097
5. Зима В.М. Молдовян А.А., Молдовян Н.А Безопасность глобальных сетевых технологий [Книга]. - СПБ. : БХВ-Петербург, 2003. - стр. 368. - ISBN: 5-94157-213-1.
6. Guntheroth K. Optimized C++: Proven Techniques for Heightened Performance [Книга]. - California (USA): O'Reilly Media Inc., 2016.
7. Summerfield M. Advanced Qt Programming: Creating Great Software with C++ and Qt 4 [Книга]. - London, England: Pearson Education (UK), 2016.
8. Куняев Н. Н. Демушкин А. С., Фабричнов А. Г., Конфиденциальное делопроизводство и защищенный электронный документооборот [Книга]. - Москва : Логос, 2011.
9. Мао В. Современная криптография. Теория и практика. [Книга]. - Москва : Вильямс, 2005.
10. Молдовян Н. А. Теоритический минимум и алгоритмы цифровой подписи [Книга]. - Санкт-Петербург: БХВ-Петербург, 2010.
11. Назаров С.В. Архитектура и проектирование программных систем: Монография [Электронный ресурс]. - М.: НИЦ Инфра-М, 2013 г. URL: http://www.znanium.com (дата обращения: январь 2017 г.).

УДК 0004.75

СОЗДАНИЕ ПЕРИМЕТРА БЕЗОПАСНОСТИ В ОБЛАЧНОЙ СРЕДЕ

Рыжков Сергей Романович
Санкт-Петербургский институт информатики и автоматизации РАН,
Россия, Санкт-Петербург, 14 линия, 39
email: Ryzhkov@iias.spb.su

***Аннотация*:** в статье рассмотрены возможности новой технологии блокчейн применительно к гарантированному хранению геометок с целью создания периметра безопасности

***Ключевые слова**: блокчейн; геометки; периметр*

BUILDING CLOUD SECURITY PERIMETER

Ryzhkov Sergey
The St. Petersburg Institute for Informatics and Automation of RAS,
Russia, St. Petersburg, 14-ya liniya V. O., 39
email: Ryzhkov@iias.spb.su

Abstract: The article presents how the blockchain technology can be used to create the guaranteed geotag storage to build a trusted security perimeter

***Keywords**: blockchain; geotaging; perimeter*

Введение. Периметр в облачных вычислениях виртуализован, т.к. он определяется параметрами виртуальной среды и выполняемых приложений. Тем не менее, при использовании облачных вычислений периметр динамически изменяется, размывается за счёт многоуровневой туннелированой вложенности и зависит от прохождения пакета по стеку протоколов. Каждый уровень вложенности позволяет создать снимок своего периметра, что позволяет, используя привязку к физическому периметру, затем разместить их на карте. Предлагается использование на физических серверах обеспечивающих работу виртуальных ферм, а также на аппаратных межсетевых экранах совокупности

технологий аппаратных модулей доверенной загрузки (АМДЗ) и модуля глобального позиционирования (ГЛОНАС), распределённой базы блокчейн для хранения данных ГЛОНАС в совокупности со слепком (хэшем) эталонного состояния виртуальных машин. Благодаря криптографическому опечатыванию данных работа с ними осуществляется только внутри периметра облачной среды. В случае завершения сеанса, выхода за пределы сетевого экрана, данные перестают читаться из-за недействительности сеансового ключа.

На уровне структур дополнительных процессов применение совокупности технологий геотегирования и блокчейн позволяет создать доверенный периметр, контролировать перемещаемые данные. «Геотегирование» представляет собой процесс определения, создания и инициализации набора объектов геолокации стационарного вычислительного устройства. Актуальным применением геотега является обеспечение соблюдения пограничного контроля на основе геотегов в концепции, называемой «геозаслон» [1]. Блокчейн можно представить, как информационную сеть нового поколения, которая базируется на уникальной единице хранения информации — транзакции. Уникальность технологии связана с тем, что эффект «сцепления» обуславливает зависимость каждого отдельного блока от всех блоков, обработанных перед ним, а не только от предыдущего блока, а распределённо хранимая база исключает возможность фальсификации. Блокчейн позволяет идентифицировать любые нуждающиеся в идентификации Сущности, т.е. данные геолокации стационарного вычислительного устройства (например межсетевого экрана) хранящиеся в распределённой блокчейн базе можно считать верифицированными. Созданный за счёт геотегирования доверенный периметр возможно дополнить функцией контроля перемещения данных за счёт криптографического опечатывания данных (при выходе за пределы периметра геометок данные не читаемы).

На рис. 1. представлена блок-схема системы управления данными внутри периметра облачных вычислений.

Рис. 1. Блок-схема системы управления данными внутри периметра облачных вычислений

Для РФ технология блокчейн конкурентно важна. Следует отметить уникальную возможность РФ для внедрения технологии блокчейн, она обусловлена следующими факторами:

1. Необходимость развития собственной независимой платёжной системы;
2. Наличие собственных, национальных криптографических алгоритмов (ГОСТ Р 34.11-2012(стрибог)) [2];
3. Контроль за лицензируемой деятельностью в области криптографии со стороны государственного регулятора;

4. Распределённая сеть аккредитованных удостоверяющих центров, которые могут выступать в роли гарантированных «майнеров» (поиск новых блоков, формирование хеш-последовательностей и майнинг-верификация блоков).

Всё вышеперечисленное может стать основой внедрения отечественной технологии блокчейн при условии сотрудничества между операторами, разработчиками и регуляторами.

Наделение данных пользователя системы облачных вычислений геометками происходит по следующему методу: клиент облачного провайдера, подключаясь к консоли управления, представленной на рис.1 управляет инициализаций меток и компонентов управляющих жизненным циклом принадлежащих ему данных, а также получает доступ к конкретному физическому серверу для контроля целостности платформы и доверенного хранения геометок. Клиент получает возможность убедиться, что данные аттестованного с помощью системы глобального позиционирования периметра картографированы, рабочий пул данных получает сессионный ключ доступа, а база блокчейн распределена только в разрешённых, геотегированных центрах обработки данных.

Технология блокчейн, а точнее база транзакций содержащая данные геолокации стационарного вычислительного устройства может быть применена в системах подтверждения состояния рабочих станций, работающих в реальном времени, по начальному (проверенному или доверенному) состоянию системы строится ХЭШ, который сравнивается с ХЭШ нового состояния. В таких системах единожды проверив программно-аппаратное обеспечение в любой момент времени, можно убедиться, что в эталонное состояние не было внесено изменений [3]. Более того, построенный таким образом периметр позволяет картографировать исходное состояние объекта информатизации, чтобы затем иметь возможность контролировать перемещение данных мобильными пользователями. Для этого каждый мобильный пользователь, оснащается средствами глобального позиционирования и средствами криптографической защиты информации. С определённой периодичностью мобильное устройство передаёт данные о своём местонахождении на сервер доступа и получает авторизацию, право на работу с данными. В случае выхода за пределы периметра данные блокируются. Для усиления защиты данных они могут хранится благодаря высокой фрагментации множества географически распределенных репликаций, а также благодаря использованию особого метода кодирования в момент записи, что позволяет гарантированно восстановить данные при аппаратном сбое. Логика хранения реализуется шлюзами, осуществляющими фрагментацию, распределение по удаленным серверам хранения и выполнение обратной операции сборки данных в единое целое из фрагментов с коррекцией в случае обнаружения ошибок [4].

Криптомодули АМДЗ не обеспечивают высокую производительность, так как выполняют только одну команду за раз, что затрудняет масштабируемость облачных сервисов, которые используют АМДЗ и подвержены атакам отказа в обслуживании. Тем не менее, использование криптографического преобразования эталонного состояния аппаратного узла на котором размещена виртуальная ферма в совокупности с данными геолокации этого аппаратного узла, возможно, использовать в качестве корня доверия для построения дерева сертификации и опечатывания данных, которое позволит ограничить пересечение границ периметра облачных вычислений. Доверенная платформа, т.е. платформа, чьё состояние гарантированно совпадает с эталонным, чья целостность гарантирована, измерена и подтверждена. Данные измерений описывают свойства и характеристики измеряемых компонентов. Аттестация платформы и запуск безопасного гипервизора являются основой надежности платформы, и благодаря постоянному мониторингу предоставляют более высокую скорость обнаружения проблем безопасности. Благодаря измерению эталонного состояния аппаратных и предстартовых составляющих системы генерируется корень доверия, внутри периметра доверие к распространяемым данным подтверждается по подтверждённым геометкам. При использовании дополнительного протокола безопасности геометки встраиваются в систему криптографически защищённого транспорта для обеспечения контроля над перемещением данных. Именно доверенное выполнение кода программ является основой системы. Аппаратный корень доверия создается организацией с уникальным идентификатором узла и метаданными платформы, хранится в антивандальном оборудовании. Эта информация доступна с помощью защищенных протоколов, чтобы можно было быть уверенным в целостности платформы и подтвердить местоположение узла.

Через механизм аттестационного протокола геотегирования информация (сформированная на этапе конфигурации сервера) сохраняется в виде зашифрованного хеш-значения в криптографическом модуле АМДЗ. Для обеспечения ограничений геолокации перед развертыванием и миграцией рабочей нагрузки запускается мониторинг геолокации. АМДЗ в защите периметра выполняет следующие функции:

— подтверждение данных геолокации;
— применение ограничений геолокации;
— запуск мониторинга геолокации

и специфически служит для гарантированного доверенного хранения, мониторинга и аудита за счет использования содержащегося в аппаратной части криптопроцессора, обеспечивающего средства безопасного создания ключей шифрования (с той же степенью неповторимости, что и генератор случайных чисел), а также средства ограничения использование ключей (как для подписи, так и для

шифрования/дешифрования). Модуль АМДЗ также используется для подтверждения подлинности аппаратных средств за счет уникальности специфических устройств, что делает возможным однозначное установление подлинности доверенной платформы [3].

Сервер доступа и мобильные устройства, находящиеся внутри периметра, обмениваются сессионными ключами, позволяющими авторизовать устройство для доступа к данным. Сессионный ключ имеет дополнительный идентификатор периметра, в котором разрешено обрабатывать данные.

Заключение. Облачные технологии не только изменили понятие платформы, виртуализировав взаимоотношения операционной системы с оборудованием, но и остро поставили задачу по созданию периметра безопасности в облачной среде [5]. На сегодняшний день актуальна задача по измерению географического ландшафта вычислительной структуры облачных вычислений, что позволяет классифицировать угрозы выхода за границу ландшафта. Комбинация технологий блокчейн и геометок позволяет обеспечить надежность облачных сервисов, конфиденциальность и целостность данных, защиту от инсайдеров, а также гарантировать расположение данных в определённых географических или юрисдикционных границах. Используя эталонные измерения как базу, администраторы систем осуществляют необходимую тонкую настройку политик размещения рабочих нагрузок и обработки конфиденциальных данных на конкретных серверах, так называемых доверенных вычислительных пулах.

СПИСОК ЛИТЕРАТУРЫ

1. Воробьев В. И., Рыжков С. Р., Фаткиева Р. Р. Защита периметра облачных вычислений //Программные системы: теория и приложения. – 2015. – Т. 6. – №. 1-1. – С. 61-71.
2. http://protect.gost.ru/document1.aspx?control=31&id=180209
3. Руднев Д. О., Сычугов А. А. МЕТОД ПОВЫШЕНИЯ ДОВЕРИЯ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ //Известия Тульского государственного университета. Технические науки. – 2016. – №. 11-1.
4. Черняк Л. Хранилище данных на кодах Рида–Соломона //Открытые системы. СУБД. – 2012. – №. 2. – С. 52-52.
5. Фаткиева Роза Равильевна, Рыжков Сергей Романович Геолокация для аутентификации и защиты данных // УЭкС. 2015. №12 (84). URL: http://cyberleninka.ru/article/n/geolokatsiya-dlya-autentifikatsii-i-zaschity-dannyh (дата обращения: 24.09.2017).

УДК 004.7.056.53

МЕТОДИКИ И ИНСТРУМЕНТЫ АУДИТА СЕТЕВОЙ БЕЗОПАСНОСТИ

Садикова Анастасия Александровна[1], Титова Юлия Алексеевна[2], Савков Сергей Витальевич[3]
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
Россия, Санкт-Петербург, пр-кт Кронверкский, 49
emails: nastya.sadkoo@mail.ru, titova.yulishna@mail.ru, sergsavkov@gmail.com

***Аннотация*:** Со временем сетевая инфраструктура усложняется, расширяются виды приложений и данных. Все эти изменения приводят к тому, что при осуществлении системы информационной безопасности, пользователь может не заметить некоторые уязвимости сети. В связи с этим необходимо проведение регулярного аудита безопасности. В данной статье обобщены виды аудита сетевой безопасности, рассмотрены методологии IAM и SAFETAG, а также особенности их проведения. Приведена краткая характеристика некоторых сканеров уязвимостей. Сделан вывод о том, что, хотя аудит безопасности и носит рекомендательный характер, он является необходимым для обеспечения целостности и конфиденциальности персональных данных людей, так или иначе связанных с организацией.

Ключевые слова: *аудит, тест на проникновение, сканеры уязвимостей, методология аудита, SAFETAG, IAM, сетевая безопасность, международные стандарты безопасности.*

METHODS AND TOOLS OF THE AUDIT OF NETWORK SECURITY

Sadikova Anastasia, Titova Yulia, Savkov Sergei
Saint Petersburg National Research University of Information Technologies, Mechanics and Optics «ITMO», Russia, St. Petersburg, Kronverkskiy prospekt, 49
emails: nastya.sadkoo@mail.ru, titova.yulishna@mail.ru, sergsavkov@gmail.com

Abstract: Over time, the network infrastructure becomes more complicated, expanding the types of applications and data. All these changes lead to the fact that the implementation of the information security system, the user may not notice some network vulnerabilities. In this regard, it is necessary to conduct regular security audit. This article summarizes the types of network security audit reviewed the methodology and IAM SAFETAG, as well as peculiarities of their implementation. A brief description of some of the vulnerability scanners. It is concluded that, although the security audit and is Advisory in nature, it is necessary to ensure the integrity and confidentiality of personal data of people involved with the organization.

Keywords: audit, penetration testing, vulnerability scanners, audit methodology, SAFETAG, IAM, network security, international security standards.

Введение. В современном мире сетевая безопасность имеет колоссальное значение. Под сетевой безопасностью понимают комплекс требований, которые предъявляются к инфраструктуре компьютерной сети, при выполнении которых обеспечивается защита сетевых ресурсов от несанкционированного доступа и эффективное функционирование сети в целом.

Одной из задач организации является предоставление своим сотрудникам безопасного доступа к сетевым ресурсам в любое время. Для решения задачи безопасности сети на предприятии проводят аудит сетевой безопасности. В коммерческих организациях руководство озабочено обеспечением безопасности своих активов, поэтому понимает важность проведения аудита. В некоммерческих организациях (далее – НКО) аудиту уделяется намного меньше внимания. Такое пренебрежение чревато тем, что персональные данные граждан, которые по ряду причин обратились в конкретную НКО, а также сотрудников, работающих в данной НКО, могут попасть в руки злоумышленников.

В наше время специалистами используется несколько определений аудита. Но наибольшее распространение получили два из них:

— аудит информационных систем — это проверка используемых компанией информационных систем, систем безопасности, систем связи с внешней средой, корпоративной сети на предмет их соответствия бизнес-процессам, протекающим в компании, а также соответствия международным стандартам с последующей оценкой рисков сбоев в их функционировании;

— аудит информационной безопасности — системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определенными критериями и показателями безопасности.

Как видно, суть обоих определений, в общем-то, одинакова и сводится к следующему. Аудит безопасности информационных систем — это их проверка, тестирование, которое должно выявить потенциальные опасности и уязвимости в защите. При этом используется принцип сравнения результатов теста с неким идеалом, установленным целями аудита, а также личным опытом самого аудитора. При этом должно учитываться множество самых разнообразных факторов, в том числе и информация о компании: область её деятельности, размер фирмы и прочее.[1]

Целями проведения аудита безопасности являются:

— анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов информационной системы (далее – ИС);

— оценка текущего уровня защищенности ИС;

— локализация узких мест в системе защиты ИС;

— оценка соответствия ИС существующим стандартам в области информационной безопасности;

— выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

Существует три вида аудита:

— Активный аудит;

— Экспертный аудит;

— Аудит на соответствие стандартам.

Экспертный аудит можно условно представить как сравнение состояния информационной безопасности с «идеальным» описанием, которое базируется на следующем:

— требования, которые были предъявлены руководством в процессе проведения аудита;

— описание «идеальной» системы безопасности, основанное на аккумулированном в компании-аудиторе мировом и частном опыте.

При выполнении экспертного аудита сотрудники компании-аудитора проводят следующие виды работ:

— сбор исходных данных об информационной системе, об её функциях и особенностях, используемых технологиях автоматизированной обработки и передачи данных (с учетом ближайших перспектив развития);

— сбор информации об имеющихся организационно-распорядительных документах по обеспечению информационной безопасности и их анализ;

— определение точек ответственности систем, устройств и серверов ИС;

— формирование перечня подсистем каждого подразделения компании с категорированием критичной информации и схемами информационных потоков.

Результаты экспертного аудита могут содержать разноплановые предложения по построению или модернизации системы обеспечения информационной безопасности.

Суть аудита на соответствие стандартам наиболее приближена к тем формулировкам и целям, которые существуют в финансовой сфере — при проведении данного вида аудита состояние информационной безопасности сравнивается с неким абстрактным описанием, приводимым в стандартах. Официальный отчет, подготовленный в результате проведения данного вида аудита, включает следующую информацию:

— степень соответствия проверяемой информационной системы выбранным стандартам;

— степень соответствия собственным внутренним требованиям компании в области информационной безопасности;

— количество и категории полученных несоответствий и замечаний;

— рекомендации по построению или модификации системы обеспечения информационной безопасности, позволяющие привести её в соответствие с рассматриваемым стандартом;

— подробная ссылка на основные документы заказчика, включая политику безопасности, описания процедур обеспечения информационной безопасности, дополнительные обязательные и необязательные стандарты и нормы, применяемые к данной компании.[2]

В данной статье будет более подробно рассмотрен активный аудит сетевой безопасности.

Активный аудит. Данный вид аудита является на данный момент одним из самых распространенных. Также его называют инструментальным аудитом. Он заключается в том, что исследование защищенности сети происходит с точки зрения злоумышленника. В процессе данного аудита осуществляется сбор информации о состоянии системы сетевой защиты с помощью программного обеспечения и специальных методов.

При данном виде аудита аудитор ставится на место злоумышленника, владеет минимумом информации (только той, которая находится в открытом доступе). Аудитор в таком случае должен смоделировать как можно больше видов атак на систему сетевой защиты, которые мог бы осуществить хакер. В результате подобного аудита формируется информация об уязвимостях, степени их критичности и методах устранения, а также предоставляются рекомендации по модернизации сетевой защиты. Полнота этой информации зависит от квалификации аудитора и используемых систем анализа защищенности.

Примером активного аудита является Pentest. Тест на проникновение (англ. penetration testing, pentest) – один из методов оценки безопасности компьютерных сетей средствами моделирования атаки злоумышленника. Целью такого испытания является оценка возможности проникновения в сеть и прогнозирование экономических потерь в случае удачной атаки.

Чтобы просканировать сеть и ее устройства, обнаружить в ней уязвимости, используют сканеры уязвимостей. Данный вид анализа занимает меньше времени, чем тест на проникновение, а также требует меньше денежных вложений. В результате работы сканера пользователь получает более конкретную и объективную оценку защищенности сети, поскольку сканеры уязвимостей представляют собой программные или аппаратные средства. С помощью сканера можно получить более широкий спектр уязвимостей, чем при использовании теста на проникновение. Получив этот список можно уже разработать план действий по устранению или смягчению этих уязвимостей. Также могут быть использованы низкоуровневые средства, такие как сканер портов, для выявления и анализа возможных приложений и протоколов, выполняющихся в системе.[7], [8]

1. Nessus. Чтобы проверить надежность сервисов, можно использовать как стандартные методы, так и имитацию сетевых атак с использованием базы данных. В результате работы Nessus представит отчет, содержащий список уязвимых мест, рекомендации по их устранению и уровень риска для каждого из них. Можно сконфигурировать сканер так, чтобы после первоначального исследования системы в дальнейшем он будет опираться на полученные данные, отмечая только изменения в результатах исследования. Также в данный сканер встроен сканнер портов, который распознает сервисы, причем не по привязке к портам, а с помощью сигнатур, количество которых также может быть расширено. Его отличительной особенностью является то, что данный сканер использует плагины. Полезным свойством сканера становится возможность планирования сканирования заданных хостов, определенных до этого как наиболее важные с точки зрения исследования защищенности. Но есть у него и два недостатка. Первый — при отключенной опции «safe checks» некоторые тесты на уязвимости могут привести к нарушениям в работе сканируемых систем. Второй — цена. Годовая лицензия может обойтись в 114 тысяч рублей.[3], [4]

2. OpenVAS – сканер уязвимостей, а также средство управления уязвимостями с открытым исходным кодом. Так же, как и Nessus, использует архитектуру клиент – сервер. Предназначен для активного мониторинга узлов вычислительной сети на предмет наличия проблем связанных с безопасностью, оценки серьезности этих проблем, а также для контроля их устранения. Активный мониторинг означает, что OpenVAS выполняет какие-то действия с узлом сети: сканирует открытые порты, посылает специальным образом сформированные пакеты для имитации атаки или даже авторизуется на узле, получает доступ к консоли управления, и выполняет на нем команды. Затем OpenVAS анализирует собранные данные и делает выводы о наличии каких-либо проблем с безопасностью. Эти проблемы, в большинстве случаев касаются установленного на узле необновленного ПО, в котором имеются известные и описанные уязвимости, или же небезопасно настроенного ПО.

3. Nmap используется для сканирования хостов и служб в сети. Nmap имеет продвинутые функции, которые могут выявить различные приложения, запущенные на системах, также как службы и особенности отпечатков ОС. Это один из наиболее широко используемых сетевых сканеров, он является очень эффективным, но в то же время и очень заметным. Nmap рекомендуется к применению в специфичных ситуациях, для предотвращения срабатывания механизма защиты. Если пользователь

тестирует на проникновение конкретный компьютер/сервер, то необходимо проверить все порты — с первого до последнего (65535). [4]

Примеры стандартов, на соответствие которым проводится аудит безопасности:

— ISO 27000 – Международные стандарты управления информационной безопасностью – это семейство включает в себя Международные стандарты, определяющие требования к системам управления информационной безопасностью, управление рисками, метрики и измерения, а также руководство по внедрению;

— ISO 15408 – Общие критерии оценки безопасности информационных технологий – содержат обобщенное формализованное представление знаний и опыта, накопленного в области обеспечения информационной безопасности на протяжении десятилетий;

— ISO 18028 – Международные стандарты сетевой безопасности – Этот стандарт содержит руководство по созданию сетей и организации взаимодействия с учетом аспектов безопасности при соединении сетей между собой и при получении удаленного доступа к сети. Руководство включает идентификацию и анализ факторов связанных с сетевыми взаимодействиями, которые следует принимать во внимание при определении требований к сетевой безопасности, идентификация необходимых областей контроля при подключении к сетям и обзор возможных областей контроля, включая проектирование и внедрение,;

— BSI\IT Baseline Protection Manual – Немецкий стандарт «Руководство по обеспечению безопасности ИТ» – содержательный и практичный стандарт по информационной безопасности. Он представляет собой набор документов, в которых содержатся подробные руководства по обеспечению информационной безопасности применительно к различным аспектам функционирования ИС и различным областям ИТ. Данный стандарт постоянно совершенствуется с целью обеспечения его соответствия текущему состоянию дел в области ИТ и информационной безопасности. К настоящему времени накоплена уникальная база знаний, содержащая информацию по угрозам и контрмерам в хорошо структурированном виде.

Методология IAM. Для оценки сетевых систем правительства Соединенных Штатов Америки Агентство Национальной Безопасности разработала методологию The INFOSEC Assessment Methodology, или IAM. Данная методология сейчас используется как государственными, так и негосударственными организациями. Целью IAM проекта является оказание помощи предприятию в улучшении позиции ее службы информационной безопасности. Оценка проводится в три этапа.

На первом этапе проводится оценка системы управления информационной безопасностью. На втором этапе – технологический аудит защищенности. Третий этап представляет собой анализ информационных рисков.

Отличительной особенностью IAM является то, что данная методология не просто содержит набор определений и требований, в ней описан процесс подготовки к оценке, непосредственный процесс выполнения оценки и описание документирования проекта. Есть 3 категории и 18 классов в рамках этих категорий, которые должны быть обязательно оценены в процессе тщательной IAM оценки, которая проводится на втором этапе. Этими категориями являются:

— Категория управления: 4 класса (например, планирование на случай чрезвычайных ситуаций и управление конфигурацией);

— Техническая категория: 9 классов (например, аутентификация, контроль подключений к сети);

— Категория операций: 5 классов (например, маркировка, образование и обучение).

Одной из целей аудита является проверка на соответствие стандартам. Если в организации необходимо проведение данного вида аудита, то IAM является подходящей ступенью в подготовке к подобной деятельности.[5]

Методология SAFETAG. Традиционный аудит сетевой безопасности основывается на предположении о том, что организация имеет время, деньги, а также возможность стремиться к как можно более полной безопасности. К сожалению, это непозволительная роскошь для малых компаний. Именно поэтому международной организацией Internews была разработана SAFETAG (Security Auditing Framework and Evaluation Template for Advocacy Groups) – методология аудита цифровой безопасности для НКО. Аудит SAFETAG состоит из нескольких шагов по сбору информации и подтверждению, а также научно-исследовательских мероприятий с сотрудниками, организованные для сбора задач, каждая из которых поддерживает основные цели SAFETAG, создавая оценку риска при одновременном наращивании потенциала организации. Отличительной особенностью этой методологии является то, что она распространяется по лицензии Creative Commons и имеет открытый исходный код. Мероприятия и структура SAFETAG показаны на рис. 1 и рис. 2.

В процессе работы аудитор сначала подготавливает необходимые технические компоненты аудита, затем фокусируется на непосредственном наблюдении за организацией и ее инфраструктурой. Эта фокусировка состоит из пассивной разведки публично доступных источников данных. Данная деятельность необходима для определения общедоступных ресурсов, связанных с компанией, и сбора информации об этих ресурсах. На следующем этапе определяются конфиденциальные данные организации, места их хранения, а также способы передачи.

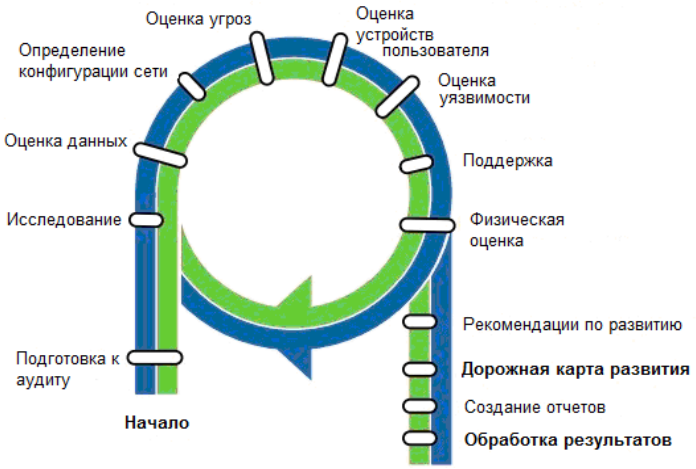


Рис. 1. Мероприятия SAFETAG

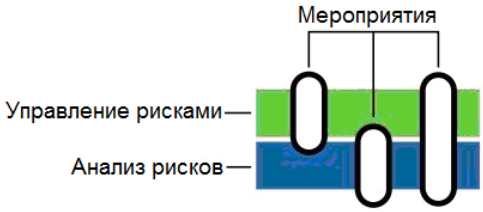


Рис. 2. Структура SAFETAG

Далее происходит идентифицирование сетевых устройств хоста; услуг, которые используются этими устройствами, а также средства защиты этих устройств. Следующий компонент использует разнообразные мероприятия по выявлению возможных атак и сбору справочной информации о способности этих атак поставить под угрозу деятельность организации. Компонент «Оценка устройств пользователя» позволяет аудитору оценить безопасность отдельных устройств сети путем интервью, обзора и осмотра этих устройств. За счет тестирования работы сети против различных онлайн и оффлайн ресурсов, таких как база данных уязвимостей, появляется возможность обнаружить недостатки устройства предприятия. Также аудитор оказывает необходимую помощь, такую как исправление инструментов, консультирование по вопросам будущих проектов. В течение этапа «Физическая оценка» аудитор анализирует потенциальные риски, связанные с физическим доступом, хранением, резервным копированием и шифрованием цифровых данных, а также предлагает новые политики безопасности и практики. Далее определяются сильные и слабые стороны компании к принятию новых методов цифровой и физической безопасности; новые введения, которые организация могла бы принять к сведению после обнаружения уязвимостей. «Дорожная карта развития» представляет собой сортировку рекомендаций в отношении организации, а также угроз и возможностей. Аудитор взвешивает затраты на реализацию этих рекомендаций, а затем создает оптимальную дорожную карту для предприятия. Далее создается отчет, в котором указаны замечания к рекомендациям, а также в нем содержится информация о текущем состоянии безопасности. На этапе «Обработка результатов» аудитор получает обратную связь о своем докладе, а также оценивает успешность процесса с течением времени через постоянные переговоры с компанией.[6]

Заключение. Аудит как средство защиты информации носит сугубо рекомендательный характер, другими словами, эта процедура не привносит изменений в саму систему. Однако анализ полученных данных позволяет говорить о мерах защиты от несанкционированного доступа к конфиденциальным ресурсам. Сканеры безопасности охватывают довольно обширную сферу проблем, поэтому благодаря их использованию можно не только искать уязвимые программы в сети, но и изменять политику безопасности, реагируя на обнаруженные проблемы.[7] При планировании проверки состояния системы информационной безопасности важно не только точно выбрать вид аудита, исходя из потребностей и возможностей компании, но и не ошибиться с выбором исполнителя. Результаты любого вида аудита содержат рекомендации по модернизации системы обеспечения информационной безопасности. Если аудит проводит консалтинговая компания, которая кроме консалтинговой деятельности занимается еще и разработкой собственных систем защиты информации, она, по понятным причинам, заинтересована в том, чтобы результаты аудита рекомендовали организации использовать её продукты. Для того чтобы рекомендации на основе аудита были действительно объективными, необходимо, чтобы компания-аудитор была независима в выборе используемых систем защиты информации и имела большой опыт работы в области информационной безопасности.[9]

СПИСОК ЛИТЕРАТУРЫ

1. Кравчук Д. И., Коркушко Д. А. Аудит безопасности корпоративных информационных систем // Молодой ученый. — 2015. — №10. — С. 697-700.
2. Просянников Р. Виды аудита информационной безопасности // Журнал «Connect!». 2004. №12. [Электронный ресурс]. – Режим доступа: http://www.bre.ru/security/24272.html , свободный, Яз. рус. (дата обращения 07.01.2017)
3. Сетевые сканеры безопасности: возможности, принцип работы и передовые решения. [Электронный ресурс]. – Режим доступа: http://www.kp.ru/guide/setevye-skanery-bezopasnosti.html , свободный. Яз. рус. (дата обращения 26.12.2016)
4. Милосердов А. В., Гриднев Д. А. Тестирование на проникновение с помощью Kali Linux 2.0.: WebWare, 2015. – 348 с.
5. Official page «SystemExperts». [Электронный ресурс] — Режим доступа. — URL: https://systemexperts.com/ , свободный, Англ. яз. (дата обращения 26.12.2016)
6. Official page «SAFETAG». [Электронный ресурс] — Режим доступа. — URL: https://safetag.org/# , свободный, Англ. яз.(дата обращения 26.12.2016)
7. Обзор бесплатных инструментов для аудита web-ресурсов и не только. [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/post/125206/ , свободный. Яз. рус. (дата обращения 26.12.2016)
8. Лучшие инструменты пен-тестера: сканеры безопасности. // Журнал «Хакер». 2010. [Электронный ресурс]. – Режим доступа: https://xakep.ru/2010/04/13/51777/ , свободный. Яз. рус. (дата обращения 26.12.2016)
9. Аудит безопасности: когда и чем проводить? // CNews – Издание о высоких технологиях. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/articles/audit_bezopasnosti_kogda_i_chem_provodit_ , свободный, Яз. рус. (дата обращения 26.12.2016)

КОМПЛЕКСНАЯ СИСТЕМА ИНЖЕНЕРНО ТЕХНИЧЕСКОЙ ЗАЩИТЫ КАБИНЕТА РУКОВОДИТЕЛЯ. ЭФФЕКТИВНОСТЬ РАБОТЫ ПРИБОРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ КОМПЛЕКСНОЙ СИСТЕМЫ ИНЖЕНЕРНО ТЕХНИЧЕСКОЙ ЗАЩИТЫ КАБИНЕТА РУКОВОДИТЕЛЯ

Фаязов Кобилджон Абдукаюмович
Россия, Санкт-Петербург, Университет ИТМО, Кронверкский проспект 49;
email: kobil93@mail.ru

Аннотация: В статье рассмотрены системы защиты информации, также эффективность используемых приборов, различные вопросы инженерно-технической защиты информации также предпринята попытка систематизировать большой объем часто противоречивых сведений по инженерно-технической защите информации.

Ключевые слова: *защита кабинета; руководитель; защита информации; средства защиты.*

INTEGRATED SYSTEM OF ENGINEERING AND TECHNICAL PROTECTION OF THE MANAGER'S OFFICE. THE EFFECTIVENESS OF THE WORK OF INFORMATION SECURITY DEVICES ON THE EXAMPLE OF AN INTEGRATED SYSTEM OF ENGINEERING AND TECHNICAL PROTECTION OF THE MANAGER'S OFFICE

Fayazov Kobiljon Abdukayumovich
Russia, St. Petersburg, University of ITMO, Kronverkskiy prospect 49;
email: kobil93@mail.ru

Abstract: The article considers information security systems, also the efficiency of the devices used, various issues of engineering and technical protection of information, an attempt is also made to systematize a large volume of often contradictory information on engineering and technical protection of information..

Keywords: *protection of the cabinet; leader; data protection; protection devices.*

Введение. Защита информации представляет собой многоцелевую проблему, часть которой еще даже не имеет четкой постановки. Наиболее разработаны вопросы защиты информации, содержащей государственную, коммерческую и прочие тайны.

Система защиты информации, обрабатываемой с использованием технических средств, должна строиться по определенным принципам. Это обусловлено необходимостью противодействия целому ряду угроз безопасности информации.

Основным принципом противодействия угрозам безопасности информации, является превентивность принимаемых мер защиты, так как устранение последствий проявления угроз требует значительных финансовых, временных и материальных затрат.

Принцип системного подхода к построению системы противодействия угрозам безопасности позволяет заложить комплекс мероприятий по защите информации уже на стадии проектирования, обеспечив оптимальное сочетание организационных и технических мер защиты информации. Важность реализации этого принципа основана на том, что дополнение функционирующей незащищенной автоматизированной системы средствами защиты информации сложнее и дороже, чем изначальное проектирование и построение защищенной системы.

Необходимо отметить, что актуальность и значимость проблем, касающихся обеспечения информационной безопасности государства, личности и общества в нашей стране, давно вывели их за узкотехнические рамки, придав им общественно-политическую значимость. Динамично развивается тенденция расширения круга лиц интересующихся вопросами защиты информации, как важного компонента обеспечения их законных прав и демократических свобод.

Рассмотрению различных вопросов инженерно-технической защиты информации посвящен данный дипломный проект. Здесь предпринята попытка систематизировать большой объем часто противоречивых сведений по инженерно-технической защите информации.

Особенностью методических основ инженерно-технической защиты информации является то, что в них рекомендуется объединить практические и лабораторные работы единым сценарием решения сложной практической задачи по защите информации. В качестве примера такого сценария в дипломе рассматриваются методические вопросы защиты информации в одном из наиболее сложных объектов — кабинете руководителя организации.

Технические средства противодействия наблюдению

Основными средствами скрытия объектов наблюдения в оптическом диапазоне являются краски, различные маски и экраны. При выборе красок для маскировочного окрашивания кроме цвета важно учитывать характер изменения коэффициента отражения от длины волны. Чем меньше отличаются коэффициенты отражения краски в видимом и инфракрасном диапазонах волн, тем лучше ее маскирующая способность.

Искусственные оптические маскировочные маски в зависимости ее формы и способа расположения возле объекта делятся на следующие типы:

- маски-навесы;
- вертикальные маски;
- маски перекрытия;
- наклонные маски;
- радиопрозрачные маски.

Маски-навесы предназначены для скрытия объектов, расположенных на открытых сверху площадках и защищают их от наблюдения с помощью средств, размещаемых на верхних этажах высотных зданий, возвышенностях и горах, на самолетах и космических аппаратах.

Вертикальные маски защищают объекты от наблюдения с земли. Маски перекрытия состоят из каркаса и маскировочного покрытия, которые полностью закрывают объект. Они применяются, прежде всего, для защиты объектов, перевозимых на открытых платформах.

Наклонные маски используются в основном для скрытия теней объемных объектов, по длине которых с учетом положения солнца определяют высоту объектов при наблюдении сверху (с самолетов и космических аппаратов).

Радиопрозрачные маски выполняются из радиопрозрачных материалов (стеклопластика, пенопласта и др.), обычно в форме шара, для скрытия демаскирующих признаков и физической защиты антенн.

Для дезинформирующего скрытия применяются кроме деформирующих масок ложные сооружения и конструкции, создающие признаки ложного объекта (объекта прикрытия). Ложные сооружения могут быть плоскими и объемными, функциональными и нефункциональными. Они относятся к наиболее дорогим средствам защиты информации, особенно объемные и функциональные, так как должны воспроизводить полный набор демаскирующих признаков объекта прикрытия в динамике в течение всего периода защиты. Если, например, имитируется объект, на котором работают люди, то они должны убедительно изображать соответствующую деятельность, а не устраивать непрерывные перекуры или греться на солнышке.

Энергетическое скрытие демаскирующих признаков объектов достигается путем уменьшения яркости объекта и фона ниже чувствительности глаза или технического фотоприемника, а также их ослепления. Наиболее естественным способом энергетического скрытия является проведение мероприятий, требующих защиты информации о них, ночью. Яркость объектов, имеющих искусственные источники света, снижается путем их выключения или экранирования светонепроницаемыми шторами и экранами.

Для экранирования объектов наблюдения в помещении применяются шторы, занавески, жалюзи, тонированные стекла и пленки. Эффективные экраны создают жалюзи. По виду материалов жалюзи делятся на тканевые, пластиковые, деревянные и металлические. Лучшие эксплуатационные свойства имеют деревянные и металлические жалюзи. По расположению ламелей жалюзи бывают вертикальные, горизонтальные и рулонные. Технические средства предотвращения утечки информации с помощью закладных подслушивающих устройств. Классификация технических средств обнаружения и локализации закладных устройств приведена на рисунке 1.

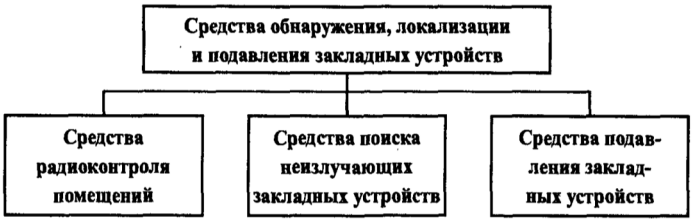


Рисунок 1. Классификация средств обнаружения и локализации закладных устройств.

Средства радиоконтроля помещения предназначены для обнаружения закладных устройств, излучающих радиоволны во время их поиска. Для обнаружения не излучающих при поиске закладок — дистанционно управляемых и передающих сигналы по проводам применяются средства, реагирующие не на радиоизлучения, а на иные демаскирующие признаки закладок. Наконец, средства подавления закладных устройств обеспечивают энергетическое скрытие их сигналов, нарушение работоспособности закладок или их физическое разрушение.

Информационно-техническое сопряжение сканирующих приемников с переносными компьютерами послужило технической основой для создания автоматизированных комплексов для быстрого и надежного поиска радиоизлучающих подслушивающих устройств.

Обнаружитель поля представляет собой широкополосный приемник прямого усиления (в простейшем случае— детекторный) с телескопической штыревой антенной. Усиленные сигналы, превышающие по уровню вручную устанавливаемое пороговое значение, подаются на световой и звуковой индикаторы, информирующие оператора о наличии в месте нахождения антенны электромагнитного поля с мощностью, превышающей пороговое значение. Перед поиском закладки индикатор поля настраивается на уровень фона в обследуемом помещении. С этой целью оператор, находясь в точке помещения на удалении нескольких метров от возможных мест размещения закладок, устанавливает регулятор чувствительности в такое положение, при котором индикатор находится на грани срабатывания. При приближении индикатора поля к излучающей закладке напряженность электромагнитного поля возрастает, повышается уровень сигнала в антенне и, соответственно, на входе индикатора поля. При превышении уровня порогового значения, определяемого положением регулятора чувствительности, индикатор срабатывает, оповещая о появлении в обследуемой зоне электромагнитного поля мощностью, превышающей мощность фона. С целью большей информативности световых индикаторов их выполняют в современных обнаружителях поля в виде линейки из 4-10 светодиодов. Каждый последующий светодиод излучает свет при повышении уровня электромагнитного поля.

Комплекс при минимальном участии оператора определяет и запоминает уровни и частоты радиосигналов в контролируемом помещении, выявляет в результате корреляционной обработки спектрограмм вновь появившиеся излучения, с использованием тестового акустического сигнала распознает скрытно установленные в помещении радиомикрофоны и определяет их координаты. Возможности комплексов расширяют также включением в их состав блока контроля проводных линий, позволяющего обнаруживать подслушивающие устройства, подключенные к проводам кабелей.

В комплект современных автоматизированных комплексов радиомониторинга включают генератор прицельных помех. Он обеспечивает возможность оперативно настраиваться на частоту обнаруженного закладного устройства и подавлять его сигналы в условиях, когда нет времени на поиск и нейтрализацию закладного устройства, например, во время совещания.

С целью сокращения времени просмотра диапазона частот до нескольких минут анализ сигналов в перспективных комплексах проводится на основе быстрого преобразования Фурье.

Создание и применение автоматизированных комплексов для непрерывного радиомониторинга помещений с конфиденциальной информацией является наиболее эффективным направлением развития средств для комплексной защиты информации от утечки по радиоэлектронному каналу.

Средства контроля телефонных линий и цепей электропитания.

Учитывая повсеместное распространение телефонов как средств коммуникаций и повышенный интерес злоумышленников к подслушиванию телефонных разговоров, большое внимание при обеспечении защиты информации уделяется способам и средствам контроля телефонных линий.

Способы контроля телефонных линий основаны на том, что любое подключение к ним вызывает изменение электрических параметров линий и сигналов в них: напряжения и тока в линии, значений емкости и индуктивности линии, активного и реактивного ее сопротивлений. В зависимости от способа подключения подслушивающего устройства к телефонной линии (последовательного — в разрыв провода телефонного кабеля или параллельного) влияние подключаемого подслушивающего устройства может существенно отличаться. Так как закладное устройство использует энергию телефонной линии, величина отбора мощности закладкой из телефонной линии зависит от мощности передатчика закладки и его коэффициента полезного действия.

Для контроля телефонных линий применяются следующие устройства:

– устройства оповещения световым и звуковым сигналом об уменьшении напряжения в телефонной линии, вызванном несанкционированным подключением средств подслушивания к телефонной линии;

– измерители параметров телефонных линий (напряжения, тока, емкостного сопротивления, волнового сопротивления и др.), при отклонении которых от номинального значения формируется сигнал тревоги;

– «кабельные радары», позволяющие выявлять неоднородности телефонной линии и измерять расстояние до неоднородности (асимметрии постоянному току в местах подключения подслушивающих устройств, обрыва, короткого замыкания и др.)

Технические средства предотвращения утечки информации с помощью закладных подслушивающих устройств.

Одной из наиболее сложных задач в области защиты информации является поиск внедренных ЗУ, не использующих радиоканал для передачи информации, а также радиозакладок, находящихся в пассивном (неизлучающем) состоянии. Традиционные средства выявления такие, как панорамные радиоприемники, анализаторы спектра или детекторы поля, в этом случае оказываются неэффективны. Визуальный осмотр также не гарантирует обнаружение подобных ЗУ, так как современные технологии позволяют изготовлять их с любым видом камуфляжа, прятать в элементах строительных конструкций и интерьера. Именно эта проблема и привела к появлению совершенно нового вида поискового прибора, получившего название нелинейного радиолокатора. Это, пожалуй, наиболее уважаемый вид поисковой техники (жаль, что в силу высокой цены не наиболее покупаемый!). Обусловлено это его уникальной способностью обнаруживать любые радиоэлектронные устройства в строительных конструкциях, предметах интерьера и т.д., что делает нелинейные локаторы абсолютно незаменимыми при проведении поисковых мероприятий. Именно к нелинейным локаторам по праву можно отнести утверждение, что российская спецтехника по цене значительно ниже, а по качеству выше, чем зарубежные аналоги.

Профессиональный нелинейный локатор "NR-900V"

Преимущества:

– возможность работы в сложных помеховых условиях, высокая результативность поиска при обследовании капитальных строительных конструкций, режим «идентификация» снижает вероятность ложных обнаружений;

– дополнительный индикатор уровней сигнала, расположенный на антенной системе;

– продолжительное время непрерывной работы без замены источника питания.

Нелинейный локатор "NR-T"

Предназначен для поиска электронных средств связи (СИМ-карт, миниатюрных средств звукозаписи, сотовых телефонов, радиостанций) в местах, где пользование ими запрещено (СИЗО, места лишения свободы) а также для выявления средств связи (сотовых телефонов, радиостанций) и других радиоэлектронных устройств независимо от их функционального состояния «включено/выключено», в сторожевом или ждущем режиме.

Преимущества:

– эффективно обнаруживает малоразмерные цели (СИМ-карты, миниатюрные злектронные устройства)

– повышенная помехоустойчивость к откликам от строительных конструкций и элементов интерьера (контакты МОМ)

– дополнительно усиленные разъемные соединения, дополнительные меры по защите от влаги и коррозии для сложных условий эксплуатации

– облегченная батарея повышенной емкости, встроенная в блок приемопередатчика, продолжительное время непрерывной работы без замены источника питания

– специальный подсумок для размещения аппаратуры на теле оператора

Детектор скрытых видеокамер "WCH-900"

WCH-900 представляет собой детектор камер, передающих изображение в диапазоне от 900 МГц до 2700 МГц. Указанный диапазон является стандартным для радиоканальных камер.

Детектор скрытых камер WCH-900 способен принимать сигнал радиоканальных видеокамер, что позволяет просматривать их изображение, а так же локализовывать их место нахождения. Видео-сканер автоматически сканирует заданный диапазон частот и определяет модуляцию, что позволяет детектору скрытых камер WCH-900 в автоматическом режиме просматривать изображение радиоканальной видеокамеры. Этот прибор обеспечит полную безопасность Ваших встреч или переговоров!

Особенности детектора скрытых камер WCH-900:

– WCH-900 способен автоматически определять протокол передаваемого сигнала.

– Видео-сканер имеет автоматический и ручной режимы настройки прибора.

– Дальность обнаружения равняется дальности передатчика.

– Детектор камер имеет возможность прослушивания акустического сигнала.

– На экране прибора отражена следующая информация: чувствительность антенны, частоты сканирования, заряд АКБ.

– Питание WCH-900 происходит от 4 батарей AA или от сетевого адаптера.

– В видео-сканере имеется возможность скоростного сканирования диапазона 900–2700 МГц.

Автоматизированные Поисковые Комплексы

Для обнаружения, поиска и нейтрализации подслушивающих устройств в последнее время все более широко используются автоматизированные поисковые комплексы. В простейшем случае такие комплексы состоят из стандартного сканирующего приемника, управляющей ПЭВМ и специального программного обеспечения. Наиболее известные на российском рынке системы такого рода комплекс RS1000 и комплексы, построенные на базе ПО SEDIF.

Более сложные комплексы помимо сканирующего приемника (чаще всего модернизированного) имеют в составе ряд дополнительных устройств, расширяющих их функциональные возможности (устройства для проверки проводных коммуникаций, постановщики помех, блоки БПФ и т.п.). В качестве примера таких устройств можно привести семейство комплексов АРК, ДЕЛЬТА, КРОНА. К сожалению, стоит отметить, что цена таких комплексов увеличивается прямо пропорционально количеству используемых в них дополнительных устройств.

В настоящее время наибольший интерес вызывают многофункциональные комплексы типа RS1100 и АРК-Д3, построенные по модульной схеме, на базе которых можно создавать многоканальные системы (до 24 каналов) для одновременного контроля нескольких пространственно разнесенных помещений или всего здания.

– Цифровой Зонд/монитор "СРМ-700" (Акула)

– СРМ-700 — универсальный прибор для обнаружения основных типов электронных устройств негласного съема информации, включая комнатные, телефонные, носимые на теле "жучки" видеопередатчики и звукозаписывающие устройства.

– Многофункциональный поисковый прибор ST 032

Предназначен для проведения мероприятий по обнаружению и локализации специальных технических средств негласного получения информации, для выявления естественных и искусственно созданных каналов утечки информации, а также для контроля качества защиты информации.

Представляет собой модификацию модели ST 031 "ПИРАНЬЯ".

Отличается компактным исполнением и простотой эксплуатации.

СПИСОК ЛИТЕРАТУРЫ

1. Торокин А. А. Инженерно-техническая защита информации. — М.: Гелиос АРВ, 2005.
2. Хорев А. А. Способы и средства защиты информации.— М.: МО РФ, 1998.
3. Волокитин А.В., Маношкин А.П., Солдатенков А.В., Савченко С.А., Петров Ю.А. Информационная безопасность государственных организаций и коммерческих фирм. - Справочное пособие (под общей редакцией Реймана Л.Д.) М: НТЦ «ФИОРД-ИНФО», 2002г.-272с.
4. Бюро научно-технической информации http://www.bnti.ru/
5. Защита информации http://www.sinf.ru/index.htm

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 681.142

ИНСТРУМЕНТАЛЬНОЕ СРЕДСТВО ВИЗУАЛИЗАЦИИ МАРШРУТОВ ВЫПОЛНЕНИЯ КОМПЬЮТЕРНЫХ ПРОГРАММ

Безруков Вячеслав Алексеевич [1], Синещук Юрий Иванович[2] Синещук Максим Юрьевич[3]
[1]Санкт - Петербургский национальный исследовательский университет информационных технологий, механики и оптики
Россия, Санкт-Петербург, Кронверкский пр-т, д. 49
[2]Санкт-Петербургский университет МВД России Россия, Санкт-Петербург, ул. Летчика Пилютова, д. 1
[3]Санкт-Петербургский университет ГПС МЧС России
Россия, г. Санкт-Петербург, Московский просп., 149
emails: bezrukov.1950@mail.ru , sinegal@rambler.ru, smaxim@inbox.ru

Аннотация: Рассмотрена проблема разработки инструментальных средств позволяющих визуализировать маршруты выполнения программ защиты информации.

Ключевые слова: *защита информации, программное обеспечение, сертификация, граф, визуализация.*

THE PROBLEM OF VISUALIZING ROUTES RUN COMPUTER PROGRAMS

Bezrukov Vjacheslav[1], Sineshchuk Yuri[2] Sineshchuk Maxim[3]
[1]Saint - Petersburg national research University of information technologies, mechanics and optics
Russia, St. Petersburg, Kronverksky broad street, 49
[2] Saint-Petersburg University of MIA of Russia
Russia, Saint-Petersburg, letchika Pilyutova Street 1,
[3]Saint-Petersburg university of State fire service of EMERCOM of Russia
Russia, St. Petersburg, Moscow broad street, 149.
emails: bezrukov.1950@mail.ru , sinegal@rambler.ru, smaxim@inbox.ru

Abstract**:** The problem of development of tools allowing you to visualize the routes of program execution of information protection.

Keywords**:** *information security, software certification, graph, visualization..*

Введение. Научно-технический прогресс, создание и глобальное распространение электронных технологий, особенно сети Интернет, стало основной причиной появления и распространения киберугроз. Чтобы обеспечить превосходство над потенциальными противниками(конкурентами), специальные подразделения ищут слабые звенья и уязвимые места в их компьютерных системах.

Для предотвращения кибератак, реализующих соответствующие киберугрозы создаются системы защиты информации (СЗИ), при этом особую актуальность приобретает вопрос обеспечения контроля отсутствия недекларированных возможностей программного обеспечения(ПО) СЗИ. Эта проблема обусловлена большим количеством разработчиков и разнообразием ПО, при разработке которого, зачастую основное внимание уделяется его функциональности, и, в значительно меньшей степени, - его безопасности. Вместе с тем, существующая статистика неумолимо свидетельствует о большом количестве уязвимостей, выявляемых в ПО. Указанные обстоятельства обуславливают необходимость сертификации ПО СЗИ на соответствие требованиям безопасности[1].

Процедура сертификации, как эффективное средство управления безопасностью, предполагает осуществление контроля отсутствия недекларированных возможностей (НДВ). Реализацией недекларированных возможностей, в частности, являются программные закладки, представляющие собою преднамеренно внесенные в ПО функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций ПО, приводящих к нарушению конфиденциальности, доступности или целостности обрабатываемой информации. Отдельные организации(заинтересованные лица), используя эти закладки, смогут осуществлять скрытый мониторинг и съем любой информации и использовать ее по своему усмотрению.

В общем случае, к основным проверкам в системе сертификационных испытаний ПО относятся следующие технологические операции: контроль полноты и отсутствия избыточности исходных текстов; контроль соответствия исходных текстов ПО его объектному коду; контроль связей функциональных объектов по управлению и информации; контроль информационных объектов различных типов; синтаксический контроль наличия заданных конструкций в исходных текстах ПО из списка (базы) потенциально опасных программных конструкций; и т.п. Одним из важных инструментов в этой системе является статический анализ исходных текстов программ, который предполагает формирование перечня маршрутов выполнения функциональных объектов. В качестве функциональных объектов могут выступать процедуры, функции, ветви, операторы и т.п. элемент программы, осуществляющий выполнение действий по реализации законченного фрагмента алгоритма программы.

Маршрут выполнения представляет собой ориентированный граф. Как известно, существует три способа задания графа [2]: аналитический; матричный; геометрический.

Наибольшее распространение получил матричный способ. Матричный способ заключается в задании графа в виде матрицы смежности или матрицы инцидентности и используется при обработке данных вычислительными средствами. В процессе формирования перечня маршрутов, на основании матрицы вызова функциональных объектов, составляется множество всех возможных маршрутов выполнения функциональных объектов и их анализ.

Процедура формирования маршрутов выполнения функциональных объектов и ветвей программного обеспечения средств защиты информации характеризуется высокой сложность, обусловленной большими временными затратами, сложностью аналитической работы эксперта(пользователя), что в ряде случаев делает сертификацию недоступной для разработчиков ПО. Одним из решений, в рамках решения указанной проблемы, может служить снижение требований к автоматизированному рабочему месту эксперта(пользователя) за счет возможности взаимодействия с результатом визуализации маршрутов.

Визуализация графов представляет собой отдельную дисциплину на стыке теоретической информатики и математики. Данная дисциплина получила широкое развитие в силу разнообразия областей практического применения[3], [4], [5].

Из различных видов алгоритмов иерархический, или поуровневый, способ изображения является наиболее широко используемым для отслеживания порядка выполнения функциональных объектов и ветвей при анализе программного обеспечения.

Традиционный метод Сугиямы предполагает наличие четырех этапов [3]: удаление циклов; разбиение на слои; минимизация пересечений ребер; назначение x-координат.

В оригинале метод Сугиямы предполагал работу с ациклическими графами, поэтому удаление циклов рассматривается в качестве этапа предварительной подготовки [9]. Для ориентированного графа понятие ацикличности отлично от неориентированного: орграф может иметь неориентированные циклы и при этом быть ацикличным.

Проблема построения наибольшего подграфа без циклов чаще всего формулируется как проблема поиска наименьшего множества ребер обратной связи, или FAS.

Разбиение на слои – следующий этап алгоритма Сугиямы, который на выходе присваивает каждой вершине графа дополнительный параметр – уровень.

Минимизация пересечений ребер. По результатам предыдущего этапа сформирован граф, который с немалой вероятностью обладает большим количеством пересечений. Пересечения не несут полезной информационной нагрузки, при этом затрудняя восприятие пользователем изображения. Это обусловливает необходимость минимизации пересечений.

Основным фактором наличия пересечений выступают относительные позиции вершин [6], поэтому минимизация пересечений ребер признается комбинаторной проблемой, которая сводится к нахождению такого упорядочения вершин, что число пересечений между слоями становится минимальным. Существует множество методов минимизации пересечений. Наиболее простыми методами считаются метод барицентров и метод медиан.

Назначение координат. После того, как относительный порядок вершин определен, остается найти абсолютные координаты вершин и построить изображения ребер[3]. Задача вычисления координат вершин решается либо с помощью оптимизации некоторой целевой функции при заданных ограничениях, либо методами итеративного улучшения имеющегося размещения.

Архитектуры программного комплекса, реализующего поставленную задачу отражает два этапа формирования изображения графа: присваивания координат и вывод полученной укладки (Рисунок 1).

Передача данных на модуль формирования укладки графа осуществляется через модуль получения и обработки входных данных, или результатов анализа. Данное разделение позволяет унифицировать входной формат для модуля формирования укладки при изменении характера данных, подлежащих визуализации, на стороне анализатора.

На сторону конечного пользователя подается результат работы модуля формирования укладки графа, представляющий собой сериализованный объект, содержащий информацию о вершинах графа (функциональных объектах или ветвях) и их связях, а также координаты вершин.

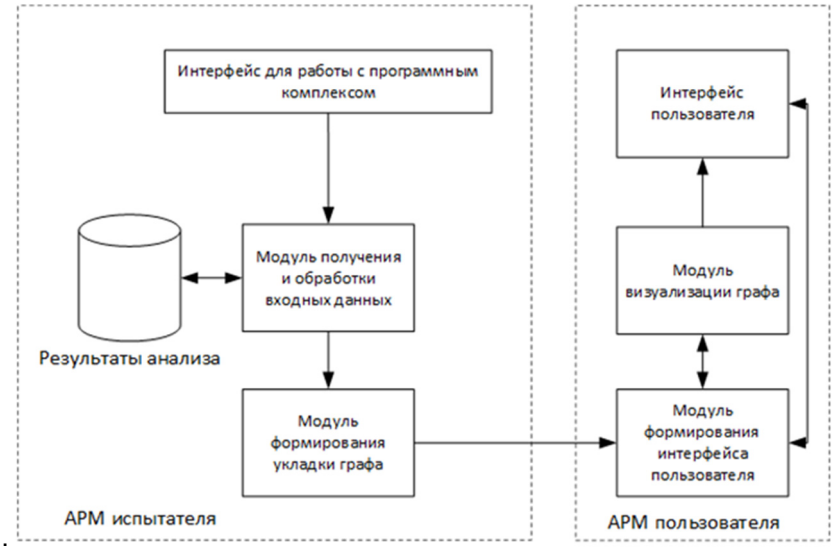


Рис. 1. Архитектура программного комплекса

Модуль формирования интерфейса, получая на вход сериализованный объект, передает его модулю визуализации, который создает окончательное изображение, являющееся частью графического интерфейса; другая часть графического интерфейса, несущая регулирующую функцию, формируется с помощью этого же модуля.

Модуль получения и обработки входных данных:

– обрабатывает информацию, переданную при помощи прикладных программных интерфейсов от анализатора;

– осуществляет соединение с хранилищем данных, содержащим результаты работы анализатора;

– запрашивает и получает данные о функциональных объектах и ветвях программного обеспечения средств защиты информации;

– преобразует полученные данные в единый формат, пригодный для работы модуля формирования укладки графа.

Модуль формирования укладки графа:

– осуществляет анализ поступивших данных о вершинах и ребрах графа;

– производит преобразование графа посредством добавления координат к каждой вершине, обозначающей функциональный объект или ветвь программного обеспечения, в соответствии с методом Сугиямы;

– экспортирует полученный граф в сериализованный объект, пригодный для дальнейшей обработки модулем формирования интерфейса пользователя.

Модуль формирования интерфейса пользователя:

– принимает и при необходимости обрабатывает сериализованный объект, полученный в результате работы модуля формирования укладки графа, для последующей передачи модулю визуализации графа;

– получает от графического интерфейса пользователя сигналы о виде взаимодействия с графом и отправляет их модулю визуализации графа;

– осуществляет первичную обработку полученного сигнала и формирует параметры для взаимодействия с модулем визуализации графа.

Модуль визуализации графа:

– формирует изображение графа вызовов;

– принимает команды от модуля формирования интерфейса пользователя;

– изменяет изображение графа в соответствии с командами пользователя.

Разработка программного комплекса велась на языках Python 3.4 и JavaScript. В качестве тестового примера была выбрана программа fbReader, исходные тексты которой находятся в открытом доступе. В программе было насчитано более восьми тысяч функциональных объектов.

На рисунке 2 представлен общий вид результата работы программного комплекса. Вершинами являются функциональные объекты, ребра представляют связи между ними. Информация о функциональном объекте представлена на рисунке 3. Подсвеченные вершины имеют непосредственную связь с искомым функциональным объектом. При исследовании исходных кодов программного обеспечения перед испытателем зачастую возникает задача выяснения наличия связи между двумя функциональными объектами. С помощью программного комплекса удается выяснить наличие подобной связи и вывести маршрут выполнения, что показано на рисунке 4

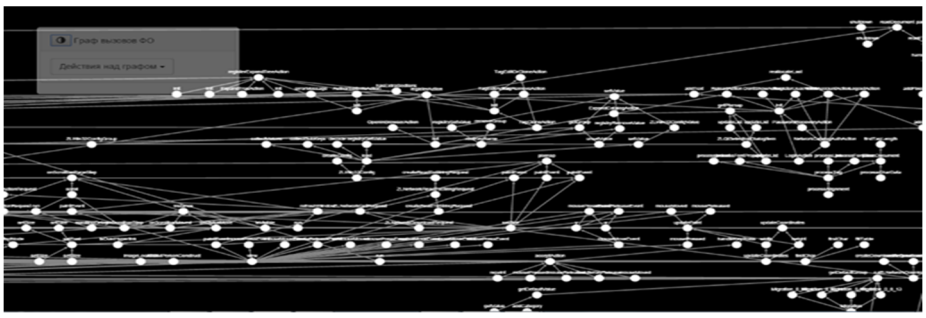


Рис. 2. Граф вызовов функциональных объектов, увеличенный

Рис. 3. Информация о функциональном объекте

Рис. 4. Маршрут между заданными функциями

Заключение. Задача уменьшения требований к автоматизированному рабочему месту эксперта при сохранении возможности взаимодействия с результатом визуализации решена благодаря архитектурному разделению программного комплекса на две компоненты, первая из которых формирует укладку графа и передает её в виде сериализованного объекта, а вторая выполняется независимо от первой, принимает на вход укладку графа и формирует средствами браузера искомое изображение, а также обеспечивает возможность взаимодействия пользователя с графом.

СПИСОК ЛИТЕРАТУРЫ

1. Беляков И. А., Еремеев М. А. Применение интеллектуальных технологий в процессе сертификации программного обеспечения // Молодой ученый. — 2011. — №11. Т.1. — С. 23-31.
2. Graph Drawing [Electronic resource] // Graph Drawing Symposium [Official website]. URL: http://www.graphdrawing.org/
3. K. Sugiyama, S. Tagawa, M. Toda. Methods for visual understanding of hierarchical system structures [Text] // IEEE Transactions on Systems, Man, and Cybernetics, - SMC-11: 1981. - 2.
4. Documentation [Electronic resource] // Graphviz – Graph Visualization Software [Офиц. сайт]. Режим доступа: http://www.graphviz.org/Documentation.php
5. З.В. Апанович. Методы визуализации информации при помощи графов. Часть 2. Методы визуализации ориентированных и неориентированных графов [Электронный учебник] // Электронная образовательная среда НГУ [Офиц. сайт]. Режим доступа: http://193.124.209.204/?db=book_apanovich2&int=VIEW&class=ROOT&templ=VIEW
6. A. Shabbeer. Crossing Minimization within Graph Embeddings [Text] / A. Shabbeer, C. Ozcaglar, K. P. Bennett. – Cornell University: 2012.

УДК 004.05

ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ СВЯЗИ

Вилков Валерий Борисович[1], Сычев Сергей Евгеньевичвич[2], Черных Андрей Климентьевич[2]
[1] Военная академия материально-технического обеспечения им. генерала армии А.В. Хрулёва,
Россия, Санкт-Петербург, наб. Макарова, д. 8,
[2] Санкт-Петербургский военный институт войск национальной гвардии Российской Федерации,
Россия, Санкт-Петербург, ул. Лётчика Пилютова, д. 1,
emails: amirusha@rambler.ru, s75sichev@mail.ru

Аннотация: В статье рассматривается подход к созданию систем связи, в максимальной степени обеспечивающих информационную безопасность обрабатываемых в их рамках данных. Предложен оптимальный алгоритм, реализующий указанный подход, который проиллюстрирован примером. Приведены постановки задачи, реализующей создание указанных систем связи, основанные на идеях многокритериальной оптимизации.

Ключевые слова: *информационная безопасность системы, надежность системы связи, теория нечетких множеств, нечеткая логика, максимальный остов.*

QUESTIONS OF INFORMATION SAFETY OF SYSTEMS OF COMMUNICATION

Vilkov Valeriy[1], Sychev Sergey[2], Chernykh Andrey[2]
[1] Military academy of logistics behalf of the army general A. V. Khrulyov,
Russia, St.-Petersburg, nabereznaya Makarova, 8,
[2] St.-Petersburg institutes of armies of national guards of Russian Federation,
Russia, St.-Petersburg, Pilot Pilutova str. 1,
emails: amirusha@rambler.ru, s75sichev@mail.ru

Abstract: In clause the approach to creation of systems of communication, in the maximal degree of the processable data, ensuring information safety in their frameworks is considered(examined). The optimum algorithm realizing specified approach is offered which is illustrated with an example. The statements of the task realizing creation of the specified systems of communication, based on ideas multicriterions of optimization are given.

Keywords: *information safety of system, reliability of system of communication(connection), theory of indistinct sets, indistinct logic, maximal skeleton.*

Введение. В статье рассматривается задача по созданию наиболее эффективной, по критерию информационной безопасности (в дальнейшем надежной), системы связи. Эта задача является модификацией известной задачи о кратчайшем соединении [1], [2], [3], [4]. Отличие состоит в том, что в качестве характеристики канала связи используется не его стоимость, а его надежность (информационная безопасность), для чего привлекается теория нечетких множеств и нечеткая логика [5], [6], [7], [8], [9], [10], [11], [12], [13].

Отметим, что с помощью этой задачи Росси, Хайзер и Кинг предложили схему прокладки телевизионных кабелей, соединяющих все станции в единую сеть [14]. Кроме того предложенная задача актуальна и в ряде других случаев, когда требуется связать определенные узлы (пункты) с наименьшей затратой сил и средств, то есть построить минимальную сеть. В [15] рассмотрен пример, в котором в качестве характеристики канала связи используется вероятность утери информации при его использовании. В литературе отмечается, что некоторые задачи приводят к необходимости построить сеть не минимального, а максимального веса. К этой задаче также применим алгоритм Краскала, если изменить знак веса каждого ребра на противоположный. Если требуется найти сеть с минимальным произведением весов ребер, то, учитывая, что log(ab) = log(a) + log(b), минимальное остовное дерево графа, в котором веса ребер заменены их логарифмами, дает нужное решение. Правда, вес ребер обязательно должен быть положительным.

Дадим формулировку рассматриваемой задачи на языке теории графов [2] [3]. Ребро, которому соотнесено некоторое число (длина, вес, пропускная способность, надежность и т.п.), будем называть взвешенным. Граф, все ребра которого взвешенные, будем называть взвешенным. Назовём остовом связного графа G подграф, представляющий собой дерево и содержащий все вершины графа G. Требуется найти самый надежный остов.

Сформулированная задача особенно актуальна при создании сетей связи, когда важно минимизировать доступ хакеров к информации в них циркулирующей.

Под надежностью канала связи естественно понимать то, насколько мы уверены в безопасности его использования в ходе информационного обмена. В качестве показателя надежности канала связи можно использовать вероятность того, что никаких отрицательных последствий из-за воздействия на него со стороны хакеров, природных и техногенных катаклизмов в ходе информационного обмена не будет. Но здесь возникает серьезный вопрос – откуда взять эти вероятности, особенно, если параметры функционирования канала связи конфиденциальные, что вполне естественно. К тому же

даже, если эти вероятности известны, остается достаточно сложная технически задача по определению оптимального варианта использования всей сети связи.

Мы предлагаем для определения надежности каналов связи и всей сети связи использовать теорию нечетких множеств. Напомним необходимые для дальнейшего понятия этой теории.

Понятие нечеткого множества – эта попытка математической формализации нечеткой информации для построения математических моделей. В основе этого понятия лежит представление о том, что составляющие данное множество элементы, обладающие общим свойством, могут обладать этим свойством в различной мере и, следовательно, принадлежать к данному множеству с различной степенью. При таком подходе, говоря о том, что некоторый элемент принадлежит данному множеству, необходимо указать с какой степенью этот элемент удовлетворяет свойствам данного множества.

Нечетким множеством $\hat{A}$ на универсальном множестве U называется совокупность пар $(\mu_{\hat{A}}(u), u)$, где $\mu_{\hat{A}}(u)$ - степень принадлежности элемента $u \in U$ к нечеткому множеству U. Функция $\mu_{\hat{A}}(u)$ называется функцией принадлежности нечеткого множества $\hat{A}$, $\mu_{\hat{A}}(u)$ выражает степень принадлежности элемента $u \in U$ к нечеткому множеству $\hat{A}$. Степень принадлежности - это число из отрезка [0, b]. Чем выше степень принадлежности, тем в большей мере элемент универсального множества соответствует свойствам нечеткого множества, тем с большей надежностью мы можем утверждать, что он является элементом этого множества.

Как правило, предполагается, что функция принадлежности принимает значения из отрезка [0, 1]. Вопросы, связанные с определением вида функции принадлежности и их построения, изучаются, например, в [10] [16].

В дальнейшем мы часто вместо словосочетания «значение функции принадлежности» будем использовать словосочетания «степень принадлежности», «информационная безопасность», «надежность».

Определения нечетких теоретико-множественных операций объединения, пересечения и других могут быть обобщены из обычной теории множеств. Приведем определения нечетких теоретико-множественных операций пересечения и объединения, предложенные Л. Заде.

Пересечением нечетких множеств $\hat{A}$ и $\hat{B}$, заданных на U, называется нечеткое множество $\hat{C} = \hat{A} \cap \hat{B}$ с функцией принадлежности

$$\mu_{\hat{C}}(u) = min\{\mu_{\hat{A}}(u), \mu_{\hat{B}}(u)\} \quad (1)$$

для всех $u \in U$ (см. рисунок1).

Операция нахождения минимума также обозначается знаком ∧, т.е.

$\mu_{\hat{C}}(u) = \mu_{\hat{A}}(u) \wedge \mu_{\hat{B}}(u)$.

Объединением нечетких множеств $\hat{A}$ и $\hat{B}$ заданных на U называется нечеткое множество $\hat{D} = \hat{A} \cup \hat{B}$ с функцией принадлежности

$$\mu_{\hat{D}}(u) = \max\{\mu_{\hat{A}}(u), \mu_{\hat{B}}(u)\} \quad (2)$$

для всех $u \in U$ (см. рисунок 2).

Операция нахождения максимума также обозначается знаком ∨, т.е. $\mu_{\hat{D}}(u) = \mu_{\hat{A}}(u) \vee \mu_{\hat{B}}(u)$.

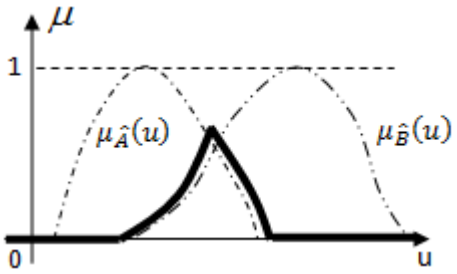


Рис.1. Пересечение нечетких множеств

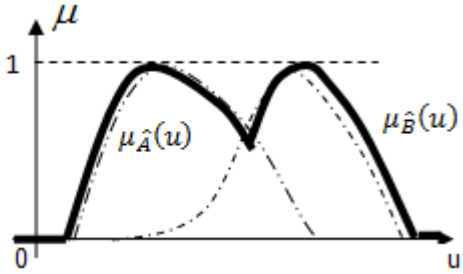


Рис. 2. Объединение нечетких множеств

Нечеткие множества в случае, когда универсальным множеством является числовая ось, принято называть нечеткими величинами. Нечеткая величина, функция принадлежности которой непрерывна и имеет единственный максимум, называется нечетким числом.

Следуя [17], [18], [19], введем некоторые понятия нечеткой логики. В классической математической логике значениями истинности высказываний могут быть только два значения – «истина» и «ложь», при этом значению «истина» соответствует число 1, значению «ложь» - число 0. В нечеткой логике рассматриваются нечеткие высказывания, которые могут быть истинными или ложными в какой-то степени. Степень истинности нечеткого высказывания принимает значения из замкнутого промежутка $[0; 1]$, при этом 0 совпадает со значением «ложь», 1 – со значением «истина».

Степень истинности нечеткого высказывания $\hat{F}$ обозначим через $\mu(\hat{F})$.

Над нечеткими высказываниями вводятся различные логические операции, остановимся на двух из них: конъюнкции и дизъюнкции.

Рассмотрим два нечетких высказывания $\tilde{A}$ и $\tilde{B}$. Нечеткие логические операции И ($\wedge$) и ИЛИ ($\vee$) по аналогии с теоретико-множественными операциями объединения и пересечения выполняются по правилам:

$$\mu(\tilde{A} \wedge \tilde{B}) = min\{\mu(\tilde{A}), \mu(\tilde{B})\}, \quad (3)$$

$$\mu(\tilde{A} \vee \tilde{B}) = max\{\mu(\tilde{A}), \mu(\tilde{B})\}. \quad (4)$$

Под надежностью канала связи будем понимать степень истинности нечеткого высказывания «канал связи надежен». Предполагается, что этот показатель известен для любого из каналов связи, который можно создать. В силу определения конъюнкции нечетких высказываний (формула (3)) надежность (степень истинности) сети равна минимальной из надежностей (степеней истинности) каналов связи, входящих в эту сеть.

Итак, пусть дан связный взвешенный граф $G = (E, V)$, его ребра соответствуют каналам связи, каждому из них соотнесено число - степень истинности нечеткого высказывания «канал связи надежен».

Требуется найти остов этого графа, для которого степень истинности нечеткого высказывания «все каналы связи надежны» максимальна.

Решать задачу будем, используя модифицированный алгоритм Крускала, заменив в нем только критерий присоединения очередного ребра к уже построенному (перспективному) множеству ребер, и искать будем не минимальный, а максимальный остов (остов максимального веса). Обозначать максимальный остов будем МакО.

Для рассматриваемого случая имеют место теоремы 1 и 2.

Теорема 1. Среди решений задачи о самой надежном подграфе, содержащем все ребра рассматриваемого графа имеется остов.

Доказательство. Предположим противное, т.е. что подграф, являющийся решением задачи (соединяющий все вершины рассматриваемого графа и имеющий максимальный вес), не является деревом. Тогда в нем существует цикл. Убрав произвольный канал связи этого цикла, мы получим подграф, содержащий все вершины, но не меньшего веса. Если полученный подграф является деревом, то мы получили требуемый остов, в противном случае в этом подграфе имеется цикл, убирая в нем произвольное ребро, получим новый подграф не меньшего веса и т.д. В силу конечности числа ребер в исходном графе, мы, в конце концов, получим требуемый остов. Теорема доказана.

Изменяя с учетом рассматриваемого понятия «веса» алгоритм Краскала, получаем следующий алгоритм.

Пусть дан связный граф $G = (V, E)$, имеющий n вершин и m ребер, пусть для любого ребра $e \in E$ определен его вес $d(e)$ (его надежность).

Начинаем с графа $G_0 = (V, \emptyset)$, который состоит только из вершин графа $G = (V, E)$ и не имеет ребер. Этот граф можно рассматривать как n компонент связности, каждая из которых состоит из одной вершины.

В дальнейшем алгоритм состоит из последовательности этапов. На этапе с номером k $(k = 1,2, \dots, n-1)$ строится граф $G_k = (V, T_k)$, для этого к множеству ребер T_{k-1} графа G_{k-1} добавляется одно ребро, которое выбирается по следующему правилу:

– в графе $G = (V, E)$ выбираем ребро максимального веса из числа ребер, не принадлежащих T_{k-1};

– если добавление этого ребра к T_{k-1} не приводит к образованию цикла, то присоединяем это ребро к T_{k-1}, получаем T_k и граф $G_k = (V, T_k)$;

– если цикл образуется, то из оставшихся ребер графа $G = (V, E)$ не принадлежащих T_{k-1}, выбираем ребро максимального веса и т.д.

Граф G_{n-1} является остовом графа G максимального веса.

Теорема 2. Изложенный алгоритм дает МакО. (Для классической постановки см. [4]).

Доказательство. Покажем сначала, что при $0 < i < n-1$ граф G_i можно построить. Действительно, рассмотрим множества ребер T_{i-1} и $E \backslash T_{i-1}$. В силу связности графа G найдется такое ребро (k, l), что $k \in T_{i-1}$ и $l \in E \backslash T_{i-1}$. Это ребро не образует цикла с ребрами из T_{i-1}. Выбрав из всех таких ребер ребро с максимальным весом, получим ребро, присоединение которого к T_{i-1} даст T_i.

Докажем теперь, что T_{n-1} является остовом максимального веса в графе G.

Рассмотрим граф G_{n-1} с множеством ребер T_{n-1}. Так как он связный, состоит из n вершин, $n-1$ ребра и не имеет циклов, то он является деревом (см. [20]). Покажем, что вес дерева G_{n-1} максимален.

Предположим, что это не так. Среди всех остовов графа G, имеющих максимальный вес, выберем такой остов с множеством ребер T, который имеет с T_{n-1} максимальное число общих ребер.

Пусть $e_i = (a, b)$ - ребро из T_{n-1}, не содержащееся в T и имеющее минимальный номер среди ребер множества T_{n-1}, не входящих в T. (Предполагается, что ребра в множестве T_{n-1} получили номера в процессе его построения, в порядке их присоединения к строящемуся графу). В множестве T есть простая цепь, соединяющая вершины a и b, присоединив к ней ребро e_i, получим цикл. В этом цикле есть ребро e, не входящее в T_{n-1}. Заменив в T ребро e на e_i, получим новый остов $\hat{T} = T \backslash \{e\} \cup \{e_i\}$. Но

T - остов максимального веса, следовательно, вес $\grave{T}$ не больше веса T. Отсюда следует, что ребро e_i весит не больше ребра e.

С другой стороны, присоединяя ребро e к T_{i-1} (при $i = 1$ полагаем $T_{i-1} = \emptyset$), мы не получим цикла, поскольку ребра $e_1, e_2, \dots, e_{i-1}, e$ входят в множество T. Если бы вес ребра e был больше веса ребра e_i, то при построении дерева T_i мы взяли бы не e_i, а e (или другое ребро с весом большим веса e_i). Следовательно, вес ребра e_i равен весу ребра e, и веса деревьев с множествами ребер T и $\grave{T}$ одинаковые.

Итак, $\grave{T}$ - остов максимального веса. Число ребер, общих для множеств $\grave{T}$ и T, больше, чем число общих ребер для T_{n-1} и T ($\acute{T} = T\backslash\{e\} \cup \{e_i\}$), что противоречит выбору множества T. Полученное противоречие доказывает теорему.

Проиллюстрируем предложенные теоретические положения примером.

Возможные линии связи представлены в виде графа G на рисунке 3. Рядом с ребрами, изображающими линии связи, указаны надежности этих линий (например, степень нашей уверенности в том, что при передаче информации по данной линии несанкционированного доступа к информации не будет). Основным источником информации (пунктом выдачи директивных указаний) является пункт 1, т. е. необходимо передавать сообщения из пункта 1 во все остальные пункты. Определить какие каналы связи необходимо создать, чтобы надежность передачи информации без нарушения её конфиденциальности в рамках этой системы связи была бы максимальной.

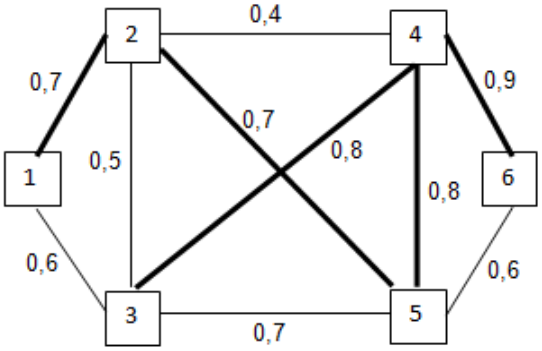


Рис. 3. Граф, на котором указаны все возможные каналы связи

Определим $\mathrm{G}_0 = (\emptyset, \mathrm{V}), \mathrm{V} = \{1,2,3,4\}$. Перечислим ребра, из которых состоит МакО, указав их в том порядке, в котором они присоединялись к создаваемому остову:

$$(4,6), (3,4), (4,5), (2,5), (1,2).$$

Это остов максимальной надежности, его показатель надежности равен 0,7.

Заметим, что порядок построения остова мог быть и другим. Отметим также, что присоединение ребра $(3,5)$ вместо, скажем, $(2,5)$ невозможно, так как ребра $(3,5), (3,4), (4,5)$ образуют цикл.

Усложним немного формулировку рассмотренной задачи, будем учитывать не только показатель надежности канала связи, но и стоимость его создания. Пусть каждому ребру графа $G = (E, V)$ соотнесена степень истинности высказывания «канал связи надежен» (надежность) и значение стоимости его создания (стоимость). Рассмотрим в связи со сказанным две задачи.

1. Построить максимально надежный остов при условии, что его стоимость не должна быть больше S.

Эту задачу можно решать, последовательно исключая из исходного графа ребра минимальной надежности.

Решение начинается с рассмотрения исходного графа, для которого строится остов минимальной стоимости. Пусть его стоимость меньше S и его надежность равна r_1. Удаляем из исходного графа каналы связи, надежность которых не превосходит r_1. Для получившегося графа опять строим остов минимальной стоимости. Стоимость и надежность получившегося остова будет не меньше, чем остова, полученного ранее. Пусть его надежность равна r_2. Удаляем из исходного графа каналы связи, надежность которых не превосходит r_2 и т.д. пока не получим остов стоимостью больше S или граф, не содержащий все вершины исходного.

2. Построить остов минимальной стоимости при условии, что его надежность должна быть не меньше R.

Для решения этой задачи уберем из исходного графа каналы связи, надежность которых меньше R, и построим остов минимальной стоимости для полученного графа. Если при этом мы получим граф, который содержит не все вершины исходного, то, значит, сформулированная задача не имеет решения.

Заключение. В качестве заключения отметим, что в статье предложен легко программируемый алгоритм создания системы связи, в максимальной степени обеспечивающей информационную безопасность, реализуемого в её рамках информационного обмена.

СПИСОК ЛИТЕРАТУРЫ

1. Белоусов А. И., Ткачев С. Б. Дискретная математика. – М., 2006. – 744 с.
2. Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К. Минимальные остовные деревья // Алгоритмы: построение и анализ / Под ред. И. В. Красикова. 2-е изд. – М., 2005. – 1296 с.
3. Таха Т. Введение в исследование операций. – М.: Вильямс, 2005. – 912 с.
4. Kruskal B. On the Shortest Spanning Subtree of a Graph and the Travelimg Salesman Problem. – Proc. AMS. 1956. Vol 7, No. 1.
5. Черных А. К., Вилков В. Б. Управление безопасностью транспортных перевозок при организации материального обеспечения сил и средств МЧС России в условиях чрезвычайной ситуации //Пожаровзрывобезопасность. 2016. Т. 25. № 9. С. 52-59.
1. DOI: 10.18322/PVB.2016.25.09.52-59.
6. Вилков В. Б., Черных А. К., Гарькушев А. Ю., Зайцев А. И. Алгоритм поиска оптимального маршрута выдвижения подразделения войск национальной гвардии // Известия Российской академии ракетных и артиллерийских наук. 2017. № 1 (96). С. 29-33.
7. Вилков В. Б., Черных А. К., Флегонтов А. В. Теория и практика оптимизации решений на основе нечетких множеств и нечёткой логики. – СПб.: Изд. РГПУ им. А.И. Герцена, 2017. – 160 с.
8. Заде Л. Понятие лингвистической переменной и его применение к принятию приближенных решений. – М., 1976. – 166 с.
9. Кофман А. Введение в теорию нечетких множеств. – М.: Радио и связь,1982. – 429 с.
10. Леоненков А. В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. – СПб.: БХВ-Петербург, 2005. – 725 с.
11. Орловский С. А. Проблемы принятия решений при нечеткой исходной информации. – М., 1981. – 206 с.
12. Яхъяева Г. Э. Нечеткие множества и нейронные сети. – М.: Бином, 2006. – 315 с.
13. Zadeh L. Fuzzy sets // Information and Control. –1965. – № 8. P. 338-353.
14. D. Rossi J. A., Heiser R. S., King N. S. A Cost Analysis of Minimum Gistance NV Networking for Broadcasting Medical Information. – RM-6204-HLM RAND Corp. Santa Monica. Calif., February 1970.
15. Кристофидес Н. Теория графов. Алгоритмический подход. – М.: Мир, 1978. – 432 с.
16. Борисов А.Н., Крумберг О.А., Федоров И.П. Принятие решений на основе нечетких моделей: Примеры использования. – Рига: Зинатне, 1990. – 184 с.
17. Заде Л. Понятие лингвистической переменной и его применение к принятию приближенных решений. – М.: Мир, 1976. – 166 с.
18. Тэрано Т., Асаи К., Сугэно М. Прикладные нечеткие системы. – М.: Мир, 1993. – 368 с.
19. Штовба С.Д. Введение в теорию нечетких множеств и нечеткую логику. – Винница: УНИВЕРСУМ-Винница, 2001. – 71 с.
20. Емеличев В.А., Мельников О.И., Сарванов В.И., Тышкевич Р.И. Лекции по теории графов. – М.: Наука. Гл. ред. физ.-мат. лит., 1990. – 384 с.

УДК 004.056.5

О СОЦИАЛЬНЫХ СЕТЯХ ВУЗОВ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кононов Олег Александрович, Кононова Ольга Васильевна
Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Россия, Санкт-Петербург, ул. Большая Морская, д. 67,
emails: o2kon@mail.ru

Аннотация: В статье рассмотрены актуальные вопросы использования социальных сетей в образовательной области.

Ключевые слова: *социальные сети; информационно-коммуникационные технологии; информационная безопасность, образовательная среда.*

ABOUT SOCIAL NETWORKS OF UNIVERSITIES AND INFORMATION SECURITY

Oleg Kononov, Olga Kononova
Saint-Petersburg State University of Aerospace Instrumentation,
Russia, Saint-Petersburg, Bolshaya Morskaya street 67,
emails: o2kon@mail.ru

Abstract: In article topical issues of using social networks in the educational sphere are considered.

Keywords: *social networks; information and communication technologies; information security, educational sphere.*

Введение. Сегодня для многих социальные сети являются основным местом проведения времени в Интернете, так как 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.

Активные пользователи и целевая аудитория. На сегодняшний день в мире существует множество социальных сетей от мега популярных и до совершенно неизвестных, в мире в целом насчитывается социальных сетей около пятисот. Одни сети развиваются, другие наоборот сокращают свою деятельность, есть социальные сети тематические, а есть просто для общения, выбор очень и очень велик.

Однако, нужно заметить, что лишь небольшая часть из них является международными. Всего таковых около 10 штук. К ним относятся, например, FaceBook, ВКонтакте, LinkedIn, Живой журнал и

другие. В большинстве стран есть собственные социальные сети, такие, например, как российские Одноклассники.

Самые популярные социальные сети в мире по количеству активных пользователей в месяц в 2017 году приведены на рис.1 [1].

По данным на апрель 2017 года самой популярной социальной сетью в мире остается Facebook. Ее ежемесячная аудитория составляет почти 2 млрд. человек (точнее — 1968 млн.).

Вторую строчку рейтинга по популярности занимает система мгновенного обмена текстовыми сообщениями WhatsApp — 1200 млн. На третьей позиции располагается видеохостинг YouTube — 1000 млн. Однако такие же результаты продемонстрировал и Facebook Messenger — 1000 млн.

Далее по популярности идут социальные сети: WeChat (мобильная коммуникационная система для передачи текстовых и голосовых сообщений) — 889 млн., QQ (популярнейший китайский сервис мгновенного обмена сообщениями) — 868 млн., Instagram — 600 млн., QZone (крупнейшая в Китае социальная сеть) — 595 млн., Tumblr — 550 млн., Twitter — 319 млн. Так выглядит первая десятка самых популярных социальных сетей в мире в 2017 году.

Но помимо перечисленных в мире есть и другие сайты и приложения социальных сетей: Sina Weibo — 313 млн., Baidu Tieba — 300 млн., Snapchat — 300 млн., Skype — 300 млн., Viber — 260 млн., LINE — 220 млн., Pinterest — 150 млн., YY — 122 млн., LinkedIn — 106 млн., Telegram — 100 млн., BBM — 100 млн., VKontakte — 95, Kakaotalk — 49 млн. [1].

Как видно, среди популярных систем есть не только традиционные социальные сети, но и различные приложения и сервисы по обмену сообщениями. Самые крупные из них по-прежнему американские. Но в последнее время все популярнее становятся китайские социальные сети.

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.

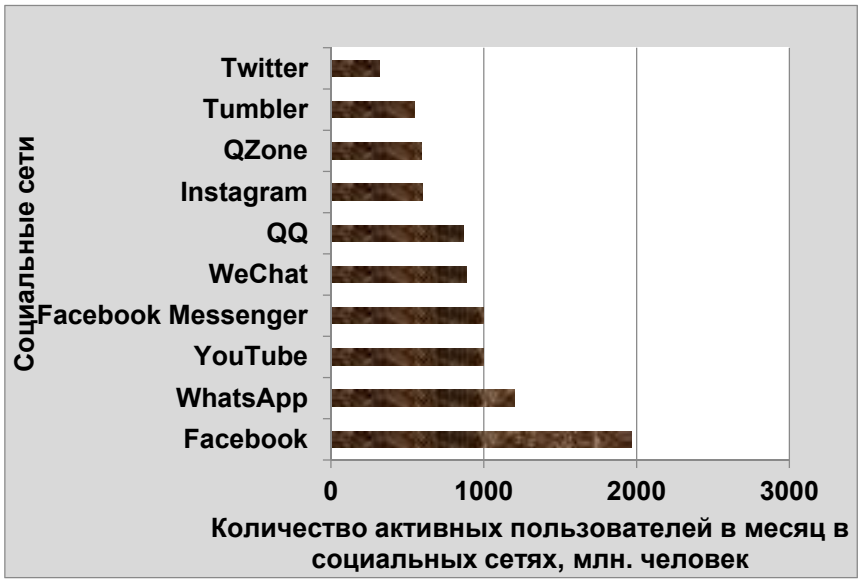


Рис 1. Количество активных пользователей в социальных сетях в месяц в 2017 году, млн. человек

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. Данная аудитория довольно обширна, и этот факт открывает огромные перспективы для рекламы и продвижения разного рода проектов именно в социальных сетях (рис. 2) [1].

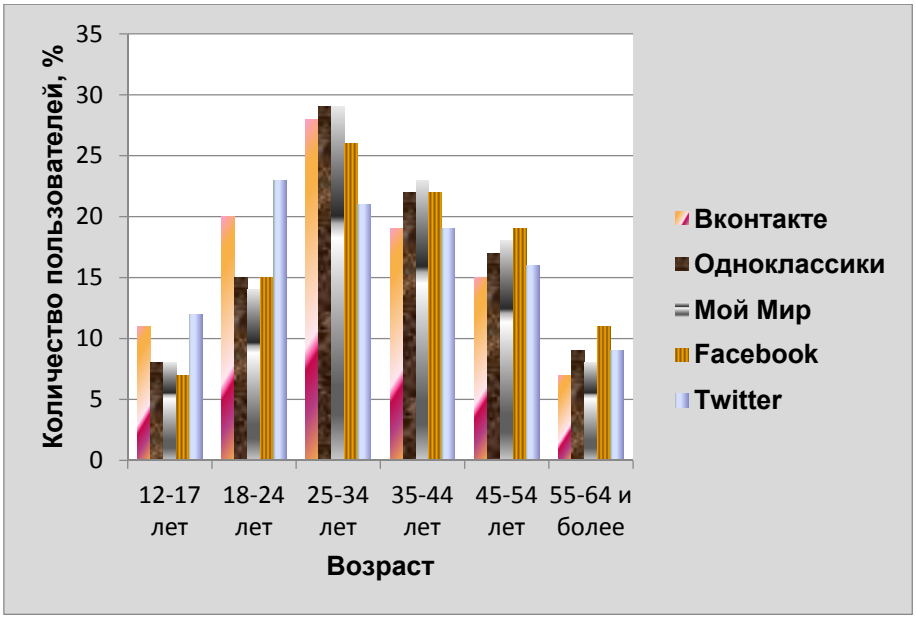


Рис. 2. Количество пользователей социальных сетей разного возраста

Социальная среда вуза. Сегодня создание социальной среды в вузе, мотивирующей сотрудников и студентов на постоянный рост собственных знаний и постоянное совершенствование процессов получения и закрепления новых знаний, является необходимым условием процветания.

В настоящее время в государственных и корпоративных, гражданских, научных, тематических и профессиональных сообществах приобрели популярность различные формы сетевого общения с использованием ИКТ, которые применяются в различных областях деятельности организаций, таких, как распространение информации внутри компании, коллективная разработка проектов, связи с клиентами, управление контентом, маркетинг и PR, а также в управлении знаниями [3].

Применительно к вузам основными процессами, где происходит извлечение, накопление и распространение знаний являются учебный процесс, научные исследования и разработки, материализация и коммерциализация результатов НИР и НИОКР, разработка учебных материалов.

Современный вуз по своему годовому финансовому обороту, по размерам, по объему и стоимости основных средств, по структуре ничем не отличается от крупных предприятий производства или сферы услуг.

Роли различных форм сетевого общения применительно к вузам приведены на рис. 3 [4].

Социальная структура. Социальную сеть можно определить как социальную структуру, объединяющую отдельных людей или даже целые организации.

Социальная сеть показывает, каким образом ее участники связаны друг с другом теми или иными отношениями — от случайных знакомств до тесных семейных связей.

В вузе объектами внимания должны становиться разномасштабные группы людей, причем в первую очередь такими объектами должны быть учебные группы студентов.

Связи в группах могут быть прямыми или косвенными, сильными или слабыми, односторонними или двусторонними. Персоны с большим количеством прямых связей играют важную роль в структуре взаимоотношений данной группы, часто демонстрируют большую продуктивность работы и большую удовлетворенность ею, чем участники сети с меньшим числом прямых связей. Эти персоны выполняют функции основных посредников между людьми, соединенными косвенными, непрямыми связями. Такое посредничество может оказывать как положительное, так и отрицательное влияние на взаимоотношения в социальной сети, помогая или, наоборот, препятствуя распространению информации либо налаживанию отношений между различными подгруппами сети. В структуре взаимоотношений данной группы желательно наличие преподавателей, включенных внутрь сетевого общения.

Важно соблюдать баланс между слабыми и сильными связями в социальных сетях — первые дают дополнительные источники инноваций, а вторые помогают создавать и поддерживать необходимый рабочий микроклимат.

Наличие двусторонних взаимодействий в группах часто помогает повысить эффективность работы группы. Преподаватель не только является источником информации для остальных членов группы, но и сам черпает нужные ему сведения, обращаясь к коллегам.

Исследование социальных сетей открывает резервы повышения эффективности совместной работы, позволяет лучше использовать таланты и знания участников группы, определять узкие места при реализации тех или иных решений, внедрении новаторских подходов и технологий.

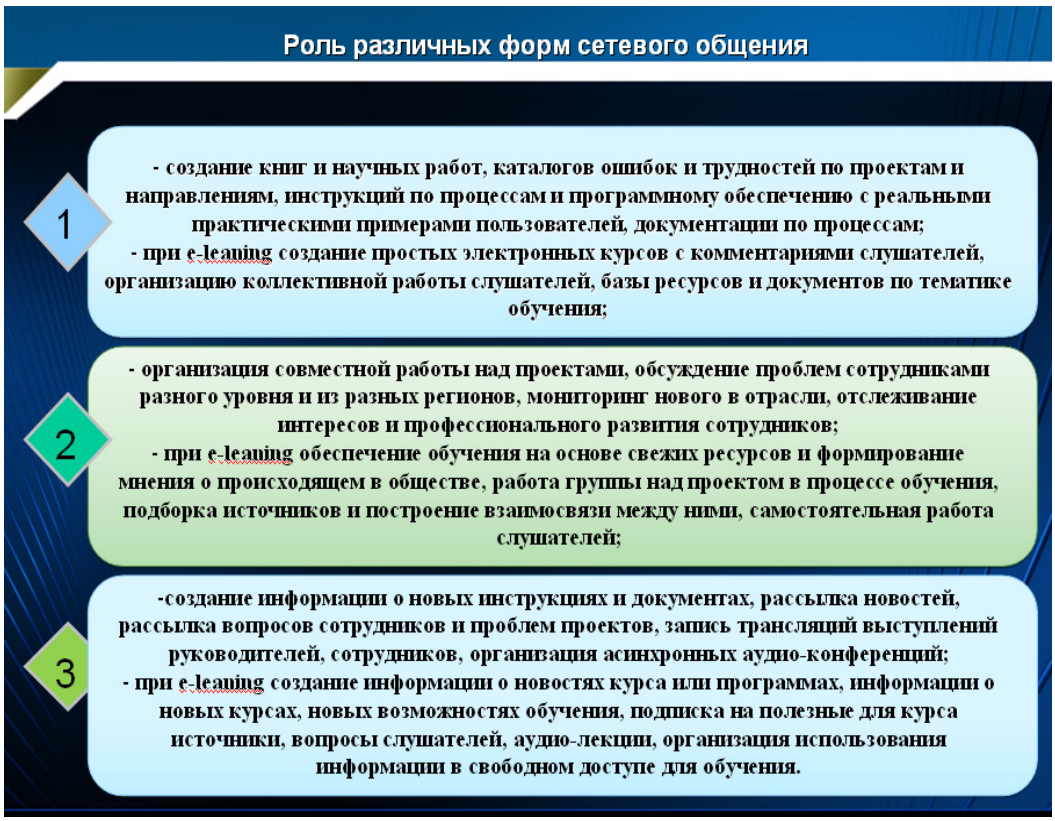


Рис. 3. Роли различных форм сетевого общения

Социальные сети могут выявить неформальные связи между участниками группы, что может оказаться полезным в организации образовательного процесса.

Социальные сети помогают наводить мосты между иерархической организационной структурой ВУЗа и неформальной горизонтальной структурой социальных связей для достижения стратегических целей обучения.

Для идентификации социальных сетей с целью последующего анализа используются, как правило, интервью, опросы, специальные методы наблюдений. Множатся сайты, поддерживающие виртуальные сообщества.

ВУЗ объединяет людей, которые заинтересованы в приобретении и развитии знаний в определенной области, их использовании на практике и для достижения таких целей постоянно взаимодействуют друг с другом.

Вузовские сообщества, по сути, и осуществляют сегодня управление явным и неявным знанием. Члены вузовского сообщества хорошо понимают друг друга, поскольку работают над схожими проблемами. Они способны оценить уровень квалификации, проблемы и озарения коллег, получить друг от друга недостающие им знания. Эти знания являются основой для решения стоящих перед ними задач и базой для формирования новых знаний. А технологии, системы и структуры накопления и доступа к информации, такие как внутрикорпоративные сети, порталы и программные продукты совместной работы, обеспечивают инструментальную поддержку управления знаниями.

Опасности социальных сетей. Однако необходимо учитывать, что социальные сети, обеспечивая поддержание связи между людьми; создание групп по интересам, превращают нашу жизнь в открытую книгу, где информацию о нас могут прочесть не только наши друзья, но и недоброжелатели. Поэтому необходимо помнить о возможных угрозах со стороны социальных сетей.

На рис. 3 показаны главные опасности, таящиеся в социальных сетях. Список может пополняться вместе с тем, как мы будем продолжать пользоваться социальными сетями, а они, в свою очередь, будут развиваться самым непредсказуемым образом вместе с новыми технологиями.

Социальные сети предоставляют мошенникам возможность нанести вред пользователям за счет открытости данных, кражи базы данных провайдера, использования вводящих в заблуждение сайтов, а также распространения вредоносных Интернет-адресов через группы объявлений, чаты или отправку личных сообщений.

Заключение. Информационно-коммуникационные технологии при их умелом использовании могут и должны стать мощным инновационным ресурсом совершенствования промышленности, науки и образования. При этом социальные сети могут служить инструментом развития, однако необходимо учитывать таящиеся в них опасности.

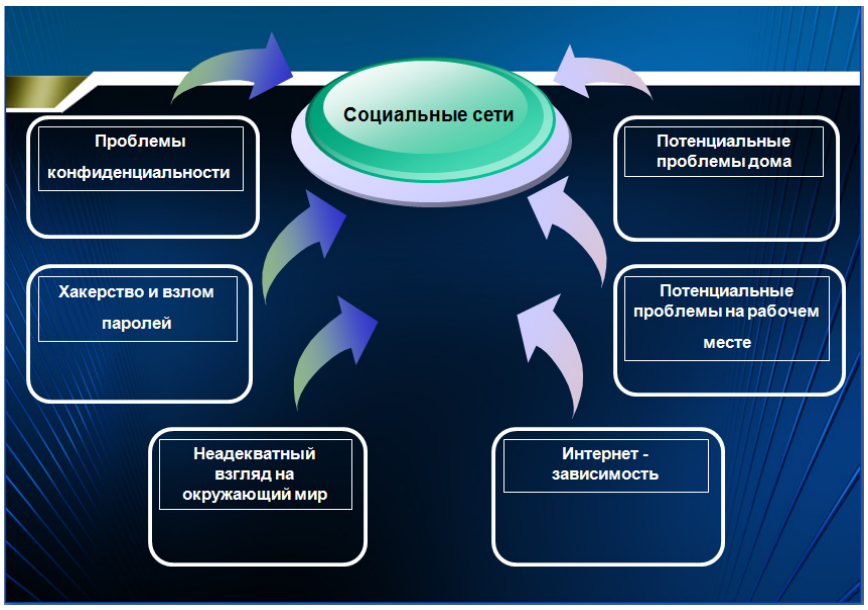


Рис. 3. Опасности социальных сетей

СПИСОК ЛИТЕРАТУРЫ

1. Какие социальные сети самые популярные в 2017 году // Российский Бизнес-журнал http://www.rosbj.ru/2017/05/13/1250 -2017/ (дата обращения – 19.09.2017).
2. Фролова Е.В. Самые популярные сети в мире 2016. http://www.pro-smm.com/populyarnye-socialnye-seti-2016/ (дата обращения – 19.09.2017).
3. Кононов О.А. Кононова О.В. Социальные сети и образовательный процесс. XV Санкт-Петербургская международная конференция «Региональная информатика – 2016 (РИ-2016)»: материалы конференции. – СПб.: СПОИСУ, 2016. С.366-367.
4. Кононов О.А. Кононова О.В. Социальные сети и управление знаниями. Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 2 / СПОИСУ. - СПб, 2016. - С.245-249.
5. Букин М.В. Об угрозах в Сети мало что известно. http://nag.ru/articles/article/20826/ob-ugrozah-v-seti-malo-chto-izvestno.html (дата обращения – 19.09.2017).

УДК 37.062

ПЕДАГОГИЧЕСКИЕ КОММУНИКАЦИИ В СОВРЕМЕННОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ

Костюк Анатолий Владимирович
Санкт-Петербургский военный институт войск национальной гвардии Российской Федерации
Россия, Санкт-Петербург, улица Летчика Пилютова, д. 1,
emails: kostyuk.anatoliy.2015@mail.ru

Аннотация: В статье рассмотрены необходимость и возможности профессионального педагогического взаимодействия в среде интернет. Проанализированы особенности коммуникаций при отсутствии непосредственного визуального контакта, выявлены особенности профессиональных педагогических коммуникаций и обусловлена необходимость формирования определенных ИКТ-компетенций для участников образовательного процесса в электронной среде.

Ключевые слова**:** *информационные и педагогические коммуникации; вербальная (языковая) коммуникация; электронная среда обучения и общения; компьютерные телекоммуникации; коммуникационные компетенции.*

PEDAGOGICAL COMMUNICATIONS IN THE MODERN EDUCATIONAL ENVIRONMENT

Kostyuk Anatoliy, Bobonets Sergey
St. Petersburg military institute of troops of national guard of the Russian Federation
Russia, St. Petersburg, Pilot Pilyutov Street, 1,
emails: kostyuk.anatoliy.2015@mail.ru,sbobon@mail.ru

Abstract: In the article the necessity and possibilities of professional pedagogical interaction in the Internet environment are considered. Features of communications are analyzed in the absence of direct visual contact, features of professional pedagogical communications are revealed and the necessity of forming certain ICT competences for the participants of the educational process in the electronic environment is determined.

Keywords: *information and pedagogical communications; verbal (language) communication; electronic learning and communication environment; computer telecommunications; communication competence.*

В современных условиях, в стремительно развивающемся информационном обществе, новым требованием, предъявляемым к образовательной системе, является необходимость инновационных

подходов в организации и осуществлении образовательного процесса, а также развитие и усовершенствование технологий по передаче, приему и обработке информации.

Информационные потоки в общественной жизни расширяются с «гипер» скоростью. Информация в обществе, науке и образовании требует быстрой, качественной и защищенной передачи от одного абонента к другому. Для этого человечество обращается к информационным и телекоммуникационным технологиям [1].

Категория «информационная технология» является общепринятой, несмотря на то, что в последнее время трактовка данного термина частично трансформировало его содержание. Сравнительно пространное определение приводится в ГОСТ Р 34.003 «информационная технология – приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных». Тем не менее, в приведенном определении, как и в некоторых других, отсутствует существенная составляющая, которая предопределяет всякую технологию – получение установленных, заведомо определенных результатов. Поэтому предлагается определение, учитывающее цели технологии и ее инструментальные средства: «информационная технология является процессом, который использует фиксированный набор средств, способов и методов автоматизированного сбора, обработки, хранения, обработки и передачи информации для получения определенных, заведомо ожидаемых результатов» [1,2].

Телекоммуникационные технологии, на наш взгляд, представляют собой процесс, в ходе которого используется совокупность методов и алгоритмов передачи информации и современные средства связи, которые обеспечивают информационное взаимодействие пользователей, как на локальном, так и глобальном уровне, в том числе в сети Интернет.

Новейшие средства телекоммуникационных технологий функционируют на основе соединения компьютерных сетей и средств телефонной, телевизионной, спутниковой связи, интегрируются в системы приема-передачи, обеспечивают информационное взаимодействие, как индивидуальных пользователей, так и организаций, регионов, государств. Это дает возможность осуществлять операции обмена текстовой, графической, звуковой, видеоинформацией между отдельными участниками компьютерной сети или центральным хранилищем информации и пользователями компьютеров, подключенных к одной из линий связи [2].

Подавляющее большинство педагогов использует термин педагогические коммуникации, и рассматривают обучение, как совокупность и взаимодействие нескольких ключевых составляющих: преподаватель – учебный контент – обучающийся/обучающиеся. Педагогические коммуникации необходимо рассматривать в качестве специфической формы общения, для которой характерны общие психологические закономерности, типичные общению как форме взаимодействия человека с другими людьми, включающей коммуникативный, интерактивный и другие компоненты.

В педагогических коммуникациях в электронной среде обучения и общения коммуникацию следует рассматривать в качестве первичного процесса, который координирует целеустремленные, практичные действия ее участников. Отличительными чертами данных взаимодействий между участниками процесса коммуникации представляется то, что такое взаимодействие выполняется не прямо, а посредством компьютерных каналов связи (компьютерных телекоммуникаций).

Необходимо отметить, что опыт коммуникации (лицом к лицу) в традиционной среде общения не может быть автоматически перенесен на опосредованное ИКТ-общение в компьютерной среде обучения. Это объясняется тем, что коммуникативная и интерактивная работа преподавателя и самого учащегося существенно изменяются под влиянием новой среды общения.

К тому же необходимо принимать во внимание, что именно опосредованность процесса коммуникации требует вежливого отношения со своими оппонентами, толерантности и культуры общения.

Внедрение в образовательную деятельность информационно-телекоммуникационных сетей и технологий дает новый импульс в развитие информатизации образования. Особенно сильное воздействие на развитие коммуникационных технологий оказывает глобальная сеть интернет, обеспечивающая доступ к громадным объемам распределенной информации, которая хранится в разнообразных частях нашей планеты. Значительная часть эксперты рассматривают интернет-технологии как революционный прорыв.

Современные коммуникационные технологии и среда интернета существенно расширили возможности коммуникаций в профессиональной области. Открытость, и демократизм интернет-взаимодействия с одной стороны обеспечивают [3,4]:

– высокую скорость взаимодействия, образующую мобильную обратную связь с партнерами (при условии их активного участия во взаимодействии);

– расширение круга единомышленников не только в своей стране, но и за рубежом;

– дополнительные возможности преподавателям для удовлетворения своих информационно-образовательных и профессиональных потребностей;

– экспертную оценку своих публикаций и достижений, собственную оценку публикаций и достижений других участников взаимодействия в сети Интернет (самовыражение, самоутверждение, самореализация);

– возможность анонимного участия во взаимодействии (снятие страхов, фобий и других психопатических ограничений).

С другой стороны, профессиональное педагогическое взаимодействие посредством интернета с учетом особенностей сетевого этикета требуют ответственности за процесс и результат взаимодействия, поскольку оно подвергается публичной оценке и критике. Эти риски отрицательно влияют на мотивацию к взаимодействию. Как показывает анализ форумов, сайтов педагогических сообществ, интернет-семинаров и конференций, педагогическое сообщество в целом пока недостаточно готово к публичности и объективности на этой стадии [2,4].

Участники профессионального педагогического взаимодействия посредством сети интернет могут иметь персонифицированные интернет-сервисы с различными потребительскими и технологическими характеристиками или общие для всех участников взаимодействия интернет-сервисы, предоставляемые со стороны организаторов информационного взаимодействия [5]. Поэтому при формировании пространства целей, конкретизации целей и задач следует учитывать особенности персонифицированных интернет-сервисов.

Выделенные особенности педагогического взаимодействия в сети интернет обуславливают необходимость формирования определенных ИКТ-компетенций, которые в иных случаях соприкосновения с информационно-коммуникационными технологиями (ИКТ) или их применения в обучении не являются существенными (например, умения подготовить сообщение для различных категорий субъектов взаимодействия, умения использовать метафоры, сленг, паралингвистические приемы и т. д). Эти и другие специальные ИКТ-компетенции необходимо формировать как у работающих в рамках повышения квалификации, так и у будущих педагогов.

Новые коммуникационные технологии способны обеспечить индивидуализацию и активизацию образовательного процесса даже в границах группового обучения, которое основывается на представлении учебного материала, ориентированного на «усредненного» обучающегося.

Благодаря преимуществам коммуникационных технологий формы и методы традиционной системы образования приобретают импульс в дальнейшем развитии. Например, учебные вопросы, восприятие которых не нуждается в дополнительных разъяснениях, могут быть представлены на сайте в электронном виде. Индивидуальные коммуникации реализуются, как правило, при помощи интернет-телефонии, которая обеспечивает общение с преподавателем в приватной форме. Коммуникационные технологии видео- и электронных конференций, чатов обеспечивают проведение, как оперативных коллективных обсуждений, дискуссий, так и достаточно продолжительных по времени виртуальных электронных семинаров, конференций, выполнение проектов и других видов работ, которые требуют совместного общения.

Проведенные исследования показывают что, несмотря на очевидные достоинства коммуникационных технологий, выявилась низкая готовность, как обучающихся, так и преподавателей к результативному применению современных средств коммуникации, а также неумение взаимодействовать в ходе интерактивного диалога в режиме форума, недопонимание предоставляемых возможностей для образовательного процесса видеоконференций и интернет-трансляций. Кроме того, неготовность к использованию новых компьютерных коммуникаций выражается в достаточной пассивности участников образовательного процесса, в отсутствии твердых навыков кратко и корректно выразить свои мысли, в недостаточных умениях использовать современные средства общения для консультаций и защиты выполненных работ в новых условиях взаимодействия.

Для эффективного использования компьютерных коммуникаций участники образовательного процесса в первую очередь должны обладать коммуникативной компетенцией, т. е. способностью реализовывать эффективное общение в электронной среде с другими участниками, напрямую принимающими участие в педагогическом процессе, а также хорошо ориентироваться в современных средствах коммуникации. Приобретение и формирование умений и навыков взаимодействия в компьютерной среде быть может осуществлено лишь в процессе активной деятельности, которая должна включать различные формы компьютерной опосредованной коммуникации.

Решение задач, которые требуют напряженного взаимодействия в сетевой компьютерной среде, требует выбора эффективных способов коммуникации участников образовательного процесса, например, проведение дистанционных курсов, использование методов обучения в сотрудничестве (collaborative learning), которые основаны на коммуникации в малых группах (3-5 человек), включающие проектные, проблемные и кооперативные методы обучения.

Особое значение для профессионального педагогического взаимодействия в сети интернет имеют медиалингвистические особенности сообщений. По сравнению с традиционным взаимодействием информационная (содержательная) и коммуникативная (процессуальная) составляющие взаимодействия в сети интернет являются более существенными.

В сети интернет как информационно-коммуникационной среде информационное взаимодействие зачастую сводится к обмену текстовыми сообщениями, поэтому основой взаимодействия является вербальная (языковая) коммуникация и преимущественно в письменной форме [2]. При взаимодействии средствами письменно-речевой коммуникации, реализуемой текстами сообщений электронной почты, чатов, содержанием веб-страниц и пр., существенным образом акцентируются различные роли пишущего, автора (отправитель, адресант) и читателя (получатель, адресат) [5]. При этом отсутствие непосредственного визуального контакта существенным образом изменяет процесс взаимодействия. Субъекты взаимодействия могут и не иметь личных контактов до взаимодействия,

например, взаимодействие участников формируемого сетевого педагогического сообщества или взаимодействие сетевого педагога и сетевого обучающегося.

Отсутствие личного контакта затрудняет взаимодействие, так как достаточно сложно через письменную коммуникацию «спроектировать» личность, определить ее творческие и профессиональные интересы и психологические особенности. С другой стороны, отсутствие личного контакта, а в будущем и невозможность его установления, упрощает взаимодействие, поскольку снимает большинство существующих при реальном взаимодействии психологических барьеров.

Во втором случае, отсутствие личного контакта ограничивает степени свободы взаимодействующих и создает условия для более тонкой настройки на виртуального, но известного, адресата. Взаимопонимание между преподавателями, как правило, основывается на общности профессиональных интересов и проблем, причем последнее является наиболее существенным. Именно эти проблемы и их обсуждение инициируют обмен опытом.

В тоже время потребность установления взаимопонимания и предисловия взаимодействия между преподавателями и обучающимися актуализирует необходимость использования особенностей письменно-речевой коммуникации, принятой в молодежной среде.

Таким образом, для эффективного использования компьютерных коммуникаций участники образовательного процесса в первую очередь должны обладать коммуникативной компетенцией. Приобретение и формирование умений и навыков педагогического взаимодействия в компьютерной среде быть может осуществлено лишь в процессе активной деятельности, которая должна включать различные формы компьютерной опосредованной коммуникации и выбора эффективных способов коммуникации участников образовательного процесса. Современные педагогические коммуникации требуют использования особенностей письменно-речевой коммуникации, принятой в молодежной среде.

Для дальнейшего формирования теории и методики педагогической коммуникации в электронной образовательной среде необходимы совместные исследования, как в области педагогики, так и в других гуманитарно-социальных и технических науках.

СПИСОК ЛИТЕРАТУРЫ

1. Костюк А.В. Использование информационно-коммуникационных технологий для подготовки офицеров национальной гвардии // Направления и перспективы развития образования в военных институтах войск национальной гвардии Российской Федерации. / Сборник научных статей VIII Межвузовской научно-практической конференции с международным участием. 2017. С. 462-466.
2. Костюк А.В., Бобонец С.А. Информационные технологии в науке и образовании. Учебник. Часть 1.– СПб.: Астерион, 2017. – 256 с.
3. Костюк А.В., Бобонец С.А. Проблемы информационной безопасности в технологиях дистанционного обучения / Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 2 / СПОИСУ. – СПб., 2016. – 491 с. (стр. 100-102)
4. Костюк А.В., Примакин А.И. Информационная поддержка образовательного процесса / /Вестник Санкт-Петербургского университета МВД России. 2016. № 1. С. 170-174.
5. Бобонец С.А., Костюк А.В. Информационно-образовательная среда как фактор повышения эффективности образовательного процесса.//В сборнике: Эффекты реализации исследовательских проектов в военных институтах внутренних войск материалы научно-методического семинара. Санкт-Петербургский военный институт внутренних войск МВД России. 2016. С. 74-78.

УДК 681.3.067

МОДЕЛЬ ФОРМИРОВАНИЯ ТРЕБОВАНИЙ К КОНФИДЕНЦИАЛЬНОСТИ, ЦЕЛОСТНОСТИ И ДОСТУПНОСТИ ДАННЫХ В СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Куватов Валерий Ильич, Примакин Алексей Иванович
Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, ул. летчика Пилютова, д. 1,
emails: kyb.valery@yandex.ru, a.hrimakin@mail.ru, a.primakin@mail.ru

***Аннотация*:** В статье рассматривается задача формирования требований к конфиденциальности, целостности и доступности данных в системе защиты информации средств вычислительной техники и автоматизированных систем. Показано, что для решения этой задачи может быть использован метод анализа иерархий и кластерный анализ. Разработана методика решения задачи на основе этих двух методов.

***Ключевые слова**: конфиденциальность; целостность; доступность; защита информации; матрица парных сравнений; собственное число; собственный вектор.*

MODEL FOR FORMATION OF REQUIREMENTS FOR CONFIDENTIALITY OF INTEGRITY AND ACCESSIBILITY OF DATA IN THE SYSTEM OF INFORMATION PROTECTION OF MEANS OF COMPUTER ENGINEERING AND AUTOMATED SYSTEMS

Kuvatov Valery, Primakin Alexey
St. Petersburg University of the Ministry of Internal Affairs of Russia,
Russia, St. Petersburg, st. pilot Pilutov, 1,
emails: kyb.valery@yandex.ru, a.hrimakin@mail.ru, a.primakin@mail.ru

***Abstract**:* The article considers the problem of formation of requirements to the confidentiality, integrity and availability of data in the system of information security of computer equipment and automated systems. It is shown that for solutions of this task can be used analytic hierarchy process and cluster analysis. The developed method of solving the problem based on these two methods.

Keywords: *confidentiality; integrity; availability; data protection; matrix of paired comparisons; eigenvalue; eigenvector.*

Введение. Задача обеспечения информационной безопасности средств вычислительной техники (СВТ) и автоматизированных систем (АС) по мере внедрения компьютеров во все стороны жизни личности, общества и государства становится все более важной. Поэтому раздел теории информационной безопасности, направленный на разработку систем защиты информации в СВТ и АС, является одним из наиболее востребованных разделов.

Основная часть. Наибольшую сложность при разработке системы защиты информации в СВТ и АС представляет задача формирования требований к защите каждого вида используемой в системе конфиденциальной информации, ее носителей и процессов обработки. Эта сложность в первую очередь связана с отсутствием формальных моделей сравнительной оценки величины требований конфиденциальности, целостности и доступности информации хранящейся и обрабатываемой в СВТ, АС.

Классический подход к решению этой задачи основан на учете только одного свойства безопасности информации - ее конфиденциальности [1]. Требования к обеспечению целостности и доступности информации, как правило, фигурируют опосредовано, в общих требованиях к СВТ и АС. Считается, что раз доступ к информации имеет узкий круг доверенных лиц, вероятность ее искажения (нарушения целостности) или блокирования (нарушения доступности) незначительна. Такой подход правомерен, если важность конфиденциальности много выше важности целостности и доступности.

В общем случае это не всегда так. В некоторых случаях, особенно при работе с коммерческой информацией, более важными могут оказаться такие качества как целостность и доступность.

Современный подход [1] предполагает, наряду с требованиями по обеспечению конфиденциальности информации, формирование требований по обеспечению целостности и доступности информации (последнее – только для санкционированных пользователей). Так для платежных документов самым важным свойством является свойство целостности (достоверности), следующим по важности является свойство доступности. Требование конфиденциальности для платежных документов является не столь важным.

Для каждого типа требований разрабатывается несколько уровней. Число уровней и их смысл могут различаться, важно чтобы они указывались конкретно, исходя из величины возможного ущерба, наносимого субъектам информационных отношений. Порядок определения уровня принято описывать следующим образом: Составляется перечень типов информационных ресурсов. Для этого данные делятся по тематике, по функциональному назначению, по одинаковости информационных технологий и др. признакам. Для каждого типа данных и каждого свойства безопасности информации определяются: перечень и важность субъектов информационных отношений (важность незначительная, малая, средняя, высокая, очень высокая), интересы которых затрагиваются при нарушении данного свойства безопасности информации и уровень наносимого субъекту ущерба (незначительный, малый, средний, большой, очень большой).

Для каждого типа информации с учетом значимости субъектов и уровней наносимого им ущерба устанавливается степень необходимой защищенности по каждому из свойств безопасности информации. В качестве уровней защищенности могут выступать: отсутствие требований по данному свойству, низкий, средний, высокий, очень высокий уровень требований. При равенстве значений для разных субъектов, в итоге выбирается максимальное значение уровня (таблица 1).

Таблица 1

Пример представления результатов оценки требований к защищенности некоторого типа информации

Субъекты	Требования по уровням защищенности		
	конфиденциальность	целостность	доступность
№1	нет	средняя	низкая
№2	низкая	низкая	высокая
№3	средняя	высокая	средняя
Итоговый уровень	средняя	высокая	высокая

Наиболее важный недостаток такого подхода связан с использованием ранговой шкалы для оценки величины каждого свойства. Ранги разных свойств информации одного типа не связаны между собой. Несвязанными являются также ранги одного свойства информации разных типов. Все это не дает возможности рационально распределять ресурсы между обеспечением различных свойств одного и того же типа информации, между одинаковыми свойствами разных типов информации [2].

В данной работе предлагается:

– метод сравнительной оценки важности субъектов, важности показателей конфиденциальности, целостности и доступности информации для каждого из субъектов;

– метод разделения субъектов информационных отношений на классы с одинаковыми требованиями к конфиденциальности, целостности и доступности информации.

В идейном отношении метод базируется на схеме анализа иерархий [2] и кластерный анализ [3]. Методику применения метода анализа иерархий рассмотрим на примере задачи оценки важности субъектов.

Задача оценки важности субъектов. Пусть в состав АС входит n субъектов. Объективно существуют, но нам неизвестны веса, характеризующие важность каждого из них, w_i. Эксперт на основе опыта и интуиции задал величины α_{ij}, характеризующие его суждения о преимуществе i-го субъекта над j-м. В идеале, когда эксперт действует безошибочно, $\alpha_{ij} = w_i / w_j$. В реальности это равенство, как правило, не соблюдается, и чем больше по абсолютному значению разность $\alpha_{ij} - w_i / w_j$, тем больше ошибки эксперта.

Сформируем матрицу парных сравнений (суждений) эксперта $A = \|\alpha_{ij}\|$, размерностью $n \times n$. Очевидно, что эта матрица будет обратно симметричная, т.е. для любых i и j будет иметь место соотношение $\alpha_{ij} = 1/\alpha_{ji}$, причем для всех i $\alpha_{ii} = 1$. Назовем матрицу A', для каждого элемента которой выполняются соотношения $\alpha'_{ij} = w_i / w_j$, полностью согласованной.

Для полностью согласованной матрицы получим, $\alpha'_{ij} \cdot w_j = (w_i / w_j) \cdot w_j = w_i$, i, j=1,..,n. В реальности это соотношение, как правило, выполняться не будет. Однако если предположить, что ошибки эксперта являются несмещенными, то есть их математическое ожидание равно отношению w_i / w_j, то, при достаточно большом n для обратно симметрической матрицы А будет иметь место равенство, $w_i = \sum_{j=1}^{n} w_j \cdot \alpha_{ij} \Big/ \lambda_{\max}$, где $\lambda_{\max} \approx n$, i=1,..,n. Перепишем это выражение: $w_i \cdot \lambda_{\max} = \sum_{j=1}^{n} w_j \cdot \alpha_{ij}$. Получим известную из линейной алгебры задачу отыскания собственных векторов и собственных значений матрицы А. Как известно, собственные значения матрицы А находятся из матричного уравнения $A - \lambda \cdot E = 0$, где Е - единичная матрица, причем количество собственных значений совпадает с размерностью матрицы, т.е. равно n.

Каждому собственному значению матрицы А соответствует бесконечное множество собственных векторов. В случае если ранг матрицы А равен n, то все собственные вектора, относящиеся к одному собственному значению матрицы коллинеарны, т.е. для любых двух векторов $W = (w_1,.., w_n)$ и $V = (v_1,.., v_n)$, принадлежащих одному λ, существует скалярная положительная величина с, такая, что $W = c \cdot V$. Поэтому вектор W всегда можно выбрать так, чтобы $\sum_{i=1}^{n} w_i = 1$. Но тогда компоненты данного вектора и будут представлять собой нормализованные веса важности субъектов информационных отношений. С учетом того, что данный вектор характеризует важность субъектов информационных отношений, обозначим его Wc.

В линейной алгебре доказано, что если матрица А полностью согласована, то все ее собственные значения равны 0, за исключением одного, равного n. Доказано также, что если элементы α_{ij} положительной обратно симметричной матрицы незначительно изменить, то ее собственные значения также изменятся незначительно.

С учетом двух приведенных фактов, по результатам решения уравнения $A - \lambda \cdot E = 0$ можно судить о степени согласованности матрицы парных сравнений. Чем больше $\lambda_{\max}$ отличается от n, а остальные собственные значения - от нуля, тем более рассогласованной является эта матрица.

Степень рассогласования матрицы парных сравнений оценивают с помощью так называемого индекса согласованности, $\delta_{uc} = (\lambda_{\max} - n)/(n-1)$. Принято считать, что если индекс согласованности

не превышает по абсолютному значению 0.1, то матрица парных сравнений согласована достаточно хорошо. В противном случае матрица считается рассогласованной и ее необходимо согласовать.

Простейший вариант повышения согласованности матрицы парных сравнений заключается в следующем. Вычислим вспомогательную матрицу в соответствии с выражением, $b_{ij} = \alpha_{ij} - w_i / w_j$, где w_i, w_j компоненты собственного вектора матрицы А. Найдем строку, для которой $b = \max_{i,j} b_{ij}$ и попросим эксперта откорректировать ее. Процесс необходимо продолжать, пока абсолютная величина индекса согласованности не окажется в заданных пределах.

Методика оценки важности субъектов:

– Составить матрицу парных сравнений $A = \|\alpha_{ij}\|$.

– Найти максимальное собственное значение матрицы парных сравнений λmax.

– Рассчитать индекс согласованности δис и, в случае необходимости, откорректировать матрицу парных сравнений.

– Рассчитать нормализованный собственный вектор W, соответствующий максимальному собственному значению. Этот вектор и будет представлять нормализованные веса важности субъектов информационных отношений.

Задача оценки важности показателей конфиденциальности, целостности и доступности информации субъектов информационных отношений. Пусть в АС имеется m типов информации, требующих обеспечения конфиденциальности, целостности и доступности. Известно, что требования по этим свойствам для разных субъектов могут различаться. Составим матрицу парных сравнений конфиденциальности размера nxn для информации первого типа (таблица 2).

Таблица 2

Матрица парных сравнений оценки требований конфиденциальности субъектов информационных отношений для информации первого типа.

Конфиденциальность	Номер субъекта информационных отношений		
Номер субъекта информационных отношений	Субъект 1	……..	Субъект n
Субъект 1	α_{11}	α_{12}	α_{13}
……	α_{21}	α_{22}	α_{23}
Субъект n	α_{31}	α_{32}	α_{33}

Действуя по вышеприведенной методике, получим нормализованный вектор Wк1, характеризующий требования к конфиденциальности для каждого из n субъектов.

Рассуждая аналогично, получим нормализованный вектор Wц1 характеризующий относительную важность целостности и нормализованный вектор Wд1 характеризующий относительную важность доступности информации первого типа для каждого из n субъектов.

Переходя к информации второго…, m-го типа, получим в конечном итоге множество из n векторов размерностью 4m (матрицу размера 4mxn), содержащую информацию о важности каждого субъекта, о требованиях конфиденциальности, целостности и доступности информации каждого типа по отношению к каждому из n субъектов. Теперь, воспользовавшись кластерным анализом [4], поделим это множество на классы с близкими уровнями требований по конфиденциальности, целостности и доступности информации.

Заключение. Метод анализа иерархий позволяет в данном случае получать более объективные экспертные оценки, чем оценки, получаемые другими методами, а кластерный анализ – делить множество субъектов на близкие по требованиям конфиденциальности, целостности и доступности информации.

СПИСОК ЛИТЕРАТУРЫ

1. М. А. Борисов, И. В. Заводцев, И. В. Чижов. Основы программно-аппаратной защиты информации. — М.: URSS, 2015 — 412 с.
2. Куватов В. И., Синещук Ю. И., Синещук М. Ю. Проблемы выбора рационального состава системы защиты информации.// Труды Юбилейной XV Санкт-Петербургской международной конференции «Региональная информатика «РИ-2016».С. 219-220.
3. Куватов В. И., Величко Г. А. Исследование операций. – Петродворец: ВВМУРЭ, 2005 – 425 с.
4. Неслухов Д.С. Использование кластерного и регрессионного анализа в изучении экономической деятельности судостроительных и судоремонтных предприятий //Интернет-журнал «НАУКОВЕДЕНИЕ» Том 8, №4 (2016) http://naukovedenie.ru/PDF/78EVN416.pdf (доступ свободный).

УДК 351.74:004

СУБЪЕКТНЫЙ СОСТАВ ПРАВООТНОШЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Лепёхин Александр Николаевич
Академия МВД Республики Беларусь
Республика Беларусь, г. Минск, просп. Машерова, д. 6
email:prav_informatika@mail.ru

Аннотация: в статье расматривается анализ действующих подходов к осуществлению информационно-аналитической работы в правоохранительных органах государств-членов ОДКБ. В рамках проведенного исследования сформулирована система субъектов правоотношений в сфере информационно-аналитического обеспечения правоохранительной деятельности, а также определен перечень правоохранительных органов (адресатов рекомендаций), сформированный по функционально-активному критерию, направленности на выявление правонарушений.

Ключевые слова: *информационно-аналитическая работа, рекомендации по правовому регулированию, адресаты рекомендаций, система субъектов правоотношений.*

SUBJECT COMPOSITION OF RELATIONSHIPS IN THE FIELD OF INFORMATION AND ANALYTICAL ENFORCEMENT OF LAW ENFORCEMENT ACTIVITY

Lepyokhin Alexander Nikolaevich
Academy of the Ministry of Internal Affairs of the Republic of Belarus
Republic of Belarus, Minsk, prosp. Masherova, 6
email: prav_informatika@mail.ru

Abstract: The article analyzes the analysis of current approaches to the implementation of information and analytical work in the law enforcement agencies of the CSTO member states. Within the framework of the research, a system of subjects of legal relations in the field of information and analytical support of law enforcement activities was formulated, and a list of law enforcement agencies (recommendations recipients), formed according to a functionally active criterion, aimed at identifying offenses, was determined.

Keywords*: information-analytical work, recommendations on legal regulation, addressees of recommendations, system of subjects of legal relations.*

Введение. Анализ действующих подходов к проведению информационно-аналитической работы (далее ИАР) в правоохранительных органах показывает, что в основном она имеет поверхностный характер, заключающийся в сравнении определенных показателей оперативно-служебной деятельности с предыдущим периодом, а также в проведении в ряде случаев факторного анализа и разработке регрессионных моделей, используемых в прогнозной деятельности. Полагаем, что такая методика имеет серьезные методологические ограничения, как по срокам проведения прогнозной деятельности, так и по качеству ее реализации. Очевидно, возникает необходимость в совершенствовании инструментария ИАР, а также формировании правовых основ такой деятельности. Поскольку эффективная реализация правоохранительной функции государства, напрямую зависит от ее информационно-аналитического обеспечения и является одним из ключевых факторов обеспечения национальной безопасности государств – членов ОДКБ.

В этой связи, в современных условиях особую значимость приобретает совершенствование действующей, а также разработка новой нормативной правовой базы и подходов по гармонизации законодательства государств – членов ОДКБ в области информационно-аналитической работы правоохранительных органов. Это обусловлено необходимостью формирования иерархически организованной и непротиворечивой системы актов законодательства, регламентирующих соответствующие общественные отношения, и потребностью повышения эффективности реализации правоохранительной функции уполномоченными государственными органами.

Для указанных целей предлагается сформировать следующую систему субъектов правоотношений в сфере информационно-аналитического обеспечения правоохранительной деятельности:

1. Субъекты, наделенные государственно-властными полномочиями (государственные органы);
2. Взаимодействующие субъекты в рамках государственно-частного партнерства (юридические и физические лица, оказывающие содействие государственным органам в реализации их информационной и аналитической функций);
3. Юридические и физические лица как субъектно-объектная составляющая информационно-аналитической деятельности государственных органов.

Заключение. Таким образом, полагаем, что разработка подходов к системе субъектов позволяет выделить и сгруппировать перечень правоохранительных органов, сформированный по функционально-активному критерию, направленности на выявление правонарушений, а также провести их классификацию с учетом реализуемых ими задач и функций:

1. Государственные органы, реализующие функции в сфере борьбы с преступностью:
2. Государственные органы, реализующие функции в сфере защиты конституционного строя:
3. Государственные органы, реализующие функции в сфере защиты экономической безопасности:
4. Государственные органы, реализующие функции в сфере реализации пограничной политики:

СПИСОК ЛИТЕРАТУРЫ

1. Кудрявцев в.н., лебедев а.в. организация информационно-аналитической работы в учреждениях и органах, исполняющих наказания // уголовно-исполнительная система: право, экономика, управление. 2008. № 1. с. 44.
2. Поминов с. н. принципы организации деятельности овд в сфере противодействия религиозному экстремизму // закон и право, 2007. № 5.

УДК 629.75.33 + 533.6.013.622

О МЕТОДЕ ИДЕНТИФИКАЦИИ БЕСПИЛОТНЫХ ВОЗДУШНЫХ СУДОВ ПРИ РЕАЛИЗАЦИИ КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ

Беляев Сергей Алексеевич[1], Остапченко Юрий Борисович[2], Кудряков Сергей Алексеевич[3], Рубцов Евгений Андреевич[3]
[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
[2] ОАО «НИЦ СПб ЭТУ», Россия, Санкт-Петербург, ул. Политехническая, д. 22, лит. «Н»
[3] Санкт-Петербургский государственный университет гражданской авиации, Россия, Санкт-Петербург, ул. Пилотов, д. 38,
emails: beliaev@nicetu.spb.ru, ou@nicetu.spb.ru, psi_center@mail.ru, rubtsov.spb.guga@rambler.ru

***Аннотация*:** В статье рассматривается метод идентификации беспилотных воздушных судов для обеспечения безопасности полетов в населенных пунктах и на объектах транспортной инфраструктуры. Метод предполагает оснащение беспилотных воздушных судов приемо-передающими модулями, включающими SIM-карту и позволяющими производить идентификацию аппаратов в сетях мобильной связи. Проанализирована возможность внедрения данного метода в комплексных системах безопасности.

***Ключевые слова**: беспилотное воздушное судно; идентификация; безопасность полетов; объекты транспортной инфраструктуры.*

ABOUT THE METHOD OF UNMANNED AIRCRAFT IDENTIFICATION IN THE IMPLEMENTATION OF COMPLEX SAFETY SYSTEMS

Belyaev Sergey[1], Ostapchenko Yuriy[2], Kudryakov Sergey[3], Rubtsov Evgeny[3]
[1] The St. Petersburg State Electrotechnical University "LETI", Russia, St. Petersburg, Professor Popov str. 5,
[2] Research and Engineering Center of Saint-Petersburg Electro-Technical University JSC, Russia, St. Petersburg, Politechnicheskaya str. 22, building “N”
[3] Saint-Petersburg state University of civil aviation, Russia, St. Petersburg, Pilotov str. 38,
emails: beliaev@nicetu.spb.ru, ou@nicetu.spb.ru, psi_center@mail.ru, rubtsov.spb.guga@rambler.ru

Abstract: The article considers the method of unmanned aircraft identification for ensuring flight safety in the settlements and transport infrastructure. The method involves equipping an unmanned aircraft with receiving and transmitting modules, including a SIM card and enabling the identification vehicles within mobile networks. Possibility of implementing this method in complex safety systems is analyzed.

***Keywords**: unmanned aircraft; identification; flight safety; transport infrastructure.*

Введение. Развитие новых видов транспортных средств заставляет по-новому взглянуть на проблему обеспечения безопасности в населенных пунктах и на объектах транспортной инфраструктуры. Беспилотные воздушные суда (БВС) стали общедоступными, их характеристики (дальность и время полета, потолок, взлетный вес, полезная нагрузка) позволяют пользователям по неосторожности или со злым умыслом причинить огромный вред объектам транспортной инфраструктуры, а также самим транспортным средствам [1].

Для предотвращения катастроф и инцидентов, или уменьшения их количества целесообразно внедрять комплексные системы безопасности, подразумевающие сбор данных о всех элементах транспортной системы, прогноз на заданную глубину, обнаружение и разрешение конфликтных ситуаций. При постановке задачи сбора данных о беспилотных воздушных судах, становится очевидной проблема, связанная с их учетом, регистрацией и идентификацией. В рамках статьи предложен метод, позволяющий решить данную проблему.

Комплексные системы безопасности

Транспортная инфраструктура включает в себя объекты, большинство из которых выступает в качестве мест массового скопления людей, а, значит, существенно повышается уровень опасности и требует повышенного внимания от контролирующих органов и наличия развитой системы мониторинга ситуации, прогнозирования и разрешения конфликтных ситуаций. С этой точки зрения целесообразно на уровне города или значимого региона внедрять комплексные системы безопасности. При этом должно учитываться не только техническое состояние транспортной инфраструктуры, но и контролироваться транспортные и пассажирские потоки. Обобщённая структура комплексной системы безопасности приведена на рисунке 1 [2].

Комплексная система безопасности должна включать в себя непрерывный дистанционный мониторинг всех значимых объектов транспортной инфраструктуры, что позволит обеспечить надёжность зданий и сооружений, которые могут повлиять на безопасность контролируемого участка. Системы контроля и управления доступом обеспечивают контроль прохождения в различные учреждения и на территории, требующие повышенного внимания, такие как метрополитены, аэропорты, железнодорожные станции и т.п. Видеонаблюдение используется повсеместно, но классическое видеонаблюдение уже не справляется с огромными потоками информации, поэтому целесообразно использовать интеллектуальное видеонаблюдение, которое позволяет с одной стороны автоматизировать процесс выявления нарушений, с другой стороны обеспечить контроль гораздо большей территории одним оператором [2].

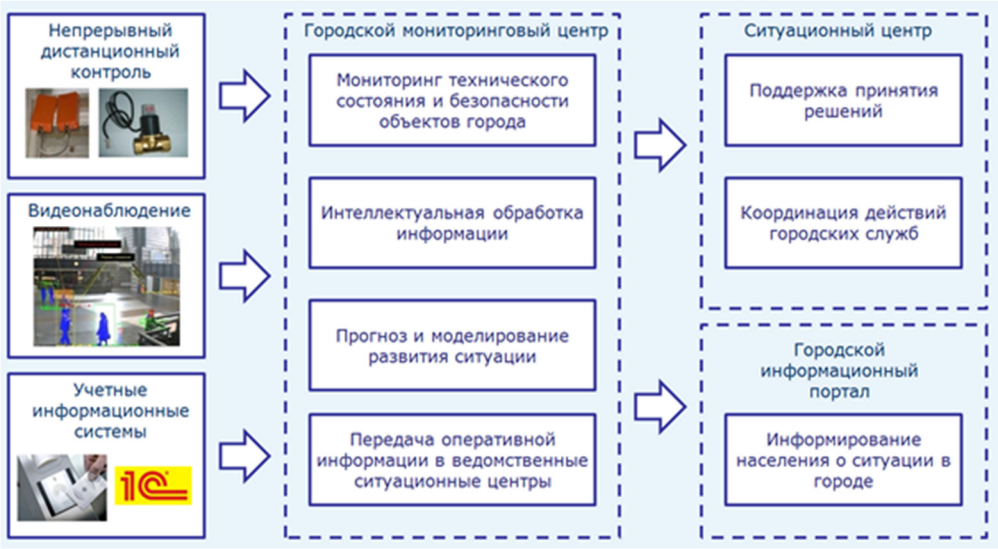


Рис. 1. Обобщенная структура комплексной системы безопасности

Информация, собираемая от источников в виде датчиков комплексов непрерывного дистанционного контроля, видеонаблюдения, систем контроля и управления доступом поступает в городской мониторинговый центр, который обеспечивает решение следующих ключевых задач [2]:

1) мониторинг технического состояния и безопасности объектов, благодаря чему обеспечивает контроль технического состояния транспортной инфраструктуры;

2) интеллектуальная обработка информации, благодаря чему с одной стороны уменьшается влияние человеческого фактора, с другой стороны появляется возможность в автоматическом режиме учитывать типовые ситуации, учитывать историю развития событий и прослеживать зависимости между различными ситуациями;

3) прогноз и моделирование развития ситуации, благодаря чему обеспечивается поддержка принятия управленческих решений;

4) передача оперативной информации в ведомственные ситуационные центры, что соответствует современным тенденциям по информационному взаимодействию с федеральными органами исполнительной власти.

Информация городского мониторингового центра поступает в ситуационный центр и городской информационный портал. На уровне ситуационного центра она используется для поддержки принятия решений и координации действий городских служб, на уровне информационного портала позволяет информировать население об опасных явлениях.

Мониторинг технического состояния и безопасности объектов города обеспечивает [2]:

– автоматическое получение информации от встроенных систем контроля технического состояния;

– допусковый контроль текущих значений критических параметров и анализ их изменения с автоматическим информированием (e-mail, sms) при превышении пороговых значений;

– прогнозирование технического состояния объекта и остаточного ресурса систем на заданный период времени;

– информирование о выявленных отклонениях в техническом состоянии объектов с формированием и выдачей рекомендаций для принятия решений;

– трехмерное моделирование объектов контроля с отображением текущего технического состояния;

– непрерывный и периодический мониторинг технического состояния объектов контроля на основе ультразвукового, тепловизионного, тензометрического и других методов контроля;

– системный анализ характера изменения всех контролируемых параметров с выдачей рекомендаций по возможному возникновению нештатных или аварийных ситуаций.

Техническая реализация мониторинга технического состояния включает в себя сбор информации от разнородных датчиков, предназначенных для контроля основных параметров, сохранение её в различные специализированные базы данных, репликацию с использованием адаптеров сопряжения, выгрузку с учётом существующих каналов связи и сбор в едином хранилище для предоставления к нему доступа в центре мониторинга.

Технология интеллектуальной обработки и анализа данных обеспечивает [2]:

– выявления зависимостей в данных (статистическая обработка и сегментация данных, выполнение многомерного анализа, распознавание образов, ассоциативный анализ);

– систематизацию информации об объектах с целью классификации их состояний;

– выявление нетипичного поведения объектов;

– поиск причин отклонения поведения объектов;

– сокращение объемов хранимых данных без потери информации.

Разработано большое количество методов и подходов, обеспечивающих интеллектуальную обработку информации, их корректное применение существенно зависит от конкретной решаемой задачи. В качестве основных источников данных могут выступать как модули непрерывного дистанционного мониторинга, так и комплексы видеонаблюдения, а также и другие информационные системы. Возможны различные варианты построения системы видеонаблюдения.

Диспетчерский центр, обеспечивающий, в том числе интеллектуальную обработку информации должен состоять из нескольких подсистем: ввода, администрирования, визуализации, диспетчеризации, анализа и базы данных. Служба безопасности с использованием подсистемы ввода выполняет редактирование профилей нарушителей, регламентов работы системы и регистрацию объектов наблюдений, с использованием подсистемы администрирования задаёт и контролирует права доступа. Старший диспетчер с использованием подсистемы визуализации управляет формами отображения, настраивает отображение на плане-схеме, просматривает историю событий. Диспетчер работает как с исходным видео, так и с результатами его обработки, сохранёнными в компонентах Service Desk. Непосредственный анализ информации выполняется в подсистеме анализа, при этом в качестве внешних источников используется не только видео, поступающее от видео- и телекамер, но и данные внешних информационных систем, которые могут включать в себя системы контроля и управления доступом, системы мониторинга технического состояния и других систем [2].

Разрабатываемые в настоящее время комплексные системы безопасности предназначены для работы с железнодорожным, автомобильным и авиационным транспортом. Широкое распространение беспилотных воздушных судов требует внесения срочных и кардинальных коррективов в структуру данных систем безопасности. Из-за малых размеров беспилотный аппарат довольно сложно обнаружить с помощью радиолокационных и оптических систем наблюдения, однако гораздо большей проблемой является отсутствие общепринятой и законодательной утвержденной системы учета, регистрации и идентификации БВС.

Метод идентификации беспилотных воздушных судов

Чрезвычайные происшествия на транспорте в России и за рубежом происходят по причинам, в большой степени обусловленным человеческим фактором. При этом к числу причин возникающих аварий и катастроф часто относятся не только прямые ошибки в деятельности персонала, но и общая тенденция к пренебрежению установленными правилами и инструкциями, а также правовой нигилизм.

В области беспилотной авиации проблему осложняет тот факт, что пользователями воздушного движения (внешними пилотами) становятся люди имеющие довольно слабую теоретическую и практическую подготовку, либо не имеющие такой подготовки. Беспилотное воздушное судно, управляемое неподготовленным оператором может потерять управление, выйти за пределы зоны действия радиотехнических средств станции внешнего пилота (в простейшем случае – пульта управления беспилотным аппаратом) и при выполнении маневра, заложенного в бортовой модуль автопилота, столкнуться со зданиями, сооружениями, транспортными средствами, либо упасть в местах массового скопления людей с соответствующими последствиями.

Для мониторинга беспилотных воздушных судов можно применять входящие в состав комплексных систем безопасности средства видеонаблюдения, в том числе интеллектуального видеонаблюдения. Однако, из-за малых размеров беспилотных аппаратов, дальность действия средств видеонаблюдения будет ограничена, особенно в сложных метеоусловиях. Возможно применение средств радио мониторинга, позволяющих отслеживать сеансы радиообмена между БВС и станцией внешнего пилота, но потребует внедрения дополнительных технических средств в

комплексную систему безопасности и приведет к увеличению как стоимости самой системы, так и стоимости обслуживания [3].

Воздушный кодекс Российской Федерации требует учета беспилотных воздушных судов массой от 250 г до 30 кг и государственной регистрации для БВС массой более 30 кг [4]. Процедуры учета и регистрации на законодательном уровне пока еще не оговорены, этим обстоятельством пользуется ряд компаний, выдающих сертификаты учета БВС на основе своих собственных правил.

При возникновении опасных ситуаций или предпосылок к опасным ситуациям, связанным с беспилотными воздушными судами, владелец имеет шанс уйти от ответственности по причине практической недоказуемости того, что беспилотный аппарат принадлежит именно ему. Беспилотные воздушные суда в настоящее время не имеют уникальных идентификаторов и в полете являются по сути обезличенными.

Решением перечисленных проблем может стать введение процедуры учета и регистрации БВС путем обязательной установки приемо-передающего модуля с SIM-картой оператора мобильной связи. Для получения SIM-карты пользователь должен предъявить документ удостоверяющий личность. Данные о владельце заносятся в базу данных, что в будущем позволит однозначно определить владельца БВС. Кроме того, предоставление паспортных данных имеет важный психологический аспект и повышает уровень ответственности пользователя беспилотного аппарата.

При выполнении полета беспилотное воздушное судно периодически или по запросу излучает сигнал содержащий уникальный номер, соответствующий данному аппарату, таким образом решается проблема идентификации БВС. По сравнению с визуальной идентификацией (по типу автомобильных номеров), идентификация с помощью SIM-карты имеет ряд:

1) возможность идентификации мини и микро аппаратов, плохо наблюдаемых визуально или с помощью средств видеонаблюдения;

2) стабильная работа в неблагоприятных метеоусловиях (туман, дождь);

3) возможность определения местоположения БВС при использовании имеющихся в мобильных сетях методах позиционирования абонентов;

4) применение существующей инфраструктуры средств мобильной связи, что позволит значительно снизить расходы на внедрение системы идентификации БВС.

Для реализации описанного метода идентификации БВС в комплексных системах безопасности необходимо обеспечить сопряжение с сетями мобильной связи, либо получить доступ к информации о положении абонентов-БВС, их передвижении и выполняемых полетах.

Заключение. Разрабатываемые в настоящее время комплексные системы безопасности несомненно позволят снизить риск катастроф и инцидентов. Для этого предполагается развернуть обширную сеть средств мониторинга, включающих интеллектуальное видеонаблюдение. Анализ собранных данных позволит производить прогноз, выявлять и разрешать конфликтные ситуации.

В то же время комплексные системы безопасности должны отвечать современным вызовам, выразившимся в лавинообразном росте числа беспилотных воздушных судов у населения. Новый вид транспорта требует применения дополнительных средств для обеспечения мониторинга обстановки.

Отмеченные в Воздушном кодексе процедуры учета и регистрации беспилотных воздушных судов рекомендуется дополнить требованием установки на борту беспилотных воздушных судов приемо-передающего модуля с SIM-картой. Оборудованные БВС можно легко и однозначно идентифицировать, а также определять их местоположение, используя штатные возможности позиционирования в мобильных сетях связи.

Внедрение метода идентификации с помощью SIM-карт позволит однозначно определять принадлежность беспилотного воздушного судна конкретному владельцу, что повысит уровень ответственности пользователей, а также заставит их более серьезно подходить к вопросу подготовки и проведения полетов.

СПИСОК ЛИТЕРАТУРЫ

1. Беспилотные авиационные системы. Учебное пособие / С.А. Кудряков, В.Р. Ткачев, Г.В. Трубников, В.И. Кисличенко // СПб.: Свое издательство. – 2015. – 121 с.
2. Опыт создания комплексных систем безопасности на объектах транспортной инфраструктуры / С.А. Беляев, Ю.Б. Остапченко, С.А. Кудряков, Е.Н. Шаповалов, М.Г. Павловский // Актуальные проблемы защиты и безопасности. Комплексная безопасность на транспорте. Труды XIX Всероссийской научно-практической конференции. Том 6. – 2016. – С. 52-57.
3. Радиотехническое обеспечение полетов воздушных судов и авиационная электросвязь. Учебное пособие / С.А. Кудряков, В.К. Кульчицкий, Н.В. Поваренкин, В.В. Пономарев, Е.А. Рубцов, Е.В. Соболев, Б.А. Сушкевич // СПб.: Свое издательство. – 2016. – 287 с.
4. Воздушный кодекс Российской Федерации: [федер. закон №60-ФЗ: принят Гос. Думой 19 фев. 1997 г.: ред. от 06.07.2016: с изм. и доп., вступ. в силу с 5.07.2017]. – 66 с.

ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК 681.324

ФУНКЦИОНАЛЬНАЯ НАДЕЖНОСТЬ И УСТОЙЧИВОСТЬ ВЫЧИСЛИТЕЛЬНОГО ПРОЦЕССА

Богатырев Владимир Анатольевич[1], Богатырев Станислав Владимирович[2]
[1]Санкт-Петербургский государственный экономический университет
Россия, Санкт-Петербург, ул. Садовая, д. 21
[2]Компания „Самсунг-Электроникс “,
Корея, Сеул, Сеочо-Гу, Сеочо 2-донг
e-mails:Vladimir.bogatyrev@gmail.com, realloc@gmail.com

***Аннотация*:** Проанализировано влияние на надежность и устойчивость вычислительного процесса интегрального влияния отказов и задержки обслуживания функциональных запросов

Ключевые слова: *надежность отказоустойчивость, задержки обслуживания*

FUNCTIONAL RELIABILITY AND STABILITY OF THE COMPUTATIONAL PROCESS

Vladimir Bogatyrev [1],Stanislav Bogatyrev[2]
[1]Saint-petersburg state university of economics
Russia, St. Petersburg, Sadovaya str. 21,
2.Samsung Electronics,
Korea. Seoul, Seocho-gu, Seongchon-gil 56, 2
e-mails:Vladimir.bogatyrev@gmail.com , realloc@gmail.com

Abstract: Analyzed the impact on the reliability and stability process the integrated impact of failures and latency functional queries

Keywords: *reliability, fault tolerance, latency*

Введение. Информационные системы и сети, как основа цифровой экономики [1,2], должны соответствовать высоким требованиям к безопасности устойчивости реализуемых бизнес процессов, в том числе в условиях сбоев, отказов и внешних деструктивных воздействий случайного или злонамеренного характера [1-4]. В связи с этим вычислительные системы должны обладать как структурной, так и функциональной надежностью, под которой подразумевают способность системы безошибочно выполнять предусмотренные функциональные задачи (функции) в условиях сбоев, ошибок и отказов, а также внешних деструктивных случайных или преднамеренных воздействий.

Надежность реализации вычислительного процесса, во многом зависит от организации реконфигурации, копирования данных, резервирования вычислений, балансировки загрузки узлов, мобильной динамической миграции ресурсов, распределения и перераспределения запросов.

Компьютерная система может рассматриваться как систем массового обслуживания, потери запросов в которых обусловливаются не только отказами и сбоями программно-аппаратных средств, но и недостаточностью или несбалансированностью ресурсов, а также перегрузками, приводящим к нестационарности функционирования, недопустимым задержкам или потерям запросов [4-5].

При обеспечении функциональной надежности систем ответственного назначения, в том числе систем реального времени в ряде случаев требуется поддержка своевременности и непрерывности вычислительного процесса, даже при условии отказов, реконфигурации и миграции информационных ресурсов и вычислений с отказавших на работоспособные узлы. Своевременность вычислений особенно значима при критичности задержек вычислений реального времени, когда условием отказа может быть не выполнение запроса к заданному моменту времени [4-6].

Устойчивость вычислительного процесса должна обеспечиваться не только при отказах компьютеров, но и при внешних деструктивных воздействиях, препятствующих корректной реализации вычислительного процесса, в том числе своевременности получения результатов.

Отказоустойчивость компьютерных и коммуникационных систем и сетей может быть структурной или функциональной.

Структурная отказоустойчивость подразумевает потенциальную готовность системы к сохранению работоспособности (к требуемому функционированию) после возникновения (накопления) отказов и реконфигурации аппаратно-программных средств. Структурная отказоустойчивость может достигаться реконфигурацией резервированной системы при ее возможной деградации,

проявляющейся в снижении качества функционирования и потере возможностей (ресурсов) по обеспечению надежности.

Под функциональной отказоустойчивостью понимается способность системы к своевременному, безошибочному, а возможно и непрерывному выполнению функциональных задач, в условиях возникновения сбоев, отказов и ошибок по внутренним или внешним причинам. При этом к внешним причинам, нарушающим устойчивость вычислительного процесса, могут быть отнесены злонамеренные или случайные природные или техногенные деструктивные воздействия [4-6].

Функциональная надежность подразумевает способность сохранения работоспособности по выполнению требуемых функций с учетом вероятностей возможных отказов, причем именно эти вероятности в основном определяет надежность наряду с организацией противодействия отказам в результате восстановления или реконфигурации (самовосстановления). Функциональная отказоустойчивость – включает только адаптацию к отказам на основе самовосстановления и при ее оценке не должно учитываться вероятность возникновения отказов, а только способность их парирования. Таким образом, понятие функциональная надежность является более общим и включает отказоустойчивость как одно из решений по сохранению непрерывности вычислительного процесса после возникновения отказов .

К деструктивным воздействиям, приводящим к отказу выполнения функций из-за нарушений своевременности обслуживания потока запросов сервером, могут быть отнесены преднамеренные атаки или случайные воздействия, вызывающие увеличении интенсивности запросов к ресурсам.

При поддержке функциональной отказоустойчивости компьютерной системы к ней могут предъявляться требования обеспечения устойчивости вычислительного процесса или сохранения при накоплении отказов готовности к выполнению требуемого набора функций.

В первом случае устойчивость функционирования может достигаться миграцией вычислительного процесса, прерванного отказом, на исправные узлы системы, возможно в идеале при обеспечении непрерывности восстанавливаемого процесса. Под непрерывностью вычислительного процесса понимается возможность продолжения его выполнения после отказа без нарушения выдачи результатов в требуемые моменты времени.

Сохранение устойчивости вычислительного процесса может поддерживаться на основе технологии виртуализации и миграции виртуальных вычислительных машин или иных необходимых для выполнения функций ресурсов. Поддержка отказоустойчивости вычислительного процесса может сопровождаться реконфигурацией системы или достигаться на основе предоставления требуемых для реализации процесса ресурсов другими узлами системы по запросам перераспределяемым через сеть. Восстановление вычислительного процесса после отказов при сохранении его непрерывности возможно при занесении результатов в памяти, одновременно доступной для отказавшего компьютера и компьютера, выделяемого для возобновления прерванного отказами вычислительного процесса.

Отказоустойчивость вычислительного процесса достигается при его резервированном выполнении на разных узлах системы. Резервирование вычислительного процесса обеспечивает его непрерывность при условии успешного реализации хотя бы одной резервной копии вычислительного процесса. Условием успешности выполнения копии вычислительного процесса является безотказность и безошибочность всех узлов, задействованных при ее реализации.

Отказоустойчивость по сохранению набора требуемых функций, допускает возможность после отказа потерю запроса или его результатов . Допустимость потери функциональных возможностей или снижения качества предоставляемых услуг [4-7] обусловливается особенностями реализуемых прикладных задач [8-12].

Заключение. Таким образом обоснование выбора проектных решений требует формирование комплексных показателей эффективности и надежности, отражающих не только способность структуры к сохранению функционирования в условиях отказов, но и возможность своевременного и безошибочного обслуживания запросов в условиях помех, отказов, временных отключений ресурсов, изменений интенсивности входного потока запросов, в том числе в результате злонамеренных воздействий.

СПИСОК ЛИТЕРАТУРЫ

1. Советов Б. Я. Колбанёв, М. О., Татарникова Т. М. Технологии инфокоммуникации и их роль в обеспечении информационной безопасности //Геополитика и безопасность. -2014.-№ 1(25). -С. 69-77.
2. Колбанёв М. О., Коршунов И. Л., Левкин И. М., Микадзе С. Ю. К вопросу информационно-экономической безопасности//Геополитика и безопасность. 2015. Т. 31, № 3. С. 87-91.
3. Емельянов А. А., Коршунов И. Л. Опыт реализации политики информационной безопасности на предприятии малого бизнеса в целях обеспечения информационно-экономической безопасности// ИБРР-2015. 2015. С. 213-214
4. Богатырев В. А. Информационные системы и технологии. Теория надежности. М.: Юрайт, 2016. 318 с.
5. Богатырев В.А., Богатырев А.В. Модель резервированного обслуживания запросов реального времени в компьютерном кластере // Информационные технологии -2016. - Т. 22. - № 5. - С. 348-355
6. Bogatyrev V.A., Bogatyrev A.V, “Functional reliability of a real-time redundant computational process in cluster architecture systems”, *Automatic Control and Computer Sciences*, vol. 49, No. 1, 2015, pp. 46-56
7. Татарникова Т. М. Структурный синтез центра сопряжения корпоративных сетей // Информационно-управляющие системы. – 2015. № 3(76). – С. 92-98.

8. Пуха Г.П., Попов П.В., Драчев Р.В., Попцова Н.А. Построение системы интеллектуальной поддержки принятия решений по организации услуг мобильной связи. – Изв. Вузов. Приборостроение. 2014. Т. 57. № 9. С. 70-75
9. Н. А. Верзун, М. О. Колбанев, Т. М. Татарникова Технологическая платформа четвертой промышленной революции // Геополитика и безопасность. – 2016. – № 2 (34). – С. 73–78.
10. Богатырев В.А., Богатырев С.В. Резервированная передача данных через агрегированные каналы в сети реального времени // Известия высших учебных заведений. Приборостроение - 2016. - Т. 59. - № 9. - С. 735-740
11. Гатчин Ю. А., Жаринов И. О., Коробейников А. Г. Математические модели оценки инфраструктуры системы защиты информации на предприятии // Науч.-техн. вестник ИТМО. 2012. № 2(78). С. 92 – 95.
12. Емельянов А.А. Оценка затрат на системы информационно-экономической безопасности / А.А.Емельянов, И.Л.Коршунов // Технологии информационно-экономической безопасности: сб. статей сотр. каф. ИС и Т. – СПб.: Изд-во СПбГЭУ, 2016. – С.63–69

УДК 53.087.92

АНАЛИЗ ОБЛАСТЕЙ ПРИМЕНЕНИЯ АРОМОСЕНСОРНЫХ СИСТЕМ БЕЗОПАСНОСТИ

Дмитрий Сергеевич Афанасьев[1], Елена Андреевна Бардакова[2], Денис Сергеевич Быстряков[1]
[1]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
[2]Санкт-Петербургский государственный экономический университет
Россия, Санкт-Петербург, ул. Садовая, д. 21
emails: dmitr-afanas@yandex.ru, bardakova.elena95@mail.ru, bystryakov.denis@gmail.com

***Аннотация*:** В статье предлагается организовать мониторинг аромобезопасности пространства при помощи аромосенсорных систем и сетей терминалов запахов. Аромобезопасность – отсутствие в пределах жизненного пространства запахов (летучих веществ), которые указывали бы на возможность возникновения событий, несущих опасность для человека или группы людей. Показано, что подход позволяет создавать эффективные системы для обеспечения безопасности жизненного пространства, защиты от техногенных процессов и социальных взаимодействий, обусловленных терроризмом, алкоголизмом, наркоманией и др. факторами.

***Ключевые слова**: Аромобезопасность; датчики запахов; электронный нос; интернет вещей; сенсорные сети; обработка данных; облачные вычисления.*

ANALYSIS OF AROMOSENSOR APPLICATION AREAS SYSTEMS OF SAFETY

Dmitry Afanasiev[1], Elena Bardakova[2], Denis Bystryakov[1]
[1] The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
[2] St. Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str. 21
emails: dmitr-afanas@yandex.ru, bardakova.elena95@mail.ru, bystryakov.denis@gmail.com

Abstract: The article is proposed to organize space aromosecurity monitoring by means of aromosensor systems and smell terminal networks. Aromosecurity stands for the absence of smells (volatile substances), indicating the likelihood of events that pose a threat to a person or a group of people within the vital space. It was demonstrated that the approach allows creating effective systems for ensuring vital space security, protection against man-caused processes and social interactions caused by terrorism, alcoholism, drug addiction and other factors.

Key words: Aromosecurity, sensors of smells, electronic nose, Internet of things, sensor networks, data handling, cloud computing.

Введение. Практическим инструментом движения России к цифровой экономике является Национальная технологическая инициатива. НТИ – это долгосрочная комплексная программа по созданию условий для обеспечения лидерства российских компаний на новых высокотехнологичных рынках, которые будут определять структуру мировой экономики в ближайшие 15–20 лет.

Согласно одному из принципов, которые лежат в основе выбора рынков будущего – рынок должен представлять собой [1-3]:

– сеть, которая содержит сенсорные поля, измеряющие физические характеристики жизненного пространства,

– логический уровень, на котором, при помощи телекоммуникационных технологий данные с сенсоров объединяются в облачных хранилищах,

– уровень сервиса, на котором при помощи специального программного обеспечения осуществляется обработка, анализ собранных данных и вырабатываются управляющие воздействия.

Одним из типов сенсоров такого рода могут служить сенсоры запахов [4-5]. Они способны преобразовать в цифровой вид любые запахи, возникающие в пространстве. Характеристики сенсоров все время улучшаются так, что они становятся все дешевле, могут работать автономно продолжительное время и регистрировать концентрации в долях ppm.

Безопасность одна из главных проблем современности. На сегодняшний день актуальна защита от внешних угроз безопасности. Одним из возможных решений данной проблемы является разработка аромосенсорных систем.

Система строится на трех уровнях [6]:

– физический уровень – терминалы запахов;

– логический уровень – сеть терминалов, реализованная при; помощи технологий мобильного доступа и интернета вещей;

– когнитивный уровень - протоколы взаимодействия с пользователями при помощи технологий третьей платформы информатизации.

На физическом уровне [7-8] датчики преобразуют летучие вещества, образующие запах, в электромагнитные сигналы, передаваемые на логический уровень системы. На логическом уровне реализуется управление группой терминалов запахов и контроль их технического состояния, а именно сбор сигналов, поступающих от датчиков, их предварительная обработка и передача на интеллектуальный уровень. На когнитивном уровне накапливаются сообщения логического уровня, реализуется анализ результатов мониторинга аромобезопасности и взаимодействие с пользователем.

Целью всех аромосистем является обеспечение безопасности человеческой жизни и контроль состояния среды обитания.

Рассмотрим области применения аромосенсорных систем.

Одной из самых главных проблем в наше время является террор. Существуют сенсоры, способные регистрировать тротил, тринитрофенол, гексоген, октоген и другие вещества. Эти сенсоры будут основой аромосистемы. Объектами применения данных сенсорных аромосистем могут быть места потенциально большого скопления людей, такие как аэропорты, ЖД и авто - вокзалы, концертные и театральные залы и площадки, торгово-развлекательные центры, комплексы и конференц-залы, образовательные учреждения. Эффективнее устанавливать датчики обнаружения опасных веществ в следующие места: лифты, входы и выходы, контрольно-пропускные пункты.

Следующей немаловажной сферой применения систем является контроль производственных процессов. К данной группе относятся сенсорные поля, регистрирующие аммиак, сернистый ангидрид, фосген, окись этилена, сероуглерод, бензол и другие. В России на 2014 год Ростехнадзором зарегистрировано 190 000 опасных производственных объектов и более 463 000 предприятий различного вида экономической деятельности (добыча полезных ископаемых, обрабатывающие производства, производство и распределение электроэнергии, газа и воды). На всех этих объектах установка аромосенсорных систем приведет к обеспечению безопасности, предотвращению аварий и чрезвычайных ситуаций.

Еще одной важной сферой применения аромосенсорных систем является контроль социальных взаимодействий. На сегодняшний день на рынке представлено большое количество сенсоров этанола, способных улавливать разные степени концентрации паров спирта в воздухе. Также стоит отметить сенсоры, регистрирующие запахи наркотических веществ.

Две основные области применения сенсоров такого типа:

– Контроль трезвости сотрудников, занимающих должности с большой долей ответственности принимаемых решений и значительной степенью их влияния;

– Запрет употребления алкогольных и наркотических веществ в общественных местах.

К первому пункту можно отнести предприятия с опасным производством (химические опасные объекты, добыча нефти, бурение, металлургия, мебельные фабрики). Также к этому пункту относится мониторинг рабочих мест (помещений) органов исполнительной власти, осуществляющих надзор и контроль в области гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера, обеспечения пожарной безопасности и безопасности людей на водных объектах.

Ко второму - контроль отсутствия алкогольных и наркотических веществ в образовательных организациях (детских садах, школах, ВУЗах), концертных и театральных залах, торгово-развлекательных центрах.

Следующей сферой является контроль бытовых газов. К этой группе относится регистрация запаха метана, угарного газа, горючих веществ. По данным «Росгазификации», в жилом секторе за последние пять лет ежегодно происходит около 230 происшествий, связанных с использованием газа в быту. При этом погибает в среднем 130 человек. Таким образом, современная защита от таких ситуаций неэффективна и необходимо использовать системы обеспечения безопасности нового поколения, например, предоставить эту задачу аромосистемам.

Обширной сферой применения систем аромобезопасности является экологический мониторинг. К ней относятся сенсоры, регистрирующие параметры смога в больших городах, запахи, возникающие вследствие вредных выбросов на химических производствах. К основным загрязнителям атмосферы относятся углекислый газ, оксид углерода, диоксиды серы и азота, способные оказывать влияние на температурный режим тропосферы. Важно, что все элементы атмосферы осаждаются на почву, попадают в воду и на растения, что негативно сказывается на урожае, выращенном в черте крупного города, на качество водных ресурсов. Одна только строительная промышленность ежегодно

выбрасывает в воздух более 3 млрд. тонн пыли, цемента, которые, смешиваясь с дымом, сажей и ядовитыми веществами химической промышленности, образуют канцерогенную смесь, которой нам приходится дышать.

Увеличение содержания метана в атмосфере способствует усилению парникового эффекта, также изменяются химические процессы в атмосфере, что может привести к ухудшению экологической ситуации на Земле.

Кроме того, всем нам известей огромный объем негативных последствий после лесных и торфяных пожаров. Его можно значительно сократить посредством использования аромосистем.

Таким образом, загрязнения промышленными выбросами оказывают вредное воздействие на людей, животных, растения, здания и всю окружающую среду. Существуют нормы ПДК (предельно допустимые концентрации) веществ в воздухе, за которыми должны следить специальные органы, например, лаборатория загрязнения окружающей среды, и принимать какие-либо меры: от штрафа до закрытия предприятия.

Эффективнее с этой задачей могут справиться системы аромобезопасности, оснащенные различными сенсорами.

Одна из главных потребностей человека – воздух, а именно чистый воздух. Необходимы системы контроля качества воздуха, которые регистрируют недопустимые концентраций углекислых газов в офисных, образовательных, жилых и др. помещениях.

Далее приведены примеры ситуаций, когда эффективно использовать системы для оценки качества воздуха:

Во-первых, анализ состояния качества продуктов питания, анализируя воздух в холодильной камере, подача сигнала по истечению срока годности некоторых продуктов.

Во-вторых, заправочные станции для различных видов средств передвижения следует оборудовать сенсорными сетями для сигнала разлива топлива, содержания опасных веществ и дыма на их территории.

Кроме того, можно разработать устройства, обнаруживающие определенные аллергены в воздухе для человека, страдающего повышенной чувствительностью к некоторым веществам, вызывающим болезненное состояние.

Разработка сенсорных систем имеет огромный потенциал, так как на рынке представлено большое количество отдельно функционирующих устройств с сенсорами запахов, но не имеющих связи с интернетом и другими устройствами. Не смотря на то, что Интернет вещей стремительно развивается, 99% объектов физического мира к Интернету еще не подключены. На сегодняшний день существует ограниченное количество полномасштабных систем личной безопасности, которые, в свою очередь, имеют большую стоимость, соответственно далеко не каждый имеет возможность ее приобрести. В ближайшее несколько лет ожидается снижение цен на устройства, с одновременным ростом производительности, также, на смену персональным компьютерам приходят смартфоны и планшеты, стремительно развивается высокоскоростной беспроводной и мобильный интернет. Все эти факторы способствуют быстрому росту Интернета вещей.

Заключение. Подводя итоги, можно сказать, что системы контроля различных запахов необходимы обществу, потому что безопасность на сегодняшний день одна из ключевых проблем, которую можно эффективно решить посредством разработки различных сенсорных систем аромобезопасности, тем более для этого существуют все необходимые условия.

СПИСОК ЛИТЕРАТУРЫ

1. Афанасьев Д. С., Быстряков Д. С., Колбанёв М. О. Принципы построения системы аромобезопасности // Информационные технологии и телекоммуникации. 2016. Том 4. № 4. С. 97–103.
2. Колбанёв М.О., Татарникова Т.М. Информационный объем базовых информационных процессов // Информационно-управляющие системы. – СПб.: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2014. С.42–47.
3. Быстряков Д.С., Ипатов О.С., Колбанёв М.О. Система аромобезопасности // Технологии информационно-экономической безопасности: сборник статей сотрудников кафедры ИСиТ. – СПб.: Изд-во СПбГЭУ, 2016. С.16–22.
4. Афанасьев Д. С., Бардакова Е. А., Быстряков Д. С. Аналитический обзор датчиков летучих веществ для интернета вещей // Информационные технологии и телекоммуникации. 2016. Том 4. № 4. С. 1–12.
5. Газовые датчики и сенсоры // Портал www.gassensor.ru [Электронный ресурс]. URL: http://www.gassensor.ru/ru/sensors (дата обращения: 11.09.2017).
6. Быстряков Д.С., Колбанёв М.О., Цехановский В.В. Архитектура сетецентрической системы мониторинга аромобезопасности жизненного пространства // XX Международная конференция по мягким вычислениям и измерениям (SCM-2017). Сборник докладов в 2-х томах. Санкт-Петербург. 24-26 мая 2017 г. Т.2. – С.293–296.
7. D. S. Bystryakov; M. O. Kolbanev; V. V. Tsehanovsky. Architecture of a network-centric vital space aromosecurity monitoring system. 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM). Year: 2017. Pages: 648–650. IEEE Conference Publications.
8. Афанасьев Д.С., Колбанёв М.О., Цехановский В.В. Физический уровень системы мониторинга аромобезопасности // XX Международная конференция по мягким вычислениям и измерениям (SCM-2017). Сборник докладов в 2-х томах. Санкт-Петербург. 24-26 мая 2017 г. Т.2. – С.297–300.

УДК 681.324

ОПТИМИЗАЦИЯ ПЕРИОДИЧНОСТЬ ТЕСТОВОГО КОНТРОЛЯ ПРИ ОБЕСПЕЧЕНИИ ГОТОВНОСТИ СИСТЕМЫ К БЕЗОПАСНОМУ ФУНКЦИОНИРОВАНИЮ

Богатырев Владимир Анатольевич[1], Богатырев Станислав Владимирович[2]
[1.]Санкт-Петербургский государственный экономический университет
Россия, Санкт-Петербург, ул. Садовая, д. 21.,
[2]Компания „Самсунг-Электроникс “,
Корея, Сеул, Сеочо-Гу, Сеочо 2-донг
emails:Vladimir.bogatyrev@gmail.com, realloc@gmail.com

***Аннотация*:** Для компьютерных систем, наделенных средства оперативного и тестового контроля, предложена постановка и решение задачи оптимизации периодичности тестового контроля с учетом возможности не обнаружения нарушений функционирования во время тестирования. Оптимизация проводится с целью обеспечения максимума готовности к безопасному функционированию системы

***Ключевые слова:** тестирование, контроль безопасность готовность, оптимизация.*

OPTIMIZATION OF THE FREQUENCY OF THE TEST CONTROL, WHILE ENSURING THE SYSTEM'S READINESS FOR SAFE OPERATION

Vladimir Bogatyrev [1],Stanislav Bogatyrev[2]
[1.]Saint-petersburg state university of economics
Russia, St. Petersburg, Sadovaya str. 21,
[2.]Samsung Electronics,
Korea. Seoul, Seocho-gu, Seongchon-gil 56, 2
emails:Vladimir.bogatyrev@gmail.com, realloc@gmail.com

Abstract: For computer systems, possess the means of operational and test monitoring, the proposed formulation and solution of the problem of optimizing the periodicity of the test control with the possibility of not detecting malfunctions during testing. Optimization is conducted to maximize readiness for safe operation of the system

***Key words:** testing, control, security readiness, optimization.*

Введение. Эффективность экономической деятельности предприятий во многом определяется безопасностью и эффективностью ее инфрокоммуникационной инфраструктуры [1-4]. Безопасность, надежность, эффективность [5-10] и устойчивость функционирования компьютерных систем [11–13] различного прикладного назначения [14, 17] во многом определяется организацией вычислительного процесса [18,19] контроля их функционирования и процесса обслуживания и восстановления после отказов. Снижение безопасност компьютерных систем, как правило, связана с необнаружением средствами контроля отказов или нарушений защищенности в результате деструктивных воздействий. Устойчивости и безопасность функционирования компьютерных систем поддерживается средствами оперативного и тестового контроля. Эффективность обнаружения нарушений в системе во многом определяется полнотой оперативного контроля и периодичностью тестового контроля, задание которой связана с необходимостью разрешения технического противоречия, так как увеличение частоты тестирования приводит к повышению безопасности при снижении готовности системы из-за ее простоев при тестировании [20–21]. Таким образом, для защищенных информационных систем с целью повышения их готовности к безопасному обслуживанию запросов возникает потребность определения оптимальных интервалов тестирования.

Объект исследования компьютерная система, содержащая средства оперативного и тестового контроля. В [20–21] предложены Марковские модели компьютерных систем, позволяющий найти периодичность контроля, при которой достигается максимум готовности системы к безопасному обслуживанию потока запросов. Модели [20–21] предполагают идеальность тестового контроля и не отражают возможность не обнаружения отказа во время тестирования, например, если, отказывает уже протестированное оборудование.

Цель работы – определение оптимальных интервалов инициализации тестирования, обеспечивающих максимум готовности системы к безопасному функционированию с учетом возможности не обнаружения отказов во время тестирования. При тестировании будем считать, что средства оперативного контроля отключены.

Граф состояний и переходов Марковской модели, исследуемой компьютерной системы представлен на рис. 1, на котором выделены состояния: готовности системы к безопасному выполнению запросов (вероятность состояния P0); тестирования в отсутствии нарушений функционирования (P1); восстановления безопасной работоспособности (P2); необнаруженных нарушений и (P3); тестирования при наличии необнаруженных нарушений функциональности (P4).

Состояние необнаруженных нарушений функциональности является опасным. Состояния восстановления и тестирования соответствуют простоям системы.

По графу на рис. 1 для определения вероятностей состояний в установившимся режиме составляется система уравнений Колмогорова–Чепмена как:

$$-(\lambda 0+\lambda)\cdot P0+\mu 10\cdot P1+\mu P2=0,$$
$$-(\mu 10+\mu 12+\mu 13)P1+\lambda 0\cdot P0=0,$$
$$-\mu\cdot P2+g\cdot\lambda\cdot P0+\mu 12\cdot P1+g\cdot\lambda\cdot P3+\mu 42\cdot P4=0,$$
$$(g\cdot\lambda+\lambda 0)\cdot P3+(1-g)\lambda\cdot P0+\mu 13\cdot P1=0,$$
$$P0+P1+P2+P3+P4=1,$$

где g – доля оборудования, охватываемая средствами оперативного контроля (вероятность обнаружения нарушений при оперативном контроле), $\lambda,\lambda 0$ интенсивности отказов и инициализации тестового контроля, μ интенсивность восстановления работоспособности после обнаружения нарушений функционирования, а $\mu 0$ интенсивность тестирования (обратная величина среднему времени тестирования). Вероятности перехода между состояниями графа по рис.1 определяются как

$$\mu 10=\mu 0e^{-\lambda/\mu 0},$$
$$\mu 12=\mu 13=0,5\cdot\mu 0\cdot(1-e^{-\lambda/\mu 0}).$$

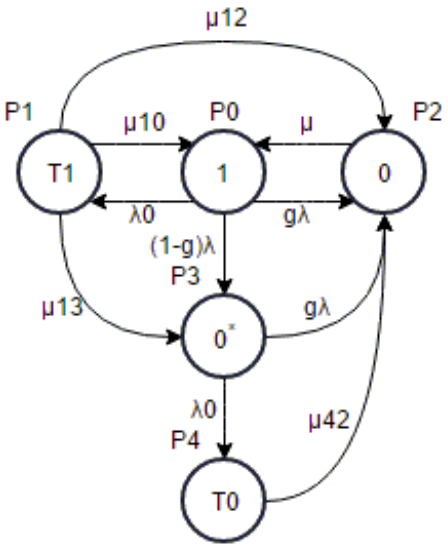


Рис. 1. Граф состояний и переходов системы

При проектировании защищенных компьютерных системы может ставиться задача нахождения интервалов инициализации тестирования, при которых находится максимум вероятности состояния готовности к безопасному функционированию (P0). Решение задачи оптимизации проведено при использовании встроенных средств системы компьютерной математики MathCAD 15, включая средства символьной математики решения систем алгебраических уравнений.

Оптимизация интервалов тестирования связана с техническим противоречием достижения максимума готовности системы и минимума вероятности ее опасных состояний.

В качестве критерия при разрешении указанного противоречия воспользуемся критерием – прибыль от обслуживания запросов [20]. Будем считать, что каждый запрос, поступающий в состоянии готовности системы к его безопасному выполнению, обеспечивает прибыль s0, а в состоянии простоя прибыль s1 (s1<s0, что обусловлено дополнительными задержками по завершению тестирования и (или) восстановления системы после обнаружения ее нарушений). Запрос, поступающий в опасном состоянии необнаруженных нарушений функционирования, приводит к убыткам (штрафу) – s3. Таким образом, математическое ожидание прибыли от обслуживания запроса вычисляется как:

$$S=s_0P_0-s_3P_3+s_1(1-P_0-P_3).$$

Результаты расчета зависимости вероятности готовности к безопасному функционированию от интенсивности инициализации тестирования представлены на рис. 2, на котором кривые 1,2.3 соответствуют интенсивности тестирования μ0= 1; 0,6; 0,3. Результаты расчетов подтверждают существование оптимальной интенсивности инициализации тестирования, причем с возрастанием интенсивности тестирования оптимальная интенсивность инициализации тестирования увеличивается.

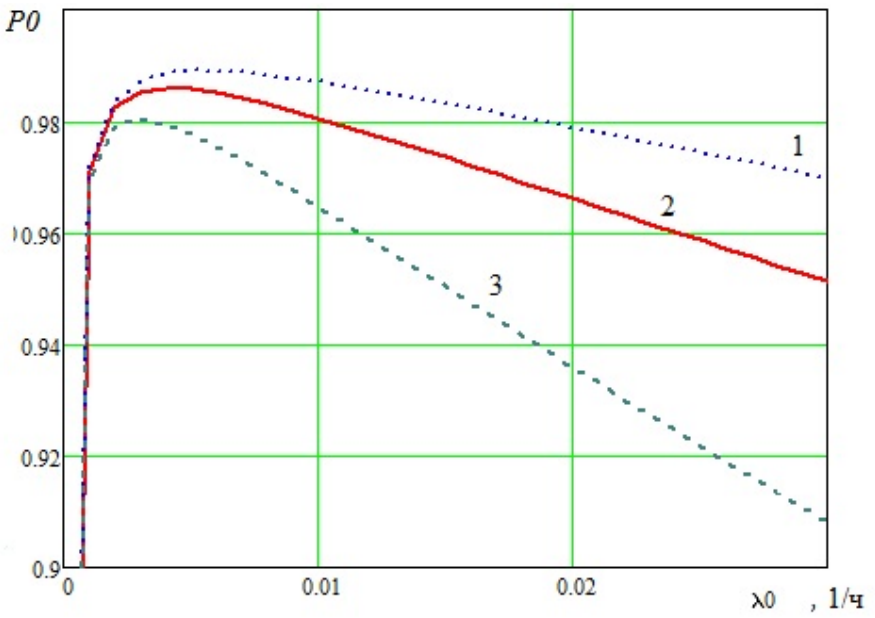


Рис.2. Готовности к безопасному функционированию системы

Заключение. Таким образом, предложена Марковская модель вычислительной системы с реализацией оперативного и тестового контроля, позволяющая проанализировать влияние периодичности инициализации тестового контроля на эффективность обслуживания потока запросов и готовность системы к безопасному выполнению требуемых функций.

Показано существование оптимальной периодичности тестового контроля, при которой достигается максимума вероятности готовности системы к безопасному выполнению требуемых функций.

СПИСОК ЛИТЕРАТУРЫ

1. Максимцев И.А. О технологических основаниях новой доктрины информационной безопасности Российской Федерации/И. А. Максимцев, М. О. Колбанёв, И. Л. Коршунов, И. М. Левкин, С. Ю. Микадзе//Новые горизонты глобального мира: сб. научн. тр./Балт. Гос. Техн. ун-т. СПб. -2015. -С. 270-281.
2. Воробьёв А.И., Колбанёв М.О., Татарникова Т.М. Оценка вероятностно-временных характеристик процесса предоставления информационно-справочных услуг //. Известия высших учебных заведений. Приборостроение. 2014. т. 57. № 9. С. 15-18.
3. Коршунов И.Л. Состояние и концепция развития информационных технологий в сфере сервиса//Известия высших учебных заведений. Приборостроение. 2014. т. 57. № 9. с. 7-10
4. Советов Б. Я. Технологии инфокоммуникации и их роль в обеспечении информационной безопасности // Б. Я. Советов, М. О. Колбанёв, Т. М. Татарникова // Геополитика и безопасность.- 2014. - №1(25).- С.69-77.
5. Гатчин Ю. А., Жаринов И. О., Коробейников А. Г. Математические модели оценки инфраструктуры системы защиты информации на предприятии // Науч.-техн. вестник ИТМО. 2012. № 2(78). С. 92 – 95.
6. Korobeynikov A.G., Fedosovsky M.E., Maltseva N.K., Baranova O.V., Zharinov I.O., Gurjanov A.V., Zharinov O.O. Use of information technologies in design and production activities of instrument-making plants. Indian Journal of Science and Technology2016. Vol. 9, no. 44, art. 104708
7. Верзун Н. А. Технологическая платформа четвертой промышленной революции / Н. А. Верзун, М. О. Колбанев, Т. М. Татарникова // Геополитика и безопасность. – 2016. – № 2 (34). – С. 73–78.
8. Богатырев В.А., Богатырев С.В. Резервированная передача данных через агрегированные каналы в сети реального времени // Известия высших учебных заведений. Приборостроение - 2016. - Т. 59. - № 9. - С. 735-740
9. Богатырев В.А. Оптимальное резервирование системы разнородных серверов // Приборы и системы , управление. Контроль,диагностика. 2007 № 12 С 30-36
10. Алиев Т.И. Основы моделирования дискретных систем: Учебное пособие. – СПб: СПбГУ ИТМО. – 2009. – 363 с.
11. Емельянов А.А. Оценка затрат на системы информационно-экономической безопасности / А.А.Емельянов, И.Л.Коршунов // Технологии информационно-экономической безопасности: сб. статей сотр. каф. ИС и Т. – СПб.: Изд-во СПбГЭУ, 2016. – С.63–69.
12. Пуха Г.П. Методология формирования и реализации систем интеллектуальной поддержки принятия решений. СПб.: СМИО-Пресс, 2012
13. Татарникова Т.М. Задача синтеза комплексной системы защиты информации в ГИС//Ученые записки Российского государственного гидрометеорологического университета. 2013. № 30. С. 204-211.
14. Кутузов О.И., Татарникова Т.М. Из практики применения метода Монте-Карло//Заводская лаборатория. Диагностика материалов. 2017. Т. 83. №3. С. 65-70.
15. 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. Санкт-Петербург, 2015. С. 310-312
16. Левкин И.М., Галкова Е.А.Математическое описание динамической среды угроз информационной безопасности // Национальная безопасность и стратегическое планирование. 2014. № 1 (5). С. 46-53
17. Головкин Ю.Б., Гусаренко А.С. Применение нечетких гиперграфов в моделях генерации web-компонентов // Изв. Вузов. Приборостроение.2014.Т.57. №9.С.47-53.
18. Гатчин Ю.А., Жаринов И.О. Основы проектирования вычислительных систем интегрированной модульной авионики: монография. М.: Машиностроение, 2010. 224 с.

19. Aleksanin S.A., Zharinov I.O., Korobeynikov A.G., Perezyabov O.A., Zharinov O.O Evaluation of chromaticity coordinate shifts for visually perceived image in terms of exposure to external illuminance// ARPN Journal of Engineering and Applied Sciences. 2015. Т. 10. № 17. С. 7494-7501
20. Богатырев В.А., Богатырев А.В. Оптимизация периодичности контроля защищенности компьютерных систем // Научно-технический вестник информационных технологий, механики и оптики - 2015. - Т. 15. - № 2(96). - С. 300-304
21. Богатырев В.А., Богатырев А.В., Богатырев С.В. Оптимизация интервалов проверки информационной безопасности систем // Научно-технический вестник информационных технологий, механики и оптики - 2014. - № 5(93). - С. 119-125

УДК 004.75

МОДЕЛЬ ДОСТУПА СЕНСОРНЫХ УСТРОЙСТВ В «ТУМАННЫХ ВЫЧИСЛЕНИЯХ» ИНТЕРНЕТА ВЕЩЕЙ

Елизаров Максим Андреевич
Санкт-Петербургский государственный экономический университет
Россия, Санкт-Петербург, ул Садовая, д 21,
emails: elizarovmaks@gmail.com

Аннотация: В статье предложена модель оценки времени получения доступа сенсорных устройств к центральному узлу «туманных вычислений» Интернета вещей.

***Ключевые слова*:** *Интернет вещей, «туманные вычисления», доступ к центральному узлу, время доступа, моделирование, нагрузка.*

MODEL ACCESS TO THE TOUCH DEVICES IN THE "FOG COMPUTING" OF IOT

Elizarov Maksim
Saint-Petersburg State University of Economics
Russia, St. Petersburg, Sadovaya str, 21,
emails: elizarovmaks@gmail.com

Abstract: The article proposes a model for estimating the access time of sensory devices to the central node of IoT "Fog Computing ".

Keywords: *Internet of things, “Fog Computing”, access to the central node, data transfer time, simulation, load.*

Введение. Интернет вещей (Internet of Things, IoT) представляет собой совокупность разнообразных сенсорных устройств (СУ), объединенных в сеть посредством доступных каналов связи, использующих ZigBee, Wi-Fi, Bluetooth и другие протоколы беспроводной связи малой зоны действия для взаимодействия между собой и IP-протокол для доступа в глобальную сеть Интернет [1, с.45].

Интернетом вещей могут решаться сложные задачи, которые требуют значительных вычислительных ресурсов, реализуемые облачными технологиями. Облачные технологии разделяются на две:

- облачные вычисления (Cloud Computing),
- туманные вычисления (Fog Computing).

Облачные вычисления – это модель обеспечения удобного сетевого доступа по требованию к некоторому общему фонду конфигурируемых вычислительных ресурсов. Облачные вычисления реализуются сетевой инфраструктурой центров обработки данных [2, 178].

Туманные вычисления – это разновидность облачных сервисов, расположенных не в «облаке», а в окружающей среде и реализуются локальными сетями, из которых интегрируется Интернет вещей [3, с17]. Концепция туманных вычислений предполагает децентрализацию обработки данных за счет передачи части работы по обработке данных с «облака» непосредственно вычислительным ресурсам локальной сенсорной сети – «туману».

Данные, поступающие от разных СУ в «туманных вычислениях» агрегируются на шлюзе для дальнейшей передачи на сервер. В связи с этим, необходимо учитывать возможность одновременной передачи данных сразу от нескольких СУ. Управляющая программа сервера должна распознавать и устранять такую ситуацию [4, с. 152]. В статье предлагается модель, позволяющая оценить время передачи данных от СУ на сервер в зависимости от различных параметров.

1. Постановка задачи. Пусть «туман» имеет кластерную структуру с центральным узлом в виде шлюза или сервера и некоторого количества СУ; число СУ в силу динамических характеристик сети IoT заранее неизвестно. Оценим время, необходимое для получения доступа к центральному узлу при заданном количестве СУ и максимально возможное количество СУ при заданной нагрузке.

2. Описание работы модели доступа. Сенсорные устройства начинают передачу данных только по запросу центрального узла. Если у СУ нет подготовленного для передачи пакета данных, то специальный логический механизм СУ формирует идентификационный пакет, содержащий уникальный идентификационный номер (ID) сенсорного устройства. Задача центрального узла идентифицировать все сенсорные устройства, которые находятся в зоне его покрытия и если у СУ есть данные для передачи, то принять их.

Процесс опроса центральным узлом – временной интервал, который разделен на блоки – окна. Окна – нефиксированные отрезки времени, размер которых определяется количеством слотов, на которые он делится. 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, то есть его определяет оборудование, используемое в системе. Пример разделения времени опроса приведен на рис. 1.

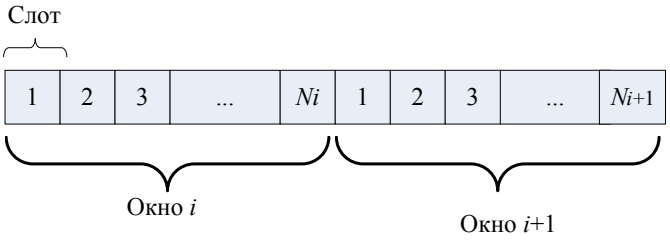


Рис.1. Разделение времени опроса центральным узлом на окна и слоты

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 [5, с. 47].

В процессе доступа в слоте возможно возникновение трех событий. 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 – когда более одного СУ начинают передавать данные в текущем слоте.

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

Пример работы модели доступа представлен на рисунке 2. Центральный узел посылает сигнал «опроса» со значением времени начала доступа и количества слотов, в данном случае 5. Сенсорные устройства, находящиеся в зоне покрытия, в данном примере – их 4 штуки, принимают сигнал и по полученным данным выбирают случайным образом слот от 1 до 5. На рисунке 2 видно, что 4-е СУ выбрало первый слот, а 1-е и 2-е СУ выбрали второй слот, 3-е СУ выбрало 4-й слот. В соответствии с выбранным слотом СУ передают свои идентификаторы и данные при наличии.

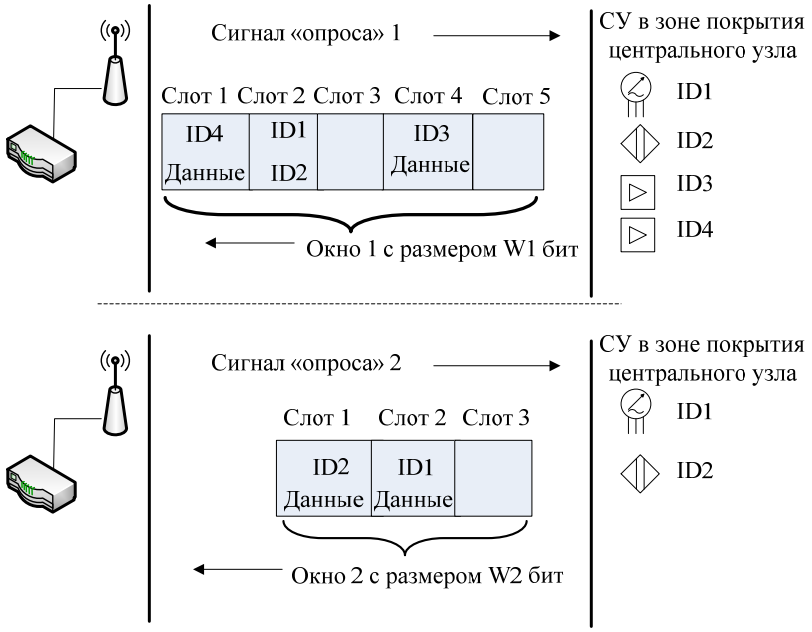


Рис.2. Пример получения доступа СУ к центральному узлу

Центральный узел анализирует каждый слот и выполняет некоторые действия. Если слот – успешный, то он регистрирует СУ по ее идентификатору и увеличивает счетчик успешных окон, если слот – пустой, увеличивается счетчик пустых окон, если слот – конфликтный, увеличивается счетчик конфликтных слотов. По завершению текущего окна, происходит вычисление размера следующего окна.

Размер следующего окна *W* определяется от количества конфликтов *Er* текущего окна по правилу: $W=Er\times2+1$. Счетчик конфликтных слотов обнуляется. Данный способ является эвристическим, поскольку параметры выбираются естественным путем. В примере на рисунке 2.4, узел рассчитал размер следующего окна, равного 3-м слотам.

3.Оценка времени доступа. Время, необходимое для выполнения операции опроса зависит от физических характеристик канала взаимодействия, которые и определяют задержку распространения [6, с.1123].

Время получения доступа обслуживания $t_д$ сенсорным устройством формируется следующим образом:

$$t_д = t_o + \frac{\overline{b}}{C}, \quad (1)$$

где t_o – время, затрачиваемое на сигнал опроса, [с]; $\overline{b}$ – среднее значение длины пакета, [бит]; *C* – пропускная способность канала, [бит/с].

Соответственно, полный цикл взаимодействия *N* сенсорных устройств и центрального узла составляет $T=Nt_д$.

Время t_o включает как время формирования опроса, так и задержку распространения. Отношение b/C – это время, необходимое для передачи *b* бит со скоростью *C* бит в секунду. Если опрашиваемое СУ не имеет готового сообщения для передачи, то *b* – очень мало, поскольку передается только ID сенсорного устройства. Если же в буфере сформирован пакет данных, то *b* равно числу бит идентификационного номера СУ плюс пакет данных.

Отношение (1) позволяет оценить среднее время обслуживания одного СУ при условии, что дисперсия *b* значительно меньше, чем $\overline{b}$.

Если каждое СУ передает в среднем λ пакетов в секунду, то при наличии в системе *N* сенсорных устройств, общая интенсивность потока данных составит λN пакетов в секунду, а средний интервал между их поступлениями $1/\lambda N$ с. Следовательно, во избежание неограниченного роста очередей, время доступа $t_д$ должно соответствовать условию [7],[8]:

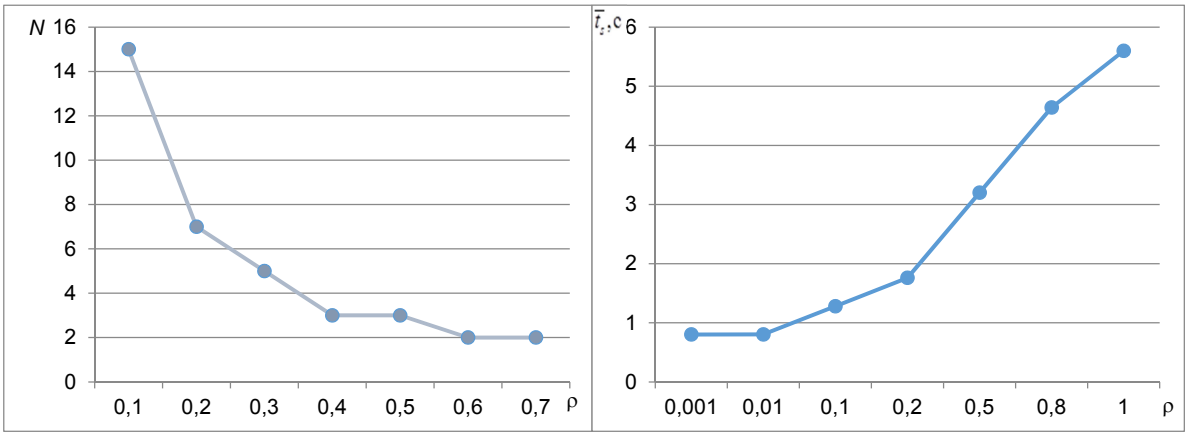
$$\overline{t_д} = t_o + \frac{\overline{b}}{C} \le \frac{1}{\lambda N}, \quad (2)$$

Решая (2) относительно C, получим условие гарантирующее отсутствие очереди для каждого СУ

$$C \ge \frac{\lambda N \overline{b}}{1-\lambda N t_o}. \quad (3)$$

Условие (3) объясняется тем, что любое из СУ опрашивается каждые $1/\lambda$ секунд и в то же время в нем формируется очередной пакет данных.

3. Анализ результатов. С увеличением количества СУ, подключенных к центральному узлу «тумана» среднее время передачи увеличивается (рисунок 3). Таким образом, исходя из требований ко времени доступа, модель позволяет определить максимально возможное количество СУ, подключенных к центральному узлу.



а) б)

Рис. 3. Результаты эксперимента
а) зависимость *N* от ρ б) Зависимость $t_д$ от ρ

Заключение. Проектирование систем Интернета вещей связано с рядом задач, требующих моделирования процессов информационного взаимодействия. Предложенная модель имитирует доступ СУ к центральному узлу для передачи данных и позволяет оценить время доступа с учетом стохастического характера данного процесса.

СПИСОК ЛИТЕРАТУРЫ

1. Татарникова Т.М., Елизаров М.А. Модель оценки временных характеристик при взаимодействии в сети Интернета вещей// Информационно-управляющие системы. – 2017. № 2 (87). *С. 44-50.*
2. Аль-Хаками Али Мохаммед Омар, Татарникова Т.М. Оценка вероятностно-временных характеристик сетей хранения данных SAN//Программные продукты и системы. 2009. № 4. С. 177-179.
3. Татарникова Т.М. Аналитико-статистическая модель оценки живучести сетей с топологией mesh// Информационно-управляющие системы. – 2017. № 1 (86). – С. 17-22.
4. Татарникова Т.М., Елизаров М.А. Процедура разрешения коллизий в RFID-системе// Известия высших учебных заведений. Приборостроение. – 2017. Т. 60. № 2. – С. 150-157.
5. Татарникова Т.М. Елизаров М.А. Модель оценки временных характеристик при взаимодействии в сети интернета вещей//Информационно-управляющие системы.. – 2017. № 2 (87). – С. 44-50.
6. Татарникова Т. М., Елизаров М.А. Имитационная модель виртуального канала// Научно-технический вестник информационных технологий, механики и оптики. – 2016. Т.16. № 6. – С. 1120-1127.
7. Кутузов О.И. , Татарникова Т.М. Инфокоммуникационные сети. Моделирование и оценка вероятностно-временных характеристик.– СПб.: ГУАП, 2015. – 382 с.
8. Кутузов О.И. Татарникова Т.М. Моделирование систем и сетей телекоммуникаций. – СПб: РГГМУ, 2012. –134 с.

УДК 004.7.056.53

ОЦЕНКА И ПРОГНОЗИРОВАНИЯ РИСКОВ ДЛЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Капанов Алексей Александрович, Мещеряков Евгений Евгеньевич, Косолапов Владимир Викторович, Астахова Татьяна Николаевна
Нижегородский государственный инженерно-экономический университет
Россия, Нижегородская обл., г. Княгинино, ул. Октябрьская, д. 22а.
emails: alesnim@gmail.com, leonline5@mail.ru, vladimir.kosolapov@mail.ru, ctn_af@mail.ru

***Аннотация*:** В статье рассмотрены ключевые проблемы обеспечения безопасности информационных систем на базе предприятия за счет применения методик оценки и прогнозирования возможных рисков воздействия внешних хакерских атак.

***Ключевые слова**: информационная система; риск; прогнозирование; оценка.*

ESTIMATION AND FORECASTING OF RISKS FOR INFORMATION SECURITY SYSTEMS

Alexey Kapanov, Evgeny Meshcheryakov, Vladimir Kosolapov, Tatyana Astakhova
Nizhny Novgorod State University of Engineering and Economics,
Russia, Knyaginino, Oktyabrskaya Str., 22a.
emails: alesnim@gmail.com, leonline5@mail.ru, vladimir.kosolapov@mail.ru, ctn_af@mail.ru

Abstract: Key problems of ensuring the security of information systems on the basis of the enterprise due to application of techniques for assessing and predicting the possible risks of external hacker attacks are considered in the article.

***Keywords**: information system; risk; forecasting; assessment.*

Введение. Развитие информационных технологий, средств и систем, их активное внедрение в жизнь общества ставит проблему обеспечения безопасности объектов информационно-телекоммуникационной инфраструктуры в разряд первоочередных.

Основной задачей системы обеспечения информационной безопасности является обеспечение функционирования объекта, исключая или предотвращая нарушения безопасности объекта, недопущение хищения материальных или денежных средств при помощи информационной системы, предотвращение противоправных деяний и обеспечение деятельности всех объектов, зависимых от информационной системы.

Важнейшей задачей для создания и проектирования систем информационной безопасности является задача прогнозирования рисков [1].

Основу риска образуют возможные уязвимости и угрозы для организации, поэтому выявление потенциальных или реально существующих рисков нарушения конфиденциальности и целостности информации, распространения вредоносного программного обеспечения и финансового мошенничества, классификация угроз информационной безопасности является первостепенной задачей информационной безопасности.

Оценку риска нужно проводить постоянно, проводя их переоценку. Для облегчения процессов дальнейшей переоценки рекомендуется встраивать оценку рисков в жизненный цикл информационной системы (далее – ИС) [2].

На примере нашего университета проведем оценку рисков информационной безопасности (ИБ) для данных используемых в процессе обучения студентов. В настоящий момент используются различные бумажные варианты прогнозирования и оценки угроз и рисков, в достоинство которых входит гибкость и адаптивность. Так же существуют программные комплексы, позволяющие проводить анализ рисков, но их функционал предполагает использование в достаточно крупных фирмах с

уровнем ИБ выше среднего. Поэтому будет проведен теоретический анализ угроз ИБ без использования специального программного обеспечения [3].

Для оценки рисков выделим основные этапы жизненного цикла информационной системы:

– инициация, согласно различным процессам организации;
– установка;
– эксплуатация;
– выведение из эксплуатации.

Под ИС университета «НГИЭУ» понимается совокупность баз данных, программ обработки документации, физические машины и локальная сеть университета. Для такой обобщенной системы так же справедливы правила управления риском.

Обобщенный алгоритм управления риском для ИС:

1. Выявление потенциальных угроз. В данном случае сосредоточимся на риске утечки информации, взломе и выведение ИС из рабочего состояния.

2. Анализ потенциальных угроз. Размер статьи не позволяет приводить полный анализ угроз, в таблице 1 указаны конечные оценки по упрощенной методике CRAMM.

Таблица 1

Конечные оценки потенциальных угроз

	Уровень угрозы	Уровень уязвимости	Уровень финансовых потерь	Суммарная оценка угрозы
Утечка информации	Высокий	Очень высокий	Низкий	Средний
Взлом	Средний	Низкий	Высокий	Низкий
Выведение ИС из рабочего состояния	Высокий	Высокий	Средний	Высокий

3. Создание системы безопасности. В качестве контрмер предполагаются стандартные действия по настройке и обновлению антивирусных программ и повышение компьютерной грамотности пользователей.

4. Обнаружение реальных угроз. Примером реальной угрозы рассмотрим выход из строя ПК в одной из лабораторий университета после заражения вирусом. В результате ПК вышел из строя и заразил сегмент сети крипто-вирусом.

5. Сдерживание реальных угроз. Были проведены мероприятия по сдерживанию вируса внутри сегмента сети при помощи изоляции сегмента на время проведения работ.

6. Ликвидация последствий угроз. Проведена проверка системы на наличие сигнатуры вируса на каждом ПК в сегменте и его удаление, а также мероприятия по предотвращению проникновения такого типа вирусов вновь в локальную сеть.

Все пункты алгоритма выполняются циклически на протяжении всего жизненного цикла ИС. С каждым циклом производится модификация системы ИБ для защиты от актуальных угроз.

Все этапы выполняются последовательно, позволяя охватить наиболее полно все виды угроз и степень их опасности для ИС. Используя различные методики оценки рисков, как одного из наиболее важных этапов, возможно радикально снизить уровень опасности угроз для ИС.

Заключение. Поскольку полное устранение рисков не представляется возможным, существуют методики уменьшения последствий атаки. В ходе устранения последствий и модификации системы безопасности ИС следует руководствоваться целесообразностью и достаточностью в ходе применения регуляторов безопасности.

Анализ рисков для ИС является важным элементом стратегии обеспечения устойчивого и бесперебойного функционирования системы.

СПИСОК ЛИТЕРАТУРЫ

1. Костогрызов Андрей Иванович, Лазарев Виктор Михайлович, Любимов Алексей Евгеньевич Прогнозирование рисков для обеспечения эффективности систем информационной безопасности в их жизненном цикле // Правовая информатика. 2013. №4. С.4-16
2. Риски информационной безопасности веб-приложений // habrahabr URL: https://habrahabr.ru/company/pentestit/blog/279219/ (дата обращения: 05.09.17).
3. Оценка рисков ИБ, разработка моделей угроз // УЦСБ URL: http://www.ussc.ru/catalog/id/39 (дата обращения: 05.09.17)..
4. Ендовицкий Д.А., Бабушкин В.А., Батурина Н.А. Анализ инвестиционной привлекательности организации: научное издание / под ред. Д.А. Ендовицкого. – М.: КНОРУС, 2010, 376 с.

УДК 004.7

ПАРАДИГМЫ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ: ЕДИНСТВО И ОТЛИЧИЯ

Кутузов Олег Иванович[1], Татарникова Татьяна Михайловна[2]
[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
[2] Санкт-Петербургский государственный университет аэрокосмического приборостроения
Россия, Санкт-Петербург, ул. Большая Морская, д. 67,
emails: oleg-kutuzov@mail.ru, tm-tatarn@yandex.ru

Аннотация: Обсуждаются особенности реализации продвижения системного времени в существующих парадигмах имитационного моделирования: дискретно-событийного, динамического, системной динамики и мультиагентного подхода. В моделях с непрерывными процессами предлагается выбирать значение шага продвижения во времени в соответствии с теоремой Найквиста-Котельникова.

Ключевые слова**:** *Имитационное моделирование, симулятор, шаг продвижения системного времени, календарь событий, схема процессов и событий, моделирование случайностей, ускорение*.

SAFETY INFORMATION INTERACTION

Oleg Kutuzov[1], Tatiana Tatarnikova[2]
[1] The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
[2] Saint-Petersburg State University of Aerospace Instrumentation
Russia, St. Petersburg, Bolshaya Morskaia str. 67,
emails: oleg-kutuzov @mail.ru, tm-tatarn@yandex.ru

Abstract: The implementations of the system time promotion in existing paradigms of simulation: discrete event, dynamic, system dynamics and multi-agent approach. In models with continuous processes are invited to choose the value of the step advance in time according to the Nyquist-Kotelnikov theorem.

Keywords: *Simulation modeling, simulator, step of moving the system time, calendar of events, a scheme of processes and events, simulation of randomness, acceleration*.

Введение. Имитационное моделирование при современном уровне развития информационных технологий переживает второе рождение [1]. В практической реализации оно опирается на четыре парадигмы: дискретно-событийное моделирование, динамическое моделирование, системная динамика в смысле Форрестера и мультиагентный подход [2],[3].

В дискретно-событийном моделировании функционирование системы представляется как хронологическая последовательность событий. Событие происходит в определенный момент времени и сопровождается изменением состояния системы. Продвижение системного времени реализуется посредством программирования симулятора – «движителя» времени. Симулятор воспроизводит во времени смену состояний объекта моделирования, отображая, таким образом, действие механизма причинно-следственных связей.

Имитация сводится к заданию начального состояния системы, пуску симулятора и наблюдению за воспроизведением траектории моделируемого объекта в пространстве смены его состояний.

Дискретно-событийный способ применяется для моделирования процессов, присущих информационным и телекоммуникационным сетям, системам с отказами и восстановлением элементов, дискретным производствам и т.п.

Динамическое моделирование применяется для моделирования процессов, описываемых дифференциальными уравнениями, представленными в форме Коши, которые решаются численными методами с автоматическим подбором шага по времени.

В дифференциальных уравнениях значения переменных в конце интервала времени [t, t+dt] выражаются через их значения относительно начала интервала времени так, как это определяется причинно-следственными связями, действующими в системе.

При компьютерной имитации символьные бесконечно малые приращения dt заменяются численными конечными приращениями времени Δt, и имитация системы выполняется в дискретном времени. Траектория смены состояний моделируемого объекта определяется действием учитываемых моделью причинно-следственных связей. Выбор значения шага Δt не связан с принципом имитации и обусловлен динамикой моделируемых процессов.

Таким образом, логика так называемого «непрерывного» динамического моделирования в части механизма продвижения во времени совпадает с логикой дискретно-событийного моделирования.

В системной динамике структурными элементами модели являются уровни и темпы. Уровни обладают накопительным свойством (накопители). Темпы играют роль скоростей и характеризуют потоки, входящие и выходящие из накопителей. Взаимодействие в модели отображается непрерывными процессами, представленными в виде уравнений в конечных разностях. В плане

обеспечения имитации системная динамика отличается от «непрерывного» динамического моделирования лишь формализацией. В системной динамике отсутствует промежуточная фаза описания объекта на языке дифференциалов. Объект отображается в виде совокупности условно независимых сетей.

Шаг Δt в системе разностных уравнений уровней системной динамики можно рассматривать как шаг смены значений уровней и потоков во времени.

Мультиагентное моделирование исследует поведение децентрализованных агентов и то, как такое поведение определяет поведение всей системы в целом. Агенты – это объекты модели, интерпретируемые как независимые активные сущности. Поведение агентов определяется на индивидуальном уровне, а глобальное поведение возникает как результат деятельности множества агентов (моделирование «снизу вверх»). Агент – это, по сути, атомарный процесс – последовательность событий и работ, описывающая поведение во времени какого-либо объекта в моделируемой системе. Действия агентов имитируются в модели точно так же, как и любые другие события – как прямые следствия из достигнутого состояния системы. И модельное время продвигается симулятором строго вперед, в точном соответствии с механизмом причин и следствий.

Единство «парадигм» имитационного моделирования. Во всех рассмотренных четырех версиях имитационного моделирования симулятор продвигает вперед системное время и создает на каждом очередном шаге текущий временной слой системы. Этот слой содержит сведения о возможных ближайших предстоящих и последних произошедших изменений для рекуррентного пересчета показателей. Симулятор продвигает этот временной слой вперед в модельном времени вдоль множества фактов отслеживаемой им причинно-следственной цепи и достигает заданных целей. Этот принцип и является сущностью компьютерного имитационного моделирования.

Следовательно, все четыре «парадигмы», по сути, просто разные реализации имитационного моделирования, разные подходы к построению траекторий смены состояний. Все они используют причинно-следственный механизм продвижения процессов во времени. Различия относятся лишь к выбору того или иного набора базовых математических и программных объектов, а логика имитации процессов одинакова. Построение траектории функционирования моделируемого объекта выполняется продвижением системного времени. Это возможно реализовать как с детерминированным шагом Δt, так и с шагом случайной длительности.

Таким образом, переход в имитационном моделировании от одного из четырех подходов к другому, например, от дискретно-событийного подхода к мультиагентному и т.п. не является, по сути, сменой парадигм. Более того, в практической реализации задач моделирования осуществляется гибкий переход между рассмотренными методами. Интегрированная среда может включать модельные агенты, управляемые в духе подхода Дж. Форрестера или массовые потоки дискретных событий, обобщаемые как уровни и потоки системной динамики [3]. Объединенная логика имитационного моделирования открывает путь к фабрикам имитационных моделей, первые образцы которых уже существуют [4].

Принципы продвижения системного времени. В моделях с непрерывными процессами продвижение во времени (пересчет значений переменных величин в ходе модельного времени), осуществляется в имитационной модели по «принципу малых Δt» [5]. Но насколько «малых»?

В технике связи в основе соответствия между непрерывными и дискретными сигналами лежит теорема Найквиста-Котельникова [6], которая обосновывает представление (передачу) аналоговых сигналов отдельными выборочными значениями через шаг

$$\Delta t = 1/2F_{гр},$$

где Fгр – граничная частота; частота, ограничивающая сверху эффективную полосу спектра аналогового сигнала.

Частотная характеристика является отличительным признаком любой динамической системы. Поэтому такой подход к назначению шага Δt применяется и при имитационном моделировании динамических систем [7].

Поскольку доля частотного спектра, примыкающего к этой граничной частоте очень мала по сравнению с областью более низких частот этого ограниченного спектра, то возникает много участков в дискретной интерпретации аналогового сигнала, в которых последовательные выборочные значения практически не отличаются друг от друга.

Поэтому, например, в технике связи от циклической дискретизации с шагом Δt перешли к адаптивной дискретизации со случайным шагом.

При адаптивной дискретизации относительно представленного (переданного) значения выставляется некоторая зона (апертура), и очередное выборочное значение берется (передается) через временной интервал, когда это значение отклоняется от предыдущего представленного (переданного) в большую или меньшую сторону на величину, превышающую значение апертуры. Это и задает случайный шаг между представляемыми (передаваемыми) значениями (событиями!) аналогового сигнала.

Такую связь между непрерывным и дискретным имеем во всех четырех «парадигмах» имитационного моделирования. И если фиксированный шаг используется при динамическом моделировании, системной динамике, то при дискретно-событийном и агентном моделировании используют как фиксированный, так и случайный шаги продвижения системного времени [5].

При построении «движителя» системного времени применяют две основные схемы построения алгоритмов моделирования – схема событий и схема процессов. Схема событий используется при дискретно-событийном моделировании, а схема процессов – при мультиагентном моделировании.

И в той и другой схеме для продвижения системного времени применяется принцип «особых» моментов [5]. Чтобы компьютер мог вычислить очередной «особый» момент, используется календарь, в котором для каждого типа события указан ближайший момент, когда такое событие произойдет. По календарю определяется очередной особый момент. Это наименьший из моментов, записанных в календаре.

Сопоставим схемы событий и схемы процессов.

Схема событий более стройна: события не пересекаются, за один шаг имитируется одно событие, события имитируется в хронологическом порядке, алгоритм шага делится на этапы с четким функциональным назначением (имитация события, пополнение статистик, планирование новых событий). Основная трудность при разработке модели по схеме событий – в сложных ситуациях довольно трудно сформировать перечень типов событий и правильно разработать соответствующие им части алгоритма так, чтобы не упустить каких-то нужных элементарных событий и правильно учесть взаимосвязи.

Схема процессов не требует при разработке алгоритма учитывать сразу все, что может происходить в системе, а допускает раздельную разработку отдельных процессов. Особенно упрощается разработка имитационных моделей при использовании готовой системы моделирования, когда пользователю требуется только описать последовательность событий и работ в процессах, а учет взаимодействия процессов, сбор статистики, управление порядком имитации процессов берет на себя система моделирования.

Однако, схема процессов не позволяет выделить функционально различные части алгоритма: пополнение статистик и планирование событий исследуют с операциями смены состояний в рамках одной фазы процесса. Это чревато упущениями при разработке алгоритма.

На этапе начального обучения моделирование и при моделировании простых систем целесообразно применять схему событий, а при моделировании сложных систем с использованием универсальных средств предпочтительнее схема процессов.

По схеме событий на каждом очередном шаге выполняется то особое состояние, время наступления которого ближайшее к текущему моменту. При этом на каждом шаге возможен переход к любому из программных модуле. А это, в свою очередь, влечет вызов другой структуры данных, соответствующий типу особого состояния.

Схема процессов обеспечивает переход к нужному модулю и позволяет выполнять несколько последовательных особых состояний при очередном переходе к определенному модулю, что, как показывают приведенные расчеты, существенно сокращает число обращений к календарю событий и тем самым ускоряет процесс моделирования.

С другой стороны, в схеме процессов число процессов не постоянно: некоторые из них появляются, например, очереди или заявки, а потом исчезают. В связи с этим невозможно заранее определить объем календаря и приходится под каждый процесс отводить заведомо больше ресурсов памяти.

Схема процессов удобно реализуется с использованием объектно-ориентированного подхода, который широко применяется при построении мощных инструментальных систем моделирования, как например система AnyLogic [4].

Прежде чем объект моделирования будет отображен программной имитационной моделью, для него формируется концептуальная модель и формализованное представление объекта в виде адекватной математической модели. Программная модель реализует численный эксперимент с этой математической моделью.

Моделирование случайностей. При моделировании стохастических систем парадигма имитационного моделирования включает две составляющие: симулятор – «движитель», реализующий продвижение системного времени, и метод Монте-Карло, обеспечивающий разыгрывание «случайностей» [9]. В совокупности эти две составляющие и строят траектории – реализации функционирования моделируемой системы, в которой присутствуют случайные факторы и объекты. Обе составляющие наличествуют во всех четырех подходах ИМ.

Имитационное моделирование с учетом влияния случайных факторов сопряжено с многократным воспроизведением возможных вариантов развития процессов. Многократность позволяет получить полосу наиболее вероятных траекторий для статистических оценок искомых показателей. Точность получаемых оценок характеризует точность ИМ, как меру соответствия численного решения, получаемого с помощью ИМ, точному решению поставленной математической задачи.

Известный недостаток метода Монте-Карло заключается в его медленной сходимости, который особенно проявляется при моделировании редких событий и в задачах большой размерности. И здесь особенно актуальным становится проблема ускорения имитационного моделирования с использованием метода Монте-Карло за счет сокращения количества численных экспериментов.

Аналитико-имитационное моделирование. Общей стратегией снижения цены точности является ускорение сходимости вычисляемых оценок. Ускорение может достигаться: а) за счет соответствующего аналитического преобразования решаемой задачи [10]; б) системотехническими методами ускорения расчетов, в частности, путем организации параллельных вычислений и распределенного моделирования [11]. Наибольшего эффекта удается достичь тогда, когда методы ускорения учитывают специфику моделируемых объектов, решаемых задач и алгоритмов их решения. Так, например, в [10, 11] оба названных подхода к ускорению ИМ развиваются и излагаются применительно к задачам моделирования инфокоммуникационных сетей. Теоретической основой ускоренного аналитико-имитационного моделирования сетей являются методы расслоенной выборки [12], равновзвешенного моделирования [13], элементы теории экстремальных статистик [14].

Заключение. Разные реализации имитационного моделирования, основанные на одной из четырех парадигм – дискретно-событийное моделирование, динамическое моделирование, системная динамика и мультиагентный подход отличаются способами построения траекторий смены состояний. Различия относятся как к выбору того или иного набора базовых математических и программных объектов, так и шага продвижения системного времени.

Назначение шага продвижения системного времени осуществляется исходя из циклической дискретизации с детерминированным шагом Δt и шагом случайной длительности.

В моделях с непрерывными процессами предлагается выбирать значение шага продвижения во времени в соответствии с теоремой Найквиста-Котельникова. Фиксированный шаг рекомендуется применять при динамическом моделировании и системной динамике. При дискретно-событийном и агентном моделировании в зависимости от постановки задачи моделирования используют как фиксированный, так и случайный шаги продвижения системного времени.

При построении симулятора независимо от способа назначения шага применяют две схемы построения алгоритмов моделирования – схема событий и схема процессов, сравнение которых на примере модели виртуального канала показало преимущество схемы процессов по числу обращений к календарю событий.

Выбор одной из парадигм имитационного моделирования имеет большое значение при построении имитационной модели. Рекомендации по выбору шага продвижения системного времени, приведенные в статье, позволяют ускорить процесс моделирования и экономить вычислительные ресурсы.

СПИСОК ЛИТЕРАТУРЫ

1. Лычкина Н.Н. Инновационные парадигмы имитационного моделирования и их применение в сфере управленческого консалтинга и стратегического менеджмента. Материалы XX Международной студенческой школы-семинара «Новые информационные технологии» (пленарные доклады), 2012 г. с. 94-105.
2. Задорожный, В.Н. Управление сложными техническими объектами и парадигмы имитационного моделирования / В.Н. Задорожный, И.И. Семёнова / Омский научный вестник, 2006. – № 2(35), С. 102–108.
3. Горбунов А.Р., Лычкина Н.Н. Инновационные парадигмы имитационного моделирования: новое в решении задач стратегического управления (объединенная логика имитационного моделирования)//БИЗНЕС-ИНФОРМАТИКА №2-2007 с 60-66 (67)
4. Карпов Ю.Г. Имитационное моделирование систем. Введение в моделирование с AnyLogic 5. – СПб.: БХВ-Петербург, 2005. – 400 с.
5. Советов Б.Я., Яковлев С.А. Моделирование систем: учеб. для вузов. – М. : Высш. шк., 2007. – 343 с
6. Биккенин Р. Р., Чесноков М. Н. Теория электрической связи. — М.: Издательский центр «Академия», 2010. — 329 с.
7. Быков В.В. Цифровое моделирование в статистической радиотехнике.- М.:Сов. радио, 1971.-328 с.
8. Кутузов О.И. К оценке эффективности мультиагентного моделирования // Седьмая всероссийская НПК «Имитационное моделирование. теория и практика» (ИММОД–2015): Труды конф. 21-23 окт. 2015 г. Г. Москва: в 2 т /Ин-т проблем упр. им. В,А. Трапезникова Рос. Акад. наук: М.: ИПУ РАН, 2015. ISBN978-5-91450-172-0 С/ 127-131
9. Поляк Ю.Г. Вероятностное моделирование на ЭВМ – М.:Сов. Радио 1971.– 400 с.
10. Кутузов О. И. Инфокоммуникационные сети. Моделирование и оценка вероятностно-временных характеристик: монография / О.И. Кутузов, Т.М Татарникова. – СПб. ГУАП, 215. – 382 с.
11. Олзоева С.И. Распределенное моделирование в задачах разработки АСУ. - Улан-Удэ, изд-во ВСГТУ, 2005, 219 с.
12. Клейнен Дж. Статистические методы в имитационном моделировании: Пер. с англ. / Под ред. Ю.П. Адлера и В.Н. Варыгина. – М. : Статистика, 1978. – Вып.1. – 221 с.; вып. 2. – 335 с.
13. Плакс Б.И. Расчет надежности систем со сложной структурой ускоренным методом Монте-Карло //Изв. АН СССР. Техническая кибернетика.- 1983.- N6.- С. 158-162.
14. Галамбош Янош. Асимптотическая теория экстремальных порядковых статистик / Пер. с англ.-М. Наука, 1984. – 303 с.

УДК 347.775

ФОРМИРОВАНИЕ И ИСПОЛЬЗОВАНИЕ В УЧЕБНОМ ПРОЦЕССЕ СИТУАЦИОННОГО ЦЕНТРА ДЕЛОВОЙ РАЗВЕДКИ

Левкин Игорь Михайлович, Микадзе Сергей Юрьевич
Санкт-Петербургский государственный экономический университет (Санкт-Петербург),
Россия, Санкт-Петербург, улица Садовая, дом 21,
email: mik@finec.ru, lev.kin@yandex.ru

***Аннотация*:** В статье рассмотрены особенности построения и использования учебных ситуационных центров при подготовке бакалавров в сфере деловой разведки. Приведены примеры учебных задач, которые могут решаться в индивидуальном порядке и в составе рабочих подгрупп.

***Ключевые слова**: учебный ситуационный центр, деловая разведка, основные виды занятий.*

FORMATION AND USE IN THE EDUCATIONAL PROCESS OF THE SITUATIONAL CENTER FOR BUSINESS INTELLIGENCE

Levkin Igor Mikhailovich, Mikadze Sergey
Saint-Petersburg state economic University (St. Petersburg),
Russia, Saint-Petersburg, Sadovaya street, the house 21,
email: mik@finec.ru, lev.kin@yandex.ru

Abstract: the article considers the features of the construction and use of training centers in the preparation of bachelors in the field of business intelligence. Examples of learning tasks that can be addressed individually and in the composition of the working groups.

***Keywords**: educational situation centre, business intelligence, principal occupations.*

Введение. Подготовка бакалавров по направленностям Информационные технологии в деловой разведке и Деловая аналитика предполагает формирование, в частности, таких компетенций как умение: пользоваться научными методами выявления и систематизации данных об окружающем мире; пользоваться необходимыми методами добывания (сбора), обработки, анализа и синтеза информации для оценки конкурентной, экономической, финансовой и других видов обстановки; применять автоматизированные системы сбора, систематизации и научной интерпретации экономической и других видов информации; осуществлять оптимальный выбор пакетов прикладных программ математической обработки, анализа и синтеза результатов профессиональных исследований; разрабатывать математические модели функционирования экономических систем с использованием инструментов и методов системного анализа для управления бизнесом; и другие.

При этом многие из этих задач предполагают последовательное решение некоторого связанного множества частных задач, выполняемых индивидуально, а также задач, выполняемых в составе групп из 3 – 4-х студентов и более с использованием информационных систем коллективного пользования. К числу таких задач можно отнести задачи: оценки и прогнозирования конкурентной, экономической, транспортной, социально-психологической и других видов обстановки; моделирование экономических, информационных и других угроз, прогнозирование их формирования, развития и степени опасности в различных условиях обстановки; оценки сильных и слабых сторон конкурентов и выпускаемой ими продукции; выявления конкурентоспособности хозяйствующего субъекта; разработки предложений по совершенствованию бизнес-процессов в информационной сфере; разработка фрагментов информационной системы умного города; разработка фрагментов системы управления большими данными, промышленного интернета (интернета вещей), технологии виртуальной и дополненной реальностей и другие.

Эффективное решение этих задач невозможно без создания и внедрения в учебный процесс учебных ситуационных центров (УСЦ), которые не только помогают принимать управленческие решения, но и служат средством о бучения специалистов [1,2].

Учебный ситуационный центр позволяет [3,4]:

– связать различные знания пользователей в единую, постоянно развивающуюся систему знаний, способствующую интенсификации процесса получения эффективного управленческого решения;

– сформировать и совершенствовать навыки управления и, прежде всего управленческого мышления, при разработке и реализации конкретных проектов, учитывая индивидуальные когнитивные особенности и образовательные потребности пользователей;

– значительно облегчить практическую работу пользователей, перевести их в исследовательский режим. Сделать эту работу интересной и захватывающей, повысить производительность интеллектуальной деятельности;

– привить вкус пользователей к культуре аналитической работы;

– минимизировать затраты на программное обеспечение управленческой подготовки пользователей и ее главной составляющей управленческого мышления (один программный комплекс для самых разных управленческих ситуаций: политических, регионоведческих, социологических, экономических и др.).

В настоящее время УСЦ активно используются в учебных процессах Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации [5], Белгородский юридический институт МВД России [6], МГИМО [7] и других вузах.

По опыту эксплуатации УСЦ при обучении в их среде знания формируются «эволюционно» на основании экспериментов с соответствующими моделями. Правила работы, критерии и методы оценки обучающихся могут значительно изменяться, что не позволяет использовать традиционный подход к обучению. Таким образом, само функционирование УСЦ предопределяет переход в учебном процессе к инновационным, субъектно- и деятельностно-ориентированным методам обучения (эволюционному обучению, рефлексивно-гуманистической психологии, педагогике сотворчества, проективной педагогике и др.). Самостоятельной проблемой становится разработка методики оценки деятельности учащегося в коллективе (в рамках учебного процесса в среде УСЦ) при отсутствии четко сформулированной цели.

К основным видам занятий, которые целесообразно проводить в УСЦ деловой разведки можно отнести: лекции демонстрации, лекции дискуссии, практические занятия по разработке технических и программных средств, семинар, решение многоэтапных и групповых бизнес-кейсов, деловая игра. Наиболее развитой (в том числе и в коммуникативном плане) методикой проведения занятий в УСЦ следует считать электронный деловой театр с использованием концепции организационно-мыследеятельностных игр, типа «мозговой штурм» [8]. Кроме того, на территории УСЦ могут проходить защиты курсовых и выпускных квалификационных работ.

Важной функцией УСЦ должна также стать возможность проведения научных исследований в рамках студенческого научного общества (так, например, в состав центра предлагается включить лабораторию интернет вещей), а также осуществление научно-практической деятельности в рамках хоздоговорной деятельности с научными, промышленными и бизнес структурами.

УСЦ деловой разведки может быть построен как совокупность программно-технических средств, научно-математических методов и инженерных решений для автоматизации процессов отображения, моделирования, анализа ситуаций и управления. Он должен позволять автоматизировать обработку самой ситуации, а не только исходных данных, необходимых для ее последующего выявления и анализа субъектом. При этом в таком УСЦ должна быть обеспечена возможность решения двух групп практических задач: задачи программно-технического обеспечения (доработка используемой техники и программных продуктов, разработка фрагментов и макетов информационных систем и технологий цифровой экономики); задачи анализа ситуаций и принятия управленческие решения.

Решение задач обеих групп может осуществляться в двух режимах – индивидуальном и коллективном. В первом случае каждый студент может работать только в своей фиксированной области и не согласовывает свою деятельность с другими членами группы. Во втором случае студенты могут работать над решением общей проблемы и должны учитывать возможные влияния своих решений на деятельность коллег.

Программно-техническое обеспечение УСЦ должно обеспечивать: доступ к информационному пространству, возможность формирования и предоставления пользователям обобщенной информации, возможность анализа агрегированных данных; возможность использования средств прогнозирования, выявления тенденций исследуемого явления или процесса; ситуационное (динамическое) моделирование как возможность получить ответ на вопрос «что будет, если», позволяющее вносить возмущения и определять возможные последствия, связанные с наступлением того или иного события; формирование рекомендаций по выбору одного из многих вариантов решения; возможность проведения оценки рисков при расчете шансов реализации прогноза; возможность разработки и совершенствования программно-технических решений.

Техническое решение по оснащению учебных ситуационных центров включает широкий спектр специализированных систем и технологий, в том числе [9]: экраны коллективного пользования, средства видеоконференц-связи, мощную звуковую систему, беспроводную сеть для подключения индивидуальных ноутбуков к общей информационной системе, мобильную систему синхронного перевода, источники сигналов, систему документирования, средства коммутации, систему управления, индивидуальные рабочие места, специализированную мебель.

Для реализации этих целей в состав ситуационного центра могут быть включены:

– программные продукты: программный комплекс SPSS, PaloMARS, SuperNova, Galileo (для «Социологии»), информационно-аналитическая программа «Enterprise Miner» (для «Зарубежного регионоведения»), интеллектуальная информационно-поисковая система «Истра 2006» (для «Международных отношений», «Политологии»), психолингвистическая программа «ВААЛ» (для «Журналистики», «Рекламы и связей с общественностью»);

– спутниковое телевидение, презентационные и мультимедийные средства, демонстрационные программы для реализации различных форм обучения;

– электронные учебные пособия, интерактивные учебные программы для изучения основных приемов владения информационными технологиями.

В вопросах деловой разведки УСЦ должен обеспечить следующие возможности [4]:

– демонстрацию основных видов, форм и способов конкурентной борьбы, ее законов и закономерностей, в том числе атаковые, оборонительные и фланговые стратегии; порядок и приемы применения действия сил и средств предприятия (организации, фирмы) и привлекаемых сил и средств при решении задач конкурентной борьбы и т.п. Демонстрация основных законов конкурентной борьбы (закон определяющей роли экономических целей конкурентной борьбы; закон зависимости хода и исхода конкурентной борьбы от экономических, социально-политических, научно-технических и других возможностей конкурирующих сторон и др.; закон зависимости успеха конкурентной борьбы от соразмерности между целями и применяемыми силами и средствами в их соотношении с силами и средствами конкурента, с учетом факторов пространства и времени; закон зависимости успеха в конкурентной борьбе от создания материальных условий на каждом этапе конкурентных действий — организованном материально-техническом и информационном обеспечении) должна наглядно демонстрировать сложность и жесткость этих социально-экономических процессов. В этом плане могут быть использованы видеоматериалы, вербальные модели и сценарии, практические примеры конкуренции хозяйствующих субъектов в нашей стране и за рубежом и т.п.;

– юридическое сопровождение деловой разведки, в процессе которого должна представляться информация о законных методах добывания информации, примерах нарушения действующего нормативного законодательства, об ответственности за его нарушения. Для этого: во-первых, должна быть создана информационная база соответствующих нормативно-правовых документов, которая может актуализироваться в автоматическом режиме; во-вторых, система проверки разрабатываемых информационных продуктов на законность используемой в них информации; в-третьих, система профилактики возможных нарушений при выполнении решаемых в УСЦ деловой разведки задач; другие функции;

– моделирование технологических процессов добывания и обработки информации в деловой разведке. Эти модели должны быть реализованы в отношении процессов поиска информации, ее систематизации, учета, первичной обработки, анализа и синтеза, разработки информационных документов, планирования и управления этими процессами и т.п.;

– моделирование и разработка информационных систем, решающих задачи деловой разведки. Реализация этих возможностей должна быть обеспечена созданной аппаратно-программной базой и предполагать дальнейшее совершенствование этой базы;

– оценивать свойства информационных источников в документной, электронной, предметно-вещевой и одушевленной средах, физических (доступность, степень обработки, тип носителя, объем, изобразительные, измерительные и технологические свойства) и прагматических (важность, срочность, достоверность, ценность, отношение к области деятельности, старение, полнота, новизна, доказательность, оптимальность) свойств информации и определять пространственно-временные характеристики фрагментов информационного пространства (зоны особого внимания (например, агрегаторы новостей, сайты игроков рынка, отраслевые on-line базы данных, странички экспертов и интересующихся, площадки, где идет обсуждение тем, связанных с задачами деловой разведки (в т.ч. блоги, форумы, соцсети и т.д).)) с целью ориентирования на них средств добывания информации при решении конкретных информационных задач;

– разрабатывать априорные словари информационных признаков простых и сложных объектов, мероприятий, ситуаций и обстановок, деятельности хозяйствующих субъектов путем ведения активного наблюдения, проведения информационного поиска, моделирования процесса функционирования объекта (явления), прогнозирования;

– строить информационно-признаковые модели (вербальные, табличные, иерархические, сетевые и др.) угроз различной природы, с учетом объективно сложившейся совокупности неблагоприятных условий и факторов (в том числе форс-мажора); субъективных намерений (замыслов, желаний); объективных возможностей реализации субъективных намерений; условий создаваемых субъектов; наличия существующих сил и средств; наличия необходимых и достаточных условий; условий, складывающих без участия субъекта. Использовать существующие математические методы работы с информационно-признаковыми моделями различных выводов и разрабатывать новые;

– определять стратегии поиска информации, поисковые технологии и отрабатывать методы автоматизированного и автоматического адресного, семантического, документального и фактографического поиска в видимой и невидимой частях сети Internet при помощи существующих информационно-поисковых систем и систем, создаваемых для поиска информации в информационной базе УСЦ с оценками точности и полноты, коэффициента информационного шума, коэффициента потерь, оперативности, стоимости и трудоемкости. Проводить непрерывный мониторинг новостей (не только то, что публикуется в новостных лентах информационных агенств, но и любые сообщения отражающие изменения в ситуации на рынке) как на родном, так и на иностранных языках;

– разрабатывать классификаторы информационных задач по всей совокупности объектов (явлений) наблюдения деловой разведки и формировать соответствующие базы данных. Работать с пространственно-распределенной картографической информацией – геоинформационными системами, представляющими собой закономерное расширение концепции баз данных, дополняющее их наглядностью представления и возможностью решать задачи пространственного анализа;

– использовать современные методы автоматизированной семантической обработки информации, в том числе основанные на методах искусственного интеллекта (например, методы автоматического перевода с различных языков, методы семантических сетей с использованием семантико-синтаксического анализатора и др.);

– использовать методы автоматизированной разработки отчетно-информационных документов;

– разрабатывать модели и методики решения основных задач деловой разведки (моделирование и методика вскрытия конкурентных угроз; изучение конкурентной обстановки и бизнес-процессов; анализ конкурента; определение конкурентноспособности, сильных и слабых сторон создаваемых продуктов; исследование конкурентоспособности фирмы: разведка намерений конкурента; оценка лояльности персонала внутри хозяйствующего субъекта и динамики ее изменения, выявление центров напряженности; вскрытие фальсифицированных данных, поступающих в высшие эшелоны управления компании от собственных сотрудников и исключение дезинформации высшего руководства и другие);

– оценивать эффективность деловой разведки.

Для решения этих задач должны быть привлечены как известные модели процессов добывания и обработки информации, так и модели и программное обеспечения, разработанное преподавательским составом и студентами (в процессе проведения исследований в рамках студенческого научного общества, практических занятий по дисциплинам информационные основы деловой разведки, информационно-аналитическая работа в деловой разведке, информационные системы и технологии в экономике и др.)

Заключение. Внедрение УСЦ в учебный процесс позволит существенно повысить его эффективность как на уровне бакалавриата, так и на более высоких уровнях образовательных траекторий.

СПИСОК ЛИТЕРАТУРЫ

1. Ситуационные центры в образовании [Электронный ресурс]. - Режим доступа: http://it-claim.ru/Library/Articles/publications_Philippovich_Andrew/sit_centres_education/sit_centres_in_education.htm (дата обращения 26.08.2017).
2. В МГИМО построена система учебных ситуационных центров [Электронный ресурс]. - Режим доступа: http://www.cnews.ru/news/line/v_mgimo_postroena_sistema_uchebnyh_(дата обращения 26.08.2017).
3. Маркова Н.И., Аксенова В.И., Первухин Н.А. Учебный ситуационный центр – инструмент интерактивных образовательных технологий в высшей школе [Электронный ресурс]. - Режим доступа: https://core.ac.uk/download/pdf/38165298.pdf; (дата обращения 26.08.2017).
4. Ситуационный центр [Электронный ресурс]. - Режим доступа: https://linguanet.ru/fakultety-i-instituty/institut-mezhdunarodnykh-otnosheniy-i-sotsialno-politicheskikh-nauk-fakultet/situatsionnyy-tsentr/ (дата обращения 26.08.2017).
5. Манушин М.А., Митин А.И. Учебный ситуационный центр как образовательная среда университета Москва: Издательство "Ритм", 2012.
6. Манышев В.В. Учебный ситуационный центр оперативного управления – новые технологии обучения [Электронный ресурс]. - Режим доступа: https://cyberleninka.ru/article/n/uchebnyy-situatsionnyy-tsentr-operativnogo-upravleniya-novye-tehnologii-obucheniya (дата обращения 26.08.2017).
7. Уникальная система учебных ситуационных центров МГИМО [Электронный ресурс]. - Режим доступа: http://www.allprojectors.ru/ap_module/content/article/400-professional/3009/11158 (дата обращения 26.08.2017).
8. Митин А.И. Учебные ситуационные центры в университетском образовании [Электронный ресурс]. - Режим доступа: http://www.iiorao.ru/iio/pages/izdat/ison/publication/ison_2013/num_16_2013/Mitin.pdf (дата обращения 26.08.2017).
9. Уникальная система учебных ситуационных центров МГИМО http://www.allprojectors.ru/ap_module/content/article/400-professional/3009/11158
10. Левкин И.М., Микадзе С.Ю. Добывание и обработка информации в деловой разведке. – СПб.: НИУ ИТМО, 2015.

УДК 004.72

ОСОБЕННОСТИ МОДЕЛИРОВАНИЕ САМОПОДОБНОГО СЕТЕВОГО ТРАФИКА

Татарникова Татьяна Михайловна
Санкт-Петербургский государственный экономический университет
Россия, Санкт-Петербург, ул Садовая, д 21
email: tm-tatarn@yandex.ru***Аннотация:*** Обсуждаются вопросы моделирования трафика, адекватно отображающего реальную нагрузку в сети, а также существующие подходы к имитационному моделированию самоподобного сетевого трафика.

Ключевые слова**:** *сетевой трафик, фрактальные свойства трафика, методы моделирования самоподобного трафика*.

PECULIARITIES OF SIMULATING A SELF-SIMULATED NETWORK TRAFFIC

Tatiana Tatarnikova
Saint-Petersburg State University of Economics
Russia, St. Petersburg, Sadovaya str, 21
email: tm-tatarn@yandex.ru

Abstract: Discusses the issues of modeling traffic that adequately reflects the real load on the network, as well as existing approaches to simulating simulated self-similar network traffic.

Keywords: *network traffic, fractal properties of traffic, methods for modeling self-similar traffic.*

Введение. При проектировании и модернизации инфокоммуникационных систем и сетей возникают многочисленные задачи моделирования трафика, адекватно отображающего реальную нагрузку в сети.

Объединение новых и существующих технологий передачи и коммутации данных с разнородными смесями сервисов и приложений сделали пакетный трафик более сложным, охватывающим сильно отличающиеся масштабы времени – от микросекунд до секунд и даже минут. При этом, в каждом масштабе времени возможны, как периоды активности со всплесками нагрузки, так и менее активные периоды.

Исследования различных типов сетевого трафика за последние полтора десятка лет доказывают, что сетевой трафик является фрактальным (fractal) по своей природе и структуре [1].

1. Фрактальные свойства сетевого трафика. К фрактальным свойствам обычно относят такие понятия, как долговременная зависимость и самоподобность.

Эти свойства, полученные в результате наблюдения за реальным сетевым трафиком, существенно отличаются от свойств трафика, сгенерированного традиционными моделями.

В-первых, традиционные модели пакетного трафика являются кратковременно зависимыми, то есть имеют экспоненциально затухающие корреляции; данные измеренного пакетного трафика проявляют долговременную зависимость, то есть гиперболически затухающие корреляции. К основным факторам, которые могут вызывать в сетевом трафике долговременную зависимость, относят: поведение пользователя, объединение трафика, средства управления сетью и другие.

Во-вторых, свойство самоподобности связано с особой структурой трафика – присутствие некоторого количества выбросов при относительно небольшом среднем уровне трафика, сохраняющейся при многократном масштабировании. На практике это проявляется в том, что пакеты, при высокой скорости их движения по сети, поступают на узел не по отдельности, а целой пачкой. В традиционных моделях сетевого трафика удается отобразить проявление пульсирующего характера на коротких масштабах времени, но пульсации сильно сглаживаются на длинных временных масштабах, что свидетельствует об отсутствии долговременной зависимости.

В результате оказывается, что традиционный анализ характеристик инфокоммуникационных систем и сетей, в основе которого лежит предположение о пуассоновском потоке, не может достаточно точно предсказать производительность сети или узла в условиях пульсирующего трафика, которому свойственна долговременная зависимость. Самоподобность приводит к увеличению потерь, задержке, джиттера при прохождении трафика через узлы сети [2, 3 с. 49].

Говорят, что распределение случайной переменной X медленно затухает (имеет «тяжелый хвост»), если

$$1 - F(x) = P[X - x] \sim \frac{1}{x^{\alpha}} \text{ при } x \to \infty,\ \alpha > 0. \quad (1)$$

Показатель α отвечает за тяжесть «хвостов» устойчивого распределения, и, следовательно, за пульсирующую структуру процесса. Показатель α может принимать значения на интервале [0, 2). Чем меньше это значение, тем тяжелее «хвост».

Для характеристики пульсаций трафика применяют статистические критерии, связанные с распределением интервалов между поступлениями. Это отношение пика к среднему значению интенсивности трафика (PMR – Peak to Mean ratio). Считается, что для компьютерных систем обычным является отношение 1000:1. В качестве меры пульсирующей структуры при принятии концепции самоподобности был предложен показатель Херста H, который связан с параметром α отношением H =(3 – α)/2 [4].

2. Обзор методов моделирования самоподобного трафика. На сегодняшний день разработано множество моделей, предназначенных для имитации фрактального трафика. Анализ доступных публикаций по моделированию самоподобного трафика позволяет выделить следующие модели.

Фрактальное броуновское движение (Fractional Brown Motion − FBM). В основе модели FBM лежит случайный процесс движения некоторой гипотетической частицы, которая совершает хаотическое перемещение в пространстве. Движение частицы рассматривается как результат большого количества малых случайных смещений. В отличие от классического броуновского движения у фрактальной модели отдельные шаги перемещения не являются абсолютно случайными и независимыми, а определяются предысторией движения во все предыдущие моменты. Зависимость перемещения броуновской частицы вдоль одной из пространственных координат от времени задается следующим соотношением:

$$B_H(t) = \frac{1}{\Gamma(H - 1/2)} \int_{-\infty}^{t} K(t - t')dB(t'), \quad (2)$$

где Г(.) – гамма функция;

H – показатель Херста, определяющий фрактальную размерность кривой, 0 ≤H ≤1;

dB(t ') – независимые случайные перемещения обычной броуновской частицы в моменты времени t';

функция K (t - t ') отвечает за память системы и определяется следующим соотношением:

$$K(t-t') = \begin{cases} (t-t')^{H-1/2}, & 0 \le t' \le t \\ (t-t') - (-t')^{H-1/2}, & t' \le 0. \end{cases} \quad (3)$$

Получаемые в результате моделирования фрактальные кривые являются самоаффинными, а не самоподобными. Кроме того, эти кривые являются однозначными.

Фрактальный гауссовский шум (Fractional Gaussian Noise − FGN). FGN – стационарный в широком смысле стохастический процесс с определенным параметрами (средним значением, дисперсией, показателем Херста) и автокорреляционной функцией заданного вида. По сравнению с обычным гауссовым шумом, FGN имеет дополнительный параметр Херста, который количественно определяет степень фрактального масштабирования.

Для построения берется отрезок единичной длины на оси абсцисс X. Этот отрезок разбивается на N = 2m частей, где m – любое положительное целое число.

Исходный единичный отрезок постепенно разбивается на более мелкие части посредством многократного деления пополам. При этом каждый раз вычисляется значение функции y в середине нового рабочего отрезка x, исходя из значений yleft и yright в граничных точках этого отрезка xleft и xright. Для этого используется следующее выражение:

$$y_c = \frac{(y_{left} + y_{right})}{2} + h, \quad (3)$$

где h – случайная величина, распределенная по нормальному гауссову закону с нулевым средним и дисперсией D, которая определяется следующим соотношением:

$$D = r^H, \quad (4)$$

где r = (xright - xleft) / 2 – расстояние от средней точки рабочего отрезка x, здесь вычисляется новое значение функции, до концов этого отрезка;

H – показатель Херста, непосредственно связанный с фрактальной размерностью моделируемой кривой. Основная трудность использования FBM и FGN – подбор наилучших значений параметров для получения генерируемого трафика, близкого по свойствам к экспериментально снятым реализациям трафика [5], [6].

Хаотические отображения (Chaotic Map – CMAP). Такие модели являются достаточно распространенными и концептуально простыми, они используют меньшее число параметров, чем FGN и FBM, и их выбор имеет более наглядную трактовку.

В основе лежит логистическое уравнение следующего вида:

$$X_{n+1} = CX_n - C(X_n)^2 = CX_n(1 - X_n), \quad (5)$$

где C – внешний параметр, определяющий скорость распространения случайной величины X и определяет границу перехода от равновесия к состоянию хаоса, при

– C<1 с ростом n фрактальность значений X вымирает;

– в области 1<C<3 значение пачки (фрактала) приближается к постоянному значению X0=1-1/C, что является областью стационарных фиксированных решений;

– при значении C=3 функция уже никогда не сходится в одной точке;

– в диапазоне 3<C<3,57 начинает проявляться самоподобность, функция колеблется между двумя значениями: сначала резко возрастает, а потом уменьшается;

– при C≥3,57 поведение становится хаотичным.

Модели на основе техники «динамического моделирования Маркова» (Dynamic Markov Modelling – DMM). Эти модели представляют собой автоматы с конечным числом состояний, изображаемые орграфами или диаграммами состояний модели. В процессе обучения модели, при получении очередного символа входного потока, происходит переход модели в следующее состояние и модификация частотных счетчиков, соответствующих вероятностям переходов. Выходом модели является набор вероятностей появления символов.

Модели с использованием нечеткой логики. Построение нечетких моделей, как правило, основано на настройке функций принадлежности по параметрам нечетких множеств, используемых в правилах, весов правил и на настройке операций.

Задание уровней пачечности может быть представлено в виде ступенчатой функции полезности. В таблице 1 показан пример, как может быть задан самоподобный трафик ступенчатой функцией полезности.

Таблица 1

Вероятность − *P*	Объем пачки − *S*
≤ *P*0	*S*0
] *P*0 ÷ *P*1]	*S*1
] *P*1÷ *P*2]	*S*2
] *P*2÷ *P*3]	*S*3
> *P*3	*S*4

Нейросетевые модели, которые позволяют решить задачу аппроксимации функций нескольких переменных по обучающей выборке путем погружения временного ряда в многомерное пространство. Временной ряд самоподобного процесса задается в виде:

$$\{X(t),\ t \in \overline{1, N}\}, \tag{7}$$

где X(t) – интенсивность трафика в момент времени t.

Тогда для построения нейронной сети вектор входных переменных будет задан как:

$$Z(t) = \{t, X(t), X(t-1),\ldots, X(t-4)\}, \tag{8}$$

Необходимо построить отображение вида:

$$Y(t) = \hat{F}(Z(t)), \tag{9}$$

где $\hat{F}(.)$ – оператор нейросетевого отображения.

Авторегрессионные модели (Autoregressive Models − AR) широко применяются для моделирования и предсказания благодаря свойству длительной памяти самоподобных процессов. В этих моделях текущее значение генерируемой величины рассчитывается как взвешенная сумма N предыдущих отсчетов плюс случайная переменная. Суть всех этих моделей в общем виде может быть представлена таким образом «завтра будет также, как в среднем за прошедшее время».

Как разновидности таких моделей используются модели ARMA − процесс «скользящего среднего», смысл которых заключается в том, что учитывается только ближайшее прошлое на заданное количество отсчетов по времени в глубину и следующая пачка трафика строится, основываясь только на этих данных. Например, для трех отсчетов выражение для прогноза следующей пачки трафика будет выглядеть следующим образом

$$X(t) = [X(t-1) + X(t-2) + X(t-3)]/3. \tag{10}$$

Известны и такие разновидности модели, как ARIMA − интегральный процесс скользящего среднего и FARIMA − фрактальный интегральный процесс скользящего среднего

$$X(t) = \beta_0 + \beta_1 X(t-1) + \beta_2 X(t-2) + \ldots, \tag{11}$$

где βi – коэффициент регрессии, которые подбираются исходя из прошлых наблюдений.

ON/OFF-модели. В этих моделях трафик рассматривается как комбинация источников, которые его генерируют. Каждый источник имеет следующую структуру. Некоторый период времени они могут генерировать пакеты информации (так называемые ON-периоды), при этом внутри одного периода пакеты приходят с одинаковыми интервалами между ними. После ON-периода следует OFF-период, когда источник не генерирует пакеты. Размер ON- и OFF-периодов является случайной величиной, которая, как показано в работе [1], должна иметь конечное математическое ожидание и бесконечную дисперсию.

Время T0, проведенное в состоянии OFF, это случайная переменная с функцией плотности вероятности w0(t), а время T1, проведенное в состоянии ON, это случайная переменная с плотностью вероятности w1(t). Распределения w0(t), w1(t) являются распределениями с «тяжелыми хвостами», то есть

$$w_i(t) \sim t^{-(\alpha+1)}, \text{ где } i = 0, 1, \alpha \in (1, 2) \text{ и } w_i(t) = 0 \text{ для } t < 0. \tag{11}$$

Средние времена T0 и T1, проведенные в каждом состоянии, являются конечными.

Заключение. Практически все рассмотренные модели подходят для моделирования самоподобного трафика инфокоммуникационных сетей с коммутацией пакетов. Все модели обладают такими необходимыми для качественного моделирования свойствами, как долговременная зависимость, маштабируемость, стационарность и т.д. Однако современные исследования экспериментально снятых реализаций трафика показывают, что характеристики трафика могут изменяться в самых широких пределах и зависеть от большого числа параметров и настроек реальных сетей, характеристик протоколов, передаваемой информации и поведения пользователей.

Общим недостатком, используемых в настоящее время моделей сетевого трафика, является их направленность на какую–либо конкретную разновидность трафика либо сети и отсутствие универсальности. Кроме того, применение их на практике приводит к большому объему исследовательской работы, требуемой для адаптации (обучения) модели к параметрам сетевой конфигурации или параметра трафика. Все это значительно усложняет построение универсальной модели, из-за большого разнообразия, как самих источников, так и сетевых конфигураций, оказывающих влияние на их работу.

СПИСОК ЛИТЕРАТУРЫ

1. Шелухин О. И., Осин А. В., Смольский С. М. Самоподобие и фракталы. Телекоммуникационные приложения. − М.: Физматлит, 2008. − 368 с.
2. Kutuzov O., Tatarnikova T. Evaluation and Comparison of Classical and Fractal Queuing Systems//XV International Symposium "Problems of Redundancy in Information and Control Systems", September 26-29, 2016. St. Petersburg, Russia.
3. Кутузов О.И., Татарникова Т.М. К оцениванию и сопоставлению очередей классических и фрактальных систем массового обслуживания//Информационно-управляющие системы. 2016. Т. 81. № 2. С. 48-55.
4. Кутузов О.И., Татарникова Т.М. Инфокоммуникационные сети. Моделирование и оценка вероятностно-временных характеристик. – СПб.: ГУАП, 2015. – 382 с.
5. Богатырев В.А. Имитационная модель поддержки проектирования инфокоммуникационных резервированных систем // Научно-технический вестник информационных технологий, механики и оптики. / В.А. Богатырев, Н.С. Кармановский, Н.А. Попцова, С.А. Паршутина, С.В. Богатырев.– 2016. Т. 16. № 5(105). – С. 831-838.
6. Татарникова Т. М. Имитационная модель виртуального канала / Т.М. Татарникова, М.А. Елизаров // Научно-технический вестник информационных технологий, механики и оптики. 2016. Т.16. № 6. С. 1120-1127.

УДК 004.72

МЕТОДИКА ПРОЕКТИРОВАНИЯ ГИС КОРАБЛЯ

Яготинцева Наталья Владимировна
Российский государственный гидрометеорологический университет,
Россия, Санкт-Петербург, Малоохтинский пр., дом 98,
email: solnishko234@yandex.ru***Аннотация:*** В статье рассматривается методика проектирования структурно-функциональной модели ГИС, предназначенная для решения задачи формирования инфраструктуры ГИС поддержки принятия решения при управлении морским судном. Методика включает описание архитектуры ГИС и последовательность действий для приближения этой архитектуры к заданному набору свойств.

Ключевые слова**:** *управление морским судном, ГИС корабля, архитектура ГИС, локальная вычислительная сеть, технология коммутации сегментов сети, методика проектирования.*

METHODOLOGY OF DESIGNING A GIS SHIP

Natalia Yagotinceva
Russian State Hydrometeorological University,
Russia, St. Petersburg, Malookhtinsky prospect, 98,
email: solnishko234@yandex.ru

Abstract: The article deals with the methodology of designing a structured and functional GIS model designed to solve the problem of forming a GIS infrastructure for decision support in the control of a ship. The methodology includes a description of the GIS architecture and a sequence of actions to bring this architecture closer to the specified set of properties.

Keywords: *ship's GIS control, GIS architecture, local area network, technology of switching network segments, design methodology*.

Введение. Методика проектирования ГИС морского судна (корабля) включает в себя, во-первых, алгоритм решения, обеспечивающий формирование инфраструктуры ГИС и во-вторых, приближение архитектуры ГИС к заданному набору свойств.

1. Структура ГИС корабля. ГИС корабля, представляет собой трехслойнойую структуру: внутренний слой, соответствует информационному обеспечению, средний – программному обеспечению и внешний – аппаратному обеспечению. Информационное обеспечение ГИС морского судна определяют картографические данные и данные, необходимые для управления судном, вместе они образуют электронные картографические навигационные информационные системы. Программное обеспечение реализует функциональные возможности ГИС и состоит из базового программного обеспечения, такого как операционные системы, системы управления базами данных, системы визуализации данных и других, и прикладного программного обеспечения, предназначенного для решения специализированных задач судовождения, обработки сигналов, обработки и передачи данных. Аппаратный слой ГИС представлен функциональными модулями (ФМ), состоящих из устройств и средств, реализующих соответствующую функцию (рисунок 1) [1-4].

Транспортной основой ГИС является локальная вычислительная сеть с коммутацией сегментов [5], технология построения которой позволяет одновременно передавать данные между всеми взаимодействующими парами «Клиент-Сервер» (рисунок 2) [6].

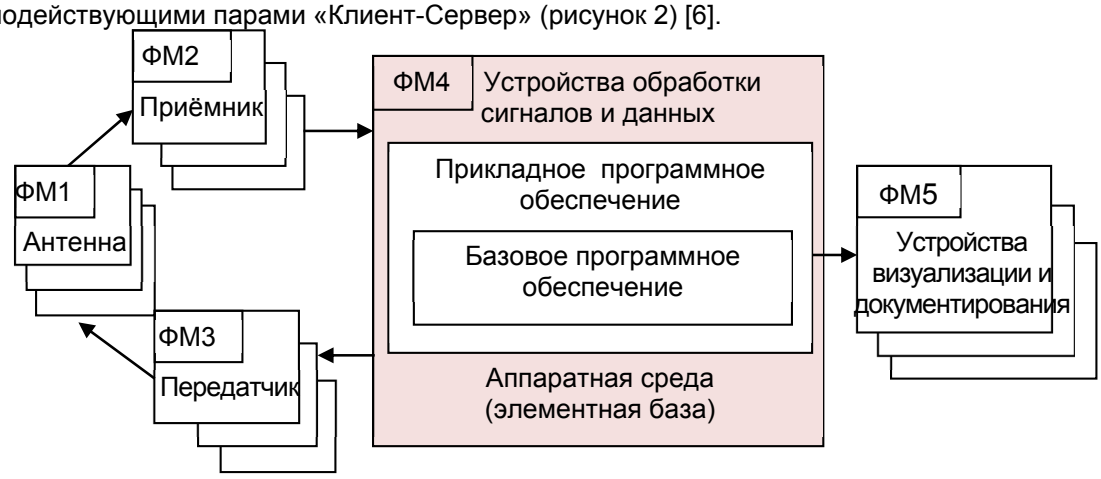


Рис. 1. Модель аппаратного обеспечения ГИС морского судна

Рис. 2. Схема взаимодействия Клиентов ГИС с серверной частью ГИС корабля

Модель ГИС представим количественно

$$G = f(P, C, S), \tag{1}$$

где G – структурно-функциональная модель ГИС морского судна;

P – множество параметров, которые задаются как технические требования на функциональные модули ГИС;

C – множество стоимостных характеристик функциональных модулей ГИС;

S – множество пространственных параметров (форм-факторов) функциональных модулей ГИС.

Выбор облика ГИС решается как целочисленная задача условной многопараметрической оптимизации с ограничениями второго рода по стоимости, производительности и ограничений на площади, выделяемые под проект ГИС:

$$C \to \min_{P} \tag{2}$$

где *C* – стоимость ГИС, которая является аддитивной функцией стоимостных характеристик ее составных элементов;

$$\overline{t}_{\text{дост}}(G) \le T_{\text{доп}}, \tag{3}$$

где $\overline{t}_{\text{дост}}(G)$ – среднее время доставки данных клиенту ГИС;

Тдоп – ограничения на время доставки, рекомендуемые стандартами распространения пространственных данных;

$$S \leq S_{доп}, \quad (4)$$

где Sдоп – ограничения на выделяемые площади под ГИС на судне.

2. Алгоритм формирования инфраструктуры ГИС. Алгоритм состоит из следующих действий:

– Определение исходных данных для построения ГИС.

– Исходными данными являются назначение объекта и морской район. Определение категории судна позволяет определить количество АРМ и предполагаемый объем геоинформации. Минимальный состав оборудования на судне дает морской район, который в Российской Федерации определяется Глобальной морской системой связи при бедствии (рисунок 3).

– Оценка временных характеристик.

Требования к времени обработки информации определяются исходя из времени приема пространственной информации с функциональных модулей ФМ1, ФМ2 и ФМ3 корабельной ГИС. Допустимое время передачи данных Тдоп будет прямо пропорционально удаленности источника распространения сигнала:

– в морском районе А1 максимальное расстояние от берегового источника составляет 30 миль, или приблизительно 48,28 км. Зная скорость распространения радиоволн Тдоп =32,1·10-5 с.

– в морском районе А2 максимальное расстояние от берегового источника составляет 100 миль, или приблизительно 160 км, следовательно Тдоп =106·10-5 с.

– в морских районах А3 и А4 для навигации используется спутниковые системы, в таком случае максимальное расстояние от источника составляет 20000 км, следовательно Тдоп =0,65·10-1 с.

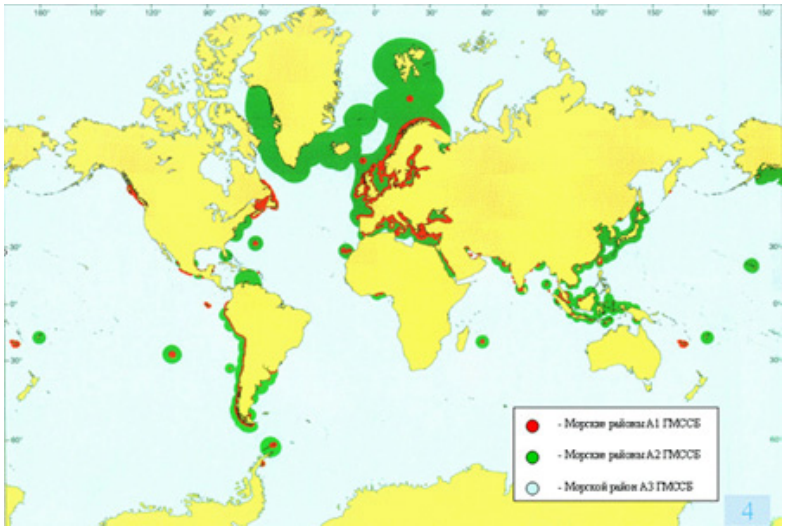


Рис. 3. Районы плавания

Минимальный состав оборудования в зависимости от района плавания приведен на рисунке 4.

Район	оборудование
А1, А2, А3, А4	УКВ радиостанция АИС Приемник ЦИВ Приемник НАВТЕКС Аварийный радиобуй
А2, А3, А4	Носимые УКВ СЧ/ПВ – радиоустановка с радиотелефоном Судовая земная станция «Инмарсат-С» с приемником расширенного группового вызова
А3, А4	ПВ/КВ – радиоустановка с радиотелефоном, ЦИВ и УБПЧ ПВ/КВ – радиоустановка для радиосообщений общего назначения
А4	Радиопередатчик 500 КГц Радиоприемник 500 КГц

Рис. 4. Минимальный состав оборудования

1. Оценка временных характеристик.

Требования к времени обработки информации определяются исходя из времени приема пространственной информации с функциональных модулей ФМ1, ФМ2 и ФМ3 корабельной ГИС.

Допустимое время передачи данных $T_{доп}$ будет прямо пропорционально удаленности источника распространения сигнала:

– в морском районе А1 максимальное расстояние от берегового источника составляет 30 миль, или приблизительно 48,28 км. Зная скорость распространения радиоволн $T_{доп}$ =32,1·10^{-5} с.

– в морском районе А2 максимальное расстояние от берегового источника составляет 100 миль, или приблизительно 160 км, следовательно $T_{доп}$ =106·10^{-5} с.

– в морских районах А3 и А4 для навигации используется спутниковые системы, в таком случае максимальное расстояние от источника составляет 20000 км, следовательно $T_{доп}$ =0,65·10^{-1} с.

2. Определение полного списочного состава элементов с техническими характеристиками, на которых строится ГИС, таких как канал связи и АРМы (процессор, жесткий диск, оперативная память) удовлетворяющего требованию производительности ГИС.

В случае если в списочном составе имеется по одному наименованию элементов, то этот список является единственным сценарием для комплексирования аппаратуры, удовлетворяющего требованиям. В обратном случае, проводится оптимизация структуры по стоимости и эргономике.

3. Определение «узкого» места в структуре ГИС.

При невыполнении директивных требований к передаче данных средствами моделирования определяется «узкое» место маршрута от источника *i* к приемнику *j* [7-9]. Это «узкое» место является причиной увеличения времени передачи данных.

3. Приближение архитектуры ГИС к заданному набору свойств. Последовательность действий для приближения архитектуры ГИС к заданному набору свойств (2)-(4) состоит в следующем:

1. Анализ исходных данных.

1.1. Определение минимального количества АРМ исходя из назначения и категории судна.

1.2. Определение минимального состава оборудования в зависимости от морского района плавания.

1.3. Определение количества узлов сети в зависимости от морского района плавания.

2. Расчет временных характеристик [10-11].

2.1. Определение временных характеристик доставки данных $t_{дост}$ до лица принимающего решение при управлении судном в зависимости от морского района плавания.

2.2. Проверка условия ограничения на время доставки $T_{доп}$, рекомендуемые стандартами распространения пространственных данных $t_{дост} \le T_{доп}$

3. Определение полного списочного состава облика ГИС.

3.1. Определение модели и количества коммутаторов как компонента локально вычислительной сети, исходя из директивных характеристик на установление соединения.

3.2. Определение вида кабеля, исходя из директивных характеристик на установление соединения и времени передачи.

3.3. Определение списка моделей процессоров, исходя из директивных характеристик обработки информации.

3.4. Определение списка моделей ОЗУ, поддерживаемые процессорами.

3.5. Определение списка моделей жесткого диска, исходя из директивных характеристик обработки информации.

3.6. Оптимизация списка оборудования обработки информации на АРМ по стоимостным характеристикам.

4. При невыполнении условия ограничения на $t_{дост}$, рекомендуемые стандартами распространения пространственных данных.

4.1. Определение участка маршрута, вносящего наибольшую задержку, исходя из модели «узкое» место.

4.2. Рекомендации замены «узкого» места на другой узел с лучшими характеристиками производительности.

Заключение. Предложенная методика проектирования структурно-функциональной модели ГИС предназначена для решения задачи формирования инфраструктуры ГИС поддержки принятия решения при управлении морским судном. В рамках верификации методики разработана экспертная система по выбору облика ГИС морского судна [12], которая позволяет в диалоговом режиме формировать списочный состав функциональных модулей и оборудования необходимого при проектировании.

СПИСОК ЛИТЕРАТУРЫ

1. Директоров Н.Ф., Катанович А.А. Современные системы внутрикорабельной связи. СПб.: Судостроение, 2001.
2. Татарникова Т.М., Яготинцева Н.В. Характеристика проблемы интеграции образцов радиоэлектронного вооружения корабля//Ученные записки РГГМУ. 2012. №25. С. 156-162.
3. Татарникова Т.М., Яготинцева Н.В. Новый подход к организации информационной инфраструктуры корабля//67-я научно-техническая конференция, посвященная дню радио: Сб. науч. тр. СПб. 2012. С. 24-25.
4. Татарникова Т.М., Яготинцева Н.В. Интеграция образцов радиоэлектронного вооружения на основе информационной транспортной сети корабля// Региональная информатика и информационная безопасность сборник трудов. Сб. науч. тр. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2015. С. 148-151.

5. Татарникова Т.М. Структурный синтез центра сопряжения корпоративных сетей//Информационно-управляющие системы. 2015. № 3 (76). С. 92-98.
6. Яготинцева Н.В. Модель информационной транспортной сети корабля// Региональная информатика и информационная безопасность сборник трудов: Сб. науч. тр. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2016. С. 415-418.
7. Татарникова Т.М., Яготинцева Н.В. Модель оценки характеристик локальной вычислительной сети корабля //Материалы международной конференции «Теоретические и прикладные проблемы науки и образования в 21-м веке», часть 5, Тамбов. С. 143-144.
8. Богатырев В.А., Богатырев А.В. Функциональная надежность систем реального времени**//**Научно-технический вестник информационных технологий, механики и оптики. 2013. № 4. С. 150-151
9. Татарникова Т.М., Яготинцева Н.В. Оценка функциональной надежности корабельной сети передачи данных// Известия высших учебных заведений. Приборостроение. 2014. Т. 57. № 9. С. 62-66.
10. Татарникова Т.М., Яготинцева Н.В. Вероятностная модель установления соединения в инфокоммуникационной сети// Известия высших учебных заведений. Приборостроение. 2017. Т. 60. № 2. С. 157-166.
11. Татарникова Т.М., Яготинцева Н.В. Предоставление услуг передачи данных на корабле // Инновационные технологии в сервисе: Сб. науч. тр. IV Международной научно-практической конференции. Под ред. А. Е. Карлика. 2015. С. 321-322.
12. Татарникова Т.М., Яготинцева Н.В. Принципы организации экспертной системы выбора структуры локальной сети корабля// Современное общество, образование и наука сборник научных трудов по материалам: Сб. науч. тр. Международной научно-практической конференции: в 16 частях. 2015. С. 142-144.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ИМПОРТОЗАМЕЩЕНИЕ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

УДК 004.94

РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ ИБ ДЛЯ КРИТИЧНОГО ОБЪЕКТА ТЭК

Лившиц Илья Иосифович[1], Маликов Владимир Викторович[2]
[1]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
Российская Федерация, 197101, Санкт-Петербург, Кронверкский пр., д. 49
[2] УО "Центр повышения квалификации руководящих работников и специалистов" Департамента охраны МВД Республики Беларусь,
223030 Минский р-н, Горанский с/с, р-н д. Горани,
emails: Livshitz.il@yandex.ru, malvvv104@mail.ru

***Аннотация*:** В статье рассматриваются аспекты создания современных систем управления, в частности, обеспечения заданных режимов функционирования и параметров контроля объекта. Для решения данной задачи применяются различные методики, которые подразумевают получение оценки безопасности для критичных объектов ТЭК. Однако в настоящее время не создано единого подхода к расчету безопасности для информационных систем, что не позволяет в должной мере реализовать безопасное управление сложными промышленными объектами ТЭК. В данном исследовании предпринята попытка анализа систем управления для сложных промышленных объектов с позиции определения безопасности такой системы. Представлен пример оценки систем в терминах термодинамической теории И. Пригожина

***Ключевые слова**: система управления, интегрированная система менеджмента; информационная система; информационная безопасность; аудит.*

THE DEVELOPMENT OF IT-SECURITY MANAGEMENT SYSTEM FOR CRITICAL INDUSTRIAL OBJECT

Livshitz Ilya [1], Malikov Vladimir [2]
[1] The St. Petersburg National Research University of Information Technologies, Mechanics and Optics
Kronverkskiy prospekt, 49, St. Petersburg, 197101, Russia
[2] “Center of improvement of professional skill of executives and specialists” of the Interior Ministry Department of the Republic of Belarus
Gorany, Goransky distr., Minsk, 223030, Belarus
emails: Livshitz.il@yandex.ru, malvvv104@mail.ru

Abstract: Creation the modern management systems it is important to provide specific modes of operation and parameters of control object. For this task apply a variety of techniques which involves the estimate of the Information systems. However, currently there is no common approach to the calculation of IT-Security for the Information systems, that is not taken into account in modern control systems of complex industrial facilities. This study attempts to analyze the control systems for complex industrial facilities from the position of determining the security assessment of such a system, explored the possibility of establishing systems in terms of thermodynamic theory of Ilya Prigogine.

***Keywords**: Management system, Integrated management system; Information system; Information security; Audit.*

Введение. При создании современных систем управления (СУ) представляется важным обеспечение не только заданных технологических режимов и параметров контроля объектов (в данном случае информационных систем — ИС), но и достижение определенной цели устойчивого безопасного функционирования ИС в составе сложного промышленного объекта (СлПО). Применительно к специфике объекта — ИС особое значение приобретает не только обеспечение устойчивости, но и в целом проблема обеспечения информационной безопасности (ИБ).

В настоящее время для решения данной комплексной задачи применяются различные методики, часть из которых подразумевает учет различных компонент — внутренних и внешних подсистем и мониторинг ИС: работы Агуреева [1-5] и работы зарубежных ученых [6-8]. В современных риск-ориентированных стандартах введен специальный термин, описывающий влияние внутренних и

внешних подсистем — «контекст» [9-12]. В известных работах поддерживается тезис, что «мониторинг (энтропии) в информационной системе целесообразен для поддержания устойчивой работы» [9-21]. В данной работе авторы расширяют классический термин ИБ [9], в том числе и на свойство обеспечения устойчивости СлПО. Также в ряде изданий отмечается, что это свойство в ИС имеет физический смысл и может быть рассчитана и измерена косвенными методами» [14, 15, 22, 21]. Далее под открытой системой понимается СУ для СлПО, в состав которой входят ИС, для которых необходимо обеспечение ИБ, в том числе — обеспечение функциональной устойчивости (в терминах [14, 24, 26]). Однако в ряде публикаций отмечается, что в ИС диссипация (рассеяние информации) в «чистом виде» не существует [19-21]. Этот факт может означать, что в настоящее время «чистые» ИС (и конкретно — ИС в составе СУ для СлПО) не рассматриваются с должным вниманием к протекающим процессам, в том числе — с точки зрения обеспечения безопасности. Соответственно, для СУ и систем обеспечения ИБ в их составе, не предложено описание потоков энергии и уравнения полной энергии, в том числе с учетом диссипативного характера.

Формирование пространства состояний для открытых систем. Современный этап развития теории управления и, соответственно, синтез СУ, включает в себя не только моделирование физических аспектов функционирования систем обеспечения ИБ (насколько это необходимо для создания адекватной модели), но и учет аспектов экономических факторов. Вторая (экономическая) часть СУ необходима для учета внешних аспектов любой открытой системы (в терминах стандартов [9-12]) и разнородной структуры требований. Влияние указанных аспектов позволяет осуществить учет как внешних аспектов открытой системы, так и разнородной структуры требований безопасности [9-11]. Построение обобщенной модели СУ начинается с формирования начальных условий, определяющих состояния объекта управления в моменты времени (t_1,…, t_k). Для подсистемы управления ИБ важно, чтобы выбор шага (дискретности) был четко увязан с известным множеством ограничений, связанных с особенностями функционирования СлПО. Например, на объектах электроэнергетики рекомендуется формировать несколько представлений энергетического состояния СУ и далее контролировать их расхождения в зависимости от воздействий [24, 25]. В частности, различные состояния функциональной безопасности возможно отследить, начиная от начального состояния СУ — Z_1, и далее под воздействием условий к состоянию ΔZ_1. Состояния СУ предлагается обозначать как Z_1, Z_2, Z_K. В рассматриваемой системе каждый компонент под воздействием особых условий (в терминах [24] — «условия принуждения») меняет свое состояние: $Z_1 \rightarrow Z_2$. Соответственно, это позволяет предложить общую схему формирования пространства состояний Z_K (рисунок 1). В этой схеме учтены начальное состояние Z_1, воздействия («условия принуждения») перехода в последующие состояния (ΔZ_1) и дискретные моменты времени (t_1, …, t_k).

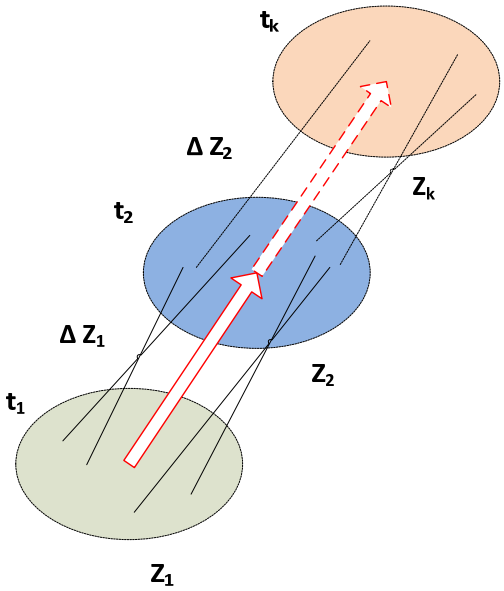


Рис. 1. Формирование пространства состояний открытой системы

Рассмотрим далее пример СлПО в терминологии [17], для которого целесообразно представить более подробное описание необходимых параметров модели с учетом обеспечения функциональной безопасности.

Общая модель объекта. Рассмотрим общую модель более сложной системы, которая включает СлПО (как объект управления) и СУ, реализованную на базе интегрированной системы менеджмента (ИСМ) в терминах [12] (рисунок 2).

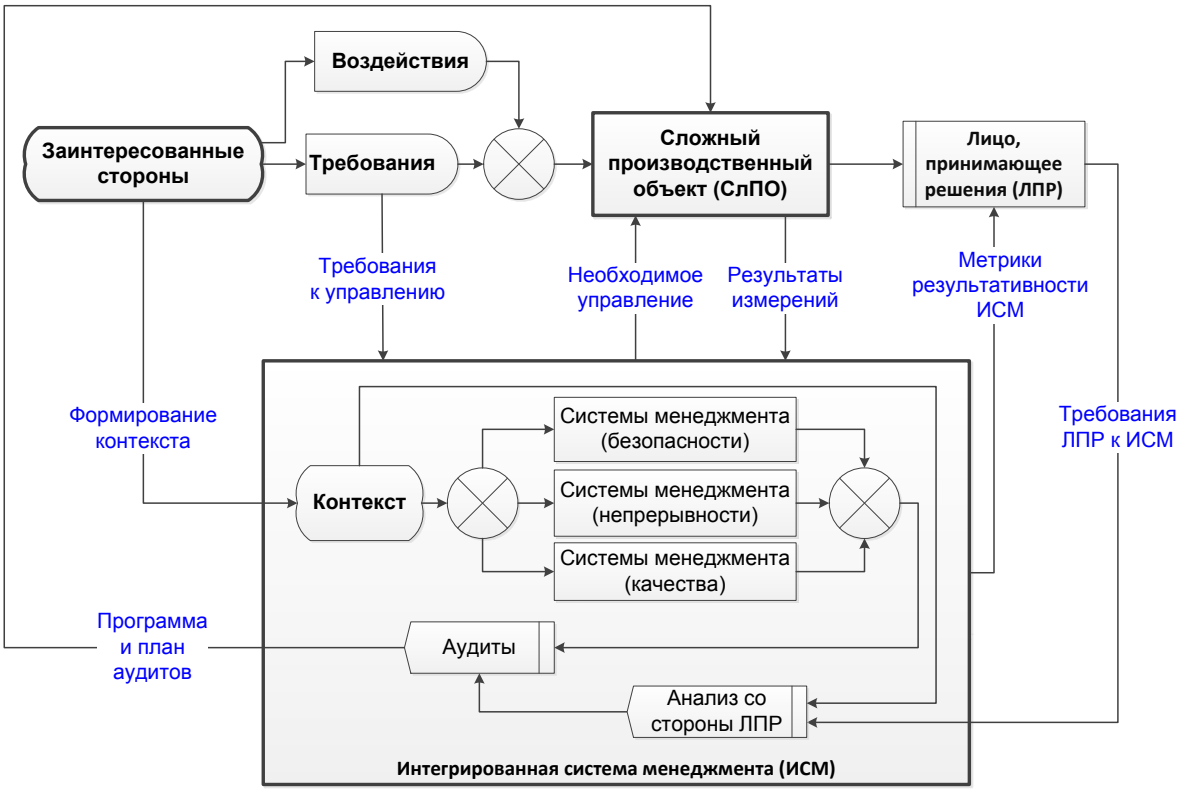


Рис. 2. Общая модель ИСМ для обеспечения безопасности СлПО

Моделирование СлПО выполняется для оценивания функций безопасности и, прежде всего, управления множеством процессов ИБ. С учетом применения риск-ориентированных стандартов в ИСМ важным представляется гарантирование «замыкания» цикла «Plan-Do-Check-Act» (PDCA) при управлении ИБ для СлПО и формирование контекста для управления СлПО как «открытой системы» в терминах И. Пригожина [26]. Для общей модели предлагается выделить следующие основные векторы: это векторы входных, внутренних, внешних и выходных параметров соответственно:

{ xi (t) } = x (t) — вектор входных параметров;
{ qi (t) } = q (t) — вектор внутренних параметров;
{ yi (t) } = y (t) — вектор выходных параметров;
{ zi (t) } = z (t) — вектор внешних параметров;
где i = 1, n.

При данном допущении функциональные уравнения относительно выходных параметров возможно определить в обобщенном виде:

$$y(t) = F\,[x(t), q(t), z(t)] \qquad (1)$$

где оператор F реализует закон изменения состояния системы:

$$y(t_1) = F_1\,[\,Z_1(t_1), Z_2(t_2), t(t_1)]$$

$$y(t_k) = F_k\,[\,Z_{k-1}(t_{k-1}), Z_k(t_k), t(t_{k-1})]$$

Поскольку в обобщенной модели рассматривается именно «замкнутый» цикл управления ИБ в СУ для СлПО посредством аудитов (принятых в ИСМ), возможно выполнить сопоставление планируемых и реальных состояний объекта управления (СлПО) в каждый конкретный интервал времени. Тогда определим:

$$y(t_1)_{\text{план}} = F_1\,[\,Z_1(t_1), Z_2(t_2), t(t_1)]$$

$$y(t_1)_{\text{факт}} = F_2\,[\,Z_1(t_1), Z_2(t_2), t(t_1)]$$

и представим решение поставленной задачи как анализ существующих отклонений Δ y:

$$\Delta\, y = y(t_1)_{\text{план}} - y(t_1)_{\text{факт}}$$

$\Delta\, y \;\to 0$.

Подробное конкретное решение оптимизационной задачи не рассматривается в рамках данной публикации.

В работах [24, 25] приводится пример оценивания различных систем с позиции их развития (деградации), что может быть выполнено на плановой основе (например, в рамках периодических аудитов ИБ в ИСМ) и тем самым обеспечен контроль и финансовых параметров функционирования объекта управления (СлПО) [18]. Соответственно, для системы аудитов ИБ в ИСМ предлагается следующая базовая модель (рисунок 3), в которой учтены все основные векторы, указанные выше; реализована возможность сопоставлять планируемые и реальные состояния объекта управления (как

объекта оценки), реализуется «замкнутый» цикл аудитов PDCA (в смысле выполнения всех обязательных процедур аудита ИБ согласно [10]).

Для конкретной задачи управления ИБ в СУ для СлПО «замкнутый» цикл аудитов означает гарантированное достижение результатов всех фаз PDCA, выявления несоответствий и самое важное — получение гарантий результативного выполнения всех запланированных корректирующих действий в отношении всех выявленных несоответствий применительно к ИБ [10, 12, 18].

Рис. 3. Базовая модель аудитов ИСМ

Обратим внимание, что в базовой модели вводятся различные интерфейсы предоставления данных (внутренний и внешний), что, во-первых, отражает требования стандартов ИБ [9], во-вторых, определяет требования лица, принимающего решения (ЛПР) в части ограниченного распространения чувствительных данных [16]; и в-третьих, учитывает необходимость коммуникаций открытой системы с внешней средой с позиции энергетического обмена [19, 20, 27].

Заключение. На основании учета компонент различной природы предложен подход к формированию оценки в СУ для СлПО для обеспечения функциональной безопасности, как расширение классического базового понятия «информационная безопасность». Показана возможность рассмотрения современных СУ для СлПО с целью достижения устойчивого функционирования и обеспечения требуемого уровня ИБ.

СПИСОК ЛИТЕРАТУРЫ

1. Агуреев И.Е., Денисов М.В. Математическое описание динамики пассажирских транспортных систем // Мир транспорта и технологических машин. 2011. Вып. 1. С. 15-22.
2. Агуреев И.Е., Тропина В.М. Динамика логистической системы в транспортных цепях поставок // ИзвестияТулГУ. Технические науки. 2011. Вып. 4. С. 158-167.
3. Агуреев И.Е., Атлас Е.Е., Пастухова Н.С. Хаотическая динамика в математических моделях транспортных систем // Известия ТулГУ. Технические науки. 2012. № 3. С. 372-389.
4. Агуреев И.Е., Богма А.Е., Пышный В.А. Динамическая модель транспортной макросистемы // ИзвестияТулГУ. Технические науки. 2013. Вып. 6. Ч. 2. С. 139-145.
5. Агуреев И.Е., Гладышев А.В. Динамика производства и спроса в диссипативной модели логистической системы // ИзвестияТулГУ. Технические науки. 2013. Вып. 6. Ч. 2. С. 152-160.
6. Baumgarte J. Stabilization of constraints and integrals of motion in dynamical systems // Comp. Math. Appl. Mech. Eng. 1972. No. 1. P. 1-16.
7. Ascher U.M., Hongsheng Chin, Petzold L.R., Reich S. Stabilization of constrained Mechanical systems with DAEs and invariant manifolds // J. Mechanics of Structures and Machines. 1995. Vol. 23. P. 135-158.
8. Amirouche F. Fundamentals of Multibody Dynamics. Theory and Applications. Birkhauser, Springer, 2005. 684 p.
9. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements, International Organization for Standardization. 2013. 23 p.
10. ISO 19011:2011.Guidelines for auditing management systems;
11. ISO 55001:2014 Asset management – Management systems – Requirements // International Organization for Standardization, 2014. – 14 pages.
12. PAS-99:2012 «Specification of common management system requirements as a framework for integration»

13. Хайтун С.Д. Трактовка энтропии как меры беспорядка и ее негативное воздействие на современную научную картину мира // Вопросы философии. 2013. Вып. 2. С. 62.
14. Шеннон К. Работы по теории информации. – М.: Изд-во иностранной литературы. 1966. 88 с.
15. Лившиц И.И. Практические применимые методы оценки систем менеджмента информационной безопасности // Менеджмент качества. 2013. Вып. 1. С. 22–34.
16. Лившиц И.И. Подходы к применению модели интегрированной системы менеджмента для проведения аудитов сложных промышленных объектов – аэропортовых комплексов // Труды СПИИРАН. 2014. Вып. 6. С. 72–94.
17. Лившиц И.И. Методика выполнения комплексных аудитов промышленных объектов для обеспечения эффективного внедрения систем энергоменеджмента // Энергобезопасность и энергосбережение. 2015. Вып. 3. С. 10-15.
18. Лившиц И.И. Формирование концепции мгновенных аудитов информационной безопасности // Труды СПИИРАН. 2015. Вып. 6. С. 272 – 300.
19. Андрианова Е.Г., Мельников С.В., Раев В.К. Диссипация и энтропия в физических и информационных системах. Фундаментальные исследования. 2015. Вып. 8. С. 233 – 238
20. Кудж С.А., Цветков В.Я. Особенности развития направлений информатики // Перспективы науки и образования. 2013. Вып. 6. С. 11.
21. Маркин А.А., Мельников С.В. Философский и естественнонаучный аспекты понятия информационной энтропии // Труды российской научной конференции «Инновационные стратегии развития науки, техники и общества», Минобрнауки РФ, МГТУ МИРЭА. М., 2014. С. 98–102.
22. Аюров В.Д. Круговорот товаров и физика денег. Неделя горняка - 2003. - ГИАБ, Изд-во МГГУ. 2003. Вып. 5. с. 90
23. Аюров В.Д. Синергетика экономики. М.: Изд-во МГГУ. 2005. 124 с.: ил.
24. Игонин В.И. Технологические особенности энергообследования зданий, сооружений и инженерных сетей. // Курс лекций. – Вологда: ВоГТУ. 2012. 104 с.
25. Игонин В.И. Методология научных исследований и научно-техническое развитие «субъекта» // Методическое пособие для магистров. – Вологда. ВоГТУ. 2013. 111с.
26. Пригожин И., Гленсдорф П. Термодинамическая теория структуры, устойчивости и флуктуаций. М.: МИР. 1973. 124 с.
27. Тарасенко Ф. П. Прикладной системный анализ (наука и искусство решения проблем): Учебник. Томск; Издательство Томского университета, 2004. ISBN 5-7511-1838-3

УДК 004.94

ФОРМИРОВАНИЕ ТРЕБОВАНИЙ К ОЦЕНКЕ ДОВЕРИЯ КРИТИЧНЫХ ОБЪЕКТОВ НА БАЗЕ СОВРЕМЕННЫХ СТАНДАРТОВ ИСО

Лившиц Илья Иосифович[1], Маликов Владимир Викторович[2]
[1] Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»,
Российская Федерация, 197101, Санкт-Петербург, Кронверкский пр., д. 49
[2] УО "Центр повышения квалификации руководящих работников и специалистов" Департамента охраны МВД Республики Беларусь,
223030 Минский р-н, Горанский с/с, р-н д. Горани,
emails: Livshitz.il@yandex.ru, malvvv104@mail.ru

***Аннотация*:** В статье рассматриваются результаты революции в области ИТ, произошедшей в конце XX века, среди которых отмечен следующий: вопросы информационной безопасности (ИБ) практически полностью утратили самостоятельность и стали органичной и неотъемлемой частью ИТ. Соответственно, возросла значимость корректного определения сущностей, подлежащих защите, и именуемых активами в нотации стандарта ISO 27001. В работе рассмотрены несколько примеров несуществующих (или мнимых) активов, для которых применяется термин – «токсичный актив». Выявление таких активов очень важно для формирования требований к оценке доверия критичных объектов на базе современных стандартов ISO. Отмечается необходимость создания в России национальной, сбалансированной и самодостаточной индустрии ИТ, которая от базиса до самого верхнего слоя надстройки будет «пронизана» функциями безопасности. Представлено обоснование, что навык распознавания токсичных активов в области ИТ и очистки от них поможет специалистам существенно улучшить требуемый уровень ИБ.

***Ключевые слова**: система управления, система менеджмента информационной безопасности; активы; аудит.*

THE FORmulation OF REQUIREMENTS FOR ASSESSMENT OF CRITICAL OBJECTS BASED ON MODERN ISO STANDARDS

Livshitz Ilya [1], Malikov Vladimir [2]
[1] The St. Petersburg National Research University of Information Technologies, Mechanics and Optics
Kronverkskiy prospekt, 49, St. Petersburg, 197101, Russia
[2] “Center of improvement of professional skill of executives and specialists” of the Interior Ministry Department of the Republic of Belarus
Gorany, Goransky distr., Minsk, 223030, Belarus
emails: Livshitz.il@yandex.ru, malvvv104@mail.ru

Abstract: The IT revolution, which had been in the XX century, had a very interesting consequence. During this revolution the IT-security almost completely lost its independence and become an organic and

integral part of IT. Respectively, increased the importance of correct determination of entities to be protected and referred to as assets in the notation of ISO 27001. The paper considers several examples of non-existent (or imaginary) assets, which introduced the term "toxic asset". It is noted that it is necessary to create in Russia a national full-length, balanced and self-sustaining IT industry, which from the basis to the top layer of the add-in should be "riddled" with security features. Presents the rationale that learning to recognize the toxic assets in the field of it and cleaning them, the professionals can significantly improve the required level of IT-security.

Keywords: *Management system, IT-Security management system; Asset; Audit.*

Введение. Замысел статьи появился под впечатлением от документа Организации по безопасности и сотрудничеству в Европе (ОБСЕ) «Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства» (далее – Руководство) [1]. Одна деталь Руководства заставила авторов задуматься о целесообразности дополнения широко используемого в мире информационных технологий (далее – ИТ) понятия актива, еще одной характеристикой – токсичностью. Заметим, что мир финансов, в свое время утративший видение меры и получавший проблемы нестабильных инвестиций, ввел общее понятие «токсичного» актива. Токсичность актива, безусловно, величина относительная, т.е. со временем может изменяться (интересующихся точными примерами классификации и базовыми процессами управления активами просят ознакомиться со стандартами ISO серии 27000 или их аналогами ГОСТ Р ИСО) [2 – 5]. Положительным следствием введения понятия токсичного актива в мире финансов явился вывод ряда активов из некой зоны стыдливого умолчания, организацию их учета и контроля и в целом усиления институционально роли надзора.

Революция в области ИТ, произошедшая в конце XX века за рубежом, имела одно весьма интересное следствие. В ходе революции вопросы информационной безопасности (далее – ИБ) практически полностью утратили самостоятельность и стали органичной и неотъемлемой частью ИТ [6 – 8]. Данный тезис подтверждается многими фактами из зарубежной практики: это и структура организаций, их процессы, и практика взаимодействий организаций [9, 10]. Поскольку сегодня общее понятие «ИТ» органично включают в себя вопросы ИБ, то далее уместно говорить предметно не только о токсичности активов, но и о влиянии токсичных активов на ИБ.

Документы, датированные 90-ми годами прошлого века, представляются несколько утратившими актуальность. ИТ являются чрезвычайно динамичной направлением, в котором все меняется быстро и непрерывно. Соответственно, самые актуальные документы – это документация производителей на компоненты систем обработки информации (далее – СОИ). За ними стараются «успеть» международные стандарты и нормативные документы государств, имеющих под своей юрисдикцией развитую индустрию ИТ. В последнее время наблюдается переход к сертификации средств защиты в соответствии с ГОСТ 15408 [11 – 13]. ГОСТ 15408 абсолютно адекватный документ, являющийся переводом международных стандартов ISO/IEC серии 15408. В реальной СОИ вероятность преодоления защиты не равна нулю, и для того чтобы связать вероятность такого события с последующим ущербом давно используют понятия рисков ИБ (например, ранее Guide 73, позже ISO 27005). В мире для организаций уже созданы реестры рисков общепринятых «отраслевых» форматов (Basel, SOLAS-74, ISO 31000, IATA).

Здесь можно рекомендовать создание технологии, в которой все решения в области ИБ и их компоненты будут изначально разрабатываться в едином безопасном процессе, например Security Development Lifecycle (SDL). Для этого потребуется создать структуру, подобную Configuration Management Database (CMDB), для контроля уровня безопасности, поддержки версионности и отслеживания «родителей» и «потомков» всех оцененных по требованиям ИБ компонент — программных и аппаратных. Финальная «сборка» защищенных ИС возможна только из «доверенных» компонент, прошедших в установленном порядке все положенные тесты ИБ, внесенных в национальную CMDB и позволяющих обеспечивать заданный уровень ИБ. В РФ уже существуют необходимые национальные стандарты для реализации SDL, в частности:

1. ГОСТ Р ИСО/МЭК 12207—2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств»;
2. ГОСТ Р 51583—2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

Следующая сложность обеспечения требуемого уровня ИБ — создание национального полного замкнутого цикла управления ИБ, например, по образцу ЖЦ в NIST (специальные публикации NIST: FIPS 199/SP 800-60 «Информационная безопасность», FIPS 200/SP 800-53 «Меры обеспечения безопасности и приватности для Федеральных информационных систем и организаций»):

1. Категорирование активов (FIPS 199/SP 800-60);
2. Выбор мер безопасности (FIPS 200/SP 800-53);
3. Реализация мер безопасности (SP 800-160);
4. Оценка мер безопасности (SP 800-53A0);
5. Мониторинг мер безопасности (SP 800-137).

В качестве основы индустрии ИТ должен рассматриваться гражданский сектор ИТ, как самый массовый и динамичный, с их развитием и адаптацией под специфические требования. Это обеспечит сбалансированность индустрии, которую можно будет схематично представить в виде пирамиды, в основании которой лежит гражданский широкий сектор, а выше к вершине – специальные сектора.

Необходимо безусловно обеспечить единообразие и прозрачность процедур оценки соответствия требованиям ИБ, для чего необходимо внести изменения в нормативно-правовые акты по техническому регулирования. В целях обеспечения процедур оценки соответствия, предлагается признать целесообразным использование для данных целей установленных как ГОСТ Р актуальных международных документов:

1. ГОСТ Р ИСО/МЭК серии 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»;
2. ГОСТ Р ИСО/МЭК серии 27000 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности».

Использование вышеперечисленных документов обеспечит единство шкал и методов оценки соответствия с зарубежными центрами компетенций в области ИТ, что позволит объективно, в сопоставимых измеряемых величинах, оценивать степень соответствия российских ИТ мировому уровню (кстати, это уже делают в «Лаборатории Касперского» в AV-TEST).

Доверие к системе, типовым способом формирования которого в настоящее время является «доверие через оценку». Но для того чтобы получать адекватные результаты, нужно понимать, в какой момент времени производить оценку. Мировая практика предусматривает оценку «по мере необходимости». Применение данного подхода в российских условиях диктует необходимость отказа от лицензирования деятельности в области защиты открытой информации (оставив только безусловное обеспечение безопасности ОГВ) и проведения оценки соответствия в открытых и прозрачных системах, поддерживаемых сообществом участников рынка ИТ. Представляется целесообразным производить оценку безопасности в ИТ в соответствии с требованиями стандартов ИСО/МЭК 15408, а оценку процессов управления — ИСО/МЭК 27001.

Важной проблемой является обеспечение компетентных кадров для создания безопасного ЖЦ решений в области ИБ. К сожалению, приходится констатировать невысокий общий уровень подготовки специалистов по профильным специальностям в сфере ИБ даже в ведущих вузах РФ. Участие в аттестации магистров и бакалавров выявило наличие двух подходов к написанию дипломных работ: они либо полностью отвечают требованиям государственных регуляторов (например, по защите персональных данных) и при этом абсолютно не учитывают требования действующих в мире стандартов, либо разрабатываются под зарубежные спецификации и игнорируют национальные ограничения, например в области криптографии.

Заключение. Навык распознавания токсичных активов в области ИТ и очистки от них может существенно улучшить показатели устойчивости организации в России. Необходимо признать неизбежность того, что вопросы ИБ должны практически полностью утратить иллюзорную самостоятельность и стать неотъемлемой частью ИТ. Предлагается пересмотреть практикуемое в раздельное «выращивание» ИБ и ИТ и обеспечить формирования требований к оценке доверия критичных объектов на базе современных стандартов ISO.

СПИСОК ЛИТЕРАТУРЫ

1. Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства (http://www.osce.org/ru/atu/110472?download=true)
2. ISO/IEC 27000:2014. Information technology — Security techniques — Information security management systems — Overview and vocabulary, International Organization for Standardization, 2014. – 31 pages.
3. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements, International Organization for Standardization, 2013. – 23 pages.
4. ISO/IEC 27004:2009. Information technology — Security techniques — Information security management — Measurement, International Organization for Standardization, 2009. – 55 pages.
5. ISO/IEC 27005-2011. Information technology — Security techniques — Information security risk management, International Organization for Standardization, 2011. – 68 pages.
6. Лившиц И.И. Практическая оценка результативности СМИБ в соответствии с требованиями различных систем стандартизации: ИСО 27001 и СТО Газпром / Лившиц И.И., Полещук А.В. // Труды СПИИРАН. – 2015. – № 3. – С. 33 – 44.
7. Лившиц И.И. Подходы к решению проблемы учета потерь в интегрированных системах менеджмента // Информатизация и Связь. – 2013, № 1. – С. 57 – 62.
8. Лившиц И.И. Подходы к применению модели интегрированной системы менеджмента для проведения аудитов сложных промышленных объектов – аэропортовых комплексов // Труды СПИИРАН. – 2014, № 6. – С. 72 – 94.
9. Шишкин В.М., Юсупов Р.М. Доктрина информационной безопасности Российской Федерации — опыт количественного моделирования // Труды СПИИРАН. Вып. 1, т. 1. - СПб: СПИИРАН, 2002.
10. Юсупов Р. М., Шишкин В. М. О некоторых противоречиях в решении проблем информационной безопасности // Труды СПИИРАН. Вып. 6. — СПб.: Наука, 2008. С. 39–59.
11. ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель». 2012.
12. ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности». 2013
13. ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности». 201*3*

УДК 004.94

ОЦЕНКА ВЛИЯНИЯ СОВРЕМЕННЫХ РИСК-ОРИЕНТИРОВАННЫХ СТАНДАРТОВ НА ОБЕСПЕЧЕНИЕ ИБ КРИТИЧНЫХ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ

Лившиц Илья Иосифович[1], Маликов Владимир Викторович[2]
[1]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Российская Федерация, 197101, Санкт-Петербург, Кронверкский пр., д. 49
[2] УО "Центр повышения квалификации руководящих работников и специалистов" Департамента охраны МВД Республики Беларусь,
223030 Минский р-н, Горанский с/с, р-н д. Горани,
emails: Livshitz.il@yandex.ru, malvvv104@mail.ru

***Аннотация*:** В статье рассмотрена проблема оценки влияния современных риск-ориентированных стандартов для обеспечения безопасности и защищенности критичных и сложных промышленных объектов (СлПО). Основное внимание уделено обеспечению цикла PDCA для процессов обеспечения безопасности СлПО, в том числе – информационной безопасности (ИБ). Приведены практические примеры формирования унифицированной системы оценки безопасности СлПО для топливно-энергетического комплекса (ТЭК) на основании приказов ФСТЭК и современных стандартов ISO.

***Ключевые слова**: информационная безопасность, стандарт, система менеджмента информационной безопасности; сложный промышленный объект; активы.*

EVALUATION OF THE IMPACT OF ACTUAL RISK-BASED STANDARDS FOR IT-SECURITY ASSURANCE FOR AN CRITICAL INFRASTRUCTURE FACILITIES

Livshitz Ilya [1], Malikov Vladimir [2]
[1] The St. Petersburg National Research University of Information Technologies, Mechanics and Optics
Kronverkskiy prospekt, 49, St. Petersburg, 197101, Russia
[2] “Center of improvement of professional skill of executives and specialists” of the Interior Ministry Department of the Republic of Belarus
Gorany, Goransky distr., Minsk, 223030, Belarus
emails: Livshitz.il@yandex.ru, malvvv104@mail.ru

Abstract: This issue discusses the problem of assessing the impact of modern risk-oriented standards to ensure the safety and security of Complex Industrial Facilities (CIF). The main attention is paid to ensure the PDCA-cycle for general security processes of CIF, including IT-security. The practical examples of the formation of a unified system of safety CIF assessment for the fuel and energy objects on the basis both Russian FSTEC and modern ISO standards.

***Keywords:** IT-Security, Standard, IT-Security management system; Complex Industrial Facilities Asset.*

Введение. В настоящее время проблема формирования требований для обеспечения безопасности СлПО ТЭК является актуальной для специалистов в области обеспечения ИБ. Для лиц, принимающих решения (ЛПР) важно унифицировать совокупность требований, принятых на законодательном уровне: Федеральные законы, приказы ФСТЭК и дополнительно применять современные стандарты ISO, прежде всего ISO серии 27001 и «целевой» стандарт для энергетики ISO 50001, которые совместно формируют методологическую основу обеспечения ИБ для СлПО ТЭК.

Отметим, что в классическом труде Н. Винера по теории кибернетики отмечается: «Для получения приемлемых результатов в приемлемое время необходимо довести до максимума скорость элементарных процессов и добиться, чтобы течение этих процессов не прерывалось существенно более медленными шагами». Для выполнения требований нормативных документов и стандартов ISO предлагается далее применять обобщенный термин СлПО, под которым будем понимать «технический объект, несанкционированное изменение штатного режима функционирования которого, связанное с нарушением свойств ИБ, может привести к угрозе техногенных катастроф с необратимыми последствиями».

В любой системе менеджмента одним из важнейших вопросов является вопрос корректного выявления перечня активов (в нотации ISO 27000 – “asset”), для которых требуют обеспечить защиту от актов незаконного вмешательства. Для ТЭК проблему выявления и защиты критически важных промышленных объектов возможно сопоставить с общей проблемой выявления и защиты ценных для бизнеса активов СлПО в СМИБ и/или ИСМ. В стандартах ISO изложена четкая логика данного процесса – выделенная совокупность ценных (критичных) активов, намеченных ЛПР к защите в составе СМИБ объектов ТЭК, требует определенных ресурсов (временных, технических, персонал) для оценки уязвимостей, анализа соответствующих угроз, формирования файла рисков и плана обработки рисков. Однако на объектах ТЭК требуется принятие решений в режиме, близком к режиму реального времени.

Пример явно завышенного времени выполнения процесса показан в работе Л. Кини и Х. Райфа, когда ЛПР для обдумывания различных альтернатив может потребоваться неделя.

На основании сформированного перечня активов, подлежащих защите, на следующем шаге определяется перечень уязвимостей и угроз, для противодействия применяются определенные меры (средства) обеспечения ИБ (в нотации ISO 27000 – “control”). Конечной целью применения мер (средств) обеспечения ИБ является снижение потенциального ущерба (потерь) в отношении выбранных активов СлПО ТЭК до приемлемой меры (уровня риска), установленной ЛПР. Для формирования перечня угроз рекомендуется использовать совместно Приложение «В» стандарта ISO 27005 и Приказ ФСТЭК № 31. В качестве возможных критериев, используемых для определения ценности актива, могут быть выбраны: исходная (балансовая) стоимость, стоимость замены (воссоздания) актива в случае реализации неблагоприятного сценария акта незаконного вмешательства (события риска ИБ), или дополнительная ценность (например, ценность репутации и политических рисков).

Требования по выполнению проверок (аудитов) активов СлПО ТЭК установлены, соответственно, в п. 9.2 в ISO 27001 и п. 4.6.3 ISO 50001. Наиболее важные проверки на объектах ТЭК установлены Приказом ФСТЭК № 31 и, дополнительно ISO 27001 (см. Табл. 1). Отметим, что в Приказе ФСТЭК № 31 многократно отмечается важная роль ISO 27001 (даны прямые ссылки, соответственно, на п.п. 13.4 и 15.2).

Таблица 1.

Перечень проверок СлПО ТЭК

№ п.п.	Требование проверки	ФСТЭК Приказ 31	ISO 27001
1.	При проектировании системы защиты АСУ осуществляется проверка, в т.ч. при необходимости с использованием макетов или тестовой зоны.	14.1.	A.12.1, A.12.4, A.12.6
2.	При внедрении организационных мер защиты информации осуществляется проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий персонала АСУ	15.3.	A.7.2, A.9.2, A.14.2
3.	Предварительные испытания системы защиты АСУ проводятся с учетом ГОСТ 34.603 и включают проверку работоспособности системы защиты АСУ.	15.5.	A.14.2, A.14.3
4.	В ходе анализа угроз безопасности информации в АСУ и возможных рисков от их реализации осуществляются: — Периодический анализ изменения угроз безопасности информации в АСУ, возникающих в ходе ее эксплуатации; — Периодическая оценка последствий от реализации угроз безопасности информации в АСУ (анализ риска).	16.4.	A.8.1, A.12.6, A.12.7, A.16.1
5.	Меры по управлению обновлениями ПО должны обеспечивать безопасное получение, проверку и установку обновлений ПО на компонентах АСУТП.	18.15	A.12.1, A.12.7, A.14.2
6.	Меры по обучению персонала должны обеспечивать информирование персонала об угрозах безопасности информации, о правилах эксплуатации системы защиты АСУ, а также практическое обучение(в том числе проведение тренировок) по эксплуатации системы защиты АСУ.	18.18	A.7.2, A.17.1

Анализ уязвимостей для СлПО проводится в целях оценки возможности преодоления нарушителем системы защиты и нарушения безопасного функционирования за счет реализации угроз безопасности информации. Анализ уязвимостей включает анализ уязвимостей средств защиты информации, технических средств и ПО. Среди методов оценки технических уязвимостей можно отметить методы тестирования ИС, которые применяются для эффективного выявления уязвимостей. Эти методы тестирования включают, например:

- Автоматизированные инструментальные средства поиска уязвимостей;
- Тестирование и оценка безопасности;
- Тестирование на проникновение;
- Проверка кодов.

В ст. 9 Приказа ФСТЭК № 31 определено, что паспорт, признанный по результатам актуализации подлежащим замене и утратившим силу, хранится в порядке, установленном субъектом ТЭК, в течение 25 лет. Это требование также соответствует требованиям, соответственно, п. 9.3 в ISO 27001 и п. 4.7 в ISO 50001 по анализу со стороны руководства (“*Management Review”*). В тоже время в постановлениях Правительства не отражены в явном виде требования к обеспечению полного цикла управления

рисками для организаций ТЭК. Также не предусмотрена оценка остаточного риска (“*Residual risk*”), которая позволяет дополнительно оценить уровень оценки защищенности активов СлПО ТЭК после применения выбранных мер (средств) обеспечения ИБ и определенного перечня рисков. Это обстоятельство может быть компенсировано как применением стандартов ISO, например, серии 27001, где требование менеджмента рисков установлено в явном виде, так и созданием ИСМ – с теми же требованиям и/или дополнительным внедрением «целевого стандарта» ISO серии 31000.

Предложенный методический подход позволяет «мягко» преобразовать существующую систему к требованиям СМИБ и обеспечить результативное проведение различных аудитов и мониторинга состояния СлПО, находящихся под воздействием угроз нарушения ИБ. Методика основана на преобразовании базовой системы и учете требований по идентификации всех групп активов в соответствии с требованиями к СМИБ на базе стандартов ISO серии 27001 и серии 27005.

В методике представлена последовательность шагов и набор соответствующих базовых таблиц для преобразования к требованиям СМИБ. Начинается процесс с идентификации активов, их категорирования и первичной оценки со стороны владельцев для принятия решения о включении с область применения (“*scope*”). Например, на этом шаге могут определяться права собственности на помещения, владельцы лицензий ПО, ответственность за процессы СМИБ.

Далее на основании первичного перечня активов выполняются стандартные процедуры оценки рисков, установление критериев принятия рисков и приемлемых уровней рисков, формирование плана обработки рисков. Например, на этом шаге могут быть использованы результаты классификации активов в соответствии с нотацией СОИБ как входные данные и выполнена полная оценка рисков (в том числе и остаточных) в соответствии с требованиями ISO серии 27001. На последующих шагах выполняется выбор мер (средств) обеспечения ИБ, формирование «Заявления о применимости», далее – выполнение внутренних аудитов СМИБ, проведение анализа СМИБ со стороны руководства и определение возможностей для постоянного улучшения СМИБ.

Учет активов в соответствии с требованиями стандарта ISO серии 27001 позволит привнести в СМИБ управляемость по единым целям, измеримых в терминах бизнеса, что позволит выполнять в дальнейшем интеграцию с другими системами менеджмента. Соответственно, для СМИБ могут быть применены соответствующие количественные метрики как доказательства «полезности» для бизнеса.

Различные виды метрик для целей обеспечения ИБ представляется целесообразным сгруппировать следующим образом:

– Для оценки основного бизнеса (например, доля на рынке);
– Для управления издержками (например, ТСО – совокупная стоимость владения);
– Для оптимизации текущей деятельности (например, оптимизация затрат OPEX).

С целью снижения издержек текущей деятельности, могут быть применены метрики, отражающие степень достижения возможного максимума (например, выполнение в срок инфраструктурных проектов). Соответственно, предлагаются различные типы метрик:

– простые метрики (например, количество выявленных инцидентов ИБ);
– сложные метрики (например, отношение стоимости СЗИ к стоимости ИТ активов);
– комплексные метрики (например, число произошедших инцидентов ИБ, приведших к ущербу (вынужденному простою) в АС, определенных как критичные для бизнеса).

Заключение. Процесс формирования требований к защищенности СлПО ТЭК рекомендуется реализовать на базе системы современных нормативных документов (ФСТЭК) и стандартов ISO серии 27001 и ISO серии 50001. Предлагаемый подход позволит обеспечить необходимый уровень обеспечения безопасности СлПО, в том числе уровень ИБ, адекватный современным требованиям к оценке угроз, анализу уязвимостей и менеджмента рисков на объектах ТЭК.

СПИСОК ЛИТЕРАТУРЫ

1. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements, International Organization for Standardization, 2013. – 23 pages.
2. ISO/IEC 27004:2009. Information technology — Security techniques — Information security management — Measurement, International Organization for Standardization, 2009. – 55 pages.
3. ISO/IEC 27005-2011. Information technology — Security techniques — Information security risk management, International Organization for Standardization, 2011. – 68 pages.
4. Лившиц И.И. Практическая оценка результативности СМИБ в соответствии с требованиями различных систем стандартизации: ИСО 27001 и СТО Газпром / Лившиц И.И., Полещук А.В. // Труды СПИИРАН. – 2015. – № 3. – С. 33 – 44.

УДК 004.75

МОДЕЛИРОВАНИЕ ГИБРИДНОГО ПРОТОКОЛА МАРШРУТИЗАЦИИ В БЕСПРОВОДНОЙ СЕТИ

Молокович Игорь Аркадьевич
АО «Научно-производственное объединение «Импульс»,
Россия, Санкт-Петербург, ул. Киришская, д.2,
emais: molokovich@mail.ru

Аннотация: В статье рассмотрено моделирование гибридного протокола маршрутизации в беспроводной сети, имеющей стационарную и подвижные компоненты.

Ключевые слова: *моделирование; гибридный протокол маршрутизации; беспроводная сеть.*

SIMULATION HYBRID PROTOCOL ROUTING IN WIRELESS NETWORK

Molokovich Igor
Joint-stock company “Research-and-production union "Impuls",
Russia, St. Petersburg, Kirichskay str. 2,
email: molokovich@mail.ru

Abstract: The article presents simulation hybrid protocol routing in *wireless network*, having stationary and mobile component

Keywords: *modeling; hybrid protocol routing; wireless network.*

Введение. Рассмотрим беспроводную сеть, которая состоит из нескольких ad hoc компонентов (Mobile Ad Hoc NETworks – сети без предварительной инфраструктуры, с изменяющейся из-за подвижности узлов топологией) и стационарных маршрутизаторов области ретрансляторов, которые работают в качестве ядра сети.

Каждый ad hoc компонент рассматривается как отдельный регион. Маршрутизатор, подключенный к этому региону, несет ответственность за выдачу адресов узлам, маршруты к узлам других регионов и сетей и управление в этом регионе. Предлагаемый протокол маршрутизации состоит из трех компонентов маршрутизации:

– протокола маршрутизации внутри ad hoc региона (Intra Region Routing Protocol) – IRRP;
– протокола маршрутизации стационарных маршрутизаторов области ретрансляторов (Router Infrastructure Routing Protocol) – RIRP;
– протокола маршрутизации между ad hoc регионами (Region Gateway Routing Protocol) – RGP.

Маршрутизаторы области ретрансляторов используют Router Infrastructure Routing Protocol. Поскольку маршрутизаторы области ретрансляторов статические, RIRP относится к семейству беспроводных активных протоколов маршрутизации. RIRP работает на каждом статическом маршрутизаторе и обеспечивает маршруты в регионы, связанные с маршрутизаторами. Таблицы маршрутизации всегда актуальны, чтобы обеспечить немедленную маршрутизацию. Это позволяет существенно сократить задержки при определении маршрута.

В конкретном регионе или ad hoc компоненте маршруты поддерживаются с помощью протокола Intra Region Routing Protocol (IRRP). IRRP – это реактивный протокол маршрутизации, который поддерживают расширенный поиск маршрутов и услуги технического обслуживания маршрута на основе локальных подключений к региону в режиме ad hoc.

Region Gateway Protocol используется, когда требуется маршрут между двумя ad hoc узлами разных регионов. Он получает информацию о маршрутах от RIRP и IRRP и создает полный маршрут от источника к получателю и предоставляет его в исходный узел. Когда узел требует маршрут, RGP получает информацию от RIRP и IRRP обоих ad hoc регионов, строит маршрут и отправляет его IRRP и RIRP.

Каждый раз, когда новый маршрутизатор включается в сеть или в случае сбоя соединения, RIRP должен знать о событии. Для этого RIRP использует либо Neighborhood Discovery Protocol (NHDP) для доступа к MAC-уровню или обеспечивает эти функциональные возможности самостоятельно. Каждый узел посылает hello-пакеты, содержащие информацию о соседних узлах, другим узлам в этом районе через постоянные интервалы времени. Если время ожидания истекает и hello-пакет не получен, то можно сказать, что есть проблема с соединением. Благодаря такому обмену каждый узел сети получает представление об узлах в двухшаговой окрестности и о свойствах соединений между этими узлами.

Аналогичным образом, когда новый узел приходит в сеть, он может заявить о себе, передавая hello-пакет. Каждый раз, когда узел должен послать некоторые данные другим узлам, он проверяет, имеет ли он маршрут к месту назначения. Если активного маршрута нет, узел начинает фазу обнаружения маршрута. Механизм обнаружения маршрута имеет три этапа: запрос маршрута, формирование маршрута и маршрут-ответ.

На этапе запроса маршрута запрос посылается в соседние узлы, используя IRRP. Если соседние узлы не имеют маршрута до места назначения, они пересылают запрос другим узлам. Если ни один узел не имеет маршрут до пункта назначения, запрос отправляется на RGP, работающий на

маршрутизаторе, подключенном к ad hoc компоненту. Здесь RGP пытается найти маршрутизатор, подключенный к необходимому ad hoc компоненту с помощью RIRP. Когда маршрут к маршрутизируемому узлу найден, RGP использует IRRP в ad hoc регионе, в котором находится узел назначения, чтобы найти к нему путь.

После того, как маршрут до пункта назначения находится, весь маршрут от источника до пункта назначения формируется посредством RGP. Эта фаза называется фазой формирования пути. Когда полный маршрут сформирован, маршрут-ответ с полной информацией отправляется к исходному узлу, на этом фаза поиска маршрута завершается.

Если узел назначения существует в том же регионе, что узел отправитель или в качестве передающего узла выступает ad hoc компонент, используется только реактивная маршрутизация. IRRP обнаруживает возможные маршруты и отправляет данные по обнаруженным маршрутам.

Если принимающий узел и передающий узлы не из того же региона или ad hoc компонента, то для поиска маршрута используются и реактивные, и активные протоколы маршрутизации. Этап запроса маршрута дополнительно разделяется на две фазы: активную и реактивную. Маршрутизатор, подключенный к ad hoc региону узла отправителя, несет ответственность за активную фазу и маршрутизатор, подключенный к ad hoc области узла назначения, ответственен за реактивную фазу.

Сначала маршрутизатор узла-отправителя обнаруживает маршрут к ad hoc области узла назначения при помощи RIRP. После этого маршрутизатор узла в ad hoc области назначения выполняет реактивное определение маршрута с использованием IRRP, чтобы найти маршрут к узлу назначения. RGP отвечает за создание полного маршрута из двух маршрутов найденных RIRP и IRRP и отправляет его узлу-отправителю.

Протокол обслуживания маршрута определяет, когда топология сети изменилась, и принимает решение, если альтернативный маршрут может быть использован (при наличии) или если Route Discovery Protocol (RDP) должен быть запущен, чтобы найти новый путь. Обслуживание маршрута вызывается при обнаружении разрыва соединения во время того, как отправитель активно использует маршрут. Промежуточный узел, который определяет, что следующий узел в маршруте недоступен, посылает пакет ошибки обратно отправителю. Отправитель после получения уведомления об ошибке может использовать другой маршрут или может выполнить поиск маршрута.

Знание топологии сети региона может быть использовано для обеспечения лучшего обслуживания маршрута. В маршрутизаторе области ретрансляторов много путей для маршрутизации обеспечит надежность, балансировку нагрузки и лучшее обслуживание маршрута с небольшой задержкой и меньшим контролем трафика.

В IRRP, в связи с динамически меняющейся топологией мобильных клиентских узлов, обслуживание маршрутов имеет очень важное значение. До тех пор, пока нового маршрута не обнаружено, пакеты отбрасываются и реактивный протокол занимает больше времени при определении маршрута. Поэтому многолучевой протокол маршрутизации был бы лучшим вариантом для построения соединения вместо того, чтобы найти новый путь.

Кэш может также служить для уменьшения задержки, а также контролировать трафик при поиске путей. Каждый узел может активно кэшировать маршруты и, таким образом, уменьшать частоту запуска процедуры обнаружения маршрута. Недоступный путь может быть заменен на другой, который локально может не охватить целый ad hoc регион. Этот новый путь будет использоваться для замены старых поврежденных и сообщения обновлений путей могут быть отправлены другим узлам. Если эти восстановления путей снижают эффективность маршрутов, новая фаза поиска маршрута может начаться после определенного количества таких локальных восстановлений.

Рассмотрим сеть, представленную на рис. 1, в которой есть две области ad hoc и инфраструктура стационарных маршрутизаторов в области ретрансляторов. Узел A должен послать пакет узлу L. Узел A будет использовать IRRP для поиска пути к узлу L. Так как маршрут не найден в регионе, создается запрос с использованием RGP на маршрутизатор G. Теперь маршрутизатор G ищет в своей таблице маршрутизации маршрут к месту назначения – ad hoc области, который он построил через RIRP. Допустим, маршрутизатор G имеет маршрут к месту назначения через маршрутизатор I. Таким образом, запрос маршрута отправляется на маршрутизатор I, который выполняет маршрутизацию по требованию, используя IRRP, и находит путь к узлу L. Далее на маршрутизаторе I работает RGP для отправки этого маршрута к маршрутизатору G, который создает полный маршрут от источника A до пункта назначения L и отправляет маршрут-ответ на узел A.

Если были доступны несколько путей к месту назначения, то все пути будут направлены в узел A.

Для активного компонента предлагается использование протоколов Destination Sequenced Distance Vector (DSDV) или Optimized Link State Routing (OLSR). Эти протоколы маршрутизации имеют процедуры поиска маршрута в области инфраструктуры стационарных маршрутизаторов. Кроме того, для выполнения этой задачи в ad hoc регионах предлагается использовать протокол Adhoc Ondemand Distance Vector (AODV) в качестве реактивного протокола маршрутизации. Необходимо разработать реализацию Region Gateway Protocol, который вычисляет весь маршрут и предоставляет его запрашивающему узлу.

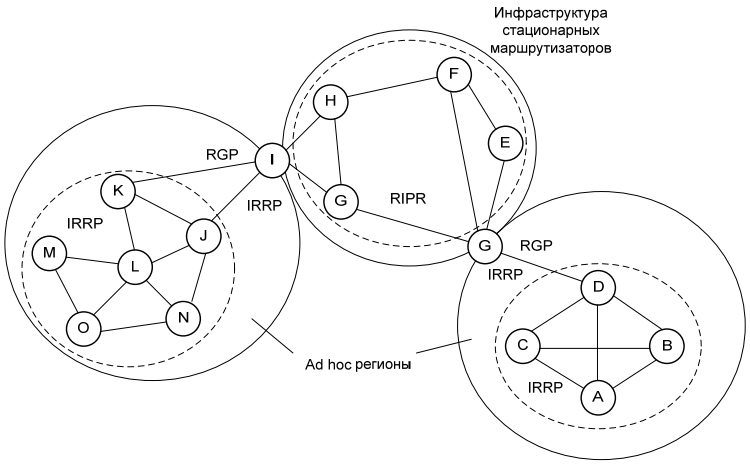


Рис. 1. Структура беспроводной сети

Рассмотрим задачу подключения мобильных узлов к стационарным узлам в беспроводной сети по критерию минимального расстояния [1].

Пусть $X=\{x_k\}$, $k=\overline{1,r}$ – множество мобильных узлов; $Y=\{y_i\}$, $i=\overline{1,n}$ – множество стационарных узлов; d_{ki}, – матрица расстояний от k-го мобильного узла до i-го стационарного узла, где r – количество мобильных узлов, n – количество стационарных узлов. Основным ограничением рассматриваемой задачи является то, что каждый мобильный узел $x_k \in X$ может быть подключен только к одному стационарному узлу $y_i \in Y$.

Введем переменную

$$z_{ik} = \begin{cases} 1, \text{åñëè óçåë } x_k \text{ ïîäêëþ÷åí} \quad \text{ê óçëó } y_i, \\ 0 - \text{â ïðîòèâíîì} \quad \text{ñëó÷àå}. \end{cases} \tag{1}$$

Тогда ограничения рассматриваемой задачи примут следующий вид:

$$\sum_{i=1}^{n} z_{ki} = 1, \; k=\overline{1,r}, \tag{2}$$

а задача подключения мобильных узлов к стационарным узлам будет сведена к минимизации суммы расстояний от мобильных до стационарных узлов с учетом того, что каждый мобильный узел присоединяется к одному стационарному узлу. В этом случае для решения задачи необходимо найти минимум критерия:

$$F = \sum_{k=1}^{r}\sum_{i=1}^{n} z_{ki} d_{ki} \to \min. \tag{3}$$

Считается, что размещение стационарных узлов уже произведено.

Задача оптимизации критерия (3) является задачей линейного целочисленного программирования с ограничениями типа равенств (2). Решение таких задач может эффективно осуществляться в среде MatLab с помощью функции bintprog, реализующей метод ветвей и границ [2]. Для этого необходимо перейти от набора z_{ki}, $k=\overline{1,r}$, $i=\overline{1,n}$, к одномерному массиву неизвестных z_{1j}, $j=1, r*n$. То же самое относится к расстояниям: от матрицы $||d_{ki}||$ переходим к одномерному массиву d_{1j}, $j=1, r*n$.

Стандартное обращение к функции при отсутствии ограничений типа неравенств будет следующим: [*z*1, *fval*]=bintprog (*d*1, [], [], *Aeq*, *beq*), где *fval* – минимальное значение критерия *F* в (3); *z*1 – булевый вектор решения, то есть его компоненты принимают значение 0 (мобильный узел не подключен к стационарному узлу) или 1 (подключен).

Матрицы ограничений типа равенств *Aeq*, *beq* формируются в соответствии с (2), а их размерности равны *Aeq* [*r*×*n*], *beq* [*r*×1].

При возникновении необходимости в передаче узел-отправитель из множества узлов мобильной сети $X=\{x_k\}$, $k=\overline{1,r}$ при отсутствии у него маршрута до узла-получателя передает широковещательный запрос поиска маршрута всем соседним узлам, соседние узлы передают запрос своим соседним узлам за исключением узла, откуда поступил запрос, и т.д. до достижения узла-получателя.

Соседние узлы определяются матрицей связности Z размера [*r*×*r*], где $z_{ij}=1$, если *i*-й узел находится в зоне радиодоступа *j*-го узла, или $z_{ij}=0$ в противном случае. Если $z_{ij}=1$, то запрос передается от *i*-го узла-отправителя к *j*-му соседнему узлу, $j=\overline{1,r}$, $j \neq i$.

По номеру i_S узла-отправителя в *i*-ой строке матрицы связности *Z* выбираются элементы $z_{ij}=1$, которые определяют соседние *j*-е узлы для передачи запроса. Если *j*-е узлы не являются получателями, то для каждого из них определяются соседние узлы для дальнейшей передачи запроса, исключая узел-отправитель, т.е. *i=j* и по *i*-м строкам матрицы связности *Z* выбираются соседние узлы, исключая узел-отправитель ($j \neq i_S$). Если среди выбранных узлов нет получателя, то процедура передачи запроса продолжается.

После получения запроса узлом-получателем определяется маршрут до узла-отправителя, т.е. если $j = j_D$, то из матрицы связности *Z* выбираются z_{ij_D} и $z_{i_S j}$.

Из всех поступивших на узел-отправитель маршрутов выбирается кратчайший по длине:

$$d_{i_S j_D} = z_{i_S j} + \ldots + z_{ij_D} \rightarrow \min . \quad (4)$$

После определения маршрута узел-отправитель начинает передачу информации узлу-получателю.

Если маршрут в данной мобильной сети не найден, т.е. j_D узел-получатель находится в другой мобильной сети, то i_S узел-отправитель передает запрос маршрута на узел сети стационарных узлов *Y*={y_i}, $i=\overline{1,n}$, к которому подключена данная мобильная сеть.

По номеру узла стационарной сети y_i в матрице связности *Z* выбирается строка, элементы которой $z_{ij}=1$ определяют узлы, подключенные к данному стационарному узлу. Из них выбирается номер узла, принадлежащий множеству *X*={x_k}, $k=\overline{1,r}$.

Далее узел-отправитель i_S передает широковещательный запрос поиска маршрута до мобильного узла-шлюза в стационарную сеть по алгоритму, описанному выше.

После получения ответа с маршрутом узел-отправитель i_S на стационарный узел передает запрос маршрута до мобильного узла-получателя j_D.

По номеру j_D мобильного узла-получателя из матрицы связности *Z* выбирается строка, по элементам $z_{ij}=1$ которой определяется, к какому узлу стационарной сети подключен j_D узел-получатель. На этот узел по сети стационарных узлов передается запрос маршрута к мобильному j_D узлу-получателю, по которому он посылает широковещательный запрос маршрута в подключенную к нему сеть мобильных узлов по алгоритму, рассмотренному выше.

После получения запроса мобильным j_D узлом-получателем определяется маршрут до узла стационарной сети, к которому подключена данная мобильная сеть, т.е. если $j = j_D$, то из матрицы связности *Z* выбираются z_{ij_D} и $z_{i_S j}$. Далее этот маршрут отправляется на узел стационарной сети, к которому подключена мобильная сеть i_S узла-отправителя, на котором формируется составной маршрут и передается на мобильный i_S узел-отправитель по маршруту поступления запроса.

Заключение. Для дальнейшего исследования алгоритм предложенного гибридного протокола выбора маршрута в беспроводной сети будет реализован в программах Matlab и Network Simulator 2.

Для анализа качества работы протокола маршрутизации предполагается использовать следующие метрики:

– процент доставленных пакетов — это отношение числа доставленных пакетов к числу отправленных источником данных пакетов;

– среднее время доставки пакетов данных — это среднее время доставки одного пакета в исследуемой сети. Включает в себя все возможные задержки, связанные с буферизацией во время процесса обнаружения маршрута, постановкой в очередь отправки радиоинтерфейса, повторными передачами на уровне MAC, временем передачи данных;

– нормированное число пакетов маршрутизации — это среднее количество пакетов маршрутизации, приходящихся на один доставленный пакет данных.

СПИСОК ЛИТЕРАТУРЫ

1. Дмитриев Г.А., Марголис Б.И., Музанна М.М. Синтез структуры абонентских телекоммуникационных сетей // Программные продукты и системы. 2014, № 1. С. 158 – 162.
2. Кетков Ю.Л., Кетков А.Ю., Шульц М.М. MATLAB 7: программирование, численные методы. – СПб.: БХВ-Петербург, 2005. – 752 с.

УДК 004.9

СОВРЕМЕННЫЙ ПОДХОД К ВЫЯВЛЕНИЮ И УПРАВЛЕНИЮ МЕДИЦИНСКИМИ СИГНАЛАМИ В СИСТЕМЕ FLEX DATABASES

Сухов Родион.Владимирович
Санкт-Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лоцманская, д. 3,
emails: RS-Anti@yandex.ru

***Аннотация*:** В статье рассматривается современный подход к выявлению и управлению, медицинскими сигналами на примере системы FLEX DATABASES.

***Ключевые слова**: сигнал; статистические методы; качественные методы; валидация; приоритизация.*

MODERN APPROACH TO DETECTION AND MANAGEMENT, MEDICAL SIGNALS IN THE FLEX DATABASES SYSTEM

Rodion Sukhov
St. Petersburg State Marine Technical University "SPbGMTU"
Russia, St. Petersburg, st. Lotsmanskaya, 3,
emails: RS-Anti@yandex.ru

Abstract: In the article the modern approach to revealing and management of medical signals on an example of system FLEX DATABASES is considered.

***Keywords:** signal; statistics methods; quality methods; validation; priority.*

Введение. Выявление и управление сигналами – важная часть процесса фармаконадзора, они являются необходимой частью периодических отчетов по безопасности. Сигналы представляют собой новую, ранее неизвестную информацию о связи нежелательной реакции и препарата. В системе *Flex Databases* реализованы как качественные, так и количественные методы выявления сигналов, а также отдельный раздел для управления сигналами. Работу с сигналами в системе *Flex Databases* можно разделить на четыре раздела:

– уведомления системы о возможном появлении сигнала при вводе сообщения;
– качественные методы выявления возможных сигналов и формирование серий случаев (Striking/Index case, SMQ, IME, DME, TME);
– количественные методы выявления возможных сигналов (частотные и байесовские/Data Mining);
– управление сигналами, валидация, приоритизация, оценка.

Система сообщает пользователю о наличии возможного сигнала в одном из следующих случаев:

– попадание закодированного симптома в списки IME (Important Medical Events, список EMA, не изменяется пользователями), TME (Targeted Medical Events, список симптомов по конкретному препарату, настраивается пользователем), DME (Designated Medical Events, список симптомов по компании в целом, настраивается пользователем);
– появление SUSAR;
– повторное появление серьезного НЯ по одному и тому же препарату.

В карточке случая появляется признак подозрение на возможный сигнал. На основании этой информации пользователь может сформировать серию случаев, чтобы использовать их как доказательную базу для обоснования сигнала. Пользователю доступен набор фильтров по закодированным симптомам, попаданию в списки IME, TME, DME, времени появления реакции после приема препарата, вопросам Dechallenge и Rechallenge, серьезности сообщения.

По серии случаев дополнительно пользователь может провести статистическую проверку диспропорциональностей в частоте репортирования.

Количественные методы поиска сигналов. В системе используются такие популярные в индустрии методы, как:

– Proportional Reporting Ratio (PRR);
– Reporting Odds Ratio (ROR);
– Relative Reporting Ratio (RRR);
– Empirical Bayes Geometrical Mean (EBGM);
– Bayesian Confidence Propagation Neural Network (BCPNN).

На основе серии случаев пользователь создает карточку возможного сигнала.

Управление сигналами. В карточке сигнала пользователь может провести валидацию, приоритизацию и оценку сигнала, согласно рекомендациям CIOMS VIII. Поля на этих этапах настроены на основании вопросов, рекомендуемых WHO и MHRA. Таблица разделения случаев приведена в табл.1.

Таблица 1

Таблица разделения случаев

	Явление (R)	Все другие явления	Всего
Исследуемый продукт (ИП)	A	C	A+C
Все другие ИП	B	D	B+D
Всего	A+B	C+D	N =A+B+C+D

A – количество случаев, где есть подозрение на связь ИП с конкретным явлением (R)

B – количество случаев, где есть подозрение на связь явления с другими ИП

C – количество случаев, где есть подозрение на связь ИП с другими явлениями

D – количество случаев, где есть подозрение на связь других явлений с другими ИП

Proportional Reporting Ratio (PPR)

Коэффициент пропорционального репортирования (диспропорциональный анализ) позволяет выявить показатели, которые оказались выше ожидаемого уровня. Данный метод сравнивает, сколько было зарепортировано случаев побочных эффектов для конкретного препарата в сравнении с другими событиями, вызванными приемом данного препарата. Другими словами, это отношение количества зарепортированных случаев побочного эффекта ко всем случаям побочных эффектов для данного препарата. Рекомендуемое пограничное значения принятия решения о связи – 2. Сопутствующие лекарственные препараты в расчеты не включаются.

Указанный коэффициент пропорционального репортирования описан в виде:

$$PRR = \frac{\mathrm{A}(B+\mathrm{D})}{C(A+C)}, \quad (1)$$

90% доверительный интервал коэффициента PPR представлен в виде:

$$PRR90\min(-) = \frac{PRR}{e^{1.96S}} \text{ – нижняя граница доверительного интервала,} \quad (2)$$

$$PRR90\max(+) = PRRe^{1.96S} \text{ – верхняя граница доверительного интервала,} \quad (3)$$

$$S = \sqrt{\frac{1}{A}+\frac{1}{C}-\frac{1}{A+B}-\frac{1}{C+D}} \text{ – стандартное отклонение,} \quad (4)$$

В приведенных формулах показывается расчет нижней и верхней границы доверительного интервала для определения статистической значимости полученного коэффициента (PPR). Доверительный интервал не должен переходить границу в 1 для того, чтобы принять результат за статистически значимый. Хи-квадрат в данном случае используется как измерение значимости связи между ИП и явлением и представляется в виде:

$$\chi^2 = \frac{(AD-BC)^2(A+B+C+D)}{(A+B)(C+D)(A+C)(B+D)}, \quad (5)$$

Reporting Odds Ratio (ROR)

Еще один метод диспропорционального анализа, который позволяет выявлять сигналы в базе случаев. Данный метод позволит увидеть, насколько статистически значима связь произошедшего явления (нежелательного явления) с исследуемым продуктом. Рекомендуемое пограничное значения принятия решения о связи – 2. ROR коэффициент позволяет проиллюстрировать, насколько представленная измеряемая характеристика связана с определенным событием.

ROR коэффициент представлен в виде:

$$ROR = \frac{AD}{BC}, \quad (6)$$

$$ROR90max = e^{\ln(ROR)+1.96\sqrt{V}} \text{ – нижняя граница доверительного интервала,} \quad (7)$$

$$ROR90min = e^{\ln(ROR)-1.96\sqrt{V}} \text{ – верхняя граница доверительного интервала ,} \quad (8)$$

$$V = \frac{1}{A}+\frac{1}{B}+\frac{1}{C}+\frac{1}{D} \text{ – вариация,} \quad (9)$$

В приведенных формулах показывается расчет нижней и верхней границы доверительного интервала для определения статистической значимости полученного коэффициента (ROR). Доверительный интервал не должен переходить границу в 1 для того, чтобы принять результат за статистически значимый. Обозначения соответствуют расписанным выше.

Relative Reporting Ratio (RRR). Коэффициент RRR – показатель вероятности того, что явление связано с ИП. Рекомендуемое пограничное значения принятия решения о связи – 2. В приведенных формулах показывается расчет нижней и верхней границы доверительного интервала для определения статистической значимости полученного коэффициента (PPR). Доверительный интервал не должен переходить границу в 1 для того, чтобы принять результат за статистически значимый.

Коэффициент RRR представлен в виде:

$$RRR = \frac{\mathrm{A}(\mathrm{A+B+C+D})}{(A+C)(A+B)}, \quad (10)$$

$$s = \frac{A}{A(A+C)}+\frac{C+D}{(A+B)(A+B+C+D)} \text{ – стандартное отклонение,} \quad (11)$$

$RRR95max = e^{\ln(RRR)+1.96\sqrt{s}}$ – нижняя граница доверительного интервала, (12)

$RRR95min = e^{\ln(RRR)-1.96\sqrt{s}}$ – верхняя граница доверительного интервала, (13)

Заключение. В итоге мировой опыт использования различных статистических методов для определения и выявления сигналов, показывает свою эффективность. Что позволяет использовать статистический, количественный подход для своевременного реагирования на возникновение сигнала в системе FLEX DATABASES.

СПИСОК ЛИТЕРАТУРЫ

1. W. DuMouchel. Bayesian Data Mining in Large Frequency Tables, With an Application to the FDA Spontaneous Reporting System. In: The American Statistician, 1999, Vol. 53, 177-202.
2. W. DuMouchel and D. Pregibon. Empirical Bayes Screening for Multi-Item Associations. In: Proceedings of the 7th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco (USA), 2001, 67-76.

ПОДГОТОВКА И ПЕРЕПОДГОТОВКА ИТ-СПЕЦИАЛИСТОВ

УДК 004.056.53

ЛАБОРАТОРНЫЕ РАБОТЫ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»

Барабаш Павел Александрович, Панасенко Михаил Александрович
Смольный институт Российской академии образования,
Россия, Санкт-Петербург, Полюстровский пр., д. 59,
email: barabash_p@yahoo.com, panasenko16.01.93@mail.ru

***Аннотация*:** в статье описывается цикл лабораторных работ по учебной дисциплине «Безопасность информационных систем. Приведен перечень лабораторных работ, цели и задачи при их выполнении студентами.

***Ключевые слова**: безопасность информационных систем; сервер безопасности; система защиты информации; учетные записи.*

LABORATORY PRACTICUM ON EDUCATIONAL DISCIPLINE "SECURITY OF INFORMATION SYSTEMS"

Barabash Pavel, Panasenko Mikhail
Smolny Institute of the Russian Academy of Education,
Russia, St. Petersburg, Polyustrovsky ave., 59,
email: barabash_p@yahoo.com, panasenko16.01.93@mail.ru

Abstract: the article describes a series of laboratory works on the academic discipline "Information Systems Security. The list of laboratory works, goals and tasks are given at their implementation by students.

***Keywords:** the security of information systems; server security; security system information; accounts.*

Введение. Учебная дисциплина «Безопасность информационных систем» относится к блоку Б1.В вариативной части учебного плана по направлению подготовки 09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ (уровень бакалавриата).

В соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по указанному направлению подготовки [1], дисциплина поддерживает следующие компетенции:

– понимание сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности (ОПК-4);

– владение основными методами защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий (ОК-12);

– знание своих прав и обязанностей как гражданина своей страны, способность использовать действующее законодательство и другие правовые документы в своей деятельности, демонстрировать готовность и стремление к совершенствованию и развитию общества на принципах гуманизма, свободы и демократии (ОК-9).

Трудоемкост учебной дисциплины составляет 108 часов, из которых 16 часов – лекционных и 24 часа запланировано на выполнение лабораторных работ.

Лекционный курс состоит из 3 Модулей и включает 12 Тем, позволяющих сформировать у студентов представление о механизмах обеспечения безопасности информационных систем [2], [3].

Для закрепления навыков практической работы со специальными программными средствами защиты информации разработан комплекс лабораторных работ.

Структурная схема комплекса представлена на рис. 1.

В компьютерном классе устанавливается ПО виртуализации - Microsoft Virtual PC 2007 SP1, позволяющее запустить две виртуальные машины. На первой виртуальной машине устанавливается Windows Server 2003 и «Сервер безопасности» Dallas Lock, которые, в частности, выполняют роли Контроллера домена, Файлового сервера, DNS – сервера и позволяют выполнить настройку правил «Сервера безопасности» Dallas Lock. Сервер безопасности Dallas Lock 8.0 предоставляет следующие возможности:

— централизованное управление пользователями и группами пользователей на клиентах;

— централизованное управление политиками безопасности клиентов;

— централизованный сбор журналов с клиентов;
— управление доступом к ресурсам файловой системы и к устройствам на клиентах;
— просмотр состояния отдельных клиентов;
— объединение клиентов в группы.

Некоторые параметры безопасности могут быть настроены сразу для всего Домена безопасности, некоторые – для групп клиентов, некоторые – для отдельных клиентов.

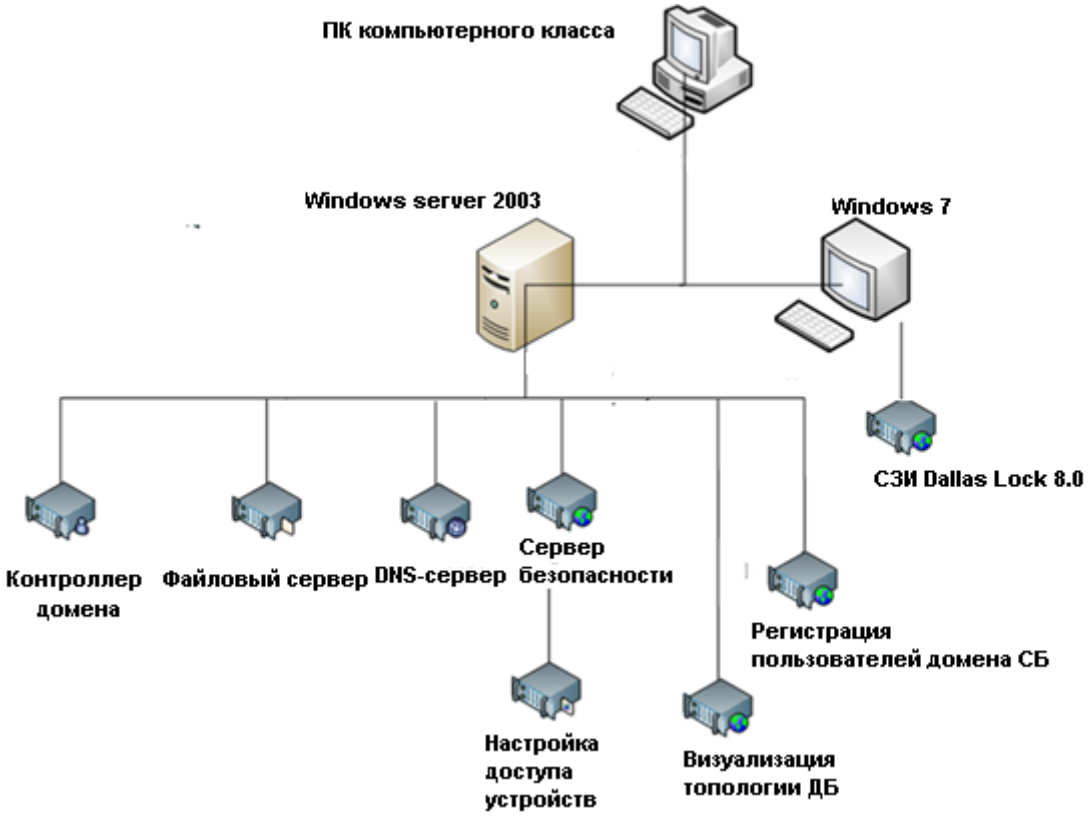


Рис.1 Структурная схема лабораторного комплекса

На вторую виртуальную машину устанавливается ОС Windows 7 и средство защиты информации (СЗИ) Dallas Lock 8.0, предназначенное для изучения студентами возможностей этого программного продукта. Выбор этих программных продуктов диктуется техническими параметрами ПК в компьютерном классе, а также особенностями Dallas Lock 8.0, приведенными в таблице 1.

Таблица 1

Характеристики Dallas Lock 8.0-С

Наименование параметра	Значение параметра
Тип СЗИ	Программно-аппаратный комплекс
Сертификат соответствия ФСТЭК России	№ 2945 от 16.08.2013 г. действителен до 16.08.2019 г.
Класс защищенности СВТ	3
Класс защищенности МЭ	3
Класс защиты СОВ	4
Класс защиты СКН	2
Уровень контроля отсутствия НДВ	2
Авторизация до загрузки ОС	Да
Мандатный принцип разграничения доступа	Да

Рассмотрим основные цели и задачи, решаемые каждой лабораторной работой.

Целью Лабораторной работы №1 является ознакомление студентов с процессами загрузки виртуальной машины и установки на ней Windows Server 2003. В ходе лабораторной работы студентам требуется выполнить установку виртуальной машины с помощью Мастера установки, настроить параметры домена, роли и компоненты, установить DNS сервер, при этом виртуальная машина с Windows 7 будет добавлена в домен, доменным контроллером которого выступает Windows Server 2003.

Лабораторная работа №2 знакомит с общими принципами работы сервера безопасности и предполагает его установку. Сервер безопасности (СБ) реализован в виде службы, которая автоматически запускается при подключении к ПК лицензионного ключа СБ. Управление СБ осуществляется программой «Консоль сервера безопасности». Для установки СБ студенты запускают программу «Dallas Lock 8.0 Сервер безопасности».

Лабораторная работа №3 посвящена изучению вопросов администрирования сервера безопасности (СБ), работой с консолью СБ (КСБ). Перед студентами поставлены задачи по администрированию СБ, изучению инструментов КСБ, работе в консоли СБ, работе с клиентами Windows из консоли управления. С помощью КСБ можно настроить параметры безопасности для следующих объектов Домена безопасности: для всего Домена безопасности (ДБ), определив настройки при выборе объекта, обозначающего СБ в дереве объектов КСБ; для группы клиентов, определив настройки при выборе объекта, обозначающего группу в дереве объектов КСБ; для индивидуального клиента, выбрав его объект в дереве КСБ.

Для дальнейшей работы студентам в Лабораторной работе №4 необходимо с помощью Мастера установить новую виртуальную машину Windows и поставить на ней ОС Windows 7.

При выполнении Лабораторной работы №5 студенты устанавливают систему защиты информации (СЗИ) Dallas Lock 8.0 на виртуальную машину, установленную ранее в Лабораторной работе №4. После запуска программы установки необходимо выполнять действия по подсказкам программы.

Лабораторная работа №6 знакомит студентов с подсистемой управления доступом Dallas Lock 8.0 и полномочиями на управление этой системой. Регистрировать и удалять пользователей, а также просматривать и редактировать учетные записи может только пользователь, наделенный соответствующими полномочиями по администрированию.

Целью Лабораторной работы №7 является ознакомление с этапами отладки управления доступом и полномочиями на управление учетными записями. Ставятся задачи: научить студентов создавать учетные записи путем копирования, создавать и удалять группы пользователей, регистрировать доменных пользователей, регистрировать доменные учетные записи по маске. С зарегистрированными в СЗИ доменными пользователями можно проводить любые операции по реализации политик безопасности.

Лабораторная работа №8 посвящена тонким настройкам учетных записей в СЗИ, в частности, определению числа разрешенных сеансов для данной учетной записи, смене пароля для авторизации средствами ОС, смене пароля с помощью оболочки администратора, работе с сессиями-исключениями, работе с заблокированными пользователями. При установленном значении для каждой учетной записи (локальной или доменной) проверятся количество одновременных интерактивных и сетевых сессий (входов). Для создания пароля, отвечающего всем требованиям параметров безопасности, установленных системой защиты Dallas Lock 8.0, можно воспользоваться помощью генератора паролей системы защиты.

Лабораторная работа №9 позволяет ознакомить студентов с вариантами тонкой настройки учетных записей для контроля доступа и устройств, в частности, с настройкой полномочий на управление контролем устройств, разграничением доступа к устройствам, понятиями дискреционного принципа разграничения доступа к устройствам и мандатного доступа. В разных версиях ОС Windows в диспетчере устройств одно и то же физическое устройство может идентифицироваться по-разному. Это следует учитывать при определении прав доступа к устройству/классу устройств, особенно при централизованной настройке средствами Сервера безопасности. Важно помнить об этом, особенно при назначении мандатных уровней для доступа к устройствам - устройство может не включиться после входа пользователя под «разрешенным» уровнем, для включения устройства будет требоваться перезагрузка ОС. Установка мандатного доступа на устройство происходит путем определения уровней конфиденциальности в дескрипторе объекта, для работы под которыми устройство должно быть доступно. На рис. 2. показано окно настройки мандатного доступа.

В Лабораторной работе №10 студенты знакомятся с вариантами тонкой настройки учетных записей для настройки Домена безопасности и работы с ним в среде СБ. Они осуществляют ввод клиента в Домен безопасности, ввод защищенного компьютера в ДБ, вывод клиента из ДБ, настройки ДБ, настройку сервера лицензий для СБ, производят визуализацию топологии ДБ. Ввести компьютер в ДБ можно либо в процессе установки СЗИ Dallas Lock 8.0, либо, когда СЗИ Dallas Lock 8.0 уже установлена. В процессе ввода компьютеров в Домен безопасности пароли локальных пользователей с одинаковыми логинами (именами) не синхронизируются. В Консоли СБ Dallas Lock 8.0 имеется средство отображения топологии ДБ. На рис. 3. приведено окно визуализации топологии Домена безопасности. В рабочей области визуализации сети отображается многоуровневая архитектура ДБ: Сервер безопасности, группы клиентов Сервера безопасности, клиенты. С помощью панели действий можно добавлять и редактировать надписи в топологии, возвращать измененную топологию в исходное состояние.

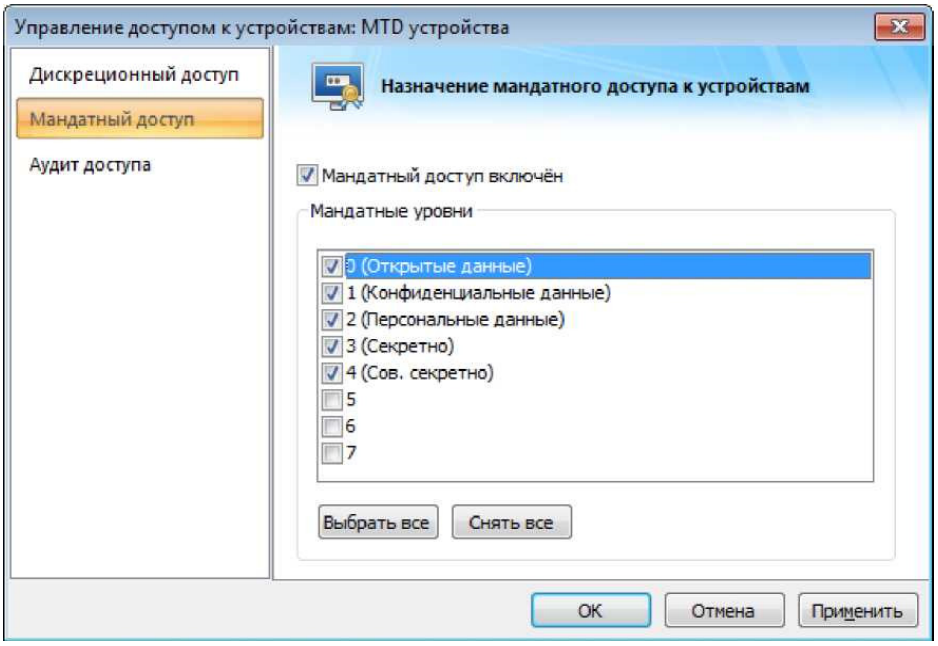


Рис. 2. Настройка мандатного доступа

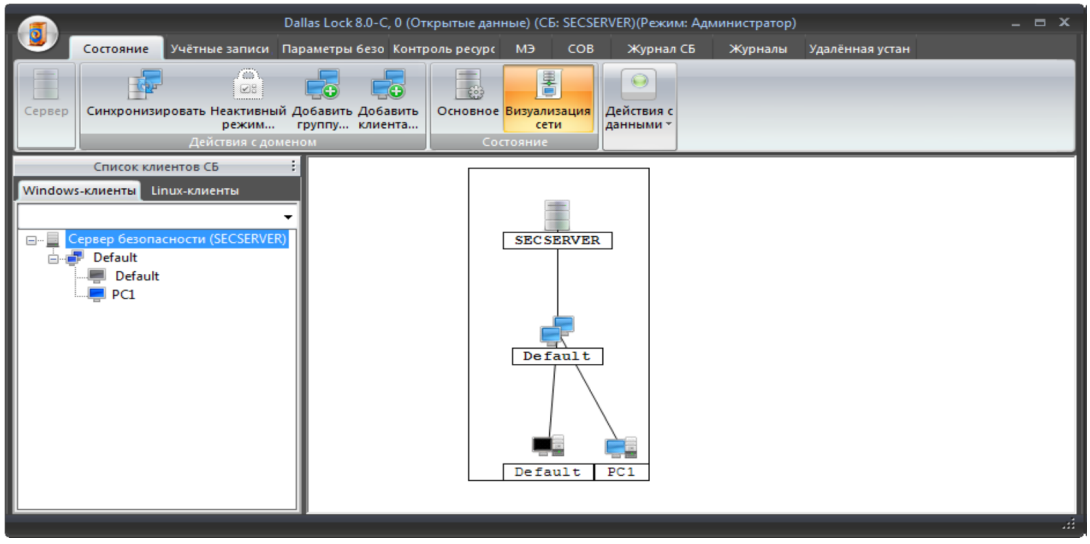


Рис. 3. Визуализация топологии Домена безопасности

Заключение. После выполнения каждой лабораторной работы студенты создают отчет, представляющий собой текстовый файл, оформленный в соответствии с определенными требованиями, содержащий скриншоты (снимки экрана компьютера) операций с описанием процедур выполнения. Отчет размещается в личном кабинете электронной образовательной среды института. Таким образом, формируется часть портфолио студента, в соответствии с требованиями ФГОС ВО [1].

СПИСОК ЛИТЕРАТУРЫ

1. ФЕДЕРАЛЬНЫЙ ГОСУДАРСТВЕННЫЙ ОБРАЗОВАТЕЛЬНЫЙ СТАНДАРТ ВЫСШЕГО ОБРАЗОВАНИЯ. Уровень высшего образования БАКАЛАВРИАТ. Направление подготовки 09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ. (Министерство образования и науки РФ, приказы № 219 от 12.03.2015 г., № 999 от 09.09.2015 г.).
2. Барабаш П.А., Воробьев С.П., Курносов В.И., Советов Б.Я. Инфокоммуникационные технологии в Глобальной информационной инфраструктуре – Санкт-Петербург,: Наука, 2008, 552 с.
3. Безопасность персональных данных. Учебное пособие /П.А. Барабаш. – СПб. : Политехника, 2012. – 167 с.

УДК 371.1

МЕТОДИКА ОЦЕНКИ КАЧЕСТВА ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ВЕРИФИКАЦИИ ИХ ЗНАНИЙ

Большакова Людмила Валентиновна, Яковлева Наталья Александровна
Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, ул. Летчика Пилютова, д. 1,
emails: blv5505@mail.ru, kumirova@mail.ru

***Аннотация*:** В статье рассмотрен новый подход к оценке качества образования будущих сотрудников в сфере информационной и экономической безопасности с применением математико-статистических методов и метода экспертных оценок. Результаты, полученные с помощью предлагаемого подхода, могут быть использованы для совершенствования программ обучения студентов (курсантов) и выявления степени сформированности профессиональных компетенций выпускаемых вузами специалистов.

***Ключевые слова**: качество образования; методика оценки; метод экспертных оценок; тестирование; эксперты.*

METHODS OF EVALUATION THE QUALITY OF TRAINING IN THE FIELD OF ENSURING INFORMATION AND ECONOMIC SECURITY ON THE BASIS OF VERIFICATION OF THEIR KNOWLEDGE

Bolshakova Lyudmila, Yakovleva Natalia
The St.-Petersburg University of the Ministry of Internal Affairs of Russia,
Russia, St. Petersburg, Pilot Pilyutov Street 1,
emails: blv5505@mail.ru, kumirova@mail.ru

Abstract: The article describes a new approach to the assessment of the quality of education of future employees in the field of information and economic security with the use of mathematical-statistical methods and expert judgment. The results obtained using the proposed approach can be used to improve learning programmes students (cadets) and identify the level of formation of professional competences produced by universities.

***Keywords:** the quality of education; methods of evaluation; method of expert evaluations; testing; experts.*

Введение. Решение сложных проблем, связанных с безопасностью личности, общества и государства в условиях развития информационного общества, невозможно осуществить в отсутствие высококвалифицированных профессиональных кадров. В настоящее время одним из значимых направлений государственной политики является подготовка компетентных специалистов, обладающих всеми необходимыми для обеспечения информационной и экономической безопасности знаниями и навыками. В этой связи представляется целесообразным обозначить в качестве одной из важнейших задач успешной реализации данного направления исследование и совершенствование качества образования при подготовке сотрудников в рассматриваемой сфере национальной безопасности. Единой системы проверки качества образования в масштабах всего государства не существует, однако есть отдельные подходы, которые в настоящее время не всегда можно использовать. Например, проводившаяся в прошлые годы проверка знаний обучающихся по тестам Министерства образования не может быть применена по следующей причине. В новых ФГОС ВО не указано не только примерное содержание дисциплин, но нет даже перечня основных базовых дисциплин по соответствующей специальности. В связи с этим составление общих для всех вузов тестов не представляется возможным. Проверка и оценка знаний, умений и навыков учащихся является важным структурным компонентом процесса обучения и должна осуществляться в течение всего периода обучения. Однако на сегодняшний день не существует такой методики оценки качества обучения, которая давала бы достаточно объективную оценку знаниям обучающихся и выдерживала критику специалистов в сфере высшего образования.

Особенностью авторской методики является универсальность ее применения, что позволяет оценить качество профессиональной подготовки курсантов (студентов) на различных уровнях, как в рамках структурного подразделения (группа, курс) или в рамках вуза, так и на федеральном уровне. Таким образом, данная методика может применяться как преподавателями, при оценке знаний курсантов (студентов) на семинарских занятиях, при приеме зачетов, экзаменов, так и Федеральной службой по надзору в сфере образования и науки, а также Департаментом государственной службы и кадров.

Предлагаемая новая методика оценки качества образования, полученного в образовательных учреждениях обозначенного профиля, состоит из двух этапов.

На первом этапе исследуются вопросы изменения уровня владения профессиональными знаниями от курса к курсу для конкретного учебного заведения. Разумным является предположение о том, что уровень подготовки студента или курсанта находится в прямой зависимости от номера курса, на котором он обучается, поскольку его осведомленность в тех или иных вопросах растет с каждым годом по мере накопления и усвоения получаемых знаний.

Основная работа первого этапа состоит в проведении тестирования обучающихся по некоторым, заранее определенным, профильным дисциплинам. Проводиться данная процедура может, например, для учащихся первого, третьего и четвертого курсов. Всем тестируемым предлагаются одинаковые тесты; время, предоставляемое обучаемым на их решение, должно быть ограничено и заранее оговорено. Существенным моментом также является то, что задания в проводимом тестировании необходимо, на наш взгляд, подчинить определенному требованию: вопросы должны быть составлены таким образом, чтобы для их понимания тестируемому не требовалось наличия специальных знаний. Опрашиваемому должна быть доступна суть вопроса, даже если он не располагает, как компетентный специалист, достаточными сведениями в рассматриваемой области; однако правильный ответ дать человеку, не получившему профильного образования, будет не просто [3].

Для составления тестов предполагается создание рабочей группы, состоящей из экспертов, которые способны профессионально оценить качество образования в вузе: преподаватели учебного заведения или же, возможно, практические работники.

Анализ результатов первого этапа должен быть проведен с использованием различных математико-статистических методов и представлением в наглядной форме для удобства анализа, оценки результатов и формирования выводов о качественном уровне знаний опрошенных групп. Наиболее удобно анализировать полученные результаты, представив их в графическом виде, например, с использованием гистограммы. Гистограмма позволит охарактеризовать плотность распределения опрашиваемых по проценту выполнения тестов. Общий вид этого распределения поможет применительно к различным курсам исследуемого вуза оценить доли учащихся, справившихся с заданиями в определенных процентных промежутках, а также провести сравнительный анализ результатов тестирования и сделать необходимые выводы. Так, например, сравнивая составленные гистограммы, можно определить, присутствует ли в учебных заведениях тенденция повышения уровня профессиональных знаний от «младших» курсов к «старшим». В конце анализа должна быть проверена статистическая гипотеза о существенном накоплении знаний обучающихся от курса к курсу.

В основе второго этапа лежит метод экспертных оценок. Использование данного метода обусловлено тем, что в современных условиях довольно часто возникают ситуации, при которых принятие грамотного управленческого решения не может быть произведено на основе точных расчетов. Метод экспертных оценок позволяет дополнить точные математические расчеты рекомендациями специалистов-экспертов, что способствует восполнению недостающей информации, проверке ее достоверности или оценке качественных признаков. Таким образом, главной целью проведения экспертного исследования является создание возможности выработки решения с учетом всех этапов исследуемого процесса.

Особенностями метода экспертных оценок, которые отличают его от обычной экспертизы, являются научная обоснованность организации проведения исследования и применение математико-статистических методов при обработке и анализе полученной информации. Эти особенности определяют основные этапы метода экспертных оценок, для каждого из которых существуют свои задачи, при решении которых могут применяться различные способы и методы проведения процедуры экспертного оценивания [5]. Этапы проведения метода экспертных оценок представляют собой определенный алгоритм действий и операций, позволяющий прийти к выработке совместного решения. В общем виде выделяют следующие этапы метода экспертных оценок:

— постановка целей и задач исследования;
— подготовка информационных материалов, опросных листов, бланков анкет;
— подбор экспертов;
— проведение экспертизы;
— статистический анализ результатов.

Суть второго этапа состоит в следующем. Определяется некоторое задание для процедуры экспертного оценивания. Например, предлагается оценить влияние различных факторов на то или иное социально-экономическое явление. Отбор факторов проводится с привлечением как грамотных теоретиков исследуемой сферы, так и опытных практиков, непосредственно сталкивающихся с изучаемыми явлениями в профессиональной деятельности. В качестве экспертов выбирается две группы. Первая состоит из работников практической сферы, обладающих высокой компетенцией. Вторая группа – из курсантов (студентов), знания которых необходимо оценить. Результаты экспертного оценивания двух групп сравниваются на предмет согласованности и делаются соответствующие выводы.

Стоит отметить, что на этапе подбора экспертов (практических работников) в первую группу, возникает одна из самых главных проблем применения метода – формирование списка действительно

компетентных специалистов, от действий которых напрямую зависит успех проведения исследования. Несмотря на то, что в некоторых работах предлагаются методы или формулы определения необходимого количества экспертов, на сегодняшний день этот вопрос остается открытым. Иными словами, попросту не существует определенного правила, по которому число отобранных экспертов является единственно правильным и научно обоснованным. При создании экспертной группы также нужно учитывать, что при малом числе экспертов может появиться излишнее влияние каждого отдельного эксперта, а при большом – возможна несогласованность и большой разброс во мнениях.

Необходимо отметить, что наиболее существенным моментом на данном этапе будет являться выявление степени согласованности данных полученных от каждой из этих двух групп опрашиваемых по отдельности. Согласованность мнений для каждой группы можно выяснить по значению коэффициента конкордации. При отсутствии согласованности (значение коэффициента конкордации меньше 0,5) выбрать общие результаты по каждой из групп экспертов не представляется возможным. Особое значение имеет наличие согласованности во второй группе – группе обучающихся. Если согласованность отсутствует, то с группой может быть проведено обсуждение рассматриваемой проблемы, например, в виде «мозгового штурма», после которого экспертиза повторяется. Если и после этого согласованность будет отсутствовать, то это может указывать на получение недостаточно качественного образования, а также на неспособность обучаемых к выработке коллективного решения. Однако возможна еще одна причина несогласованности. В группе имеется небольшое число обучающихся, которые не ориентируются в контрольном блоке дисциплин или которые недобросовестно отнеслись к проводимому исследованию. В этом случае можно применить метод парных сравнений и «убрать» тех экспертов, у которых наблюдалось несоответствие в присвоенных рангах. Затем повторить процедуру экспертного оценивания [4].

Если согласованность мнений курсантов и практических работников по отдельности подтверждается, то далее проверяется согласованность ответов между общими результатами курсантов и общими результатами практических работников. Такую проверку чаще всего проводят на основе коэффициента ранговой корреляции Спирмена. Проанализировав подобным образом экспертные данные, можно сформулировать выводы относительно степени согласованности мнений курсантов (студентов) и практических работников, а, следовательно, о том, насколько теоретические знания в области информационной и экономической безопасности, усвоенные обучающимися, совпадают с мнением опытных специалистов, ежедневно решающих профессиональные задачи в этой сфере на практике. В случае большой согласованности можно сделать вывод о том, что обучаемые неплохо разбираются в своей будущей специальности. Отсутствие согласованности говорит о том, что, возможно, существуют какие-то пробелы в процессе обучения.

Стоит отметить, что можно также провести сравнение полученных результатов среди различных ВУЗов, что позволит определить, учащиеся какого учебного заведения показали как наиболее высокий, так и самый низкий результат, а, следовательно, и отметить среди них то, которое успешнее осуществляет подготовку кадров заданной специальности. Для такого анализа в качестве объекта исследования можно взять данные, полученные в ходе тестирования старших курсов. Результаты, как и на первом этапе, удобно интерпретировать графически, используя гистограммы.

Одной из особенностей разработанной методики является то, что она не требует вмешательства специалистов для вынесения оценки качества знаний обучающихся, в роли преподавателей здесь выступают сами курсанты (студенты). Привлечение специалистов требуется только в следующих случаях:

– формирование опросного листа для процедуры экспертного оценивания;

– получение решений практических работников по заявленной проблеме, являющихся эталоном для изучения качества знаний обучающихся.

Для сбора и аккумулирования мнений экспертов необходимо использовать различные формы получения экспертных оценок, подразумевающие всевозможные опросы, совещания, тестирования. В одних с каждым экспертом работают отдельно, при этом он может не знать, кто еще является экспертом, а потому высказывает свое мнение независимо от авторитетов. В других экспертов собирают вместе, при этом они обсуждают проблему друг с другом, учатся друг у друга, и неверные мнения отбрасываются. В одних методах число экспертов фиксировано и окончательно, в других - число экспертов растет в процессе проведения экспертизы, например, при использовании метода «снежного кома». На сегодняшний день наиболее известной и распространенной формой проведения экспертного исследования является метод «Дельфи».

Стоит отметить, что конкретной формы экспертного оценивания, которая позволяла бы получить наиболее комплексное и всеохватывающее решение за минимально короткие сроки, пока не существует. Применение каждой из этих форм (метод совещаний, деловые игры и др.) способствует достижению определенной цели, т.е. выработке решения по заявленной проблеме. В зависимости от различных факторов (например, недостаток временных или человеческих ресурсов), необходим выбор той или иной формы оценивания, наиболее подходящий под условия проведения процедуры экспертного исследования.

Для упорядочивания и анализа экспертных оценок также существуют различные методы, позволяющие оценить степень влияния того или иного фактора на изучаемое явление. Так, если для экспертов поставлена задача, в которой требуется как-то оценить факторы, не поддающиеся непосредственному измерению, то для ее решения может быть применен способ простого ранжирования. Трудности, возникающие при ранжировании большого числа факторов, значительно уменьшаются, если применять метод парных сравнений. Надо сказать, что процедуры ранжирования и парного сравнения предполагают нахождение некой условной оценки – ранга фактора, по которой невозможно определить, насколько один фактор более значим, чем другой. Если для экспертов поставлена задача не только упорядочить факторы, но и найти вес каждого фактора в решении проблемы, то в процедуре экспертного оценивания применяется способ непосредственной оценки или задания весовых коэффициентов. Очевидно, что разнообразные способы сравнения и оценивания факторов могут использоваться экспертами и в комплексе, например, для упорядочения объектов может быть использовано парное сравнение и ранжирование с последующим анализом рангов факторов, полученных разными способами.

Оценка качества подготовки потенциальных сотрудников в сфере информационной и экономической безопасности посредством использования разработанной методики позволит определить направленность обучения курсантов (студентов) и степень соответствия приобретаемых знаний тем основным положениям, владение которыми позволяет практическим работникам выполнять свой служебный долг на высоком профессиональном уровне.

Заключение. Подводя итог вышеизложенному, необходимо отметить, что исследование качества образования при подготовке сотрудников в сфере информационной и экономической безопасности является актуальной и важной проблемой современности. Предложенный в данной статье анализ уровня профессиональных знаний обучающихся дает возможность сформулировать научно обоснованные выводы, которые в дальнейшем могут послужить основой для принятия соответствующих решений, связанных с преобразованиями в установившейся системе подготовки кадров, выработки направлений дальнейших исследований.

Нами предложенная методика направлена на получение объективной оценки соответствия качества подготовки выпускников уровню профессиональной компетенции специалистов в сфере практической деятельности. Объективность данной методики заключается в том, что оценку качеству своих знаний обучающиеся дают сами, организаторам проведения процедуры оценивания остается лишь рассчитать степень согласованности мнений студентов (курсантов) и соответствия этих мнений оценкам профессионалов в сфере заказывающего управления.

Результаты, полученные с помощью предложенной методики можно использовать для совершенствования программ обучения студентов (курсантов) и выявления степени сформированности профессиональной компетенции выпускаемых вузами специалистов.

СПИСОК ЛИТЕРАТУРЫ

1. Иванченко И. В. Проблема повышения качества образования в вузе // Молодой ученый. 2016. №5.1. С. 18-21.
2. Орлов А. И. Теория принятия решений – Экзамен, 2005. 656 с.
3. Примакин А.И., Большакова Л.В. Метод экспертных оценок в решении задач обеспечения экономической безопасности хозяйствующего субъекта. - Вестник Санкт-Петербургского университета МВД России. 2012. №1. С. 191-200.
4. Кунтурова Н.Б., Яковлева Н.А., Подход к оцениванию профессиональной компетентности специалистов силовых структур по видам деятельности при организации контроля формирования профессиональной компетентности. - Вестник Санкт-Петербургского университета МВД России. 2016. №2. С. 146-151.
5. Вилков В.Б., Большакова Л.В., Черных А.К., Яковлева Н.А. Применение методов оптимизации при выработке решений в обучении курсантов в образовательных организациях силовых структур. - Вестник Санкт-Петербургского университета МВД России. 2017. №2. С. 165-173.

УДК 378.145

МНОГОУРОВНЕВЫЙ ПОДХОД В ПОДГОТОВКЕ И ПЕРЕПОДГОТОВКЕ КАДРОВ В СФЕРЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Бурлов Вячеслав Георгиевич, Грачев Михаил Иванович, Примакин Алексей Иванович
Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, улица Летчика Пилютова, д. 1,
emails: burlovvg@mail.ru, mig2500@mail.ru, a.primakin@mail.ru

***Аннотация*:** В статье рассмотрены вопросы необходимости подготовки и проведения переподготовки квалифицированных кадров в сфере безопасности информационных технологий в правоохранительной сфере кафедры специальных информационных технологий Санкт-Петербургского университета МВД России с целью повышения эффективности деятельности как правоохранительных органов, так и безопасности в целом. Предложена модель принятия управленческого решения по обеспечению информационной безопасности.

***Ключевые слова**: Web-технологии; информационные технологии; управленческие решения; модель решения.*

MULTI-LEVEL APPROACH IN TRAINING AND TRAINING IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

Burlov Vyacheslav Georgievich, Grachev Mikhail Ivanovich, Primakin Alexey Ivanovich
Ministry of Internal Affairs Sankt-Peterburgsky university of Russia,
Russia, St. Petersburg, Pilot Pilyutov Street, 1,
emails: burlovvg@mail.ru, mig2500@mail.ru, a.primakin@mail.ru.

Abstract: The article discusses the need to train and conduct retraining of qualified personnel in the field of information security in the law enforcement sphere of the Special Information Technologies Department of the St. Petersburg University of the Ministry of Internal Affairs of Russia in order to improve the effectiveness of both law enforcement agencies and security in general. A model for making managerial decisions to ensure information security is proposed.

Keywords: *Web-technologies; Information Technology; management decisions; solution model.*

Введение. Развитие современного общества и рост значения информационных технологий (всеобщая компьютеризация, интернет, автоматизация производства на базе компьютерных технологий, всевозможные Web-технологии и Web-приложения, а также другие информационные ресурсы), приводят к необходимости подготовки специалистов в области защиты информации и информационных технологий. С целью повышения навыков принятия правильных управленческих решений, возникающих в процессе решения задач по защите информации. Рассмотрение вопросов информационной безопасности в современном обществе рассматривается, как приоритетное направление в государственных структурах, коммерческих и научных учреждениях. Следует отметить, что обеспечение защиты информации и информационных технологий, порой носит бессистемный характер. Такой подход, недопустим, так как влечет за собой расходование ресурсов, как физических так и финансовых, но не выполняет свои функции.

Интерес государственных органов власти к вопросам развития информационных технологий и в первую очередь к защите информации, логично отражается в утвержденных Указах Президента Российской Федерации [1,2], регламентирующих их дальнейшее развитие и направление. Подготовка и переподготовка кадров в сфере защиты информации и информационных технологий становится одной из приоритетных и необходимых для постоянного поддержания уровня знаний необходимых для борьбы с возникающими угрозами.

Следующий уровень информационной безопасности в информационных технологиях в состоянии обеспечить только системный многоуровневый подход, который предполагает использование от двух и более защитных барьеров (сертификация рабочих мест, шифрование данных, использование антивирусной защиты, допуск к рабочему месту через логин и пароль и прочие методы защиты). Необходимо отметить, что многоуровневый подход, также включает в себя анализ развития социально-общественных отношений и направления их приоритетного развития. Возникающие проблемы управления социальными процессами, которые определят направления дальнейшего воздействия. Важным и необходимым инструментом управления становятся социологические исследования. Их результаты, в частности, способствовали переходу к комплексному социально-экономическому планированию и управлению в масштабе предприятия, объединения, города и района. В настоящее время такие исследования ведутся в области социального планирования и управления применительно к отрасли народного хозяйства, создаются социологические службы на промышленных предприятиях, в регионах. В процессе решения практических задач развиваются и углубляются сами социологические исследования, возникают новые проблемы, совершенствуются методы и техника исследований [3].

В Санкт-Петербургском университете МВД России осуществляется подготовка специалистов по технической специальности: «Безопасность информационных технологий в правоохранительной сфере» (Специализация № 1 «Технологии защиты информации в правоохранительной сфере»). Профессиональная подготовка и переподготовка кадров в сфере безопасности информационных технологий для университета являются новыми и требуют особого подхода в организации учебного процесса и создании материально-технической базы.

Выпускники, получив соответствующую квалификацию, направляются в свой комплектующий отдел, от которого они направлялись на учебу. Зачастую в своей повседневной деятельности они сталкиваются с состоянием неопределенности, когда необходимо выбрать наиболее правильное управленческое решение. И только проанализировав имеющиеся информационные данные, которые могут также быть не точны, частично не правильны или просто ошибочны мы переходим к мыслительному процессу со всеми за и против для принятия наиболее подходящего правильного решения. В настоящее время Web-технологий помогают нам проводить анализ имеющихся данных, что ускоряет процесс принятия наиболее подходящего и правильно управленческого решения [4].

Если же затронуть подразделения обеспечивающие безопасность дорожного движения, то управление безопасностью дорожного движения есть многогранный сложный процесс. Особыми возможностями для повышения эффективности управления безопасностью дорожного движения

обладают Web – технологии. Лицо, принимающее решение, формирует процессы обеспечения безопасности дорожного движения в форме модели своего решения. В рамках направления использования информационных технологий для управления безопасностью дорожного движения следует рассмотреть разработку математической модели управления безопасностью дорожного движения, учитывающей возможности Web-технологий. В основу аналитической динамической модели положен закон сохранения целостности объекта. Разработка системы управления безопасности дорожного движения на основе предлагаемой модели позволит повысить оперативность управления безопасности дорожного движения при удовлетворении требований гарантии достижения цели управления [5].

Следующим, особенно важным ресурсом, который оказывает определяющее влияние на национальную безопасность, становится информация, циркулирующая в обществе, а также ее сохранность. В процессе своей деятельности социально-экономические образования различного уровня иерархии, такие как: различные государственные и коммерческие организации, коллективы людей, общественные объединения; работающие по несовпадающим целям в итоге приходят к конфликту. В основе деятельности лежит решение человека. Деятельность основывается на модели [3]. А под информацией обычно понимают сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством. Сведения, используемые человеком в своей деятельности, имеют у него модельную интерпретацию процессов окружающего мира. Зависимость деятельности человека от информации (модельного представления) сформировала новое направление в противоборстве социально - экономических образований как информационное, которое в конце 20-го века получило название «информационная война» [6]. Для решения комплекса задач защиты информации и информационных технологий необходимо разработать теорию. Правильно построенная теория имеет три уровня, три составляющих. Методология. Методы. Технология. Лицо принимающее решение воспринимает окружающий мир и осуществляет свою деятельность через процессы. Процесс – это объект в действии при фиксированном предназначении [3].

Основа деятельности человека – это решение. Решение – это условие реализации предназначения объекта управления или самоуправления. Лицо принимающее решение при управлении может выполнять в различных сочетаниях две функции:

— идентифицировать или распознавать появившуюся проблему;

— нейтрализовать проблему или задействовать ресурсы по нейтрализации проблемы.

Деятельность человека будет реализовываться через управление в соответствующей обстановке. Обстановке соответствует среднее время образования (проявления) проблемы для лица принимающего решения $\Delta t_{пп}$. Информационно-аналитической работе – среднее время распознания или идентификации проблемы $\Delta t_{ип}$. Решению – среднее время нейтрализации проблемы, возникшей перед руководителем - $\Delta t_{нп}$. Графически данные три элемента можно представить в виде рис. 1.

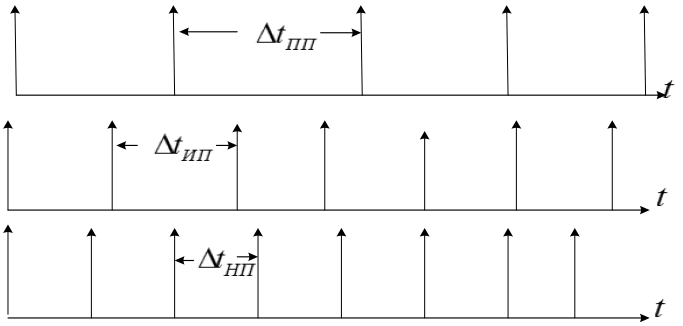


Рис. 1. Диаграмма проявления базовых элементов формирования модели решения.

Представим структурную схему управления следующим образом (Рис.2.). Где:

λ – величина, обратная среднему времени проявления проблемы;

v1 – величина, обратная среднему времени идентификации проблемы;

v2 – величина, обратная среднему времени нейтрализации проблемы.

Величина времени имеет наиважнейшее значение, так как является невосполнимым ресурсом.

Поэтому модель решения руководителя или лица принимающего решение характеризуется четырьмя базовыми состояниями:

A_{00} – руководитель не идентифицирует и не нейтрализует;

A_{10} – руководитель идентифицирует и не нейтрализует;

A_{01} – руководитель не идентифицирует и нейтрализует;

A_{11} – руководитель идентифицирует и нейтрализует.

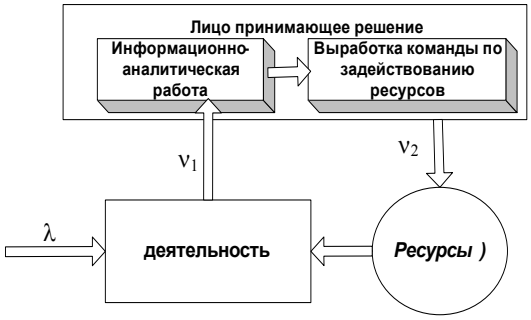


Рис.2. Структурная схема управления процессом обеспечения безопасности

В соответствии с описанной особенностью управленческого решения необходимо ввести вероятности нахождения нашей системы управления в этих четырёх состояниях. Представим наш процесс графом рис. 3. Мы получаем четыре вероятности P_{00}, P_{10}, P_{01}, P_{11}, соответствующие нахождению системы в состояниях A_{00}, A_{10}, A_{01}, A_{11}. Процесс формирования решения можно рассмотреть как цепь Маркова [6]. Такой подход не позволяет в достаточной мере учитывать динамику процесса. Поэтому необходимо использовать непрерывные цепи Маркова. Для реализации такого подхода необходимо составить систему дифференциальных уравнений Колмогорова – Чепмена [3]. Характеристику переходов системы представим на рис. 3. Допустим, что система находится в начальном состоянии A_{00}. При появлении проблемы под воздействием интенсивности λ она переходит в состояние A_{10}, т.е. в состояние распознания проблемы. Из этого состояния система под воздействием интенсивности v_1 осуществляется переход в состояние A_{01}, в котором система начинает процесс нейтрализации проблемы с интенсивностью v_2 и переводит систему в состояние A_{00}. Эта ситуация возможна, если проблема нейтрализована, а очередная проблемы еще не образовалось. Если образовалась проблема, под воздействием интенсивности λ система переходит в состояние A_{11}. Находясь в состоянии A_{11}, под воздействием интенсивности v_1 система переходит в состояние A_{01}, если проблема распознана, и переходит в состояние A_{10} под воздействием интенсивности v_1, если одна проблема нейтрализована. Далее на вход поступает очередная проблема и её надо распознавать. Процесс повторяется

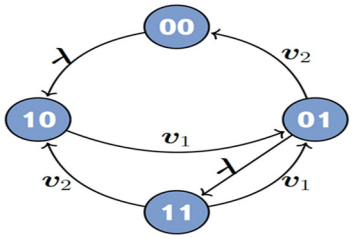


Рис.3. Граф состояний, процесса формирования управленческого решения.

Применяя метод агрегирования, получим условие существования решения в виде следующего соотношения $P = F(\Delta t_{пп}, \Delta t_{ип}, \Delta t_{нп})$. Где P – характеризует степень достижения цели в определенных условиях. Это и есть вероятность того, что проблема идентифицирована и нейтрализована.

Заключение. Во время стремительно развивающихся информационных технологий и компьютеризацией практически всех сфер жизнедеятельности человека, возросло и количество атак с использованием компьютерных технологий, приводящих к хищению информации, информационных ресурсов и информационных систем, что не могло не отразиться на развитии таких направлений подготовки и переподготовки кадров, которые в последующем смогут подготовить специалистов, способных противостоять возникающим угрозам. Дальнейшее развитие и подготовка специалистов по технической специальности: «Безопасность информационных технологий в правоохранительной сфере» считаю приоритетным и заслушивающим внимания. Предложенная модель принятия управленческого решения по обеспечению информационной безопасности позволяет распознавать, идентифицировать и нейтрализовать угрозы, а в случае появления критических угроз, адекватно на них реагировать.

СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента Российской Федерации от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001201705100002 (дата обращения: 11.09.2017).
2. Указ Президента Российской Федерации от 05.12.2016 г. № 646 [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 11.09.2017).
3. Бурлов В. Г. Основы моделирования социально – экономических и политических процессов (Методология. Методы). – СПб.: факультет комплексной безопасности СПБГПУ. 2007 г. – 270 с.

4. Burlov V.G., Grachev M. I., Shlygina N. S. «Adoption of management decisions in the context of the uncertainty of the emergence of threats» // 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM) [Электронный ресурс]. URL: http://ieeexplore.ieee.org/document/7970510/ (дата обращения: 11.09.2017).
5. Burlov V.G., Grachev M. I. «Development of a Mathematical Model of Traffic Safety Management with Account for Opportunities of Web Technologies» // Transportation Research Procedia [Электронный ресурс]. URL: https://doi.org/10.1016/j.trpro.2017.01.023 (дата обращения: 11.09.2017).
6. Бурлов В. Г. О философии информационной войны // Фундаментальные исследования в технических университетах. Национальная безопасность, Том 2, – СПб.: СПбГТУ, 2004 - С. 132-148.

УДК 007

СЕТЕЦЕНТРИЧЕСКАЯ ПАРАДИГМА УПРАВЛЕНИЯ В ЦИФРОВОМ ОБЩЕСТВЕ

Верзун Наталья Аркадьевна[1], Колбанев Михаил Олегович[1], Касаткин Виктор Викторович[2]
[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия, д. 39,
emails: verzun.n@unecon.ru, mokolbanev@mail.ru, v.v.kasatkin@iias.spb.su

***Аннотация*:** В статье описываются основные принципы и характерные особенности новой сетецентрической парадигмы управления. Сетецентризм рассматривается как информационно-технологическая основа цифрового общества, как перспективный подход к управлению деятельности человека способный адаптивно подстраиваться под глобальные вызовы современности. Приводится пример деятельности, базирующейся на использовании сетецентрической концепции управления: цифровое земледелие.

***Ключевые слова**: сетецентризм; сетецентрический подход к управлению; цифровая экономика; цифровое земледелие; информационная решетка; интеллектуальное сельское хозяйство.*

NETWORK-CENTRIC CONTROL PARADIGM IN A DIGITAL SOCIETY

Verzun Natalya[1], Kolbanev Mikhail[1], Kasatkin Victor[2]
[1] The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
[2] St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
Russia, St. Petersburg, 14 Line, 39
emails: verzun.n@unecon.ru, mokolbanev@mail.ru, v.v.kasatkin@iias.spb.su

Abstract: The article describes the main principles and characteristics of the new network-centric management paradigm. Network-centric is seen as a technological and information-based digital society, as a promising approach to the management of human activities capable of adaptive to adapt to global challenges. An example of activities based on the use of network-centric management concept: digital agriculture.

***Keywords**: network-centric; network centric management approach; digital economy; digital agriculture; information grid; intelligent agriculture.*

Введение. Традиционный подход к управлению, основанный на жесткой вертикали власти, “не справляется” в условиях динамично, неожиданно и непредсказуемо меняющейся обстановки, большого числа неопределенностей, растущих объемов информации, требуемых для адекватной оценки ситуации и т.д., которые характерны для цифровой экономики. На смену ему приходят новые подходы к управлению деятельности человека способные адаптивно подстраиваться под глобальные вызовы современности. С этим связано и появление новой парадигмы управления – так называемой поствинеровской кибернетики [1], компонентом которой является, в частности, сетецентризм [2].

Возникший на рубеже веков, изначально термин “сетецентризм” (network-centric) использовался в военной сфере для определения войны нового типа – сетецентрической (или сетецентричной) [3]. Однако вскоре тема сетецентризма, из изданий военного и политического характера “перекочевала” в работы экономической, социально-экономической, гуманитарной и пр. направленностей. А идеи данного, нового подхода к управлению вышли за рамки военной сферы и сегодня приобрели более широкое “гражданское” значение [4–6]. Так, например:

– в [4] упоминается, что “современные принципы управления сложными системами стали … сетецентричными”;

— в работе [5] под сетецентричностью понимается принцип организации систем управления, позволяющий “реализовать режим ситуационной осведомлённости благодаря формированию и поддержанию единой для всех ярусов управления, целостной, контекстной информационной среды и включения в процесс её непрерывной актуализации возможно большего числа источников первичной информации”;

— в [6] отмечается, что суть сетецентрического управления (называемого автором также субсидиарным) заключается “в выделении полномочий и прав самостоятельного принятия решений от центральных органов периферическим”.

Существует и более узкое понятие термина сетецентризм – под ним подразумевается необходимость в насыщении систем управления современными средствами инфокоммуникаций. Обществом постепенно осознается их ключевая и ведущая роль в развитии человечества [7-11], Современный этап становления инфокоммуникаций связывают с внедрением совокупности технологий третьей платформы информатизации. К ним относят: облачные и туманные вычисления; интернет вещей; большие данные; мобильный широкополосный доступ; наложенные сервисы [12]. Применение данных технологий значительно расширяет возможности использования информационных ресурсов в различных отраслях деятельности, повышая их эффективность.

Сетецентрический подход к управлению появился в ходе поисков новых методов управления. В [13] отмечается, что в наши дни ”развитие теории управления стимулируют тенденции «миниатюризации», «децентрализации» и «интеллектуализации» систем, которые состоят из большого числа взаимодействующих между собой автономных агентов технической, социальной или информационной природы” и, соответственно, наблюдается постепенный переход от традиционной, централизованной системы управления с явно выраженной вертикалью власти и жестким регламентом к децентрализованной (распределенной) с поддержкой коммуникаций как по вертикали, так и по горизонтали. Основным эффектом при правильной реализации концепции сетецентризма в какой-либо деятельности является синергетический эффект, проявляющийся, например, в повышении скорости принятия решений, быстрой адаптации к изменениям, в уменьшении уязвимости к неблагоприятным или разрушающим внешним воздействиям, появлении новых возможностей.

На рис.1 показаны два подхода к управлению – традиционный со строгой пирамидой власти и сетецентрический. Ключевым и связующим инфраструктурным элементом сетецентрической деятельности является информационные и телекоммуникационные технологии, поддерживающие, во-первых, единую информационную среду доступную всем участникам на всех уровнях управления, а, во-вторых, взаимодействие между участниками деятельности [2]. Именно благодаря наличию и интенсивному развитию ИКТ становится возможным применение на практике концепции сетецентризма в экономических, социально-экономических и др. сложных системах.

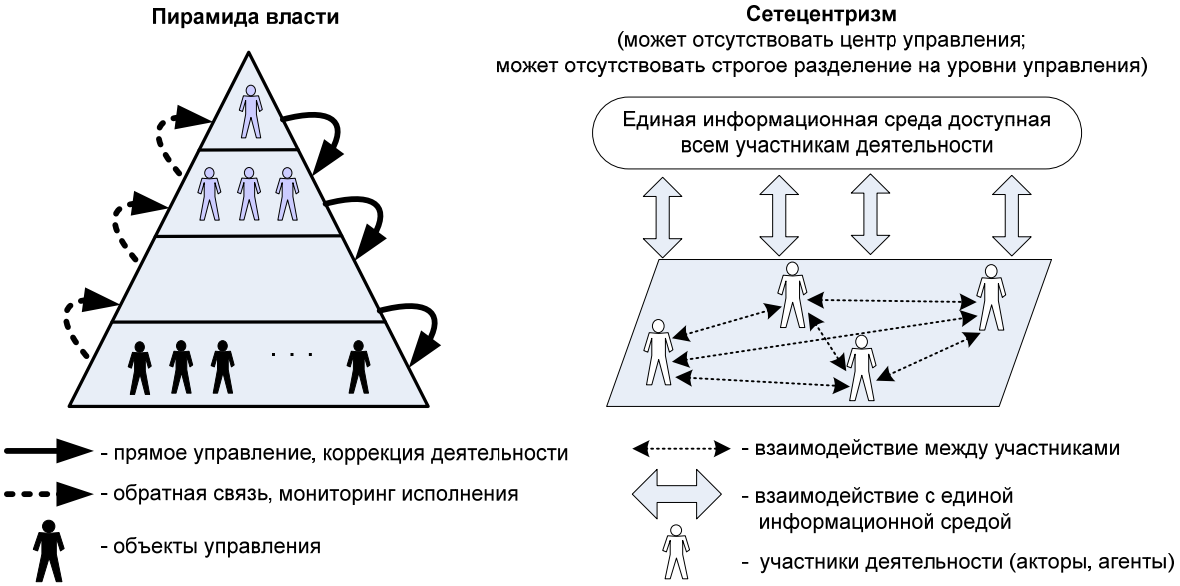


Рис. 1 Классический и сетецентрический подходы к управлению деятельностью

По мнению авторов, сегодня сетецентризм надо понимать, как концепцию деятельности, в основе которой лежит стремление накрыть пространство (территорию) инфокоммуникационной сетью для комплексных измерений в реальном времени параметров пространства, формирования цифровых моделей всех его объектов, создания единой среды информационного взаимодействия и обеспечения согласованности действий всех участников, под которыми теперь понимаются не только люди, но технические устройства, программные компоненты.

Характерными особенностями сетецентрических систем являются:

- цифровое описание всех объектов предметной области;
- распределенная неоднородная сетевая архитектура;
- точность информационного описания всех событий;
- совместная мобильность сетевых объектов;
- охват территорий произвольных размеров и конфигурации;

– работа в реальном масштабе времени;
– надежность и неуязвимость всего комплекса информационных ресурсов [14-17] и др.

В целом основные идеи сетецентрического принципа управления деятельностью независимо от сферы его применения можно сформулировать следующим образом:

1) ориентирован на повышение эффективности деятельности в условиях: динамично изменяющейся обстановки; многообразия и большого числа событий, на которые необходимо оперативно реагировать; неопределенности и риска; ограниченности ресурсов (физических, материальных, финансовых, энергетических); нехватки или избытка информации; жесткой конкурентной борьбы и пр.

2) предполагает переход от централизованной модели управления, от концепции властной вертикали, жесткой структуры к распределенной системе, к наделению правом самостоятельного принятия решений периферических равноправных территориально разнесенных автономных участников процесса (агентов). Агенты могут иметь разную природу и в зависимости от рассматриваемой деятельности: это могут быть люди или команды людей; технические объекты: роботы, умные вещи (smart things) интернета вещей; программы (softbots) и др. [18, 19].

3) самоорганизация и самосинхронизация, что является следствием высокой степени самостоятельности и ответственности участников деятельности на всех уровнях управления. Для социально-экономических систем это, например, проявляется в неформальном сотрудничестве и творческом подходе, в замене административных методов управления на социально-психологические, учитывающие профессиональные и психофизиологические характеристики людей. Для технических систем, это, например, применение биоподобных алгоритмов для информационного взаимодействия агентов различной природы, так, для решения задач маршрутизации в самоорганизующихся сенсорных сетях находят применение принципы роевого интеллекта [19].

4) необходимым условием реализации концепции сетецентризма на практике является создание единой доступной для всех уровней управления информационной среды, благодаря наличию которой в любой момент времени все участники (агенты) деятельности обладают актуальной и достоверной информацией, что обеспечивает высокую скорость реагирования на изменяющуюся ситуацию и повышает качество принятия решений. Важным фактором при этом является достоверность, оперативная обновляемость и пополняемость информационных ресурсов.

5) для формирования единой информационной среды деятельности создается полносвязная инфокоммуникационная инфраструктура, с наложенной на неё сетью средств: мониторинга внешнего окружения, контроля результатов деятельности, коррекции деятельности и пр. Все участники деятельности находятся в устойчивом сетевом взаимодействии.

6) инфокоммуникационная инфраструктура построена на открытых стандартах и протоколах, пригодна для масштабирования и модернизации, а при её реализации на практике применяются апробированные технические решения. Отдается предпочтение программным продуктам и техническим средствам, доступным на рынке COTS-продуктам (commercial off-the-shelf).

Применение вышеизложенных принципов организации деятельности уже сейчас в той или иной степени можно обнаружить в сфере госуправления, финансов, образования, экономики и пр. В частности, на рис. 2 представлен пример использования идей сетецентризма в цифровом земледелии (digital farming**,** digital agriculture).

Цифровое земледелие ориентировано на максимальное использование всех, задействованных в выращивании агрокультур ресурсов (земли, семян, воды, удобрений, сельскохозяйственной техники, топлива и пр.) и является инновационным направлением в оздоровлении сельского хозяйства во всем мире [20]. Основная цель цифрового земледелия – получение максимального урожая при минимальных затратах ресурсов, что становится возможным благодаря организации агротехнических мероприятий в соответствии с реальными потребностями выращиваемых в данном месте культур [21].

Основными инструментами цифрового земледелия выступают мониторинг текущего состояния посевов и анализ многолетних данных.

Наблюдение за посевами предполагает ”накрытие” всей площади с посадками информационной решеткой (инфокоммуникационной сетью), которую составляют различные технические средства наблюдения:

Искусственные спутники Земли (ИСЗ) проводят регулярную съемку посевов и окружающей их местности, наблюдают и прогнозируют погодные условия. Уже сегодня все страны с развитой космической отраслью применяют спутниковый мониторинг в сельскохозяйственных целях [22].

Беспилотные летательные аппараты (БПЛА) [23] и дистанционные видеокамеры ведут видеосъемку: следят за состоянием почвы и посевов. Так, например, наблюдают за:

– всхожестью, полеганием, созреванием, болезнями посевов;
– колориметрическими характеристиками посевов (изменение цвета зеленой части растения свидетельствует о недостатке или избытке каких-либо минеральных веществ);
– распространением сорняков и вредителей;
– характером рельефа поля и состоянием грунта;

– за изменением температуры поверхности земли (для дальнейшего построения термограммы визуализированного представления распределения температур на поверхности поля);
– работой и состоянием агротехнического оборудования.

Рис. 2. Применение концепции сетецентризма в цифровом земледелие

В случае применения БПЛА и систем видеонаблюдения различные стресс-факторы (болезни растений, сорняки, вредители и пр.) могут быть обнаружены раньше, чем они станут заметны человеческому глазу и нанесут существенный урон урожаю.

Разнообразные датчики предоставляют возможность определять:
– уровень увлажненности и химический состав грунта;
– степень освещенности посевов;
– целостность защитных сооружений и пр.

Собирать информацию, накопленную датчиками за время их автономной работы, позволяют БПЛА [23].

Информация, получаемая непрерывно в режиме реального времени от различных средств мониторинга сельскохозяйственной территории (от информационной решетки) затем может использоваться ”на местах” для управления исполнительными элементами или доставляться в облако (на серверы) для дальнейшей обработки/анализа.

1) В случае использования ”на местах”: децентрализовано на основании полученных данных принимаются решения по координации действий различных исполнительных устройств (см. рис. 2). Так, например:
– при выявлении датчиком влажности сухой почвы запускаются системы орошения;
– при недостатке света включается дополнительное освещение;
– при нарушении заграждения идет вызов службы охраны, ремонтной бригады;
– БПЛА помогают в сборе необходимых данных при проведении агротехнических операций (посев, рыхление, сбор урожая) сельскохозяйственным роботам и машинам – сообщают о рельефе и типе почвы, управляют направлением движения техники;
– БПЛА не только выполняют функции мониторинга и сбора данных, но и сами выступают в качестве исполнительных элементов цифрового земледелия. Они применяются для: равномерного опрыскивания урожая ядохимикатами и минеральными удобрениями, посадки растений и пр. Разработаны сельскохозяйственные дроны, выстреливающие в почву капсулами с семенами. BioCarbon Engineering весной 2015 г. объявил о планах сажать в будущем с применением подобной технологии до 1 млрд. деревьев в год [24].

Также оперативную информацию о состоянии полей и посевов может получать и непосредственно сам фермер на планшет/смартфон. Специально разработанные для мобильных устройств приложения позволяют быстро получать данные о текущей ситуации на поле, консультации по каким-либо вопросам (например, компания Bayer разработала мобильное приложение, которое автоматически распознает сорняки на основе фотографии [25]), что способствует принятию обоснованных решений по управлению агротехническими мероприятиями.

2) Собранные данные используются не только ”на местах”, но и передаются ”в облако”, где происходит накопление, обработка, анализ информации, получаемой от информационной решетки. По результатам манипуляций с данными:

– планируют посев сельскохозяйственных культур и формируют стратегии ухода за ними, применимые к конкретным условиям;

– предсказывают распространение вредителей и болезней на ранних стадиях;

– создают прогнозные карты урожайности, термограммы почвы и пр.

Заключение. Сетецентрический подход к управлению является одним из перспективных направлений поствинеровской кибернетики [1, 26]. Его можно рассматривать как новую методологию и основу деятельности современного человека в условиях цифрового общества. Данный подход, связанный с накрытием пространства инфокоммуникационной сетью, позволяет в реальном времени вести его непрерывный мониторинг, что обеспечивает согласованность действий, точность, оперативность и корректность принимаемых решений и в конечном итоге повышает эффективность деятельности. Так, например, в сельском хозяйстве, в частности, в земледелии, внедрение данного подхода в совокупности с применением цифровых технологий позволит сделать деятельность по выращиванию агрокультур более интеллектуальной, технологичной, эффективной и устойчивой. Однако для полного раскрытия потенциала цифрового сельского хозяйства необходимо: создание соответствующего правового поля и налаживания экономических стимулов, а также формирование развитой цифровой инфраструктуры. Последнее особенно сложно реализуемо в условиях сельской местности и существующей проблемы цифрового неравенства.

СПИСОК ЛИТЕРАТУРЫ

1. Хохлова М. Н. Гармогенез. Поствинеровская кибернетика / Русский инженер. 2013. – №2(37). – С.34–35.
2. Верзун Н. А., Ипатов О. С., Колбанёв М. О. О сетецентрических моделях цифровой экономики // Сборник: Информационные технологии цифровой экономики: сб. статей. – СПб.: Изд-во СПбГЭУ, 2017. С.35–41.
3. Осипов В. Ю. Куприянов А. А. Принципы сетецентрического подхода и их применимость при решении задач управления силами (войсками). URL: http://www.apu.npomars.com/images/pdf/17_11.pdf
4. Рыжов В. А. Сетецентризм – управление сложностью. [Электронный ресурс]. Режим доступа: http://spkurdyumov.ru/networks/setecentrizm-upravlenie-slozhnostyu/
5. Чемезов С. В. Турко Н. И., Куликов С. А., Дроговоз П. А. Развитие системы стратегического менеджмента интегрированных структур ГК «Ростехнологии» на основе концепции сетецентричности / Проблемы стратегического менеджмента и механизмы военно-гражданской интеграции в высокотехнологичных отраслях промышленности: сб. науч. статей. – М. : ЦОП АВН, 2011. – С. 93-104.
6. Кудж С. А. Принципы сетецентрического управления в информационной экономике // Госсоветник. 2013. №4. URL: http://cyberleninka.ru/article/n/printsipy-setetsentricheskogo-upravleniya-v-informatsionnoy-ekonomike .
7. Верзун Н. А., Колбанёв М. О., Михайлов С. В. Информационные технологии в периодизации истории / Ученые записки Международного банковского института. Вып. 13. – СПб.: Изд-во МБИ. – 2015. – С.150–161.
8. Максимцев И. А., Колбанёв М. О., Коршунов И. Л., Левкин И. М., Микадзе С. Ю. О технологических основаниях новой доктрины информационной безопасности Российской Федерации / Новые горизонты глобального мира: сб. научн. тр./ Балт. Гос. Техн. ун-т. СПб. – 2015. – С.270–281.
9. Колбанев М. О., Коршунов И. Л., Левкин И. М. Проблемы информационно-технологической деятельности / Изв. вузов. Приборостроение. – 2017. – Т.60, № 2. – С.105–109.
10. Верзун Н. А., Колбанев М. О, Омельян А. В. Введение в инфокоммуникационные технологии и сети Future Networks: учебное пособие. – СПб.: Изд-во СПбГЭУ, 2016. – 51 с.
11. Верзун Н.А., Касаткин В.В., Колбанёв М.О. Цифровые технологии: инфокоммуникации и экономика // Сборник: Информационные технологии цифровой экономики: сб. статей. – СПб.: Изд-во СПбГЭУ, 2017. С.29-34.
12. Верзун Н. А., Колбанёв М. О., Татарникова Т. М. Технологическая платформа четвертой промышленной революции / Геополитика и безопасность. – 2016. – № 2 (34). – С.73–78.
13. Новиков Д. А. Кибернетика: Навигатор. История кибернетики, современное состояние, перспективы развития. – М.: ЛЕНАНД, 2016. –160 с.
14. Богатырев В. А., Богатырев С. В. Надежность мультикластерных систем с перераспределением потоков запросов / Изв. вузов. Приборостроение - 2017. - Т. 60. - № 2. - С.171–177.
15. Левкин И. М. Информационно-экономическая безопасность как специфический элемент экономической безопасности / Технологии информационно-экономической безопасности: сб. статей сотр. каф. ИС и Т. – СПб.: Изд-во СПбГЭУ, 2016. – С.79–89.
16. Колбанёв М. О., Коршунов И. Л., Левкин И. М. Информационно-экономические угрозы и механизм их формирования / Геополитика и безопасность. – 2016. – № 1 (33). – С.85–89.
17. Верзун Н. А., Колбанёв М. О., Татарникова Т. М. Аспекты безопасности информационно-экономической деятельности / Технологии информационно-экономической безопасности: сб. статей сотр. каф. ИС и Т. – СПб.: Изд-во СПбГЭУ, 2016. – С.52–56.
18. Верзун Н. А., Ипатов О. С., *Колбанев* М. О. Интернет вещей и информационно-технологическая безопасность / Технологии информационно-экономической безопасности: сб. статей сотр. каф. ИС и Т. – СПб.: Изд-во СПбГЭУ, 2016. – С.37–43.
19. Боронин П. Н. Кучерявый А. Е. Интернет вещей как новая концепция развития сетей связи / Информационные технологии и телекоммуникации. 2014. №3(7). – С.7–30.
20. Шилерова Е., Овчинников А. С., Балашова Н. Н. Использование принципов точного земледелия для управления бизнесом. Using the principles of the precision agriculture for a business management // Известия НВ АУК. 2015. №1 (37). – С.218-223.
21. Махотлова М. Ш. Технологии и основные направления точного земледелия // Символ науки. 2016. №1-3. – С.51-53.
22. Материалы конференции по цифровому земледелию http://sk.ru/events/3123.aspx
23. Вырелкин А. Д., Кучерявый А. Е., Прокопьев А. В. Исследование возможности применения беспилотного летательного аппарата в качестве временного головного узла кластеров наземной сенсорной сети / Информационные технологии и телекоммуникации. – 2015. – № 1(9). – С. 27–34.
24. БПЛА как основа земледелия ближайшего будущего. https://iot.ru/selskoe-khozyaystvo/bpla-kak-osnova-zemledeliya-

blizhayshego-budushchego
25. Цифровые технологии настроены на революцию в сельском хозяйстве https://www.cropscience.bayer.ru/news/3812/
26. Верзун Н.А., Колбанёв М.О., Касаткин В.В. Инфокоммуникационная среда, реализующая сетецентрический подход к управлению деятельности / Перспективные направления развития отечественных информационных технологий: материалы III межрегиональной научно-практической конференции. Севастополь 19-23 сентября 2017 г. – Севастополь: “РИБЕСТ”, 2017. – С.76-78.

УДК 621.39

ЭВОЛЮЦИЯ СЕТЕЙ ЭЛЕКТРОСВЯЗИ И ПРИНЦИПОВ ИХ ПОСТРОЕНИЯ

Верзун Наталья Аркадьевна[1], Колбанев Михаил Олегович[1], Ипатов Олег Сергеевич[2]
[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
[2] Санкт-Петербургский политехнический университет Петра Великого,
Россия, Санкт-Петербург, ул. Политехническая, д. 29,
emails: verzun.n@unecon.ru, mokolbanev@mail.ru, ipatov_os@spbstu.ru

***Аннотация*:** В статье рассматривается эволюция сетей электросвязи сквозь призму формирования и развития базовых принципов их построения, перечень которых пополняется вместе с возникновением новых концепций создания, организации и функционирования сетей связи. Появление новых принципов построения сетей электросвязи обусловлено непрерывным обновлением требований к телекоммуникациям и расширением спектра предоставляемых ими инфокоммуникационных услуг.

***Ключевые слова**: сеть электросвязи; мультисервисная сеть; сети будущего; принцип построения сети.*

THE EVOLUTION OF TELECOMMUNICATION NETWORKS AND PRINCIPLES OF THEIR CONSTRUCTION

Verzun Natalya[1], Kolbanev Mikhail[1], Ipatov Oleg[2]
[1] The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
[2] St. Petersburg Polytechnic University Peter the Great,
Russia, St. Petersburg, Polytechnicheskaya str. 29,
emails: verzun.n@unecon.ru, mokolbanev@mail.ru, ipatov_os@spbstu.ru

Abstract: The article deals with the problem of adaptive management of low-intensity streams, including the prevention of performance degradation multiservice network for overloads, eliminate the possibility of deadlock in the network, optimize the allocation of network resources among competing flows custom messages defined by different pairs of source-receiver. Analytical relations for the assessment of both the average probability lock dial information units, so the average latency messaging users.

***Keywords**: telecommunication network; multiservice network; networks of the future; principle of building a network.*

Введение. Рассматривается эволюция сетей электросвязи сквозь призму формирования и развития принципов построения сетей связи, перечень которых пополнялся вместе с появлением новых концепций их создания, организации и функционирования, возникших в связи с непрерывным обновлением требований к телекоммуникациям и с расширением спектра предоставляемых инфокоммуникационных услуг.

Авторы выделяют следующие базовые принципы построения сетей:

1. Принцип распространения данных, который следует из коммуникационной сущности сетей связи.

Сеть должна создавать материальные объекты, способные перемещаться в пространстве и переносить информацию пользователей. Эти материальные объекты – данные (а также сообщения, сигналы, кадры, пакеты и пр.), а эффективность работы сетей связи зависит от способов реализации физических процессов распространения данных. К числу основных характеристик любой сети связи относится время перемещения данных между двумя точками пространства.

В современных инфокоммуникационных сетях в качестве физического процесса распространения данных используется электромагнитное взаимодействие, и, соответственно, сети называются сетями электросвязи [1].

Взаимодействие пользователя с сетью при получении услуг происходит с помощью интерфейсов, которые скрывают коммуникационную сущность информационных сетей от пользователя. Чем сложнее предоставляемые услуги, тем сложнее интерфейсы. При рассмотрении сети различают:

– сети на уровне интерфейсов доступа к услугам и
– сети на уровне реализуемых ими процессов, технологий, коммуникационных взаимодействий и системных свойств.

2. Принцип мультиплексирования физических цепей.

Мультиплексирование — процесс уплотнения каналов связи в одной физической среде, или иначе, передача нескольких потоков данных по одному каналу связи, с использованием специальных технических устройств [2]. На сегодняшний момент применяются различные технологии мультиплексирования: частотное, временное, кодовое, волновое, пространственное разделение, а также комбинации нескольких технологий. Все они основаны на свойстве электромагнитной волны существовать независимо в одной и той же среде от других электромагнитных колебаний, с отличающимися параметрами. Это свойство называется суперпозицией и распространяется на все типы полей.

Сеть должна мультиплексировать физические цепи первичной сети и формировать типовые каналы для распространения данных. К числу основных характеристик любой сети связи относится пропускная способность каналов. Чем выше пропускная способность, тем с большей скоростью можно передавать данные.

3. Принцип коммутации информационных потоков.

Ни по техническим, ни по экономическим причинам нельзя создать глобальную сеть связи, в которой каждый пользователь был бы соединен каналами связи со всеми другими пользователями. Каналов всегда меньше, чем пользователей, имеющих к ним доступ. Для обеспечения доступа большой группы пользователей к ограниченному количеству общесетевых каналов передачи сигналов электросвязи первичной сети используется специальное оборудование – центры коммутации [3].

Сеть использует коммутацию для организации доступа большого количества пользователей к ограниченной группе общесетевых канальных и других ресурсов. Количество каналов ограничивает:

– либо число одновременно установленных соединений;
– либо скорость передачи данных пользователей.

К числу основных характеристик любой сети связи относится время коммутации (маршрутизации). Коммутация реализуется в режиме реального времени. Все сети связи реализуют для соединения своих абонентов одну из технологий коммутации: каналов (circuit switching), сообщений (message switching) или пакетов (packet switching). От того какая технология коммутации положена в основу сети зависят её основные свойства и алгоритмы работы.

4. Принцип идентификации (или адресуемости) всех элементов сетей.

Сеть должна однозначно адресовать пользователей и свои узловые, станционные и оконечные элементы [4]. Система нумерации – это неотъемлемый элемент сети, это система цифровых, буквенных, символьных обозначений или комбинации таких обозначений, в том числе коды, предназначенные для однозначного определения (или идентификации) сети связи и (или) ее узловых или оконечных элементов. Для внедрения системы нумерации создаются специальные программно-аппаратные комплексы. Структура системы нумерации (адресации) всегда повторяет структуру сети связи, в глобальных сетях – это иерархия.

Для передачи адресной информации по сети должны быть разработаны системы сигнализации.

Система сигнализации – это свод правил и процедур взаимодействия элементов сетей, следуя которым пользователи и сетевые центры заказывают услуги, занимают (освобождают) те или иные сетевые ресурсы, согласуют параметры используемых устройств, сохраняют и считывают информацию и др.

Вышеперечисленные четыре принципа относятся к традиционным сетям электросвязи. С учетом особенностей сетей NGN они были дополнены следующими:

5. Принцип мультисервисности [4].

Инфокоммуникационная сеть должна содержать единую мультисервисную сеть, которая обеспечивает не только мультиплексирование линий связи, но и коммутацию трафика всех пользователей и наложенных систем.

Сеть NGN позволяет единообразно решать задачи распространения и коммутации информационных потоков при предоставлении любых услуг. На единую сеть возложили главную функцию вторичных сетей – коммутацию. В результате вторичные сети «превратились» в наложенные сервисы. Наложенный сервис использует единые для всех услуг системы адресации и сигнализации мультисервисных сетей и создает собственные системы биллинга, техобслуживания и управления. внедрение новых услуг значительно упростилось.

Отличие между сетями XX и XXI века можно увидеть на рисунке 1.

. В XX веке, используя общую первичную сеть типовых каналов передачи, вторичные сети предоставляли пользователям специфические, характерные только этим вторичным сетям информационные услуги, использующие системы адресации, биллинга, техобслуживания, управления и сигнализации.

В современной же сети (NGN), используя общие первичную сеть типовых каналов передачи и маршрутизаторы пакетов, сети создают единую среду для информационного взаимодействия на расстоянии и обеспечивают распространение данных между оконечными точками между подключенными системами информационного обслуживания, с заданным качеством.

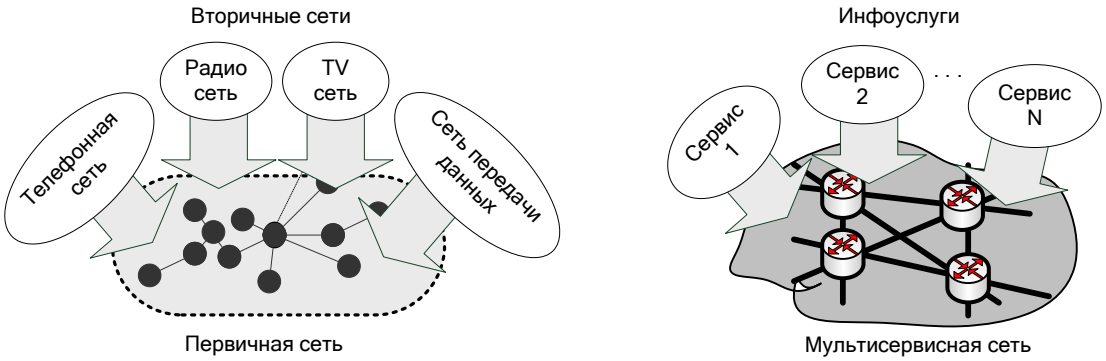


Рис. 1. Отличие между сетями XX и XXI века

6. Принцип множественного доступа к глобальным сетям.

Инфокоммуникационная сеть должна использовать множественный доступ многих пользователей к общим ресурсам последней мили [5-7].

Оборудование, которое связывает пользователя с глобальной сетью – последняя миля – претерпело изменения в NGN. В сетях XX века оно представляло собой персональную (абонентскую) линию связи и обеспечивало передачу трафика с фиксированной скоростью (в фиксированном диапазоне частот). Такой способ подключения не отвечает требованиям широкополосности и инвариантности доступа, поэтому в сетях NGN создаются специальные сети доступа (множественного доступа). Они решают, в частности, следующие задачи: согласуют терминалы пользователей с глобальной сетью на физическом, энергетическом и логическом уровнях, обеспечивают мобильность терминалов, позволяют повысить использование оборудования, расположенного на последней миле. Сети доступа – это всегда системы реального времени. К числу основных характеристик инфокоммуникационной сети относится время ожидания доступа к ресурсам сети.

Перечисленные выше принципы пополнились новыми с появлением концепции сетей будущего (Future Networks), необходимость возникновения которой была обусловлена непрерывным изменением требований к телекоммуникациям, нуждающимся в постоянном развитии, обновлении и усовершенствовании т.к.

- сети электросвязи устаревают (“изнашиваются”) физически;
- не соответствуют требованиям информационного рынка;
- не справляются с постоянно растущим объемом трафика;
- не обеспечивают инфраструктуру для внедрения новых услуг;
- не отвечают требованиям государственного управления и т.д.

Ниже приведены еще шесть принципов построения сетей, которые в отличие от ранее существовавших дополнительно учитывают перечисленные факторы, а также потребности цифрового общества (цифровой экономики). [2, 8–10]. Они сформулированы на основе международных рекомендаций. Так, например, наиболее важные и на сегодняшний день в достаточной степени не реализованные и не применяемые в существующих сетях принципы создания и функционирования (или в буквальном переводе ”целевые установки”) будущих сетей представлены в Y.3001 [10].

7. Принцип предоставления услуг.

В сетях будущего ввод новых услуг не должен требовать существенных капитальных вложений, эксплуатационных расходов или значительных временных затрат. Надо обеспечить возможность поддержки лавинообразного числа и объема услуг, ожидаемого в связи с переходом к цифровой экономике.

8. Принцип организации данных.

Данными для сети будущего должна стать вся цифровая Вселенная. Доступ к ним должен быть легким, быстрым и качественным независимо от местоположения пользователя. Должна обеспечиваться персонализация всех процессов работы с данными.

9. Принцип экологичности.

Сети будущего должны быть экологически безопасны для окружающей среды. Технические решения должны минимизировать влияние на экосистему, сократить потребление всех ресурсов, включая энергию [11-20].

Принцип экологичности (или экологический фактор) согласно Y.3001 [10], подразумевает, что:

- функционирование сетей будущего должно быть безопасно для окружающей среды;
- необходимо сократить затраты физических ресурсов (прежде всего энергетических) на всех этапах жизненного цикла сети, что, в частности, позволит уменьшить выбросы парниковых газов в атмосферу Земли;
- будет возможно применение сетей будущего для снижения вредного воздействия на окружающую среду, оказываемого другими секторами экономики.

10. Принцип социально-экономической направленности.

Сети будущего должны устранить существующее цифровое неравенство (digital divide) за счет снижения затрат на жизненный цикл услуг и типового широкополосного доступа, что в свою очередь послужит стимулом для развития цифровой экономики.

11. Принцип единого идентификатора пользователя услуг.

Сегодня, каждая предоставляемая пользователю инфокоммуникационная услуга, имеет свой идентификатор (номер стационарного телефона, номер мобильного телефона, e-mail, адрес персональной web-страницы и пр.). Таким образом, имеем: 1 сервис = 1 адрес. Подобная ситуация, ведет к тому, что растет число записей в базах данных персональной информации, растет число контактной информации, которую необходимо хранить каждому конечному пользователю и т.п. В сетях будущего предполагается переход к единому, заново присваиваемому, идентификатору для всех пользователей сети, который не будет зависеть: от местоположения пользователя, от типа/вида устройства, с которого идет обращение к инфоуслугам, от используемого при этом протокола сетевого уровня.

Необходимо также отойти от однозначного соответствия: конечный пользователь=человек, т.к. в сетях будущего участниками информационного взаимодействия могут быть как люди, так и технические устройства (умные вещи), которые наряду с человеком будут иметь уникальный идентификатор.

12. Принцип виртуализации ресурсов.

В сети будущего должна поддерживаться виртуализация сетевых ресурсов, которая обеспечит логическое разделение между сервисами; совместное использование физической сетевой инфраструктуры многими виртуальными ресурсами; возможность создания объединенных ресурсов.

Заключение. Для того чтобы сети связи нового поколения удовлетворяли требованиям цифровой экономики они должны создаваться и функционировать согласно представленным в статье принципам: традиционным и новым, возникшим с появлением концепции сетей будущего.

СПИСОК ЛИТЕРАТУРЫ

1. Верзун Н. А., Колбанев М. О., Омельян А. В. Перспективные технологии инфокоммуникационного взаимодействия: учебное пособие – СПб.: Изд-во СПбГЭУ, 2017. – 77 с.
2. Верзун Н. А., Колбанёв М. О., Омельян А. В. Введение в инфокоммуникационные технологии и сети Future Networks: учебное пособие. – СПб.: Изд-во СПбГЭУ, 2016. – 51 с.
3. Кожанов Ю. Ф., Колбанёв М. О. Технология инфокоммуникации. – Курск: Науком, 2011. – 260 с.
4. Кожанов Ю. Ф., Колбанев М. О. Интерфейсы и протоколы сетей следующего поколения теория и практика: учебное пособие. – СПб.: ГУАП, 2010. – 372 с.
5. Верзун Н. А., Колбанёв М. О., Коршунов И. Л., Микадзе С. Ю. Основы моделирования информационных систем множественного доступа : учеб. пособие. – СПб.: Изд-во СПбГЭУ. – 2015. – 138 с.
6. Верзун Н. А., Колбанёв М. О., Омельян А. В. Регулируемый множественный доступ в беспроводной сети умных вещей / Омский научный вестник. Сер. Информатика, вычислительная техника и управление. – 2016. – № 4 (148). – С. 147–151.
7. Верзун Н. А. Модель процесса передачи информации в двухуровневой ассоциации систем множественного доступа. / Региональная информатика и информационная безопасность. Сборник трудов. СПб общество информатики, вычислительной техники, систем связи и управления. 2016. СПб., С.145–149.
8. Верзун Н. А., Касаткин В. В., Колбанёв М. О. Цифровые технологии: инфокоммуникации и экономика / Сборник: Информационные технологии цифровой экономики: сб. статей. – СПб.: Изд-во СПбГЭУ, 2017. – С.29–34.
9. Росляков А. В., Ваняшин С. В. Будущие сети (Future networks) – Самара: **ПГУТИ, 2015. – 274 с.**
10. Y 3001: Objectives and design goals. – http://www.itu.int.
11. Росляков А. В. Оценка энергоэффективности будущих сетей / Информационные технологии и телекоммуникации. – 2015. – №3(11). – С.54–64.
12. Росляков А. В. Оценка энергопотребления будущих сетей / Электросвязь. – 2016. – №8. – С.43–50.
13. Колбанев М. О. Верзун Н. А., Омельян А. В. Об энергетической эффективности сетей пакетной передачи данных / Изв. вузов. Приборостроение. – 2014. – Т.57, № 9. – С.42–46.
14. Верзун Н. А., Колбанев А. М., Колбанев М. О. Энергетическая эффективность помехоустойчивого кодирования в беспроводных сетях интернета вещей / Изв. вузов. Приборостроение. – 2017. – Т.60, № 2. – С.143–149.
15. Верзун Н. А. Колбанев М. О., Пойманова Е. Д. Энергетические характеристики процесса долговременного хранения данных / Изв. вузов. Приборостроение. – 2017. – Т.60, № 2. – С.158–164.
16. Верзун Н. А., Колбанёв М. О., Шамин А. А. Энергетическая эффективность взаимодействия в беспроводных сенсорных сетях / Информационные технологии и телекоммуникации. 2017. Т.5. № 1. – С.88–96.
17. Верзун Н. А., Колбанёв М. О. Некоторые аспекты энергетической эффективности информационного взаимодействия / Региональная информатика и информационная безопасность. Сборник трудов. СПб общество информатики, вычислительной техники, систем связи и управления. 2015. СПб. С.327–330.
18. Воробьев А. И., Колбанев А. М., Колбанев М. О. Зеленые информационные технологии / Ученые записки Международного банковского института. Вып. 12. – СПб.: Изд-во МБИ, 2015. – С.153–165.
19. Воробьев А. И., Колбанёв А. М., Колбанёв М. О. Модель оптимизации энергопотребления умными вещами. Известия СПбГЭТУ ЛЭТИ. 2015. Т.7. – С.46–49.
20. Воробьев А. И., Колбанёв А. М., Колбанёв М. О. Экологическая безопасность информационных технологий / Геополитика и безопасность. – 2015. – № 4 (32). – С.90–99.

УДК 007

ПРИМЕРЫ РЕАЛИЗАЦИИ ОБОБЩЕННОЙ МОДЕЛИ ДЕЯТЕЛЬНОСТИ В ЦИФРОВОМ ОБЩЕСТВЕ

Верзун Наталья Аркадьевна, Колбанев Михаил Олегович, Цехановский Владислав Владимирович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
emails: verzun.n@unecon.ru, mokolbanev@mail.ru, vvcehanovsky@mail.ru

***Аннотация*:** В статье предлагается обобщенная модель деятельности в условиях цифрового общества, основанная на процедурах преобразования объектов разной природы в цифровую форму (или модель) и обратно, которые стали возможны благодаря достижениям в области информационных технологий. Излагаются признаки общества, которые позволят реализовать рассматриваемую модель на практике. Рассматриваются примеры реализации предложенной модели.

***Ключевые слова**: цифровое общество; обобщенная модель деятельности; цифровая модель объекта; информационные технологии; трансформация деятельности; аддитивное производство; цифровое земледелие.*

EXAMPLES OF IMPLEMENTATION OF THE GENERALIZED MODEL ACTIVITIES IN A DIGITAL SOCIETY

Verzun Natalya, Kolbanev Mikhail, Cehanovsky Vladislav
The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
emails: verzun.n@unecon.ru, mokolbanev@mail.ru, vvcehanovsky@mail.ru

Abstract: The article proposes a generalized model of activities in a digital society, based on the procedures of transformation of objects of different nature into digital form (or model) and back, made possible by advances in information technology. Outlines the characteristics of companies that will help you implement the model in practice. Examples of implementation of the proposed model.

***Keywords:** digital society; a generalized activity model; product model; information technology; transformation activities; additive manufacturing; digital agriculture.*

Введение. Информационное общество достигло очередного этапа развития – стало цифровым, т.е. обществом в котором деятельность реализуется через цифровое представление объектов [1, 2]. В статье авторами предлагается обобщенная модель деятельности в условиях цифрового общества, а также представлены примеры возможной реализации обобщенной модели деятельности на практике.

На рис. 1 представлена модель деятельности в условиях цифрового общества. Процедуры преобразования объектов разной природы в цифровую форму (цифровую модель) и обратно стали возможны благодаря достижениям в области цифровой информационной технологии и могут использоваться и уже используются, практически, в любых областях деятельности людей [3, 4].

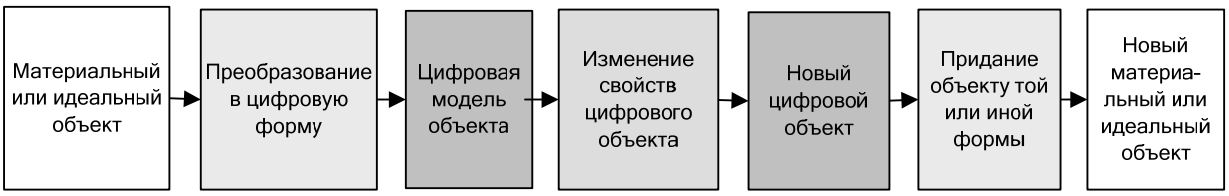


Рис. 1. Обобщенная модель деятельности в цифровом обществе

В общем случае реализация обобщенной модели деятельности на практике предполагает, что общество обладает рядом признаков:

- опора на цифровые информационные технологии;
- сетевая архитектура и цифровая коммуникация [5-7];
- цифровая форма представления объектов деятельности;
- виртуализация цифровых технологий работы с объектами;
- ориентация на знания, представленные в цифровом виде;
- инновационная движущая сила развития [8];
- интеграция и глобализация за счет стандартизированной формы цифровых объектов;
- конвергенция и высокая динамика изменений;
- трансформация всех видов деятельности и др.

На рис.2 представлен пример возможной реализации обобщенной модели деятельности на практике: аддитивное производство (additive manufacturing) [3].

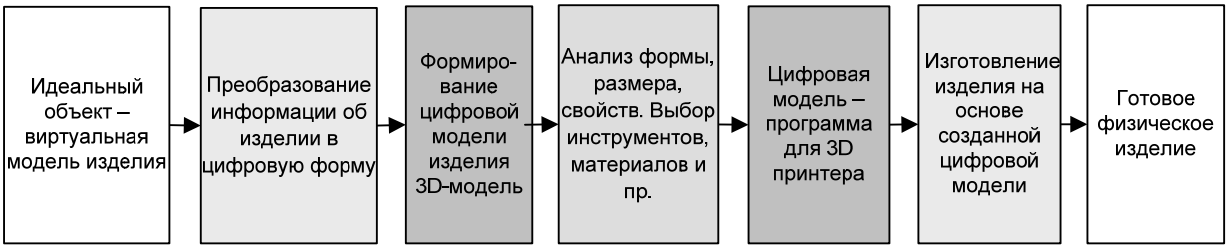


Рис. 2.. Пример реализации обобщенной модели – аддитивное производство

Аддитивное производство (additive manufacturing) – это производство, основанное на технологиях 3D печати. Оно позволяет материализовать заданную 3D модель в готовом изделии таким образом, что это изделие без дополнительных операций можно использовать по назначению. Возможности развития таких технологий производства безграничны: синтез продуктов с заданным количеством белков, жиров и углеводов или других компонентов, печать деталей любой сложности, например, оружие, ракетные двигатели, роботы и др., печать домов, пищевое производство, печать протезов, печать имплантатов и все, что угодно.

3D заводы уже сегодня готовы дистанционно получать широкий спектр трехмерных моделей и материализовать их в изделии любой сложности, при этом стоимость и время изготовления будет значительно ниже, чем существующее аналогичное традиционное производство.

Этапы деятельности при аддитивном производстве показаны на рис. 2.

Идеальным объектом, в данном случае, является модель, замысел, описание изделия в какой-либо аналоговой форме, а также требования к его физическим, механическим и/или химическим характеристикам (свойствам) – все это вместе образует виртуальную модель будущего изделия.

Осуществляется преобразование исходной информации об изделии в цифровую форму – ввод в соответствующую программу.

Затем идет формирование (генерация) цифровой модели с использованием системы трехмерного автоматизированного проектирования.

На следующем этапе происходит: анализ геометрической формы, размера, требуемых свойств изделия и пр. Далее следует выбор, на основе проведенного анализа, требуемых инструментов, материалов, количества и толщины слоев, метода (типа) технологического процесса, порядка обработки и пр.

Новый цифровой объект – цифровая модель, представляющая всю совокупность операций, требуемых для физического создания изделия – программа для станка (для 3D принтера).

Физическое изготовление изделия на основе созданной цифровой модели.

Результат аддитивного производства – материальный объект – готовое изделие, обладающее всеми требуемыми параметрами.

На рис.3 представлен еще один пример возможной реализации обобщенной модели деятельности на практике: цифровое земледелие (digital agriculture, digital farming) [4].

Рис. 3.. Пример реализации обобщенной модели – цифровое земледелие

Цифровое земледелие (digital agriculture, digital farming) предусматривает внедрение в деятельность по выращиванию сельскохозяйственной растениеводческой продукции совокупности цифровых технологий, технических средств, систем прогнозирования, принятия решений и пр., направленных на управление ростом растений в соответствии с реальной обстановкой на полях и потребностями выращиваемых в данном месте культур. Цифровое земледелие ориентировано на получение максимального урожая при минимизации затрачиваемых человеческих и других ресурсов (земли, семян, воды, удобрений, сельскохозяйственной техники, топлива и пр.), что становится возможным благодаря рациональной организации агротехнических мероприятий [9]. Внедрение

цифровых технологий в земледелие в конечном итоге повышает качество сельскохозяйственной продукции, урожайность и прибыль фермера.

Этапы цифрового земледелия приведены на рис.3.

В данном случае исходный объект – материальный – это земля под посадку или уже высаженные в почву сельскохозяйственные культуры. Осуществляется непрерывный мониторинг, сбор (в цифровом виде) и накопление информации об исходном объекте с помощью различных средств инфокоммуникационных технологий: сканирование почвы, слежение за ростом и состоянием растений, за погодными условиями, за сорняками, вредителями и пр. Затем, на основании собранной и накопленной информации, создается (или при необходимости корректируется) цифровая модель объекта – посадок растений.

На следующем этапе идет работа с полученной цифровой моделью – анализируется возможная динамика роста растений, изменения в рельефе и почве, прогноз погодных условий и пр. Исходя из этого осуществляется подбор различных вариантов удобрения, обработки растений и почвы, режимов полива. Создается, на основе различных режимов выращивания растений, прогнозная модель или несколько моделей, показывающих ожидаемый объем и качество выращенных и собранных культур, примерные сроки проведения каких-либо процедур обработки, сбора урожая. Выбирается наилучшая модель, которая в дальнейшем берется за основу при формировании/коррекции плана (регламента) выращивания сельскохозяйственной культуры. На основании разработанного регламента осуществляются агротехнические мероприятия: посадка (сев) растений, уход, полив, освещение, удобрение, обработка. Результат цифрового земледелия – материальный объект – выращенный и собранный урожай.

Заключение. Результатом реализации представленной обобщенной модели на практике будет трансформация всех видов деятельности человека и возникновение цифровой экономики, цифровой политики, цифрового образования, цифровой медицины, цифровой культуры и спорта, цифрового государства, цифрового сельского хозяйства, цифрового транспорта, цифровой безопасности, цифровой энергетики, цифровой экологии и т.д.

СПИСОК ЛИТЕРАТУРЫ

1. Советов Б. Я., Колбанёв М. О., Татарникова Т. М. Информационное общество: современные состояние, проблемы, технологии и перспективы. // Инновации в информационно-аналитических системах. – 2015, – Выпуск 11. – URL: http://iias.ru/index.php/sborniki/vypusk-11.
2. Колбанев М. О., Коршунов И. Л., Левкин И. М. Проблемы информационно-технологической деятельности / Изв. вузов. Приборостроение. – 2017. – Т.60, № 2. – С.105–109.
3. Гибсон Я., Розен Д., Стакер Б. Технологии аддитивного производства. Трехмерная печать, быстрое прототипирование и прямое цифровое производство. М.:Техносфера, 2016. – 656 с.
4. Шаяхметов М. Р., Дубровин И. А. Точное земледелие (precision agriculture) – путь к ресурсосбережению // ОНВ. 2013. №1 (118). URL: http://cyberleninka.ru/article/n/tochnoe-zemledelie-precision-agriculture-put-k-resursosberezheniyu.
5. Верзун Н. А., Касаткин В. В., Колбанёв М. О. Цифровые технологии: инфокоммуникации и экономика // Сборник: Информационные технологии цифровой экономики: сб. статей. – СПб.: Изд-во СПбГЭУ, 2017. С.29–34.
6. Верзун Н. А., Колбанев М. О., Татарникова Т. М. Технологическая платформа четвертой промышленной революции / Геополитика и безопасность. – 2016. – № 2 (34). – С.73–78.
7. Юдина Т. Н. Осмысление цифровой экономики. Теоретическая экономика, №3, 2016. – С.12–16.
8. Левкин И. М., Ковалев А. П., Морозова Е. Ю. Пути совершенствования информационного обеспечения инновационной деятельности предприятия / Управленческое консультирование 2016, № 5. С.112–120.
9. Махотлова М. Ш. Технологии и основные направления точного земледелия // Символ науки. 2016. №1-3. – С.51-53.

УДК 364

ДИСТАНЦИОННОЕ ОБУЧЕНИЕ КАК ОПЕРАЦИОННО-ДИДАКТИЧЕСКАЯ ФОРМА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ПЕДАГОГИЧЕСКИХ КАДРОВ В СИСТЕМЕ НЕПРЕРЫВНОГО ОБРАЗОВАНИЯ ВЗРОСЛЫХ

Каткова Ирина Васильевна, Цесаренко Ольга Петровна
Смольный институт Российской академии образования
Россия, Санкт-Петербург, Полюстровский проспект, д.59
email: avtofakultet@mail.ru

***Аннотация*:** В статье рассмотрена операционно-дидактическая форма повышения квалификации педагогических кадров в системе непрерывного образования взрослых.

Ключевые слова: *непрерывное образование, операционно-дидактическая форма, дистанционное образование, образовательные технологии.*

DISTANCE EDUCATION AS OPERATIONALLY DIDACTIC FORM OF PROFESSIONAL DEVELOPMENT OF PEDAGOGICAL STAFF IN CONTINUING EDUCATION ADULTS

Katkova Irina, Cecarenko Olga
Smolny Institute of the Russian Academy of education
Russia, St. Petersburg, Polyustrovskiy Prospekt, 59
email: avtofakultet@mail.ru

Abstract: The article considers operational and didactic form of professional development of pedagogical staff in continuing education of adults.

Keywords: continuous education, operational-didactic form, distance education, educational technology

Введение. Потребность учиться в течение всей жизни вызвана прежде всего быстрыми изменениями в социально-экономическом развитии, техническом оснащении производства, быстрым старением знаний. Интенсивный рост потока информации через каждые 5-10 лет обусловливает необходимость обновления знаний, чтобы соответствовать актуальным требованиям жизни. Проведенные за рубежом исследования показывают, что даже лучшие высшие учебные заведения не считают, что они выпускают специалистов, образование которых уже завершено. Таким образом, Образовательная система в информационном обществе должна стать системой опережающей. Переход от консервативной образовательной системы к опережающей должен базироваться на опережающем формировании информационного пространства Российского образования.

Отметим, что в связи с переходом индустриальных и постиндустриальных стран к информационному обществу образование, и прежде образование взрослых, становится объективной, реальной потребностью большинства, носит всеобъемлющий характер. Для нашего исследования важное значение имеют научные труды, в которых изложены идеи непрерывности образования в соответствии с потребностями человека (С. Батышев, А. Беляева, Н. Кузьмина, В. Леднев, Н. Ничкало, В. Онушкин и др.). Образование взрослых не может рассматриваться обособленно, поскольку оно является общей составляющей системы непрерывного образования и осуществляется в течение всей жизни, включая все области знаний, используя максимальные возможности для развития личности, получения новой или повышения существующей квалификации, участия в социально-экономической жизни общества. Процессы образования, в которых принимают участие дети, молодежь, взрослые, рассматриваются как единое целое. Человек учится постоянно, без относительно длинных перерывов или в образовательных учреждениях, или средствами самообразования. Он включен в образовательный процесс на всех стадиях его развития с учетом наследственности при переходе с одной ступени к другой [1].

Одновременно можно выделить некоторые принципы, на которых базируется дистанционное образование взрослых: учет личностных качеств (возраст, семейное положение, профессиональный и социальный статус, физическое и психологическое состояние здоровья и другие факторы); использования практического и жизненного опыта, ведь благодаря ему, взрослые являются носителями новых знаний, умений, культуры, это способствует тому, что одновременно они учатся сами и обучают других;признание того, что в определенной ситуации или на определенном периоде образование взрослых может играть компенсирующую роль, оно не предназначено для замены соответствующего образования молодежи, что в свою очередь является успешной предпосылкой образования взрослых. Независимо от форм организации дистанционное обучение – это особая, завершенная форма, имеющая элементы наглядного, наглядно-заочного, заочного и вечернего обучения на основе информационных технологий и систем мультимедиа. Комплекс образовательных услуг, предоставляемых с помощью специализированной информационно-образовательной среды на любом расстоянии от образовательных учреждений, определяет дистанционное образование как одну из форм непрерывного образования, образования «на протяжении жизни».

Характерными чертами дистанционного образования является гибкость, модульность, экономичность, технологичность, социальное равенство, интернациональность, новая роль преподавателя, качество и др. Роль преподавателя в дистанционном образовании расширяет и обновляет роль преподавателя, делает его наставником-консультантом, который должен координировать познавательный процесс, постоянно совершенствовать те курсы, которые он преподает, повышать творческую активность и квалификацию в соответствии с нововведениями и инновациями. На преподавателя возлагается новая роль. Он координирует процесс обучения на основе видоизмененного курса, проводит консультации при составлении индивидуального учебного плана, руководит учебными проектами, направляет обучение групп взаимоподдержки, помогает слушателям, в их профессиональном самоопределении. На основе анализа отечественной и зарубежной теории и практики организации повышения квалификации педагогических кадров показано, что этим требованиям может удовлетворять операционно-дидактическая система, выстроенная как форма, в которой должны быть воплощены особенные принципы непрерывного образования. Непрерывное образование – процесс и принцип формирования личности, предусматривающий создание таких систем образования, которые открыты для людей любого возраста и поколения и сопровождают человека в течение всей его жизни, способствуют постоянному его развитию, вовлекают в непрерывный процесс овладения знаниями, умениями, навыками и способами поведения (общения). Операционно-дидактическая форма - упорядоченный набор целей, содержания, форм, методов и средств обучения.

Основу процесса обучения как дидактической системы составляет учебная деятельность. Учебная деятельность выполняется человеком на протяжении всей его жизни. Дистанционное

образование - это организационная форма, при которой коммуникация между обучающимся и обучающим осуществляется по преимуществу опосредованно на расстоянии на основе использования самых разнообразных средств. Образовательные технологии - это внедрение основных направлений педагогической стратегии, которая достигается программой и стандартом образования целей по конкретному учебному предмету. В государственной стратегии развития России важнейшими целями модернизации образования признаются: развитие интеллектуального потенциала личности, аналитических способностей, критического мышления, которое достигается в системе непрерывного образования. Развитие умений самоанализа и осознания собственных возможностей, постоянное пробуждение творческих способностей, инициативы, развитие коммуникабельности и выработка способности оперативно и эффективно решать возникающие проблемы, позволяет опережающему образованию, включить в себя операционно-дидактические формы. Такое образование является важнейшим методологическим принципом дальнейшего развития профессионального образования, требующим пересмотра сложившихся стереотипов.

Основная цель профессионального образования взрослого человека – профессиональное развитие личности. Опережающее обучение – осуществляется на основе прогнозирования научно-технического развития общества и условий труда, ориентации полученных знаний и умений и одновременно развитие потенциала компетентности специалиста. Основные принципы опережающего образования – развитие адаптивности, мобильности, конструктивности субъективной ориентации, личностная обусловленность выбора форм образования, интегративность и расширение спектра видов деятельности; контекстность образования, направленного на креативность как развитие способности к самоизменению, самоопределению, преодолению традиционного взгляда. Одной из основных функций опережающего образования является компетентностная функция, предполагающая развитие целостного решения проблем в познании методом операционно-дидактической формы повышения квалификации педагогических кадров. Для системы дидактической подготовки специалистов дошкольных учреждений в вузе характерна полифункциональность, выражающаяся во взаимозависимости в ее образовательной, воспитательной, развивающей, координирующей и интегрирующей функций. Их выделение условно, поскольку грани между обучением, воспитанием и развитием личности студента, а также интеграционными и координационными процессами в подготовке специалиста относительны [2]. Условная дифференциация функций дидактической подготовки необходима в целях эффективности теоретического анализа ее сущности и целесообразна для организации процесса обучения. Образовательная функция дидактической подготовки выражает ее направленность на овладение студентами фундаментальным знанием основ дидактической теории и формирование у них системы дидактических умений и навыков.

Теоретические и практические аспекты реализации образовательной функции дидактической подготовки предполагают изучение теории в контексте профессиональной деятельности будущих специалистов, что обеспечивает овладение студентами содержательно-процессуальными и организационно-методическими основами деятельности педагога дошкольного учреждения по обучению детей. Воспитательная функция дидактической подготовки отражает ее позитивное влияние на формирование профессионально-значимых качеств личности, ее ценностно-нормативной системы, мотивов учебной и будущей профессиональной деятельности. В процессе овладения дидактической теорией и соответствующими умениями у студентов формируется ценностное отношение к дидактике как отрасли педагогической науки, потребность в обогащении системы дидактических умений и навыков, интерес, ответственное и творческое отношение к педагогической деятельности и процессу дидактической подготовки к ней, осознание себя ее субъектом. В ходе дидактической подготовки, осуществляемой в контексте профессиональной деятельности, будущий специалист усваивает не только нормы компетентных предметных действий, но и нормы социальных поступков, отражающих ее ценностно-нормативную систему, ибо, как образно заметил А.А. Вербицкий, "специалист не воспитывается в социально стерильной учебной "пробирке..." [3]. Если предметное содержание будущей профессиональной деятельности обеспечивается материалом учебной дисциплины "Дидактика", то социальное "втягивается" в учебный процесс лишь при оптимальной организации индивидуальной, парной, групповой и коллективной форм деятельности студентов при ведущей роли коллективной.

Развивающая функция дидактической подготовки заключается в том, что овладение дидактическими знаниями и умениями органично связано с развитием профессионального мышления, речи, педагогических способностей, позволяющих специалисту осуществлять творческий подход к организации образовательного процесса в дошкольном учреждении. Координирующая функция дидактической подготовки связана с ее направляющим влиянием на предстоящий процесс изучения студентами курсов дошкольной педагогики и частных методик, а также спецкурсов и спецсеминаров. Особая роль данной функции прослеживается при сравнительном анализе учебно-воспитательного процесса на разных факультетах педагогического вуза. На большинстве факультетов курсы методик вооружают студентов знанием задач, принципов, содержания, форм и методов обучения по двум-трем определенным учебным предметам, в то время как на факультетах и отделениях педагогики и методики дошкольного образования изучаются пять-десять методик. Кроме того, изучаемые в вузе

будущими педагогами дошкольных учреждений методики отличаются большей внутренней спецификой, нежели курсы методик в учебных планах других факультетов. Следовательно, дидактическая подготовка будущего педагога является необходимым фундаментом всей его дальнейшей профессиональной подготовки. С реализацией координирующей роли дидактической подготовки связана ее интегрирующая функция. Обе функции обусловлены необходимостью междисциплинарного подхода к решению будущим специалистом дидактических проблем. Интегрирующая функция дидактической подготовки заключается в том, что процесс овладения дидактической теорией актуализирует, динамизирует, систематизирует и наполняет новым содержанием знания студентов, полученные ими при изучении курсов философии, социологии, психологии, теории воспитания и др. При этом, если координирующая функция дидактической подготовки студентов предполагает ее антиципирующее (предвосхищающее) влияние на предстоящие процессы, то в основе интегрирующей функции лежат рефлексия и аккумуляция достижений предшествующих и актуального этапов развития мотивационно-потребностной и операционно-действенной сфер личности. Реализация всех функций дидактической подготовки педагога осуществляется в ходе овладения студентами определенным содержанием.

Научно обоснованный отбор содержания дидактической подготовки является одним из основных условий продуктивности поисков ее оптимизации. Содержательный компонент дидактической подготовки представляет собой относительно самостоятельную область содержания педагогического образования, усвоение которой создает условия для овладения личностью дидактическими аспектами педагогической деятельности. Как известно, содержание образования формируется на трех уровнях: общего теоретического представления, учебного предмета и учебного материала [4]. Содержанием дидактической подготовки в нашей модели выступает педагогически адаптированная система дидактических знаний, способов педагогической деятельности, опыта ее творческого осуществления и ценностно-эмоциональных отношений, усвоение которой обеспечивает формирование дидактической культуры будущего специалиста. Содержанием дидактической подготовки, рассматриваемой в контексте профессионально-педагогической деятельности, является адаптированное с учетом семиотических и психолого-дидактических требований содержание дидактики как научной дисциплины, детерминированное спецификой профессиональной деятельности специалиста дошкольного учреждения. Отбор содержания дидактической подготовки структурируется в логике развертывания учебного предмета "Дидактика" как предмета учебной, квазипрофессиональной (профессионально-подобной) и учебно-профессиональной деятельности. При этом требования со стороны будущей профессиональной деятельности являются системообразующими. В этом случае усвоение дидактических знаний осуществляется в контексте той деятельности, ориентировочной основой и средством регуляции которой они призваны выступать.

Основной единицей содержания дидактической подготовки в контексте профессиональной деятельности выступает педагогическая ситуация "во всей ее предметной и социальной неоднозначности и противоречивости" [5]. Формирование дидактической готовности педагога дошкольного образования требует включения учебной деятельности студентов в аналог будущего профессионального труда, представленный различными формами квазипрофессиональной деятельности. Моделирование содержания и динамики осваиваемой студентами профессионально-педагогической деятельности осуществляется посредством технологии контекстного обучения. Дидактическая подготовка с использованием форм и методов контекстного обучения характеризуется тем, что усвоение абстрактных по своей сути дидактических знаний "наложено на канву" профессионально-педагогической деятельности, что обеспечивает студенту их осмысление и усвоение как средства ее осуществления и регуляции.

Сущность контекстного обучения применительно к условиям дидактической подготовки педагога дошкольного образования состоит в деятельностной реконструкции профессиональной деятельности в ее предметном и социальном аспектах. Модель целостного содержания профессионально-педагогической деятельности представлена в контекстном обучении системой профессиональных проблем, задач и функций, которые получают свое отражение в совокупности учебных, квазипрофессиональных и учебно-профессиональных заданий. Создаваемые в учебном процессе модели выступают средством познания студентами оригинала - осваиваемой профессионально-педагогической деятельности - ее содержания, динамики, организационных форм, ценностей и норм, предметных задач. Совокупность дидактических задач, организационных форм и методов профессиональной деятельности специалистов, а также ситуаций их социально-психологического взаимодействия, регулируемого ценностно-нормативной системой педагогической деятельности, и составляет профессиональный контекст дидактической подготовки педагога дошкольного образования. Дидактическая подготовка педагогических кадров дошкольных учреждений осуществляется в целенаправленно моделируемой профессиональной среде на протяжении всего периода обучения в вузе и носит динамичный характер. Этот процесс представляет собой последовательность пропедевтического, ориентационно-теоретического, формирующего и преобразующего этапов, каждый из которых сопровождается целесообразным воздействием на мотивационно-потребностную сферу личности будущего специалиста. Деление целостного процесса

дидактической подготовки педагога дошкольного образования на последовательные этапы условно, поскольку формирование дидактических умений будущего специалиста неизбежно сопровождается качественными преобразованиями системы его дидактических знаний и способствует становлению представлений о сущности дидактической подготовки, а достижение необходимого уровня усвоения дидактических знаний требует их применения в практической педагогической деятельности.

Каждому этапу дидактической подготовки соответствует определенная базовая форма организации деятельности студентов: учебная деятельность академического типа, квазипрофессиональная или учебно-профессиональная. Их последовательная трансформация и составляет основное содержание технологического компонента дидактической подготовки. Проектирование дидактической подготовки студентов в контексте их будущей профессиональной деятельности требует конкретизации желаемых результатов этого процесса. Результативный компонент дидактической подготовки педагога дошкольного образования представляют взаимосвязанные аспекты дидактической готовности специалиста. Дидактическую готовность педагога дошкольного образования составляет обусловленная необходимым уровнем его дидактической культуры способность к продуктивному дидактическому взаимодействию с детьми.

Решаемым в ходе дидактической подготовки задачам соответствуют когнитивный, деятельностный, креативный и эмоционально-волевой аспекты дидактической готовности специалиста. Дидактическая подготовка студентов, осуществляемая на основе представленной структурно-функциональной модели, призвана обеспечить повышение функциональной грамотности молодых специалистов в осуществлении дидактического взаимодействия с детьми дошкольного возраста.

Заключение. Разработано методическое обеспечение реализации модели и проведена ее опытно-экспериментальная проверка. Этапы предпринятого исследования будут конкретизированы в последующих публикациях.

СПИСОК ЛИТЕРАТУРЫ:

1. Лапчик М.П. Подготовка педагогических кадров в условиях информатизации образования учебное пособие/ Лапчик М.П..— М.: БИНОМ. Лаборатория знаний, 2013.— 182 с.
2. Грязнова Е.Д. Дистанционное обучение как средство педагогического воздействия в процессе профессиональной подготовки работников таможенных органов фия/ Грязнова Е.Д.— Владивосток: Владивостокский филиал Российской таможенной академии, 2011.— 160 с.
3. Абдуллина О.А. Общепедагогическая подготовка учителя в системе высшего педагогического образования. М.: Просвещение, 1990. 141 с.
4. Борисова Н.В. Педагогические особенности создания и внедрения системы активных методов обучения в институте повышения квалификации: Дис. ...канд. пед. наук. М, 1987. 334с.
5. Вербицкий А.А. Активное обучение в высшей школе: контекстный подход. М.: Высшая школа, 1991. 207 с.

УДК 37.072

СОЗДАНИЕ СОВРЕМЕННОЙ ЛАБОРАТОРНОЙ БАЗЫ ДЛЯ ПОВЫШЕНИЯ КАЧЕСТВА ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СООТВЕТСТВИИ С ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ В СФЕРЕ ОБРАЗОВАНИЯ

Соколов Сергей Сергеевич
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Россия, Санкт-Петербург, ул. Двинская, д. 5/7
email: sokolovss@gumrf.ru

***Аннотация*:** В статье рассмотрен опыт создания в Государственном университете морского и речного флота имени адмирала С.О. Макарова современной лаборатории «Технических средств и систем в защищенном исполнении» - целевой аудитории ПАО «Газпром», как пример эффективного взаимодействия с работодателем с целью повышения качества подготовки специалистов в области информационной безопасности.

***Ключевые слова**: качество подготовки; современные технические средства; методы обучения.*

THE CREATION OF MODERN LABORATORY BASE FOR IMPROVEMENT OF QUALITY OF TRAINING IN THE FIELD OF INFORMATION SECURITY ACCORDING TO THE CURRENT LEGISLATION IN EDUCATION

Sokolov Sergey Sergeevich
“Admiral Makarov SUMIS”,
Russia, St. Petersburg, Dvinskaya str, 5/7
email: sokolovss@gumrf.ru

***Abstract*:** In this article experience of creation in the Admiral Makarov SUMIS of modern "Technical means and systems in the protected execution" laboratory - target audience of Gazprom as an example of

effective interaction with the employer for the purpose of quality improvement of specialists education in the field of information security is considered.

***Keywords**: quality of education; modern technical means; training methods.*

Введение. Высшие учебные заведения все чаще сталкиваются с противоречием: с одной стороны – увеличивающиеся требования, закрепленные в соответствующих законодательных актов и касающиеся повышения качества образовательного процесса путем обновления лабораторной базы и использования инновационных методов организации и проведения образовательного процесса, с другой – недостаточность финансирования, устаревание материальной базы, на обновление которой собственных средств ВУЗа зачастую не хватает.

В соответствии с ФГОС ВО 10.03.01 «Информационная безопасность» (уровень бакалавриата): «7.3.1. … минимально необходимый для реализации программ бакалавриата перечень материально-технического обеспечения должен включать в себя лаборатории в области: …технической защиты информации, оснащенную специализированным оборудованием по защите информации от утечки по акустическому каналу…», аналогичные, на взгляд автора, более мягкие требования содержатся и по уровням: специалитет и магистратура. [1, 2, 3]

В виду большей ориентации современного контингента обучающихся в сторону Интернет-технологий, веяния времени и законодательные предпосылки все больше ставят перед нами задачи внедрения современных методов электронного (уже как обязательное) и дистанционного (пока лишь как рекомендуемое) обучения – это можно в явном виде прочитать в требованиях к функционированию электронной информационно-образовательной среды. [1, 2, 3, 4, 5, 6]

Эти две предпосылки мы имеем с одной стороны, с другой – мы понимаем, что имеющееся финансирование с учетом устаревания материальной базы, необходимостью выполнения дородных карт (в т.ч. показателей, влияющих на сокращение учебно-вспомогательного персонала) явно недостаточно для выполнения требований и чтобы успеть или даже опередить время необходимы иные подходы.

Такими подходами могут являться: выполнение НИР и НИОКР в рассматриваемой области с целью получения дополнительного финансирования для обновления материальной базы; взаимодействие с работодателями с целью получения спонсорской помощи.

Первый подход не является предметом данной статьи и может быть рассмотрен отдельно. Второй подход тоже имеет свои особенности: спонсорские средства, выданные без целевого назначения быстро и «тонким слоем» можно распределить на массу нужд, в тоже время, финансирование конкретного проекта – видна большая, четко понятная цель, на которую средства возможно получить с большей долей вероятности (проектно-целевой подход – одна из основ современной экономики).

По этому пути пошли в Государственном университете морского и речного флота имени адмирала С.О. Макарова и обратились в ПАО «Газпром» с предложением (на что и было полученное соответствующее финансирование) выделения средств для создания многофункциональной специализированной аудитории: Целевая аудитория ПАО «Газпром», Лаборатория «Технических средств и систем в защищенном исполнении».

Многофункциональность аудитории заключается в следующем назначении: специализированная аудитория для подготовки по УГС «Информационная безопасность», оснащенная современной методической базой, компьютерной техникой и специализированным оборудованием для закладки и обнаружения закладных устройств с целью предотвращения утечки по основным рассматриваемым каналам передачи; площадка для проведения дистанционных занятий и консультаций как удаленно доступными преподавателями, так и со стороны головного ВУЗа для сети филиалов (на данный момент их у университета 10); проведение научных исследований; площадка для проведения семинаров, конференций и встреч с коллегами из учебных, научных заведений и с представителями ПАО «Газпром».

В ГУМРФ имени адмирала С.О. Макарова есть традиция по именованию таких крупных аудиторий в честь ученых, педагогов, вложивших наибольший вклад в развитие ВУЗа. Представленная аудитория решением руководства ВУЗа будет носить имя одного из основателей и первых участников северо-западного УМО по информационной безопасности, основателя диссертационного совета университета, заведующего кафедрой, научного руководителя множества докторов и десятков кандидатов наук – д.т.н., профессора Гаскарова Диляура Вагизовича.

Заключение. Очень часто мы стали вспоминать слова: «Новое – это хорошо забытое старое». Кооперация и совместные действия между ВУЗами и отраслевыми организациями – это успешно перенесенный в современную Россию опыт, который одно время не использовался, но сейчас, когда мы находимся в начале шестого технологического уклада, этот опыт важен и нужен, только совместно можно двигаться вперед.

СПИСОК ЛИТЕРАТУРЫ

1. ФГОС ВО 10.03.01 «Информационная безопасность» (уровень бакалавриата).
2. ФГОС ВО 10.03.01 «Информационная безопасность автоматизированных систем» (уровень специалитета).

3. ФГОС ВО 10.04.01 «Информационная безопасность» (уровень магистратуры).
4. Пастущак Т.Н. Приоритетные направления развития электронной информационно-образовательной среды отраслевого университетского комплекса / Пастущак Т.Н., Соколов С.С., Ковальногова Н.М., Маньковская А.В. // Информационные технологии. 2014. № 9. С. 40-46.
5. Соколов С.С. Электронная информационно-образовательная среда современного университетского комплекса / Соколов С.С., Ковальногова Н.М. // В сборнике: Морское образование: традиции, реалии и перспективы материалы научно-практической конференции. 2015. С. 157-163.
6. Пастущак Т.Н. Приоритетные направления применения электронного обучения и дистанционных образовательных технологий университетского комплекса / Пастущак Т.Н., Соколов С.С., Ковальногова Н.М., Маньковская А.В. // В сборнике: Актуальные проблемы экономики и управления на водном транспорте Материалы научно-практической конференции, посвященная 75-летию со дня рождения профессора А.С. Бутова. 2014. С. 214-224.

УДК 004.056:007.51

МЕТОДЫ ЗАЩИТЫ ОТ АТАК МЕТОДАМИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Солодянников Александр Владимирович[1], Сухостат Валентина Васильва[2],
Антонова Любовь Сергеевна[3]
[1,3] ООО «Ассоциация специалистов по безопасности»,
Россия, 194100, Санкт-Петербург, ул.Катмировская, д.7
[2] Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Россия, 197101, Санкт-Петербург, Кронверкский проспект, д.49,
emails: solod000@yandex.ru, sukhostat@mail.ru, antonova.ls@mail.ru

Аннотация: Специфичность целенаправленных атак на оператора методами социальной инженерии требует усиленного внимания к обеспечению информационной безопасности (ИБ) современной организации. В статье рассмотрены методы защиты от нетехнических угроз для ИБ и развития компетентности сотрудников противостоять опасностям социальной инженерии.

Ключевые слова: *социальная инженерия, информационная безопасность, тестирование на проникновение, обучение сотрудников.*

METHODS OF PROTECTION FROM ATTACKS BY METHODS OF SOCIAL ENGINEERING

Solodyannikov Alexander[1], Sukhostat Valentina[2], Antonova Liubov[3]
[1,3] "Association of security professionals" LLC,
Russia, 194100, St. Petersburg, Kantemirovskaya st., 7,
[2] Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics
Russia, 197101, St. Petersburg, Kronverkskiy pr., 49,
emails: solod000@yandex.ru, sukhostat@mail.ru, antonova.ls@mail.ru

Abstract: Specificity of purposeful attacks on the operator by methods of social engineering requires increased attention to the information security (IS) of a modern organization. The methods of protection from non-technical threats for IS and development of competence of employee to resist the dangers of social engineering are considered in the article.

Keywords: *social engineering, information security, penetration testing, employee training.*

Введение. Социальные инженеры могут нанести серьезный ущерб своим жертвам, в том числе и современной организации. Урон может быть социальным, экономическим или репутационным. Важно своевременно организовывать соответствующую политику безопасности, чтобы предотвратить растраты, которые могут быть потенциально вызваны в результате целенаправленных атак методами социальной инженерии. Анализ состояния изучения влияния человеческого фактора в обеспечении ИБ показывает, что человек-оператор представляет собой один из основных объектов информационной системы, где оператор и его деятельность выступают и в качестве неотъемлемого компонента самой человеко-машинной системы, и необходимого условия ее бесперебойного и эффективного функционирования. При этом сами операторы подвержены угрозам не в меньшей степени, чем информация, циркулирующая в системе, или программно-технические средства [1]. В данной статье описываются общие стратегии ослабления и нейтрализации методов несанкционированного доступа к информационной инфраструктуре предприятия на основе слабостей человеческого фактора.

Меры физической безопасности. Для серьезного бизнеса интенсивная физическая безопасность должна обеспечиваться во всей организации без исключения. В первую очередь, разработанные и внедренные четкие и сжатые политики безопасности требуют периодической проверки, чтобы определить состояние информирования о безопасности среди сотрудников. Это необходимо для выявления и устранения любых потенциальных недостатков. При этом, важно, чтобы сотрудникам постоянно напоминали, что возможность реализации угрозы реальна; это может произойти в любое время без предупреждения. Комментируя эту проблему, Кевин Митник утверждает, что люди обычно не ожидают, что их будут обманывать и кто-то будет манипулировать ими, поэтому они попадают под атаки социальной инженерии [2].

Хорошая практика – размещать во всех помещениях напоминания сотрудникам компании о том, что найденные в помещениях какие-либо USB-накопители или любое другое цифровое устройство, не стоит подключать. Такого вида устройства должны быть представлены в соответствующий отдел для экспертного анализа. Кроме того, сотрудники обязаны проявлять бдительность и сообщать о любых подозрительных действиях в отношении безопасности, независимо от того, насколько незначительным это может показаться на первый взгляд.

Физическая безопасность может быть обеспечена всеобъемлющим охватом систем видеонаблюдения в сочетании с четко определенным периметром контролируемой зоны. Установка защитных физических барьеров, сигнализаций, систем обнаружения движения и использование биометрических данных для идентификации сотрудников может значительно помочь защитить бизнес от потенциальной атаки. Однако без реализации строгих протоколов физической безопасности доступ злоумышленников к ценным ресурсам компании будет открыт.

Применение программных средств. Еще один логический шаг, который следует предпринять в борьбе с социальной инженерией, это развертывание ряда защитных программных средств. Следует отметить, что использование программных средств, с одной стороны, может быть эффективным в борьбе с некоторыми типами атак социальной инженерии, с другой, – они могут оказаться совершенно бесполезными при других видах атак. Например, надежный защитник от спама с обновленным «черным списком», дополняемый антивирусной программой и брандмауэром, может защитить компанию от фишинговых атак.

С учетом сказанного, эти меры окажутся недостаточными против физических приманок или "хвостов" (несанкционированного прохода одновременно с законным пользователем). Отсюда не следует, что предприятия не должны инвестировать средства в механизмы программно-аппаратной защиты информационных активов. Так, чтобы исключить некоторые из перечисленных рисков, использование механизмов песочницы может быть очень продуктивным [3]. Песочница – это специально выделенная изолированная виртуальная машина, использование которой защитит сеть от распространения вредоносных программ. Но они имеют тенденцию распространяться по всему домену во время непреднамеренного подключения оператором скомпрометированного USB-накопителя к своему компьютеру. Использование песочницы против некоторых атак визуального обмана настолько эффективны, что некоторые популярные браузеры [Chromium [4], Firefox [5]) построили технологии песочницы, чтобы предотвратить эксплуатацию через интернет-браузеры.

Специальные меры по предотвращению нападений, использующих технологии социальной инженерии. Другие специальные меры могут оказаться очень эффективной стратегией предотвращения атак методами социальной инженерии. Такие меры включают:

- активный мониторинг;
- агрессивную аутентификацию и учет пользователей;
- использование целевых алгоритмов машинного обучения и анализа.

После наблюдения нормального поведения системы, допустимо ее самообучение на способность различать законные и незаконные действия пользователя, несоответствие данных. Системы машинного и поведенческого обучения, в частности, стали настолько эффективными, что они способны обнаруживать и останавливать сложные атаки социальной инженерии, такие как целевой фишинг.

Описанные выше механизмы внутренней безопасности, а также многие другие решения безопасности могут служить мощным щитом, который может использоваться для защиты предприятий от атак социальной инженерии. После внедрения эти решения могут потребовать непрерывного ручного мониторинга. Примером этого может быть ежедневный, еженедельный или ежемесячный анализ обнаруженных и заблокированных атак. Компании должны понимать, что социальные инженеры и хакеры посвящают себя поиску эксплойтов, затрачивая на это полный рабочий день и больше. Особенно, если у них есть хорошая мотивация для взлома конкретной компании. Система может блокировать определенное количество попыток, но затем злоумышленник может получить преимущество и найти технический эксплойт, предоставляющий ему нужный доступ. Постоянно анализируя попытки атаки и, соответственно, улучшая инфраструктуру, предприятия могут лучше защитить себя от этих атак.

Из-за постоянно меняющейся динамики в современном ИТ-мире крайне важно, чтобы менеджеры и сотрудники знали о текущих правилах и процедурах безопасности своей компании. Политика безопасности содержит процедуры и рекомендации, которые диктуют методы защиты данных и активов организации. Крайне важно иметь краткий и четко определенный набор правил для максимальной эффективности. Эти правила должны быть доступны всем сотрудникам, независимо от их ранга. При этом политики также должны быть защищены от несанкционированного доступа, который может помочь злоумышленникам получить представление о внутренней работе компании. Отсутствие четкой политики безопасности, по сути, может стать причиной подавляющего несоблюдения правил безопасности сотрудниками, что приведет к успешным нападениям и штрафам со стороны властей.

Внедрение политик безопасности напрямую связано с использованием компьютера на работе. Сотрудник, умышленно получающий доступ к уязвимому сайту или жертва фишинговой атаки поставит

предприятие под угрозу из-за того, что его рабочая станция подключена к корпоративной сети. Усиленной и эффективной политики доступа и авторизации, а также компетентного межсетевого экрана и надежного корпоративного антивируса должно быть достаточно, чтобы противостоять непреднамеренному воздействию и нанесению потенциального вреда ИТ-инфраструктуре компании.

Применение компанией достаточных мер безопасности и уверенность в защите от нападения обусловливают поиск другого мнения об уровне обеспечения информационной безопасности своей организации. Для этого проводится тестирование на проникновение. Основная цель данного теста заключается в определении технических уязвимостей и слабых мест в сети, системах и приложениях, используемых в организации. Помимо тестирования устойчивости цифровых активов компании, многие фирмы наряду с тестированием на проникновение, определяют перспективы безопасности предприимчивых сотрудников. Таким образом, официальный тестировщик-злоумышленник, используя технологии социальной инженерии, пытается получить доступ к системе посредством манипуляций с людьми, прямого взлома или использования других трюков. После завершения симулированной атаки работодателю фирма представляет отчет с подробным описанием выявленных уязвимостей, вероятных причин слабых мест и стратегий исправления.

Проблемы безопасности в современном цифровом мире являются динамичными, сложными и запутанными. Чтобы противостоять атакам киберпреступности компаниям необходимо постоянное тестирование инфраструктуры и сотрудников. Комплексная и всеобъемлющая стратегия, связанная с управлением рисками, кибербезопасностью, поможет предпринимателям пройти долгий путь в защите от опасностей киберпреступности и нападений со стороны социальной инженерии. С помощью автоматизированных технологий можно выявить и устранить существенные пробелы в безопасности.

Стратегии ослабления последствий социальной инженерии. Люди более доступны и эксплуатируемы, чем машины, а потому человеческий фактор в бизнесе остается наиболее уязвимым для злоумышленников, использующих технологии социальной инженерии. Политики надежности паролей, двухфакторные аутентификации для входа в систему, лучшие брандмауэры и системы обнаружения вторжений становятся излишними, если сотрудники не понимают важность поддержания безопасности своих контактов, паролей и карт доступа. Безопасность компании сильна только тогда, когда сильно ее слабое звено, которым в данном случае является сотрудник.

Наиболее эффективной стратегией смягчения последствий в сфере социальной инженерии является образование. С периодическим и систематическим обучением по вопросам безопасности и частым напоминаниям о необходимости оставаться начеку и проявлять бдительность в отношении подозрительного поведения предприятия могут эффективно превратить свое самое слабое звено в самое сильное. При этом, существенно, чтобы сотрудники понимали ценность и защиты конфиденциальной информации, и значимость знаний о методах социальной инженерии. Осведомленность сотрудников обусловливает развитие знания различных векторов атак, умение определять возможность их возникновения, умение различать рассеянную или прямую атаки.

Существенной мерой, обусловливающей защиту организации от нападений, использующих технологии социальной инженерии, является постоянная и системная работа по повышению квалификации сотрудников в области информационной безопасности. Такой подход определен следующим. Согласно исследованию [6] после посещения бизнес-тренинга сотрудники в течение часа забывают 50% информации, в течение 24 часов – 70%, в течение недели – 90%. Подготовительная работа и обучение могут быть интенсивными и дорогостоящими, но это необходимые затраты, которые должны предпринять современные организации для обеспечения информационной безопасности от атак методами социальной инженерии.

Компетентность сотрудников противостоять реализации нетехнических угроз для информационной безопасности организации, по мнению Гвидо Роблинга, очень значима и в этом действительно помогают две вещи: осознание и бдительность [7]. Абсолютная безопасность никогда не может быть гарантирована, но, повышение квалификации сотрудников в вопросах безопасности может способствовать, по сути, превращению сотрудников из обязательств в активы.

По мере расширения возможностей сети интернет результативно расширяется и кругозор любопытствующих. Если раньше людям приходилось прилагать сосредоточенные усилия, чтобы изучить хакинг и социальную инженерию, то теперь, с легко доступным интернетом, полным всевозможной информации, обучение методам эксплуатации стало тривиально. Доступные учебные пособия и наличие специализированных онлайн-сайтов по обучению в области социальной инженерии означают, что свободное время и целеустремленность – это то, что необходимо для овладения искусством социальной инженерии.

Реальные выгоды от обучения сотрудников методам интернет-безопасности бесконечны. Мало того, что компании экономят деньги из-за сокращения нарушений безопасности (в том числе сокращения штрафов), они также будут защищаться от необходимости реагировать на любую негативную прессу и навязчивую проверку со стороны властей, что часто происходит после нарушения. Кроме того, безупречная репутация среди клиентов компании за то, что они компетентны и строги в отношении безопасности, что подтверждается результатами периодических тестов на проникновение, означает, что перспективы роста в клиентуре могут быть бесконечными.

Формы организации и методы повышения квалификации и информирования сотрудников о разнообразных потенциальных угрозах ИБ организации.

Обучение на месте. Такая форма организации обучения заключается в подготовке внутреннего сотрудника (или в приглашении внешнего тренера), который сможет проводить регулярное обучение навыкам безопасности для других сотрудников. Создание условий для обучения на месте состоит в том, что такого рода занятия должны быть недолгими по времени, содержать перерывы для отдыха. Для проведения занятий необходимо использовать простой (без технического жаргона) и понятный каждому обучающемуся язык. А занятия, в свою очередь, должны иметь четкие цели и фокусироваться на выявлении и предотвращении социальной инженерии.

Интранет. Интранет организации может быть применим в реализации программ повышения квалификации и информированности сотрудников. Например, компания может интегрировать курс безопасности, подготовленный локально или извне аккредитованным персоналом, и представить программу как учебное пособие в известном разделе интрасети. При этом, менеджеры должны побуждать работников к пересмотру содержания на регулярной основе, чтобы информация была выгравирована в сознании работников. Интранет также является хорошим средством для распространения уведомлений о безопасности для работников в отношении недавних угроз безопасности, инструкций о том, как справиться с угрозой и кому сообщить об инциденте.

Скринсейверы. Заставки могут играть большую роль в повышении информирования о безопасности среди сотрудников. Они могут использоваться для отображения коротких напоминаний по таким темам, как сохранение пароля в безопасности, запрет на выезд, сообщение о подозрительном поведении соответствующим отделам и т.д. Необходимо использовать для обеспечения ИБ более смелые тексты, крупные шрифты и соответствующие изображения, чтобы контент просматривался и понимался с разумного расстояния.

Плакаты. Вид ярких плакатов с большими шрифтами может быть эффективным для запоминания. Предоставление кратких и целенаправленных сообщений по вопросам безопасности, связанным с бизнесом, может стать эффективной стратегией для повышения информированности сотрудников. Общие напоминания о безопасности на плакатах должны регулярно заменяться, что позволит сотрудникам осознавать несколько сообщений безопасности. Тем не менее, плакаты с более важными и конкретными напоминаниями могут быть размещены в важной части рабочего места на полупостоянной основе.

Онлайн-курсы. Работодатели могут использовать один из многих онлайн-провайдеров для обучения безопасности. Предлагаемая интеграция интрасети и специализированного программного обеспечения в пакете, может быть применена менеджерами для наблюдения развития компетентности сотрудников со своих компьютеров. Многие онлайн-учебные сайты наряду с предоставлением платных курсов, имеют отличные и бесплатные ресурсы, доступные в Интернете. Эти веб-сайты, с одной стороны, могут быть очень эффективными в развитии знаний работника по рискам, связанным с социальной инженерией, с другой, – имеют дополнительное преимущество нулевых затрат для работодателей, что является очень выгодным для компаний, не имеющих достаточных денежных средств.

Наличие разнообразных методов обучения обусловливают повышение информирования о разнообразном характере потенциальных угроз социальной инженерии на предприятии. Следствием является адекватное осознание сотрудниками рисков, создаваемых атакующими. При этом работодатель автоматически получает преимущество в этой битве; у бизнеса меньше шансов пострадать от нападения из-за того, что их обученный персонал проявляет должную осмотрительность, чтобы защитить компанию.

Используя креативность в своих собственных изысканных методах, предприятия могут также инициировать различные поведенческие защитные инстинкты у сотрудников. Отличный способ добиться этого – проводить регулярные сеансы мозгового штурма, чтобы сотрудники могли представлять новые идеи защиты и учиться на опыте друг друга. Однако, реальность заключается в том, что нет абсолютной безопасности. Но, если все оборонительные методы, изложенные в этой статье, будут реализованы с высокой эффективностью, то эти меры обеспечения ИБ значительно усложнят попытки социального инженера проникнуть в компанию.

Заключение. Многоуровневая программа защиты от разнообразного характера потенциальных угроз социальной инженерии для информационной безопасности организации может быть эффективной в силу компетентности сотрудников понимать и признавать общие методы эксплуатации, используемые социальными инженерами. Поэтому современные организации должны тратить свое время и силы, чтобы убедиться, что их сотрудники действительно понимают угрозу социальной инженерии, предпринимая превентивные меры.

СПИСОК ЛИТЕРАТУРЫ

1. Гатчин Ю.А. Методика оценки защищенности оператора информационных систем в условиях диструктивных информационных воздействий / Ю.А. Гатчин, В.И. Поляков, В.В. Сухостат, Н.В. Малков // Вестник компьютерных и информационных технологий. 2015. №2 (128). С. 54-59.
2. Митник К. Искусство вторжения: Пер. с англ. — Семенова А.В. — М.: Компания АйТи, ДМК Пресс, 2005. — 280 стр.

3. Салем М., Хаммуде М. Defense Methods Against Social Engineering Attacks [Электронный ресурс] URL: https://www.researchgate.net/publication/319097404_Defense_Methods_Against_Social_Engineering_Attacks (дата обращения 19.09.2017)
4. The Chromium Projects (Unknown) Sandbox FAQ [Электронный ресурс] URL: https://chromium.googlesource.com/chromium/src/+/master/docs/design/sandbox_faq.md (дата обращения 19.09.2017)
5. Mozilla Wiki (Unknown) Security/Sandbox [Электронный ресурс] URL: https://wiki.mozilla.org/Security/Sandbox (дата обращения 19.09.2017)
6. Art Kohn (2014) Brain Science: The Forgetting Curve–the Dirty Secret of Corporate Training [Электронный ресурс] URL: http://www.learningsolutionsmag.com/articles/1379/brain-science-theforgetting-curvethe-dirty-secret-of-corporate-training (дата обращения 19.09.2017)
7. Роблинг Г., Мюллер М. Social engineering: a serious underestimated problem. [Электронный ресурс] URL:https://www.researchgate.net/publication/220807213_Social_engineering_a_serious_underestimated_problem (дата обращения 19.09.2017)

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ НА ТРАНСПОРТЕ

УДК 004.8

ТЕХНОЛОГИИ СЕТЕЙ НОВОГО ПОКОЛЕНИЯ (NGN) И ИХ ПРИМЕНЕНИЕ НА ВОДНОМ ТРАНСПОРТЕ

Алексеев Андрей Дмитриевич, Ерисова Анастасия Дмитриевна, Малов Сергей Сергеевич
Государственный университет морского и речного флота имени адмирала С.О. Макарова, Россия, Санкт-Петербург, ул. Двинская, д.5/7
emails: xoytlo@ya.ru, andalexs@ya.ru, Malov_sergey@mail.ru.

Аннотация: В статье рассмотрены сети нового поколения (NGN)и возможность их реализации на водном транспорте.

Ключевые слова: *сети нового поколения (NGN); водный транспорт.*

NEXT GENERATION NETWORK TECHNOLOGIES AND THEIR APPLICATION FOR THE WATER TRANSPORT

Andrey Alexeev, Anastasiya Erisova,Malov Sergey
Admiral Makarov State University of Maritime and Inland Shipping Russia,
Saint-Petersburg, Dvinskaya st., 5/7
emails: xoytlo@ya.ru, andalexs@ya.ru, Malov_sergey@mail.ru.

Abstract: The article presents Next Generation Network (NGN) and application of it for the water transport.

Keywords: Next Generation Network (NGN); water transport.

Введение. Водный транспорт, как и многие другие виды транспорта, использует множество различных средств передачи данных. Например, одними из самых распространенных на водном транспорте видов передачи данных являются такие как сети: передачи данных и телематических служб, управления движением судов, аудио-видео и диспетчерской связи. Также огромную роль в навигации и связи морского судна с сушей играет радиосвязь. Эти и многие другие средства обмена информации значительно упрощают жизнь людям, но для того чтобы ими управлять, усовершенствовать и делать их безопаснее необходимо создавать отдельные системы, и данные действия необходимо повторять для каждого вида связи. Чтобы уйти от этого и создать единую систему управления, которая должна упростить обеспечение безопасности и управление всеми видами связи, были выполнены разработки нового вида сетей. О сетях нового поколения (NGN) начинали говорить ещё в 2004 году и прогнозы были обнадеживающими, но все новости о внедрении или попытка внедрения NGN в России заканчиваются 2008 годом. В настоящее время технологии сетей нового поколения активно развиваются за рубежом. NGN подразумевает объединение систем сотовой связи (GSM,GPRS, UMTS и др.), систем связи беспроводного доступа Wi-Fi (IEEE 802.11), систем кабельного телевидения, телефонии, спутниковых и других информационных систем. Рассмотрим возможности применения технологий сетей нового поколения (NGN) на водном транспорте. Состав задач, решаемых сетями нового поколения (NGN) заключается в следующем:

1. Централизация управления всеми видами информационно-коммуникационных сетей, то есть создание возможности управления сетями управления движения судов, навигации, сетями диспетчерской связи и другими из единого центра координации действий;
2. Повышение защищенности сетей от различного рода информационных атак по средствам создания общего для всех сетей, но при этом разделенного сетевого шлюза и многочисленных, но независимых друг от друга сетевых экранов;
3. Создание обширной информационной структуры охватывающей всю область применения, а не отдельные её разделы.

На сегодняшний день развитие инфокоммуникационных услуг в большей своей степени ограничено рамками Интернета, который реализуется через традиционные сети. Но даже сейчас Интернет все еще не в состоянии предоставлять услуги отвечающие требованиям, предъявляемым современным обществом. Требуются решить ряд задач связанных с эффективным управлением информационными ресурсами, с увеличением функциональности сетей. Это говорит о том, что

необходимость в развитии современных сетей и протоколов построения сетей существует и возрастает.

Протокол IP и технология MPLS - это интернет технологии на которых основывается NGN. Сегодня существует несколько подходов к построению сетей IP-телефонии: H.323, SIP и MGCP.

H.323. Первым подходом построения сети IP-телефонии на основе утвержденных стандартов был предложен международным союзом электросвязи (МСЭ) в H.323. Сети, созданные по регламенту протоколов H.323, направлены на соединение с телефонными сетями и могут быть рассмотрены как наложенные на сети передачи данных ISDN.

SIP. Установление связи в подобных видах сетей основывается на ITU-T Q.931.SIP. Ранее использовался протокол H.323, но были выявлены некоторые проблемы с NAT traversal и абонентской линией, после чего стали применять протокол SIP. Сегодня SIP активно используется в VoIP. Независимость SIP от транспортных технологий является преимуществом перед другими распространенными протоколами.

MGCP. Следующий метод выстраивания сетей нового поколения основан на разделении шлюза по функционалу. В MGCP шлюз разделяется на три составляющие: пользовательские данные, сигнальная информация, устройство управления.

Построение сети. Для создания сети нового поколения нужно иметь следующие ресурсы:

– Протоколы и транспортные каналы связи, которые бы обеспечивали поддержку и доставку информации любого формата;

– Оборудование необходимое для поддержки и доступа к NGN как с суши, так и с воды;

– Устройства, которые обеспечивали бы связь всех подсистем входящих в водный транспорт.

Помимо вышеперечисленных ресурсов, чтобы создать подобную сеть, необходимо ориентироваться на базовые принципы NGN, а именно, разграничение функций «переноса» и «коммутации» от функций «управления вызовом» и «управления услугами». [1]

Так же, если рассмотреть все предоставляемые информационно-коммуникационные услуги и их особенности, можно выделить ряд условий, необходимых для качественного предоставления подобной сети:

— Гарантированное качество обслуживания (QoS) пользователей;

— Управление сетью должно осуществляться централизовано;

— Независимость технологий передачи (транспортных) от технологий предоставления услуг;

— В зависимости от необходимости, иметь возможность регулировать скорость передачи данных;

— Принимать и отправлять более сложно структурированную информацию, с возможностью работы с данными в реальном времени;

— Регулирование предоставляемой услуги как с клиентской стороны, так и со стороны провайдера;

— Предоставление возможности использования услуг, не ограничивая отдельными видами технологий;

— Разграничение обязанностей операторов в зависимости от области деятельности и предоставление возможности управления услугой нескольким операторам.

Структура сети NGN. Перейдем к структуре сети нового поколения, для более полного понимания того, как же построить мультизадачную сеть (см. Рисунок 1) [1].

Принцип построения и работы NGN отличается от работающих на данный момент моделей сетей. Например, интерфейсы, находящиеся между функциональными блоками в узлах ТфОП, не являются стандартизованными ИСО. Из-за этого операторы сетей и провайдеры услуг не могут самостоятельно вносить изменения в функции сетевых устройств и реализовать возможность их взаимодействия с помощью стандартных интерфейсов.

Руководящей идей сетей нового поколения является сближение существующих сетей и технологий, таких как IP или мобильные сети. Это процесс слияния всевозможных технологий и услуг связи для того, чтобы сделать работу имеющегося оборудования более обширной и многофункциональной.

Аппаратно-программные средства соединения сетей разного вида архитектур, с разными протоколами и форматами данных называются шлюзами. Они обеспечивают общение сетей друг с другом.

Наиболее подходящей, для начала реализации NGN, на данный момент технологией является TCP/IP, из которого можно взять за основу протокол IP.

Протокол IP удовлетворяет требованию к скорости передачи данных и благодаря технологии VoIP отвечает требованию к передачи информации, чувствительной к задержке по времени, то есть аудио и видео связь в настоящем времени. Но данный протокол не гарантирует качественную доставку информации. Исходя из вышеперечисленного, наиболее развитым можно считать многопротокольную технологию MPLS, которая использует коммутацию с помощью меток.

В MPLS маркер маршрута к пакету присваивается на входе в домен. Каждый LSR содержит таблицу, которая соотносит паре «интерфейс входа, метка входа» пару «интерфейс выхода, метка выхода». После получения пакета в LSR определяется для него интерфейс выхода. Метка входа заменяется исходящей (записанной в соответствующем поле таблицы), и пакет пересылается к следующему LSR.

Вся процедура занимает значительно меньше времени, чем сравнение IP-адреса отправителя с адресным префиксом в таблице маршрутов.

Для того чтобы однозначно обеспечить качество передачи данных нужно придерживаться не только указаний MPLS, но и необходима совместная работа процедур управления трафиком и процедур резервирования ресурсов.

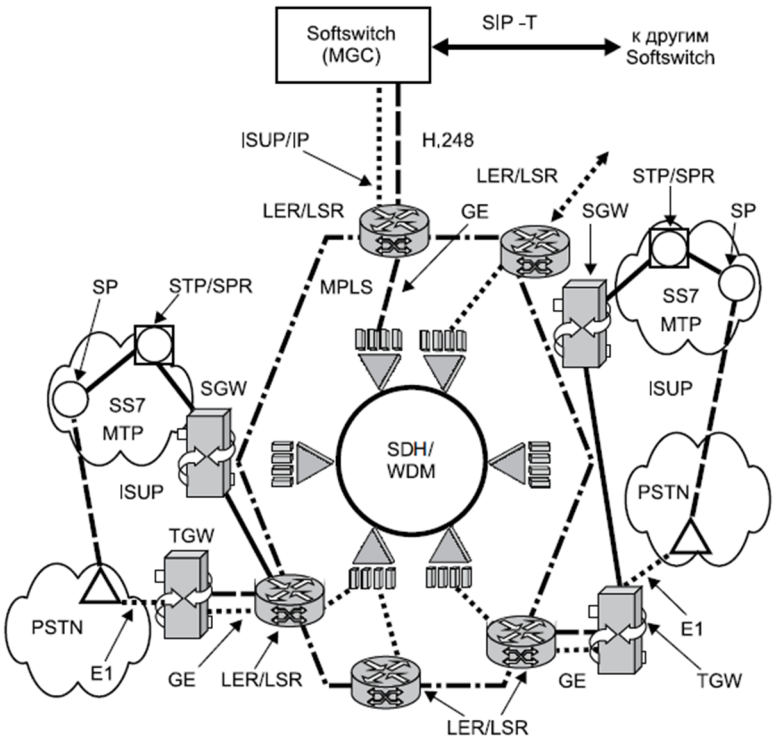


Рис.1. Структурная схема NGN

NGN можно представить в виде трех уровней: транспортного, управления коммутации и передачи информации, и уровень управления услугами (см. Рисунок 2) [2].

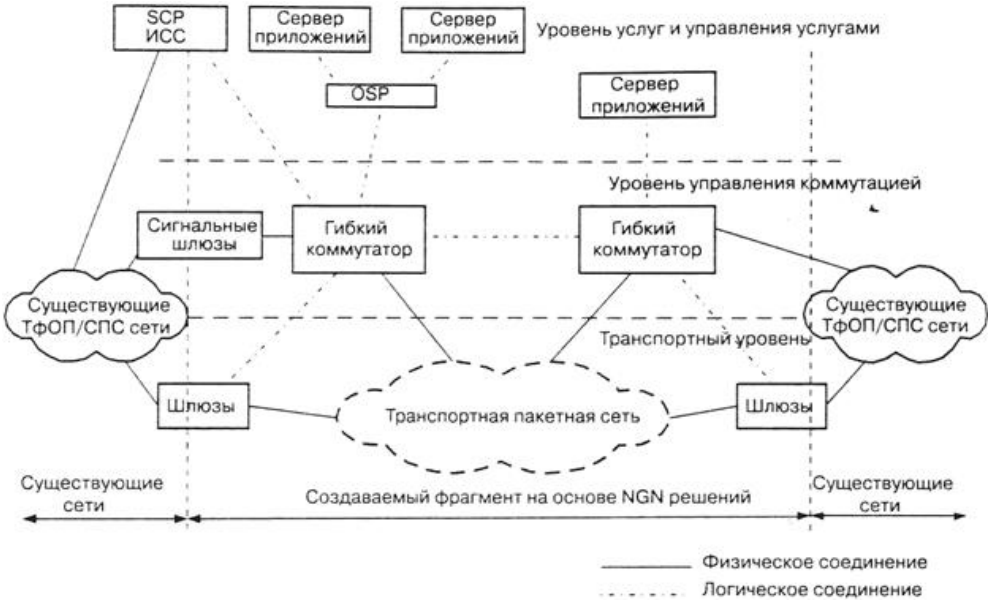


Рис. 2. Представление уровней NGN

Уровень управления коммутации и передачи информации базируется на новых программно-аппаратных комплексах, называемых Softswitch. Уровень управления сервисами, обеспечивающих необходимый набор услуг. [3]

Softswitch осуществляет управление вызовами, медиашлюзами, распределением ресурсов магистральной сети, обработкой сигнальных сообщений, аутентификацией, учетом стоимости услуг и т.д.

На уровне коммутации и передачи осуществляется коммутация пакетов с помощью маршрутизаторов и IP-коммутаторов, в которых обработка пакетов выполняется аппаратно. Эти устройства распределены в транспортной сети. На этом уровне осуществляется предоставление абонентам единообразной и интегральной платформы доставки информации с высоким качеством и большой пропускной способностью.

На уровне управления ресурсами транспортной сети осуществляется управление вызовами с использованием требуемого набора протоколов сигнализации. На этом уровне используется многофункциональный объект Softswitch (контроллер медиашлюза).

На уровне Service and Application осуществляется предоставление большого разнообразия услуг, а также поддержка целостности установленных соединений. Здесь применяются различные системы, такие как AS (Application Server), SCP (Service Control Point) и другие.

Сети должны быть обеспечены доступом к NGN при помощи оборудования пользователя и шлюзов для подключения сетей доступа. Сеть доступа (Access network) − это часть общей сети электросвязи, расположенной между пользователем и узлом предоставления услуг. Параллельно с ней используется транспортная сеть (Transport network) − это часть сети электросвязи, обеспечивающая доставку информационных и служебных сигналов по заданным адресам и состоящая из ряда подсетей. [2]

Для управления сетями доступа была создана система управления функциями сетей доступа, которая предназначена для решения следующих задач:

- обеспечение технической эксплуатации и технического обслуживания;
- управление сетью и конфигурирование;
- координация с системой управления транспортной сетью;
- обнаружение и индикация неисправностей;
- сбор и обработка статистических данных;
- управление ресурсами и безопасностью.

Перечисленные технологии обеспечивают доступ к ресурсам сети и передачу данных разного вида, но не обеспечивают требуемого качества доставки информации, так как не устанавливают соединений для доставки данных, чувствительных к задержке и потерям.

Наиболее подходящими решениями здесь можно считать протоколы сигнализации и стандартизованные протоколы и интерфейсы:

— RSVP (Reservation Protocol) − протокол резервирования ресурсов;

— Q.931 (протокол сетевого уровня абонентской цифровой системы сигнализации);

— V5.2 (интерфейс N-ISDN, позволяющий предоставить пользователям удаленный фиксированный и мобильный доступ к ресурсам). [4]

Граничный маршрутизатор LER, использующий технологию MPLS, обеспечивает согласование транспортной сети NGN и IP-сети.

На момент согласования LER анализирует виды поступающих потоков IP-пакетов, присваивает пакетам метки (Label) и определенный класс доставки. В соответствии с указаниями протоколов более высокого уровня выполняется установление постоянных виртуальных каналов в домене MPLS.

В ядре транспортной сети помеченные пакеты компилируются маршрутизаторами (LSR). Доставка этих пакетов от входного граничного маршрутизатора до выходного обеспечивается с помощью технологий GE/SDH. В состав транспортной сети NGN могут входить транзитные узлы, оконечные (конечные) узлы, контроллеры сигнализации и шлюзы, позволяющие подключать традиционные сети связи.

Эффекты, которые можно ожидать при внедрении решений сетей NGN на водном транспорте:

— повышение безопасности сети водного транспорта в целом и отдельных услуг;

— повышение конкурентоспособности сети водного транспорта;

— повышение эффективности использования сети на большом количестве станций как клиентских, так и серверных;

— повышение готовности сети к мгновенному ответу на запросы различного характера.

Заключение. Проанализировав информацию о способе построения и плюсах данной системы, а так же столкнувшись с проблемами перехода к NGN, а именно: отсутствие достаточного количества инвестиций; отсутствие единой политики перехода к NGN; единого мнения по поводу путей и темпов построения NGN; отсутствие или незаконченность стандартов, описывающих все аспекты NGN; отсутствие полной линейки оборудования для NGN; несовместимость оборудования разных изготовителей (риски по поводу масштабируемости и сохранения инвестиций). Можно прийти к выводу,

что в будущем данная технология может стать уникальной и получить распространения за счет преимуществ, рассмотренных выше, но в настоящее время из-за нехватки специализированного оборудования, квалифицированных кадров и отсутствия доработанной системы стандартов ее применение стоит под вопросом, т.к. ее реализация требует больших материальных затрат.

СПИСОК ЛИТЕРАТУРЫ

1. Jingming Li Salina, Pascal Salina. Next Generation Networks: Perspectives and Potentials - 2007.
2. Битнер В. И., Михайлова Ц. Ц. Сети нового поколения – NGN. Учебное пособие для вузов. –М.: Горячая линия – Телеком, 2011.
3. Kevin Foster, Office of the Group CTO, British Telecommunications plc (BT), UKITU-T / ATIS Workshop «Next Generation Technology and Standardization»
4. Онлайн библиотека [Электронный ресурс]: Электрон. журн. -http://www.tinlib.ru/ - [Россия] 2017г

УДК 629.75.33 + 533.6.013.622

О МЕТОДЕ ИДЕНТИФИКАЦИИ БЕСПИЛОТНЫХ ВОЗДУШНЫХ СУДОВ ПРИ РЕАЛИЗАЦИИ КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ

Беляев Сергей Алексеевич[1], Остапченко Юрий Борисович[2], Кудряков Сергей Алексеевич[3], Рубцов Евгений Андреевич[3]
[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
[2] ОАО «НИЦ СПб ЭТУ», Россия, Санкт-Петербург, ул. Политехническая, д. 22, лит. «Н»
[3] Санкт-Петербургский государственный университет гражданской авиации, Россия, Санкт-Петербург, ул. Пилотов, д. 38,
emails: beliaev@nicetu.spb.ru, ou@nicetu.spb.ru, psi_center@mail.ru, rubtsov.spb.guga@rambler.ru

***Аннотация*:** В статье рассматривается метод идентификации беспилотных воздушных судов для обеспечения безопасности полетов в населенных пунктах и на объектах транспортной инфраструктуры. Метод предполагает оснащение беспилотных воздушных судов приемо-передающими модулями, включающими SIM-карту и позволяющими производить идентификацию аппаратов в сетях мобильной связи. Проанализирована возможность внедрения данного метода в комплексных системах безопасности.

***Ключевые слова**: беспилотное воздушное судно; идентификация; безопасность полетов; объекты транспортной инфраструктуры.*

ABOUT THE METHOD OF UNMANNED AIRCRAFT IDENTIFICATION IN THE IMPLEMENTATION OF COMPLEX SAFETY SYSTEMS

Belyaev Sergey[1], Ostapchenko Yuriy[2], Kudryakov Sergey[3], Rubtsov Evgeny[3]
[1] The St. Petersburg State Electrotechnical University "LETI", Russia, St. Petersburg, Professor Popov str. 5,
[2] Research and Engineering Center of Saint-Petersburg Electro-Technical University JSC, Russia, St. Petersburg, Politechnicheskaya str. 22, building “N”
[3] Saint-Petersburg state University of civil aviation, Russia, St. Petersburg, Pilotov str. 38,
emails: beliaev@nicetu.spb.ru, ou@nicetu.spb.ru, psi_center@mail.ru, rubtsov.spb.guga@rambler.ru

Abstract: The article considers the method of unmanned aircraft identification for ensuring flight safety in the settlements and transport infrastructure. The method involves equipping an unmanned aircraft with receiving and transmitting modules, including a SIM card and enabling the identification vehicles within mobile networks. Possibility of implementing this method in complex safety systems is analyzed.

***Keywords**: unmanned aircraft; identification; flight safety; transport infrastructure.*

Введение. Развитие новых видов транспортных средств заставляет по-новому взглянуть на проблему обеспечения безопасности в населенных пунктах и на объектах транспортной инфраструктуры. Беспилотные воздушные суда (БВС) стали общедоступными, их характеристики (дальность и время полета, потолок, взлетный вес, полезная нагрузка) позволяют пользователям по неосторожности или со злым умыслом причинить огромный вред объектам транспортной инфраструктуры, а также самим транспортным средствам [1].

Для предотвращения катастроф и инцидентов, или уменьшения их количества целесообразно внедрять комплексные системы безопасности, подразумевающие сбор данных о всех элементах транспортной системы, прогноз на заданную глубину, обнаружение и разрешение конфликтных ситуаций. При постановке задачи сбора данных о беспилотных воздушных судах, становится очевидной проблема, связанная с их учетом, регистрацией и идентификацией. В рамках статьи предложен метод, позволяющий решить данную проблему.

Комплексные системы безопасности

Транспортная инфраструктура включает в себя объекты, большинство из которых выступает в качестве мест массового скопления людей, а, значит, существенно повышается уровень опасности и требует повышенного внимания от контролирующих органов и наличия развитой системы мониторинга ситуации, прогнозирования и разрешения конфликтных ситуаций. С этой точки зрения целесообразно на уровне города или значимого региона внедрять комплексные системы безопасности. При этом должно учитываться не только техническое состояние транспортной инфраструктуры, но и контролироваться транспортные и пассажирские потоки. Обобщённая структура комплексной системы безопасности приведена на рисунке 1 [2].

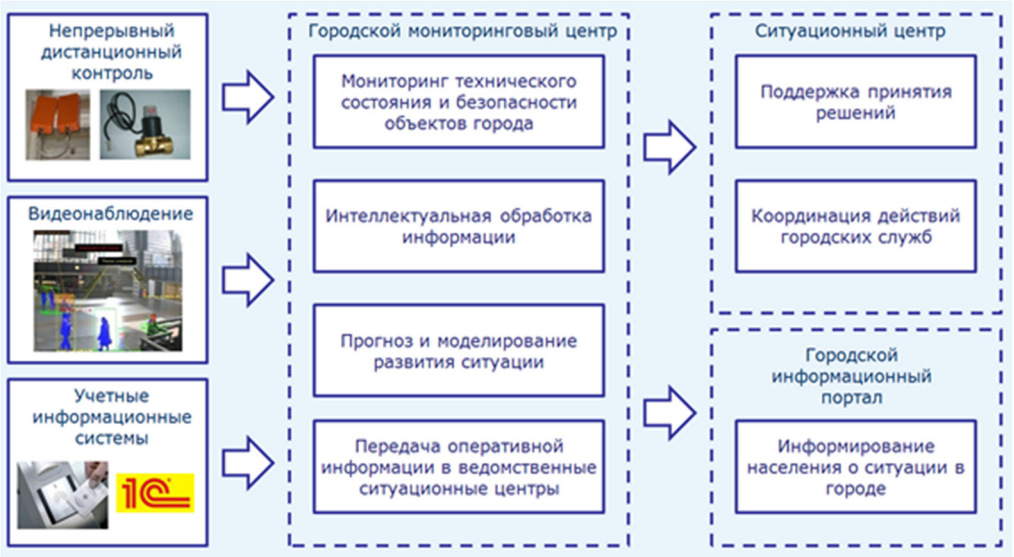


Рис. 1. Обобщенная структура комплексной системы безопасности

Комплексная система безопасности должна включать в себя непрерывный дистанционный мониторинг всех значимых объектов транспортной инфраструктуры, что позволит обеспечить надёжность зданий и сооружений, которые могут повлиять на безопасность контролируемого участка. Системы контроля и управления доступом обеспечивают контроль прохождения в различные учреждения и на территории, требующие повышенного внимания, такие как метрополитены, аэропорты, железнодорожные станции и т.п. Видеонаблюдение используется повсеместно, но классическое видеонаблюдение уже не справляется с огромными потоками информации, поэтому целесообразно использовать интеллектуальное видеонаблюдение, которое позволяет с одной стороны автоматизировать процесс выявления нарушений, с другой стороны обеспечить контроль гораздо большей территории одним оператором [2].

Информация, собираемая от источников в виде датчиков комплексов непрерывного дистанционного контроля, видеонаблюдения, систем контроля и управления доступом поступает в городской мониторинговый центр, который обеспечивает решение следующих ключевых задач [2]:

1) мониторинг технического состояния и безопасности объектов, благодаря чему обеспечивает контроль технического состояния транспортной инфраструктуры;

2) интеллектуальная обработка информации, благодаря чему с одной стороны уменьшается влияние человеческого фактора, с другой стороны появляется возможность в автоматическом режиме учитывать типовые ситуации, учитывать историю развития событий и прослеживать зависимости между различными ситуациями;

3) прогноз и моделирование развития ситуации, благодаря чему обеспечивается поддержка принятия управленческих решений;

4) передача оперативной информации в ведомственные ситуационные центры, что соответствует современным тенденциям по информационному взаимодействию с федеральными органами исполнительной власти.

Информация городского мониторингового центра поступает в ситуационный центр и городской информационный портал. На уровне ситуационного центра она используется для поддержки принятия решений и координации действий городских служб, на уровне информационного портала позволяет информировать население об опасных явлениях.

Мониторинг технического состояния и безопасности объектов города обеспечивает [2]:

– автоматическое получение информации от встроенных систем контроля технического состояния;

– допусковый контроль текущих значений критических параметров и анализ их изменения с автоматическим информированием (e-mail, sms) при превышении пороговых значений;

– прогнозирование технического состояния объекта и остаточного ресурса систем на заданный период времени;

– информирование о выявленных отклонениях в техническом состоянии объектов с формированием и выдачей рекомендаций для принятия решений;

– трехмерное моделирование объектов контроля с отображением текущего технического состояния;

– непрерывный и периодический мониторинг технического состояния объектов контроля на основе ультразвукового, тепловизионного, тензометрического и других методов контроля;

– системный анализ характера изменения всех контролируемых параметров с выдачей рекомендаций по возможному возникновению нештатных или аварийных ситуаций.

Техническая реализация мониторинга технического состояния включает в себя сбор информации от разнородных датчиков, предназначенных для контроля основных параметров, сохранение её в различные специализированные базы данных, репликацию с использованием адаптеров сопряжения, выгрузку с учётом существующих каналов связи и сбор в едином хранилище для предоставления к нему доступа в центре мониторинга.

Технология интеллектуальной обработки и анализа данных обеспечивает [2]:

– выявления зависимостей в данных (статистическая обработка и сегментация данных, выполнение многомерного анализа, распознавание образов, ассоциативный анализ);

– систематизацию информации об объектах с целью классификации их состояний;

– выявление нетипичного поведения объектов;

– поиск причин отклонения поведения объектов;

– сокращение объемов хранимых данных без потери информации.

Разработано большое количество методов и подходов, обеспечивающих интеллектуальную обработку информации, их корректное применение существенно зависит от конкретной решаемой задачи. В качестве основных источников данных могут выступать как модули непрерывного дистанционного мониторинга, так и комплексы видеонаблюдения, а также и другие информационные системы. Возможны различные варианты построения системы видеонаблюдения.

Диспетчерский центр, обеспечивающий, в том числе интеллектуальную обработку информации должен состоять из нескольких подсистем: ввода, администрирования, визуализации, диспетчеризации, анализа и базы данных. Служба безопасности с использованием подсистемы ввода выполняет редактирование профилей нарушителей, регламентов работы системы и регистрацию объектов наблюдений, с использованием подсистемы администрирования задаёт и контролирует права доступа. Старший диспетчер с использованием подсистемы визуализации управляет формами отображения, настраивает отображение на плане-схеме, просматривает историю событий. Диспетчер работает как с исходным видео, так и с результатами его обработки, сохранёнными в компонентах Service Desk. Непосредственный анализ информации выполняется в подсистеме анализа, при этом в качестве внешних источников используется не только видео, поступающее от видео- и телекамер, но и данные внешних информационных систем, которые могут включать в себя системы контроля и управления доступом, системы мониторинга технического состояния и других систем [2].

Разрабатываемые в настоящее время комплексные системы безопасности предназначены для работы с железнодорожным, автомобильным и авиационным транспортом. Широкое распространение беспилотных воздушных судов требует внесения срочных и кардинальных коррективов в структуру данных систем безопасности. Из-за малых размеров беспилотный аппарат довольно сложно обнаружить с помощью радиолокационных и оптических систем наблюдения, однако гораздо большей проблемой является отсутствие общепринятой и законодательной утвержденной системы учета, регистрации и идентификации БВС.

Метод идентификации беспилотных воздушных судов

Чрезвычайные происшествия на транспорте в России и за рубежом происходят по причинам, в большой степени обусловленным человеческим фактором. При этом к числу причин возникающих аварий и катастроф часто относятся не только прямые ошибки в деятельности персонала, но и общая тенденция к пренебрежению установленными правилами и инструкциями, а также правовой нигилизм.

В области беспилотной авиации проблему осложняет тот факт, что пользователями воздушного движения (внешними пилотами) становятся люди имеющие довольно слабую теоретическую и практическую подготовку, либо не имеющие такой подготовки. Беспилотное воздушное судно, управляемое неподготовленным оператором может потерять управление, выйти за пределы зоны действия радиотехнических средств станции внешнего пилота (в простейшем случае – пульта управления беспилотным аппаратом) и при выполнении маневра, заложенного в бортовой модуль автопилота, столкнуться со зданиями, сооружениями, транспортными средствами, либо упасть в местах массового скопления людей с соответствующими последствиями.

Для мониторинга беспилотных воздушных судов можно применять входящие в состав комплексных систем безопасности средства видеонаблюдения, в том числе интеллектуального видеонаблюдения. Однако, из-за малых размеров беспилотных аппаратов, дальность действия средств видеонаблюдения будет ограничена, особенно в сложных метеоусловиях. Возможно

применение средств радио мониторинга, позволяющих отслеживать сеансы радиообмена между БВС и станцией внешнего пилота, но потребует внедрения дополнительных технических средств в комплексную систему безопасности и приведет к увеличению как стоимости самой системы, так и стоимости обслуживания [3].

Воздушный кодекс Российской Федерации требует учета беспилотных воздушных судов массой от 250 г до 30 кг и государственной регистрации для БВС массой более 30 кг [4]. Процедуры учета и регистрации на законодательном уровне пока еще не оговорены, этим обстоятельством пользуется ряд компаний, выдающих сертификаты учета БВС на основе своих собственных правил.

При возникновении опасных ситуаций или предпосылок к опасным ситуациям, связанным с беспилотными воздушными судами, владелец имеет шанс уйти от ответственности по причине практической недоказуемости того, что беспилотный аппарат принадлежит именно ему. Беспилотные воздушные суда в настоящее время не имеют уникальных идентификаторов и в полете являются по сути обезличенными.

Решением перечисленных проблем может стать введение процедуры учета и регистрации БВС путем обязательной установки приемо-передающего модуля с SIM-картой оператора мобильной связи. Для получения SIM-карты пользователь должен предъявить документ удостоверяющий личность. Данные о владельце заносятся в базу данных, что в будущем позволит однозначно определить владельца БВС. Кроме того, предоставление паспортных данных имеет важный психологический аспект и повышает уровень ответственности пользователя беспилотного аппарата.

При выполнении полета беспилотное воздушное судно периодически или по запросу излучает сигнал содержащий уникальный номер, соответствующий данному аппарату, таким образом решается проблема идентификации БВС. По сравнению с визуальной идентификацией (по типу автомобильных номеров), идентификация с помощью SIM-карты имеет ряд:

1) возможность идентификации мини и микро аппаратов, плохо наблюдаемых визуально или с помощью средств видеонаблюдения;

2) стабильная работа в неблагоприятных метеоусловиях (туман, дождь);

3) возможность определения местоположения БВС при использовании имеющихся в мобильных сетях методах позиционирования абонентов;

4) применение существующей инфраструктуры средств мобильной связи, что позволит значительно снизить расходы на внедрение системы идентификации БВС.

Для реализации описанного метода идентификации БВС в комплексных системах безопасности необходимо обеспечить сопряжение с сетями мобильной связи, либо получить доступ к информации о положении абонентов-БВС, их передвижении и выполняемых полетах.

Заключение

Разрабатываемые в настоящее время комплексные системы безопасности несомненно позволят снизить риск катастроф и инцидентов. Для этого предполагается развернуть обширную сеть средств мониторинга, включающих интеллектуальное видеонаблюдение. Анализ собранных данных позволит производить прогноз, выявлять и разрешать конфликтные ситуации.

В то же время комплексные системы безопасности должны отвечать современным вызовам, выразившимся в лавинообразном росте числа беспилотных воздушных судов у населения. Новый вид транспорта требует применения дополнительных средств для обеспечения мониторинга обстановки.

Отмеченные в Воздушном кодексе процедуры учета и регистрации беспилотных воздушных судов рекомендуется дополнить требованием установки на борту беспилотных воздушных судов приемо-передающего модуля с SIM-картой. Оборудованные БВС можно легко и однозначно идентифицировать, а также определять их местоположение, используя штатные возможности позиционирования в мобильных сетях связи.

Внедрение метода идентификации с помощью SIM-карт позволит однозначно определять принадлежность беспилотного воздушного судна конкретному владельцу, что повысит уровень ответственности пользователей, а также заставит их более серьезно подходить к вопросу подготовки и проведения полетов.

СПИСОК ЛИТЕРАТУРЫ

1. Беспилотные авиационные системы. Учебное пособие / С.А. Кудряков, В.Р. Ткачев, Г.В. Трубников, В.И. Кисличенко // СПб.: Свое издательство. – 2015. – 121 с.
2. Опыт создания комплексных систем безопасности на объектах транспортной инфраструктуры / С.А. Беляев, Ю.Б. Остапченко, С.А. Кудряков, Е.Н. Шаповалов, М.Г. Павловский // Актуальные проблемы защиты и безопасности. Комплексная безопасность на транспорте. Труды XIX Всероссийской научно-практической конференции. Том 6. – 2016. – С. 52-57.
3. Радиотехническое обеспечение полетов воздушных судов и авиационная электросвязь. Учебное пособие / С.А. Кудряков, В.К. Кульчицкий, Н.В. Поваренкин, В.В. Пономарев, Е.А. Рубцов, Е.В. Соболев, Б.А. Сушкевич // СПб.: Свое издательство. – 2016. – 287 с.
4. Воздушный кодекс Российской Федерации: [федер. закон №60-ФЗ: принят Гос. Думой 19 фев. 1997 г.: ред. от 06.07.2016: с изм. и доп., вступ. в силу с 5.07.2017]. – 66 с.

УДК 004.08

НАУЧНО-МЕТОДИЧЕСКИЕ ПОДХОДЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ТРАНСПОРТЕ

Белов Андрей Сергеевич[1], Барабанов Владимир Викторович[2]
[1]Михайловская военная артиллерийская академия, Россия, г. Санкт-Петербург, ул. Комсомола 22,
[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия, д. 39,
emails: andrej2442016@yandex.ru,vlbar@yandex.ru

***Аннотация*:** В статье рассматривается процесс ведения нарушителем несанкционированного мониторинга информационных систем посредством анализа демаскирующих признаков, а также предлагается способ управления демаскирующими признаками информационных систем на транспорте, как один из вариантов обеспечения их безопасности.

Ключевые слова: *демаскирующий признак, программное воздействие, информационные системы, способ управления.*

SCIENTIFIC AND METHODOLOGICAL APPROACHES TO ENSURE SAFETY OF INFORMATION SYSTEMS IN TRANSPORT

Belov Andrey[1], Barabanov Vladimir[2]
[1]Mikhailovskaya military artillery Academy, Russia, St. Petersburg, Komsomola str.22,
[2]St. Petersburg Institute of Informatics and Automation of the Russian Academy of Sciences,
Russia, St. Petersburg, 14 line, 39,
emails: andrej2442016 @ yandex.ru, vlbar @ yandex.ru

Abstract: The article deals with the process of keeping the infringer of unauthorized monitoring of information systems by means of analysis of unmasking features, and also provides a way to manage the unmasking features of information systems in transport as one of the options for ensuring their safety.

Keywords: *unmasking feature, software impact, information systems, management method.*

С развитием информационных и телекоммуникационных технологий, совершенствованием средств связи, обработки, хранения и распределения информации, становится актуальным процесс развития информационных систем (ИС), заключающийся в переходе к новым, более совершенным формам и организации сетей связи путем цифровизации и интеграции их в общемировое телекоммуникационное пространство.

В свою очередь, интеграция ИС на транспорте в общемировое телекоммуникационное пространство существенно увеличивает возможности нарушителей по их идентификации, вскрытию и воздействию [1-3].

Анализ информационных систем осуществляется нарушителем посредством ведения несанкционированного мониторинга (Рис. 1). Из Рис. 1 видно, что процесс ведения несанкционированного мониторинга ИС осуществляется поэтапно. Сначала определяются цели мониторинга (необходимость определения состава ИС, вскрытие структуры, либо выявление алгоритмов функционирования ИС).

Далее анализируются (исследуются) демаскирующие признаки ИС и процессов их функционирования. Процесс анализа демаскирующих признаков реализуется двумя подсистемами: активной и пассивной. Пассивное исследование осуществляет сбор типовых демаскирующих признаков ИС. К типовым демаскирующим признакам относятся: форма огибающей сигнала; спектр сигналов; вид излучения, вид модулирующего сигнала; значения параметров сигнала; мощность излучения; количество излучаемых фиксированных частот и величины разноса между ними, взаимные удаления элементов по пеленгам (средств, комплексов, узлов связи); площадь размещения транспортных средств и др. [4-7].

Активное исследование предполагает использование деструктивных комплексных программных воздействий, включающих совокупность воздействий различных классов, объединенных единым сценарием.

В настоящее время наиболее часто реализуемые программными воздействиями являются [8-11]: анализ сетевого трафика, сканирование ИС, угроза выявления пароля, подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа, навязывание ложного маршрута ИС, внедрение ложного объекта ИС, отказ в обслуживании; удаленный запуск приложений.

Множество характеристик описания процесса комплексных программных воздействий на ИС со стороны злоумышленника представляется в виде [12-15]:

$$U = \left\{ (u_1^{\text{дпв}}, \ldots, u_n^{\text{дпв}}), (u_1^{\text{пз}}, \ldots, u_m^{\text{пз}}), (u_1^{\text{нсд}}, \ldots, u_k^{\text{нсд}}) \right\},$$

где $u_1^{\text{ДПВ}},\ldots, u_n^{\text{ДПВ}}, u_1^{\text{ПЗ}},\ldots, u_m^{\text{ПЗ}}, u_1^{\text{НСД}},\ldots, u_k^{\text{НСД}}$ - подмножества характеристик деструктивных программных воздействий, процесса преодоления системы защиты ИС и осуществления несанкционированного доступа (НСД) соответственно, n, m, k - число типов соответствующих воздействий.

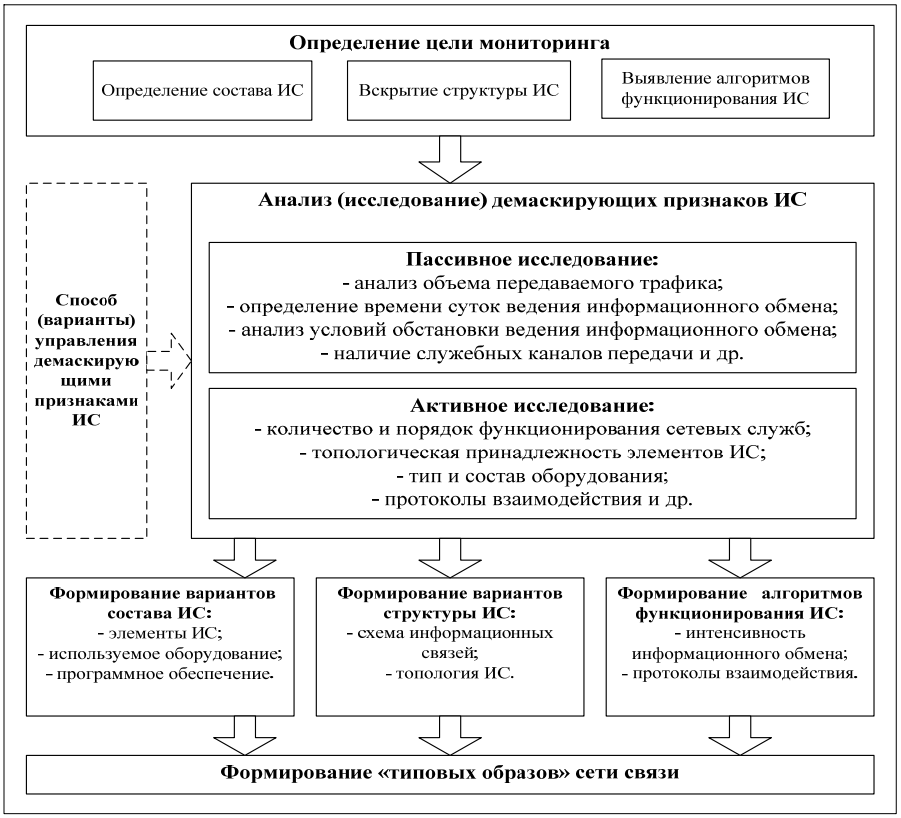


Рис. 1- Обобщенный порядок проведения несанкционированного мониторинга ИС (вариант)

В свою очередь каждое подмножество $u_i \in U$ имеет следующие характеристики: τ_i - оценка интервала времени между проведением каждого из воздействий i-го типа; T_i - оценка времени реализации воздействия i-го типа; V_i - оценка величины потенциального ущерба, нанесенного ИС в случае реализации воздействия i-го типа.

После анализа демаскирующих признаков переходят к формированию множества вариантов построения ИС, необходимых злоумышленнику для проведения полноценного исследования. Основными группами таких вариантов являются: варианты состава ИС, ее структуры и алгоритмов функционирования. Формирование вариантов ИС включает в себя не только прямое отображение параметров по демаскирующим признакам, но также их обобщение и интеллектуальный анализ, что в конечном итоге позволит сформировать «типовые образы» ИС, отражающие ее функциональные особенности [16,17].

Таким образом, в настоящее время становится актуальным вопрос по разработке научно-методического обеспечения, практических рекомендаций, а также средств, методов (способов) и систем защиты, соответствующих современным условиям безопасного функционирования ИС и их элементов в условиях ведения злоумышленником несанкционированного мониторинга.

При решении вопросов разработки средств, методов и систем защиты ИС необходимо [4]:

– определить цели защиты;
– провести анализ демаскирующих признаков и возможных каналов утечки информации;
– оцеить возможности злоумышленника по осуществлению несанкционированных воздействий;
– разработать и осуществить технически и экономически обосновнные меры, способы и системы защиты;
– обеспечить контроль эффективности принимаемых мер защиты.

Анализ существующих средств и методов защиты позволил определить, что демаскирующие признаки ИС, выявляемые активным исследованием, могут быть скрыты методами разграничения доступа (в частности межсетевого экранирования) и криптографического закрытия семантической составляющей информационного обмена [18,19].

Однако существующие методы защиты не всегда эффективны. В связи с этим возникает необходимость разработки научно-методических подходов, позволяющих осуществлять формирование защищенных ИС, путем управления (ослабления, устранения) их демаскирующими признаками.

В качестве научно-методического подхода разработан способ управления демаскирующими признаками ИС, основанный на варьировании значениями управляемых демаскирующих признаков по соответствующим правилам и в заданных пределах, в результате чего, злоумышленник вводится в заблуждение относительно структуры ИС и параметров их функционирования, что приводит к повышению устойчивости ИС в условиях деструктивных программных воздействий [19,20].

Обобщенная схема, поясняющая способ управления демаскирующими признаками ИС представлена на рис. 2.

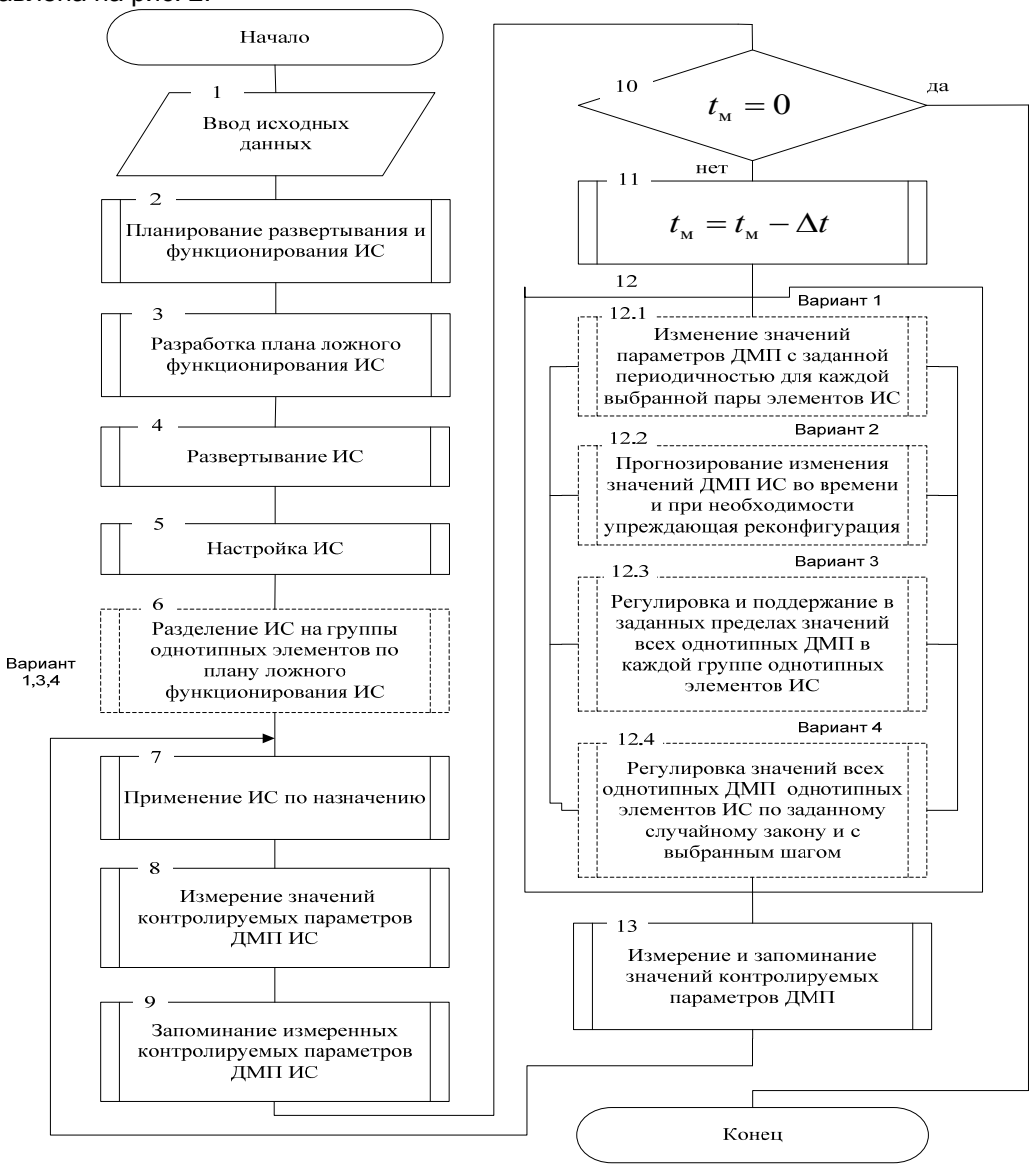


Рис. 2- Обобщенная схема способа (вариантов) управления демаскирующими признаками ИС

В качестве исходных данных задают множество контролируемых параметров демаскирующих признаков ИС, представляемое в виде:

$$N = \left\{ N_1 , N_2 ,..., N_{n-1} ,..., N_{\text{n}} \right\},$$

где N – множество контролируемых параметров демаскирующих признаков ИС, причем $N \geq 2$.

В результате измерения значений данных контролируемых параметров, в ходе выполнения цикла анализа, формируют $G \geq 2$ групп контролируемых параметров демаскирующих признаков и задают коэффициенты важности – (k_1,k_2…k_n) для каждой G-ой группы:

$$G = \left\{ k_1 (N_{G_1}), k_2 (N_{G_2}),..., k_{n-1} (N_{G_{n-1}}),..., k_n (N_{G_n}) \right\}.$$

Дополнительно определяется количество управляемых и неуправляемых демаскирующих признаков. Перед развертыванием, разрабатываются варианты ложного функционирования ИС. После

этого осуществляют развертывание ИС, настраивают основные параметры и применяют ее по назначению. На функционирующей ИС производят измерение значений контролируемых параметров демаскирующих признаков и запоминают их с целью дальнейшего использования.

Способ предполагает управление защищенностью ИС путем нескольких научно-методических подходов (вариантов обеспечения безопасности ИС).

В первом варианте злоумышленник вводится в заблуждение относительно структуры ИС и их параметров за счет периодического (по необходимости корректируемого) взаимного изменения демаскирующих признаков на выбранных парах элементов ИС.

Во втором варианте злоумышленник вводится в заблуждение относительно структуры ИС и их параметров на основе прогнозирования значений показателей демаскирующих признаков и, при необходимости, упреждающей реконфигурации ИС.

В третьем варианте злоумышленник вводится в заблуждение относительно структуры ИС и ее параметров за счет принудительной регулировки (с заданной периодичностью) и поддержания в установленных пределах на однотипных элементах ИС значений всех однотипных признаков.

В четвертом варианте злоумышленник вводится в заблуждение относительно структуры ИС и ее параметров за счет одновременного изменения всех однотипных параметров демаскирующих признаков в каждой группе всех однотипных элементов ИС по заданному случайному закону и шагу с заданным периодом так, чтобы параметры демаскирующих признаков элементов ИС попали в заданный интервал значений.

Таким образом, в каждом варианте, на основе измерения и прогнозирования характеристик демаскирующих признаков ИС, реализована возможность корректировки (изменения и поддержания) значений управляемых демаскирующих признаков их элементов в заданных значениях и упреждающей реконфигурации. Это, в конечном итоге, снижает эффективность несанкционированного мониторинга и преднамеренных деструктивных программных воздействий.

Научно-методические подходы реализованы в виде патента РФ на изобретение [20]. Кроме того, полученные результаты могут использоваться при проведении исследований и выполнении научно-исследовательских работ по разработке методов и способов защиты ИС в условиях внешних деструктивных программных воздействий, а также при проектировании систем защиты ИС в рамках определения защитного ресурса.

СПИСОК ЛИТЕРАТУРЫ

1. Зима В. М., Молдовян А. А., Молдовян Н. А. Безопасность глобальных сетевых технологий. СПб.: БХВ - Петербург, 2003. – 368 с: ил.
2. Теоретические основы создания систем поддержки принятия решений в интересах комплексной транспортной безопасности/ А.М. Сазыкин [и др.]// Известия Российской академии ракетных и артиллерийских наук. 2015. № 3. С. 10-15.
3. Проблема сравнения и выбора варианта построения системы безопасности/ В.В. Барабанов [и др.]/ В сборнике: Актуальные проблемы защиты и безопасности. - Труды Четвертой Всероссийской научно-практической конференции. 2001. С. 348-351.
4. Меньшаков Ю. К. Защита объектов и информации от технических средств разведки. – М. :Российск. гос. гуманит. ун-т, 2002. – 399 с.
5. Показатели эффективности межведомственного информационного взаимодействия при управлении обороной государства/ Е.Г. Анисимов, В.Г. Анисимов [и др.]// Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2016. № 7-8 (97-98). С. 12-16.
6. Анисимов В.Г., Селиванов А.А., Анисимов Е.Г. Методика оценки эффективности защиты информации в системе межведомственного информационного взаимодействия при управлении обороной государства// Информация и космос. 2016. № 4. С. 76-80.
7. Риск-ориентированный подход к организации контроля в подсистемах обеспечения безопасности информационных систем/ П.Д. Зегжда [и др.]// Проблемы информационной безопасности. Компьютерные системы. 2016. № 3. С. 61-67.
8. Руководящий документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). – М.: ФСТЭК, 2008. – 69 с.
9. Модели организации и проведения испытаний элементов системы информационного обеспечения применения высокоточных средств/ В.В. Барабанов [и др.]// Труды Военно-космической академии им. А.Ф. Можайского. 2015. № 648. С. 6-12.
10. Модель оценки эффективности информационного обеспечения применения высокоточного оружия в контртеррористических операциях/ А.Ю. Гарькушев, А.М. Сазыкин [и др.]// Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2015. № 1-2. С. 44-53.
11. Методика расчета латентного эффекта применения системы управления рисками/ В.Г. Анисимов Е.Г., Анисимов [и др.]// Вестник Российской таможенной академии. 2015. № 2 (31). С. 115-123.
12. Алгулиев Р. М. Угрозы корпоративным сетям и формализация их отношений с системами защиты. – Баку, 2000. – 30 с.
13. Основы построения моделей интеллектуализации в системах безопасности/ А.Ю. Гарькушев, А.М. Сазыкин [и др.]// Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2014. № 9-10. С. 22-27.
14. Модель причинного анализа на основе использования данных об особых ситуациях/ *В.В. Балясников, Ю.В. Ведерников* [и др.]// Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2015. № 1-2. С. 31-38.
15. Расчет эффективности межведомственного информационного взаимодействия в области обороны государства/ Е.Г. Анисимов [и др.]/ В сборнике: Система межведомственного информационного взаимодействия при решении задач в области обороны Российской Федерации. Сборник материалов II Межведомственной научно-практической конференции. Национальный центр управления обороной Российской Федерации/ Под общей редакцией И.В. Солохова.- 2016. С. 21-26.
16. Показатели эффективности защиты информации в системе информационного взаимодействия при управлении сложными распределенными организационными объектами/ Т.Н. Сауренко, С.П. Присяжнюк [и др.]// Проблемы информационной безопасности. Компьютерные системы. 2016. № 4. С. 140-145.
17. Петренко С. А. Методы информационно-технического воздействия на киберсистемы и возможные способы противодействия. – Труды ИСА РАН, том 41, 2009. 104-146 с.
18. Белов А. С. и др. Способ защиты автоматизированных систем. Патент РФ на изобретение № 2408927 от 21 июля 2009 г. – 11 с.
19. Белов А. С. и др. Способ контроля демаскирующих признаков системы связи. Патент РФ на изобретение № 2419153 от 30 июня 2009 г. – 22 с.

20. Белов А. С. и др. Способ (варианты) управления демаскирующими признаками системы связи. Патент РФ на изобретение № 2450337 от 10 мая 2012 г. – 19 с.

УДК 004.77

ПРИМЕНЕНИЕ МЕТОДА АНАЛИЗА ИЕРАРХИЙ В ЗАДАЧЕ ОПТИМИЗАЦИИ САЙТА НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ КОМПАНИИ

Москалева Валерия Дмитриевна, Кривцов Александр Николаевич
Санкт-Петербургский государственный университет,
Россия, Санкт-Петербург, Университетская наб., 7/9,
emails: a_kriv@mail.ru, lera.mosk@gmail.com

Аннотация: В статье представлены результаты применения метода анализа иерархий для решения задачи оптимизации сайта научно-исследовательской компании ООО «Инновационный центр транспортных исследований».

Ключевые слова: *веб-сайт; оптимизация сайта; научно-исследовательская организация*

APPLICATION OF THE HIERARCHY ANALYSIS METHOD IN THE PROBLEM OF OPTIMIZATION OF THE SITE OF THE SCIENTIFIC RESEARCH COMPANY

Moskaleva Valeriia, Krivtsov Alexander
Saint-Petersburg State University,
Russia, Saint-Petersburg, Universitetskaya emb., 7/9,
emails: a_kriv@mail.ru, lera.mosk@gmail.com

Abstract: The article presents the results of applying the hierarchy analysis method to solve the problem of site optimization of a research company.

Keywords*: website; site optimization; research organization*

Введение. Для научно-исследовательских компаний вопросы совершенствования сайтов являются важными и актуальными в связи с расширением базы проведённых научных исследований, распространением сферы деятельности на международный уровень и необходимости в привлечении научных кадров и источников финансирования.

Неотъемлемой частью оптимизации сайта является его грамотный и качественно проведённый аудит. Применение методов технического, текстового, поискового, маркетингового и юзабилити аудита [1] было рассмотрено на примере анализа сайта ООО «Инновационный центр транспортных исследований».

ООО «Инновационный центр транспортных исследований» - это малое инновационное предприятие, созданное в Санкт-Петербургском государственном университете в 2011 году. Сайт данной компании представляет собой её визитную карточку и предназначен для расширения клиентской базы, предоставления пользователям информации о деятельности компании и осуществлении обратной связи.

Следует отметить важность наличия веб-ресурса у научно-исследовательской организации: на сегодняшний день сайт является не только площадкой для размещения материалов по популяризации своих научных открытий, исследований, достижений и привлечения новых кадров через глобальную сеть Интернет. Кроме этого, сайт принимает активное участие в формировании единого информационного пространства, которое объединяет ученых с разных уголков мира и способствует распространению и развитию научных знаний [2]. Веб-ресурс во многом определяет имидж научно-исследовательской компании.

В связи с расширением базы проведённых научных исследований в сфере транспорта и увеличением количества успешно реализованных проектов руководителем ООО «Инновационный центр транспортных исследований» была поставлена задача проведения реинжиниринга сайта с учетом дальнейших международных перспектив расширения деятельности организации. Еще одна важная задача, в решении которой участвует сайт, это поиск источников финансирования. Также в связи с получением патента под проект для Министерства образования и науки Российской Федерации у исследовательского центра появилась необходимость в привлечении научных кадров и разработчиков.

Каждый из пяти упомянутых выше видов аудита сайта затрагивает проверку множества параметров: удобство навигационной структуры, информативность контента, видимость по ключевым фразам семантического ядра и т.д. При проведении подробного аудита сайта необходимо осуществлять проверку всех критериев, однако нередко бывают ситуации, когда в связи с отсутствием времени или ресурсов на проведение подробного анализа, требуется получить экспресс-оценку текущего состояния сайта.

Для определения ключевых критериев оптимальности сайта выполним ранжирование параметров на основании экспертных оценок [3] с помощью метода анализа иерархий (МАИ) [4] в программе MPriority (URL: http://www.tomakechoice.com/mpriority.html).

Верхний уровень иерархии содержит цель проведения ранжирования: получить экспресс-оценку текущего состояния сайта.

Средний уровень иерархии содержит вышеперечисленные виды аудита сайтов:

1. технический аудит,
2. маркетинговый аудит,
3. поисковый аудит,
4. текстовый аудит,
5. юзабилити аудит.

Нижний уровень иерархии содержит критерии оптимальности сайта:

– информативность, полезность, уникальность контента – КОНТЕНТ,
– удобство и понятность навигационной структуры – НАВИГАЦИЯ,
– видимость сайта в различных поисковых системах, оптимизированность в соответствии с семантическим ядром – СЕМ.ЯДРО,
– наличие технических ошибок – ТЕХ.ОШИБ.,
– удобство восприятия текстовых, графических и мультимедийных элементов, представленных на сайте – ЭЛЕМЕНТЫ,
– наличие необходимых контактных данных – КОНТАКТЫ,
– адаптивность и кроссбраузерность сайта – МОБИЛЬНАЯ,
– корректность работы форм обратной связи и отправки сообщений – ФОРМЫ.

Иерархия для ранжирования критериев оптимальности представлена на рисунке 1.

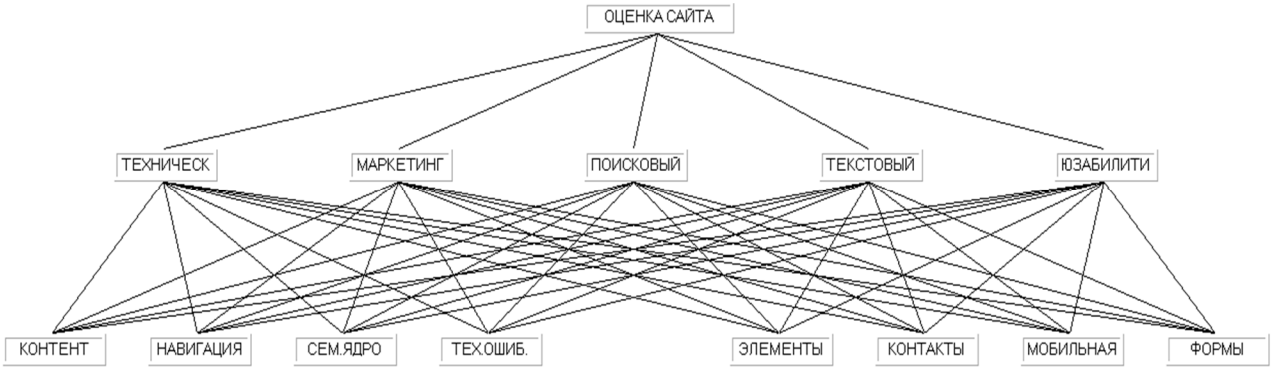


Рис. 1. Иерархия МАИ для ранжирования критериев

На рисунке 2 в качестве примера представлена одна из матриц парных сравнений критериев оптимальности относительно маркетингового аудита.

Работа эксперта

Производим попарные сравнения относительно объекта

МАРКЕТИНГ

		1.	2.	3.	4.	5.	6.	7.	8.	Приоритет
1.	КОНТЕНТ	1	2	3	7	1	3	4	3	0,2387
2.	НАВИГАЦИЯ	1/2	1	3	7	1	3	4	4	0,208
3.	СЕМ.ЯДРО	1/3	1/3	1	2	1/4	3	2	1	0,0833
4.	ТЕХ.ОШИБ.	1/7	1/7	1/2	1	1/4	1/3	1/2	1/4	0,0304
5.	ЭЛЕМЕНТЫ	1	1	4	4	1	5	7	2	0,2299
6.	КОНТАКТЫ	1/3	1/3	1/3	3	1/5	1	3	1/4	0,0573
7.	МОБИЛЬНАЯ	1/4	1/4	1/2	2	1/7	1/3	1	1/7	0,0362
8.	ФОРМЫ	1/3	1/4	1	4	1/2	4	7	1	0,1159

СЗ: 8,6466
ИС: 0,0923
ОС: 0,0655

Применить | Закрыть | Отмена | Исследовать

Рис. 2. Матрица парных сравнений критериев относительно маркетингового аудита

Следует отметить, что все матрицы парных сравнений являются согласованными.

На рисунке 3 представлена матрица парных сравнений видов аудита по важности их вклада в получение общей оценки сайта.

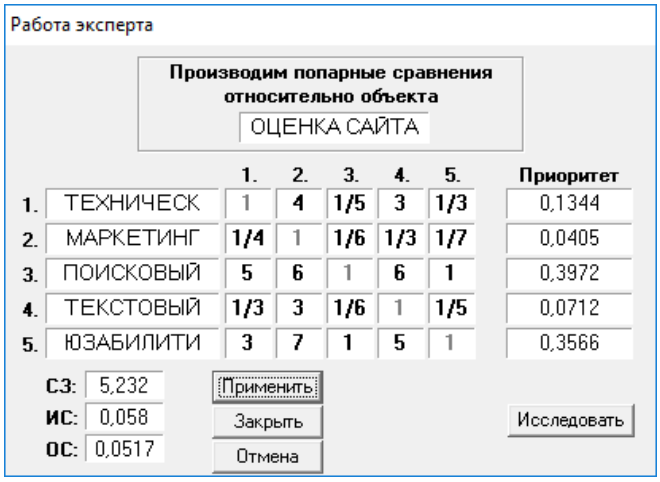


Рис. 3. Матрица парных сравнений видов аудита

Результат ранжирования представлен в таблице 1.

Таблица 1

Результат ранжирования ключевых критериев оптимальности сайта

№	Критерий	Приоритет
1	Видимость сайта в различных поисковых системах, оптимизированность в соответствии с семантическим ядром	0,1993
2	Удобство и понятность навигационной структуры	0,182
3	Информативность, полезность, уникальность контента	0,1655
4	Удобство восприятия текстовых, графических и мультимедийных элементов, представленных на сайте	0,1099
5	Наличие технических ошибок	0,0922
6	Корректность работы форм обратной связи и отправки сообщений	0,0888
7	Наличие необходимых контактных данных	0,0857
8	Адаптивность и кроссбраузерность сайта	0,0762

Из данной таблицы видно, что SEO-оптимизация, удобство навигационной структуры и полезный и уникальный контент являются наиболее значимыми при проведении экспресс-оценки сайта. Это означает, что при разработке нового сайта основное внимание, прежде всего, следует обратить именно на наиболее приоритетные критерии.

В результате проведения подробного аудита сайта были выявлены основные проблемы и узкие места в его организации, а также сформированы рекомендации по реинжинирингу и развитию. На основе сформированных рекомендаций по реинжинирингу сайта было сформировано техническое задание в соответствии с ГОСТ 34.602-89, в результате которого был спроектирован и разработан новый сайт. Для проведения сравнительного анализа старого и нового сайтов и выбора оптимального на основании экспертных оценок также воспользуемся методом анализа иерархий [4].

Верхний уровень иерархии – цель: выбрать оптимальный сайт.

Средний уровень иерархии содержит ключевые критерии оптимальности сайта:

1. информативность, полезность, уникальность контента - КОНТЕНТ,
2. удобство и понятность навигационной структуры – НАВИГАЦИЯ,
3. видимость сайта в различных поисковых системах, оптимизированность в соответствии с семантическим ядром – СЕМ.ЯДРО,
4. наличие технических ошибок – ТЕХ.ОШИБ.,
5. удобство восприятия текстовых, графических и мультимедийных элементов, представленных на сайте – ЭЛЕМЕНТЫ,
6. наличие необходимых контактных данных – КОНТАКТЫ,
7. адаптивность и кроссбраузерность сайта – МОБИЛЬНАЯ,
8. корректность работы форм обратной связи и отправки сообщений – ФОРМЫ.

Нижний уровень иерархии содержит ранжируемые сайты:

— старый сайт (URL: http://innoctr.ru/)

— новый сайт (URL: http://transport-research.org/).

Иерархия представлена на рисунке 4.

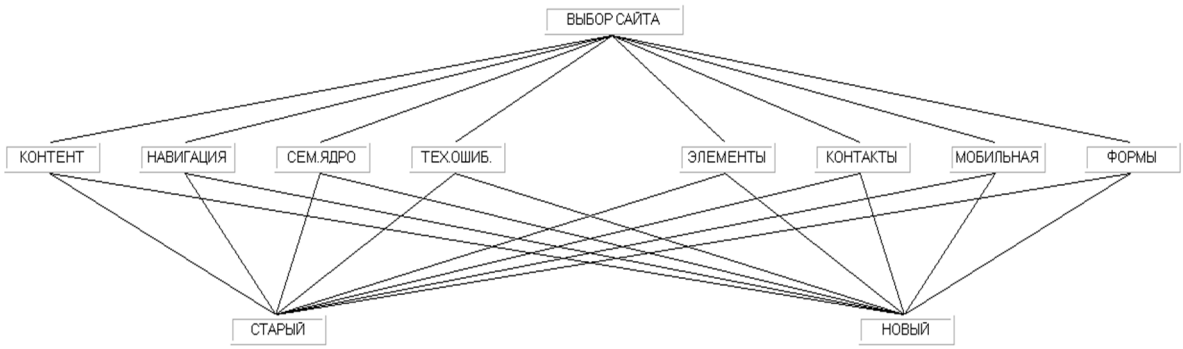


Рис. 4. Иерархия МАИ для выбора оптимального сайта

На рисунке 5 в качестве примера представлена одна из матриц парных сравнений сайтов относительно информативности, полезности и уникальности контента, представленного на сайте.

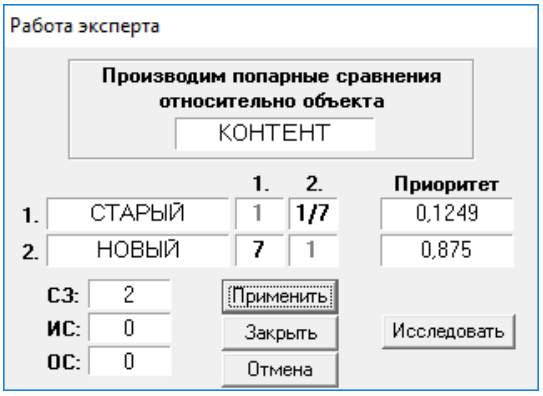


Рис. 5. Матрица парных сравнений сайтов относительно полезности и уникальности контента

Следует отметить, что все матрицы парных сравнений также являются согласованными.

В результате проведённого анализа был получен вектор приоритетов: приоритет нового сайта составил 0,64, а приоритет старого сайта – 0,36. Можно сделать вывод о том, что в результате проведённого сравнительного анализа старого и нового сайтов на основе экспертных оценок было выявлено явное преимущество нового сайта по большинству выделенных ключевых критериев оптимальности.

Заключение. Таким образом, были продемонстрированы результаты применения метода анализа иерархий в решении задачи оптимизации сайтов заданной структуры.

СПИСОК ЛИТЕРАТУРЫ

1. Кривцов, А. Н. Реинжиниринг сайтов: классификация, виды и основные этапы анализа / А. Н. Кривцов, В. Д. Москалева // Развитие технических наук в современном мире: сборник научных трудов по итогам международной научно-практической конференции (11 декабря 2016 г., Воронеж). / Инновационный центр развития образования и науки; ред. Э. К. Аракелян [и др.]. – Инновационный центр развития образования и науки, 2016. № 3. – 128 с. – С. 115-119.
2. Москалева, В. Д. Выбор оптимальной структуры интернет-представительства инновационной исследовательской компании на основе анализа существующих структур сайтов / В. Д. Москалева // Интеллектуальные информационные технологии, энергетика и экономика: сборник трудов XIV международной научно-технической конференции студентов и аспирантов в 3 т. (22-23 июня 2017 г., Смоленск). / Филиал ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске. – ООО «Принт-Экспресс», 2017. – Т. 1. – 244 с. – С. 36-40.
3. Кривцов, А. Н. Применение метода анализа иерархий в задаче выбора системы обеспечения сервиса программно-технического уровня информационной безопасности / А. Н. Кривцов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V-я Международная научно-техническая и научно-методическая конференция: сб. научных статей в 2 т. / ред. С.В. Бачевский, сост. А.Г. Владыко, Е.А. Аникевич, Л.М. Минаков. – СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. Проф. М.А. Бонч-Бруевича, 2016. – Т. 2. – С. 121-127.
4. Саати Т. Принятие решений. Метод анализа иерархий. – М.: Радио и связь, 1993. – 320 с.

УДК 656.02

ЭВРИСТИЧЕСКИЕ ПОДХОДЫ К РЕШЕНИЮ ЗАДАЧ МАРШРУТИЗАЦИИ С ВРЕМЕННЫМИ ОКНАМИ ДЛЯ ОПТИМИЗАЦИИ ПРОЦЕССОВ ОНЛАЙН-РИТЕЙЛА

Котляр Софья Денисовна, Кривцов Александр Николаевич
Санкт-Петербургский государственный университет,
Россия, Санкт-Петербург, ул. Чайковского д.62,
emails: kotlyar.sofya@gmail.com, a_kriv@mail.ru

***Аннотация*:** В статье рассматривается задача маршрутизации с временными окнами, ее роль в процессах Интернет-торговли и подходы к ее решению. Проанализированы возможности применения эвристического подхода к решению данной задачи в рамках совершенствования и модернизации функционала складских и транспортных систем онлайн-ритейла.

***Ключевые слова**: задача маршрутизации; временные окна; эвристические методы*

CONSTRUCTION HEURISTIC FOR SOLVING VEHICLE ROUTING PROBLEM WITH TIME WINDOWS FOR E-FULFILLMENT PROCESS OPTIMIZATION

Kotliar Sofia, Krivtsov Aleksand
The St. Petersburg State University,
Russia, St. Petersburg, Chaykovskogo str. 62,
emails: kotlyar.sofya@gmail.com, a_kriv@mail.ru

Abstract: The article deals with the vehicle problem with time windows, presenting its role in the e-commerce processes and revealing approaches to its solution. The possibilities of applying a heuristic approach to solve this problem are analyzed in the framework of improving and modernizing the functionality of warehouse and transport systems of e-commerce.

***Keywords**: vehicle routing problem; time windows; construction heuristic*

Введение. В электронной коммерции доставки на дом, т.е. процесс доставки товаров из места хранения розничной торговли (например, распределительного центра, магазина) до клиента, играет решающую роль. Фактически, доставка на дом является доминирующем каналом распределения в электронной коммерции B2C («Бизнес-Потребитель»). И хотя, доставка «последней мили» является одной из самых важных направлений цепочки поставок, она в то же время считается на данный момент очень дорогой и неэффективной. Непосредственная доставка заказа клиенту представляет собой вызов, так как потребители должны быть дома, чтобы физически и юридически получать заказы. Для данного типа поставок, предприятия и потребители электронной коммерции должны взаимно договориться о доставке, чтобы избежать дорогостоящих сбоев и проблем поставок. Поэтому определяющей задачей торговли становится выбор временного окна доставки заказа клиенту, а также время начала сборки заказов, так как минимизация времени нахождения собранного заказа позволяет интернет магазинам сокращать издержки на аренду складов и расширять ассортиментный ряд при равной площади склада. Таким образом, возникает тесная связь между системами складского учета и системами управления транспортом. Разработчики систем складского учета стремятся расширить свой функционал с целью удовлетворения растущих потребностей онлайн-ритейла. Одним из направлений совершенствования функционала системы складского учета является автоматизация маршрутизации в рамках системы на основе применения задачи транспортной маршрутизации с временными окнами.

Класс задач, занимающихся поиском оптимальных маршрутов транспортных средств, называют задачами маршрутизации транспортных средств (The vehicle routing problems - VRP). Впервые математическая постановка базовой задачи была сформулирована Г. Данцигом и Дж. Рамсером более 50 лет назад и связана с составлением оптимального набора маршрутов для автопарка транспортных средств с целью обслужить заданное множество клиентов. В данной статье будет рассмотрена задача транспортной маршрутизации с добавлением ограничения на время посещения каждого из клиентов, т.е. задача транспортной маршрутизации с временными окнами (VRP with Time Windows, VRPTW), где клиент может быть обслужен только в пределах заданного временного интервала.

В 1986 году Дж. Джоу адаптировал традиционный алгоритм для решения задач маршрутизации с временными окнами. Эвристика выбирает клиентов в порядке увеличения раннего времени загрузки, вставляет выбранного клиента в самую дешевую возможную позицию на существующих маршрутах или добавляет неиспользуемый автомобиль к проблеме, если ни одна возможная позиция не найдена.

Для однотранспортной задачи с временными окнами Ван дер Брюгген и другие в 1993 году разработал эвристический алгоритм двухфазного локального поиска. Первый этап заключается в построение первоначального маршрута, полученного путем посещения мест в порядке возрастания среднего времени их временного окна, принимая во внимание транспортные ограничения. Первоначальный маршрут по времени может выходить за рамки допустимых значений. Далее, на первоначальный маршрут накладываются штрафные расходы за нарушение временных рамок и во второй фазе маршрут улучшается последовательной перестановкой заказов [1].

В 1995 году Иоачим предложил приближенный алгоритм для мультитранспортной задачи с временными окнами. Алгоритм сначала создает набор кластеров путем решения сокращенной задачи, используя генерацию столбцов. Каждый кластер представляет собой небольшой маршрут, посещающий определенное число клиентов. Затем с помощью решения задачи множественного коммивояжера получается последовательность кластеров, формирующая единый конечный маршрут[2].

В 2000 году Нанри и Барнс представляют реактивный алгоритм табу-поиска (или поиска с запретами, “tabu search”) для решения мультитранспортной задачи. Первоначальные маршруты формируются с помощью «жадного» метода вставки. Затем для улучшения первоначального маршрута применяется реактивный табу-поиск с тремя предлагаемыми соседями [3].

В 2001 году Ландрье сформулировал вероятностный табу-поиск (tabu-search), «поиск с запретами», для решения однотранспортной задачи. В том же году Ли и Лим предложили метаэвристический подход для многотранспортной задачи VRPTW. Вначале находится локальный оптимум, основанный на трех известных соседях. Затем с помощью симуляции и применения методики табу поиска для избежания циклования улучшается локальный оптимум путем многократного перезапуска вариантов [4].

В 2002 году Лао и Лианг презентовали двухфазный алгоритм для мультитранспортной задачи. В рамках первой фазы происходит кластеризация точек, строится маршрут, который будет выполняться каждым транспортным средством. На второй фазе полученное решение улучшается с помощью табу поиска [5].

В 2004 году Диана и Дессуки представили параллельный регрессионный метод эвристики для нахождения оптимального маршрута [6].

Ниже представлено описание математической модели задачи VRPTW.

Пусть имеется некоторый направленный граф G=(V,A) с множеством вершин |V|=n+2, так что n вершин представляют n клиентов, и A – множество дуг графа. Вершина 1-го поставщика чаще обозначается как депо (depot) или склад, с которого товары развозятся по клиентам. Таким образом, депо описывается двумя вершинами 0 и n+1, как представлено на рисунке 1.

Предположим, что K множество транспортных средств и |K|=m, m — количество машин. Каждый

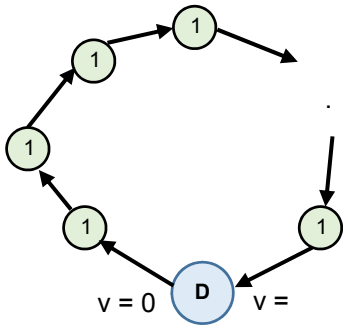


Рис. 1 Графическая презентация задачи VRP

клиент i обслуживается в течение времени обслуживания si. Время обслуживания в депо s0, т.е. время необходимое на загрузку заказов, не учитывается в задаче и равно нулю, так как комплектация товара происходит заранее и входит в задачу складского процесса. Время возвращения в депо sn + 1 также нулевое, s0 = sn + 1 = 0. Объем заказа, поставляемого i-му клиенту, обозначается буквой qi, Q обозначает пропускную способность транспортного средства. Пусть tij обозначает время, необходимое для перемещения от клиента i к клиенту j, и cij, (i, j) ∈A - стоимость поездки от клиента i к клиенту j. Бинарная переменная $xijk$, (i, j) ∈A, k∈K равна 1 тогда и только тогда, когда путь (i, j) обслуживается транспортным средством k. Предположим также, что δ + (i) = {j: (i, j) ∈A} и δ- (j) = {i: (i, j) ∈A}.

Чтобы сформулировать задачу с временными окнами необходимо ввести следующие параметры:

– [a_i,b_i]− временной интервал доставки для выполнения запроса клиента i∈N=V\{0,n+1}
– [a_0,b_0],[a_{n+1},b_{n+1}]− временной интервал для депо
– a_0=$min_{i∈N}\{a_i-t_{0i}\}$
– b_0=$max_{i∈N}\{b_i-t_{0i}\}$
– a_{n+1}=$min_{i∈N}\{a_i+s_i+t_{i,n+1}\}$
– b_{n+1}=$max_{i∈N}\{b_i+s_i+t_{i,n+1}\}$
– w_i^k, i∈N, k∈K – момент времени, когда транспортное средство k начинает обслуживание клиента i

Таким образом, каждые две клиентские вершины, связанные ребром в рамках маршрута, описываются следующим образом, как показано на рисунке ниже (Рис.2):

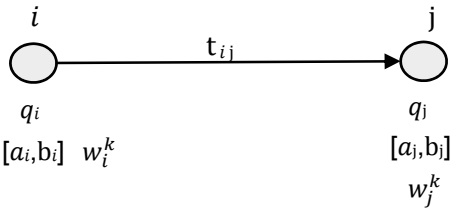


Рис. 2 Часть маршрута в VRPTW

Согласно Барнхарту и Лапорту [7] модель VRPTW может быть описана как модель многотоварного сетевого потока с временными окнами и ограничением по грузоподъемности следующим образом:

$$min \sum_{k \in K} \sum_{(i,j) \in A} c_{ij}\, x_{ij}^k$$

при условии:

$$\sum_{k \in K} \sum_{j \in \delta+(i)} x_{ij}^k = 1,\ i \in N \quad (1)$$

$$\sum_{j \in \delta+(0)} x_{0j}^k = 1,\ k \in K \quad (2)$$

$$\sum_{j \in \delta-(j)} x_{ij}^k - \sum_{j \in \delta+(j)} x_{ij}^k = 0,\ k \in K, j \in N \quad (3)$$

$$\sum_{j \in \delta-(n+1)} x_{i,n+1}^k = 1, k \in K \quad (4)$$

$$x_{ij}^k\ (w_i^k + s_i + t_{ij} - w_{ij}^k) \leq 0,\ k \in K,\ (i,) \in A \quad (5)$$

$$a_i \leq\ w_i^k \leq\ b_i,\ k \in K,\ \ i \in V \quad (6)$$

$$\sum_{i \in N} q_i \sum_{j \in \delta+(i)} x_{ij}^k\ \leq Q, k \in K \quad (7)$$

$$x_{ij}^k \in \{0,1\},\ k \in K,\ (i,j) \in A \quad (8)$$

Целевая функция направлена на минимизацию общих затрат на маршрутизацию транспортных средств. Ограничения (1) и (2) указывают, что каждый клиент должен посещаться ровно один раз, и каждое транспортное средство должно использоваться ровно один раз, что означает, что у каждого транспортного средства есть только один маршрут. Ограничения (3) и (4) необходимы для обеспечения того, чтобы не нарушалась консистенция потока в каждой вершине маршрута: начиная маршрут, каждое транспортное средство выходит из депо ровно один раз и в конце его маршрута возвращается в депо также ровно один раз; если автомобиль прибывает к клиенту, он должен покинуть этого клиента после завершения службы доставки. Следующие два ограничения используются для устранения подциклов и обеспечения согласованности окон времени. Ограничения (7) определяют ограничение грузоподъемности (ёмкости) транспортного средства. Последнее выражение определяет формат переменной принятия решения x_{ij}^k .

Следует отметить, что описанная выше модель VRPTW предполагает, что обслуживание клиента не может начаться раньше установленного времени, даже если автомобиль прибыл на место раньше.

Проблема VRPTW является NP-трудной задачей. И, хотя существуют некоторые точные алгоритмы, которые используют методы математического программирования для нахождения оптимального решения VRPTW, эти алгоритмы обычно позволяют решить обсуждаемую проблему только для случаев, в которых используется до 100 клиентов в течение соответствующего периода времени. Следовательно, многие исследования сосредоточены на разработке соответствующей эвристики для решения VRPTW, именно поэтому основное внимание в литературе и исследованиях уделяется эвристическим алгоритмам.

Эвристические подходы являются мощной альтернативой точным методам решения VRPTW, поскольку они способны довольно быстро по сравнению с точными методами разрабатывать решения соответствующего качества.

Первый класс эвристики – конструктивная эвристика – нацелен на то, чтобы построить допустимое решение, путем вставки в частичные маршруты клиентов, которые будут посещаться один за другим. Процедуру вставки можно выполнить последовательно или параллельно. Каждая конструктивная эвристика определяется и отличается выбором, сделанным для двух основных вариантов:

— последовательность вставки клиентов в маршрут

— между какими двумя соседствующими в текущем маршруте клиентами выбранный клиент должен быть вставлен.

Алгоритм эвристической вставки «Insertion heuristic I1» последовательно организует маршруты и нацелен на максимизацию выгоды посещения клиента не по прямому маршруту, а по частичным составляющим. Соответствующий алгоритм включат следующее:

Инициализация:

– выбор изначального клиента:

1 вариант: первый клиент – самый дальний, не добавленный в маршрут, клиент

2 вариант: первый клиент – не добавленный в маршрут клиент с самой ранней верхней границей временного окна доставки

Итерация:

– последовательность: выбор из оставшихся клиентов одного с максимальным сберегающим значением, принимая во внимание расстояние от депо и затраты на вставку

– место: добавление выбранного клиента в текущий маршрут на позицию, минимизируя стоимость меры дополнительного времени и дополнительного расстояния, необходимого для посещения клиента

Терминация:

1 случай: все клиенты добавлены в маршрут

2 случай: невозможно найти следующего клиента с допустимым вариантом вставки в маршрут, т.е. добавление в маршрут клиента вызовет нарушение некоторых ограничений

Если на этапе завершения имеет место второй случай, текущий маршрут должен быть завершен, и новый маршрут должен быть инициализирован. Алгоритм повторяется до тех пор, пока не наступит первый вариант терминации, то есть больше не останется клиентов, которые должны быть посещены.

Следующий класс эвристики для решения VRPTW задач - это улучшенная эвристика. Она применяется для того, чтобы улучшить исходно созданное возможное решение итеративно, не нарушая допустимости решения. На каждой итерации происходит некоторый обмен, «улучшение». Процедура улучшения обычно заканчивается, если не существует более возможных обменов, которые не ухудшат решение.

Одним из типов обменной эвристики является 2-opt* эвристика Соответствующая процедура состоит из следующих шагов (Рис. 3):

— выбрать два маршрута – $k1$ и $k2$

— исключить последних $n1$ клиентов из маршрута $k1$

— вставить последние $n1$ клиента, удаленных из $k1$, после первых $n2$ клиентов маршрута $k2$

— соединить начальную часть маршрута $k1$ с заключительной частью маршрута $k2$

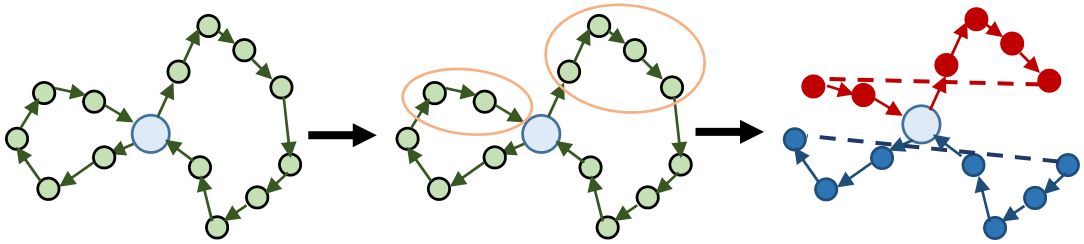


Рис. 3 Иллюстрация пошаговой процедуры 2-opt*алгоритма

Наиболее важным свойством 2-opt* эвристики является то, что алгоритм сохраняет ориентацию измененных подмаршрутов.

И последний, но не менее важный класс эвристических подходов, рассматриваемых в этой статье, называется метаэвристика. Алгоритмы такого рода продолжают исследование поискового пространства даже после нахождения локального минимума. Для VRPTW разработан широкий спектр метаэвристик. Среди них следует выделить две большие группы[7]:

— Эвристика на основе генетических алгоритмов

— Эвристика на основе поиска с запретами («tabu search»)

Первая группа - генетические алгоритмы - применяет фундаментальные принципы эволюционных алгоритмов, а вторая группа использует процедуру поиска с запретами в разных вариантах. Метаэвристика обычно состоит из нескольких этапов, сначала нахождение исходного решения, а затем попытки улучшить его. С целью иллюстрации механизма поиска решения VRPTW с помощью метаэвристического алгоритма была выбрана эвристика поиска с запретами для VRPTW проблем. [8]

Эвристика поиска с запретами для VRPTW управляет специальным пулом маршрутов, называемым адаптивной памятью. Этот пул состоит из маршрутов, которые были выбраны из лучших решений, полученных во время поиска. Вначале адаптивная память заполняется P различными начальными решениями, построенными с использованием рандомизированной эвристической эвристики.

На рисунке 4 белые круги обозначают клиентов, черные квадраты определяют депо. На первом шаге некоторые фрагменты исключаются из двух маршрутов: участки ($X1$,$X1'$), ($Y1$,$Y1'$) из первого маршрута, участки ($X2$,$X2'$), ($Y2$,$Y2'$) из второго. После этого проектируются новые маршруты путем создания ребер ($X1$,$X2'$), ($Y2$,$Y1'$), ($X2$,$X1'$) and ($Y1$,$Y2'$).

На этапе улучшения эвристического алгоритма поиска с запретами применяется специальный оператор обмена CROSS (рис.4).

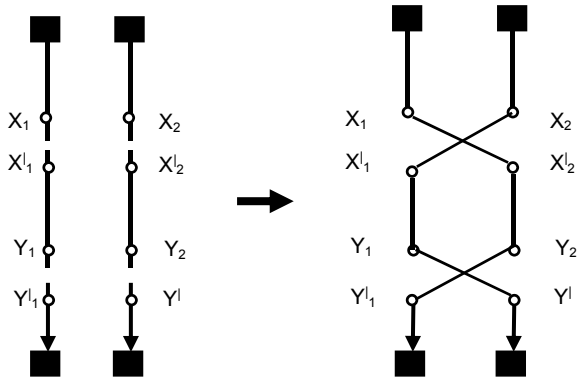


Рис. 4 Пример CROSS обмена

Основные шаги эвристического алгоритма поиска с запретами для VRPTW представлены ниже:

Инициализация:

– построение первоначального решения путем объединения маршрутов, взятых из адаптивной памяти

– разделение выбранных маршрутов на подмножества, каждое из которых буден задано как входные данные для процедуры поиска с запретами

Итерация:

– улучшение исходного решения с помощью табу-поиска в сочетании с оператором обмена CROSS

– если полученные результаты лучше, происходит помещение их в адаптивную память

Терминация*:*

– табу-поиск останавливается после определенного количества выполненных итераций (рассчитанных по специальной формуле)

Индивидуальные маршруты обрабатываются особым образом после нахождения окончательного наилучшего решения.

Заключение. Таким образом, можно предположить, что рассмотренные эвристические подходы к решению задач маршрутизации с временными окнами для оптимизации процессов онлайн-ритейла составят основу автоматизации этих задач и будут одним из направлений совершенствования функционала системы складского учета.

СПИСОК ЛИТЕРАТУРЫ

1. Van der Bruggen, L.J.J., Lenstra, J.K., Schuur, P.C., 1993.Variable-depth search for the single vehicle pickup and delivery problem with time windows. Transportation Science 27, 298–311.
2. Ioachim, I., Desrosiers, J., Dumas, Y., Solomon, M.M., Villeneuve, D., 1995. A request clustering algorithm for door-to-door handicapped ‘‘transportation’’. Transportation Science 29 (1), 63–78.
3. Nanry, W.P., Barnes, J.W., 2000. Solving the pickup and delivery problem with time windows using reactive tabu search. Transportation Research B 34 (2), 107–121.
4. Li, H., Lim, A., 2001. A metaheuristic for the pickup and delivery problem with time windows. In: Proceedings 13th IEEE ICTAI 2001, Los ALAmitos, CA, pp.160-167
5. Lao, H.C., Liang, Z., 2002. Pickup and delivery with time windows: Algorithms and test case generation. International Journal on Artificial Intelligence Tools (Architectures, Languages, Algorithms) 11 (3), 455–472.
6. Diana, M., Dessouky, M.M., 2004. A new regret insertion heuristic for solving large-scale dial-a-ride problems with time windows. Transportation Research B 38, 539–557.
7. Barnhart C., Laporte G. (Eds.), (2007). Handbook in OR & MS, Vol. 14, 367–428
8. Taillard, É.D., Badeau, P., Gendreau, M., Guertin, F., Potvin, J.-Y. (1997). A tabu search heuristic for the vehicle routing problem with soft time windows. Transportation Science, 170–186.

УДК 004.056

УГРОЗЫ БЕЗОПАСНОСТИ VOIP

Полугина Юлия Константиновна
ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова»,
Россия, Санкт-Петербург, ул. Двинская, 5/7,
email: u13-@mail.ru

***Аннотация*:** В статье рассматривается основные способы взлома и хищения трафика в телефонных сетях нового поколения – VOIP сетях. Выявлены наиболее критичные уязвимости данной технологии передачи голосовых данных и предложены методы исключения несанкционированных действий путем построения правильной архитектуры сети и соблюдением рекомендуемых мер и политик безопасности.

***Ключевые слова**: VOIP; безопасность; перехват трафика; firewall; телефония.*

SECURITY THREATS OF VOIP

Polugina Julia
Admiral Makarov SUMIS",
Russia, St. Petersburg, Dvinskaya str, 5/7
email: u13-@mail.ru

Abstract: The article considers the main ways of hacking and stealing traffic in next-generation telephone networks - VOIP networks. The most critical vulnerabilities of this technology for voice data transmission are identified and methods for eliminating unauthorized actions are proposed by building the correct network architecture and observing the recommended security measures and policies.

Keywords*: VOIP; security; interception of traffic; firewall; telephony.*

Введение. VOIP – новая технология, которая несет с собой не только новые возможности передачи данных, но новые угрозы для взлома, кражи и мошенничества. В отличие от традиционной телефонии, VOIP обеспечивает передачу данных по протоколу IP, в частности, могут быть использованы сторонние IP сети и общедоступная сеть Интернет. Передача незащищенных данных представляет собой привлекательную цель для взлома. Перенаправление, хищение трафика оказывают серьезное влияние на коммуникацию компаний, помимо возможного хищения конфиденциальных данных телефонных разговоров. Именно поэтому задача обеспечения безопасной передачи данных в VOIP является актуальной задачей, которая требует постоянной актуализации в разрезе активно развивающихся технологий.

Возможные варианты взлома

Прослушивание устройств и автоподбор. Практически любой тип устройства можно отыскать в сети автоматизированным способом, т.к. оно отвечает на ряд типичных для данного вида устройств запросов. Так и VOIP оборудования постоянно находится в режиме «прослушивания» VOIP сигналов. После обнаружения необходимого устройства начинается подбор логина и пароля устройства. Такой метод возможен, если клиентские устройства и шлюзы выведены непосредственно в сеть Интернет, без использования шлюзов, firewall и транков.

Доступ к абоненту внутренней телефонной сети через DISA. DISA – функция, позволяющая после набора основного номера телефона указать дополнительный номер абонента во внутренней сети в тональном режиме. Служит для организации работы автоматического секретаря. В данном случае злоумышленник может для выясненного по DISA внутреннего номера подобрать в автоматическом режиме пароль и получить авторизацию на чужой АТС.

Инъекция компрометирующих данных в общий трафик VOIP. Поскольку VOIP - пакетная передача данных, значит, в общий поток данных со взломанной АТС можно добавить сторонние данные-команды для попытки получения доступа к другой АТС.

DoS атака. Самый простой, эффективный и самый убыточный для атакуемой компании способ вывода из строя телефонии. Данный способ атаки достаточно легко осуществить, если IP АТС подключена к оператору связи через Интернет и не защищена промежуточными устройствами. АТС напрямую получает огромное количество запросов, которые просто не в состоянии обработать и телефония оказывается парализована.

SPIT spam. Вариант рассылки голосового спама, используя голосовое меню автоответчиков или автоматического секретаря с тоновым набором. Данный вариант не в полной мере относится к вариантам взлома, т.к. требует ответных действий от абонента, которому пришел спам. Абонент может осуществить ответный звонок на источник спама и неосознанно предоставить некоторые данные, которые могут быть использованы для взлома, такие как внутренний номер, логин, пароль для авторизации на АТС. Иногда этих данных может быть достаточно для следующего метода взлома.

Перехват сеанса, перехват данных. Злоумышленник может перехватить данные от клиента к его АТС, подменив часть/полностью данные и получить недостающие данные от клиента, не подозревающего о вводе пароля, например, на сторонней АТС.

Сканирование портов. По-умолчанию VOIP АТС использует порты 5060, 9000-9049 для передачи данных. На эти порты в первую очередь будут проводиться атаки. Помимо этого не некорректно настроенная АТС может иметь «открытые» порты, через которые можно получить к ней доступ (22-ssh, например)

Использования трафика злоумышленниками

В зависимости от типа взломанного устройства и мотивов злоумышленников зависит последующий ущерб.

– Нанесение экономического ущерба компании путем вывода из строя АТС
– Использование АТС для осуществления звонков за чужой счет
– Увеличение счета на оплату аренды АТС путем генерации несуществующего трафика
– Хищение конфиденциальных данных сотрудников (например, личные номера телефонов, на которые настроена переадресация)
– Хищение данных для последующей рассылки спама

– Прослушивание чужих звонков
– Сбор и использование данных о звонках

Необходимые меры безопасности

Запрос выделенной голосовой VLAN – виртуальной сети для подключения VOIP-транка к оборудованию провайдера, вместо подключения к провайдеру через Интернет. Отсутствие прямого доступа к сети значительно усложнит задачу взлома мошенниками.

Использование VLAN для отделения VOIP трафика от прочего трафика данных. Пример использования виртуальной сети проиллюстрирован на рис.1

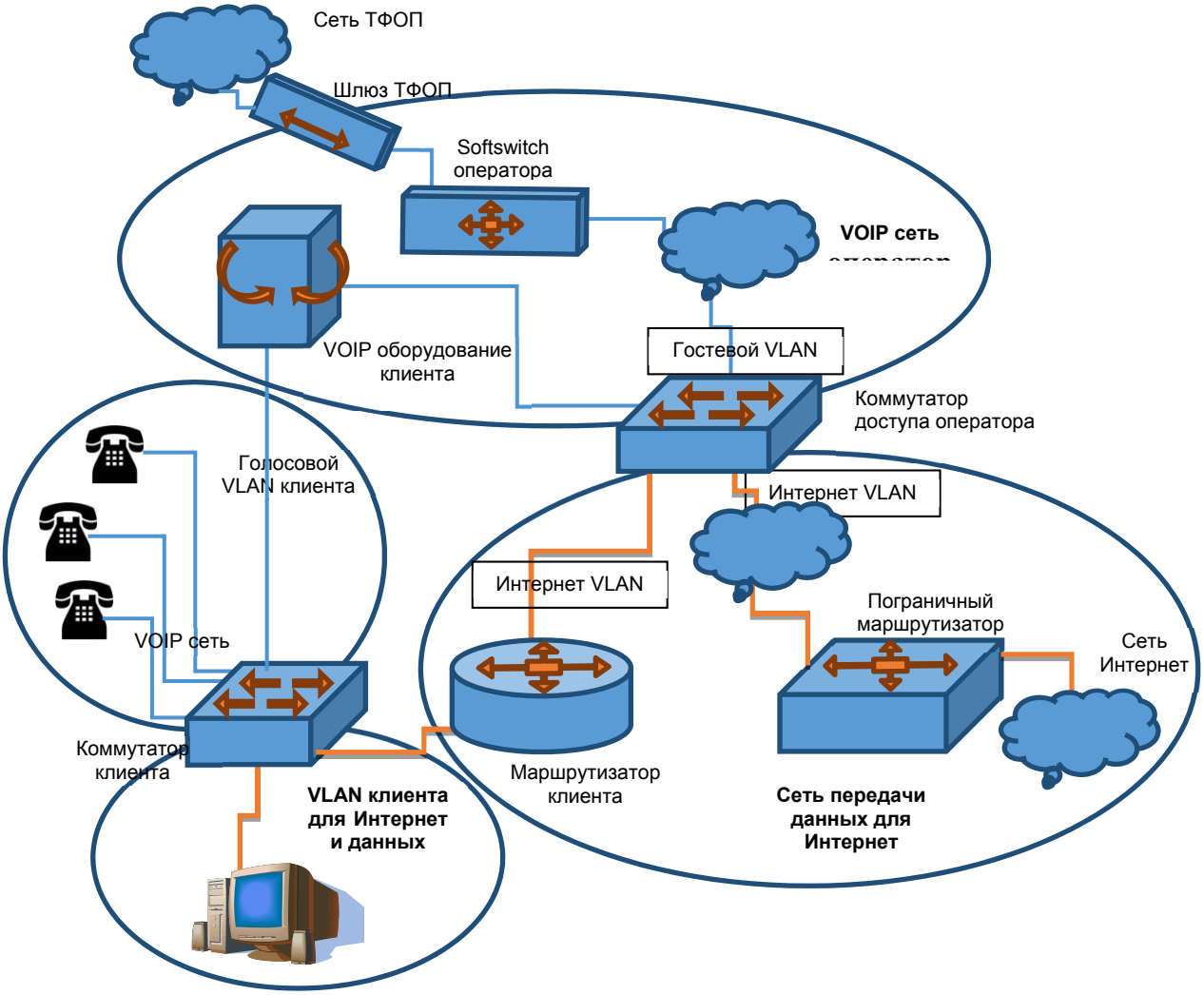


Рис. 1. Использование VLAN для отделения VOIP

Многослойность. Защита VOIP оборудования путем «закрытия» его firewall-ом. Этот метод позволяет избежать DoS атак непосредственно на АТС. Существует специализированное оборудование, которое способно обрабатывать большое число запросов, распределять трафик, блокировать атаки. Такое оборудование должно быть у любой компании, обеспокоенной защитой своей сети, не только защитой своей телефонии.

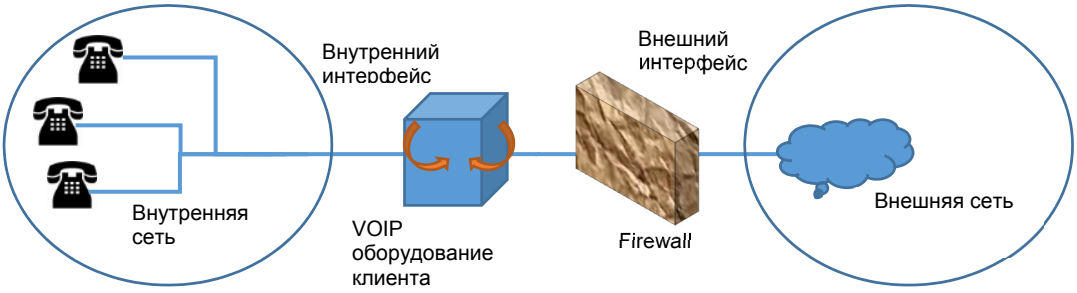


Рис. 2. Использование firewall

Ограничение физического доступа. Немаловажным фактором является возможность физического доступа к оборудованию, как на территории компании, так и в дата-центрах.

Порты и ограничения. Использование нестандартных портов для управления значительно повысит безопасность. Помимо этого, не лишним будет закрытие не используемых портов и установка определенных правил доступа. Так самое простое правило для доступа к АТС лишь с определенных IP адресов убережет от потенциального взлома.

Обновления. Любое оборудование и программное обеспечение устаревает и всегда есть вероятность обнаружения «дыры в безопасности». Своевременное обновление ПО и замена устаревшего оборудования сводят к минимуму опасность кражи данных.

Шифрование. Этот способ борьбы целесообразно включать лишь при осуществлении звонков вне корпоративной сети, т.к. любое шифрование добавляет «вес» передаваемому трафику, нагружает сеть передачи данных. Но в то же время обеспечивает конфиденциальность разговоров именно там, где они больше всего подвержены атакам – в сети Интернет.

Клиентское оборудование. Конечные пользователи пользуются физическими телефонами или программным обеспечение, оба варианта подключаются к АТС по логину/паролю и могут быть уязвимы. Обновление ПО машины, где установлен VOIP-клиент и защита надежными паролями физических устройств – обязательный пункт.

Внутренние политики безопасности. Введение обязательных требований к сложности логина/пароля, ограничение на звонки группах пользователей, логирование работы системы – все эти меры помогут внутри компании настроить правила и политики пользования АТС, которые могут предотвратить несанкционированные действия из вне.

Заключение. В век высоких технологий самой ценной валютой становится информацию, получить которую можно все большим числом способов. Защита информации, передаваемой от VOIP АТС – является комплексной задачей, включающей все аспекты организации защиты объектов информатизации – от ограничения физического доступа и защиты firewall-ом, до соблюдения внутренних политик безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Баталова Н. Безопасность VoIP у операторов связи: "классика" IP-сетей и новые задачи // Connect! Мир связи. – 2011. – № 6.
2. Вихров Н.М., Ныркова А.П., Шнуренко А.А., Соколов С.С., Некрасова А.А., Полугина Ю.К. Современные методы оптимизации передачи данных в информационно-вычислительных сетях на транспорте // Морской вестник. – 2017. - №1. – С. 95-98.
3. Куриленко Е. Гибридные IP-АТС Yeastar MyPBX U-серии // Технологии и средства связи. – 2013. – № 2. – С. 22–23.
4. Ныркова А.П. Обеспечение необходимого режима информационной защищенности активов мультисервисной сети транспортной отрасли / А.П. Ныркова, С.С. Соколов, Е.А. Мустакаева, В.А. Мальцев // Проблемы информационной безопасности. Компьютерные системы. –2014. – № 1. – С. 47-51.
5. Ныркова А.П., Соколов С.С., Башмаков А.В. Методика проектирования безопасных информационных систем на транспорте // Проблемы информационной безопасности. Компьютерные системы. – 2010. –№ 3. – С. 58–61.
6. Сети ЭВМ: протоколы стандарты, интерфейсы. Ю. Блэк; перев. с англ. - М.: Мир, 1990.
7. Ушанев К.В., Макаренко С.И. Преобразование структуры трафика с учетом требований по качеству его обслуживания // Радиотехнические и телекоммуникационные системы. 2015. № 2 (18). С. 74-84.
8. Hedrick C.L. Routing Information Protocol. RFC 1058, 1988.
9. H. Takagi. Explicit delay distribution in first-come first-served M/M/m/K and M/M/m/K/n queue and a mixed loss-delay system // in Proceedings of Asia-Pacific Symposium on Queueing Theory and Its Applications to Telecommunication Networks, Seoul, Korea, 2006.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СОЦИОКОМПЬЮТИНГЕ

УДК 57.054

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ЗАЩИТЫ ОТ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ С ПОМОЩЬЮ РЕЗОНАТОРОВ

Копыльцов Александр Васильевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
email: kopyl2001@mail.ru

***Аннотация*:** В статье рассмотрена задача математического моделирования взаимодействия резонаторов «АЙРЭС» с электромагнитным излучением. Резонатор «АЙРЭС» представляет собой кремниевую пластинку (диаметр 7,5 мм, толщина 1 мм), на которой методом травления по определенному алгоритму нанесены круговые щели (шириной 1 мкм и глубиной 1,2 мкм), рисунок которых выполнен на основе аффинных преобразований. Пластинка изготавливается из кремния, текстолита и других диэлектриков. Линейные размеры пластинки (диаметр, толщина) и щелей (ширина, глубина) могут достигать нескольких сантиметров и миллиметров, соответственно. При взаимодействии электромагнитного поля с резонатором наблюдается отражение, преломление и поглощение. При моделировании рассматривались различные варианты облучения. По длине волны расчеты проводились от долей микрометра до нескольких десятков сантиметров, т.е. от видимого света до радиоволн. Облучение осуществлялось как от дискретного количества источников (от одного до нескольких сотен), так и непрерывного (от пластин и полусфер). Если на пластинку падает волна с некоторой частотой, то результирующая волна, отходящая от пластинки, представляет собой суперпозицию двух волн (за счет падающей волны и за счет слабо связанных электронов атомов пластинки). Расчеты на компьютере показали, что результирующая волна имеет другие характеристики по сравнению с падающей волной (над центральной частью резонатора период колебаний увеличивается в 3,2 раза, а частота убывает в 3,2 раза), т.е., резонатор работает как преобразователь частоты электромагнитного излучения.

***Ключевые слова**: электромагнитное излучение; взаимодействие с веществом; математическое моделирование; защита от излучения.*

MATHEMATICAL MODELING OF PROTECTION AGAINST ELECTROMAGNETIC RADIATION BY MEANS OF RESONATORS

Alexander Kopyltsov
Saint- Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str., 5,
email: kopyl2001@mail.ru

***Abstract*:** In the article the problem of mathematical simulation of the interaction of "AIRES" resonators with electromagnetic radiation is considered. Resonator "AIRES" is a silicon plate (diameter 7.5 mm, thickness 1 mm), on which etched by a certain algorithm, circular slots (1 μm wide and 1.2 μm deep), whose pattern is made on the basis of affine transformations. The plate is made of silicon, textolite and other dielectrics. Linear dimensions of the plate (diameter, thickness) and slits (width, depth) can reach several centimeters and millimeters, respectively. When the electromagnetic field interacts with the resonator, reflection, refraction and absorption are observed. Various types of irradiation were considered in the simulation. The wavelengths were calculated from micrometer fractions to several tens of centimeters, i.e. from visible light to radio waves. Irradiation was carried out both from a discrete number of sources (from one to several hundred), and continuous (from plates and hemispheres). If a wave with a certain frequency falls on the plate, then the resulting wave from the plate is a superposition of two waves (due to the incident wave and due to the weakly bound electrons of the plate atoms). Calculations on the computer showed that the resulting wave has other characteristics in comparison with the incident wave (the oscillation period increases 3.2 times, and the frequency decreases 3.2 times), that is, the resonator works as a frequency converter for electromagnetic radiation.

***Keywords:** electromagnetic radiation; interaction with matter; mathematical modeling; protection against radiation.*

Введение. Резонатор «АЙРЭС» представляет собой кремниевую пластинку (диаметр 7,5 мм, толщина 1 мм), на которой методом травления по определенному алгоритму нанесены круговые щели (шириной 1 мкм и глубиной 1,2 мкм), рисунок которых выполнен на основе аффинных преобразований. Пластинка изготавливается из кремния, текстолита и других материалов. Линейные размеры пластинки (диаметр, толщина) и щелей (ширина, глубина) могут достигать нескольких сантиметров и миллиметров, соответственно. При взаимодействии электромагнитного поля с резонатором наблюдается его отражение, преломление и поглощение [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11].

В экспериментах, проведенных на крысах линии Вистар, помещенных в клетку Фарадея и подвергнутых электромагнитному облучению с помощью Wi-Fi роутера, показано, что генетические характеристики крыс отличаются в зависимости от наличия или отсутствия резонаторов, а так же от их количества расположенных на стенках клетки Фарадея [12].

При моделировании рассматривались различные варианты облучения. По длине волны расчеты проводились от долей микрометра до нескольких десятков сантиметров, т.е. от видимого света до радиоволн. При моделировании облучение осуществлялось как от дискретного количества источников (от одного до нескольких сотен), так и непрерывного (от пластин и полусферы). Если на пластину падает волна с некоторой частотой, то результирующая волна, отходящая от пластины представляет собой сумму двух слагаемых (за счет отражения и за счет электронов атомов пластинки).

Рассматривалась освещенность крыс Wi-Fi роутером. Освещенность прямо пропорциональна интенсивности излучения и косинусу угла между нормалью к освещаемой поверхности и направлением падающего излучения и обратно пропорциональна квадрату расстояния от источника излучения до освещаемой пластинки. Расчеты на компьютере показали, что если мощность источника равна 0,25 Вт (максимум 0,6 Вт, в России максимум 0,25 Вт) и расстояние от источника излучения до поверхности равно 0,5 м, то освещенность этой поверхности равна 0,1-0,2 лк. Если же на стороны клетки Фарадея повесить 4 резонатора, то освещенность поверхности увеличится примерно на 10 % на частоте падающего излучения. Появится также освещенность за счет отражения от резонаторов на частоте в 3,2 раза меньшей частоты падающего излучения, т.е., резонатор работает как преобразователь частоты электромагнитного излучения (Рисунок 1, Рисунок 2, Рисунок 3).

Описание модели. Облучение пластинки резонатора электромагнитным полем порождает смещения слабо связанных внешних электронов атомов пластинки, что приводит к генерации поля испускаемого атомными электронами. В результате электрическое поле испускаемой резонатором волны является суперпозицией поля испускаемого атомными электронами и поля падающей волны

$$E = \Delta E_0 \cos(\theta - \frac{\pi}{2}) + E_0 \cos\theta, \quad (1)$$

где

$$\theta = \omega(t - \frac{z}{c}), \quad (2)$$

$$\Delta E_0 = \frac{2\pi k_0 n_e e^2 \omega}{c m_e (\omega_0^2 - \omega^2)} E_0 \Delta z, \quad (3)$$

$$\omega_0 = \sqrt{\frac{4\pi k_0 e\rho}{m_e}} \quad (4)$$

частота колебаний электрона в равномерно заряженной пластинке, ne – концентрация электронов, $\rho = n_e e$ - заряд единичного объема пластины, e – заряд электрона, me – масса электрона, Δz - толщина пластины, c – скорость света, k0 =9 109 Н м2/Кл2 - постоянная [13].

Напряженность электрического поля описывается уравнением

$$\frac{\partial^2 E}{\partial t^2} = \mathrm{D}_3 \left(\frac{\partial^2 E}{\partial x^2} + \frac{\partial^2 E}{\partial y^2} + \frac{\partial^2 E}{\partial z^2} \right), \quad (5)$$

где D3 - коэффициент, t – время, x, y, z – декартовые координаты.

Рассматривались различные варианты граничных и начальных условий, в частности, без учета или с учетом взаимовлияния напряженности на резонаторах и в окружающем пространстве, наличие или отсутствие стоков в центре или по краям резонатора.

Освещенность, создаваемая точечным источником, плоской поверхности

$$J = \frac{I \cos\alpha}{r^2}, \quad (7)$$

где I – сила света, α - угол между нормалью к поверхности и направлением светового потока, r – расстояние от источника до освещаемой поверхности.

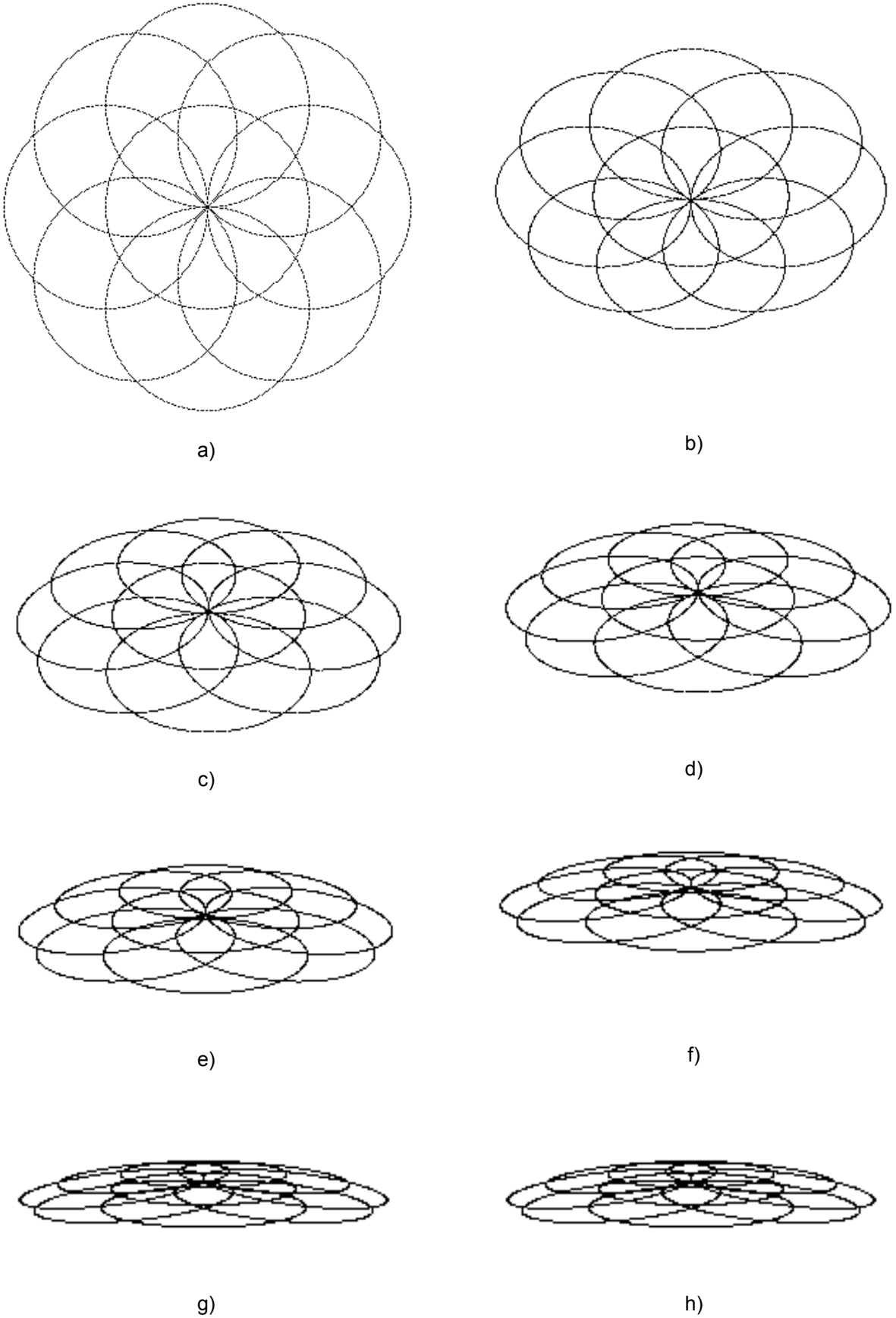


Рис. 1. Результирующее излучение от резонатора на пластину расположенную под разными углами к плоскости резонатора: a) 0 рад, b) 1/16 π рад, c) 2/16 π рад, d) 3|16 π рад, e) 4/16 π рад, f) 5/16 π рад, g) 6/16 π рад, h) 7/16 π рад.

Применяя численные методы для решения системы уравнений с соответствующими начальными и граничными условиями, определяем напряженность поля *E* в пространстве. Расчеты проводились при следующих параметрах: частота облучения $w=5,5*10^{14}$ Гц, шаг по пространству h=0,84 мм, шаг по времени $ht=1,14*10^{-16}$ с.

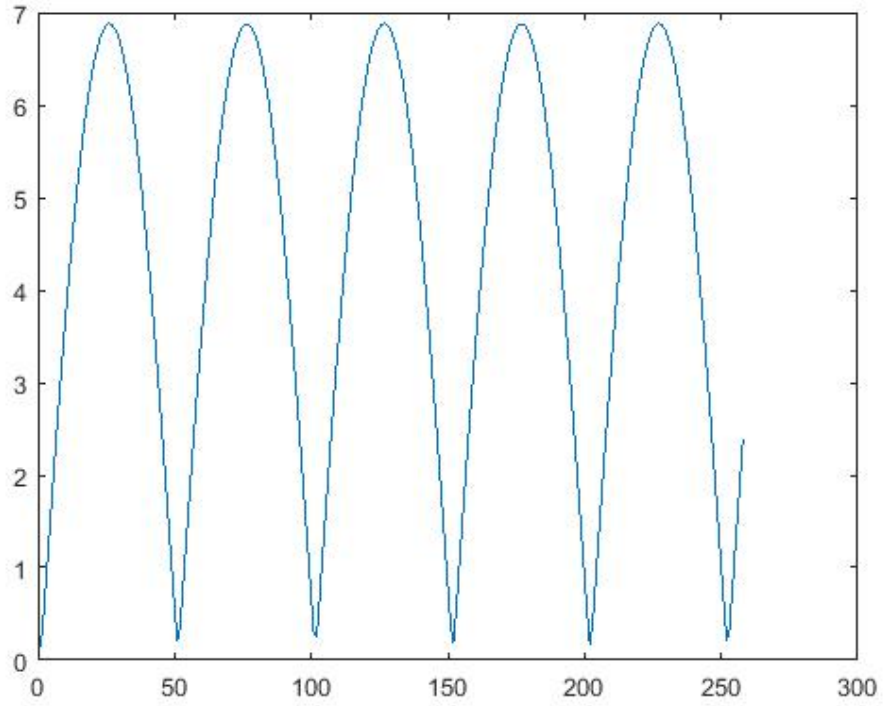


Рис. 2. Изменение напряженности E (В/м) (ось ординат) во времени (ось абсцисс) над центральной частью резонатора на расстоянии 0,84 мм от пластинки. Диаметр пластинки 7,5 см.

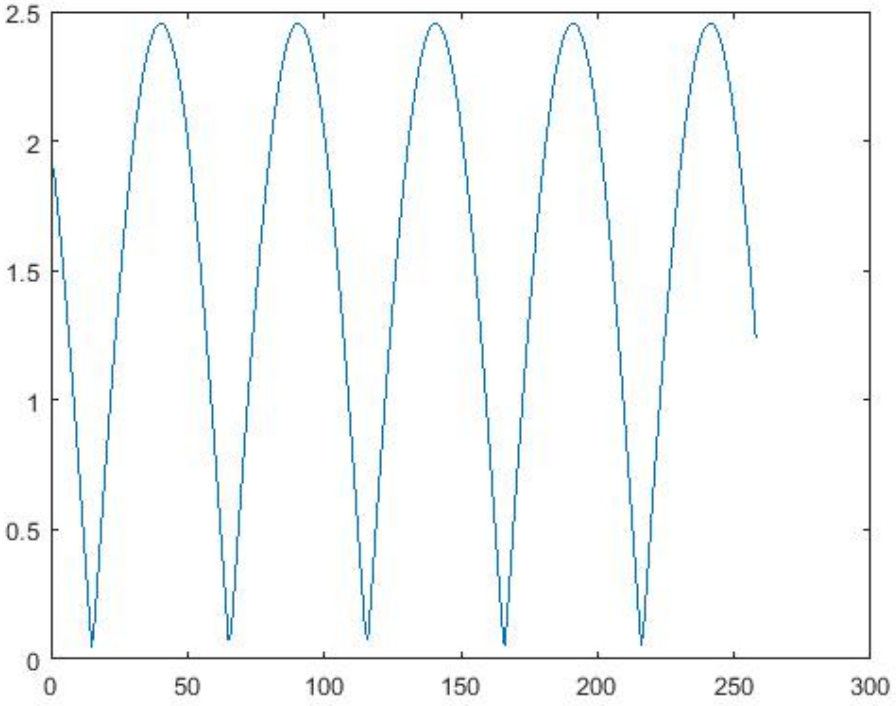


Рис. 3. Изменение напряженности E (В/м) (ось ординат) во времени (ось абсцисс) над центральной частью резонатора на расстоянии 1,68 мм от пластинки. Диаметр пластинки 7,5 см.

Заключение. Проведенные расчеты на компьютере показали, что резонатор работает как преобразователь частоты электромагнитного излучения, в частности, частота результирующего излучения уменьшается. Исходя из того, что меньшие частоты приносят меньше вреда живому организму, можно сделать вывод, что резонатор может использоваться как устройство обеспечивающее защиту от электромагнитного излучения. На основании экспериментальных данных и расчетов на компьютере можно придти к выводу, что резонаторы «АЙРЭС» могут быть использованы для защиты людей от электромагнитных полей, что особенно актуально в больших городах и на производстве. Резонатор также можно использовать при разработке электронных замков, поскольку подбирая материал резонатора, рисунок на поверхности резонатора и другие характеристики, можно получить на выходе определенную частоту излучения, если известны характеристики падающего излучения.

СПИСОК ЛИТЕРАТУРЫ

1. Серов И.Н., Лукьянов Г.Н., Копыльцов А.В. Безопасность электромагнитного излучения при его взаимодействии с самоаффинной поверхностью // Материалы IV Санкт-Петербургской межрегиональной конференции «ИБРР-2005». СПБ: СПОИСУ. 14-16 июня, 2005, С.75.
2. Серов И.Н., Копыльцов А.В., Лукьянов Г.Н. Взаимодействие полупроводниковой пластины с самоаффинным рельефом поверхности с электромагнитным излучением // Нанотехника (инженерный журнал), 2006, № 4(8), С. 44-49.
3. Серов И.Н., Копыльцов А.В., Лукьянов Г.Н. Взаимодействие электромагнитного излучения с поверхностями с самоаффиным рельефом. // Белая книга «Исследования в области наночастиц, наноструктур и нанокомпозитов в Российской Федерации», М: 2006, С.165-166.
4. Серов И.Н., Копыльцов А.В., Лукьянов Г.Н. Математическое моделирование взаимодействия электромагнитного излучения с кремниевой самоаффинной поверхностью. Материалы научн.-практ. конф. «Голография ЭКСПО-2006», М: 2006.
5. Копыльцов А.В., Серов И.Н., Лукьянов Г.Н. Математическое моделирование взаимодействия электромагнитного излучения с кремниевой самоаффинной поверхностью. Вестник ИНЖЕКОНА, серия «технические науки», 2007, С.199-205.
6. Kopyltsov A., Lukyanov G., Serov I. Coherent emission of Electromagnetic Radiation from the surface of semiconductor plate with the self-affine relief // The 3rd International IEEE Scientific Conference on Physics and Control (PhysCon 2007). September, 3rd-7th, Potsdam, Germany.
7. Kopyltsov A.V., Lukyanov G.N.,Serov I.N. Modelling of the interaction between electromagnetic radiation and semiconductor silicon surface having affine relief // HoloExpo-2007, Moscow, Russia. P. 143-146.
8. Короткова А.К., Коротков К.Г., Шапин А.В., Петрова Е.Н., Серов И.Н., Лукьянов Г.Н., Копыльцов А.В. Исследование кольцевых дифракционных решеток фонда «АЙРЭС» // Сознание и физическая реальность. 2009. Т. 14. № 9. С. 36-41.
9. Копыльцов А.В.. Лукьянов Г.Н., Серов И.Н. Моделирование на кластере высокопроизводительных параллельных вычислений взаимодействия электромагнитного излучения с полупроводниковой пластинкой с самоаффинным рельефом. Материалы XII Санкт-Петербургской международной конференции «Региональная информатика - 2010», СПБ: СПОИСУ, 2010, С.49.
10. Копыльцов А.В., Коршунов К.А., Лукьянов Г.Н., Серов И.Н. Распределенные вычисления взаимодействия электромагнитного излучения со структурированной поверхностью // 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. 526.
11. Копыльцов А.В., Коршунов К.А., Лукьянов Г. Н., Серов И.Н. Распределенные вычисления взаимодействия электромагнитного излучения со структурированной поверхностью // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 2 / СПОИСУ. – СПб., 2016. С. 383-387
12. Дюжикова Н.А., Копыльцов А.В., Коршунов К.А., Лукьянов Г.Н., Пучкова В.А., Серов И.Н. Действие электромагнитного излучения высокой частоты и влияние резонаторов-преобразователей на частоту хромосомных аберраций в клетках костного мозга самцов крыс линии Вистар // Электромагнитные волны и электронные системы. 2017, № 10, С. 53-59.
13. Орир Дж. Физика. М: Мир, 1981, т.1, 336 с., т.2. 288 с.

УДК 57.054

АЛГОРИТМ ОЦЕНИВАНИЯ БЕЗОПАСНОСТИ СЛАБО ФОРМАЛИЗОВАННОЙ ИНФОРМАЦИИ

Копыльцов Антон Александрович
Санкт–Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт–Петербург, ул. Профессора Попова, д. 5,
email: kopyl2001@mail.ru

***Аннотация*:** В статье рассмотрены проблемы безопасности при обработке слабо формализованной информации. Задача состоит в том, как неформализованную информацию формализовать таким образом, чтобы не исказить смысл и выявить какую-либо опасность, содержащуюся в слабо формализованной информации. Предполагается, что имеется объект наблюдения и система наблюдения, с большим количеством разнообразных датчиков. Объектом наблюдения может быть техническая система с установленными на ней датчиками, с которых снимается периодически слабо формализованная информация и обрабатывается. Система наблюдения включает в свой состав модули, например, модули ответственные за видеоинформацию, аудиоинформацию и другие. Система наблюдения и объект наблюдения могут работать без сбоев или со сбоями. Если система наблюдения работает без сбоев, то все в порядке. Если же в процессе работы системы появляются сбои, то систему нужно диагностировать. Исходными данными служат названия возможных неисправностей системы. Неисправности (выход из строя) модулей характеризуются конечным множеством признаков, представленных в виде набора вопросов, имеющих ответы либо «да», либо «нет». Алгоритм основан на том предположении, что вновь поступающая информация не должна в какой-то степени противоречить имеющейся информации, поступившей от разных модулей.

Причины несоответствия поступающей информации имеющейся информации могут быть различными: либо сбой в системе (неисправность объекта наблюдения, датчиков, каналов связи и т.д.), либо целенаправленный вывод системы из строя, т.е. вредительство.

***Ключевые слова**: безопасность, слабо формализованная информация; обработка информации.*

ALGORITHM OF SAFETY EVALUATION OF WEAKLY FORMALIZED INFORMATION

Anton Kopyltsov
Saint-Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str., 5,
email: kopyl2001@mail.ru

***Abstract*:** In the article discusses security issues when processing weakly formalized information. The task is how to formalize information that has not been formalized in such a way as to not distort the meaning and reveal any danger contained in weakly formalized information. It is assumed that there is an observation object and a surveillance system, with a large number of different sensors. The object of observation can be a technical system with sensors installed on it, from which periodically weakly formalized information is removed and processed. The monitoring system includes modules, for example, modules responsible for video information, audio information and others. The surveillance system and the object of observation can work without failures or with failures. If the monitoring system works without failures, then everything is in order. If there are failures during the operation of the system, then the system needs to be diagnosed. The initial data are the names of possible system malfunctions. Failures of modules are characterized by a finite set of characteristics, represented as a set of questions with answers either "yes" or "no". The algorithm is based on the assumption that the incoming information should not to some extent contradict the available information received from the different modules. The reasons for the inconsistency of the incoming information of the available information can be different: either a failure in the system (failure of the object of observation, sensors, communication channels, etc.), or a purposeful system failure, i.e. sabotage.

***Keywords:** safety; weakly formalized information; data processing.*

Введение. Формализованная информация может быть переведена в слабо формализованную с целью ее сокрытия, т.е. она будет доступна только тому, кому предназначена. Например, во многих языках используются иносказания, понятные только носителям языка, например, в исландских сагах и особенно в стихах доходит до 17 степеней иносказания. Фактически из формализованной информации делают неформализованную информацию. Задача состоит в том, как неформализованную информацию формализовать таким образом, чтобы не исказить смысл и выявить какую-либо опасность, содержащуюся в слабо формализованной информации.

Предполагается, что имеется объект наблюдения и система наблюдения, с большим количеством разнообразных датчиков. Объектом наблюдения может быть техническая система с установленными на ней датчиками, с которых снимается периодически слабо формализованная информация и обрабатывается. Система наблюдения и объект наблюдения могут работать без сбоев или со сбоями. Под сбоем понимаем ненормальную (неправильную) работу системы, т.е. когда система работает с ошибками [1]. Возможны случаи:

1.Система наблюдения и объект наблюдения работают без сбоев;

2. Система наблюдения работает без сбоев, а объект наблюдения работает со сбоями;

3. Система наблюдения работает со сбоями, а объект наблюдения работает без сбоев;

4. Система наблюдения и объект наблюдения работают со сбоями;

Прежде чем оценивать работоспособность объекта наблюдения необходимо убедиться, что система наблюдения работает удовлетворительно, т.е. слабо формализованная информация, поступающая с датчиков, достоверная. Система наблюдения включает в свой состав модули, например, модули ответственные за видеоинформацию, аудиоинформацию и другие. Количество и наименование модулей зависит от конкретной задачи. Если система наблюдения работает без сбоев, то все в порядке. Если же в процессе работы системы появляются сбои, то систему нужно диагностировать. Исходными данными служат названия возможных неисправностей системы. В начале работы системы можно использовать вероятности сбоев работы модулей. Эти вероятности могут быть определены на основе данных работы системы за предыдущий период, например, за прошедший год. Если же такая информация отсутствует, то можно считать, в первом приближении, что вероятности выхода из строя модулей одинаковые. Эти вероятности в процессе работы системы, при конкретных условиях будут, в случае необходимости, корректироваться Неисправности (выход из строя) модулей характеризуются конечным множеством признаков, представленных в виде набора вопросов, имеющих ответы либо «да», либо «нет» [2], [3], [4], [5], [6], [7], [8], [9], [10], [11].

Алгоритм основан на том предположении, что вновь поступающая информация не должна в какой-то степени противоречить имеющейся информации, которая поступила от разных модулей. То есть, если поступающая информация соответствует имеющейся информации, то уровень

безопасности равен единице (L=1), а если она противоречит информации по нескольким модулям (M<=N, N – общее число модулей), то L=M/N<1. Причины несоответствия поступающей информации имеющейся информации могут быть различными: либо сбой в системе (неисправность объекта наблюдения, датчиков, каналов связи, системы наблюдения и т.д.), либо целенаправленный вывод системы из строя, т.е. вредительство.

Описание алгоритма. Алгоритм включает следующие 7 этапов.

Этап 1. Ввод данных (наименования неисправностей, их количество и характеристики). Каждая неисправность определяется множеством признаков: признаки 1 типа (есть всегда), признаки 2 типа (отсутствуют всегда) и признаки 3 типа, которые могут быть, а могут и не быть.

Тогда эту информацию можно записать в следующем виде:

($A, P_A, N1^1, P1_1^1, P1_2^1, N1^2, P1_1^2, P1_2^2, \ldots\ldots\ldots\ldots\ldots\ldots, N1^j, P1_1^j, P1_2^j,$

$N2^1, P2_1^1, P2_2^1, N2^2, P2_1^2, P2_2^2, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, N2^k, P2_1^k, P2_2^k,$

$N3^1, P3_1^1, P3_2^1, N3^2, P3_1^2, P3_2^2, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, N3^m, P3_1^m, P3_2^m$),

где A – номер неисправности, P_A – вероятность неисправности с номером А; $N1^i$ - номера признаков 1 типа (вопросов) (j – количество признаков 1 типа (вопросов), $1 \le i \le j$), $P1_1^i$ и $P1_2^i$ - вероятности ответа «да» и «нет» на i – ый вопрос; $N2^i$ - номера признаков 2 типа (вопросов) (k – количество признаков 2 типа (вопросов) $1 \le i \le k$), $P2_1^i$ и $P2_2^i$ - вероятности ответа «да» и «нет» на i – ый вопрос; $N3^i$ - номера признаков 3 типа (вопросов) (m – количество признаков 3 типа (вопросов) $1 \le i \le m$), $P3_1^i$ и $P3_2^i$ - вероятности ответа «да» и «нет» на i – ый вопрос, при условии

$P1_1^i+P1_2^i=1$, $P2_1^i+P2_2^i=1$, $P3_1^i+P3_2^i=1$ и сумма всех P_A по всем неисправностям A равна 1.

Количество вопросов 1, 2 и 3 типов удовлетворяет неравенствам $j \ge 1$, $k \ge 1$, $m \ge 1$. Всего вопросов $V=j+k+m$ и вопросы хранятся в виде списка.

Этап 2. Из списка вопросов выбирается вопрос, которому соответствует наибольшая вероятность при ответе «да».

Этап 3. Новый список неисправностей выделяется из списка неисправностей при условии, что на заданный вопрос ответу "да" соответствует вероятность $P>P^*$, где $0<P^*<1$. Конкретное значение числа P^* зависит от решаемой задачи и определяется при отладке.

Этап 4. Из вероятностей с ответом "да" на вопросы 1, 2 и 3 типа выбирается наибольшая. В случае если их оказалось несколько, то берется любая. Этой наибольшей вероятности соответствует определенный вопрос, который и задается. На этот вопрос можно получить ответит либо "да", либо "нет". Из общего списка вопросов этот вопрос исключается.

Этап 5. В случае ответа "да" на вопрос просматриваются все вопросы 1, 2 и 3 типа с ответом "да" и выбирается наибольшая вероятность. В том случае, когда их несколько, выбирается любая. Этому выбору вероятности соответствует вопрос, который задается и из списка вопросов исключается.

Из упорядоченного списка неисправностей удаляются те неисправности, в которых на этот заданный вопрос вероятность ответа «да» меньше некоторого значения $P<P^{**}$, где $0<P^{**}<1$. Численное значение P^{**} зависит от задачи и определяется при отладке.

В случае ответа "нет" просматриваются все вопросы 1, 2 и 3 типа с ответом "нет" и выбирается наименьшая вероятность. В том случае, когда их несколько, выбирается любая. Этому выбору вероятности соответствует вопрос, который задается и из списка вопросов исключается.

Из списка вопросов убираются вопросы, соответствующие тем неисправностям, в которых на эти вопросы вероятность ответа «нет» больше некоторого значения $P>P^{***}$, где $0<P^{***}<1$. Численное значение P^{***} зависит от задачи и определяется при отладке.

Этап 6. В случае, если количество оставшихся неисправностей несколько, то происходит переход на этап 4. В противном случае, ответом является эта неисправность.

В итоге, список неисправностей становится все меньше и меньше, и последняя неисправность является ответом. Можно составить ранжированный список неисправностей, по мере их исключения из общего списка неисправностей. Можно взять несколько неисправностей, которые были удалены в конце процедуры последними. Окончательное решение эксперта о неисправности принимается им самостоятельно, и вся ответственность лежит на нем.

Этап 7. Обучающую выборку загружает эксперт. Список неисправностей, например, обнаруженных за некоторый промежуток времени можно использовать как обучающую выборку, Далее эксперт определяет вероятности ответов либо «да», либо «нет» на вопросы. При новых наблюдениях вероятности пересчитываются и сохраняются в таблице вероятностей. Количество новых наблюдений, после которых вероятности пересчитываются, может быть любым, например, можно взять 100 или 1000 в зависимости от конкретной задачи и определяется при отладке.

Если до коррекции вероятностей было NN наблюдений и для A - ой неисправности имели

($A, P_A, N1^1, P1_1^1, P1_2^1, N1^2, P1_1^2, P1_2^2, \ldots\ldots\ldots\ldots\ldots\ldots, N1^j, P1_1^j, P1_2^j,$

$N2^1, P2_1^1, P2_2^1, N2^2, P2_1^2, P2_2^2, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, N2^k, P2_1^k, P2_2^k,$

$N3^1, P3_1^1, P3_2^1, N3^2, P3_1^2, P3_2^2, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, N3^m, P3_1^m, P3_2^m$),

и в последующем провели еще MM наблюдений и в случае неисправности A было $A1$ случаев, в которых:

— на вопрос с номером $N1^i$ ($1 \le i \le j$) ответ «да» был в $N1p^i$ случаях и «нет» – в $N1m^i$ случаях,

— на вопрос с номером $N2^i$ ($1 \le i \le k$) ответ «да» был в $N2p^i$ случаях и «нет» – в $N2m^i$ случаях,

— на вопрос с номером $N3^i$ ($1 \le i \le m$) ответ «да» был в $N3p^i$ случаях и «нет» – в $N3m^i$ случаях,
— то в результате коррекции получим
(A, $P_A{}^N$, $N1^1$, $P1_1{}^{1N}$, $P1_2{}^{1N}$, $N1^2$, $P1_1{}^{2N}$, $P1_2{}^{2N}$, ……..., $N1^j$, $P1_1{}^{jN}$, $P1_2{}^{jN}$,
$N2^1$, $P2_1{}^{1N}$, $P2_2{}^{1N}$, $N2^2$, $P2_1{}^{2N}$, $P2_2{}^{2N}$, …..... $N2^k$, $P2_1{}^{kN}$, $P2_2{}^{kN}$,
$N3^1$, $P3_1{}^{1N}$, $P3_2{}^{1N}$, $N3^2$, $P3_1{}^{2N}$, $P3_2{}^{2N}$, ……..…..….. $N3^m$, $P3_1{}^{mN}$, $P3_2{}^{mN}$),
и новые значения вероятностей
$P_A{}^N$, $P1_1{}^{1N}$, $P1_2{}^{1N}$, $P1_1{}^{2N}$, $P1_2{}^{2N}$, ……..,. $P1_1{}^{jN}$, $P1_2{}^{jN}$,
$P2_1{}^{1N}$, $P2_2{}^{1N}$, $P2_1{}^{2N}$, $P2_2{}^{2N}$, …..... .., $P2_1{}^{kN}$, $P2_2{}^{kN}$,
$P3_1{}^{1N}$, $P3_2{}^{1N}$, $P3_1{}^{2N}$, $P3_2{}^{2N}$, ……..…….., $P3_1{}^{mN}$, $P3_2{}^{mN}$
можно перезаписать следующим образом:

$$P_A{}^N = (NN \cdot P_A + A1) / (NN + MM),$$

$$P1_1{}^{iN} = (NN \cdot P_A \cdot P1_1{}^i + N1p^i) / (NN \cdot P_A + A1),\ P1_2{}^{iN} = 1 - P1_1{}^{iN},\ 1 \le i \le j,$$

$$P2_1{}^{iN} = (NN \cdot P_A \cdot P2_1{}^i + N2p^i) / (NN \cdot P_A + A1),\ P2_2{}^{iN} = 1 - P2_1{}^{iN},\ 1 \le i \le k,$$

$$P3_1{}^{iN} = (NN \cdot P_A \cdot P3_1{}^i + N3p^i) / (NN \cdot P_A + A1),\ P3_2{}^{iN} = 1 - P3_1{}^{iN},\ 1 \le i \le m,$$

где $NN+MM$ – общее число случаев после коррекции, $NN \cdot P_i$ - число случаев с неисправностью A до коррекции, ($NN\,P_A + A1$) - число случаев с неисправностью A после коррекции.

Заключение. Если система работает без сбоев, то считается, что уровень безопасности L=1. Если система работает неудовлетворительно, то выявляем с помощью алгоритма модули, которые не работают или работают неудовлетворительно, и определяем их количество (M). А именно, берем тесты, которые включают вопросы для нескольких модулей, и выявляем с помощью алгоритма модули, которые не прошли проверку и ранжируем их по количеству сбоев. После этого с помощью алгоритма определяем причину их неисправности. Это может быть либо сбой в системе, либо целенаправленный вывод системы из строя, т.е. вредительство. В этом случае безопасность меньше единицы.

СПИСОК ЛИТЕРАТУРЫ

1. Воройский Ф. С. Информатика. Энциклопедический словарь-справочник: введение в современные информационные и телекоммуникационные технологии в терминах и фактах. - М.: ФИЗМАТЛИТ, 2011. 344 с.
2. Копыльцов А.А., Копыльцов А.В. Алгоритм обработки слабо формализованной информации, поступающей от технических систем // Известия СПбГЭТУ “ЛЭТИ” (известия государственного электротехнического университета), серия “Информатика, управление и компьютерные технологии”. 2012. № 8. С. 30 – 36.
3. Копыльцов А.А. Модель классификации информации и алгоритм ее предварительной обработки для статических и динамических объектов // Известия СПбГЭТУ “ЛЭТИ” (известия государственного электротехнического университета), серия “Информатика, управление и компьютерные технологии”. 2013. № 6. С. 134–139.
4. Копыльцов А.А. Программа для обработки слабо формализованной информации, поступающей от технических систем // Свидетельство о государственной регистрации программы для ЭВМ № 2013617310. Правообладатель: ФГБОУ ВПО «Санкт–Петербургский государственный электротехнический университет «ЛЭТИ» им В.И. Ульянова (Ленина)» (СПбГЭТУ). Заявка № 2013615041. Дата поступления 19 июня 2013 г. Дата государственной регистрации в Реестре программ для ЭВМ 08 августа 2013 г.
5. Копыльцов А.А., Копыльцов А.В.. Обработка слабо формализованной информации, поступающей от технических систем // Вестник Нижневартовского государственного гуманитарного университета. 2013. № 1. С. 32–36.
6. Копыльцов А.А. Алгоритм коррекции связей между фрагментами слабо формализованной информации и генерация новой информации // Вестник Нижневартовского государственного университета. 2014. № 3. С. 28–34.
7. Копыльцов А.А., Копыльцов А.В. Обобщенный алгоритм обработки слабо формализованной информации и его применение // Вестник Нижневартовского государственного университета. 2014. № 35. С. 35–44.
8. Копыльцов А.А. Обработка слабо формализованной информации в живых и технических системах // Материалы Всероссийской научно-практической конференции студентов, магистров, аспирантов «Современное программирование» (16—17 апреля 2014 г.). Нижневартовск: Издательство Нижневартовского государственного университета. 2014. С. 117–121.
9. Копыльцов А.А. Применение обобщенного алгоритма обработки слабо формализованной информации для управления неравновесной химической реакцией // Инженерный вестник Дона. 2015. № 1. ч.2. URL: ivdon.ru/ru/magazine/archive/n1p2y2015/2812
10. Копыльцов А.А. Обобщенный алгоритм обработки слабо формализованной информации и его приложения // Вестник Нижневартовского государственного университета. 2015. № 5. С. 27–37.
11. Копыльцов А.А. Разработка параллельного алгоритма для обработки слабо формализованной информации // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 2 / СПОИСУ. – СПб., 2016. С. 378-381.

УДК 004.027.31

НАЦИОНАЛЬНЫЙ НАУЧНЫЙ ЯЗЫК КАК ОСНОВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Микони Станислав Витальевич
Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия, д. 39,
email: spiiras@iias.spb.su

Аннотация: Рассмотрены категории злоумышленников в информационной сфере. Отмечена роль содержания информации в информационной борьбе. В качестве объекта исследования выбран языковый уровень информационной безопасности. Перечислены проблемы в этой сфере, вызванные чрезмерным увлечением английским языком. Приведены примеры влияния плохого знания национального языка на качество публикаций. Предлагаются меры для повышения качества научных публикаций.

Ключевые слова: *информационная безопасность, национальный язык, научный язык.*

NATIONAL SCIENTIFIC LANGUAGE AS BASIS OF INFORMATION SECURITY

Mikoni Stanislav
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
Russia, St. Petersburg, 14 Line, 39,
email: spiiras@iias.spb.su

Abstract: The categories of malefactors in the information sphere are considered. The role of the content of information in the information struggle is noted. The language level of information security was chosen as the object of research. The problems in this area are listed, caused by excessive enthusiasm for English. Examples of the impact of poor knowledge of the national language on the quality of publications are given. Measures are proposed to improve the quality of scientific publications.

Keywords*: information security, national language, scientific language*

Введение. Целью информационной безопасности является сохранение того, что является тайной для другого. Если целью другого является воровство или уничтожение информации, его называют злоумышленником. Воровством информации занимаются воры, а её уничтожением – террористы. Но существует и третий тип злоумышленника. Это тот, кто хочет управлять чужой информацией, искажая её в свою пользу.

После многочисленных попыток войти на равных в западную цивилизацию руководство страны вынуждено было признать, что нас не принимают и что конфронтация с ней – это надолго. Подтвердилось то, что давно утверждали не только российские философы и историки [1, 2], но и их западные коллеги [3]. Запад всегда был геополитическим противником России независимо от временного улучшения отношений при борьбе с другим противником. Ведь Западу мало унифицировать экономическую и политическую систему России, что ему уже удалось сделать. Нужно подчинить её своим интересам, как это делают США со своими младшими партнёрами, а стержневые страны Евросоюза со своим новыми восточноевропейскими членами. Однако, это уже красная черта для российской цивилизации, если таковой она хочет остаться.

Истоки противостояния англо-саксонской и российской цивилизаций глубоки и не являются предметом рассмотрения данной работы. Важно зафиксировать сам факт такого положения вещей, что подтверждается ежедневной практикой. В настоящее время противостояние приняло форму информационной войны между двумя сторонами. Основными средствами информационной борьбы являются: сохранение своей информации, добыча чужой информации и вброс противнику уязвимой для него информации. В этой ситуации каждая из сторон стремится обеспечить свою информационную безопасность.

Проблемы. С точки зрения информационной безопасности следует различать три уровня: технологический, языковый и содержательный. На технологическом уровне осуществляется сохранение имеющейся информации различными способами кодирования. На языковом уровне используются национальные языки противоборствующих сторон. На содержательном уровне осуществляется обмен информацией между этими сторонами на своём и чужом национальном языке. Технологический и содержательный уровни – поле действия соответственно технологов и политологов. Мы рассмотрим языковый уровень информационной безопасности.

Известно, что национальный язык – стержень любой цивилизации. Он служит не только для обмена информации между членами этого сообщества, но и для познания окружающего мира. В языке каждого народа отражается его среда обитания, религия, история и традиции [4]. В качестве официального языка стран объединённого Запада был принят английский язык. Языковая унификация Запада привела к тому, что, например, в Германии современные математические работы немецких учёных – потомков великих математиков – издаются только на английском языке. Налицо ассимиляция немецкой науки в англоязычную среду.

Реформаторы России, унифицируя экономическую и политическую систему по западному образцу, отвели преувеличенную роль английскому языку с целью вхождения в глобальный (читай в западный) мир. В сфере образования это проявилось в увеличении объёма часов на преподавание английского языка и уменьшении объёма часов на изучение русского языка и литературы. В сфере науки всячески стимулируются англоязычные публикации учёных.

Спустя четверть века можно подвести некоторые итоги этой языковой политики для отечественного образования и науки. Автору работы студенты признавались, что не могут самостоятельно формулировать мысли: «Нас натаскивали на ЕГЭ». Приходилось давать образцы отчётов для оформления лабораторных и курсовых работ. Об уровне владения русским языком можно судить по информации в Интернете. В настоящее время в этом плане ситуация начинает меняться в лучшую сторону, поскольку изъяны гуманитарного образования стали очевидными для всех.

В сфере науки многие российские учёные отдают предпочтение англоязычным публикациям, хотя на признание российской науки на Западе это не повлияло. За четверть века получено всего две нобелевских премии, причём учёными советской формации. Возможно, причина этого лежит в не

прорывном характере публикаций российских учёных. Но откуда им взяться, если финансирование научной сферы и научной смены оставляет желать лучшего?

Отметим более глубокую, на наш взгляд, причину отсутствия отечественных прорывных работ или, по крайней мере, их малое количество. Окунувшись в англоязычную литературу и готовя свои работы на английском языке, большинство наших учёных не могут сравниться с носителями этого языка для того, чтобы подняться на более высокие ступени обобщения. Поэтому большинство работ наших учёных носит технологический характер в плане улучшения существующих технологий и решения частных задач. Но хуже всего то, что многие российские учёные не способны квалифицировано писать работы на своём родном языке, не понимая содержания русских терминов и злоупотребляя иностранными терминами.

Примеры. В качестве примера приведём только одну цитату из изобилующими подобными выражениями работы квалифицированных коллег [5]: «На этапе экспликации интенсионал классификационного поля (КП) раскрывается в опоре на имплицитность двух онтологий, выраженную в положениях о гомологичности, доминантности, совместимости, частотности и референтной соотнесённости, а экстенсионал КП строится на идеях прототипичности и сходности (по-русски – сходства)» [3]. Такой кириллоязычный текст не расшифруешь даже со словарём! Кодировщики машинных слов могут позавидовать. Злоумышленник, прочитавший такой текст, точно зависнет!

Спрашивается, для какой категории читателей пишутся такие тексты? Русский человек, даже владеющий английским языком, их не поймёт, иностранец читать не будет. Выходит, не случайно Казахстан решил переходить на латиницу, чтобы читать научные работы в оригинале, не испорченные кириллицей. В языковой сфере теряем своего естественного союзника. В этом факте усматривается и «заслуга» наших учёных.

Цитированная фраза появилась не на пустом месте. Почему в школе обучают переместительному (от перемены мест слагаемых сумма не меняется) и сочетательному (значение суммы не зависит от того, как сгруппированы слагаемые) закону, а в научных публикациях фигурируют коммутативный и ассоциативный законы. Для чего нужна такая замена? Чтобы приравнять себя к высшей цивилизации, стартовавшей на 500 лет раньше, или из-за простого пренебрежения к родному (по мнению противника, варварскому) языку? Слово коммутация (англ. commutation) в русском языке трактуется как соединение или переключение. Зачем вносить технический термин в математику? Смысл слова ассоциация, как объединение, ближе к русскому слову группировка. Однако при прямом соответствии предпочтение должно отдаваться русским словам.

При описании онтологий русские термины понятие, содержание и объём заменяют их англоязычными эквивалентами концепт, интенсионал и экстенсионал [6]. Что даёт такая замена при однозначном соответствии понятий? Эти же авторы слово тестирование заменили на слово аудит, получившее применение в финансовой сфере. Зачем уводить в другую область? Разве что, из-за дани моде!

В системном анализе закономерность целостности подменяется закономерностью эмерджентности [7]. Возникает вопрос, а откуда появился чуждый русскому произношению термин эмерджентность? От американского слова emerge (возникать) или от слова emergency, которое в зависимости от контекста имеет смыслы: чрезвычайный (extraordinary), аварийный (disaster), срочный (urgent), непредвиденный (unexpected)? Соответствующие им слова – не синонимы, поскольку не всё то, что возникает, невозможно предвидеть. Для человека, владеющего английским языком, по произношению слову эмерджентность ближе слово emergency, чем слово emerge.

В непредвиденное (непредсказуемое) состояние система переходит из неустойчивого состояния под воздействием случайных факторов, например, при определённом сочетании субъективного и объективного факторов в социальной системе. Эти состояния (пути развития) могут быть известны, но неизвестно, какой путь на перепутье (в точке бифуркации) выберет система, какая цель (аттрактор) будет для неё более притягательна. Но что непредвиденного пользователи этого слова видят, например, в целостных свойствах велосипеда по отношению к свойствам его частей: рамы, колёс, руля и седла? Подмена системного свойства целостности эмерджентностью проникла и учебники по системному анализу [8], где эмерджентность трактуется как возникновение в системе новых интегративных качеств, не свойственных её компонентам.

На фоне любви к иностранным терминам учёные перестали различать тонкости понятий, именуемых русскоязычными терминами. Примером тому является классификация самоорганизующихся систем по возрастанию сложности свойств, предложенная в другом учебнике по системному анализу [9]. Но такое научное понятие отсутствует. В системном анализе понятие сложность применяется к системам, а не к их свойствам. Неправильно сформулированное основание деления понятий не могло ни породить эклектическую классификацию.

Научный язык. Целью любого научного сообщения является точное и полное объяснение фактов, выявление причинно-следственных связей между ними и нахождение закономерностей [10]. Так как ведущей формой научного мышления является понятие, почти каждая лексическая единица в научном стиле обозначает понятие или абстрактный предмет. Точно и однозначно называют специальные понятия научной сферы общения и раскрывают их содержание особые лексические единицы –

термины. Термин – это слово или словосочетание, обозначающее понятие специальной области знания или деятельности и являющееся элементом определенной системы терминов.

В рекомендациях к научному стилю публикаций отсутствует какое-либо предпочтение к именованию понятий иностранными словами. Более того, в одной из первых отечественных книг по терминологии рекомендуется отдавать предпочтение словам русского происхождения [11]. Такая рекомендация объяснима. Чем вредны неоднозначно трактуемые иностранные термины? Человек, не имеющий образного эквивалента термину, мыслит только левым (знаковым) полушарием, теряя синергизм работы обоих полушарий мозга. Отсутствие синергизма не способствует появлению новых идей. Не удивительно, что большинство современных российских работ не имеет прорывного характера. Конкретизируются и реализуются чужие идеи, выдвинутые западными учёными. Они-то мыслят на родном для них языке.

Находить подходящие русские слова для новых понятий – это серьёзный труд. К нему побуждал Ф.М. Достоевский в своих работах, призывая образованную часть общества доносить плоды цивилизации до простого народа. Он верил в самобытность русского народа и выступал против его насильственной европеизации.

Между тем, многие отечественные учёные предпочитают применять термины иностранного происхождения, и уже не из греческого и латинского языков, как повелось в науке, а из «передового» американского языка. Помимо моды можно предположить, что причиной использования иностранных терминов является приблизительное понимание проблемы. А её легче всего облечь в иностранный термин, ибо ««…приблизительность мысли легче всего облечь в иностранное слово, ведь все вокруг понимают его, как и ты, приблизительно. В этом трагедия термина: термин всегда по значению точен, но обычно не знают его значения [12]».

Отсюда во многом проистекает ложная ориентация терминов [11]. Впрочем, ею грешат и зарубежные коллеги. Например, английские учёные, собравшие и обработавшие статистику об уменьшении скорости увеличения роста поколений, назвали соответствующую функцию ложно-ориентирующим термином функция регрессии в качестве противоположности прогрессу (в росте людей). Сформулированный для частного случая термин не выдерживает обобщения, ибо при прямой зависимости переменных функция регрессии, наоборот, отражает прогресс, т.е. хотя и замедляющийся, но рост. Правильно бы ориентировал термин функция взаимодействия.

Любители иностранных терминов обосновывают их применение тем фактором, что «наука интернациональна». Да, наука интернациональна, но язык-то национален! Интернационален только язык математики, поскольку лишён предметного смысла. А предметный смысл более понятен на родном языке, поскольку имеет образный эквивалент. Казалось бы, русский язык в отличие от немецкого языка защищён кириллицей. Но и это препятствие находчивые русские люди обходят переводом иностранных слов не по смыслу, а по алфавиту – с латиницы на кириллицу. Образец такого кириллоязычного текста был приведён выше. Китайский язык защищён иероглифами лучше русского, и уж если они пишут, то только на одном языке.

Заключение. Предлагать любить свою Родину, свой народ и свой язык бесполезно. Это воспитывается с детства. И уж тем более бессмысленно адресовать это интеллигенции либерального толка. Эти люди в своей горячей приверженности к западной цивилизации готовы быть в ней на вторых ролях (быть на первых ролях им никто не позволит). Деление людей на приверженных родным корням, и людей, с благоговением смотрящих на Европу, возникло с петровских времён. Ранее их делили на славянофилов и западников, а ныне – на патриотов и либералов. Равновесие между ними нарушалось то в пользу одних, то в пользу других. В наши дни горячими спорами меду ними по политике и экономике заполнены все средства массовой информации.

Равновесие, безусловно, необходимо, если обе стороны пекутся об интересах Родины, а не об интересах нашего геополитического противника. При этом нужно помнить, что общество развивается по восходящей спирали и всё повторяется в новой, более прогрессивной форме (как утверждают прогрессисты) только в отдельных направлениях. В странах Запада такая закономерность действительно имеет место, например, в науке и технологиях. Однако в общей постановке эта закономерность не соответствует закону сохранения. Если что-то улучшается, то что-то должно ухудшаться. Что касается западного образа жизни, в нём наблюдается очевидный упадок морали и деградация духовной жизни: низкие инстинкты в яркой упаковке! За всё нужно платить!

Что касается национального языка, то нас больше волнует нарушение равновесия в пользу иностранных терминов. Восстановлению равновесия должны способствовать сами учёные, озабоченные чрезмерным засорением родного языка и его всё большим отдалением от первородных корней. К решению этой задачи следует привлекать профессиональных лингвистов. Необходимо также повысить качество терминологических стандартов, привлекая к их разработке опытных специалистов, известных своими работами в соответствующей области. Следовало бы ввести такой критерий оценивания работы, как её понятность для носителя языка.

В плане стимулирования научных публикаций полезно было бы оценивать их не с точки зрения языка (английского или русского), а с точки зрения их востребованности. Стоит ли в сложившихся условиях щедро играть «в поддавки», радуя Запад своими англоязычными работами? Разве, не

достаточно англоязычных аннотаций? Захотят, пусть переводят. Свои статьи они оценивают примерно в 1000 рублей. А мы им дарим свой опыт бесплатно. Научные знания влекут новые технологии, а это деньги.

Полезно было бы редколлегиям журналов и оргкомитетам конференций обращать внимание не только на содержание и форму, но и на язык публикаций. Так поступают в редакциях ведущих англоязычных журналов. В работе [4] автор предлагал разработать в рамках корпусной лингвистики программу Антииняз, выявляющую злоупотребление иноязычной терминологией. Эта программа могла бы обнаруживать англоязычные синонимы и подсчитывать их процент в работе. Это позволило бы, как минимум, привлечь внимание к проблеме засорения национального языка необязательными иностранными словами. В конечном счёте, на улучшение ситуации с русским научным языком приходится рассчитывать на людей, не равнодушных к своей Родине, на каждого на своём посту.

Исследования, выполненные по данной тематике, проводились при финансовой поддержке грантов РФФИ № 16-08-01277, № 17-01-00139, госзадания Министерства образования и науки РФ №2.3135.2017/К, в рамках бюджетных тем №№0073–2014–0009, 0073–2015–0007.

СПИСОК ЛИТЕРАТУРЫ

1. Гумилёв Л.Н. От Руси до России. –М.: Айрис-Пресс. 2003. – 318 с.
2. Елишев С.О. Мифы и реальность. –М.: «Канон+» РООИ «Реабилитация». 2016. – 352 с.
3. Тойнби А. Постижение истории. –М.: Айрис-Пресс. 2002.
4. Микони, С.В. Проблемы современной русской терминологии // Онтология проектирования. Том 5. № 4 (18) / 2015. С. 472-484.
5. Агеев В.О., Качанова Т.Л., Туральчук К.А., Фомин Б.Ф. Метод естественной классификации на основе информационных технологий физики открытых систем. // Материалы 9-й конференции «Информационные технологии в управлении (ИТУ-2016)». –СПб.: Концерн «ЦНИИ «Электроприбор». 2016. С. 15-24.
6. Бирюков Д.Н., Ломако А.Г., Сабиров Т.Р. Абдуктивный синтез структур функциональных типов сценариев для установления аналогий в многомодельной концептуально-онтологической системе знаний // Труды СПИИРАН. 2017. Вып. 53. С. 140-158.
7. Новиков Д.А. Комплексные модели системной оптимизации производственно-экономической деятельности предприятия // Управление большими системами. Выпуск 2017. № 65. С. 118-152.
8. Качала В.В. Основы теории систем и системного анализа. 2-е издание. –М: Горячая линия-Телеком, 2015. –210 с.
9. Анфилатов В.С., Емельянов А.Л., Кукушкин А.А. Системный анализ в управлении. –М: Финансы и статистика. 2002. –367 с
10. Рыжиков Ю. И. Работа над диссертацией по техническим наукам. Требования к ученому и к диссертации; Психология и организация научной работы; Язык и стиль диссертации и др. – СПб. : БХВ-Петербург, 2005. – 496 с.
11. Лотте Д.С. Основы построения научно-технической терминологии. –М.: Изд-во АН СССР, 1961. – 157 с.
12. Колесов В.В. Культура речи – культура поведения. – Л.: Лениздат, 1988. – 272 с.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ ОБЪЕКТАМИ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

УДК 629.12

ПРОГНОЗИРОВАНИЕ РАЗВИТИЯ ОБСТАНОВКИ В ИНФОРМАЦИОННОЙ СФЕРЕ

Алексеев Анатолий Владимирович
НП «Институт автоматизации процессов борьбы за живучесть корабля, судна»
198262, Санкт-Петербург, Ленинский проспект, д. 101, пом. 162.
email: iapbgks@bk.ru

***Аннотация*:** В статье рассматриваются вопросы обеспечения комплексной безопасности на потенциально опасных объектах, прогнозирования и контроля обстановки в информационной сфере. Системному решению данной проблемы уделяется крайне малое значение в связи с особой сложностью решения данной проблемы. Представлен один из перспективных вариантов технологии автоматизированной оценки и мониторинга состояния информационной защищенности ресурсов на основе гармонического алгоритма агрегирования показателей качества. Инвариантность данной технологии к специфике решаемых задач, реализуемой в ряде смежных областей, позволяет рекомендовать её к интеграции в существующие автоматизированные системы в защищенном исполнении. Это позволит реализовать мониторинг обстановки в информационной сфере в реальном масштабе времени, её прогнозирование и эффективное управление средствами и подсистемами обеспечения защищенности информационных ресурсов объектов информатизации различного назначения.

***Ключевые слова**: информационная сфера; объекты информатизации; технологии безопасности; информационная поддержка; ошибки управления; агрегированный показатель качества.*

FORECASTING OF DEVELOPMENT OF SITUATION IN THE INFORMATION SPHERE

Alekseev Anatoly Vladimirovich
NP "Institute of automation of processes of struggle for survivability of the ship, ship"
Russia, St. Petersburg, Leninsky Prospekt, 101, of. 162.
mail: iapbgks@bk.ru

Abstract: In the article the questions of ensuring complex safety in potentially dangerous objects, prediction and monitoring of the situation in the information sphere. Systemic solution of this problem is given very little significance in connection with the particular complexity of this problem. Presents one of the most promising technology options for automated evaluation and monitoring of the state of information security resources based on harmonic algorithm for aggregating the quality indicators. The invariance of this technology to the specific character of tasks implemented in a number of related areas, allows to recommend its integration into existing automated systems in the protected execution. It will enable monitoring of the situation in the information sphere in real time, its forecasting and efficient management of funds and sub-systems ensuring information resources security information objects for various purposes.

***Keywords**: information sphere; information objects; security technologies; information support; error management; aggregate quality.*

Введение. В настоящее время среди проблем развития риск-ориентированных технологий систем автоматизации управления объектами информатизации особое место занимают технологии и системы (подсистемы) информационно-аналитической и интеллектуальной поддержки принятия решений (ИСППР) в составе автоматизированных систем в защищенном исполнении (АСЗИ). Научно-методические и технологические аспекты формирования такой поддержки для повышения качества управления и, прежде всего, в условиях обеспечения комплексной безопасности эксплуатации, локализации аварийных ситуаций и аварий, борьбы за их живучесть являются востребованными, как никогда ранее. В том числе с учетом интенсивного развития информационных технологий и появления критической уязвимости объектов информатизации – необходимости обеспечения их информационной безопасности (ИБ), эффективной защиты информационных ресурсов (ИР) [1, 2].

Создание в этих условиях эффективных ИСППР с учетом тенденции наращивания сложности объектов информатизации, мониторинг защищенности ИР, прогнозирование и контроль обстановки в информационной сфере (ИСППР-ИС) имеет особое значение для обеспечения комплексной безопасности и минимизации эксплуатационных рисков объектов информатизации различного рода.

Тем не менее, эта задача наряду со своей новизной представляется весьма сложной системно и сегодня практически не решается. Попытки же решить данную проблему только за счет потенциала администраторов ИБ (офицеров ИБ) весьма ограничены в связи с высокой динамикой и масштабами проявления современных атак на защищаемые информационные ресурсы (ИР). В этих условиях факты выявления информационных вторжений на 90-е сутки становятся в ряде случаев характерными и исключающими активные действия по защите ИР.

2. Концепция решения задачи ИСППР-ИС. При решении задач исследовательского и концептуального проектирования, системотехнического моделирования данного класса сложных эргатических систем первоочередной является *задача всестороннего обоснования системы признаков, свойств, критериев, показателей и граничных значений* оцениваемого состояния комплексной безопасности информационного пространства (сферы), защищенности информационных ресурсов.

В этом контексте с учетом опыта активного развития в последние годы технологии и систем поддержки принятия решений и управления (СПРУ) применительно к объектам морской техники и инфраструктуры [3 - 5] представляется целесообразным в качестве главного критерия безопасности использовать *агрегированный векторный критерий* и соответствующий *показатель качества* (АПК) информационной безопасности (ИБ) информационной сферы (пространства) анализируемого $n-$го объекта информатизации Q_n . Это дает возможность последующей оценки конкурентной способности (КС) объекта информатизации $\mathrm{КС}_n = Q_n/Q_{\mathrm{Б}}$ в сравнении с АПК базового объекта $Q_{\mathrm{Б}}$, а также перспективности развития (ПР) данного объекта информатизации $\mathrm{ПР}_n = Q_n/Q_{\mathrm{Э}}$ в сравнении с аналогичным значением АПК данного объекта информатизации на предыдущем этапе развития $Q_{\mathrm{Э}}$.

По определению ИБ оценивается в % и характеризует состояние безопасности ИР в информационной сфере, определяемое защищенностью жизненно-важных ИР в АСЗИ объекта информатизации от внутренних (инсайдеры) и внешних (нарушителей регламентов ИБ) угроз, при котором поддерживается заданное значение АПК ИБ и соответствующих свойств.

Как показывает анализ практик решения данной проблемы в смежных областях [5, 6], *комплексный мониторинг* частных (ЧПК), групповых (ГПК), модельного показателей качества (МПК), а также определяемого через них агрегированного (сводного, интегрального, системного) показателя качества [3], их использование в процессе информационно-аналитической и интеллектуальной поддержки принятия проектных и управленческих решений (ПУР) позволит на качественно новом уровне не только оценивать обстановку в информационной сфере, но и прогнозировать её развитие, включая обнаружение, идентификацию и классификацию информационных инцидентов (ИИ, «аварийных ситуаций» в информационной сфере). Более того, выбирать наиболее предпочтительные варианты системных ПУР, корректировать действия лиц, обосновывающих (ЛОР), принимающих (ЛПР) ответственные ПУР, а также лиц, исполняющих эти решения (ЛИР). То есть, в целом эффективнее и результативнее управлять ИИ с их локализацией и упреждением.

Для решения задачи управления в целом информационной живучестью объекта информатизации (ИЖ, понимаемой как способность противостоять ИИ, восстанавливая и поддерживая в возможной степени свою способность использования по предназначению) на основе полученных результатов в ходе проведённых в 2012-2017 г.г. НИОКР предложена *качественно новая эрготехническая концепция* [6, 7], а также реализующие её структура, состав, комплексный алгоритм и технология интеллектуальной поддержки принятия ПУР [4].

Применительно к рассматриваемой задаче прогнозирования развития обстановки в информационной сфере рассмотрим процесс мониторинга системно значимых АПК в виде комбинированной гармонической (аддитивно-мультипликативной) свёртки ГПК типа:

– Конфиденциальность защищаемых ИР, как свойство защищенности АСЗИ от утечки ИР по техническим каналам и каналам несанкционированного доступа.

– Доступность защищаемых ИР, как свойство защищенности от несанкционированных воздействий на ИР АСЗИ.

– Целостность защищаемого ИР, как свойство защищенности АСЗИ от несанкционированного изменения ИР АСЗИ.

– Защищенность ИР от воздействия субъективных факторов, как свойство защищенности АСЗИ от нерегламентированного (негативного) воздействия операторов по изменению ИР.

– Живучесть функционирования аппаратно-программных средств АСЗИ, как свойство надёжности используемых элементов, их резервирования, условий эксплуатации, устойчивости к внешним неинформационным воздействиям.

– Устойчивость системы управления (управляемость) ИБ в информационной сфере, зависящей от полноты и степени автоматизации процессов управления, качества алгоритмов автоматического и

автоматизированного управления, квалификации и психофизиологического состояния экипажа судна, включая качество ИП ПУР ЛОР, ЛПР, ЛИР.

Данные ГПК, являющиеся результатами агрегирования соответствующих ЧПК, в свою очередь, сами агрегатируются (сворачиваются) в АПК, характеризующий весь комплекс свойств и характеристик, то есть *качество обстановки по безопасности объекта информатизации в информационной сфере* в целом. Это позволяет обеспечить *комплексный контроль состояния качества обстановки* по всей совокупности ЧПК, ГПК, МПК, число которых определяется масштабом объекта информатизации и может достигать нескольких тысяч. Именно это обеспечивает по существу *объективную оценку обстановки*, а её мониторинг – своевременный анализ динамики и управляемость ЧПК, ГПК и АПК при соответствующей возможности прогнозирования обстановки. Для этого, как показала практика в смежных предметных областях [4], вполне могут быть использованы известные и адаптивный алгоритмы регрессионного и корреляционного анализа [3].

Еще более значимыми результаты системного анализа состояния обстановки в информационной сфере становятся при мониторинге данных АПК в сочетании с такими организационно-системными показателями, как КС и ПР, отражающими достигаемое при технологическом развитии инфосферы сравнительное превосходство анализируемых объектов информатизации, либо отставание в сравнении с принятыми за базу сравнения комплексными значениями АПК соответственно конкурентных объектов и АПК данного объекта, но предыдущего этапа развития.

3. Специфика решения задач ИСППР-ИС. Многоаспектный анализ специфики решения задач ИСППР для различных типов объектов информатизации позволяет выделить, прежде всего, следующие *основные задачи концептуального и исследовательского их проектирования*, которые необходимо решить при реализации сформулированной концепции:

– систематизацию данных и оптимизацию интерфейсных форм визуализации данных, представляемых операторам (ЛОР, ЛПР, ЛИР) для обеспечения их своевременного восприятия, возможности достоверного анализа и безошибочного принятия соответствующих решений в режимах обеспечения устойчивого, скрытного (в аспекте разграничения доступа) и непрерывного управления;

– снижение психофизиологической нагрузки на администраторов ИБ (офицеров ИБ) в процессе непрерывного и длительного выполнения ими задач управления ИБ объекта информатизации;

– минимизацию негативного влияния субъективных (человеческих) факторов (ЧФ) операторов в процессе управления и, в первую очередь, на эффективность и оптимальность принимаемых проектных и управленческих решений.

4. Системные требования к ИСППР-ИС. С учетом выше изложенного комплекс требований к ИСППР, реализующий сформулированную эрготехническую концепцию и методический подход к оценке их КС и ПР с соответствующими определениями в развитие [6], представлен в виде, приведенном в таблице 1 по аналогии с [8].

Тем самым сформированный проектный образ ИСППР-ИС и анализ требований по качеству прогнозирования развития обстановки позволяют перейти к проектному обоснованию технологий ИСППР операторов объекта информатизации [5, 6] с учетом возможности инвариантной к специфике решаемых задач технологической реализации.

5. Вариант реализации ИСППР-ИС. Удовлетворить столь противоречивые требования к ИСППР можно лишь путем широкого использования современных наукоемких методов вариантного анализа и синтеза, исследовательского проектирования и моделирования процессов ИСППР с соответствующими параметрами выбора архитектуры, алгоритмов и технологии реализации сформулированных требований и использованием систем моделирования оценок качества типа [2, 5, 6].

Применение представленной концепции и сформулированных требований в смежной предметной области позволили в рамках выполненной ОКР создать и успешно испытать «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)» [5]. Пример главной интерфейсной формы ПК МДО СИП ЛА-ГО приведен на рисунке 1 для условий одного из сценариев моделирования обстановки.

Использование данного программного комплекса в варианте ИСППР-ИС будет отличаться использованием соответствующих источников данных, их спецификой, интерпретацией получаемых результатов. Тем не менее, алгоритм обнаружения, идентификации и прогнозирования развития обстановки, можно полагать, будут весьма схожими.

6. Моделирование процессов в смежной области на базе разработанного ПК МДО СИП ЛА-ГО позволило проверить правильность заложенных принципов функционирования, квалиметрически оценить достигнутое качество в сравнении с лучшими вариантами ТР, представленными в Базе данных и знаний системы оценки [2] при сопоставлении с более чем 170 альтернативных ТР.

Как показали количественные оценки, достигнутый уровень качества разработанного и испытанного МДО СИП ЛА-ГО составил более АПК=6,27 (шкала - 10) при коэффициенте вариации

оценок 13,7% и индексе квалификации Экспертного совета 52,9 в соответствии с данными Сертификата качества № СК.0004, 17.04.2014 [2].

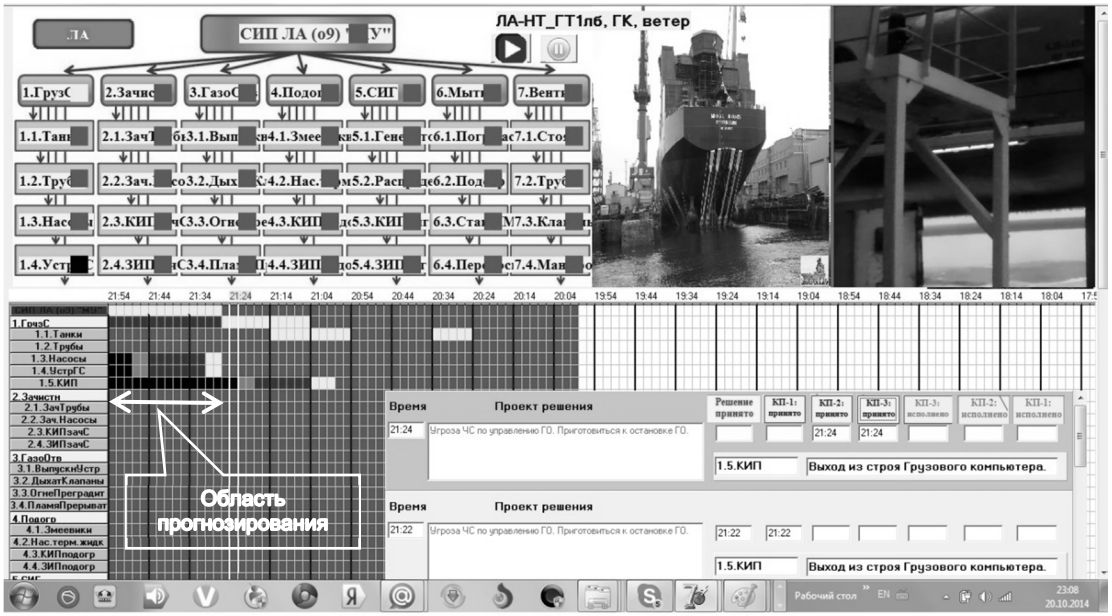


Рис. 1. Главная экранная форма ПК МДО СИП ЛА-ГО

В развитие данного технологического решения с учетом сформулированного выше подхода оценки и динамического анализа (мониторинга) КС и ПР риск-ориентированных технологий обеспечения прогнозирования развития обстановки по безопасности в инфосфере на рис. 2 приведен вариант интерфейса ИСППР-ИС для уровня ввода данных по ЧПК и ГПК для 8 разнородных ЧПК.

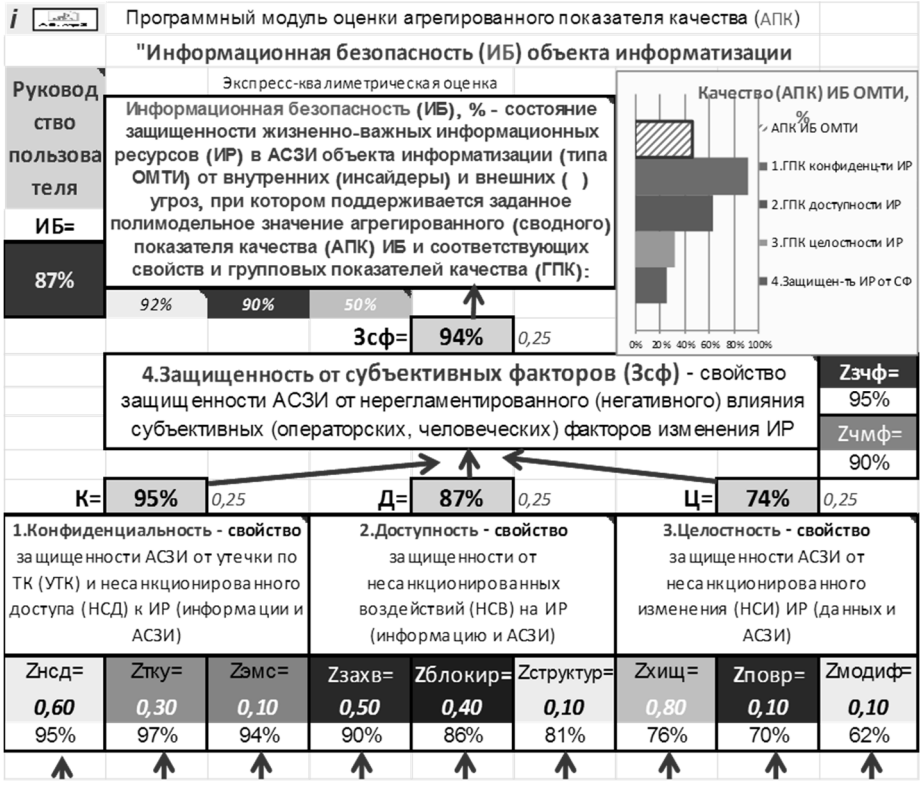


Рис. 2. Вариант интерфейсной (экранной) формы данных в ИСППР-ИС

Масштабируемость данной интерфейсной формы позволяет использовать её практически в любых конфигурациях взаимосвязей между ЧПК и практически любой архитектуры АСЗИ, что имеет весьма существенное значение для развития ИСППР-ИС.

7. Основой методики оценки АПК, КС и ПР является использование полимодельного подхода квалиметрического оценивания с гармоническим алгоритмом агрегирования ЧПК в ГПК и последующим агрегированием в МПК и АПК [3, 5]. Структурированное представление данных рис. 2 позволяет наглядно анализировать результаты влияния ЧПК на ГПК и АПК, а далее – ПР и КС [6, 7].

8. Основными задачами дальнейшего развития представляемого методического аппарата прогнозирования развития обстановки в инфосфере следует считать:

1. Систематизацию рейтинговых данных в составе квалиметрических БДЗ (КБДЗ) и сравнительный анализ возможных технологий реализации в интегрированных автоматизированных системах управления типа ИСППР-ИС в составе АСЗИ.

2. Разработку моделей и алгоритмов полимодельной оценки качества, эффективности функционирования перспективных ИСППР-ИС в составе АСЗИ с её объективной экспертной верификацией и оценкой валидности по типу [6].

3. Разработку и аттестацию программного комплекса полимодельной оценки качества, эффективности функционирования ИСППР-ИС с адаптацией их к ряду типовых задач и к соответствующим моделям критериальных предпочтений.

4. Разработку и верификацию комплекта (порядка 8) тестовых задач оценки качества и эффективности функционирования перспективных ИСППР-ИС в составе АСЗИ для сравнительного анализа и ранжирования используемых и новых методов оценивания качества и эффективности.

5. Проведение многовариантного численного эксперимента (моделирования качества) в интересах решения проектных оптимизационных системных задач в рамках исследовательского вариантного проектирования ИСППР и АСЗИ в целом.

К главным конкурентным преимуществам представляемого технологического решения прогнозирования развития обстановки в информационной сфере относятся: минимизация избыточности представления данных операторам с использованием 2-х битового цветового кодирования возможных состояний обстановки по каждому из ЧПК, ГПК и АПК; максимизация охвата функций операторов контурами автоматической обработки данных и поддержки принятия решений; прогнозирование развития обстановки с упреждением до (10…15) циклов принятия решений; представление проектов управленческих решений в текстовой форме с возможностью звуковой трансляции на посты управления; масштабируемость разработанных технологических решений с возможностью инвариантной адаптации к условиям ИСППР-ИС АСЗИ.

Тем самым, применительно к решаемым задачам возможна и целесообразна интеграция ИСППР-ИС в состав АСЗИ по технологии [5], в состав существующих автоматизированных рабочих мест администраторов ИБ объектов информатизации различного назначения [6 - 9].

Заключение. В современных условиях интенсивного развития информационных технологий и актуализации задач совершенствования средств и систем ведения противоборства в информационной сфере, непрерывного обновления (модернизации) используемых средств обеспечения защищенности информационных ресурсов одним из приоритетных направлений технологического развития следует считать создание интеллектуальных систем поддержки принятия решений для обеспечения превосходства в информационной сфере на основе технологий и средств прогнозирования развития обстановки, интегрированных в существующие АСЗИ по всем контурам управления, обеспечения их конкурентной способности и перспективности развития.

Эффективное и конкурентно способное построение и использование ИСППР-ИС позволит наряду с повышением оперативности, достоверности, устойчивости, скрытности и непрерывности управления за счет реализации возможностей информационно-аналитической и интеллектуальной поддержки принятия решений ЛОР, ЛПР и ЛИР минимизировать негативное влияние субъективных факторов операторов, что сегодня является одной из наиболее актуальных задач развития. В условиях существенного возрастания функциональности и сложности систем реализация представленных возможностей квалиметрической оценки, мониторинга и прогнозирования развития обстановки является одним из новых источников риск-ориентированного технологического развития, обнаружения, идентификации и классификации информационных инцидентов, их упреждения и эффективной нейтрализации, что приобретает особое значение и важность.

СПИСОК ЛИТЕРАТУРЫ

1. Захаров И.Г., Ем ельянов В.В., Щеголихин В.П., Чумаков В.В. Научные проблемы кораблестроения и их решение. – СПб., 2005. http://flot.com/science/sk1.htm.
2. Алексеев А.В., Антипов В.В., Бобрович В.Ю., Смольников А.В. Концепция и технология ранговой партнерской сертификации объектов морской техники и инфраструктуры / Материалы конференции «Информационные технологии в управлении» (ИТУ-2014) – СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2014. С. 29-34.
3. Смольников А.В., Сус Г.Н., Ушакова Н.П., Алексеев А.В. К вопросу выбора агрегированного векторного критерия оценки качества систем борьбы за живучесть объектов морской техники – Первая научно-практическая конференция «Современные технологии автоматизации борьбы за живучесть» - ИАП БЖКС, НПО «Аврора», 6.12.2012. С. 12-13.
4. Ушакова Н.П., Алексеев А.В., Москаленко В.А. Информационная технология представления сценариев и алгоритмов обеспечения безопасности эксплуатации сложных объектов морской техники – Региональная информатика (РИ-2014). XIV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2014)». Санкт-Петербург, 29-31 октября 2014 г.: Материалы конференции. \ СПОИСУ. – СПб, 2014. С. 434-435.
5. 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).
6. Алексеев А.В. Оперативная оценка конкурентной способности в условиях национального и мирового рынка объектов морской

техники /Актуальные проблемы морской энергетики: Материалы пятой Всероссийской межотраслевой научно-технической конференции, 18-19 февраля 2016 г. – СПб.: Изд-во СПбГМТУ, 2016.. С. 20-23.
7. Алексеев А.В. Вербальная модель процессов стратегического развития объектов морской техники и инфраструктуры / Корабельная энергетика: из прошлого в будущее: материалы Всероссийского межотраслевого научно-технического форума. – СПб.: Изд-во СПбГМТУ, 2017. С. 324 – 329.
8. Алексеев А.В., Мусатенко Р.И., Каганский М.А. Оценка конкурентной способности риск-ориентированных технологий обеспечения безопасности объектов морской техники / XX Всероссийская научно-практическая конференция «Актуальные проблемы защиты и безопасности», Санкт-Петербург, 05 апреля 2017 года. – СПб.: ГПУ, 2017.
9. Алексеев А.В., Согонов С.А., Пшеничная К.В., Максимова М.А., Прокофьева О.Е. Обеспечение безопасности автоматизированных информационных систем объектов морской техники / Методы и средства обеспечения безопасности информации: Материалы 26-й научно-практической конференции 26-29 июля 2017 г. СПб: Изд-во Потитехн. ун-та, 2017. С. 49 – 50.

УДК 004.01

ПРОБЛЕМЫ ПОДГОТОВКИ И ПЕРЕПОДГОТОВКИ КАДРОВ СИЛ ОБЕСПЕЧЕНИЯ ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ В СФЕРЕ МОРСКОГО И РЕЧНОГО ТРАНСПОРТА

Алимов Олег Михайлович
Государственный университет морского и речного флота им. адм. С.О. Макарова,
Россия, г. Санкт-Петербург, ул. Двинская 5/7,
emails: alimovom@gumrf.ru

Аннотация: В статье рассматривается процедура подготовки сил обеспечения транспортной безопасности. Даны определения основных принципов обеспечения транспортной безопасности. Приводятся ссылки на нормативные документы, регламентирующие подготовку сил транспортной безопасности. Описаны основные проблемы при подготовке специалистов транспортной безопасности.

Ключевые слова: *подготовка кадров; транспортная безопасность; информационная безопасность; морской транспорт; транспортная инфраструктура; силы безопасности.*

PROBLEMS OF TRAINING AND RETRAINING TRANSPORT SECURITY IN THE SPHERE OF MARITIME AND INLAND SHIPPING

Alimov Oleg Mihailovich
Admiral Makarov State University of Maritime and Inland Shipping,
Russia, St. Petersburg, Dvinskaya str. 5/7,
emails: alimovom@gumrf.ru

Abstract: The article deals with the procedure for training the forces for ensuring transport security. The main principles of transport security are defined. Reference is made to the regulatory documents regulating the training of transport security forces. The main problems in the training of transport safety specialists are described.

Keywords: *personnel training; transport security; information security; sea transport; transport infrastructure; security forces.*

Введение. В Российской Федерации уделяется достаточное внимание разработке и актуализации национального законодательства в области транспортной безопасности. В системе нормативных правовых актов, регламентирующих вопросы обеспечения транспортной безопасности, главенствующую роль играет Транспортная Стратегия Российской Федерации на период до 2030 года [1], одной из целей которой является повышение уровня безопасности транспортной системы страны. Важным элементом реализации Стратегии применительно к обеспечению комплексного подхода к безопасности является формирование и имплементация системы нормативно-правовых актов, принятых во исполнение Федерального закона от 09 февраля 2007 года № 16-ФЗ «О транспортной безопасности» [2]. В соответствии с указанными документами транспортная безопасность в Российской Федерации обеспечивается посредством реализации определяемой государством системы правовых, экономических, организационных и иных мер в сфере транспортного комплекса, соответствующих угрозам совершения актов незаконного вмешательства.

Основными принципами обеспечения транспортной безопасности являются:

1) законность;

2) соблюдение баланса интересов личности, общества и государства;

3) взаимная ответственность личности, общества и государства в области обеспечения транспортной безопасности;

4) непрерывность;

5) интеграция в международные системы безопасности;

6) взаимодействие субъектов транспортной инфраструктуры, органов государственной власти и органов местного самоуправления.

В соответствии с пунктом 8 части 1 статьи 10 Федерального закона от 09 февраля 2007 года № 16-ФЗ «О транспортной безопасности» работы, непосредственно связанные с обеспечением

транспортной безопасности на объектах транспортной инфраструктуры, не вправе выполнять лица, не прошедшие в порядке, установленном указанным Федеральным законом, подготовку и аттестацию сил обеспечения транспортной безопасности.

Подготовка сил обеспечения транспортной безопасности регламентирована частью 1 статьи 12.1 ФЗ-16 «О транспортной безопасности» и статьей 85.1 Федерального закона от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации» [3]. В развитие требований указанных Федеральных законов Министерством транспорта Российской Федерации изданы приказы:

– № 212 от 31июля 2014 года «Об утверждении порядка подготовки сил обеспечения транспортной безопасности»;

– № 231 от 21 августа 2014 года «Об утверждении требований к знаниям, умениям, навыкам сил обеспечения транспортной безопасности, личностным (психофизиологическим) качествам, уровню физической подготовки отдельных категорий сил обеспечения транспортной безопасности, включая особенности проверки соответствия знаний, умений, навыков сил обеспечения транспортной безопасности, личностных (психофизиологических) качеств, уровня физической подготовки отдельных категорий сил обеспечения транспортной безопасности применительно к отдельным видам транспорта»;

– № 243 от 08 сентября 2014 года «Об утверждении типовых дополнительных профессиональных программ в области подготовки сил обеспечения транспортной безопасности».

Компетентным органом в области обеспечения транспортной безопасности в сфере морского и речного транспорта в соответствии с пунктом 1 постановления Правительства Российской Федерации от 6 апреля 2004 года № 175 «Вопросы Федерального агентства морского и речного транспорта» и пункта 1 Положения о Федеральном агентстве морского и речного транспорта, утвержденного постановлением Правительства Российской Федерации от 23 июля 2004 г. № 371, является Росморречфлот [4].

Распоряжением Росморречфлота от 12.08.2015 года № АП-295-р в подведомственных образовательных учреждениях организовано и проводится обучение на курсах повышения квалификации сил обеспечения транспортной безопасности, на основе типовых программ, утвержденных приказом Минтранса России от 08 сентября 2014 года № 243 по программам:

1. Повышение квалификации работников, назначенных в качестве лиц, ответственных за обеспечение транспортной безопасности в субъекте транспортной инфраструктуры;
2. Повышение квалификации работников, назначенных в качестве лиц, ответственных за обеспечение транспортной безопасности на объекте транспортной инфраструктуры;
3. Повышение квалификации работников, назначенных в качестве лиц, ответственных за обеспечение транспортной безопасности на транспортном средстве;
4. Повышение квалификации работников субъекта транспортной инфраструктуры, подразделения транспортной безопасности, руководящих выполнением работ, непосредственно связанных с обеспечением транспортной безопасности объекта транспортной инфраструктуры и (или) транспортного средства;
5. Повышение квалификации работников, осуществляющих досмотр, дополнительный досмотр, повторный досмотр в целях обеспечения транспортной безопасности;
6. Повышение квалификации работников, осуществляющих наблюдение и (или) собеседование в целях обеспечения транспортной безопасности;
7. Повышение квалификации работников, управляющих техническими средствами обеспечения транспортной безопасности;
8. Повышение квалификации иных работников субъекта транспортной инфраструктуры, подразделения транспортной безопасности, выполняющих работы, непосредственно связанные с обеспечением транспортной безопасности объекта транспортной инфраструктуры и или транспортного средства.

Слушателями курсов являются должностные лица (персонал) субъектов, объектов транспортной инфраструктуры и транспортных средств (включая членов экипажей судов, работающих под российским флагом), подразделения транспортной безопасности, ответственные за обеспечение транспортной безопасности.

Подготовка сил обеспечения транспортной безопасности состоит из теоретической, тренажерной и практической подготовки и направлена на приобретение знаний, умений, навыков, установленных требованиями законодательства Российской Федерации. Среди обязательных изучаемых разделов есть те, в которых слушатели знакомятся с современными методами и средствами обеспечения информационной безопасности на транспорте.

Следует отметить, что в соответствии с примерными дополнительными профессиональными программами, утвержденными руководителями Росморречфлота и размещенными на официальном сайте[5], возможными формами обучения являются очная (с отрывом от производства), или смешанная (с использованием дистанционных образовательных технологий электронного обучения и проведением в очной форме практических занятий иных, чем тестирование, и итоговой аттестации).

Обучение исключительно с применением электронного обучения и дистанционных образовательных технологий не допускается.

Вместе с тем, в настоящее время «успешно» действует множество негосударственных коммерческих организаций и учебных центров, реализующих программы дополнительного профессионального образования в сфере транспортной безопасности, которые не обладают профильной тренажерной базой и не имеют в своём составе компетентных преподавателей - специалистов в области обеспечения транспортной безопасности. Как правило, данные учебные подразделения реализуют образовательные программы дистанционно.

Алгоритм обучения в таких образовательных организациях состоит из подачи заявки на обучение путем регистрации на сайте, заключения договора на оказание услуг по дистанционному обучению и его оплаты, получения логина и пароля для «прохождения обучения». Получение на электронную почту лекций в текстовом формате, различных презентаций и видео роликов. После получения информационных материалов «обучающемуся» предоставляется возможность пройти итоговый тест. После сдачи итогового теста, подписываются акты приема-передачи выполненных работ и выдаются документы установленного образца о прохождении курсов (переаттестации). При этом документы заказчику, как правило, направляются заказным письмом через Почту России, либо других почтовых операторов. Таким образом, получение сертификата о профессиональной переподготовке в области обеспечения транспортной безопасности в подобных образовательных организациях является фикцией, и не сопряжено с приобретение знаний, умений, навыков, необходимых специалисту транспортной безопасности.

Заключение. За последние годы в транспортных процессах произошли принципиальные изменения, в основном связанные с информационным обеспечением судов для более эффективного управления их движением [6], [7]. Стремительное развитие информационных технологий, внедрение автоматизированных систем управления транспортными процессами, а также различного рода информационных систем являются объективными факторами повышения безопасности транспорта. Процесс подготовки и переподготовки кадров, обеспечивающих безопасность на транспорте, также подвержен этим тенденциям. В ГУМРФ имени адмирала С.О. Макарова в соответствии с нормативно-правовой базой и с целью повышения качества образовательного процесса была создана электронная информационно-образовательная среда, обеспечивающая применение электронного обучения и дистанционных образовательных технологий, в том числе и для переподготовки кадров морского и речного флота [8].

СПИСОК ЛИТЕРАТУРЫ

1. Распоряжение Правительства Российской Федерации от 22 ноября 2008 года № 1734-р «Об утверждении Транспортная стратегия российской федерации на период до 2030 года». http://docs.cntd.ru/document/902132678.
2. Федеральный закон «О транспортной безопасности» от 09.02.2007 N 16-ФЗ (последняя редакция). http://www.consultant.ru/document/cons_doc_LAW_66069/.
3. Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 N 273-ФЗ (последняя редакция). http://www.consultant.ru/document/cons_doc_LAW_140174/.
4. Официальный сайт Росморречфлота. http://www.morflot.ru/.
5. Примерные программы для морских образовательных организаций. http://www.morflot.ru/deyatelnost/napravleniya_deyatelnosti/obrazovanie/primernyie_programmyi_podgotovki.html.
6. Нырков А.П. Автоматизированное управление транспортными системами / А. П. Нырков, С. С. Соколов, А. А. Шнуренко // СПб.: ГУМРФ имени адмирала С.О. Макарова, 2013. – 325 с.
7. Нырков А.П., Нырков А.А., Соколов С.С., Шнуренко А.А. Обеспечение безопасности объектов информатизации транспортной отрасли / под ред. А. П. Ныркова. – СПб.: Изд-во Политехн. ун-та, 2015. – 544 с.
8. Kovalnogova, N. Applying E-learning and Distance Learning Technologies in Modern University Complex / N. Kovalnogova, S. Sokolov, A. Nyrkov, S. Chernyi // Asian Journal of Applied Sciences, Volume 3, Issue 6, 2015. – Pp. 790-793.

УДК 658.58

ДИСТАНЦИОННАЯ ДИАГНОСТИКА СУДОВЫХ МАШИН И ОБОРУДОВАНИЯ

Баркова Наталия Александровна[1], Барков Алексей Васильевич[2], Грищенко Дмитрий Вячеславович[2], Федорищев Владимир Валерьевич[2]

[1] Санкт-Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лоцманская, д. 3,

[2] Ассоциация ВАСТ,
Россия, Санкт-Петербург, пр. Стачек, д. 140,
emails: barkova@vast.su, barkov@vast.su, gri_dmi@mail.ru, vvf@vast.su,

***Аннотация*:** В статье рассмотрены вопросы комплексного диагностирования судовых машин и оборудования во время длительного плавания с привлечением удаленных специалистов береговых служб диагностики и на основе технических средств отечественного производства. Изложены вопросы оптимизации номенклатуры контролируемых процессов и разделения средств диагностики на стационарные, мобильные и переносные.

***Ключевые слова**: прогноз; судовое оборудование; средства диагностики; вибрация, ток.*

REMOTE DIAGNOSTICS OF SHIPBOARD MACHINERY AND EQUIPMENT

Nataliya Barkova[1], Alexey Barkov[2], Dmitriy Grishchenko[2], Vladimir Fedorishchev[2]
[1] St. Petersburg State Marine Technical University,
Russia, St. Petersburg, ulica Lotsmanskaya 3,
[2] Association VAST
Russia, St. Petersburg, prospect Stachek 140
emails: barkova@vast.su, barkov@vast.su, gri_dmi@mail.ru, vvf@vast.su

Abstract: The article considers the issues of complex diagnostics of shipboard machinery and equipment during long sea voyages with the involvement of remote experts onshore services for diagnosis and on the basis of means of domestic production. The paper describes the optimization of the nomenclature of controlled processes and the division of diagnostic tools in stationary, mobile and portable systems.

Keywords: *prognosis; on board ship equipment; diagnostic means; vibration, current.*

Введение. К оборудованию кораблей и судов предъявляются повышенные требования к надежности и безотказности. Обеспечивают эти требования путем совершенствования конструкции и технологии производства, резервированием и аварийной защитой. Еще один путь повышения надежности – периодическая диагностика ответственных агрегатов с обслуживанием и ремонтом по состоянию, которая широко используется на многих предприятиях промышленности и транспорта. Но практический опыт использования современный средств периодической диагностики показывает, что скорости развития многих дефектов от момента их зарождения до предаварийного состояния растут по мере выработки расчетного ресурса, и прогнозировать безотказную работу оборудования во второй половине его жизненного цикла на сроки более 2-3 месяцев практически невозможно. Применительно к судам длительного плавания это указывает на необходимость проводить диагностику судового оборудования в море, что возможно лишь при обеспечении условий удаленного диагностирования, так как на судах отсутствуют штатные специалисты по диагностике.

Такая постановка задачи не означает, что все оборудование судна должно быть оснащено огромным количеством стационарно установленных датчиков рабочих и вторичных процессов и вся информация с них должна непрерывно передаваться в береговой диагностический центр. Во-первых, современные средства измерения и анализа многих процессов позволяют практически без потерь информации отказаться от использования многих из тех датчиков, без которых еще несколько лет назад невозможно было обойтись. Во-вторых, существуют дистанционно управляемые средства диагностического обследования, которые без особых проблем можно переносить с одного вида агрегатов на другой силами свободных от вахты членов команды. Последующую диагностику агрегатов с прогнозом состояния на несколько недель можно проводить удаленно, силами специалистов береговых центров. Кроме того, многие судовые машины и оборудование не вырабатывают за время плавания ту часть ресурса, на которую невозможно дать обоснованный прогноз, поэтому их можно диагностировать по приходу в порт, в том числе по накопленной во время плавания информации. Наконец, при решении необходимых организационных вопросов, можно возложить на команду судна функции «обходчика», который 2-3 раза в месяц по «маршрутам» проводит кратковременный сбор диагностических сигналов простейшими приборами в доступных точках контроля и сгружает эти сигналы в доступную для береговых специалистов базу данных

Ниже приводится анализ направлений оптимизации процессов удаленного диагностирования судовых машин и оборудования на основе разрабатываемых и выпускаемых с участием авторов технических средств и программного обеспечения для сбора диагностической информации и онлайн диагностики машин и механизмов.

Источники диагностической информации. Источниками информации о состоянии судовых машин и оборудовании являются контролируемые в них рабочие и вторичные процессы, а также свойства отдельных элементов оборудования. Контроль рабочих процессов обычно проводится по таким параметрам, как давление и температура рабочей среды, ток в электрической цепи, частота вращения и скорость движения. Из вторичных процессов для контроля состояния используются параметры таких динамических процессов, как утечки тока, жидкости и газа, износ трущихся поверхностей, вибрация и температура отдельных узлов. Могут также контролироваться механические и электромагнитные свойства отдельных элементов машин и оборудования.

Основные параметры рабочих процессов, которые контролируются и используются системами автоматического управления, зависят от выбранного режима работы оборудования и внешних условий. Поэтому их реакция на появление и развитие зарождающихся дефектов часто незаметна, но из-за высокой скорости реакции на опасные изменения состояния эти параметры используются в системах аварийной защиты оборудования. Аварийная сигнализация и зашита часто использует и результаты контроля ряда вторичных процессов – токов утечки в электрических цепях, вибрации и температуры отдельных узлов.

При использовании рабочих процессов для диагностики машин и оборудования, первой задачей становится разделение его на основную, совершающую полезную работу компоненту, и вторичные,

снижающие КПД оборудования, но имеющие диагностическую ценность. Наиболее просто такое деление производится в токе электрооборудования при его спектральном анализе, см. рис.1.

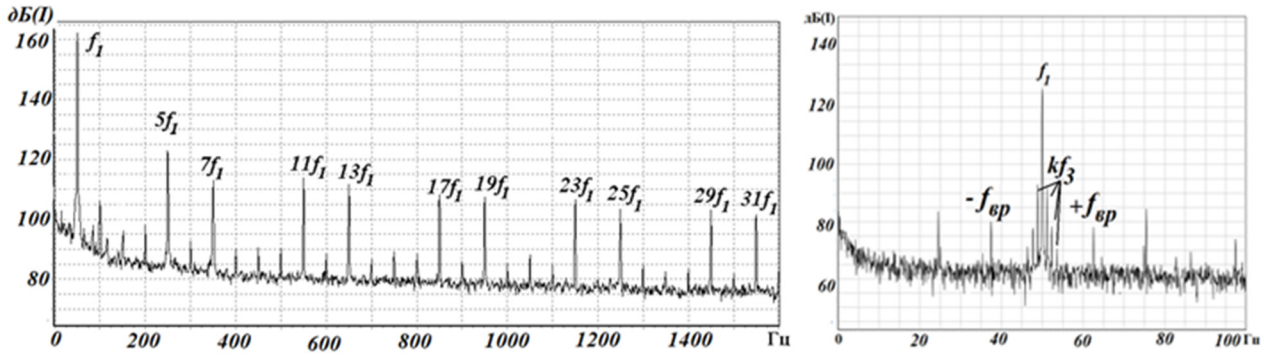


Рис.1. Спектры тока судового электроагрегата, на которых указана основная составляющая на частоте f_1=50 Гц и вторичные составляющие с вкладом в общую мощность менее 5 %, содержащие информацию о состоянии электродвигателя и присоединенного механизма

Аналогичное деление можно произвести и в сигнале с датчика давления, разделив рабочую (постоянную) компоненту и вторичные (переменные) флуктуации давления. При этом в задачах диагностики по флуктуациям давления можно не использовать датчик давления, а контролировать возбуждаемую этими флуктуациями вибрацию стенок агрегата или трубопровода.

Основные проблемы деления контролируемого процесса на рабочие и вторичные компоненты возникают при диагностике возвратно-поступательных узлов по индикаторной диаграмме давления в цилиндрах. Сложность выделения рабочей компоненты из контролируемого сигнала приводит к необходимости сравнивать мгновенную форму сигналов в разных цилиндрах, повышая пороги обнаружения дефектов и усложняя многоканальную систему диагностики таких механизмов, прежде всего судовых дизелей, используемых в гребных установках

Кроме вторичных составляющих таких рабочих процессов, как ток или давление, в средствах диагностики судовых агрегатов успешно используются параметры вторичных процессов, прежде всего вибрации агрегата и температуры его узлов с элементами трения. Контроль состояния по утечкам – это отдельное направление, относящееся к визуальной диагностике оборудования непосредственно на судне. В бортовые средства защиты оборудования включается только один вид утечки – электрического тока, а для обнаружения невидимых утечек по акустической эмиссии командой могут применяться простейшие ультразвуковые «слухачи».

Вибрация – наиболее информативный процесс для диагностики судовых машин и оборудования судовыми техническими средствами. По вибрации могут обнаруживаться и изменения состояния, сопровождающиеся изменением колебательных сил в источнике, и изменения механических свойств отдельных узлов оборудования, по которым распространяется вибрация от источника колебательных сил до точек ее контроля. Разделение сигнала вибрации на периодические, случайные и импульсные, их последующий анализ, в том числе спектральный, см. рис. 2., позволяет получить большой объем информации о состоянии оборудования с узлами вращения.

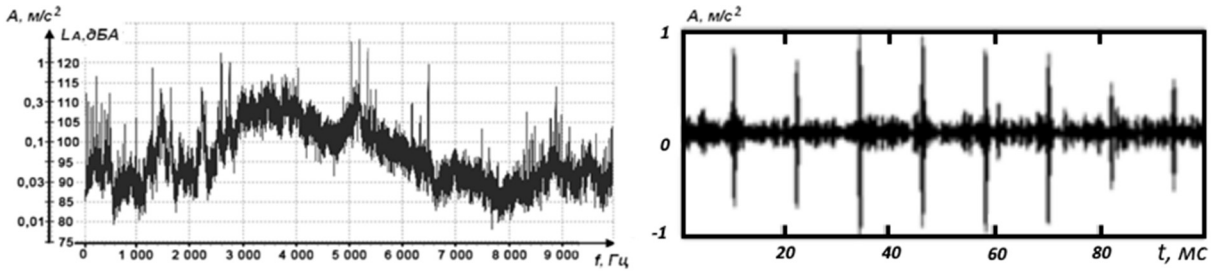


Рис.2. Спектр вибрации судовой машины на низких и средних частотах (слева) и форма вибрации на высоких частотах (справа)

Типовыми точками контроля вибрации судовых машин являются их подшипниковые узлы, через которые передается основная часть вибрационной энергии с вращающегося ротора на корпус.

Успешное использование для диагностики судовых машин и оборудования параметров вторичных процессов и вторичных составляющих рабочих процессов в объектах диагностики не означает возможности отказа от контроля основных параметров рабочих процессов. Такой контроль необходим, и не только для обеспечения автоматического управления и аварийной защиты оборудования. При решении диагностических задач необходима информация о текущем режиме работы оборудования, от которого в значительной степени зависят многие из вторичных параметров, используемых для обнаружения изменений состояния и дефектов.

Средства дистанционной диагностики. Средства, доступные для дистанционной диагностики судовых машин и оборудования, разрабатываемые и выпускаемые предприятиями Ассоциации ВАСТ, делятся на четыре основные группы.

Первая группа – стационарные системы онлайн мониторинга и диагностики СМД-4 в автоматическом режиме, строящиеся по сетевому принципу. Структура системы приведена на рис.3

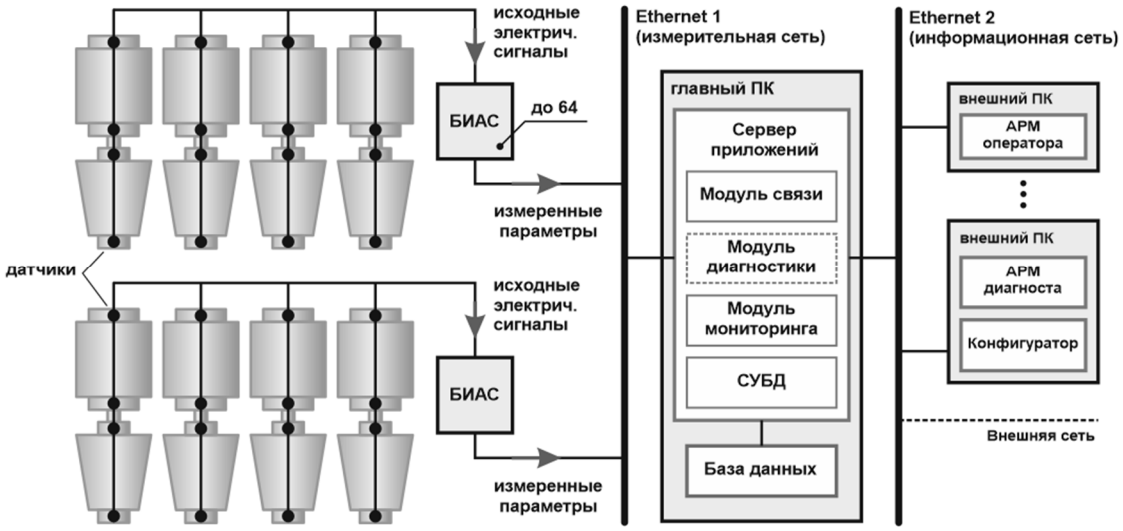


Рис.3. Структура системы диагностики СМД-4, в которой используются датчики вибрации, частоты вращения, температуры и измерительные преобразователи тока

Система состоит из группы независимых многоканальных цифровых анализаторов, датчики которых могут монтироваться на разное оборудование в разных помещениях, общей измерительной сети, к которой подключены анализаторы и диагностический сервер. В свою очередь сервер подключается к информационной сети, по которой требуемую информацию получают операторы, обслуживающие диагностируемое оборудование, средства аварийной сигнализации и другие судовые потребители диагностической информации, а также береговые службы диагностики, получающие всю необходимую информацию и возможность проведения дополнительных измерений, не прерывая основные.

Время обнаружения скачков состояния объектов контроля – от 0,5 сек., время постановки диагноза «по событию» - не более 5 сек. Все измерительные каналы работают синхронно, что позволяет проводить диагностику группы объектов и во времени, и в пространстве. На каждом предварительно указанном из возможных режимов работы оборудования диагностика проводится независимо. В однорежимном оборудовании независимая диагностика проводится на пуске, в установившемся режиме, и на выбеге.

Система СМД-4 с минимумом используемых датчиков ставится на наиболее ответственное судовое оборудование, обеспечивая его глубокое диагностирование. При установке на ДВС, обеспечивается только обнаружение опасных изменений состояния без идентификации их причины

Вторая группа – мобильные системы СМД-4М онлайн мониторинга состояния с возможностью автоматической диагностики отдельных видов машин и оборудования (см. рис.4). Их структура практически совпадает со структурой стационарной системы, но число измерительных каналов ограничено. Для обеспечения режима автоматической диагностики конкретного объекта она должна быть укомплектована модулем диагностики именно этого вида объекта.

Фактически СМД-4М - аналог систем суточного мониторинга в медицине, но ее датчики устанавливаются на объект на несколько суток, достаточных для обнаружения дефектов и выявления трендов их развития. Установка мобильной системы на конкретный объект во время плавания может осуществляться не имеющими специальной подготовки членами команды судна либо по плану, либо при появлении косвенной информации о возможном ухудшении состояния объекта. Мобильная система подключается к судовой информационной сети и ее результаты доступны команде судна и удаленному диагносту в онлайн режиме. При отсутствии модуля автоматической диагностики контролируемого объекта диагноз ставит береговая служба и вносит результат в интерфейс СМД-4М.

Стационарная и мобильная системы СМД-4, как работающие в онлайн режиме, могут быть подключены к судовой системе аварийной сигнализации. Кроме этого они могут давать оценку остаточного ресурса объекта по результатам анализа трендов развития опасных дефектов, позволяя команде судна подготовиться к безопасному выводу этого объекта из эксплуатации.

Рис.4. Мобильная система мониторинга состояния СМД-4М, многоканальный сборщик диагностических сигналов СДС-8 и многоканальный виброанализатор СД-41

Третья группа – стационарно устанавливаемые многоканальные сборщики данных (диагностических сигналов) в объектах, работающих с перерывами, наработка которых за время плавания судна не превышает прогнозируемого интервала безотказной работы на момент постановки очередного диагноза (рис.4). Накопление сигналов производится отрезками, достаточными для постановки диагноза, как периодически (3-5 раз за время плавания), так и по «событиям» - регистрируемым сборщиком опасным изменениям состояния, с записью части сигнала до события, и части сигнала – после его регистрации.

Сборщики сигналов СДС-8 не проводят диагностического анализа регистрируемых сигналов, что существенно упрощает их конструкцию, они лишь обнаруживают «события», к которым относятся скачки вибрации, превышения уровнем вибрации или отдельных составляющих спектра вибрации (тока) порогов повышенной опасности, а также появление интенсивных составляющих вибрации ударного происхождения. Задача дистанционного запуска СДС-8, анализа собранных данных, определения причины обнаруженных опасных изменений состояния, а также диагностики и прогноза состояния объекта при отсутствии опасных изменений ложится на береговые службы диагностики либо в процессе плавания, либо по возвращению судна из плавания. Результаты диагностики по накапливаемым сигналам, выполненные береговыми службами во время плавания, могут передаваться на борт судна и отображаться в сводных оценках состояния судового оборудования.

Четвертая группа – многоканальные переносные приборы для измерения и анализа диагностических сигналов, а, при необходимости, и наладки продиагностированного оборудования. Один из таких приборов – виброанализатор СД-41 приведен на рис. 4. Работа с прибором требует определенной подготовки, но при работе под руководством удаленного специалиста эта подготовка может быть сведена к минимуму. Фактически функции члена команды судна – работа «обходчика», проводящего раз в две – три недели короткие измерения вибрации в группе точек контроля по составленным удаленным специалистом маршрутам. Использование такого прибора резко расширяет номенклатуру диагностируемых вспомогательных машин и оборудования, сводя к минимуму вероятность их непрогнозируемого отказа во время плавания.

В то же время использование многоканального анализатора, выполняющего синхронные длительные измерения в судовых условиях, необходимо для обеспечения пространственной диагностики сложных агрегатов, в первую очередь машин с узлами возвратно-поступательного действия, интервалы между обслуживанием которых часто бывают меньше длительности плавания. Параллельно измерять в нескольких возвратно-поступательных узлах разные процессы – вибрацию, давление, угол полворота коленчатого вала гораздо сложнее. Но для проведения и таких измерений под управлением внешнего специалиста вполне можно обойтись без диагностической подготовки оператора. Зато такая диагностика позволит во время плавания периодически контролировать работу топливной и газораспределительной системы ДВС, а при необходимости, производить направленную замену дефектных узлов, из числа имеющих ограниченный ресурс и хранящихся в ЗИПе.

Необходимое программное обеспечение для анализатора СД-41, обеспечивающее диагностику и наладку топливной и газораспределительной систем ДВС в настоящее время готовится к выпуску. Соответственно, диагностика других медленно изнашиваемых узлов, при использовании СД-41 может проводиться по собранной простейшими сборщиками данных информации либо дистанционно, либо по приходу в порт приписки, и стационарная система для диагностики дизелей может существенно упроститься,

Кроме проведения работ по мониторингу состояния и диагностике машин и оборудования непосредственно на судне, большое внимание следует уделять и выявлению конструктивных дефектов и дефектов изготовления оборудования на заводе-изготовителе во время сдаточных испытаний нового оборудования. Стационарные и мобильные системы СМД-4 и СМД-4М обеспечивают мониторинг и диагностики машин и оборудования на испытательных стендах, учитывая основные особенности

проведения таких испытаний. В частности, одна из систем устанавливается на объединении Звезда для первичной диагностики выпускаемых редукторов на сдаточном стенде.

Выводы:

1) Для повышения надежности и снижения числа отказов выработавших значительную часть ресурса судовых машин и оборудования во время длительного плавания судна необходимо использовать широкую номенклатуру стационарных, мобильных и переносных средств сбора информации и диагностики.

2) Современные средства мониторинга и диагностики, сбора и передачи диагностической информации по рабочим и вторичным процессам позволяют выполнять работу по диагностике и прогнозу состояния судовых машин и оборудования дистанционно, силами береговых служб диагностики с привлечением членов команды к креплению датчиков на отдельные объекты.

3) Разрабатываемые и производимые в России технические средства и программное обеспечение для диагностики машин и оборудования различных предприятий могут быть адаптированы для выполнения работ по дистанционной диагностике на судах.

СПИСОК ЛИТЕРАТУРЫ

1. Неразрушающий контроль: Справочник: В 7т. Под общей редакцией В.В. Клюева. Т. 7: В 2 кн. Кн. 2: Балицкий Ф.Я., Барков А.В., Баркова Н.А. и др. Вибродиагностика, - М.: Машиностроение, 2005, 829 с.
2. Баркова Н.А., Грищенко Д.В. Направления развития информационно-измерительных технологий диагностики роторного оборудования // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 1 – СПб: СПОИСУ, 2015, С. 503-507
3. Барков А.В., Баркова Н.А., Грищенко Д.В., Федорищев В.В. Система мониторинга вибрации с оперативной идентификацией обнаруживаемых изменений // Защита от повышенного шума и вибрации. Сборник докладов всероссийской научно-практической конференции с международным участием – СПб.: БГТУ «Военмех», 2013, С. 272-278.
4. Грищенко Д.В. Система непрерывного мониторинга состояния и оперативной диагностики судового роторного оборудования // Вестник Астраханского государственного технического университета. Серия: Морская техника и технология – СПб.: ФГБОУ ВО «АГТУ», 2016, № 4. С. 54-62.
5. Грищенко Д.В. Автоматическая обработка узкополосных спектров вибрации судовых машин в целях выделения диагностически значимых компонент // Морские интеллектуальные технологии – СПб.: НИЦ «МОРИНТЕХ», 2016. Т. 2. № 4 (34). С. 8-13.

УДК 343.321.2

ДИВЕРСИОННОЕ ПРИКРЫТИЕ

Каторин Юрий Федорович, Юмашева Елена Сергеевна, Бач Марина Александровна
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Россия, Санкт-Петербург, ул. Двинская, 5/7,
emails: katorin@mail.ru, elena_umasheva@mail.ru, m.resh18@mail.ru.

Аннотация: Для создания эффективной системы безопасности следует подробно изучать историю проведения наиболее успешных диверсионных атак. Данная статья об успешном проведении в 1943 году диверсии старшим лейтенантом Луиджи Феррaро из группы «Гамма», в турецком порту Александретта; о снаряжение итальянских подводных диверсантов, тактика их действий и методика подготовки. Анализируются результаты диверсий.

Ключевые слова: *Вторая мировая война, террористический акт, морской порт, подводные диверсанты, группа «гамма», порт Александретта, старший лейтенант Луджи Феррaро.*

DIVERSIONAL COVERAGE

Katorin Yuri , Yumasheva Elena, Bach Marina
State University of the Marine and River Fleet named after Admiral S.O. Makarova
Russia, St. Petersburg, st. Dvinskaya, 5/7,
emails: katorin@mail.ru, elena_umasheva@mail.ru, m.resh18@mail.ru.

Annotation: To create an effective security system, you should study in detail the history of the most successful subversive attacks. This article gives an example of the successful conduct of sabotage in 1943 by Lieutenant Luigi Ferraro of the Gamma Group, in the Turkish port of Alexandretta. The equipment of Italian submarine saboteurs, tactics of their actions and methods of training are described, the results of sabotage are analyzed.

Keywords: *World War II, terrorist act, the seaport, underwater saboteurs, the group «G», the port Aleksandretta, Senior Lieutenant Ludzhi Ferraro.*

Сегодня терроризм превратился в одну из опаснейших глобальных проблем современности, серьезную угрозу безопасности всего мирового сообщества. В мире идет новая война – террористическая. За двести лет использования террористами взрыва, как одного из основных средств террора, человечество не научилось эффективно противостоять этому явлению. [7]

В этих условиях одной из важнейших задач правоохранительных органов является обеспечения безопасности особо важных объектов, притом комплексно. В морских портах обрабатываются грузы очень широкой номенклатуры. Кроме того, на многих терминалах для обеспечения технологических операций по хранению и перевалке груза используются опасные вещества в больших количествах. Все это делает морской порт потенциально особо опасным объектом. Возросшая вероятность совершения террористических актов с учетом потенциальной опасности морского порта для персонала, населения близлежащих населенных пунктов (иногда насчитывающих сотни тысяч и более жителей) привели к принятию в 2002 году Главы XI-2 Конвенции СОЛАС-74 и Международного кодекса по охране судов и портовых средств [8].

Российская Федерация, как один из членов Международной морской организации, активно внедряла требования этих документов на портовых средствах. Комплексные системы безопасности портовых средств предназначены для обеспечения безопасности, регулярности и эффективности работы портового хозяйства путем разработки и внедрения необходимых технических средств защиты. [11]

Однако для создания по настоящему эффективной системы безопасности надо досконально знать основные методы проведения таких операций, поэтому следует подробно изучать историю проведения наиболее успешных диверсионных актов. Данная статья приводит пример проведения диверсии с использованием дипломатического прикрытия.

2. Обсуждение

Италия накануне Второй мировой войны остро нуждалась в новом, необычном оружии, которое можно быстро изготовить и немедленно пустить в ход. В оружии, дающем возможность нанести чувствительные удары противнику в самом начале военных действий, что если и не обеспечило бы равенство сил, то, по крайней мере, поставило бы ее в менее невыгодные условия в противостоянии с Англией на Средиземном море. Выбор итальянцев пал на штурмовые средства. [5]

Для подводных диверсий в Италии был создан специальный заряд «Баулетто» («Bauletto» – Ракушка), который представлял собой мину небольших размеров, начиненную 4,5 кг мощной взрывчатки. Мина прикреплялась к подводной части корабля на магнитах или зажимах. Взрыватель имел маленький винт, раскручиваемый при движении судна. К часовому механизму добавлялось устройство, включающее винт. Как только пароход отправлялся в плавание, винт начинал вращаться, и его скорость была не больше пяти узлов. При выполнении винтом определенного числа оборотов, специальное устройство запускало часовой механизм. Взрыв происходил через значительное время после выхода судна из порта, в открытом море, что приводило к полной гибели парохода и груза. Дело в том, что в порту подрыв заряда вызывал потопление судна на небольшой глубине, а это означало не уничтожение, а лишь временный вывод из строя – обычно часть судна оставалась над поверхностью воды, что позволяло спасти груз и облегчало подъем самого судна. Но самое главное – такой акт на территории нейтральной страны мог вызвать дипломатические осложнения и весьма нежелательные политические инциденты. [2]

Когда в целях борьбы с этим оружием англичане начали широко применять стальной трос, протягиваемый двумя катерами по днищу кораблей, заряд стали снабжать дополнительно защитной скобой, по которой трос скользил не зацепляясь. В дальнейшем, когда англичане начали систематически обследовать подводную часть своих кораблей при помощи водолазов, был применен механизм, вызывавший взрыв при отвинчивании зажимов с целью отделить заряды от корпуса судна. [3]

Прикреплять такие заряды к днищам должен был боевой пловец – морской диверсант в специальном прорезиненном костюме, снабженный кислородным прибором. К своей цели он добирался вплавь, не используя технических средств. Лицо и руки покрывались черной или темно-зеленой краской, а голова маскировалась пучком морских водорослей. Маски для подводного плавания не применялись, так как могли демаскировать диверсанта.

Подводный диверсант проходил серьезную подготовку, он должен был обладать большой выносливостью, уметь отлично плавать, быть прекрасным водолазом, уверенно ориентироваться под водой и на поверхности, владеть различными способами маскировки – это определяло степень готовности добровольцев к выполнению боевых задач. Решено было подбирать их из пловцов-спортсменов, которых стали собирать со всех видов войск. В. Боргезе привлекает к отбору итальянскую федерацию плавания. Подразделение пловцов получило название группа «Гамма», и входило в состав 10-й флотилии МАС, возглавляемой В. Боргезе. К окончанию тяжелейшего курса физической и специальной подготовки каждый член группы без особых затруднений преодолевал расстояние в 2 мили, транспортируя взрывные устройства. Вначале больших побед у итальянцев не было, но операция старшего лейтенанта Луиджи Феррaро (Luigi Ferraro; 1914–2006) увенчалась полным успехом и оставила след в истории.

4. Результаты

Внимание итальянского командования давно привлекал турецкий порт Александретта (в н.в. Искендерун), где происходила погрузка на союзные суда хромовой руды, – сырья необходимого для военной промышленности. Долгое время в этом районе было тихо, но в начале июня 1943 года

итальянскому консулу в Александретте, маркизу Инъяцию ди Санфаличе представился новый служащий Л. Феррaро и вручил письмо за подписью министра иностранных дел о том, что он прислан в консульство для выполнения специальной миссии. С собой Феррaро привез 4 тяжелых и огромных чемодана, которые, как дипломатический багаж, досмотру не подлежали. Новичок сразу же сдружился с секретарем консульства Джованни Роккарди (Giovanni Roccardi), бывшим офицером разведки в звании капитан-лейтенанта и автором идеи атаки турецкого порта. В официальных отношениях и на людях секретарь консульства оказывал служащему свое покровительство и подчеркивал, что старается ознакомить его с работой, ввести в светские и дипломатические круги города, а также помочь в выборе приятных развлечений. (Borghese, 1957: 128)

С помощью Роккарди молодой лейтенант обманул бдительность британских агентов службы безопасности и переправил гидрокостюм с дыхательным прибором и подрывные заряды, придуманные специально для подрыва судов в нейтральных портах, в тайник на пляже. «Что забавно, — вспоминал Феррaро, — чтобы иметь возможность спокойно работать, я пустил слух, что я не умею плавать. Эта простая хитрость прекрасно сработала, и я мог ходить купаться по вечерам, никого, не удивляя: я был в некотором роде тем простаком, который купается по ночам, потому что стесняется это делать днем, чтобы не показать свое неумение плавать». [9]

30 июня 1943 года на рейде порта с помощью корабельных лебедок началась погрузка с барж хромовой руды на греческое судно «Орион» («Orion»; построен в 1909 г. компанией «Connel & Co. Ltd», ранее назывался «Glenshiel» (1922) и «Highland Prince» (1936), принадлежал греческой судоходной компании «Polychronis Lyras», водоизмещение 7727 т). Каждому в Александретте было известно, что судно снова выйдет в море дней через 5. Феррaро решил действовать немедленно. Вечером 30 июня Феррaро прошел в купальную кабину и принялся рыться в сумке со спортинвентарем. Через несколько минут он в полном снаряжении с двумя зарядами на поясе скользнул в воду и тотчас же исчез во мраке ночи. Проплыв 2300 м, он оказался вблизи греческого судна «Орион». Держась в тени барж, пловец включил кислородный прибор и погрузился. Прикрепить заряды к килю, вынуть предохранители и возвратиться на поверхность – потребовало лишь нескольких минут. [1]

Он, лучший пловец группы «Гамма», играючи выполнил работу, много раз отрепетированную на тренировках. Феррaро пробыл в воде более 4 часов. Он достиг берега около 4 часов утра и нашел мешок, что Роккарди оставил на пирсе, как это было согласовано. Пловец спрятал снаряжение внутри него и с большой осторожностью пробрался к задней двери консульства, которое расположено не более чем в 10 метрах от моря. А 4 часа утра Феррaро был уже в своей постели. [1]

Через 6 дней «Орион» вышел в море, но далеко он не ушел – вертушки на зарядах начали свой отсчет. В сирийских водах под корпусом прозвучал взрыв, и судно затонуло. Спасшиеся моряки, которых поместили в госпиталь в Александретте, утверждали, что «Орион» был торпедирован. Трагедию списали на немецкую подводную лодку. Успех вдохновил диверсантов на новые атаки. Утром 9 июля Роккарди и Феррaро отправились в соседний порт Мерсин, «искупались в море», а на другой день вернулись в консульство, В Александретте никто не заметил их отсутствия. [1]

Однако последствия визита сказались, когда 19 июля из порта вышло английское судно «Кайтуна» («Kaituna»; построен в 1938 г. компанией «Eriksberg Mekaniske» в Швеции, водоизмещение 9165 т, принадлежал «New Zealand Shipping Company»). Вскоре под его днищем прозвучал взрыв, но из двух прикрепленных зарядов сработал только один, и поврежденный корабль сумел выброситься на мель у берегов Кипра. [1]

Спустя несколько дней греческие водолазы спустились в воду, чтобы тщательно обследовать подводную часть теплохода. На киле судна они обнаружили какой-то странный металлический предмет. Водолазы осторожно сняли его и доставили на поверхность. Оказалось, что это подрывной заряд, снабженный маленьким винтом, ось которого погнулась. Секрет подрывного заряда «Буалетто» был разгадан благодаря новому и прочному «Кэйтуну», который оказался жертвой взрыва только одного заряда. Если бы взорвались оба, то теплоход пошел бы ко дну. Отбуксированный в порт «Кайтуна» встретил окончание войны в сухом доке. [9]

Военные власти Кипра немедленно оповестили о случившемся военно-морское командование союзных держав. Были даны приказания срочно обследовать кили всех кораблей, стоящих на рейде в турецких портах или недавно покинувших таковые. Поэтому, когда 30 июля итальянская парочка повторила в Мерсине операцию по установке мин под теплоходом «Сален Принс» («Sicilian Prince»; построен в 1912 г., водоизмещение 5000 т), то его миновала горькая участь. Контрольный осмотр водолазами, который ввели после случая с «Кайтупа», привел к изъятию обоих «Буалетто», прежде чем судно вышло в море. [3]

Менее счастливым оказался норвежский теплоход «Фернплант» («Fernplant»; построен в 1939 г компанией B&W, длина 127 м, водоизмещение 5274 т и дедвейт 7000 брт). 2 августа в 2 часа ночи на рейде Александретты Феррaро прикрепил к его корпусу два заряда. А 5 августа теплоход покинул порт и бесследно исчез вместе с 6000 тонн хромовой руды.

Через три дня, так как кончились заряды, Феррaро «ощутил внезапный приступ малярии» и был немедленно отправлен на родину. Так в результате успешных действий одного человека в турецком

порту Александретта англичане потеряли 2 больших парохода, еще 1 был сильно поврежден и практически потерян до конца войны. [5]

По возвращению в Италию старший лейтенант был награжден Золотой Медалью «За храбрость» и стал национальным героем страны. Он дожил до глубокой старости, а после войны основал всемирно известную фирму по производству подводного снаряжения «Technisub», в 2001 году дал интервью корреспонденту журнала «Морской сборник», в котором категорически опроверг версию о причастности итальянцев к подрыву и гибели в 1954 году советского линкора «Новороссийск». По его словам, бывшие служащие «Десятой флотилии» не испытывали вражды к Советскому Союзу. На протяжении всей войны они дрались с британским флотом, и всеми своими победами и унизительным поражением обязаны исключительно морякам Его Величества. Если бы вдруг у них появилась возможность реванша, их ярость обрушилась скорее на Скапа-Флоу, чем на советский Севастополь. [10]

Заключение. Капитуляция Италии 03.09.1943 года остановила практические действия 10-й флотилии МАС. Однако опыт ее боевого применения, механизмы разработки операций, наработки в области технического обеспечения уже вводились в подготовку спецподразделений флотов Германии, Англии, США. По законам военного времени делалось это быстро, без оглядки на неизбежные огромные затраты.

В первые послевоенные годы интерес к созданию подводной диверсионной техники значительно снизился. Однако с середины 50-х годов строительство штурмовых средств возобновилось, и лидерство захватила Италия. Хотя по Парижскому мирному договору 1947 года стране запрещалось иметь диверсионно-штурмовые средства, уже в 1951 году на бывшей учебной базе в Специи был возрожден центр по подготовке морских диверсантов. А если открыть книгу «Силы специальных операций», выпущенную в 1996 году, и посмотреть на подводное вооружение современных боевых пловцов-диверсантов, станет понятно – последняя глава в их истории будет написана еще не скоро.

СПИСОК ЛИТЕРАТУРЫ

1. Borghese V. The Tenth Flotilla MAS. [Trans. With Ital. S.V. Slavina and Yu.A. Karulin.] - M.: Foreign Literature Publishing House, 1957. p 288.
2. Borghese V., Demaré P. Borghese. Black Prince of torpedo people / Comp. Nikolay Nepomnyashchy. - M.: Veche, 2002. pp. 480.
3. Voldron T., Gleason D. "Submarine saboteurs in the Second World War" M .: 2002. pp. 216.
4. Каторин Ю.Ф. Люди, оседлавшие торпеды. СПб.: Галея-Принт, 2006. – 128 с.
5. Каторин Ю.Ф. Коршунов Ю.Л. Парадоксы военной истории. Санкт-Петербург, 2003. Сер. Военно-историческая библиотека
6. Каторин Ю.Ф. Защита акватории, как элемент безопасности объектов водного транспорта. Вестник полиции, 2014. - № 1. - С. 21-29
7. Каторин Ю.Ф., Ныркov А.П. Борьба с подводными диверсантами. Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2016. № 5-6 (95-96). С. 115-123.
8. International Code for the Protection of Ships and Port Facilities. 12 December 2002.
9. Miller Don. Underwater Special Forces - history, operations, equipment, weapons, training of combat swimmers. Minsk: "Harvest", 1998. c. 432.
10. Норченко А.Н. Проклятая тайна. СПб. Элмор, 1999. – 48 с.
11. Федеральный закон от 6 марта 2006 года «О борьбе с терроризмом [электронный ресурс] //http://www.fsb.ru/under/terror.html

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК 004.056.53

СОЦИАЛЬНЫЙ ИНЖИНИРИНГ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Хайруллов Артем Вадимович, Галлямова Миляуша Равильевна
Государственный университет морского и речного флота имени адмирала С.О. Макарова,
Россия, Санкт-Петербург, ул. Двинская, 5,
emails: 1516evro@mail.ru , Miljausha-18@mail.ru

***Аннотация*:** В статье рассматривается социальная инженерия. Социальная инженерия в контексте информационной безопасности относится к психологическим манипуляциям людьми, для совершения ими действий, либо разглашения конфиденциальной информации. Применятся для сбора информации, мошенничества или доступа к системе, путем получения доверия у оппонента.

***Ключевые слова*:** *политика безопасности, информационная безопасность, социальный инжиниринг, социальный инженер, несанкционированный доступ.*

SOCIAL ENGINEERING AND INFORMATION SECURITY

Khairullov Artem,Gallyamova Milyausha
Admiral Makarov State University of Maritime and Inland Shipping,
Russia, St. Petersburg, Dvinskaya str. 5,
emails: 1516evro@mail.ru, Miljausha-18@mail.ru

***Abstract:* This article discusses a s**ocial engineering**.** Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access.

***Keywords**: security policy, information security, social engineering, social engineer, unauthorized access.*

Введение. Область информационной безопасности является динамично развивающейся дисциплиной. Хотя эффективность мер безопасности для защиты конфиденциальной информации растет, люди остаются восприимчивыми к манипуляции и человеческий фактор остаётся самым слабым звеном [1].

Пока службы безопасности устанавливают новое антивирусное ПО, разрабатывают сложную систему идентификации и аутентификации, злоумышленники проникают внутрь сети с помощью сотрудников компании и, ничего не подозревающих, пользователей.

При получении доступа к сети применяется один из самых популярных методов взлома, так называемый социальный инжиниринг, на который, уделяют меньше всего внимания. Социальный инжиниринг формируется на управлении человеком, используя его личные качества, для получения желаемых целей. Опытные социальные инженеры, прежде чем тратить время и усилия на другие способы для взлома паролей и получения доступа к системам, просто позвонят работнику и получат необходимые данные.

Социальная инженерия - это самый тяжелый вид атаки, относительно защиты против него, потому что он не может быть защищен только аппаратным или программным обеспечением. Успешная защита требует эффективной информационной безопасности, начиная с политики безопасности и руководящих документов, заканчивая оценкой уязвимости.

Питер Стивенсон указал, что 30% всех взломов происходит от чужаков: то есть людьми, которые не работают в организации. Это значит, что семьдесят процентов хакеров внутри организации. Мы должны помнить об этом, когда разрабатываем защиту от социальных инженеров [2**Ошибка! Источник ссылки не найден.**].

Успех социальной инженерии зависит от способности злоумышленниками манипулировать жертвой в выполнении определенных действий или предоставления конфиденциальной информации. Сегодня социальная инженерия признана одной из величайших угроз безопасности, стоящих перед организациями. Социальное проектирование отличается от традиционного взлома, в том смысле, что атаки социальной инженерии не обязательно предполагают эксплуатацию программного обеспечения или систем. В случае успеха многие атаки социальной инженерии позволяют злоумышленникам получить законный, санкционированный доступ к конфиденциальной информации.

Социальная инженерия в контексте информационной безопасности, относится к психологической манипуляцией людьми, с целью сбора информации, мошенничества, или получения доступа к системе [3].

Термин "социальная инженерия" относится к психологической манипуляции, связанный с общественными науками, но его использование заметили среди компьютерных профессионалов и информационной безопасности. Все методы социальной инженерии основываются на конкретных атрибутах человеческого принятия решений , известные как когнитивные предубеждения. Атаки, используемые в социальной инженерии могут быть использованы для кражи конфиденциальной информации сотрудников.

Социальный инжиниринг, совместно с техническими знаниями, используют для достижения следующих целей [4]:

1. Сбор информации о потенциальной жертве.
2. Получение информации, необходимой для несанкционированного доступа.
3. Вынуждение объекта совершить необходимые социальному инженеру действия.
4. Атака социального инженера разделяется на три стадии подготовки:
5. Определение точной цели.
6. Сбор информации об объекте обработки.
7. Разработка плана действий, моральная подготовка/тренировка.

Атаки социальных инженеров представлены на рисунке 1. В общем виде схема приведена в книге белорусского психолога и социолога В.П.Шейнова, который долгое время занимался психологией мошенничества [5**Ошибка! Источник ссылки не найден.**].

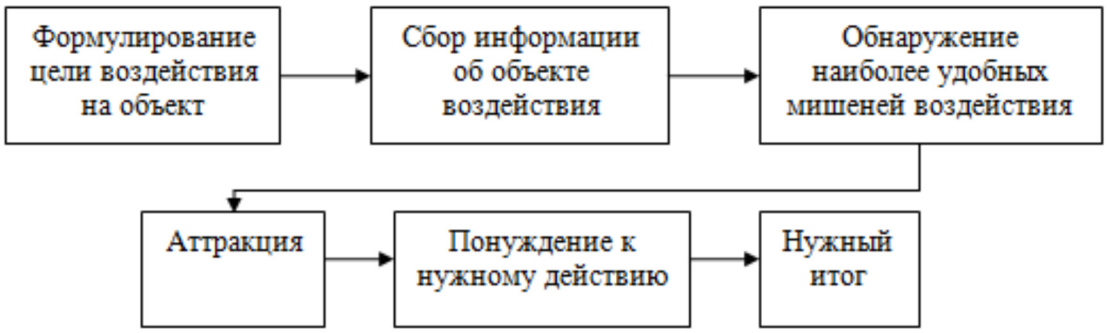


Рис. 1. Основная схема воздействия в социальном инжиниринге

Социальный инжиниринг делится на два вида: краткосрочный и долговременный.

Плюс краткосрочного в том, что он не требует лишнего времени, а минус - это то, что злоумышленник не может заставить человека сделать какие-то значимые действия.

Минус долговременного – продолжительность подготовки, ради того, чтобы подчинить себе человека. Плюс в том, что можно заставить человека сделать какие-то значимые действия.

Основными причинами успешных реализаций атак социальных инженеров являются следующие черты характера человека:

– Страх – самая используемая черта человека, так как из-за страха люди способны сделать то, чего бы они ни в коем случае не сделали в нормальных условиях.

– Любопытство - бессознательное стремление к познанию.

– Жадность - неумеренное желание владения или потребления. Людям свойственно вестись на столь очевидное "кидалово", сулящее невиданную прибыль буквально из ниоткуда.

– Превосходство - это состояние, когда ты чувствуешь себя на вершине. Но если попытаться доказать что ты не победитель, а наоборот «конкретный неудачник», то естественно это заденет самолюбие и жертва начнет доказывать что именно она тут доминирует.

– Великодушие и жалость – эти два похожих психокомплекса ориентированы на то, что людям свойственно помогать другим, если тот попал в беду.

– Доверчивость – здесь идет акцент на то, что людям проще верить, что их никто не обманет, чем думать своей головой. Именно эта черта использовалась при действии пирамид "МММ", "Русский Дом Селенга", т. д.

– Лень - для человека типично откладывать дела на потом, делать всё не по правилам, а так как ему кажется лучше и удобнее. К сожалению, из-за этого появляется много брешей в защите компании.

Теперь рассмотрим распространенные техники и виды атак, которыми пользуются социальные инженеры:

1. Претекстинг – эта техника использует преднамеренно продуманный сценарий (претекст), чтобы привлечь целевую жертву и сделать так, чтобы жертва дала информацию или выполнила действия ,которые были бы вряд ли выполнены в обычных условиях. Сложный сценарий, чаще всего включает в себя некоторые предварительные исследования и использование этой информации для установления доверительных отношений. Этот метод может быть так же использован , чтобы уничтожить бизнес, раскрыв информации о клиентах, а также частными детективами , чтобы получить записи телефонных разговоров, полезные отчеты, банковские документы и другую информацию непосредственно от представителей службы компании. Информация может быть использована для создания еще большей легитимности при более жестких расспросов с менеджером, например , внести изменения счета, получить конкретные балансы и т.д.[3**Ошибка! Источник ссылки не найден.**]

2. Фишинг – это метод ,который обманным путем получает конфиденциальную информацию, посылая массовые рассылки электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов. (В письме содержится прямая ссылка на fakelink[1]). После попадания на страницу, пользователя просят ввести свои логин и пароль, если пользователь вводит верные данные, то мошенники получают доступ к личным данным, банковским счетам и т.п.[3**Ошибка! Источник ссылки не найден.**]

3. Вишинг – данная техника использует поддельную IVR[2] систему, чтобы воссоздать, законно звучащие, официальные звонки от банковских и других IVR систем. Чаще всего, жертве приходит запрос (обычно через фишинг электронной почты) о необходимости связи с банком через (в идеале звонок бесплатный) номер, для подтверждения или обновления какой-либо информации. Система требует аутентификации пользователя с помощью ввода PIN-кода или пароля. Типичная "вишинг" система будет отклонять пользователей непрерывно, заставляя жертву вводит PIN - коды или пароли несколько раз, часто раскрывающие несколько различных паролей. Более продвинутые системы создают агента по обслуживанию клиентов или эксперта по безопасности для дальнейшего допроса потерпевшего. Основное отличие вишинга в том, что, так или иначе, задействуется телефон.[3**Ошибка! Источник ссылки не найден.**]

4. Фарминг (англ. Pharming) – перенаправление жертвы по ложному интеренет-адресу. Для этого используется некая навигационная структура (файл "hosts[3]", система доменных имен – "DNS[4]"). Жертва открывает письмо или посещает какой-либо веб-сервер, на котором выполняется скрипт-вирус, при этом происходит искажение файла "hosts", в результате жертва попадает на один из ложных сайтов. Технических методов защиты от фарминга на сегодня просто не существует, но можно защищаться постоянным повторением и изучением нового.

5. Услуга за услугу – эта техника предполагает под собой звонок злоумышленника в организацию по корпоративному (внутреннему) телефону. Социальный инженер звонит по внутреннему номеру компании, и утверждает, что он из службы технической поддержки. Он информирует жертву о каких-либо нарушениях системы и просит в целях безопасности пройти быструю проверку на возникновение технических проблем. И пока "решаются" технические проблемы, злоумышленник "заставляет" свою жертву делать то, что позволит ему получить доступ или запустить вредоносное ПО.[3**Ошибка! Источник ссылки не найден.**]

6. Троянский конь (троянская программа) – это вредоносная программа, которая используется для сбора информационных ресурсов, нарушения работы системы противника, либо доступа в саму систему. Злоумышленник отправляет e-mail, в котором содержится "классный" скрин-сейвер, важное обновление антивирусного ПО или даже компромат на сотрудника. От этой техники можно защититься тем, что можно перестать нажимать по всем подряд вложениям.[3]

Для достижения своей цели вирусописатели используют человеческие слабости:

– недостаточная подготовка;
– желание выделиться;
– жалость и милосердие;
– желание просмотра"интересного" контента;
— интерес к продукту, который нужен населению или который очень сложно достать;

---

1. [1] **Fakelink** - поддельная страница, которая внешне неотличима от настоящей, либо сайт, содержащий редирект (автоматическое перенаправление пользователей с одного сайта на другой).

2. [2] **IVR** (англ. *Interactive Voice Response*) — система предварительно записанных голосовых сообщений, выполняющая функцию маршрутизации звонков внутри call-центра с использованием информации, вводимой клиентом на клавиатуре телефона с помощью тонального набора.

3. [3] **hosts** — текстовый файл, содержащий базу данных доменных имен и используемый при их трансляции в сетевые адреса узлов. Запрос к этому файлу имеет приоритет перед обращением к DNS-серверам. В отличие от системы DNS, содержимое файла контролируется администратором компьютера.

4. [4]**DNS** (англ. *Domain Name System* — система доменных имён) — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене.

— интерес к методикам быстрого обогащения с помощью финансовых пирамид, супер-идей для успешного бизнеса или беспроигрышной игры в казино.

1. "Дорожное яблоко" – данная техника использует физические носители и опирается на любопытство или жадность жертвы. В это атаке, злоумышленники оставляют вредоносные (инфицированные) диски или USB - накопители в местах, где люди находят их (ванные комнаты, лифты, тротуаров, парковок и т.д.), наклеивают на носитель логотип фирмы и ждут, пока его найдет жертва. Любопытный сотрудник может найти его и вставить диск в компьютер, дабы удовлетворить его любопытство, или "добрый самаритянин" может найти его и вернуть в компанию. В любом случае, просто вставив диск в компьютер устанавливаются вредоносные программы, что дает злоумышленникам доступ к компьютеру жертвы и, возможно, к внутренней сети компании.[3**Ошибка! Источник ссылки не найден.**]

2. Сбор информации из открытых источников. Это сбор из открытых источников, преимущественно из социальных сетей. Например такие, как "Facebook", "Одноклассники", "VK" имеют большое количество данных, которые люди выставляют напоказ.

3. Обратный социальный инжиниринг. Это тот случай, когда жертва сама рассказывает социальному инженеру нужные ему данные. Многие люди для более быстрой работы или устранения неполадок, добровольно сообщают логины и пароли, а так же другие конфиденциальные сведения.

Обратный социальный инжиниринг действует в трех этапах:

– создание ситуации, которая вынуждает человека обратиться за помощью;
– реклама своих услуг;
– оказание помощи и воздействие.

1. Человеческий отказ в обслуживании – смысл этого метода заключается в том, чтобы потенциальная жертва (незаметно для неё) не среагировала на ситуацию, то есть социальный инженер делает так, чтобы его слова воспринимались как истина, не поддающаяся сомнению, либо отвлекает внимание жертвы. Злоумышленник представляет ложное понятие об одной операции, а на деле выполняет совсем другую. Таким образом, жертва работает над одним, не замечая другого.

2. Личный визуальный контакт – является одним из самых сложных методов социального инжиниринга. Продемонстрировать этот метод могут только профессионалы своего дела, так как при данной атаке необходимо хорошо знать психологию и уметь просчитывать действия собеседника на много шагов вперед. Техника работает следующим образом: вычисляется слабое место потенциальной жертвы, находится это с помощью анализа ответов на вопросы, дальше социальный инженер беседует с жертвой "в рамках слабого места", что в дальнейшем приведет к тому, что жертве понравится её собеседник, и та расскажет все, что необходимо социальному инженеру.

3. Системы обмена мгновенными сообщениями (IM). В данный момент в сети существует куча программ, которые могут влиять на работу ICQ, Skype, Messenger, WhatsApp и др. С их помощью злоумышленник может посылать сообщения от имени другого пользователя, в котором он может провести атаку в виде специально сформированного текста, но основным путем распространения вирусов через IM является передача файлов. Microsoft Windows по умолчанию не показывает расширения имен (например: имя файла "foto.jpg.exe" будет показано как "foto.jpg"). Для маскировки реального расширения применяется двойное расширение вроде "xxx.jpg.exe" (тут помогает то, что некоторые почтовые серверы отказываются пропускать исполняемые файлы) или добавляется большое количество пробелов, из-за чего имя файла отображается не полностью.

На рисунке 2 показано, как работает имитация при использовании электронной почты и IM.

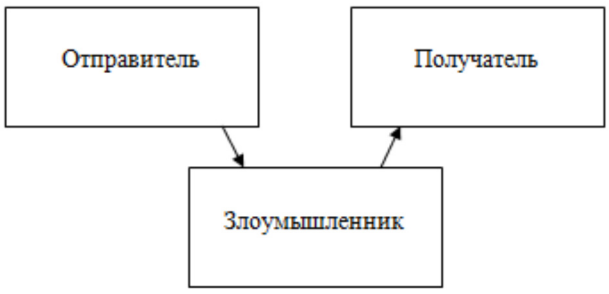


Рис. 2. Имитация при использовании IM и e-mail

1. Анализ мусора – это именно тот метод, которому уделяют, пожалуй, меньше всего времени. Социальный инженер может использовать деловые бумажные отходы таким образом, чтобы во время атаки казалось, что он является сотрудником организации. Например, устаревшие бумаги из отдела кадров, провели через шредер и выбросили на улицу. Злоумышленник их нашел, воссоздал и узнал данные о бывших сотрудниках фирмы, чем в дальнейшем он может воспользоваться.

2. Личностные подходы. Одна из самых простых методик социального инжиниринга. В данной технике используют четыре основных разновидности подхода:

– запугивание;
– убеждение;
– использование доверительных отношений;
– помощь.

Заключение. В результате мы видим, как важно защищать информационную безопасность со стороны психологии, так как самое слабое звено в системе - это человеческий фактор.

Полностью уберечь себя от атак социального инжиниринга практически невозможно, но можно соблюдать некоторые правила, благодаря которым можно добиться очень высоких результатов.

Основные рекомендации, которых стоит придерживаться любому сотруднику:

1. Постоянно изучать новые методы защиты информационной безопасности и не забывать повторять старые.
2. Проходить тренинги, которые будут повышать бдительность.
3. Соблюдать элементарные правила безопасности, несмотря ни на что.
4. Быть аккуратным и сосредоточенным.
5. Не доверять посторонним людям.
6. Не открывать конфиденциальную информацию по телефону или электронной почте, если это не прописано в политике безопасности.
7. Правильно обращаться с документами и физическими носителями, а также их устранением.
8. Ответственно относиться к работе.
9. Важно помнить, что любое должностное лицо может стать жертвой социального инженера.

СПИСОК ЛИТЕРАТУРЫ

1. Теплов Э.П. Гуманитарные аспекты информационной безопасности: методология и методика поиска истины, построения доказательства и защиты от манипуляций / Э. П. Теплов, Ю. А. Гатчин, А. П. Нырков, В. В. Сухостат. – СПб: Университет ИТМО, 2016. – 120 с.
2. Социальное проектирование: концепции и решения [Электронный ресурс] http://www.infosectoday.com/Articles/Social_Engineering.htm#.WS20jKAzqoj (последнее обращение: 12.09.2017).
3. Социальная инженерия [Электронный ресурс] https://en.wikipedia.org/wiki/Social_engineering_(security) (последнее обращение: 12.09.2017).
4. Теплов Э.П. Гуманитарные аспекты информационной безопасности: получение, анализ и оценка деловой информации / Э. П. Теплов, А. П. Нырков, А. В. Башмаков, Е. К. Брагина. – СПб.: Издательский Дом «Афина», 2016. – 160 с.
5. Социальная инженерия [Электронный ресурс] http://ru.wikipedia.org/wiki/Социальная_инженерия (последнее обращение: 11.09.2017).
6. Теплов Э.П. Гуманитарные аспекты информационной безопасности: основные понятия, логические основы и операции / Э. П. Теплов, Ю. А. Гатчин, А. П. Нырков, А. Г. Коробейников, В. В. Сухостат. – СПб: Университет ИТМО, 2016. – 122 с.

УДК 347.965.32

МЕТОДЫ ВОЗДЕЙСТВИЯ И ЗАЩИТЫ ОТ ВИРУСНЫХ ВИДЕОРОЛИКОВ

Юмашева Елена Сергеевна, Ежгуров Василий Николаевич
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Россия, Санкт-Петербург, ул. Двинская, 5/7,
emails: elena_umasheva@mail.ru.

***Аннотация**:* В данной статье будет рассмотрено создание и внедрение вирусных видеороликов, а также их психологическое и информационное воздействие на человека и методы борьбы с ними.

***Ключевые слова:** Информационное воздействие, психологическое воздействие, вирусные видеоролики.*

METHODS OF EXPOSURE AND PROTECTION FROM VIRUS VIDEOS

Yumasheva Elena, Ezhgurov Vasily
State University of the Marine and River Fleet named after Admiral S.O. Makarova
Russia, St. Petersburg, st. Dvinskaya, 5/7,
emails: elena_umasheva@mail.ru.

***Annotation**:* This article will consider the creation and implementation of viral videos, as well as their psychological and informational impact on humans and methods of combating them.

***Keywords:** Information impact, psychological impact, viral videos.*

Описание явления вирусной рекламы

Традиционная реклама стала терять свою актуальность и эффективность, в связи с достаточно простым отключением рекламных баннеров в браузерах или же переключением каналов, если реклама представлена на телевидении и т.п. На смену традиционной рекламе распространение, которой оплачивалось заказчиком, пришел вирусный маркетинг, представляющий собой метод быстрого распространения рекламного сообщения силами потребителей. Такой маркетинг в первую очередь

основан на желании людей делится новой и полезной информацией, и его главная цель создание условий (эмоциональных, психологических), благодаря которым товар начинают активно продвигать сами пользователи.

Одним из наиболее популярных инструментов вирусного маркетинга, является вирусное видео. Видео, которое распространяется в сети Интернет преимущественно через социальные сети самими интернет-пользователями путем добровольного размещения ими данного видео на своих страницах. [1] Передается открытое или же скрытое сообщение в виде смешного или невероятного видео.

Вирусный маркетинг основывается на методах скрытого воздействия на потребителя. Пользователь не должен догадываться, что стал объектом рекламного воздействия, но при этом вся необходимая информация откладывается в голове. Поэтому при создании вирусных видео прежде всего опираются, во-первых, на правильный подбор целевой аудитории (ЦА) [2]. Например, компания «Production House Компас» рекомендует, если ЦА предполагаемого объекта продвижения присутствует на рисунке 1, то обязательно использовать создание вирусных рекламных роликов для продвижения своих продуктов [3].

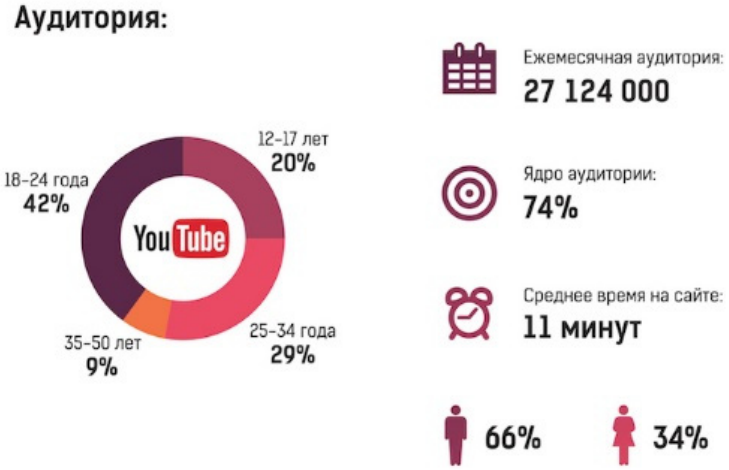


Рис.1. Целевая аудитория.

Во-вторых, на создание парадокса. Парадокс – утверждение/действие, резко расходящееся с общепринятым, устоявшимся мнением, отрицание того, что представляется «безусловно правильным» [4]. Проще говоря, условия, в которых то, что случилось с рекламируемым продуктом, случиться не могло, либо при которых это является закономерным следствием, тем не менее потрясающим всех своей парадоксальностью. Пользователям нравится, когда видео идут вразрез с их ожиданиями. Например, одним из самых ярких 2016 года стал клип американской группы «OK GO» и компании «S7 Airlines» под названием «Гравитация как привычка», благодаря, парадоксу. Никогда и никто ранее не снимал видеоклипы в невесомости, это казалось чем-то недостижимым, но вот мы видим музыкантов, легко выполняющих различные трюки с невероятным эмоциональным посылом. Они разрушают стереотипы, создав новую, неожиданную идею, и посылают огромный положительный заряд эмоций, яркими красками.

В-третьих, на хорошо продуманный сценарий. При создании сценария можно провести небольшой опрос, по имеющимся идеям, в ходе которого попросить людей предсказать, что произойдет в том или ином видео, и уже основываясь на этих предположениях и на реакции можно выбрать одну из наилучших идей. Так компания «Knorr» сняла видеоролик о социальном эксперименте, в котором психологи пытались подобрать пары на основе их кулинарных предпочтений. Однако пара должна была не просто поужинать, а кормить друг друга. Видео набрало 60,4 млн просмотров, из-за непринужденности и естественности в общении, у пользователя не возникает ощущения о том, что видео псевдо реально и его вовлекают в рекламу продукта.

Объединив 3 главных столпа, можно получить популярный ролик с многомиллионным/миллиардным количеством просмотров.

Эффекты, достигаемые вирусной рекламы[5]:

1. Эмоциональная привязка. Эмоции – это один из главных факторов заставляющий пользователя делится и запоминать контент.
2. Увеличение продаж.
3. Трафик. Посещаемость сайта может увеличится в несколько десятков раз, соответственно и возрастает прибыль.

4. Популярность. Владельцы пабликов, публичные люди, журналисты берут ролик как информационный повод, бесплатно размещая на своих площадках.

Пример создания вирусного ролика, для продвижения курсов иностранных языков.

Задача: Выпустить новый бренд на рынок. Попасть в самые крупные интернет-СМИ страны. Мотивировать людей к записи на курсы через сайт.

Идея: Поставить людей в неловкое положение из-за незнания иностранного языка.

Решение: Поиск актера с навыками разговорного английского. Его роль заключается в том, что он как заблудившийся иностранный турист предлагает 100 долларов тому, кто подскажет, как пройти на вокзал. Естественно, многие люди не готовы к такому и это ставит их в неловкое положение.

Стоит отметить, что вирусные ролики – это не прямолинейный рассказ о товаре или позиции, который превозносит качества и достоинства. Вирусные видеоролики – это только намек на продукт, услугу, позицию, здесь главное сюжет, заставляющий зрителя, поделится ссылкой с друзьями, знакомыми, коллегами. С повышением просмотров появляется все большая узнаваемость товара, вследствие чего увеличивается количество переходов на сайт рекламодателя и повышается количество заказов, по рекламируемому товару. Все это достигается путем кропотливой работы специалистов, знающих механизмы воздействия на эмоции людей через идею, картинку звук.

Одними из наиболее основополагающих и часто используемых методов информационного воздействия, являются:

– Заражение. Достаточно древний механизм, представляющий собой передачу эмоционально –психологического настроя от одного человека к другому, основывающийся на апелляции к эмоционально бессознательной сфере человека (заражение смехом, раздражением, паникой и т.п.);

– Внушение. Основано на апелляции к бессознательному т. е. на подсознание, эмоции, но уже не примером, как в заражении, а словесным средством. Причем внушающий человек должен быть абсолютно уверен в себе, его задача всем своим видом вызывать уважение к себе т.е. оказывать влияние на подсознание. Такой способ называется вербальным и осуществляется словесными средствами.

– Внушаемость. Повышенная подверженность внушениям извне или своим собственным. Чаще всего внушению подвержены люди со слабой нервной системой, имеющие склонность к подражанию, лица с резкими колебаниями внимания (женщины, дети). Немало важное влияние на степень внушения человека оказывают неразвитость логического мышления, низкий интеллект, некритический склад ума. По средству группового внушения человек видевший перед собой, например, белую и черную пирамиду, может сказать, что видит 2 белые пирамиды, потому что до него 7 человек говорили о том, что однозначно видят 2 белые пирамиды.

– Убеждение. Предполагает достаточно высокий уровень развития логического мышления и апеллирует логике и разуму человека. Однако стоит помнить, что содержание и уровень убеждения должны соответствовать уровню развития личности, уровню мышления. Процесс убеждения начинается с восприятия и оценки источника информации. Слушатель сравнивает информацию, имеющуюся у него и информацию и преподносимую источником выявляя неточности, скрытие фактов, речевые ошибки и в случае успешного выявления уровень доверия к источнику резко снижается.

Также стоит отметить, что убеждение основано на логических приемах доказательств, с помощью которых обосновывается правдивость изложенного мнения. Логические приемы доказательства:

– Тезис – мысль, истинность которой требуется доказать, тезис должен быть ясно, точно изложен и обоснован фактами;

– Довод – мысль, истинность которой уже доказана и поэтому имеет право на приведение для обоснования истинности или ложности тезиса;

– Демонстрация – логическое рассуждение, совокупность логических правил, используемых в доказательстве.

Примером убеждения является продажа «чудо» средств для людей, стремящихся похудеть, предлагая препараты мгновенного действия за определённую сумму денег с подтверждением эффекта фото, видео съемкой, комментариями в социальных сетях, людей якобы использующих это средство.

Помимо постановочных вирусных видео, существуют реальные ролики, захватившие огромное количество публики. Такие видео могут быть случайно засняты на мобильный телефон, экшн камеру или же на камеру наружного наблюдения. Однако если вирусный маркетинг основывается на психологии, выборке целевой аудитории и т.п., то как простому человеку без специалистов удается набрать бешенный рейтинг ведь в сеть каждую минуту загружают огромное количество роликов.

Существует как минимум 3 фактора популярности:

1. Знаменитые люди. Зачастую видео становится популярным после того как на них наталкивается знаменитость и делится ссылкой на него со своими подписчиками. В нынешнем году интернет взорвал танцующий подросток Рассел Хорнинг, после того как его заметила певица Кэти Перри, пригласившая его выступить вместе с ней на шоу «Saturday Nigh Live» [6].

2. Эффект неожиданности. Видео противоречит ожиданиям. Например, на данный момент видео на геймерской платформе Twitch завязано на таком эффекте [7].

3. Пародии на популярные ролики. Видео становится для миллионов пользователей инсайдерскими шутками, которыми охотно делятся. Так было с исполнителем PSY на песню «Gangnam Style» и более популярным видео японца Пико Таро «Pen Pineapple Apple Pen» [8].

Методы защиты от манипулирования сознанием человека

Снижение или полное отключение способности сопротивляться это первые ступени на пути информационного воздействия. Достаточно вывести человека из состояния равновесия и отключить формы внутреннего контроля для последующей работы с психикой человека. На этом этапе используются довольно много приемов способствующих удивлению, поражению человека.

На данном этапе могут использоваться самые разные приемы и эффекты, помогающие удивить, поразить, «сбить с толку» человека. Главной целью является психологическое воздействие на человека до такой степени пока объект не разрешит себе изменить своим принципам, себе.

Такая методика довольно стара, но все же менее эффективнее от это этого не становится. В средних веках ее активно использовали христианские миссионеры. Огромные храмы, поражающие своим великолепием, изобилие цветов, благовонья, дым свечей и конечно органная музыка. В таком месте человек легко терял, во-первых, душевное равновесие и внутренний покой, во-вторых, становился легкой мишенью, потому что достаточно просто становилось обеспокоить, ослабить существующие стереотипы и представления. Человек терял привычную позицию как внутри себя, так и в окружающем мире, после чего становится абсолютно открытым к внушению чужого мнения и различных «спасительных» установок.

Сегодня человек, находящийся в состоянии удивления, восхищения, внутреннего распутья или возмущения – самая удобная жертва для различного вида воздействия. Стоит помнить несколько методов защиты от информационного воздействия:

– Знание залог успеха. Необходимо знать основные способы манипулирования и на что они направлены.

– Эмоции и чувства. Манипулирование направлено на жонглирование эмоциональным фоном человека и психологическим, следовательно, защитой может служить самоконтроль, разумный взгляд на вещи.

– Выявление. Вскрытие замысла информационного источника, своего рода тренировка головного мозга, сначала это может быть просто увлекательно, а потом войдет в привычку.

– Оценка. Негативная оценка манипуляторного сигнала, его осуждение, все это ослабляет или сводит на нет информационное воздействие.

– Интересы. Четкое и ясное сохранение в сознании главных интересов.

– Мышление. За частую достаточно просто включить логическое мышление и все сразу станет ясно, не стоит доверять бездумно всем и каждому.

– Комфорт. В расслабленном состоянии человек становится более внушаемым.

Это одни из наиболее действенных методов, которые помогут преодолеть манипуляторное воздействие.

Заключение

Подводя итоги можно сказать, что вирусный маркетинг является одним из наиболее эффективных способов рекламы. Он основан на особенности человека делится интересной информацией. Вирусный маркетинг использует довольно старые, однако действенные и основанные на создании условий, при которых продвигаемый товар/услуга активно советуют сами потребители, способствуя сокращению расходов на проведении различных рекламных компаний. В связи с этим стоит помнить о методах противодействия, ведь с каждым днем уловок информационного воздействия на человека становится все больше.

СПИСОК ЛИТЕРАТУРЫ

1. Википедия, Свободная энциклопедия, [электронный ресурс] https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D1%80%D1%83%D1%81%D0%BD%D0%BE%D0%B5_%D0%B2%D0%B8%D0%B4%D0%B5%D0%BE
2. Вирусное видео. Секреты и технологии. Богатов Валерий. 2016 г. с. 5-10.
3. Компас, Производство вирусного ролика, [электронный ресурс] http://www.kompas.by/proizvodstvo-virusnogo-rolika.html
4. Академик, Словарь, [электронный ресурс] http://research_activities.academic.ru/809/%D0%9F%D0%B0%D1%80%D0%B0%D0%B4%D0%BE%D0%BA%D1%81
5. Про бизнес, Как «сварить» вирусное видео, которое сработает, [электронный ресурс] URL [https://probusiness.io/ideas/2275-kak-svarit-virusnoe-video-kotoroe-srabotaet-formula-ot-gomelskogo-agentstva-djo-by.html]
6. Rutube, Российский видеохостинг, [электронный ресурс] https://rutube.ru/video/f2d9aef05a5abc3bc3523d0c87ad9ed7/
7. YouTube, Streamer's daughter walks in on him while playing a scary game [электронный ресурс] https://youtu.be/VJCplifwxsI
8. YouTube, Pen-Pineapple-Apple-Pen [электронный ресурс] https://www.youtube.com/watch?v=52pFPYYEYtg

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОЛОГИИ

УДК 551.593

ЗАТМЕННОЕ ЗОНДИРОВАНИЕ ВЕРХНЕЙ АТМОСФЕРЫ ЗЕМЛИ С ПИЛОТИРУЕМОЙ ОРБИТАЛЬНОЙ СТАНЦИИ: ПОЛУЧЕНИЕ И СОХРАНЕНИЕ ИНФОРМАЦИИ

Бузников Анатолий Алексеевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
emails: aabuznikov@mail.ru

***Аннотация*:** Приведены результаты эксперимента по затменному зондированию атмосферы с пилотируемой орбитальной станции для исследования вертикального распределения малых газовых компонентов. Рассмотрены возможности получения и сохранения информации о глобальном состоянии верхней атмосферы Земли.

***Ключевые слова**: затменное зондирование атмосферы; спектрофотометрия; концентрация водяного пара.*

ECLIPSING REMOTE SENSING OF THE EARTH'S UPPER ATMOSPHERE FROM MANNED SPACECRAFT: OBTAINING AND SAVING THE INFORMATION

Buznikov Anatoliy
St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
emails: aabuznikov @mail.ru

Abstract: Results of the experiment on the eclipsing remote sensing of the Earth's upper atmosphere are given. The paper describes the opportunities for obtaining and saving the information on the global state of the upper atmosphere.

***Keywords**: eclipsing remote sensing of the atmosphere; spectrophotometry; water vapor concentration.*

Введение. Среднесрочный и долгосрочный прогнозы погоды для отдельных регионов базируются на информации о глобальном состоянии атмосферы. Причём большое значение имеет информация о распределении концентрации малых газовых компонентов, таких как водяной пар, озон, окислы азота и др., в верхних слоях атмосферы. Они непосредственно взаимодействуют с солнечным излучением и влияют на его поглощение и перенос в атмосфере.

Разработка методов и аппаратуры для постоянного слежения за распределением малых газовых компонентов в стратосфере и мезосфере важна для практического претворения в жизнь Всемирной климатической программы [1]. Интерес к изучению распределения малых газовых компонентов вызван также возрастающим уровнем загрязнения атмосферы, важностью изучения фотохимических процессов в стратосфере и мезосфере, поисками зависимостей между пространственно-временными вариациями газовых и аэрозольных компонентов атмосферы и современными изменениями климата [2]. Изменение концентрации малых газовых компонентов может вызвать нарушение естественных процессов, протекающих в атмосфере, и различные нарушения экологического равновесия. Например, увеличение содержания водяного пара приведёт к изменению альбедо системы Земля – атмосфера. Сведения о вертикальном распределении водяного пара необходимы также для построения строгой теории теплового режима стратосферы и мезосферы.

Глобальный характер поставленной задачи потребовал разработки новых методов измерений с использованием средств космической техники, позволяющих осуществлять систематическое дистанционное слежение за состоянием атмосферы в планетарном масштабе. При этом весьма перспективен метод затменного зондирования атмосферы на скользящих оптических трассах при восходах и заходах Солнца относительно космического аппарата, на котором устанавливается спектрометр, регистрирующий поглощение солнечной радиации в отдельных, наиболее информативных полосах поглощения исследуемых атмосферных газов. Схема проведения эксперимента по затменному зондированию приведена на рис. 1.

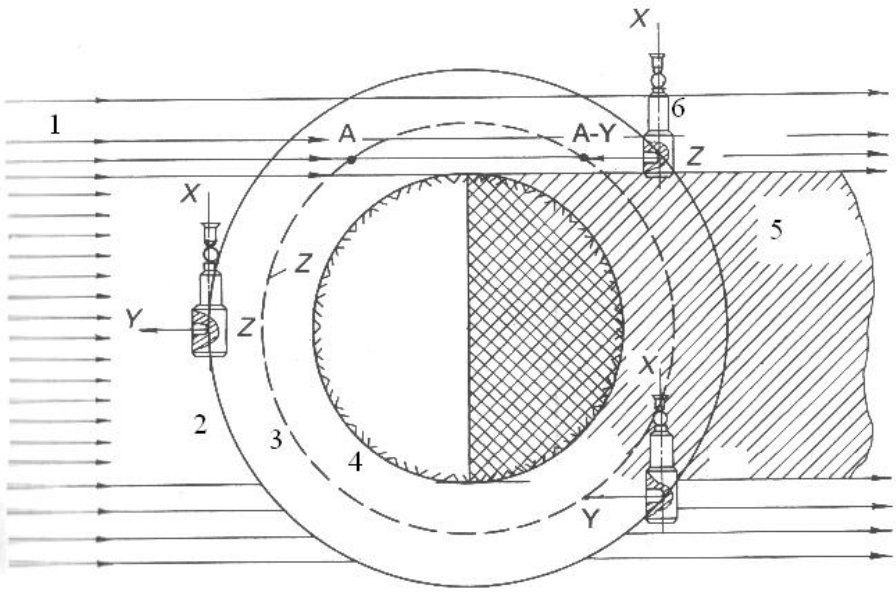


Рис. 1. Схема проведения эксперимента по затменному зондированию: 1 – солнечные лучи; 2 – орбита станции; 3 – условная верхняя граница атмосферы; 4 – поверхность Земли; 5 – тень Земли; 6 – пилотируемая орбитальная станция.

Впервые конкретная реализация метода затменного зондирования атмосферы для изучения вертикального распределения водяного пара была осуществлена во время полета орбитальной станции «Салют-4» [3], на борту которой был установлен комплекс солнечных спектрометров КСС-2. Это был первый в мировой практике негерметизированный спектрометр высокого разрешения, работавший за пределами герметичного корпуса станции в условиях высокого вакуума. С помощью КСС-2 впервые была реализована схема затменного зондирования атмосферы Земли и получены достоверные данные о вертикальном распределении водяного пара в стратосфере и мезосфере на высотах от 30 до 60 км.

Солнечная следящая система наводила входные щели спектрометров на геометрический центр солнечного диска с точностью до одной угловой минуты и удерживала их в таком положении во время проведения измерений. Параллельность входных щелей спектрометров к горизонту Земли в момент измерений осуществлялась за счет ориентации станции, совершающей поступательное движение в инерциальном режиме. Блок спектрометров КСС-2 был установлен за пределами герметичного корпуса станции «Салют-4» и включал в себя инфракрасный (ИК) спектрометр со спектральным каналом шириной 3800–3825 $см^{-1}$ и полушириной аппаратной функции 0,8 $см^{-1}$. Он осуществлял измерение поглощения солнечного излучения в 2,7 мкм полосе водяного пара. Ультрафиолетовый (УФ) спектрометр имел спектральный диапазон измерений 400 Å в области от 2000 до 3000 Å со спектральной шириной щели 2 Å. Спектрометр обладал высоким быстродействием. При измерении поглощения водяным паром в полосе 2,7 мкм каждый спектр шириной 3800–3825 $см^{-1}$ вместе с калибром записывается за 1,75 с, а контур основной информативной линии 3816,07 $см^{-1}$ – за 0,09 с.

На рис. 2 приведен пример записи спектров поглощения водяного пара на восходе Солнца. Измерения отношения смеси водяного пара в стратосфере и мезосфере, проведенные в зимний период над Маршалловыми островами, свидетельствуют о наличии сухой стратосферы с отношением смеси q_{H2O} = (2–28)×10^{-6} г/г на высотах от 30 до 60 км. Результаты детальной обработки полученных данных приведены в работе [4]. В дальнейшем разработанная методика затменного зондирования была успешно использована американцами при создании и запуске спутника UARS [5].

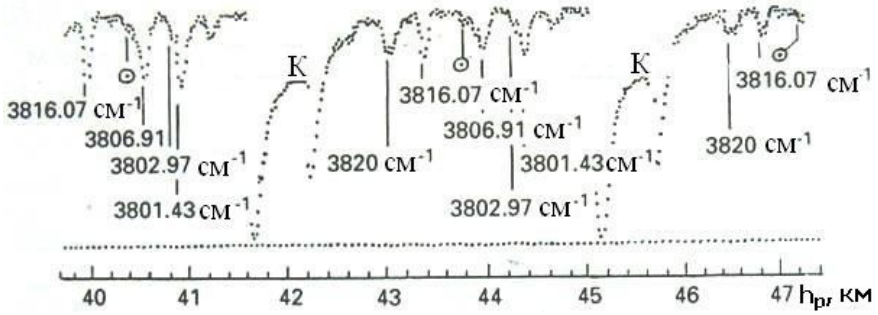


Рис. 2. Пример записи спектров поглощения солнечного излучения водяным паром в полосе 2,7 мкм на скользящих оптических трассах с помощью аппаратуры КСС-2 с пилотируемой орбитальной станции «Салют-4» при изменении высоты перигея линии визирования от 40 до 47 км (*К* – калибровочный сигнал).

При вращении космического аппарата вокруг Земли измерения проводятся на восходе и заходе Солнца. Космический аппарат за сутки делает 17 оборотов вокруг Земли, при этом спектрометр зафиксирует 34 разреза атмосферы в различных районах земного шара.

Заключение. Таким образом, за одни сутки будет получены глобальное распределение малых газовых компонентов в стратосфере и мезосфере. Последующее вращение космического аппарата позволяет получить данные о вертикальном распределении малых газовых компонентов на других участках атмосферы. Информацию о результатах затменного зондирования при пролёте над территорией России необходимо передавать на пункты приёма в реальном времени. При получении информации за пределами страны информация должна быть сохранена и передана на пункты приёма информации при пролёте над Россией или в реальном времени с использованием геостационарных ретрансляционных ИСЗ.

СПИСОК ЛИТЕРАТУРЫ

1. Кондратьев К. Я. Всемирная климатическая программа: принципиальные аспекты и перспективы осуществления // Информационный бюллетень семинара «Атмосфера–Океан–Космос» / Под ред. акад. Марчука Г.И.. М.: Межд. центр НТИ ГКНТ. 1980. Вып. 1. С. 26–46.
2. Кондратьев К.Я. Слежение за параметрами климата со спутников // Труды Главной геофизической обсерватории. 1980. Вып. 488. С. 75–102.
3. Бузников А. А. Космическая спектрофотометрия природной среды с пилотируемых орбитальных станций // Оптический журнал. 2015. Т. 82. № 7. С.114–122.
4. Кондратьев К.Я., Бузников А.А., Покровский О.М. Глобальная экология: дистанционное зондирование. М.: ВИНИТИ, 1992. 308 с.
5. UARS. Upper Atmosphere Research Satellite. NASA. Washington: D. C., 1989. 28 p.

УДК 551.501.45

ИНФОРМАЦИОННОЕ И ОПЕРАЦИОННОЕ ОБЕСПЕЧЕНИЕ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ДЕЯТЕЛЬНОСТИ СИЛОВЫХ СТРУКТУР И ОТРАСЛЕЙ ЭКОНОМИКИ РОССИИ

Доронин Александр Павлович, Щукин Георгий Георгиевич, Петроченко Вячеслав Михайлович, Козлова Наталья Александровна, Тимощук Александр Сергеевич, Шмалько Светлана Анатольевна,
Военно-космическая академия имени А.Ф.Можайского,
Россия, Санкт-Петербург, ул. Красного курсанта, д. 16
email: astim2@yandex.ru

***Аннотация*:** В статье рассматривается методический подход к проблеме обеспечения экологической безопасности деятельности силовых структур и отраслей экономики России на базе понятий информационного и операционного обеспечения. Авторами предлагаются геофизические методы и средства модифицирования окружающей среды, позволяющие устранить или в значительной мере снизить негативное влияние деятельности силовых структур и отраслей экономики России на окружающую среду.

Ключевые слова: *экологическая безопасность; окружающая среда; информационное обеспечение, операционное обеспечение.*

INFORMATION AND OPERATIONAL ENVIRONMENTAL SAFETY ACTIVITIES LAW ENFORCEMENT AGENCIES AND BRANCHES OF THE RUSSIAN ECONOMY

Doronin Aleksandr, Shchukin Georgiy, Petrochenko Vyacheslav, Kozlova Natalia, Timoshchuk Aleksandr, Shmalko Svetlana
Military - space academy named after A. F. Mozhayskiy,
Russia, St. Petersburg, Krasnogo kursanta st., 16
email: astim2@yandex.ru

Abstract: The article considers methodological approach to the problem of environmental safety activities of law enforcement agencies and branches of the Russian economy on the basis of the concepts of informational and operational security. The authors proposed geophysical methods and means of modifying the environment to eliminate or greatly reduce the negative impact of the activities of law enforcement agencies and branches of the Russian economy on the environment.

Keywords: *ecological safety; environment; information assurance, operational assurance.*

Введение. Негативное влияние загрязнения окружающей среды (ОС) на деятельность человека обусловливает необходимость поиска и разработки методов и средств, позволяющих устранить или в значительной мере снизить это негативное влияние. Наряду с совершенствованием технических средств сбора и обработки информации обокружающей среде, повышением качества прогнозирования опасных уровней загрязнения ОС в последние годы для этих целей предлагается использовать геофизические методы и средства модифицирования окружающей среды.

Информационное и операционное обеспечение экологической безопасности деятельности силовых структур и отраслей экономики России.

К настоящему времени установлено, что объектами модифицирования со стороны человека могут быть процессы и явления, наблюдающиеся практически во всех геосферах Земли (рис. 1) [1]. Вместе с тем, необходимо отметить, что уровень разработки методов и средств модифицирования (МОДИФ) различных геосфер далеко не одинаков и колеблется от уровня гипотез (как, например, в случае МОДИФ вулканов) до практического применения (как, например, в случае МОДИФ облаков и туманов).

Наличие в нашей стране конкретных методов и средств МОДИФ облаков и туманов (рис. 2, табл. 1) [2], а также многолетняя практика их применения для решения широкого круга прикладных задач (рис. 3) (например, регулярное рассеяние облаков над Москвой для проведения праздничных и спортивно-массовых мероприятий, тушение лесных пожаров искусственными осадками, перераспределение осадков и др.) приводят к пониманию того, что следует различать информационное и операционное обеспечение экологической безопасности (ИОЭБ и ООЭБ) (рис. 4).

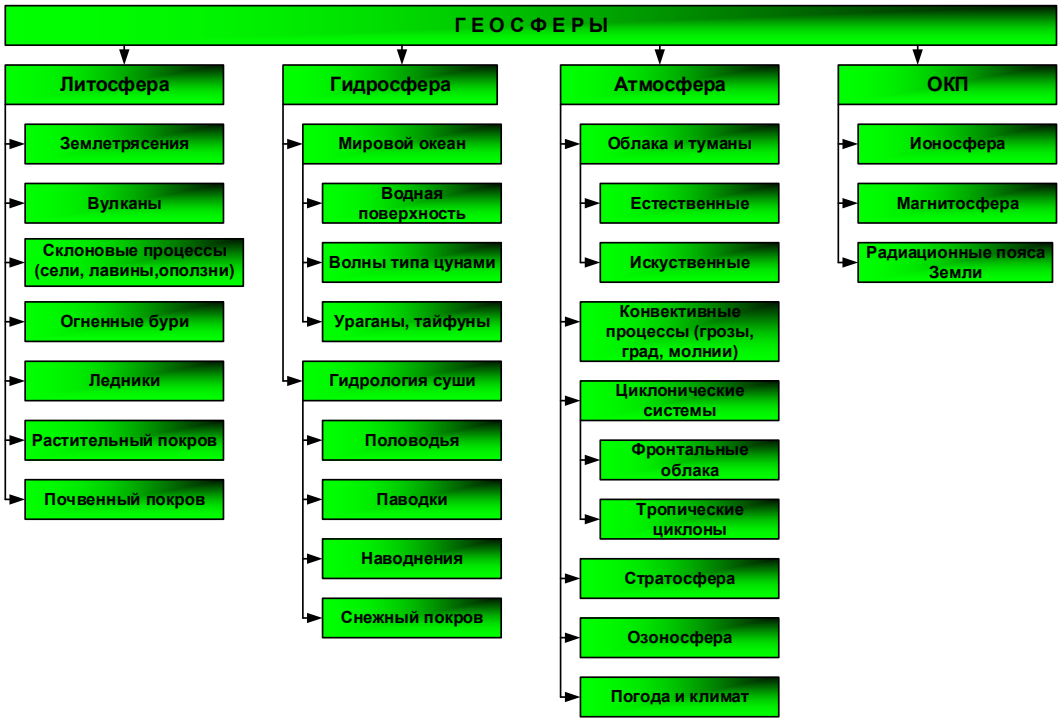


Рис. 1. Перечень геофизических процессов и явлений как возможных объектов модифицирования

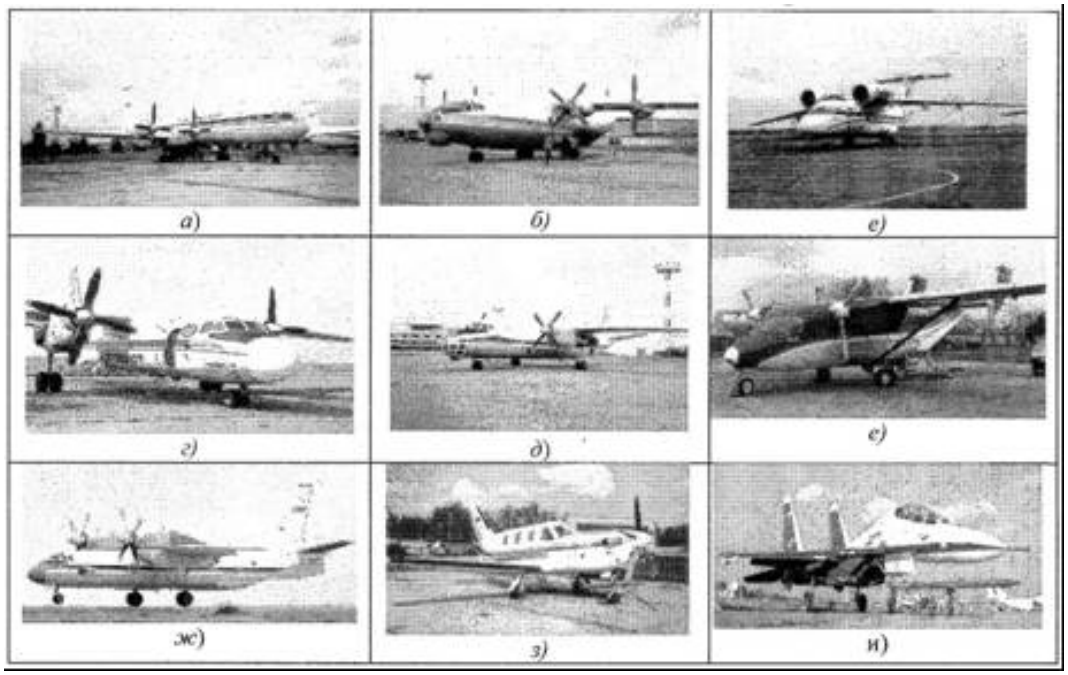


Рис. 2. Самолеты, используемые в работах по модифицированию облаков

а) Ил-18; б) Ан-12; в) Ан-72; г) Ан-26; д) Ан-30; е) Ан-28; ж) Ан-32; з) М-101Т «Гжель»; и) СУ-30

Таблица 1

Основные характеристики самолетов, используемых в работах по модифицированию облаков

Тип сам-та / Хар-ка	Ил-18	Ан-12	Ан-72	Ан-30	Ан-32	Ан-26	Ан-28	М-101Т Гжель	СУ-30
Взлетная масса, кг	61 000	61 000	33 000	21 000	27 000	24 000	6 500	3 720	33 000
Крейсерская скорость, км/ч	617	590	550	430	530	430	337	360	360-2 200
Практический потолок, м	10 000	9 800	11 800	7 300	9 400	7 300	6 000	8 000	20 000
Максимальная дальность полета, км	4 270	4 560	4 400	2 550	2 160	2 340	1 250	1 400	3 200
Максимальная полезная нагрузка, кг	13 500	20 000	10 000	5 500	6 700	4 100	2 000	630	7 000

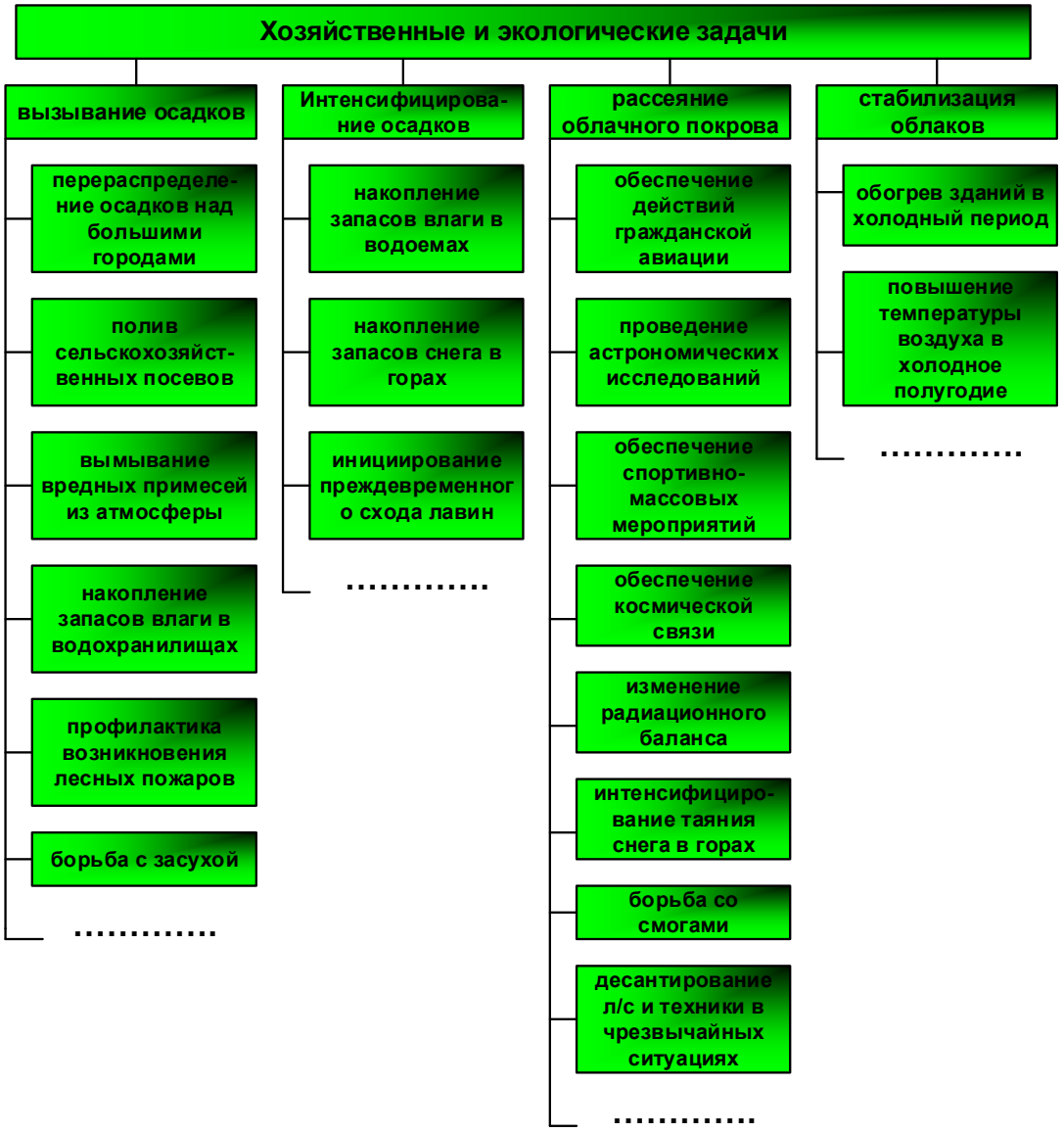


Рис. 3. Перечень прикладных задач, решаемых при модифицировании облаков

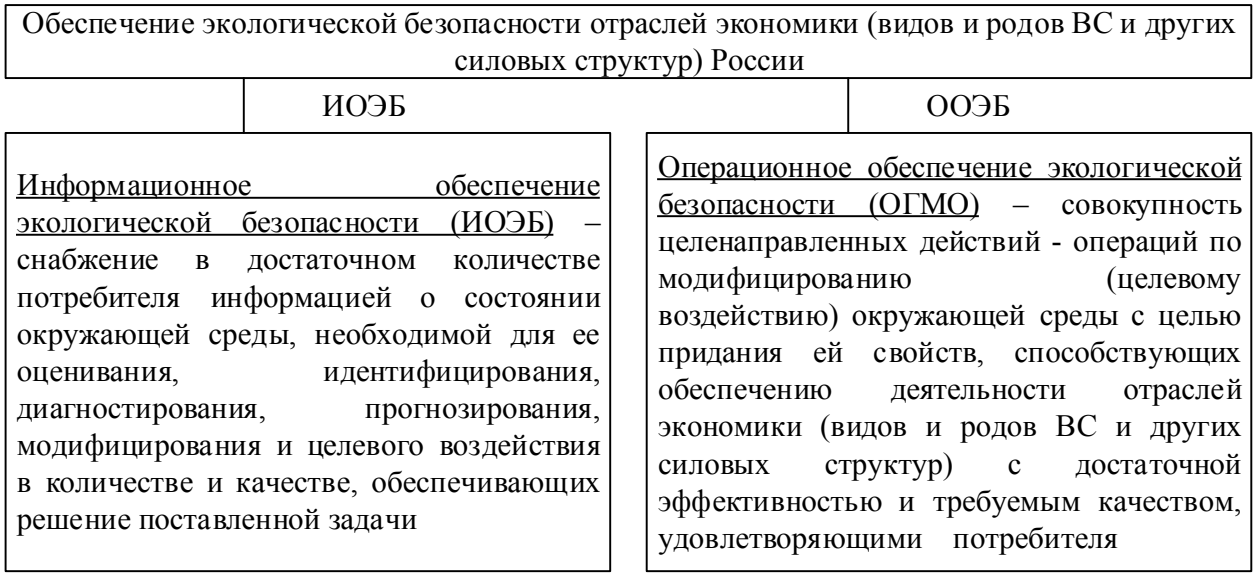


Рис.4. Информационное и операционное обеспечение экологической безопасности деятельности отраслей экономики (видов и родов ВС, других силовых структур) России

Необходимо отметить, что ИОЭБ и ООЭБ взаимосвязаны. Эта взаимосвязь проявляется в том, что для получения и переработки информации (в том числе и экологической) необходимо проводить операции (целенаправленные действия), а для организации и проведения операций необходима информация о состоянии окружающей среды. Поэтому, говоря об ООЭБ, необходимо иметь в виду потребное ИОЭБ, и, наоборот, говоря об ИОЭБ, следует иметь в виду ООЭБ. Схематично, взаимосвязь между ООЭБ и ИОЭБ изображено на рис. 5.

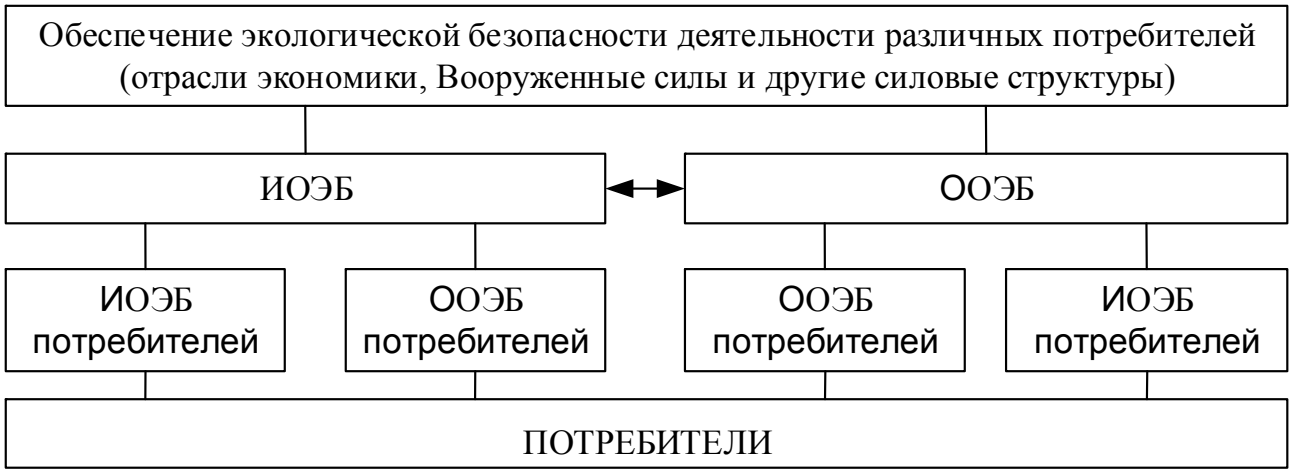


Рис.5. Взаимосвязь и совокупность ИОЭБ и ООЭБ различных потребителей

Заключение. Предложенный в настоящей работе методический подход к проблеме обеспечения экологической безопасности деятельности силовых структур и отраслей экономики России на базе понятий информационного и операционного обеспечения, по мнению авторов, позволит существенно повысить качество этого вида обеспечения, за счет оперативного внедрения в практику методов и средств модифицирования геофизических процессов и явлений и, в первую очередь, облаков и туманов.

СПИСОК ЛИТЕРАТУРЫ

1. Доронин, А.П. Состояние и перспективы работ в области модифицирования геофизических процессов и явлений в США / А.П. Доронин, Н.Г. Козлов, А.В. Костромитинов, В.В. Удриш // Сборник материалов XXIII Всероссийской межвузовской научно-технической конференции 16-18 мая 2011 года. Ч. II. – Казань, 2011. – С. 164-165.
2. Колосков Б.П., Корнеев В.П., Щукин Г.Г. Методы и средства модификации облаков, осадков и туманов. – СПб.: РГГМУ, 2012. – 343 с.

УДК 681

ЭКОЛОГИЧЕСКИЙ КОНТРОЛЬ И РАЗВИТИЕ МОДЕЛЕЙ ПОПУЛЯЦИОННОГО РОСТА

Павлова Светлана Михайловна
Смольный университет Российской академии образования
Россия, Санкт-Петербург, Полюстровский пр.59
emails: spavlova222@mail.ru

***Аннотация*:** В статье рассматривается экологический контроль который определяет особую актуальность обеспечения объективности и достоверности получаемой в процессе мониторинга информации. Ведь любое решение становится полезным и оптимальным, только когда оно основано на объективных и достоверных данных. Эта проблема понимается широким кругом ученых и практиков, связанных с философскими, математическими и информационными вопросами природоохранной и природопользовательской деятельности. Для более общих задач статистического мониторинга свойств сложного объекта, ориентированного на его специфику. При этом ЭС «АССИСТЕНТ» выступает в качестве базового модуля.

Ключевые слова: *экспертная система; информационно-измерительные системы; мониторинг; лингвистические шкалы; байесовские интеллектуальные измерения.*

ENVIRONMENTAL CONTROL AND DEVELOPMENT OF MODELS OF POPULATION GROWTH

Pavlova Svetlana Michailovna
Smolny university of the Russian Academy of Education
Russia, St. Petersburg, Polyustrovsky Ave 59,
emails: spavlova222@mail.ru

Abstract: The article presents tasks defines a special urgency to ensure the objectivity and reliability of the resulting data in the monitoring process. After all, any decision becomes a useful and optimal one only when it is based on some objective and reliable information. This problem refers to a wide range of scholars and practitioners associated with the philosophical, mathematical and informational issues on environmental and natural activities for more general problems of statistical monitoring of the properties of a complex object, based on its specific character In this case ES "ASSISTANT" acts as a basic module.

Keywords: *expert system, information and measuring systems, monitoring, linguistic scales, Bayesian linguistic measurements.*

Введение. Важность задачи мониторинга определяет особую актуальность обеспечения объективности и достоверности получаемой в процессе мониторинга информации. Ведь любое решение становится полезным и оптимальным, только когда оно основано на объективных и достоверных данных. Эта проблема понимается широким кругом ученых и практиков, связанных с философскими, математическими и информационными вопросами природоохранной и природопользовательской деятельности. Для более общих задач статистического мониторинга свойств сложного объекта, ориентированного на его специфику. При этом ЭС «АССИСТЕНТ» выступает в качестве базового модуля.

1.1.Теоретическое обоснование регуляризирующего байесовского подхода.

Одним из способов повышения степени устойчивости решений является ограничение пространства возможных решений путем формирования системы дополнительных ограничений, приводящих к созданию компактного пространства устойчивых решений [1,3].

Основная идея регуляризирующего байесовского подхода (БРП) состоит в привлечении измерительного подхода в процесс байесовского оценивания путем применения шкалирования, метризующего пространство байесовских решений. Получение результатов ИИ на компактах иерархических (согласно структурам ОИ и ВФ) метрических шкал, согласно теореме Тихонова [3], обеспечивает их устойчивость в пределах этих компактов. Таким образом, введение измерительной шкалы, обусловливая дополнительные ограничения на пространство возможных решений, оказывает регуляризирующие действия, что обосновывает название данной модификации байесовского подхода и позволяет ввести задачу ИИ на основе РБП в класс условно-корректных по Тихонову. Алгоритмы ИИ, реализующие такую идейную основу, будут обладать регуляризирующими свойствами при проведении измерений в сложных измерительных ситуациях при значительной априорной неопределенности информации об ОИ и ВФ. Интеллектуальные измерения, реализуемые на основе РБП, назовем байесовскими интеллектуальными измерениями (БИИ). Для построения алгоритмов БИИ необходимо определить их принципиальную основу, которая характеризуется уравнением измерений.

1.2. Концепция шкалы с динамическими ограничениями.

Понятие абстрактной измерительной шкалы дано в работах [3,4], которое определяет шкалу как совокупность правил, позволяющих выполнить гомоморфное преобразование Ψ для отображения реляционной системы объекта G в знаковую систему шкалы (в частности, в числовую),

представляющую собой реляционную систему G_S со свойствами $\left\{Q_{i_{G_S}}\right\}$ и отношениями $\left\{W_{j_{G_S}}\right\}$, $i_{G_S} = 1, I_{G_S}; j_{G_S} = 1, J_{G_S.}$ (1)

1.3. Основные свойства шкалы БИИ.

В измерительной практике используются разнообразные по измерительной мощности шкалы, теоретическому обоснованию и приложениям которых посвящены работы [3]. Наиболее полная их классификация приводится в литературе [3] по репрезентативной теории измерений, которая успешно развивается в настоящее время. В соответствии с нею все разнообразие шкал составляет несколько групп, к которым относятся шкалы наименований, порядка, интервалов, отношений, абсолютные, функциональные и др. В зависимости от их метрологических свойств они подразделяются на метрические и неметрические.

Метрические шкалы позволяют определять расстояние между соседними реперами носителя шкалы и организуются в метрическом пространстве результатов измерений — реперов шкалы. Неметрические шкалы [3] организуются на множестве элементов носителя шкалы, для которого понятие метрики (расстояния), как правило, не определено. К таким шкалам относятся шкалы наименований и порядка, для которых определены отношения эквивалентности (эквивалентности и порядка). Носители таких шкал могут быть представлены в виде лингвистических множеств. Эти шкалы используются в задачах классификации, распознавания, таксономии для принятия решений. Отсутствие метрических свойств в этих шкалах и целого ряда отношений, необходимых для реализации ШДО, не позволяет принять их в качестве основы для построения нового типа шкал БИИ.

1.4. Принципы синтеза шкал ШДО БИИ.

Построение любой измерительной шкалы начинается с формирования носителя шкалы, представляемого дискретным множеством результатов измерений $\{h_k\} \in H_K$, принятых в качестве представителя градаций $\{q_i^*\}$ измеряемого свойства q. Это позволяет рассматривать множество H_K как подмножество множества нешкалированных возможных результатов H. При соблюдении условий (1) множество H_K реперов шкалы неплотно покрывает множество H, а система носителя шкалы G_S является фрагментом или подсистемой системы, соответствующей множеству результатов H. Для реализации измерительной шкалы пространство ее носителя H_K должно быть метрическим, для которого определено понятие меры близости между отдельными элементами носителя шкалы. Тогда каждой паре h_i, h_j элементов носителя шкалы должно соответствовать вещественное число $p_i = p(h_i, h_j)$, удовлетворяющее аксиомам расстояния:

— неотрицательности:

$$p(h_i, h_j) = 0 \Leftrightarrow h_j = h_i; \quad (2)$$

— симметрии:

$$p(h_i, h_j) = p(h_j, h_i); \quad (3)$$

— треугольника:

$$p(h_i, h_z) \le p(h_i, h_j) + p(h_j, h_z). \quad (4)$$

1.5. Концепция и принципы построения сопряженной лингвистической шкалы БИИ

Не менее важную часть априорной информации, особенно в условиях измерительной ситуации БИИ, представляют собой сведения о лингвистической форме: естественно научные знания, наблюдения в форме описаний, аналоги из других предметных областей, лингвистические оценки экспертов, а также решения, выводы и рекомендации относительно ОИ, которые были получены ранее.

Для обработки и принятия решений на основе подобной информации развиты специальные теории: лингвистических переменных [3,4], теории возможностей, ситуационного управления и др. Основой формализации такой информации в данных теориях является аппарат теории нечетких множеств, позволяющий отображать имеющуюся информацию в виде специальных функций — функции принадлежности $\mu(\nu \mid x)$, которой придается следующий смысл:

$$\mu(\nu \mid x) \in M_{\text{Б}} \cdot (\nu \mid x) \in [0; 1], \quad (5)$$

где $\text{Б}^* = \{\langle M_{\text{Б}} \cdot (x) | x \rangle\}$ — нечеткое множество множества X, а X — базовое множество или базовая шкала значений контролируемого свойства ОИ. Носителем Б нечеткого множества Б^* на такой шкале являются те элементы X, для которых значения функции принадлежности отлично от нуля: (1)

$$\{MX(t_l)\}_k^n = \{MX(t_l)\}_k^n \mid \{MX(t_l)\}_k^{an} \mid \{MX(t_l)\}_x) * \{MX(t_l)\}_k^{an} * \{MX(t_l)\}_x \mid \text{У}_i^{\text{п}}(t_l). \quad (6)$$

2.Концептуальная основа параметрических байесовских интеллектуальных измерений.

Этап синтеза лингвистических параметрических шкал БИИ проводится в соответствии с методологией и по формулам (1,2) которые для лингвистического представления информации не имеют специфики в параметрических БИИ и поэтому не повторяются. Уравнение ПБИИ приведено далее в виде (3).

Если алгоритм ПБИИ состоит из нескольких этапов измерительных преобразований, то он реализуется в виде цепочки этапов ПБИИ.

Для статистик такими этапами алгоритма БИИ являются, как правило: этап их вычисления по эмпирическим данным по алгоритму $\varphi_{\text{ст}}$ и этап последующего шкалирования оценки статистики по алгоритму φ_s. Тогда ПБИИ принимает косвенных ПБИИ, для которых: (2)

— $\{h_k(x,t)|P_k(t)\} = \text{argmin}C_B\psi_h^{\text{п}}(x_i(t),t)|\psi_h^{\text{ап}}(A(t),t)|\text{У}_i^{\text{п}} =$
$\text{argmin}C_B\psi_s^{\text{п}}(\psi_{\text{ст}}^{\text{п}}(x_i(t),t),t)|\psi_h^{\text{ап}}(A(t),t)|x_i(t)|\text{У}_i^{\text{п}}(t);$ (7)

— КМХ результата (3):

$\{MX(x,t)\}_t = \{MX(t)\}_s^{\text{п}} * \{MX(t)\}_{\text{ст}}^{\text{п}} * \{MX(t)\}_x|h_k(x_i,t);$ (8)

— условная погрешность БИИ статистики: (3)

$f(\Delta h_k^{\text{п}}(t)|\ h_k^{\text{п}}) = f(\Delta h_{Sk}^{\text{п}}(t)) * f(\Delta h_{\text{стк}}^{\text{п}}(t)) * f(\Delta x_i(t))| * f(\Delta h_k^{\text{ап}}(t))|\text{У}_i^{\text{п}}(t).$ (9)

Алгоритм ПБИИ синтезируется вновь при меняющихся во времени условиях измерения и поступающей информации. При этом меняется и все множество алгоритмов ПБИИ $\Phi_j^{\text{п}}(t)$.

Возможна различная форма априорной параметрической неопределенности, соответствующая следующим ситуациям:

— какой-либо априорной информации о значениях или их диапазонах для параметра, а также априорного и точного выборочного распределения параметра нет;

— имеется информации о диапазоне изменения параметра, однако нет информации об априорном распределении значений параметра;

имеется информация, достаточная для определения области распределения параметра, его априорного распределения и точного выборочного распределения параметра.

Если вид точного выборочного распределения статистики неизвестен, то его определяют либо путем аналитических преобразований, либо путем имитационного моделирования, либо принимают равномерно распределенными выборочными значения статистики. Алгоритм определения выборочного распределения статистики входит как подэтап преобразования в алгоритм $\varphi_{\text{ст}}$(t). Очевидно, что с накоплением информации вид точного выборочного распределения может уточняться.

При первой ситуации на начальном этапе шкала строиться от оценки статистики $\widetilde{h_k}(t_1)$. Альтернативные решения располагаются справа и слева от нее на расстоянии $\rho(\varepsilon_{\text{доп}})$. В процессе измерений шкала развивается и достраивается, определяя истинный диапазон изменения параметра.

Для второй ситуации возможно построение универсальной параметрической шкалы БИИ, в которой элементы носителя шкалы выражены в относительных, приведенных к концу шкалы значениях.

Видно, что вид распределения вероятностей значений параметра может существенно повлиять на вид носителя шкалы БИИ. При неравновероятном априорном распределении параметра интервалы между соседними элементами носителя шкалы оказываются также неравномерными. Преимущества имеют элементы с меньшей априорной вероятностью.

Синтез алгоритмов ПБИИ статистик математического ожидания, дисперсии, коэффициентов асимметрии и эксцесса рассматривается в работах выше.

2.1. Алгоритмы БИИ статистик проверки статистических гипотез.

Можно показать, что задачи проверки статистических гипотез входя в класс задач измерительного контроля БИИ: (4)

$\{h_k|P_k\} = \psi^{\text{пр}}\left(\psi_j^{\text{о}}|x_i|\text{У}_i^o|\text{У}_i^{\text{пр}}\right);\ \psi_j^{\text{пр}} \in \psi_{\text{J}}^{\text{пр}};\ \psi_j^o \in \psi_{\text{J}}^{\text{о}},$ (10)

где $\psi^{\text{пр}}$, $\psi_{\text{J}}^{\text{о}}$ — алгоритмы БИИ принятия решений по критерию ω и оценивания соответственно.

Обобщенный алгоритм проверки статистических гипотез $\theta_i \in \theta_I$ по критерию $\omega(\theta_I, x)$ может быть представлен в виде:

$\theta = \theta_0 \leftrightarrow \hat{\theta} = \arg(P(\hat{\theta}(x)|\theta_0) = a_{\text{доп}}),$ (11)

где $P(\tilde{\theta}(x))$ — интегральный распределения статистики $\tilde{\theta}(x)$, $a_{\text{доп}}$ — уровень значимости критерия.

Можно переписать выражение для критерия в виде последовательности функциональных преобразований оценивания статистики $\varphi^{\text{ст}}$ и принятия решения по критерию φ^{ω}:

$\theta = \psi^{\omega}(\psi^{\text{ст}})(x|\theta_0, a_{\text{доп}}).$ (12)

2.2. Измерительные задачи мониторинга сложных технических и природных объектов

К одним из самых наукоемких и технически сложных задач относятся задачи мониторинга сложных объектов. Понятие сложного объекта как объекта, полностью определяемого своими свойствами и отношениями между ними и другими объектами, составляющими среду функционирования приведены в [3]. К числу сложных объектов относятся объекты, активно взаимодействующие со средой, свойства и отношения между которыми неизвестны точно. Основными свойствами сложных объектов мониторинга являются [3]:

– естественная иерархичность структуры объекта, подтверждаемая созданными человечеством классификационными системами (например, для природных объектов классификации видов живых организмов — система Менделеева, иерархия слоев околоземного пространства, планетарная структура Солнечной и других космических систем и др.);

– существование реальных признаков, определяющих принадлежность характеристик объекта к тому или иному уровню иерархии структуры объекта;

– взаимосвязанность иерархических уровней, составляющих объект как единое целое, отражающая взаимосвязь характеристик объекта;

– невозможность точного формализованного описания объекта;

– уникальность объекта, обусловливающая трудности представления типового образа объекта;

– невозможность или нежелательность по каким-либо причинам экспериментов над ним как над источником информации при изучении или моделировании его свойств;

– значительная часть информации о таком объекте обычно содержится в форме сведений, наблюдений, рекомендаций, описания ситуаций и фактов из опыта общения с ним человека, представленных в семантической форме;

– распределенность объекта во времени и географическом пространстве;

– устойчивость, саморегуляция и самоорганизуемость при меняющихся условиях функционирования.

Примерами таких объектов могут быть технические системы, состоящие из ряда подсистем, характер взаимодействия которых не может быть определен точно доступными средствами, искусственные объекты, активно взаимодействующие со средой их функционирования, а также все природные объекты.

Понятие мониторинга для сложных объектов искусственного происхождения дано в [5]. Оно определяет мониторинг как процесс слежения за состоянием объекта и сопоставления его текущего состояния с контрольными образцами (уровнями или точками).

Термин «мониторинг» как понятие для природного объекта был впервые введен в использование на Стокгольмской конференции в 1972 году. После этого начали активно развиваться два направления мониторинга природных объектов, которые принципиально отличались друг от друга принятием и отрицанием функции регулирования (управления) природным объектом.

Так, в первой концепции мониторинг природного объекта понимается как процесс сбора, хранения, преобразования экспериментальной информации об объекте мониторинга и выработке регулирующего воздействия, направляемого на объект по линиям обратной связи. В определение понятия мониторинга во втором направлении включаются все перечисленные подзадачи первого направления, кроме последней. Конечной целью мониторинга при этом считается выработка рекомендаций в поддержку тех или иных решений, оптимальных с точки зрения принятых критериев.

При втором главной целью мониторинга считается контроль состояния объекта при всемерном и всестороннем его познании и управлении процессом этого познания, а также выработке рекомендаций по регулированию антропогенного влияния, что обеспечивает, в конечном итоге, устойчивое развитие объекта.

Важность задачи мониторинга определяет особую актуальность обеспечения объективности и достоверности получаемой в процессе мониторинга информации. Ведь любое решение становится полезным и оптимальным, только когда оно основано на объективных и достоверных данных. Эта проблема понимается широким кругом ученых и практиков, связанных с философскими, математическими и информационными вопросами природоохранной и природопользовательской деятельности. Как отмечается в работе Н. Н. Моисеева [2,5], «Объективность получаемых знаний — важнейший вопрос планетарной экологии». В работе отмечается важность задачи мониторинга и получения достоверной информации для обеспечения устойчивого развития экосистем, в том числе и в России. Реализация принципов и стратегических требований всемирных форумов в 1992 году в Рио-де-Жанейро и в 1994 году в Манчестере, сформулированных в «Декларации» и «Повестке дня XXI века», а также в обращениях и докладах их участников, возможна только на основе формирования современной информационной цивилизации, базирующейся на новых методах и средствах получения точных и достоверных знаний об окружающей природной среде.

Таким образом, эффективно решить задачи мониторинга сложных объектов в сложных измерительных ситуациях и использовать результаты мониторинга для обеспечения устойчивого функционирования сложных природных или технических систем можно только с позиций измерительного подхода на принципах единства измерений и при постоянном метрологическом обосновании получаемых результатов.

Процесс реализации информационно-измерительных систем мониторинга предполагает выбор методической, информационной и технической баз ИИС. Специфика задач мониторинга сложных объектов предъявляет такого рода ИИС определенные требования, которые на основании приведенных выше рассуждений можно выразить следующим образом:

– в процессе мониторинга должно обеспечиваться познание объекта мониторинга (ОМ);

– решение задачи мониторинга должно производиться на основе всей доступной априорной информации об объекте мониторинга и среде его функционирования и информации, получаемой в процессе измерительного эксперимента;

– все получаемые промежуточные и окончательные результаты мониторинга должны иметь метрологическое обоснование в виде показателей их качества;

– для эффективного решения задач мониторинга модели объектов и СФ, а также методы, алгоритмы и средства мониторинга должны отражать основные свойства сложных объектов (в частности, свойства устойчивости, саморазвития и самоорганизации);

– результаты мониторинга должны быть представлены в формах значений параметров, аналитических выражений, выводов и решений, представленные в лингвистической форме.

Для более общих задач статистического мониторинга свойств сложного объекта, ориентированного на его специфику. При этом ЭС «АССИСТЕНТ» выступает в качестве базового модуля.

2.3. Экспертная система «АССИСТЕНТ» для статистического мониторинга сложных объектов

ЭС «АССИСТЕНТ» в настоящее время является основой нескольких ЭС для статистического мониторинга технических, искусственных и природных объектов, среди которых ЭС «АССИСТЕНТ-КЛАСС» для классификации технических и природных объектов по изображению, «АССИСТЕНТ-МЕТРОЛОГ» для метрологической исследовательской аттестации средств измерений, «АССИСТЕНТ-ГИДРОЛОГ» для мониторинга акваторий, «АССИСТЕНТ-ИХТИОЛОГ» для оценки состояния и характеристик рыбных ресурсов, «АССИСТЕНТ-БИОЛОГ» для биосферного мониторинга экосистемы и др. Кроме того, ЭС «АССИСТЕНТ» применялась в задачах статистической обработки и мониторинга технологических производственных процессов, сложных перерабатывающих комплексов и стала интеллектуальной средой в виде ЭС «АССИСТЕНТ-ЭКОЛОГ» [3,4] в ИНИИС для оценки состояния атмосферы.

Заключение. Однако, хотя к решению задач мониторинга в настоящее время привлечены усилия многих ученых и организаций, многочисленные методические и технические средства, получение объективной информации, достаточной для познания закономерностей развития природной среды и функционирования сложных объектов, а также для принятия оптимальных решений экологического управления, остаются недоступными и по сей день. Основными причинами этого являются сложность самих объектов мониторинга, отсутствие эффективных методов и средств получения информации, ориентированных на специфику сложных объектов и метрологического обеспечения результатов мониторинга, субъективность окончательных решений о состоянии объекта, что при несомненной целесообразности использования опыта специалистов не позволяет обобщить весь объем полученной информации и вносит ошибки в результаты мониторинга.

СПИСОК ЛИТЕРАТУРЫ

1. .Мэгарран Э. Экологическое разнообразие и его измерение. – М.: Мир, 1992.- 368 с.
2. .Лебедев А.Н. Модели сложных объектов. – Пенза: ППИ, 1977. – 71 с.
3. Д.Д. Недосекин, Е.А. Чернявский и др. Информационные технологии интеллектуализации измерительных процессов.- СПб.; Энергоатомиздат. Санкт- Петербургское отделение, 1995.- 178 с .: ил. ISBN 5-283-04706-76
4. Павлова С.М. Становление и развитие моделей популяционного роста/ С.-Петербург.электротех.ун-т.- СПб.,1996.- Деп. В ВИНИТИ 28.05.96, №1721-В96.
5. В.Е. Болтнев Экология.- Издательство : ТНТ 2012.- 352. – ISBN9785941782581

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

УДК 004.77

ПРОЕКТИРОВАНИЕ АППАРАТНО-ПРОГРАММНОГО КОМПЛЕКСА ИДЕНТИФИКАЦИИ СОСТОЯНИЯ ОБЪЕКТОВ И СУБЪЕКТОВ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ ИНТЕРНЕТ ВЕЩЕЙ

Дикий Дмитрий Игоревич[1], Артемьева Виктория Денисовна[2]
[1] Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский пр., д. 49,
[2] Балтийский федеральный университет им. И. Канта,
Россия, Калининград, ул. А. Невского, д. 14а,
emails: dimandikiy@mail.ru, vika_med2019@mail.ru

***Аннотация*:** В статье рассмотрен подход к проектированию аппаратно-программного комплекса, главной задачей которого является идентификация движимых и недвижимых объектов с применением технологий Интернет вещей. Данный подход планируется использовать при создании автоматизированной системы в рамках образовательного учреждения высшего образования. Это накладывает особые требования к разрабатываемому комплексу. Например, он должен работать как на идентификацию передвижения людей (людских потоков), так и материальных ценностей. Основа подхода заключается в использовании радиочастотных пассивных меток (RFID), с помощью которых можно помечать объекты и регистрировать их местоположение в реальном времени.

***Ключевые слова**: проектирование; RFID; аппаратно-программный комплекс; идентификация; локация*

DESIGN OF HARDWARE AND SOFTWARE IDENTIFY THE STATE OF OBJECTS AND SUBJECTS WITH APPLICATION OF TECHNOLOGIES OF INTERNET OF THINGS

Dikii Dmitrii[1], Artemeva Viktoriia[2]
[1] Saint Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronverksky Ave 49,
[2] Immanuel Kant Baltic Federal University,
Russia, Kaliningrad, A. Nevsky Street 14a,
emails: dimandikiy@mail.ru,vika_med2019@mail.ru

Abstract: The article describes the approach to designing hardware-software complex, whose main task is to identify movable and immovable objects with the use of technologies the Internet of things. This approach will be used for creation of automated system in educational institutions of higher education. This imposes special requirements to develop the complex. For example, it needs to work on the identification of the movement of persons (flows of people: students, teachers) and material assets (computers, expensive equipment). The approach is to use passive radio frequency tags (RFID), with which you can mark the objects and record their location in real time.

***Keywords**: design; RFID; the hardware-software complex; identification; location*

Введение. Системы мониторинга положения объектов с начала 2000х находят свое применение во многих сферах жизни человека. Одним из ярких примеров, является использование компанией Amazon системы определения положения объектов в складских помещениях и магазинах [1]. Однако данные технологии могли бы быть хорошо применимы в образовательных организациях, например, для мониторинга посещения студентами лекций и семинаров и т.д.

Описание подхода. Аппаратно-программный комплекс (АПК) предназначен для решения задач идентификации и определения места положения помеченных субъектов, документов и объектов материальных ценностей на заданных территориях. Объекты и субъекты накладываются одним или несколькими видами меток: графические (штрих коды, QR-коды), RFID-метки — пассивные метки; средства для идентификации в режиме реального времени (WiFi/GPS/GPRS-трекеры). Определение их позиции (наличия) осуществляется с помощью стационарных и портативных сканеров графических и RFID-меток [2], а также использования WiFi роутеров, мобильных и стационарных средств сотовой связи. Идентификация субъектов и объектов определяется с помощью распознавания сигнатур всех типов меток, а также средств идентификации в режиме реального времени. АПК применяется для

выполнения проверочных, инвентаризационных и исследовательских мероприятий, определяющих выполнение заданных требований по наличию и месту расположения субъектов и объектов, например, проверка комплектности документов, посещаемость зон мероприятий (в частности, студентов и преподавателей в аудиториях, участников конференции). АПК и отдельные компоненты будут эксплуатироваться в крытых помещениях или в уличных условиях при диапазоне рабочих температур от 0 до 50°С. Централизованный сбор идентификационной информации позволит реализовывать мониторинг в режиме реального времени положения и некоторых признаков состояния идентифицируемых объектов и субъектов.

Примеры процессов, в которых может применяться АПК: мониторинг потоков критических документов в кампусе учреждения высшего образования; отслеживание положения различных материальных ценностей; определение наличия документов, участников конференций и других.

Основное назначение аналогичных систем состоит в контроле человеческих потоков в учебных заведениях (в частности «Система контроля и управления доступом на основе систем SALTO XS4 RFID» [3], «RFID портал» рабочая частота UHF 860-960 МГц), либо в управлении складами или архивами (в частности, ТЭНДО: RFID-архив [4], «Система защиты бумажных носителей информации» рабочая частота UHF 860-960 МГц). Сведения об идентификации комплексных процессов с участием персон, материальных ценностей и документов в учебном заведении (в частности, для определения события выноса конкретного устройства или документа конкретной персоной из конкретного помещения) найти не удалось. Все выше перечисленные свойства систем позиционирования в реальном времени позволяют снизить затраты на расследование инцидентов информационной безопасности. Так можно своевременно зафиксировать факт кражи критически важных материальных объектов, в том числе документов, содержащих конфиденциальную информацию [5].

Предлагаемый аппаратно-программный комплекс. Для реализации аппаратно-программного комплекса предполагается использовать модульную систему. Это позволит использовать данную разработку в независимости от масштабов организации, использовать различные интерфейсы и разное количество оконечного оборудования. Основными элементами аппаратно-программного комплекса являются:

– Координирующая компьютерная система (ККС), которая осуществляет управление и координацию исполнительных устройств. Также в функции ККС входит отображение информации из баз данных.

– Сканирующие системы как проводные (СПС), так беспроводные (СБПС) в основные функции которых входит считывание идентификаторов с RFID меток, информации с оптических кодирующих элементов, таких как QR-коды и штрих-коды.

– Система идентификации субъектов и объектов в режиме реального времени (СИОС РВ). В задачи этого модуля входит локализация объектов, находящихся в зоне действия считывающих устройств.

– Сервер ККС – элемент ККС, который отвечает за вычислительную мощность аппаратно-программного комплекса, также осуществляет коммутацию всех элементов телекоммуникационных сетей.

– Специализированное программное обеспечение. Данное программное обеспечение разрабатывается под конкретные задачи аппаратно-программного комплекса. Его задачами является синхронизация всех модулей комплекса на программном уровне, обеспечение целостности, доступности и конфиденциальности информации.

– Источник бесперебойного питания (ИБП) для сервера ККС. Как следует из названия, этот элемент обеспечивает бесперебойную работу комплекса на время, необходимое для безопасного завершения работы, во избежание появления коллизий.

– Подсистема разветвления проводных каналов связи отвечает за проводное соединение всех элементов комплекса, включает в себя коммуникационное оборудование.

– Портативное рабочее место оператора. Как правило это стационарный персональный компьютер, который имеет соответствующие устройства ввода и вывода. Данный элемент должен обладать минимальными необходимыми вычислительными мощностями для выполнения возложенных задач.

– Подсистема вывода графической информации и ввода информации. Этот элемент, как подпункт портативного рабочего места оператора, должно обеспечивать регистрацию новых объектов, удаление и изменение информации об объектах. Этот модуль также предусматривает настройку RFID меток, штрих-кодов и QR-кодов.

Минимальный состав аппаратно-программного комплекса представлен в виде схемы деления на рисунке 1.

Предложенная схема аппаратно-программного комплекса удовлетворяет всем требованиям, которые необходимо соблюдать при работе в учреждении высшего учебного образования [6]. Одновременная поддержка разнообразного вида считывателей позволяет использовать данный проект при ограниченных условиях, в том числе за пределами зданий.

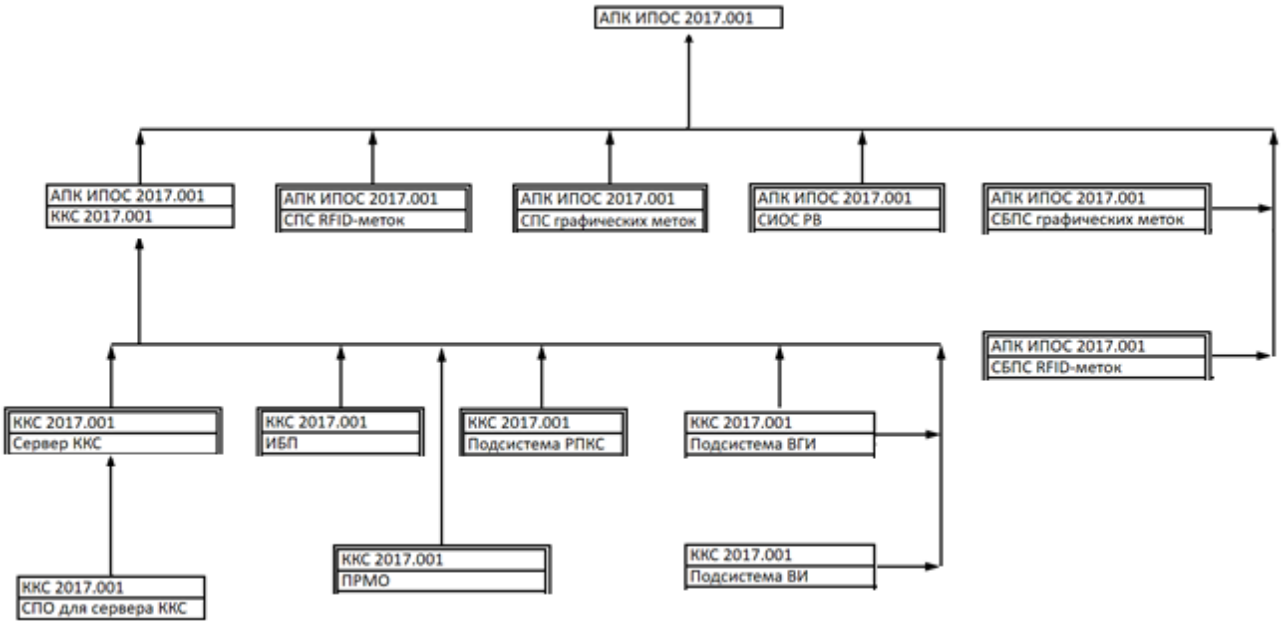


Рис. 1. Блок-схема деления аппаратно-программного комплекса

Заключение. Таким образом, в целях обеспечения своевременного и успешного расследования инцидентов информационной безопасности в том числе внутри образовательных учреждений имеет смысл создать автоматизированную систему мониторинга перемещения движимых и недвижимых объектов. Она должна содержать в себе компоненты, позволяющие адаптировать ее под нужды различных организаций. На данный момент разработаны все необходимые технологии и протоколы для выполнения этой задачи. В работе представлена общая схема и состав аппаратно-программного комплекса. Ввиду того, что затраты на переносные метки и считывали не являются периодическими, то развертывание такой системы является экономически выгодным.

СПИСОК ЛИТЕРАТУРЫ

1. How ‘Amazon Go’ works: The technology behind the online retailer’s groundbreaking new grocery store // [Электронный ресурс] URL: https://www.geekwire.com/2016/amazon-go-works-technology-behind-online-retailers-groundbreaking-new-grocery-store/ (дата обращения: 21.09.2017).
2. Brennan D, Kolaja J Real Time Location System using Passive UHF RFID // 15th International Carpathian Control Conference (ICCC). 2014. С. 58-62.
3. Концепция построения СКУД (системы контроля и управления доступом) учреждения системы здравоохранения на основе систем SALTO. // [Электронный ресурс] SaltoSystems URL: http://saltosystems.ru/application/helthcare.php (дата обращения: 21.09.2017).
4. Комплексная автоматизация бизнес процессов // [Электронный ресурс] URL: http://www.tendo.ru/ (дата обращения: 21.09.2017).
5. Указ Президента РФ от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциального характера".
6. Szymczyk T., Montusiewicz J., Gutek D. Navigation in large-format buildings based on RFID sensors and QR and AR markers // Advances in science and technology-research journal. 2016. С. 263-273.

УДК 004.056

МЕТОД РАЗРАБОТКИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ РЕГИОНАЛЬНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Козин Иван Сергеевич
«Информационные телекоммуникационные технологии»,
Россия, Санкт-Петербург, ул. Кантемировская, д.8,
emails: van@trioptimum.com

Аннотация: В статье представлен метод разработки защищённой автоматизированной системы управления информационной безопасностью региональной информационной системы. Представленный метод включает проведение комплексных мероприятий, направленных на обеспечение защищённой разработки программного обеспечения, в т.ч. формирование перспективных требований безопасности, проектирование безопасной архитектуры, оценку рисков, анализ исходного кода, проведение тестирования на проникновение. Результатом реализации метода является создание перспективной защищённой системы управления информационной безопасностью территориально распределённой информационной системы. Система управления может быть использована в сетях передачи данных различного масштаба и назначения.

Ключевые слова: *безопасная разработка; анализ поведения; оценка рисков; уязвимость; тестирование на проникновение.*

METHOD OF DEVELOPMENT OF SECURITY INFORMATION AND EVENT MANAGEMENT COMPUTER-AIDED SYSTEM OF REGIONAL INFORMATION SYSTEM

Kozin Ivan
«Inteltech» PSC,
Russia, St.-Petersburg, Kantemirovskaya str. 8,
van@trioptimum.com

Abstract: The paper presents a method of development the security information and event management computer-aided system of regional information system. The method claimed includes complex actions for protecting software development, including the forming of perspective security requirements, secured architecture design, risk management, static method, penetration testing. The result of the method claimed is development of a perspective protected security information and event management system of a territorially distributed information system. The developed management system can be used in different scale and purpose networks.

Keywords*: security development; behavior analytics; risk management; vulnerability; penetration testing.*

Введение. Неблагоприятная геополитическая обстановка и активизация действий террористов обуславливают актуальность проблем обеспечения безопасности, одним из важнейших аспектов которой является информационная безопасность. Информационная безопасность играет ключевую роль в обеспечении жизненно важных интересов Российской Федерации и ее регионов [1].

Постоянно возрастающая скорость развития информационных технологий способствует непрерывному расширению спектра угроз безопасности информации, обрабатываемой в региональных информационных системах. Решение задачи обеспечения информационной безопасности региональных информационных систем возможно на основе внедрения персептивных телекоммуникационных технологий. В этой связи актуальной является разработка защищённой автоматизированной системы управления информационной безопасностью региональной информационной системы (АСУ ИБ РИС).

В настоящей статье предлагается метод разработки АСУ ИБ РИС, учитывающий положения современных государственных стандартов по разработке защищённого программного обеспечения и анализу уязвимостей, перспективные международные научно-технические подходы к разработке, а также основные требования к архитектуре информационной системы регионального масштаба.

В основе предлагаемого метода лежит жизненный цикл безопасной разработки (ЖЦБР) – подход к предоставлению гарантий безопасности разрабатываемого программного обеспечения, дополняющий этапы процесса разработки программного обеспечения подходами к обеспечению безопасности информации. Основные принципы ЖЦБР были разработаны компанией Microsoft[5] и частично положены в основу Российского государственного стандарта[6] по разработке защищённого программного обеспечения, требования которого вступили в силу в июне 2017 года.

Предлагаемый в настоящей статье подход к реализации ЖЦБР, включает следующие основные фазы разработки АСУ ИБ РИС: формирование требований, проектирование архитектуры, разработка, тестирование.

Формирование требований. На сегодняшний день одной из основных функций, реализованных в системах управления информационной безопасностью, является автоматическое выявление фактов несанкционированного доступа. При этом мониторинг санкционированных, но аномальных действий, практически не проводится. Примером аномального действия является резкая активизация действий пользователя по отношению к конкретным информационным ресурсам (пользователь начинает открывать все возможные доступные ему документы) и сервисам (администратор домена начинает активно скачивать данные пользователей с удалённых рабочих станций). Выявление подобных аномалий может свидетельствовать о компрометации учётной записи.

Нами предлагается пример подхода к разработке АСУ ИБ РИС, направленной на решение следующих задач обеспечения информационной безопасности:

— обеспечение традиционных функций защиты информации от несанкционированного доступа (доверенная загрузка, идентификация и аутентификация, антивирусная защита и т.п.) с централизованным управлением;

- мониторинг поведения санкционированных пользователей и процессов;
- анализ поведения санкционированных пользователей и процессов, выявление аномалий;
- автоматизированная оценка рисков;

[5] URL: https://msdn.microsoft.com/ru-ru/cc448177
[6] ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования.

– автоматическое оперативное воздействие на безопасность информационной системы (в т.ч. блокировка скомпрометированных рабочих мест и сегментов сети передачи данных).

Проектирование. Известна близкая по составу функциональных возможностей система управления защитой информации в территориально распределённой прикладной системе управления [2], обеспечивающая оперативную адаптацию параметров механизмов защиты транспортной среды и каналов связи к выявленным угрозам или штатным изменениям в структуре системы в целом. Также известны система, обеспечивающая создание защищенной транспортной среды и каналов связи для локальных и территориально распределённых информационных систем [3], и система, анализирующая трафик сети на предмет аномальной активности [4]. Однако указанные технические решения не учитывают информацию о нетипичных санкционированных действиях пользователей и процессов, и не обеспечивают оперативное целенаправленное воздействие на безопасность защищаемой информационной системы в целом.

АСУ ИБ РИС условно можно подразделить на четыре сегмента: комплекс средств защиты информации конечной точки (КСЗИ-КТ), обеспечивающий защиту рабочего места пользователя; центр управления информационной безопасностью объектовой сети (ЦУБ-О), обеспечивающий безопасность объектовой сети; центр управления информационной безопасностью узла доступа (ЦУБ-У), обеспечивающий безопасность информации группы объектовых сетей; главный центр управления информационной безопасностью (ЦУБ-Г), обеспечивающий безопасность информационной системы в целом. Архитектура предлагаемой АСУ ИБ РИС представлена на рисунке 2.

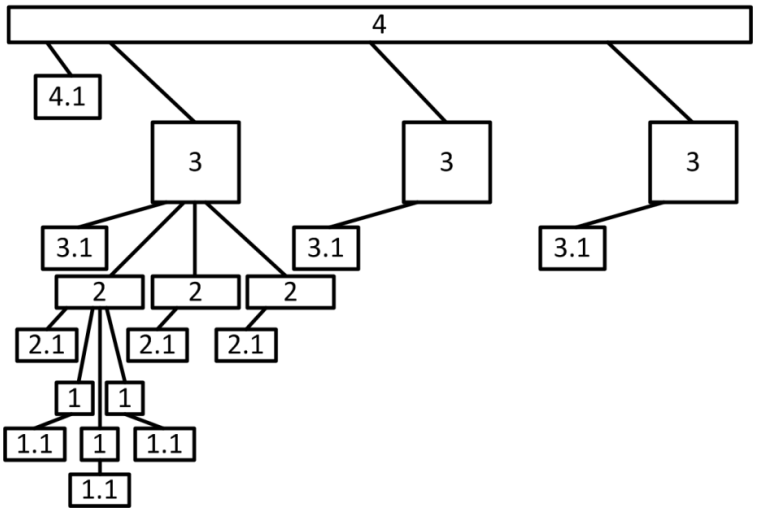


Рис. Архитектура АСУ ИБ РИС
1 – конечная точка (рабочее место пользователя); 1.1 – комплекс средств защиты информации конечной точки; 2 – объектовая сеть; 2.1 – центр управления информационной безопасностью объектовой сети; 3 – узел доступа; 3.1 – центр управления информационной безопасностью узла доступа; 4 – транспортная сеть; 4.1 – главный центр управления информационной безопасностью.

Оценка рисков при моделировании угроз безопасности информации, в общем случае, сводится к определению отношения потенциальных последствий (величины ущерба) от реализации угрозы к вероятности реализации угрозы.

При определении величины потенциального ущерба от реализации угрозы безопасности АСУ ИБ РИС необходимо учитывать состав деструктивных воздействий, к которым может привести реализация угроз, и их влияние на отдельные характеристики безопасности объектов защиты – конфиденциальность, целостность и доступность. Для определения опасности угрозы в качестве исходных данных необходимо обладать сведениями о составе потенциальных угроз. При подготовке перечня потенциальных угроз могут использоваться методические документы[7], подготовленные ФСБ России, а также методические документы[8] и банк[9] угроз безопасности информации ФСТЭК России. В состав объектов защиты должны быть включены как информационные ресурсы, так и технические средства, обеспечивающие обработку информационных ресурсов.

Общий порядок определения опасности угрозы включает в себя следующие этапы:

1. определение состава деструктивных воздействий потенциальных угроз;

[7] ФСБ России. 1) Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. 2008; 2) Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных. 2008.

[8] ФСТЭК России. 1) Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. 2008; 2) Методика определения актуальных угроз безопасности персональным данным. 2008.

[9] URL: http://www.bdu.fstec.ru

2. определение степени важности объекта защиты;
3. определение опасности нарушения конфиденциальности, целостности и доступности;
4. определение опасности осуществления конкретных деструктивных воздействий;
5. определение уровня потенциального ущерба от реализации угрозы;
6. определение опасности угрозы.

Подобный подход ранее предлагался при моделировании угроз безопасности критически важных автоматизированных систем [5] и критически важной информации [6].

При определении состава деструктивных воздействий потенциальной угрозы предполагается, что реализация любой угрозы приводит к осуществлению определённых деструктивных воздействий. Для каждой потенциальной угрозы необходимо подготовить список деструктивных воздействий, к которым может привести её реализация. В состав основных деструктивных воздействий, способных повлиять на безопасность объектов защиты, входят: хищение, ознакомление, копирование, модификация или удаление (уничтожение), блокирование.

Градация важности объекта защиты выражена четырьмя степенями: самая высокая – первая, самая низкая – четвёртая. Для оценки степени важности объекта защиты необходимо рассмотреть каждый объект защиты с позиции необходимости обеспечения состояний конфиденциальности, целостности и доступности. Таким образом, каждому объекту защиты соответствуют три характеристики важности.

Каждое *d*-ое деструктивное воздействие на *o*-ый объект описывается в виде тройки коэффициентов $K_{do\alpha}$, $K_{do\beta}$, $K_{do\gamma}$, где α, β, γ – индексы, отражающие составляющие опасности, связанные с нарушениями конфиденциальности, целостности и доступности. Значения коэффициентов деструктивных воздействий зависят от важности объектов, на которые направлены деструктивные воздействия. Коэффициенты деструктивных воздействий выражают опасность нарушения конкретных характеристик безопасности.

В качестве математического аппарата для присвоения числовых значений применялась теория нечётких множеств. Основной трудностью, мешающей применению теории нечётких множеств при решении практических задач является то, что функция принадлежности должна быть задана вне самой теории и, следовательно, её адекватность не может быть проверена непосредственно средствами теории. В каждом известном методе построения функции принадлежности формулируются свои требования и обоснования к выбору именно такого построения [7].

При построении характеристических функций принадлежности множествам опасности использовался прямой метод экспертных оценок, в рамках которого предполагалось следующее: x – значение опасности нарушения характеристики безопасности объекта защиты; U – множество значений опасности нарушения характеристики безопасности объекта защиты, $U = \{x, x \in R: 0 \le x \le 3\}$; A – множество значений высокой опасности нарушения характеристики безопасности объекта защиты; B – множество значений средней опасности нарушения характеристики безопасности объекта защиты; C – множество значений низкой опасности нарушения характеристики безопасности объекта защиты; D – множество значений безопасности (нулевой опасности) объекта защиты; μA(x) – характеристическая функция принадлежности множеству опасности A, μA(x) = [1;0]; μB(x) – характеристическая функция принадлежности множеству опасности B, μB(x) = [1;0]; μC(x) – характеристическая функция принадлежности множеству опасности C, μC(x) = [1;0]; μD(x) – характеристическая функция принадлежности множеству опасности D, μD(x) = [1;0].

Характеристические функции принадлежности множествам опасности выражают примерные значения опасности нарушения характеристики безопасности, обусловленной степенью важности объекта защиты. При определении примерных значений предполагалось: чем выше значение x, тем выше значение опасности; недопустимо делать вывод о 100%-ой принадлежности характеристической функции определённому множеству (нечёткие множества значений опасности должны быть субнормальными – ни одна характеристическая функция принадлежности не должна принимать значение, равное единице); для однозначного определения значений коэффициентов деструктивных воздействий все характеристические функции принадлежности должны иметь один максимум – быть унимодальными. Несущие множества опасности можно записать следующим образом:

$$A = 0.2/0 + 0.4/1 + 0.7/2 + 0.9/3$$
$$B = 0.4/0 + 0.7/1 + 0.7/3 + 0.9/2$$
$$C = 0.4/3 + 0.7/0 + 0.7/2 + 0.9/1$$
$$D = 0.2/3 + 0.4/2 + 0.7/1 + 0.9/0$$

где запись вида 0.2/0 выражает не деление на ноль, а значение функции принадлежности (в данном примере 0.2) при значении опасности, равном нолю. Общая форма записи нечётких подмножеств будет иметь следующий вид:

$$A = \sum_{x=0}^{3} \mu_A(x)/x = \sum_{x=0}^{0} 0.2/x + \sum_{x=1}^{1} 0.4/x + \sum_{x=2}^{2} 0.7/x + \sum_{x=3}^{3} 0.9/x$$

$$B = \sum_{x=0}^{3} \mu_B(x)/x = \sum_{x=0}^{0} 0.4/x + \sum_{x=1}^{1} 0.7/x + \sum_{x=2}^{2} 0.9/x + \sum_{x=3}^{3} 0.7/x$$
$$C = \sum_{x=0}^{3} \mu_C(x)/x = \sum_{x=0}^{0} 0.7/x + \sum_{x=1}^{1} 0.9/x + \sum_{x=2}^{2} 0.7/x + \sum_{x=3}^{3} 0.4/x \quad ((1)$$
$$D = \sum_{x=0}^{3} \mu_D(x)/x = \sum_{x=0}^{0} 0.9/x + \sum_{x=1}^{1} 0.7/x + \sum_{x=2}^{2} 0.4/x + \sum_{x=3}^{3} 0.2/x$$

$$\sum_{x=0}^{3} \mu_A(x)/x$$

где запись вида не предполагает сумму, но предполагает объединение по всем элементам конечного несущего множества значений x.

Для уточнения примерных числовых значений функций принадлежности множествам опасности были сделаны следующие допущения: на конфиденциальность не могут повлиять блокирование, модификация и удаление (уничтожение) объекта защиты; на целостность не могут повлиять ознакомление, копирование или блокирование объекта защиты; на доступность не могут повлиять ознакомление или копирование объекта защиты; опасность нарушения конфиденциальности в случае хищения или копирования объекта защиты выше опасности нарушения конфиденциальности в случае ознакомления; опасность нарушения целостности в случае модификации и удаления (уничтожения) объекта защиты выше опасности нарушения целостности в случае хищения объекта защиты; опасность нарушения доступности в случае модификации и удаления (уничтожения) объекта защиты выше опасности нарушения доступности в случае хищения или блокирования объекта защиты.

При уточнении значений функций принадлежности множествам опасности был осуществлён сдвиг по оси x на -0.1 (для Kdoα в случае ознакомления, для Kdoβ в случае хищения и для Kdoγ в случае хищения и блокирования). Общая опасность d-го деструктивного воздействия выражена коэффициентом Kdo. Коэффициент общего деструктивного воздействия Kdo в соответствии с формулой, предложенной органом государственной власти, уполномоченным по вопросам технической защиты информации, определяется следующим соотношением:

$$K_{do} = \theta_{d\alpha} K_{do\alpha} + \theta_{d\beta} K_{do\beta} + \theta_{d\gamma} K_{do\gamma}$$

где θdα, θdβ, θdγ – функции, значения которых равны единице, если в результате реализации d-го деструктивного воздействия нарушается конфиденциальность, целостность или доступность объекта соответственно; $K_{do\alpha}$, $K_{do\beta}$, $K_{do\gamma}$ – коэффициенты деструктивного воздействия по отношению к конкретным характеристикам безопасности.

Ущерб от реализации угрозы *t* по отношению к объекту *o* выражен коэффициентом ущерба D_{to}, определяемым совокупной коэффициентов K_{do} деструктивных воздействий (d_1, d_2, d_3, d_4, d_5), к которым может привести реализация угрозы. Значение коэффициента ущерба D_{to} от реализации угрозы определяется следующим соотношением (в соответствии с формулой, предложенной органом государственной власти, уполномоченным по вопросам технической защиты информации):

$$D_{to} = K_{d_1 o} + K_{d_2 o} + K_{d_3 o} + K_{d_4 o} + K_{d_5 o}$$

Опасность угрозы *t* выражается отношением ущерба D_{to}, к которому может привести её реализация, к приемлемому ущербу D_a и определяется следующим соотношением:

$$K_{to} = \frac{D_{to}}{D_a}$$

Уровень приемлемого ущерба является уникальным для каждого отдельного объекта защиты, задаётся экспертным путём и не может принимать значение, равное нулю. В случае, когда ущерб от реализации деструктивного воздействия Dto превышает допустимый ущерб Da, он принимает значение равное Da. Вербальная интерпретация опасности угрозы будет принимать следующие значения: «низкая» опасность для интервала [0.00;0.30]; «средняя» опасность для интервала [0.31;0.64]; «высокая» опасность для интервала [0.65;1.00]

Вероятность реализации угрозы характеризует динамику возникновения и реализации угрозы. Для каждой угрозы необходимо иметь свою модель расчета вероятности реализации. В рамках предлагаемого подхода предполагается следующее допущение: вероятность реализации угрозы в условиях отсутствия мер защиты приравнивается к единице, если данная угроза имеет место, и к нулю, если угроза отсутствует.

Разработка. Выявление и анализ уязвимостей программного обеспечения в настоящее время является одной из самых сложных проблем разработки программного обеспечения [8]. С 1990-х годов было разработано большое количество инструментов, направленных на обеспечение защищённости

разрабатываемых программных продуктов. Одним из наиболее популярных методов обнаружения уязвимостей является метод анализа статического кода, заключающейся в анализе программного кода и выявлении элементов кода, которые могут быть использованы злоумышленником для нарушения безопасности программы. Обзор инструментов, предназначенных для статического анализа, представлен в [9]. Статический метод реализован в ряде инструментов, таких как Parasoft C ++10, Klocwork11, а также доступен сегодня в основных средствах разработки, таких как Clang (LLVM)12 и Microsoft Visual Studio13. Статический метод предназначен для выявления различных типов уязвимостей безопасности (например, переполнение буфера), но не обеспечивает обнаружение всех типов уязвимостей. Более того, статический метод может выявлять большое количество ложных уязвимостей. Одним из подходов к выявлению всех возможных уязвимостей является выполнение исчерпывающего множества всех программных сценариев с учетом всех входных значений. Подобный подход применяется в анализе Java-программ [10]. При разработке АСУ ИБ РИС должен быть реализован комплексный подход к проведению анализа исходного кода программного обеспечения, включающий в свой состав несколько современных аналитических инструментов.

Тестирование. Уязвимости в программном обеспечении способны привести к значительным негативным последствиям для конфиденциальности, доступности и целостности информации – отказ в обслуживании, перехват передаваемой информации и т.п. Одним из наиболее популярных подходов к анализу уязвимостей программного обеспечения является тестирование на проникновение – метод оценки защищенности системы, основанный на имитации действий внешнего злоумышленника. Тестированию могут подвергаться различные элементы и технологии – операционные системы [11], подсистемы шифрования [12], автоматические телефонные станции [13], и т.п. При проведении автоматизированного тестирования могут применяться специализированные программные средства – сканеры уязвимостей. Сравнительный анализ сканеров уязвимостей представлен в [14]. При проведении тестирования изделия на проникновение в качестве методической основы должны использоваться современные государственные стандарты по анализу уязвимостей14 и разработке защищённого программного обеспечения15. В процессе тестирования на проникновение должны использоваться приемы и инструменты, применяемые настоящими злоумышленниками. Процедуру тестирования на проникновение условно можно разделить на четыре этапа: идентификация целей и сбор информации, поиск уязвимостей, эксплуатация уязвимостей, подготовка отчёта по результатам тестирования.

Так же при анализе уязвимостей могут применяться альтернативные подходы, например, ручная проверка конфигурации системы или экспертный опрос. Ручная проверка заключается в проверке настроек программного обеспечения, политик, настроек и т.п. При выполнении данной работы аудитор, как правило, опирается на свои знания и рекомендации разработчиков программного обеспечения. Результатом ручной проверки является отчёт о соответствии реальных и необходимых параметров настроек безопасности, а также рекомендации по повышению безопасности анализируемой системы. Экспертный опрос сводится к анализу потенциальных уязвимостей группой экспертов, по результатам которого делается вывод о рисках нарушения безопасности информации. К основным недостаткам методов ручной настройки и экспертного опроса относятся отсутствие возможности проведения объективной оценки выявленных уязвимостей, а также ряд трудностей, связанных с обеспечением наглядной демонстрации последствий от реализации уязвимостей. Анализ сильных и слабых сторон методов анализа уязвимостей представлен в [15]. При анализе уязвимостей АСУ ИБ РИС должен быть использован метод тестирования на проникновение.

Заключение. АСУ ИБ РИС может быть использована в сетях передачи данных различного масштаба и назначения. Предложенный метод разработки АСУ ИБ РИС обеспечивает повышенную защищённость обрабатываемой информации за счёт:

1) проведение комплексных мероприятий, направленных на обеспечение разработки защищённой АСУ ИБ РИС;

2) наличия следующих функциональных возможностей, отличающих её от аналогов:

– обеспечение анализа поведения санкционированных пользователей и процессов информационной системы, а также выявления аномалий;

– автоматизированная оценка рисков информационной безопасности и безопасности информационной системы в целом;

– обеспечение оперативного воздействия на безопасность информационной системы.

[10] URL: https://www.parasoft.com/product/static-analysis-cc/
[11] URL: https://www.klocwork.com/
[12] URL: https://clang.llvm.org/
[13] URL: https://www.visualstudio.com/
[14] ГОСТ Р 56545-2015. Защита информации. Уязвимости информационной системы. Правила описания уязвимостей; ГОСТ Р 56546-2015. Защита информации. Уязвимости информационной системы. Классификация уязвимостей информационной системы.
[15] ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования.

СПИСОК ЛИТЕРАТУРЫ

1. Ахметьянова А.И., Кузнецова А.Р. Проблемы обеспечения информационной безопасности в России и её регионах // Фундаментальные исследования. 2016. № 8-1. С. 82–86.
2. Патент РФ 113442. Автоматизированная система управления защитой информации в территориально распределённой прикладной системе управления / Эркин А.Г., Петренко С.А., Бурыка В.И., Бакушев Е.И., Александров С.В., Котлова Т.Г., Фёдоров Ю.Е., Фоканов Г.В., Сорокин Д.П., Бедеров С.И., Любимов В.А., Рудыка С.А. Заявл. 27.09.2011. Опубл. 10.02.2012. Бюл. № 4. 2 с.
3. Патент РФ 91494. Модель построения защищенного Интернета / Волков М.В., Егоров А.В., Жуковский И.В., Матиевский А.В., Матюхин Д.В., Мартинкевич Ж.К., Пугин А.А., Давыдов Е.Б., Дольников А.А. Заявл. 01.10.2009. Опубл. 10.02.2010. Бюл. № 4.
4. Патент РФ 129279. Устройство обнаружения и защиты от аномальной активности на сети передачи данных / Ващенко М.А. Заявл. 09.01.2013. Опубл. 20.06.2013. Бюл. № 17. 3 с.
5. Козин И.С., Рощин А.А. Метод построения модели угроз безопасности критических автоматизированных систем военного назначения // Новые информационные технологии в системах связи и управления: сб. докладов XV Российской науч.-технической конф. (Калуга, 1 июня 2016). Калуга: Калужский научно-исследовательский институт телемеханических устройств. 2016. С. 255–257.
6. Козин И.С., Рощин А.А. Метод построения модели угроз критически важной информации военного назначения // Техника средств связи. 2016. № 5. С. 98–103.
7. Нечёткие множества и теория возможностей. Последние достижения / под ред. Р.Р. Ягера. М.: Радио и связь, 1986. 259 с.
8. Letychevskyi O., Sukhomlinov V. An Algebraic Approach for the Detection of Vulnerabilities in Software Systems // Proceedings of the Third International Conference on Electronics and Software Science. 2017. Pp. 53–60.
9. Kulenovic M., Donko D. A survey of static code analysis methods for security vulnerabilities detection // 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). 2014.
10. Pasareanu C. Symbolic Execution of Java Byte code // ISSTA'08 Preceeding. 2008.
11. Кикоть И.Р. Исследование потенциальных уязвимостей операционной системы Linux Astra Common Edition // Труды Северо-Кавказского филиала московского технического университета связи и информатики. 2016. Т. 1. № 9. С. 335–339.
12. Алексеев А.П. Анализ уязвимостей алгоритма вычисления секретного ключа в криптосистеме RSA // Инфокоммуникационные технологии. 2015. Т. 3. № 4. С. 464–467.
13. Нечай А.А., Котиков П.Е., Логашов С.В. Анализ уязвимостей автоматических телефонных станций // Наука и современность. 2014. № 2. С. 69–75.
14. Барсуков О.М., Гулянов А.С. Сравнительный анализ сканеров уязвимостей // Актуальные проблемы деятельности подразделений УИС: сб. материалов Всероссийской науч.-практической конф. (Воронеж, 28 мая 2015). Воронеж: ВУНЦ ВВС «ВВА им. проф. Н.Е. Жуковского и Ю.А. Гагарина», 2015. С.59–61.
15. Котляров В.П., Ядыменко К.А. Современный подход к анализу уязвимостей информационных систем // Путь науки. 2014. Т. 1. № 9. С. 38–41.

УДК 004.056.53 (003.26)

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ МОДИФИКАЦИИ ПРОТОКОЛА АУТЕНТИФИКАЦИИ НА ОСНОВЕ СЛАБОГО ПАРОЛЯ

Шенец Николай Николаевич, Трухина Екатерина Евгеньевна
Санкт-Петербургский политехнический университет Петра Великого
Россия, Санкт-Петербург, ул. Политехническая, д. 29,
emails: shenets@ibks.spbstu.ru, katoniya@gmail.com

***Аннотация*:** В статье предоставляются результаты исследования модифицированной версии протокола аутентификации на основе слабого пароля (PACE). Главная цель исследования заключалась в сравнении базовой версии протокола с модифицированной по качеству генерируемых ими последовательностей.

***Ключевые слова**: PACE; аутентификация на основе пароля.*

THE RESULTS OF STUDY OF THE MODOFIED PASSWORD AUTHENTICATED CONNECTION ESTABLISHMENT PROTOCOL

Nicolay Shenets, Ekaterina Trukhina
Peter the Great St. Petersburg Polytechnic University,
Russia, St. Petersburg, Polytechnicheskaya str. 29,
emails: shenets@ibks.spbstu.ru, katoniya@gmail.com

Abstract: The results of study of the modified version of the password authenticated connection establishment (PACE) protocol are provided. The major aim of the study has been consisted in comparison of the quality o**f generated sequences in modified version X–PACE and basic PACE.**

***Keywords**: PACE; password based authentication.*

Введение. Протокол Password Authenticated Connection Establishment (PACE) [1], разработанный федеральным управлением по информационной безопасности Германии (BSI) в 2007 году, позволяет двум сторонам сформировать общий, только им известный ключ, используя при этом короткий (низкоэнтропийный) пароль. Данный протокол используется преимущественно в smart-картах и разработан специально для них. Ранее нами была предложена модификация X-PACE [2] протокола PACE, позволяющая ускорить его выполнение без изменения криптографической стойкости. В данной статье приводятся результаты экспериментального анализа протокола X-PACE.

Описание протокола PACE и его модификации X-PACE. Протокол PACE устанавливает безопасный канал связи между двумя сторонами на основе взаимной проверки их подлинности и выработки общего ключа с использованием слабого пароля. В результате стороны вырабатывают сильный сеансовый ключ, который не зависит от силы пароля. В отличие от других протоколов, направленных на аналогичные цели, PACE был разработан для обеспечения высокого уровня гибкости в отношении криптографических алгоритмов. Он позволяет сформировать сеансовый ключ для различных симметричных шифров, а также ключ для выработки имитовставки.

Протокол PACE выполняется между двумя сторонами A (чип) и B (терминал), которые обладают общим паролем π, представляющим собой последовательность символов из алфавита {0, 1}. В первую очередь стороны согласуют долговременные параметры протокола D, которые включают параметры и идентификаторы используемых в PACE алгоритмов. Базовый протокол PACE состоит из четырех этапов.

На первом этапе стороны вырабатывают общую случайную последовательность s длины l бит. Второй этап предназначен для определения сторонами общей секретной образующей $\hat{G}$ циклической группы (как правило, группы точек эллиптической кривой), в которой на третьем этапе выполняется классический протокол Диффи – Хеллмана. Четвертый этап нужен для выработки ключей шифрования и имитозащиты, а также подтверждения сторонами знания этих ключей с помощью обмена имитовставками. Детальная схема протокола приведена на рис. 1. Параметры протокола D содержат: a, b, p — параметры эллиптической кривой над простым полем Fp, G — базовая точка группы точек эллиптической кривой порядка q, $f = \{C, \mathrm{H}, \mathrm{M}\}$ — криптонабор, который определяет функции зашифрования (C), хэширования (H) и вычисления имитовставки (M) соответственно. В результате выполнения протокола стороны определяют набор общих ключей $\mathrm{key} = (K_{enc}, K_{mac})$, идентификатор сеанса связи $\mathrm{sid} = (Y_A, Y_B, D)$ и pid — признак успешного завершения протокола или код ошибки в противном случае.

Модификация базового протокола (протокол X–PACE) заключается в замене операции зашифрования C на первом этапе протокола операцией XOR. Все остальное остается без изменений. В работе [2] была теоретически обоснована возможность такой модификации, однако не было проведено никаких сравнительных вычислительных экспериментов. Настоящая статья устраняет данный пробел. Поскольку в протоколе X–PACE изменился лишь один шаг, влияющий на способ генерации последовательности s, то цель исследования заключается в изучении качества этой псевдослучайной последовательностей по сравнению с базовым протоколом.

Результаты анализа. Базовый протокол PACE подразумевает использование различных криптографических алгоритмов шифрования и контроля целостности (криптонаборов). Наряду с зарубежными криптоалгоритмами (SHA-256 [3], AES и 3DES [4]) в исследовании были использованы и отечественные («Стрибог» [5], «Магма» и «Кузнечик» [6]). Особенностью протокола PACE является то, что результатом его первого этапа является 256-битная последовать (ключ), выработанная на основе низкоэнтропийного пароля. Для обеспечения стойкости протокола необходимо, чтобы возможные генерируемые последовательности были случайными (псевдослучайными). Однако для оценки случайности таких коротких последовательностей большинство известных наборов статистических тестов непригодно. Хорошо известные статистические тесты являются состоятельными лишь при достаточно большом объеме выборки. Поэтому основная задача экспериментального исследования состояла в выборе подходящего набора статистических тестов и определения методики тестирования.

Для выбора подходящих тестов использовались известные батареи тестов: Д. Кнута, Дж. Марсальи (DIEHARD), батарея тестов NIST, пакеты CRYPT-X и TESTU01. Вместе с этим изучались работы [7], [8], [9] по тестированию коротких последовательностей для составления адекватной методики тестирования. В результате оказалось, что наиболее подходящими в данных условиях являются некоторые тесты из батареи тестов NIST с использованием методики, предложенной F. Sulak [9].

Рассмотрим определение P-значения для каждого теста из набора NIST. Вначале тестируется каждая из m последовательностей длины n, для которой определяется свое значение Pi, $i = \overline{1, m}$. Полученные P-значения согласно [10] должны подчиняться равномерному закону распределения на интервале [0, 1]. После чего строится гистограмма частот Fk , $k = \overline{1, 10}$, попадания значений Pi в каждый из подынтервалов, на которые разбит интервал [0, 1]. Для проверки равновероятности распределения значений Pi используется χ^2 -критерий.

Однако, при тестировании «коротких» последовательностей, длина которых составляет от 128 до 512 битов, возникает две проблемы [9]. Первая заключается в применении асимптотического распределения при вычислении статистики. Для коротких последовательностей оно не применимо и должно быть заменено точным распределением, которое, как правило, трудно вычислить. Вторая

проблема возникает в связи с тем, что для коротких последовательностей вероятность того, что *P*-значение находится в подынтервале, не одинакова для всех подынтервалов, поскольку точное распределение является дискретным, а асимптотическое — непрерывным.

A (чип)		B (терминал)
пароль π		пароль π
аутентификационный параметр $D = (a,b,p,q,G,f)$		
$K_\pi = \mathcal{H}(\pi\|0)$		$K_\pi = \mathcal{H}(\pi\|0)$
выбрать $s \in \mathbb{Z}_q$		
$z = C(K_\pi, s)$		
	$\xrightarrow{z}$	
		$s = C^{-1}(K_\pi, z)$
выбрать $x_A \in \mathbb{Z}_q^*$		выбрать $x_B \in \mathbb{Z}_q^*$
$X_A = x_A \cdot G$		$X_B = x_B \cdot G$
	$\xleftarrow{X_B}$	
прервать, если $X_B = 0$		
	$\xrightarrow{X_A}$	
		прервать, если $X_A = 0$
$H = x_A \cdot X_B$		$H = x_B \cdot X_A$
$\hat{G} = s \cdot G + H$		$\hat{G} = s \cdot G + H$
выбрать $y_A \in \mathbb{Z}_q^*$		выбрать $y_B \in \mathbb{Z}_q^*$
$Y_A = y_A \cdot \hat{G}$		$Y_B = y_B \cdot \hat{G}$
	$\xleftarrow{Y_B}$	
прервать, если $Y_B \notin \langle G \rangle \setminus \{0\}$		
	$\xrightarrow{Y_A}$	
		прервать, если $Y_A \notin \langle G \rangle \setminus \{0\}$
$K = y_A \cdot Y_B$		$K = y_B \cdot Y_A$
$K_{enc} = \mathcal{H}(K\|1)$		$K_{enc} = \mathcal{H}(K\|1)$
$K_{mac} = \mathcal{H}(K\|2)$		$K_{mac} = \mathcal{H}(K\|2)$
$K'_{mac} = \mathcal{H}(K\|3)$		$K'_{mac} = \mathcal{H}(K\|3)$
$T_A = \mathcal{M}(K'_{mac}, (Y_B, D))$		$T_B = \mathcal{M}(K'_{mac}, (Y_A, D))$
	$\xleftarrow{T_B}$	
	$\xrightarrow{T_A}$	
прервать, если $T_B \neq \mathcal{M}(K'_{mac}, (Y_A, D))$		прервать, если $T_A \neq \mathcal{M}(K'_{mac}, (Y_B, D))$
key$= (K_{enc}, K_{mac})$		key$= (K_{enc}, K_{mac})$
sid$= (Y_A, Y_B, D)$		sid$= (Y_A, Y_B, D)$
pid$= \epsilon$		pid$= \epsilon$

Рис. 1. Схема протокола PACE

В связи с этим F. Sulak [9] предложил способ изменения существующих методик статистического тестирования. Идея заключается в том, чтобы для каждого подынтервала вычислить вероятность попадания в этот подынтервал *P*-значения. Для этого необходимо для каждого теста составить таблицу, состоящую из всех возможных тестовых переменных и соответствующих им *P*-значений. Таким образом, для каждого $k = \overline{1,10}$ необходимо вычислить вероятность $p_k = P\left(\frac{k-1}{10} \le P - значение \le \frac{k}{10}\right)$. После этого остается применить критерий χ^2 для значений p_k.

Были отобраны и реализованы следующие тесты NIST:

1. Частотный побитовый тест (Frequency test).
2. Частотный блочный тест (Frequency Test within a Block).
3. Частотный целочисленный тест (Integer Frequency Test).
4. Тест кумулятивных сумм (Cumulative Sums Test);
5. Тест серий (Runs test);
6. Проверка максимальной длины серии в блоке (Test for the Longest Run of Ones in a Block);
7. Тест пересекающихся *m*-грамм (Serial test);
8. Тест на основе приращения энтропии (Approximate Entropy Test);
9. Тест на основе линейной сложности (Linear Complexity Test);

10. Тест на основе профиля линейной сложности (Linear Complexity Profile Test).

Был разработан программный макет на языке Java с использованием эмулятора Java-card. В макете были реализованы: базовый протокол PACE и модифицированный протокол X-PACE с подключением различных криптонаборов, а также статистические тесты согласно методике тестирования, предложенной в [9].

Программа тестирования была запущена на Java HotSpot(TM) 64-Bit Server VM (build 25.73-b02, mixed mode) с процессором Intel(R) Core(TM) i5-2450M. Для проведения тестирования был принят единый для всех пароль π = «1234»; установлены уровень значимости $\alpha = 0,01$ и количество тестируемых последовательностей m = 100.

Двоичная последовательность считается случайной, а тест пройденным, если $P\text{-}значение \geq 0,01$. В противном случае последовательность неслучайна, а тест не пройден. Считается [11], что генератор проходит тест, если $P_{выборки} \geq 0,0001$ при $r \geq r_{\min}$, где r — отношение количества последовательностей, прошедших тест, к количеству всех тестируемых последовательностей, а rmin — нижний граничный уровень, который определяется по формуле $r_{\min} = \hat{p} - 3\sqrt{\frac{\hat{p}(1-\hat{p})}{m}}$, где $\hat{p} = 1 - \alpha$. То есть для m = 100 и $\alpha = 0,01$, $r_{\min} = 0,99 - 3\sqrt{\frac{0,99 \cdot 0,01}{100}} \approx 0,96$

В таблице 1 представлены результаты тестирования генераторов, исходя из которых можно сделать вывод, что каждый генератор прошёл тестирование. Это говорит о высокой надёжности тестируемых генераторов.

Таблица 1

Результаты тестирования

№	Тест	SHA-256 + AES	SHA-256 + 3DES	SHA-256 + XOR	Стрибог + Кузнечик	Стрибог + Магма	Стрибог + XOR
1	Frequency	0,798246	0,599511	0,913429	0,075221	0,826574	0,913429
2	Block Frequency	0,399693	0,321584	0,968392	0,688987	0,379033	0,968392
3	Integer Frequency	0,502845	0,915284	0,115632	0,940597	0,353518	0,115632
4	C. Sums Forward	0,879441	0,099946	0,343515	0,479111	0,878145	0,343515
5	C. Sums Backward	0,885363	0,915073	0,696366	0,541380	0,537840	0,696366
6	Runs	0,448711	0,803700	0,128739	0,618217	0,353598	0,128739
7	Longest Runs	0,458573	0,123003	0,981435	0,758139	0,418612	0,981435
8	Serial	0,622582	0,082014	0,992648	0,030512	0,813397	0,992648
9	Approx. Entropy	0,330056	0,590576	0,765880	0,199785	0,881132	0,765880
10	Lin. Complex.	0,000405	0,968730	0,776041	0,838918	0,094836	0,776041
11	Lin. Complex. Profile	0,728193	0,238799	0,968056	0,259826	0,760552	0,968056

Доля прохождения теста на нижний граничный уровень $r_{\min}$ = 0,96, а верхняя — на «идеальный» граничный уровень, для которого при m = 100 и $\alpha = 0,01$ может быть отвергнута только одна последовательность из ста при прохождении теста. Стоит отметить, что только два генератора (SHA-256 + XOR и Стрибог + XOR) не выходят за пределы «идеального» граничного уровня. Таким образом, модификация X-PACE ничем не уступает оригинальному протоколу. Также стоит отметить, что среди генераторов, реализующих схему PACE, лучше всех себя показал генератор Стрибог + Магма.

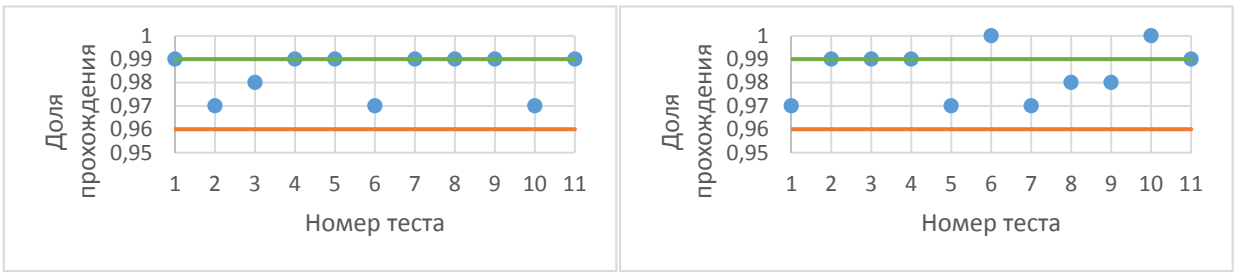


Рис. 2. Результаты тестирования: слева SHA-256+AES, справа – SHA-256+3DES

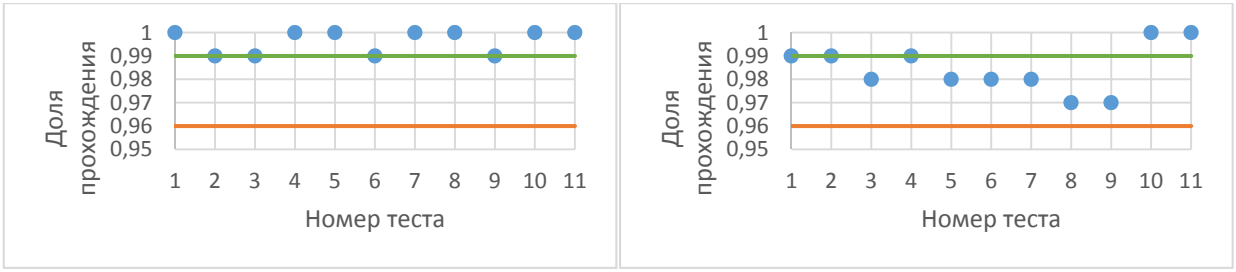


Рис. 3. Результаты тестирования: слева SHA-256+XOR, справа – Стрибог +Кузнечик

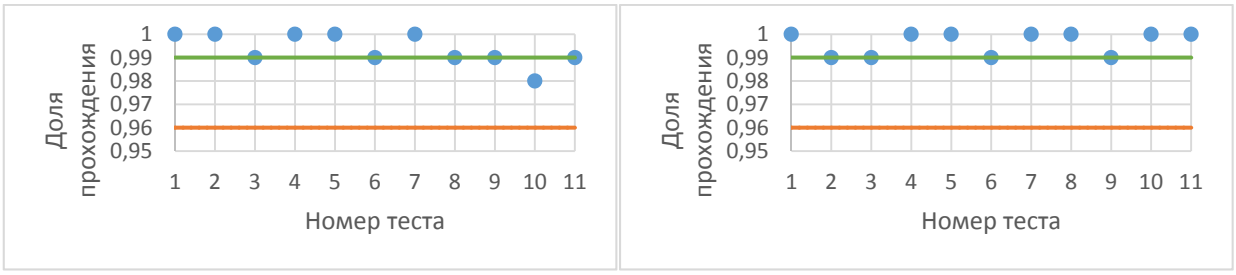


Рис. 4. Результаты тестирования: слева Стрибог+Магма, справа – Стрибог +XOR

Заключение. В результате экспериментов было показано, что модифицированная версия X-PACE протокола PACE не уступает исходной по качеству генерируемых на первом этапе ключей. Более того, оказалось, что лучшим криптонабором по этому критерию является пара отечественных алгоритмов «Стрибог» и «Магма».

СПИСОК ЛИТЕРАТУРЫ

1. Ullmann M., Kügler D., Neumann H., Stappert S., Vögeler M. Password Authenticated Key Agreement for Contactless Smart Cards // Communications of the ACM, 2008.
2. Шенец Н.Н., Трухина Е.Е. X–PACE: Модифицированный протокол аутентификации на основе слабого пароля // Проблемы информационной безопасности. Компьютерные системы. 2016, № 4, С. 106–112.
3. FIPS PUB 108-4. 2015.
4. ISO/IEC 18033-3:2010 Information technology. Security techniques. Encryption algorithms. Part 3: Block ciphers. 2010.
5. ГОСТ Р. 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. Москва: Стандартинформ, 2012.
6. ГОСТ Р. 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. Москва: Стандартинформ, 2015.
7. Soto J. Randomness Testing of the AES Candidate Algorithms // NIST Interagency or Internal Report (NIST IR) 6390, September 1999.
8. Doganaksoy A., Ege B., Kocak O., Sulak F. Cryptographic Randomness Testing of Block Ciphers and Hash Functions // Cryptography ePrint Archive: Report 2010/564, 11 November 2010.
9. Sulak F. Statistical analysis of block ciphers and hash functions // Publication of the Middle East Technical University Ph.D Examinations, February 2011.
10. Потий А., Орлова С., Гриненко Т. Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS // [Электронный ресурс]. URL: http://pnzzi.kpi.ua/2/02_p206.pdf (дата обращения 01.09.2017).
11. Rukhin A., Soto J., Nechvatal J., Smid M., et al A statistical test suite for random and pseudorandom number generators for cryptographic applications // NIST Special Publication 800-22 Revision 1a, 2010.

МОЛОДЕЖНЫЕ НАУЧНЫЕ ШКОЛЫ: БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 519.688

ПОСТРОЕНИЕ ИНФОРМАЦИОННО-МОНИТОРИНГОВОЙ СИСТЕМЫ АРОМОБЕЗОПАСНОСТИ НА АППАРАТНО-ПРОГРАММНЫХ СРЕДСТВАХ

Антонов Валерий Валентинович
Санкт-Петербургский государственный университет телекоммуникаций им.проф. М. А. Бонч-Бруевича
Россия, Санкт-Петербург, пр. Большевиков, д. 22
email: antonler@rambler.ru

Аннотация: В статье рассмотрены вопросы построения и функционирования информационно-мониторинговой системы аромобезопасности на аппаратно-программных средствах Arduino. Передаваемая информация передаётся на сервер событий который обрабатывает событие в соответствии с заданным алгоритмом реагирования. В статье рассмотрено только использование газоанализаторных датчиков, однако открытая архитектура такой системы позволяет не только использовать большое количество существующих датчиков и модулей, но и проектировать новые устройства.

Ключевые слова: *аромобезопасность; умный датчик запахов (терминал запахов); сервер событий.*

CONSTRUCTION OF THE INFORMATION-MONITORING SYSTEM OF AROMA-SAFETY ON HARDWARE AND SOFTWARE

Antonov Valery
Federal State Budget-Financed Educational Institution of Higher Education
The Bonch-Bruevich Saint - Petersburg State University of Telecommunications,
Russia, St. Petersburg, Prospekt Bolshevikov str. 22,
email: antonler@rambler.ru

Abstract: In the article the questions of construction and functioning of the information-monitoring system of aroma-safety on hardware-software means Arduino are considered. The transmitted information is transmitted to the event server that processes the event in accordance with the specified response algorithm. The article considers only the use of gas analyzers, but the open architecture of such a system allows not only to use a large number of existing sensors and modules, but also to design new devices.

Keywords*: aroma safet;, smart odor sensor (odor terminal); event server*

Введение. Современное развитие микроэлектроники позволяет создавать недорогие и миниатюрные аппаратные платформы контроля состояний различных датчиков и анализаторов. Это позволяет выделить в проблематике глобальной безопасности государства проблему «персональной безопасности личности». «Персонализация» в совокупности с информационными технологиями позволит обеспечить постоянный контроль угроз для каждого человека. К числу внешних угроз безопасности личности относятся:

– опасные для здоровья воздействия естественной и антропогенной среды, техносферы, производственных процессов и т.п.;

– социальные взаимодействия, обусловленные терроризмом, алкоголизмом, наркоманией и др. факторами.

Одним из признаков, указывающим на возникновения угроз такого типа, является запах. Возможность датчика определять не только само присутствие конкретного вещества в воздухе но и его концентрацию позволяет построить информационную систему адекватного реагирования на угрозу, то есть определить сценарий нейтрализации угрозы. И этот сценарий будет разным при минимальной утёчке бытового газа – требующий вызова аварийной машины газовой службы, или обнаружение минимальной взрывоопасной концентрации – требующий вызова всех служб быстрого реагирования и проведения эвакуации людей из опасной зоны.

Система аромобезопасности является принципиально новым объектом. Она:

– позволяет создать качественно новую защиту от угроз безопасности человека во многих практических ситуациях,

– создается на стыке самых современных технологий интернета вещей, широкополосного мобильного доступа, навигации, облачных вычислений, больших данных, наложенных сервисов и нанотехнологий,

– будет доступна и может использоваться широким кругом потребителей.

Система может быть построена на трех уровнях:

– физический уровень реализуется датчиками (сенсорами) запахов,

– логический уровень реализуется сетью датчиков при помощи технологий мобильного доступа и интернета вещей,

– когнитивный уровень реализуется протоколами взаимодействия с пользователями при помощи технологий наложенных сервисов, облачных вычислений и больших данных.

На рис. 1. Представлена упрощённая блок-схема клиентской части системы терминала запахов.

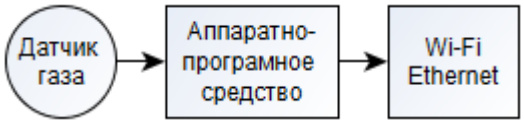


Рис.1. Блок схема клиентского модуля

Основной задачей терминала запахов является информирование сервера событий о превышении концентрации отслеживаемого вещества в окружающем терминал пространстве. Информирование осуществляется при помощи отправки сообщения о тревоге.

При включении питания на клиентском модуле запускается специализированная программа, которая считывает данные с датчика газа и устанавливает и поддерживает сеанс связи с сервером событий. Адрес сервера событий устанавливается на клиентском модуле при первоначальной настройке. Связь с сервером событий может осуществляться с использованием технологий применимых в каждом конкретном месте установки терминала запахов. Таким же образом задаются и некоторые начальные параметры, например минимальный порог срабатывания тревоги и интервал обмена диагностическими сообщениями с сервером событий. На каждое принятое диагностическое сообщение любой из модулей системы отвечает соответствующим диагностическим сообщением. Отсутствие в течении заданного интервала времени ответа на посланное сообщение приводит к включению в системе режима «тревога». При этом на сервере событий запускается соответствующий алгоритм обработки такой тревоги.

На рис. 2. Представлена упрощённая блок схема «сервера событий»

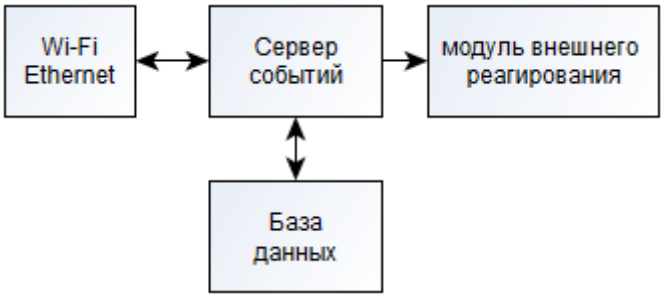


Рис.2. Блок схема серверного модуля

Основной задачей сервера событий является фиксация и обработка принятого от терминала запахов сообщения. Для каждого из сообщений приходящих на сервер существует свой сценарий обработки. Всю информацию сервер передаёт для обработки в модуль внешнего реагирования. Модуль внешнего реагирования, например, может выполнять вызов машин экстренных служб, информирование руководства района, собственника здания, включение громкоговорителей для объявлений об эвакуации и т.д.

Клиенты и сервер системы осуществляют взаимодействие посредством разработанного автором бинарного протокола. В основе протокола лежит широко применяемый в клиент серверной архитектуре принцип разбиение сообщения на части заранее определённой размерности. Все сообщения в системе в обязательном порядке состоят из:

– уникальный идентификатор сообщения – 2 Байт

– длинна тела сообщения – 4 Байт

– тело сообщения

Тело сообщения может внутри себя содержать дополнительные поля определяемые на этапе проектирование протокола взаимодействия.

Наиболее нагруженной частью системы является сервер событий. Перебои в его работе могут привести к трагическим последствиям. Для программной реализации сервера событий была применена акторная модель[1]. Применение подобной модели зарекомендовала себя с лучшей стороны в системе распознавания образов.

Заключение. Система аромобезопасности должна стать начальной платформой на которой в дальнейшем будет строится система безопасной городской среды. Применение других газовых датчиков позволит, например, контролировать наличие алкоголя в выдыхаемом воздухе водителя городского транспорта. Возможности применения такой системы ограничены только приборами контроля. Ещё одним из возможных вариантов развития является создание сети из нескольких серверов событий передающих информацию одному общему серверу системы и построение региональной системы контроля. Результатом разработки является аппаратный прототип терминала запахов с одним датчиком и прототип сервера событий

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция; сб.науч. ст. в 4 т. /Под. ред. С. В. Бачевского; сост. А. Г. Владыко, Е. А. Аникевич. СПб. : СПбГУТ, 2017. Т. 2. С. 87-90.
2. Шершнев И. Л. Национальная безопасность России как система // НАВИГУТ (приложение к журналу «Безопасность Евразии»). 2000. № 1. С. 45–54

УДК 004.021

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ ПОДХОДОВ ВИДЕОСТЕГОАНАЛИЗА

Ахрамеева Ксения Андреевна, Попов Леонид Геннадьевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича,
Россия, Санкт-Петербург, пр-кт Большевиков, д. 22, к. 1,
emails: ksenya_2002@mail.ru, leonidlitvinovo1994@mail.ru

Аннотация: Рассмотрены методы стегоанализа цифровых видеопоследовательностей, основанные на различных подходах к оценке покрывающих объектов, в которые было произведено вложение стегообъектов для осуществления скрытых коммуникаций (простая линейная коллизия, калибрование, асимптотическое незапоминающее обнаружение и др.). Описаны результаты сравнительного анализа данных методов обнаружения, а также возможность их практического применения в приложениях реального времени.

Ключевые слова: *стеганография; стегоанализ; цифровая видеопоследовательность; скрытые коммуникации.*

COMPARATIVE ANALYSIS OF EFFICIENCY OF THE VIDEO STEGANALYSIS APPROACHES

Akhrameeva Ksenia, Popov Leonid
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
Russia, Saint Petersburg, prospect Bolshevikov 22, building 4,
emails: ksenya_2002@mail.ru, leonidlitvinovo1994@mail.ru

Abstract: Methods of steganalysis of digital video sequences based on different approaches of estimation of covering object, in which covert signals was embedded to perform covert communications (simple linear collusion, calibration, asymptotic memoryless detection and others), are considered. The results of comparative analysis of these detection methods and the opportunity of its practical employment in real-time applications are described.

Keywords: *steganography, steganalysis, digital video sequence, covert communications.*

Введение. В настоящее время интернет стал источником большого количества цифровых файлов, содержащих различные формы данных (программы, изображения, видео и др.). Большой процент этих файлов нуждается в защите их целостности и авторского права создателей [1], [2], [3]. Кроме того, в этих условиях скрытые коммуникации представляют наибольшую угрозу, чем когда-либо [4], [5]. Так стеганография, используя сжатый видеопоток, может достигать большой ёмкости и высокого уровня секретности, даже при низких скоростях вложения. Поэтому всё большее внимание уделяется стегоанализу цифровых видеопоследовательностей, что является целью данной статьи. Традиционно наибольшее количество исследований и работ было посвящено стегосистемам в изображениях [6], [7], [8], [9]. Что касается проблемы стегоанализа видеопоследовательностей [10], то здесь необходимо учитывать свои особенности, обусловленные пространственными и временны́ми корреляциями между кадрами (изображениями), способом сжатия и кодирования и т.д.

В рамках данной работы были исследованы пять различных методов стегоанализа цифровых видеопоследовательностей.

Стегоанализ цифрового видео, использующий статистическую видимость во временно́й области

На рисунке 1 представлены основные этапы [11], [12]: атака коллизии $\mathfrak{C}_P$, разность между исходным (Y_k) и оценённым ($\widehat{U}_k$) кадрами, анализ остатка разности на присутствие вложения (классификатор образцов).

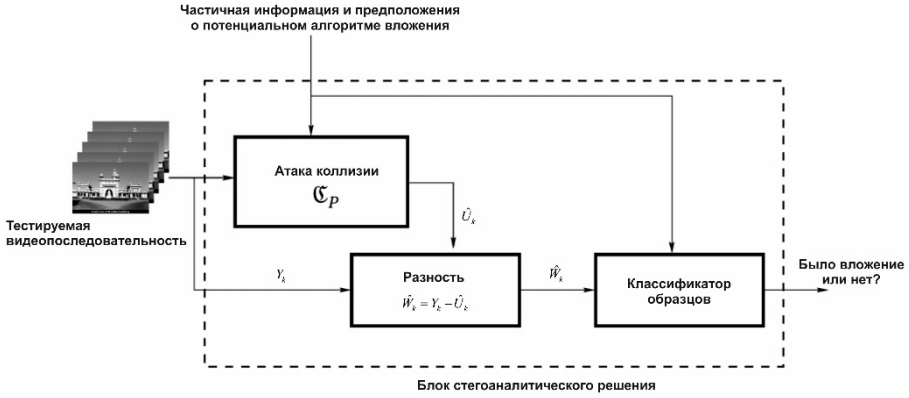


Рис. 1. Предлагаемый фреймворк для стегоанализа

В общем случае коллизия выражается формулой:

$$\widehat{U}_k = \mathfrak{C}(Y_k) = C[Y_1, Y_2, \dots, Y_n], \quad (1)$$

где $\widehat{U}_k$ – это результат коллизии и в этой статье представляет оценку k-го хост-фрейма U_k, $\mathfrak{C}_P$ – это оператор коллизии с параметром P (представляющий собой длину окна коллизии), который использует сходства и различия среди всех или выбранного подмножества возможно «заражённых» кадров изображения $Y_1, Y_2, \dots, Y_N$, чтобы создать $\widehat{U}_k$.

Предполагается, что стеганография появляется при добавлении гауссовских водяных знаков, поэтому используются параметры, которые могут измерить уровень гауссовости в сигнале. Для этого вводятся понятия эксцесса, энтропии и 25-го процентиля, которые содействуют этапу распознавания вложения.

Таким образом, данный алгоритм стегоанализа использует преимущество временно́й избыточности, присутствующей в видео, что приводит к улучшенной эффективности по сравнению с чисто пространственными методами.

Стегоанализ цифровых видео с использованием асимптотического незапоминающего обнаружения

Общая схема данного метода [13] изображена на рисунке 2.

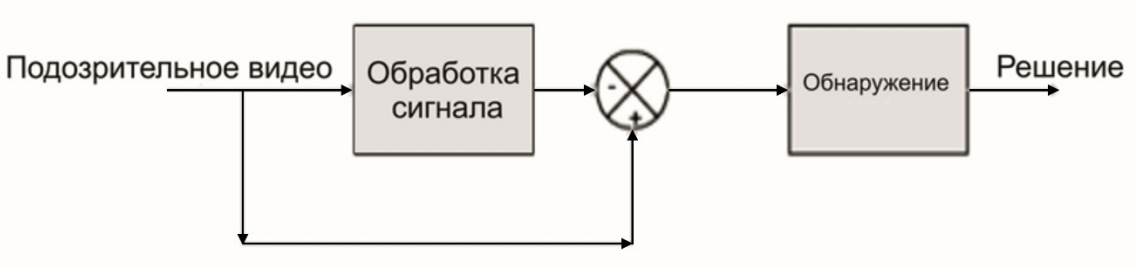


Рис. 2. Алгоритм стегоанализа

Предполагается, что один из фреймов (F_n) оказывается потерянным из видео и нуждается в интерполяции. Использованием фреймов, расположенных в непосредственной близости, которые обозначаются как F_{n-1} и F_{n+1}, восстанавливается оцениваемый фрейм $F_n^{\#}$. Метод оценки движения, который используется для сопоставления блоков – это техника суммы абсолютных разностей (САР). В результате оценки получаем разность $F_n - F_n^{\#}$, которая используется далее в детекторе.

Использование АОЭ (асимптотическая относительная эффективность) детектора требует знания нелинейности:

$$g(x) = \sum_{i=0}^{M} \alpha_i \cdot x^i, \quad (2)$$

Эта нелинейность полиномиальная, где коэффициенты α_i могут быть получены, как только эффективность η (мера производительности в тестах АОЭ) максимизирована.

Особенность данной схемы стегоанализа заключается в том, что порог T является изменяющимся в зависимости от следующих характеристик: размер видео, стандартная девиация, коэффициенты корреляции. На рисунке 3 представлена схема обнаружения вложения, где

$$H_0: Y_i = N_i; \quad (3)$$

$$H_1: Y_1 = N_i + \theta \cdot S_i, \quad (4)$$

где N_i и S_i представляют распределения шума и сигнала i-го фрейма, соответственно, θ – глубина вложения скрытого сигнала.

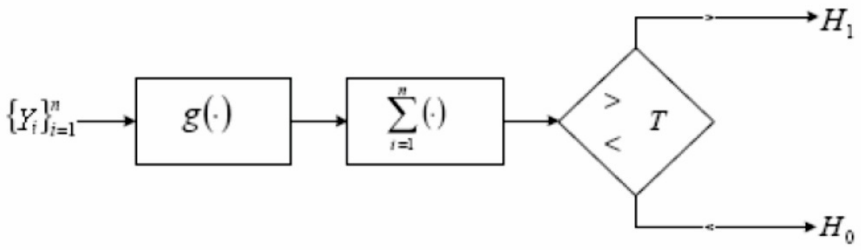


Рис. 3. Этап обнаружения

Система, работающая по данному алгоритму, позволяет определить присутствие стеганографии, даже когда вложение было произведено в небольшое количество фреймов (в отличие от предыдущего подхода). Кроме того, порог является изменяющимся в зависимости от характеристик: размер видео; стандартная девиация; его коэффициенты корреляции, а также учитывается количество кадров, которые должны быть проанализированы при каждом прохождении через детектор.

Видеостегоанализ, использующий параметры реверсии вектора движения

Данный метод [14] эффективен для видеостегообъектов, созданных с помощью MVs (Motion Vectors). Для осуществления стегоанализа используется калибровочный подход.

При декомпрессии стего-видео в пространственную область и сжатии его снова без вложения, изменённые вектора движения склонны возвращаться к своим предшествующим значениям. Вследствие чего MVs калиброванных видео имеют большинство макроскопических параметров, сходных с параметрами чистых видео.

Поэтому выполняется калибровка повторным сжатием. Теперь, если один определённый вектор движения $mv = (h, v)$ возвращается к $\widehat{mv} = (\hat{h}, \hat{v})$ после калибровки, то эта реверсия называется как «shift (изменение, сдвиг, переключение)». В связи с этим вводится такое понятие как расстояние сдвига или расстояние переключения (SD – shift distance):

$$SD(mv) = |\hat{h} - h| + |\hat{v} - v|, \qquad (5)$$

где $mv = (h, v)$ – вектор движения до калибровки, $\widehat{mv} = (\hat{h}, \hat{v})$ – вектор движения после калибровки.

Таким образом, стего-видео будет иметь меньшую часть векторов движения с нулевым сдвигом и большую долю векторов движения с ненулевым сдвигом.

Улучшение видеостегоанализа путем использования временно́й корреляции

На рисунке 4 представлена схема основных этапов [15]: предсказание скомпенсированного движения, чтобы получить PEFs (prediction-error frames); вычисление разности между PEFs и их пространственно-предсказанными кадрами; разложение результирующих фреймов с использованием 3-уровневого DWT (discrete wavelet transform); вычисление первых 3-ёх моментов характеристических функций (CFs – characteristic functions) в каждом поддиапазоне.

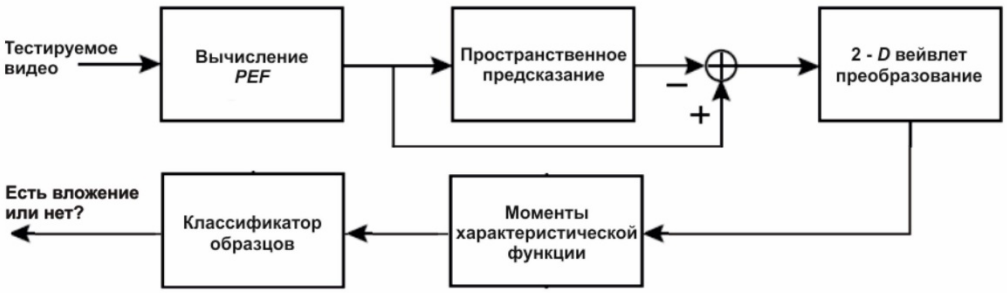


Рис. 4. Схема стегоанализа

Вследствие декоррелирующего свойства вейвлет преобразования, характеристики, извлечённые из каждого поддиапазона независимы.

n – ый момент характеристической вейвлет функции в вейвлет поддиапазоне может быть представлен как:

$$M_n = \frac{\sum_{k=0}^{N/2} f_k^n |H(f_k)|}{\sum_{k=0}^{N/2} |H(f_k)|} \qquad (6)$$

, где $H(f_k)$, $k = 0,1, \ldots N-1$ – это дискретное преобразование Фурье коэффициентов гистограммы, а N – это количество значений дискретной величины в гистограмме.

Далее, полученные характеристические вектора используются для обучения классификаторов образцов.

Стегоанализ мультипликативной широкополосной стеганографии

Следующий метод видеостегоанализа [16] эффективен по отношению к мультипликативному широкополосному вложению.

Для оценки используются шумоподавление (а точнее стационарный вейвлет с мягким определением порога [17]) и межфреймовая оценка путём сопоставления блоков 8×8 (как в стандартах видеосжатия [18]).

После извлечения некоторых параметров (дисперсия остаточных значений, островершинность распределений и др.) из видеокадров и остаточной матрицы полученное видео классифицируется как «подозрительное» или «неподозрительное».

В случае «подозрительного» видео оценивается скрытое сообщение и глубина вложения, используемая на стороне вложения.

Используя оценённое скрытое сообщение и глубину вложения создаётся новая оценка видео, которая снова подаётся на вход системы (см. рисунок 5). Следовательно, осуществляется повторная оценка покрывающего медиа, что приводит к более эффективному стегоанализу.

Рис. 5. Блок-схема системы стегоанализа

Выводы. В таблице 1 приведены основные характеристики рассмотренных методов.

Проведя анализ данных методов, можно выделить следующие закономерности:

– чем больше глубина вложения, тем выше вероятность верного обнаружения стеганографии и оценки скрытого сообщения;

– все вложения предполагаются независимыми друг от друга и имеют нулевое матожидание;

– стегоанализ улучшается, когда увеличивается количество повреждённых фреймов (для [11], [12] и [13]).

[11], [12] Оптимальная длина окна коллизии увеличивается для больших глубин вложения. В дальнейшем есть необходимость в том, чтобы длина окна выбиралась автоматически на основе характеристик видеопоследовательностей таких как: коэффициент корреляции ρ, степень глобального движения, дисперсия фреймов.

Чтобы сорвать работу коллизионного стегоанализа [11], [12] нужно использовать α от 1 до 3, но в этом случае вложение становится уязвимым к удалению.

В случае использования kNN классификатора необходимо оптимизировать его обучение и выбор параметров, ведь количество последовательностей, необходимых для обучения зависит от применения.

Отдельно стоит сказать о возможности улучшения предложенных в [14] параметров, чтобы ослабить их зависимость от склонности реверсии векторов движения. Это, в свою очередь, приведёт к устойчивости метода по отношению к оптимизации способа вложения данных, направленной на ослабление склонности векторов к реверсии.

Преимуществом схемы [15] является то, что temporal prediction error frames могут быть прямо получены частичным декодированием сжатых последовательностей, что уменьшает количество вычислений. В качестве минуса можно отметить, что производительность ухудшается при увеличении скорости вложения.

Таким образом, мы видим, что при стегоанализе видеопоследовательностей применяются похожие на стегоанализ изображений принципы, но есть свои специфические особенности, связанные с областью (пространством), в которой приходится работать стегоаналитику.

В будущем есть перспектива усовершенствовать методы для работы с быстро движущимися последовательностями и для применения к более широкому набору стеганографических подходов, т.е. повысить универсальность.

Таблица 1

Сравнение методов стегоанализа видеопоследовательностей

Параметры сравнения\название метода	Статистическая видимость во временно́й области	Асимптотическое относительное обнаружение	Параметры реверсии вектора движения	Улучшение слепого стегоанализа с использованием временно́й корреляции	Стегоанализ мультипликативной широкополосной стеганографии
Принцип действия	Временны́е корреляции	Временны́е корреляции	Вектора движения	Пространственно-временны́е корреляции	Избыточность видеофреймов, пространственно-временны́е корреляции
Вид стеганографии	Гауссовское широкополосное вложение + DCT (discrete cosine transform) вложение	Гауссовское широкополосное вложение	Вложение в вектора движения	Гауссовское широкополосное вложение	Мультипликативное широкополосное вложение
Тип вложения	Аддитивное	Аддитивное	Аддитивное	Аддитивное	Мультипликативное
Оценка исходного медиа	Простая линейная коллизия	Оценка движения	Калибрование	Пространственно-временное предсказание (оценка движения)	Шумоподавление + оценка движения
Распознавание образов	Оценка Гауссовости в разностном сигнале	Знание нелинейности	Реверсия и новые параметры, основанные на «скачке (shift)»	39-мерные характеристические вектора	Извлечение параметров из видеофреймов и остаточной матрицы
Тип классификатора	kNN (k Nearest Neighbor)-классификатор (k=1)	АОЭ-детектор	SVM-классификатор Chang-а с многочленным ядром [12]	kNN-классификатор (k=1)	SVM-классификатор с ядром в виде радиальной базисной функции
Извлечение параметров перед детектором	Да (эксцесс, энтропия, 25-ый процентиль)	Нет (детектор использует всю информацию, доступную ему)	Да + свои параметры на основе «скачка (shift)»	Да	Да
Тип порога	Неизменный	Адаптивный	Неизменный	Неизменный	Неизменный
Модель распределения	Модель Маркова первого порядка	Сигнал временно подчиняется модели Гаусса-Маркова	Лаплас для DCT	—	—

СПИСОК ЛИТЕРАТУРЫ

1. Коржик В.И., Тришневская И.А. Исследование метода аутентификации двоичных изображений при помощи цвз // Труды учебных заведений связи. 2016. Т. 2. № 1. С. 95-98.
2. Lee M.H., Korzhik V., Lusse S., Kurbatov E., Morales-Luna G. Image authentication based on modular embedding // IEICE Transactions on Information and Systems. 2006. Т. E89-D. № 4. С. 1498.
3. Красов А.В., Верещагин А.С., Цветков А.Ю. Аутентификация программного обеспечения при помощи вложения цифровых водяных знаков в исполняемый код // Телекоммуникации. 2013. № S7. С. 27-29.
4. Небаева К.А., Скородумов С.А. Стеганография в ip-телефонии и сложности ее реализации // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей V международной научно-технической и научно-методической конференции. 2016. С. 494-498.
5. Небаева К.А., Хабаев Н.С. Сокрытие данных в звуковом файле // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах. 2015. С. 372-376.
6. Коржик В.И., Небаева К.А., Герлинг Е.Ю., Догиль П.С., Федянин И.А. Цифровая стеганография и цифровые водяные знаки // Под общей редакцией профессора В.И. Коржика. Санкт-Петербург, 2016. Том. Часть 1. Цифровая стеганография.
7. Горышин К.С., Небаева К.А. Сравнение эффективности методов построения стегосистем с информированным кодером // Труды учебных заведений связи. 2016. Т. 2. № 1. С. 47-52.
8. Годлевский А.К., Коржик В.И. Стегосистемы повышенной секретности для вложения информации в неподвижные изображения // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей V международной научно-технической и научно-методической конференции. 2016. С. 320-323.
9. Коржик В.И., Панфилов Ю.Н. Оптимизация параметров нуль-битовой системы цвз с учётом возможной атаки двусмысленности // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах. 2015. С. 340-345.
10. Небаева К.А., Попов Л.Г. Анализ методов стегоанализа цифровых видеопоследовательностей // Телекоммуникации. 2017. № 1. С. 33-40.
11. Budia U., Kundur D. and Zourntos T. Digital video steganalysis exploiting statistical visibility in the temporal domain // IEEE transactions on information forensics and security. December 2006. vol. 1. no. 4. pp. 502 – 516.
12. Ахрамеева К.А., Попов Л.Г. Исследование метода стегоанализа цифровых видеопоследовательностей, основанного на феномене линейной коллизии // Труды учебных заведений связи. 2017. Т. 3. № 2. С. 28-36.
13. Jainsky J. S., Kundur D. and Halverson D. R. Towards digital video steganalysis using asymptotic memoryless detection // Proceedings of the 9th international workshop on multimedia and security. Dallas, TX, USA, 2007. pp. 161 – 168.
14. Cao Y., Zhao X. and Feng D. Video steganalysis exploiting motion vector reversion-based features // IEEE signal processing letters. January 2012. vol. 19. no. 1.
15. Pankajakshan V. and Ho A. T. S. Improving video steganalysis using temporal correlation // Proceedings of the 3rd international conference on intelligent information hiding and multimedia signal processing. November 2007. vol. 1. pp. 287 – 290.
16. Zarmehi N. and Akhaee M. A. Video steganalysis of multiplicative spread spectrum steganography // School of electrical and computer engineering college of engineering. University of Tehran, Tehran, Iran {zarmehi, akhaee} @ut.ac.ir.
17. Donoho D.L. De-noising by soft-thresholding // IEEE Trans. on Information Theory. May 1995. vol. 41. no. 3. pp. 613–627.
18. Yang J., Yin B. and Zhang N. A block-matching based intra frame prediction for h.264/avc // in IEEE international conference on multimedia and expo. July 2006. pp. 705–708.

УДК 004.42

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ШИФРОВАНИЯ БАЗ ДАННЫХ В РАЗРАБОТКЕ СОВРЕМЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Грибачев Виталий Петрович, Харитонов Георгий Дмитриевич
Санкт-Петербургский государственный университет телекоммуникаций «СПбГУТ»,
Россия, Санкт-Петербург, наб.р. Мойки, д. 23,
emails: y270166@yandex.ru, haritonov67273@gmail.com

Аннотация: В статье рассмотрено применение режима Transparent Database Encryption (TDE) для защиты баз данных. Приводится анализ результатов экспериментальных замеров времени функционирования приложения, использующего базу данных SQLite в режиме TDE, реализованном на основе использования библиотеки SQLCipher.

Ключевые слова: *шифрование данных; Transparent Database Encryption; базы данных; прозрачное шифрование данных; защита баз данных;*

PROSPECTS OF APPLICATION OF DATABASE ENCRYPTION IN MODULAR SOFTWARE DEVELOPMENT

Gribachev Vitaly Petrovich, Kharitonov Georgiy Dmitrievich
Saint-Petersburg State University of Telecommunications "SPbGUT"
Russia, St. Petersburg, nab. Moiki, 23,
emails: y270166@yandex.ru, haritonov67273@gmail.com

Abstract: The article discusses the use of the Transparent Database Encryption (TDE) mode to protect databases. An analysis of the results of experimental measurements of the running time of an application using the SQLite database in TDE mode, implemented using the SQLCipher library, is presented.

Keywords: *data encryption; Transparent Database Encryption; Database; transparent data encryption; protection of databases.*

По данным аналитических центров ведущих компаний, занимающихся защитой информации, число краж персональных данных ежегодно значительно возрастает. Так, за прошлый год в России по

данным аналитиков, число подтвержденных случаев кражи персональных данных из разных источников возросло на 80%. В числе данных инцидентов наибольшее количество случаев пришлось на различные компании, в той или иной степени занимающиеся обработкой персональных данных в своей профессиональной деятельности. Это торговые предприятия, предприятия сферы обслуживания (рестораны, отели), а также компании IT – сектора.

Число утечек данных через мобильные устройства, флешки и электронную почту существенно не увеличилось. Увеличение произошло в основном за счет сетевых подключений и, следовательно, основными объектами нападений являются базы данных, в том числе сервера, где хранятся архивные копии баз данных. В связи с этим большое значение приобретают средства защиты содержимого базы данных, в частности систем шифрования баз данных, которые могут быть как частью программного обеспечения (ПО) самой СУБД, так и ПО сторонних разработчиков. В большинстве подобных систем необходимо обеспечивать режим шифрования "на лету", то есть совершенно прозрачно для пользователя (Transparent Database Encryption, TDE).

Общие характеристики режимов шифрования некоторых наиболее распространенных баз данных приведены в таблице 1.

Таблица 1

Функции шифрования в распространенных базах данных.

База данных	Способ шифрования	Защищаемые сущности	Режим TDE	Тип лицензии	Влияние режима шифрования на производительность
Oracle	Симметричный, AES (128 бит)	Столбцы	Есть	Проприетарная	Небольшое
MSSQL	Цифровой сертификат, симметричный и ассиметричный алгоритмы	Файлы базы данных, журнал транзакций, страницы данных	Есть	Проприетарная	Существенное
1C	RSA (внешнее ПО, в том числе используя API платформы .NET)	Поля данных	Нет	Проприетарная	Сильное, в связи с ограничениями платформы
Firebird	Нет	Нет	Нет	IPL (InterBase Public License) и IDPL (Initial Developer's Public License)	Нет
SQLite	ПО сторонних разработчиков, встроенные функции	Поля данных	Есть	Общественная	Существенное
MySQL	AES, DES	Поля данных, файл базы данных	Нет	GPL	Небольшое

Из приведенной таблицы можно сделать вывод, что в современных базах данных с защитой путем шифрования в режиме TDE, дело обстоит совершенно по-разному и это не зависит от типа лицензии. В гораздо большей степени это зависит от доступности соответствующего криптографического API и желания разработчиков внедрять в программное обеспечение СУБД соответствующий режим функционирования. Кроме прочего, прослеживается три подхода к защите информации, содержащейся в базе данных.

1. Защита отдельных сущностей СУБД на основе встроенных функций шифрования.
2. Защита всего файла СУБД в режиме TDE встроенными средствами шифрования.
3. Использование ПО сторонних разработчиков для организации как режима TDE, так и для защиты на уровне отдельных сущностей.

На данный момент известно, что у шифрованных баз данных в режиме TDE имеется два существенных недостатка.

– Архивирование зашифрованных баз данных неэффективно
– Режим TDE вызывает снижение быстродействия примерно на 10 – 15%.

Очевидно, что с первым недостатком ничего поделать нельзя, поскольку алгоритмы таких традиционных архиваторов как PKZip, LHA, RAR и т.д., работают на основе использования статистической неоднородности двоичного или бинарного содержимого файла. Например, в двоичном представлении данных они выбрасывают цепочки повторяющихся ноликов или единичек.

Если мы говорим об алгоритмах шифрования, то их работа направлена как раз на то, чтобы обеспечить высокую статистическую однородность содержимого файла. Следовательно, алгоритм сжатия архиватора на таком файле становится неэффективен, и использовать его незачем.

Что касается второго недостатка, то тут интересно проверить, является ли такое свойство зависящим от реализации программного кода конкретной СУБД, или оптимизированная реализация сторонних разработчиков тоже дает примерно такую же задержку по времени, как и встроенные реализации? Для экспериментов была собрана тестовая система на основе виртуальной машины VMware player v6.06 и OS Ubuntu v14.02. Сами замеры времени производились с помощью небольшого скрипта, который фиксировал задержки по времени в микросекундах, которые проявлялись при вставке 1000 записей в таблицу СУБД SQLite. Эта база данных не имеет собственного сервера, следовательно, задержки времени на передачу

данных по сети не будут оказывать на результаты замеров никакого влияния. В качестве стороннего ПО, обеспечивающего режим TDE было использовано инсталлируемое ПО проекта SQLCipher (https://www.zetetic.net/sqlcipher/). Результаты испытаний приведены в таблице 2.

Таблица 2

Задержки времени вставки и чтения записей в режиме TDE СУБД SQLite.

№ теста	Вставка записей в режиме TDE t, (микросек.)	Чтение записей в режиме TDE t, (микросек.)	Вставка записей в обычном режиме, t, (микросек.)	Чтение записей в обычном режиме, t, (микросек.)	% Задержки на запись	% Задержки на чтение
1	80499	19393	69389	18949	13,8	2,29
2	304842	19737	88736	29874	70,89	- 51,36
3	237224	18305	109877	25940	53,68	- 41,71
4	109446	71005	166312	33574	- 51,96	52,72
5	306212	22244	107155	58170	65,01	- 161,51
6	77568	17017	59137	16989	23,76	0,17
7	220640	16312	52616	16511	76,15	- 1,22
8	215070	17986	96676	17609	55,05	2,1
Среднее					38,3	- 24,82

Анализ экспериментальных данных таблицы 2 показывает, что, как и предполагалось изначально, приложение, использующие режим TDE, действительно работает медленнее.

Замедление в среднем достигает 38,3%. Однако 38,3% ~ 40% - это довольно много! Получается, что приложение, использующее SQLCipher для доступа к базе данных, работает чуть ли не в половину медленнее, чем обычное приложение.

Также немного неожиданным оказался тот факт, что в режиме чтения приложение, не использующее SQLCipher, оказалось на 24,82% ~ 25% медленнее, чем приложение, использующее эту библиотеку. Предположительно это связано с наличием механизма внутреннего кеширования, заложенного в библиотеку SQLCipher. Встраивание такого механизма внутрь библиотеки выглядит довольно разумным решением, так как огромное замедление производительности приложения (почти на 40%), необходимо хоть чем – то компенсировать, хотя бы повышением скорости чтения. Но даже при таких условиях, следует признать, что задержки достаточно велики и при проектировании высоконагруженных и хорошо защищенных систем, эти задержки следует обязательно учитывать.

СПИСОК ЛИТЕРАТУРЫ

1. Гатчин Ю. А, Коробейников А.Г. Основы криптографических алгоритмов. Учебное пособие. – СПб.: СПб ИТМО, 2002.
2. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ – ОБРАЗ, 2001, - 368с.

УДК 004.056

ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ НАЗЕМНОГО ГОРОДСКОГО ПАССАЖИРСКОГО ТРАНСПОРТА

Ильченко Лидия Михайловна, Зайцев Святослав Игоревич
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
Российская Федерация, 197101, Санкт-Петербург, Кронверкский пр., д. 49
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Российская Федерация, 198035, г. Санкт-Петербург, ул. Двинская, 5/7
email: Lidiya9510@yandex.ru, Sunilink@yandex.ru

Аннотация: В данной работе рассматриваются особенности построения системы защиты информации в автоматизированных системах управления наземного городского пассажирского транспорта.

Ключевые слова: *информационная безопасность, интеллектуальная дорожно-транспортная система, угрозы безопасности, средства защиты информации, автоматизированная система управления наземным городским пассажирским транспортом.*

PARTICULAR QUALITIES OF CONSTRUCTION OF INFORMATION PROTECTION SYSTEM IN INTELLECTUAL SYSTEMS OF GROUND CITY PASSENGER TRANSPORT

Ilchenko Lydia, Zaytsev Svyatoslav
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics
197101, Russia, St. Petersburg, 49 Kronverksky Pr.
Admiral Makarov State University of Maritime and Inland Shipping
198035, Russia, St. Petersburg, Dvinskaya st., 5/7
email: Lidiya9510@yandex.ru, Sunilink@yandex.ru

Abstract: In this paper we consider the construction of a system for protecting information in the intellectual systems of ground city passenger transport.

Keywords: *information security, intellectual road and transport system, security threats, data protection facilities, intellectual systems of ground city passenger transport.*

Введение. На сегодняшний день транспортная система является неотъемлемой частью инфраструктуры любого развитого государства. На территории России насчитывается более 1 396 000 км сети автодорог общего пользования. В связи с чем возникает ряд необходимостей, основной из которых является максимизация качества функционирования дорожно-транспортной системы, которая особенно остро ощущающихся в больших городах, где поток транспортных средств намного превышает пропускную способность дорожной инфраструктуры.

Существует два направления решения этой задачи: использование технологий автоматизированного управления транспортной системой путем использования информационных технологий; и модернизация участков дороги.

Во время проектирования автономной информационной системы наземного транспорта, решающей отдельные задачи, появилась обоснованная необходимость в создании общей государственной стратегии развития, контроля и регламентации единого программно-аппаратного комплекса, объединяющего деятельность всех органов власти, действующих в сфере транспортной инфраструктуры государства. [6]

Система, основной функцией которой стало объединение в единый технологический и технический комплекс множество отдельных подсистем дорожного движения, получила название «Интеллектуальная дорожно-транспортная система» (далее – ИТС). [5]

Одной из ведущих подсистем ИТС является система автоматизированного управления наземным городским пассажирским транспортом (АСУ НГПТ).

Стратегическую цель создания АСУ НГПТ составляет удовлетворение спроса на пассажирский транспорт. Результатом функционирования АСУ НГПТ является описание целевых направлений построения интеллектуальной дорожно-транспортной системы:

– мониторинг дорожной ситуации;
– организация транспортного потока и пр.

В рамках управления системой городского наземного транспорта рассматривается:

– управление непосредственно самим транспортом (автобусы, трамваи, и пр), частью пригородных перевозок (связь города с вокзалами и аэропортами);
– определение местоположения транспортных средств в режиме реального времени на базе технологий ГЛОНАСС/GPS;
– система информирования пассажиров на остановочных пунктах и в транспортных средствах;
– система учета пассажиров;
– система диспетчерского управления;
– система безопасности;
– дуальный канал связи транспортных средств с диспетчерскими центрами;

Основными функциями автоматизированной системы управления наземным городским пассажирским транспортом являются:

1. Диспетчеризация:
– журналирование выполненных работ;
– управление движением в режиме реального времени;
– контроль за соблюдением расписание.[3]
2. Планирование:
– составление паспорта маршрута;
– мониторинг пассажиропотока;
– журналирование и аудит работы перевозчиков.
3. Безопасность:
– видеоконтроль;
– реагирование в случае поступления сигналов бедствия;
– информирование о чрезвычайных происшествиях. [2] [4]

Основные угрозы безопасности информации АСУ наземного городского пассажирского транспорта представлены в таблице 1. [8]

Актуальными являются угрозы: 1.1, 1.3, 1.4, 2.1-2.4, 3.1, 3.3. Для автоматизированной системы управления главными векторами обеспечения защиты является доступность и целостность. Конфиденциальность данных обеспечивается по необходимости. [9]

В качестве источников внутренних отказов автоматизированной системы управления выступают:

– непреднамеренные ошибки эксплуатации системы;
– системные ошибки из-за превышение допустимых объемов обрабатываемых данных;
– отказ программного и (или) аппаратного обеспечения;
– потеря информации и (или) физических носителей информации. [1]

Таблица 1

Потенциальные угрозы безопасности информации автоматизированной системы наземного городского пассажирского транспорта

Способы нанесения ущерба	Объекты воздействия			
	Оборудование	Программы	Данные	Персонал
Нарушение конфиденциальности данных	1.1 Хищение физических носителей информации, подключение к сетям линии связи, несанкционированное использование ресурсов	1.2 Копирование данных, перехват.	1.3 Хищение, копирование, перехват.	1.4 Разглашение сведений о защите АСУ, халатность сотрудника.
Нарушение целостности данных	2.1 Подключение, модификация, изменение режимов работы, несанкционированное использование ресурсов.	2.2 Внедрение аппаратных закладок, вирусов и «троянов».	2.3 Искажение, модификация	2.4 Человеческий фактор
Нарушение работоспособности АСУ	3.1 Изменение режимов функционирования, выход из строя, хищение, разрушение.	3.2 Искажение, подмена, удаление	3.3 Искажение, удаление, ложные данные.	3.4 Ошибки сотрудника

Для рассматриваемой системы класс защищенности определяется в соответствии с приказом ФСТЭК России от 14 марта 2014 г. № 31, и напрямую зависит от уровня значимости обрабатываемых данных, который прямо пропорционален возможному ущербу для каждого из свойств безопасности информации (целостности, доступности, конфиденциальности).

Степень возможного ущерба для АСУ наземного городского пассажирского транспорта:

– Для целостности – низкая.
– Для доступности – низкая.
– Для конфиденциальности – низкая.

Исходя из вышеуказанных данных уровень значимости системы соответствует третьему (УЗ-3), а класс защищенности, в соответствии с таблицей в п.3 Приложения №1 приказа ФСТЭК России от 14 марта 2014 г. № 31, соответствует третьему классу (К3).

Обеспечение защиты информации в АСУ наземного городского пассажирского транспорта достигается за счет комплексного подхода к организации системы защиты данных. Базовый набор мер представлен в приложении №2 приказа ФСТЭК России от 14 марта 2014 г. №31. Адаптивный набор мер формируется в результате оценки угроз информационной безопасности на базе составленной модели угроз.

Как минимум, меры защиты должны обеспечивать минимизацию, либо полную ликвидацию угроз безопасности информации, источником которых является нарушитель с низким потенциалом.

В системе защиты должны быть реализованы следующие группы мер:

– идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ);
– управление доступом субъектов доступа к объектам доступа (УПД);
– ограничение программной среды (ОПС);
– защита машинных носителей информации (ЗНИ);
– регистрация событий безопасности (РСБ);
– антивирусная защита (АВЗ);
– обнаружение (предотвращение) вторжений (СОВ);
– контроль (анализ) защищенности информации (АНЗ);
– целостность автоматизированной системы управления и информации (ОЦЛ);
– доступность технических средств и информации (ОДТ);
– защита среды виртуализации (ЗСВ);
– защита технических средств и оборудования (ЗТС);
– защита автоматизированной системы и ее компонентов (ЗИС);
– безопасная разработку прикладного и специального программного обеспечения (ОБР);
– управление обновлениями программного обеспечения (ОПО);
– планирование мероприятий по обеспечению защиты информации (ПЛН);
– обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС);
– информирование и обучение персонала (ИПО);
– анализ угроз безопасности информации и рисков от их реализации (УБИ);
– выявление инцидентов и реагирование на них (управление инцидентами) (ИНЦ);
– управление конфигурацией автоматизированной системы управления и ее системы защиты (УКФ).

Исходя из анализа Реестра сертифицированных ФСТЭК России средств защиты информации и практики их применения, можно составить перечень необходимых и достаточных средств защиты:

– СЗИ от несанкционированного доступа (СЗИ от НСД);
– средств индивидуального межсетевого экранирования (МЭ);
– средств обнаружения вторжений (СОВ);

– средств защиты виртуализации (СЗВ);
– средств резервирования (резерв.коп);
– средств антивирусной защиты информации (АВЗ).

А также средства криптографической защиты информации, сертифицированные Федеральной службой безопасности РФ (ФСБ России).

Третий класс защищенности предъявляет следующие требования:
– средства вычислительной техники не ниже 5 класса;
– СЗИ не ниже 6 класса. [7]

Общий перечень средств защиты информации и их функционал представлен в таблице 2.

Таблица 2.

Реализация функциональных комплексов

№ п/п	Усл. обознач.	СЗИ от НСД	СЗВ	МЭ + IDS	АВЗ	Резерв. Коп.	СКЗИ	Орг. меры
1.	ИАФ	+	+					
2.	УПД	+	+	+				
3.	ОПС	+	+					
4.	ЗНИ							+
5.	РСБ	+	+	+	+		+	
6.	АВЗ				+			+
7.	СОВ			+				
8.	АНЗ	+		+				+
9.	ОЦЛ	+	+	+	+	+	+	
10.	ОДТ					+		+
11.	ЗСВ		+					+
12.	ЗТС							+
13.	ЗИС	+		+	+	+	+	
14.	ОБР							+
15.	ОПО	+			+			+
16.	ПЛН							+
17.	ДНС					+		+
18.	ИПО							+
19.	УБИ							+
20.	ИНЦ	+	+	+	+		+	+
21.	УКФ							+

Выводы. При проектировании системы защиты необходимо учитывать все особенности АСУ НГПТ, а также необходимо учитывать актуальные угрозы безопасности и специфику обрабатываемых данных, акцентируя внимание на доступности и целостности обрабатываемой информации, и лишь по необходимости на конфиденциальности. Кроме этого, необходимо учитывать требования нормативно-правовых актов, регламентирующих данную категорию автоматизированных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. – М.: Горячая линия – Телеком, 2014. – 594 с.
2. Жанказиев. С.В. Интеллектуальные транспортные системы: учеб. пособие / – М.: МАДИ, 2016. – 120 с.
3. Ивченко Б.П., Мартыщенко Л.А., Монастырский М.Л. Теоретические основы информационно-статистического анализа сложных систем. – СПб.: Лань, 1997. – 320 с.
4. Коноплянко, В.И. Организация и безопасность дорожного движения / В.И. Коноплянко. – М.: Транспорт, 1991. – 183 с.
5. Косолапов, А.В. Повышение эффективности информационного обеспечения участников дорожного движения в городах: дис. …канд. техн. наук. – М., 1992.
6. Опыт создания и эксплуатации интеллектуальных транспортных систем: Информационный сборник / Федеральное дорожное агентство Министерства транспорта Российской Федерации. – М.: ООО «Принт Форс Паблишинг», 2009. – 287 с.
7. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении требований 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». – 42 с.
8. Руководящий документ «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры», от 18 мая 2007 года, ФСТЭК России.
9. Руководящий документ «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры», от 18 мая 2007 года, ФСТЭК России.

УДК 004.056

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. ФИШИНГ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ ЕМУ

Ильченко Лидия Михайловна, Уваров Роман Валерьевич, Зайцев Святослав Игоревич
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
Россия, 197101, Санкт-Петербург, Кронверкский пр., д. 49
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Российская Федерация, 198035, г. Санкт-Петербург, ул. Двинская, 5/7
email: Lidiya9510@yandex.ru, Sunilink@yandex.ru

Аннотация: В данной работе рассматриваются такие методы социальной инженерии, как фишинг, вишинг и спуфинг, а также методы противодействия им.

Ключевые слова: *социальная инженерия, фишинг, спуфинг, TCP/IP, UDP вишинг.*

SOCIAL ENGINEERING. PHISHING AND METHODS OF COUNTERING IT

Ilchenko Lydia, Uvarov Roman, Zaytsev Svyatoslav
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics
197101, Russia, St. Petersburg, 49 Kronverksky Pr.
Admiral Makarov State University of Maritime and Inland Shipping
198035, Russia, St. Petersburg, Dvinskaya st., 5/7
email: Lidiya9510@yandex.ru, Sunilink@yandex.ru

Abstract: In this paper we consider such methods of social engineering as phishing, wishing and spoofing, as well as methods of countering them.

Keywords: *social engineering, phishing, spoofing, TCP / IP, UDP vishing.*

Введение. Существует множество векторов потенциальной атаки, рассматриваемых в рамках информационной безопасности, среди них особую популярность имеют технические каналы утечки информации: вибро-акустические, акустоэлектрические, оптические каналы, утечки по каналам ПЭМИН и др. [1] В связи с чем постоянно развиваются средства противодействия потенциальным атакам. На сегодняшний день, обойти средства криптографической защиты информации, безупречные протоколы безопасности, средства физической защиты и пр. фактически невозможно, однако, руководители и специалисты по защите информации часто пренебрегают угрозами со стороны инсайдеров. [2]

Если верить статистике, число утечек информации ограниченного доступа по вине внутреннего нарушителя в 2016 году уменьшилось по сравнению с 2015 и 2014 и составляет 61,8%, однако, это говорит о том, что на долю утечек по вине персонала все еще приходится более половины всех инцидентов. В России эта цифра более внушительная и составляет 86,7% от общей доли утечек на 2016 год. Визуально данные представлены на рисунке 1.

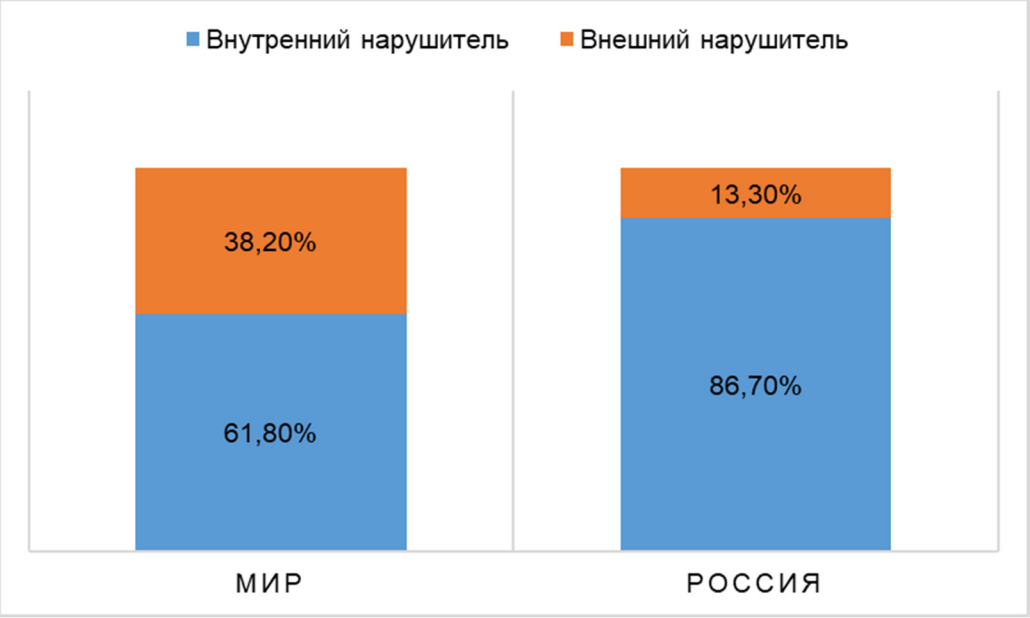


Рис. 2 Распределение утечек информации Россия – Мир.

Данные статистических исследований говорят о низком уровне культуры информационной безопасности в нашей стране. То есть сотрудники, имеющие доступ к конфиденциальным данным,

имеют свойство «забывать», что результаты их работы, а также данные, к которым они имеют доступ в соответствии со своими должностными обязанностями, являются информацией ограниченного доступа целиком и полностью принадлежат работодателю. Другой стороной данной проблемы является злоупотребление сотрудниками доступом к имеющимся у них сведениям, в том числе к персональным данным клиентов и контрагентов работодателя. [3]

Действия внутреннего злоумышленника можно разделить на умышленные и неумышленные действия, имеющие негативный характер.

Доля утечек информации по вине сотрудников сокращается в течение последних четырех лет в мире, [4] однако, это скорее связано с увеличением числа атак внешнего нарушителя, поскольку невозможно добиться сокращения инцидентов халатного или злоумышленного отношения к конфиденциальным данным одним лишь внедрением технических средств защиты информации. [5]

Социальная инженерия. На сегодняшний день на первый план выходит не новый, но редко рассматриваемый источник угроз – социальная инженерия.

Под социальной инженерией здесь и далее будет пониматься инструмент внешнего нарушителя, посредством которого реализуется атака на системы с использованием человеческого фактора, направленный на нарушение конфиденциальности, целостности и (или) доступности информационных ресурсов.

Любую атаку социального инженера условно можно разделить на ряд этапов, представленных на рисунке 2.

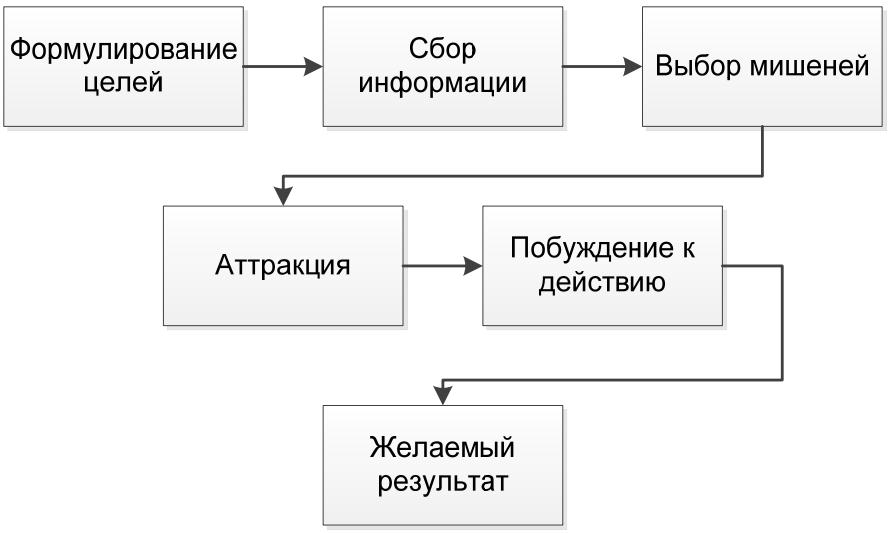


Рис. 3 Основная схема воздействия в социальной инженерии.

Однако, несмотря на одинаковую систему реализации атаки, способы, применяемые в социальной инженерии во многом различаются, среди них особое место занимает Фишинг.

Целевой фишинг – техника в социальной инженерии, направленная на получение сведений конфиденциального характера с применением средств электронной коммуникации, и выступая от другого физического или юридического лица. [6]

Основным различием целевого и массового фишинга является то, что при целевом жертвами становятся сотрудники какой-то конкретной, заранее выбранной организации, либо заранее намеченное физическое лицо, в то же время при массовом фишинге жертвами становятся случайные пользователи средств электронной коммуникации. [7]

Чаще всего фишинг реализовывается посредством электронной почты, непосредственно само письмо содержит в себе вредоносное вложение либо ссылку на фальшивый web-ресурс, содержащий форму с требованием ввести конфиденциальную информацию. Распознать фишинговую атаку бывает проблематично по причине постоянного совершенствования техник. Тем не менее для большинства фишинговых писем характерен ряд признаков:

– сообщение имеет экстренный характер. Это позволяет воздействовать на эмоции пользователя, имитируя стрессовую ситуацию;

– сообщение содержит запрос личных сведений. Это один из самых надежных признаков фишингового письма, так как во многих компаниях запрещено передавать информацию конфиденциального характера по незащищенным каналам связи, и персональные данные в том числе;

– сообщение содержит поддельные URL-адреса, отличающийся от оригинального одним или несколькими символами;

– сообщение содержит изображение в теле письма. Изображение представляет собой гиперссылку на запрещенный ресурс, это необходимо для обхода фильтров «антиспама»;

– сообщение содержит нереалистичные обещания. Примером могут выступать Нигерийские письма, получившие свое название в честь страны, в которой впервые получили массовое распространение и являются примером массового фишинга; [8]

– сообщение содержит вложение, в роли которого может выступать вредоносное программное обеспечение. Примечательно то, что расширение вложения может быть скрыто или искусственно изменено, а иконка соответствовать любому неисполняемому файлу, расширение которого указано. Кроме этого, к файлу может быть присоединен ярлык, содержащий настоящее расширение файла. Также вложение может использовать технологию RTLO или RLO (Right-to-Left) для зеркального отображения символов в названии файла. Существует множество других способов изменить вложенный файл, выше перечислена лишь часть из них.

Также фишеры часто использовали эксплоиты, которые могут предоставить доступ уязвимым к процессам и приложениям, а также ко всей операционной системе. Данные угрозы актуальны практически для всех операционных систем, включая Windows, Linux, IOS, MacOS, Android. Многие современные антивирусы снабжены системой защиты от экслоитов, однако пользователи зачатую сами пренебрегают предупреждениями со стороны антивирусных программ. Если они не будут раскрыты, у злоумышленника будет доступ к необходимым ему ресурсам неограниченное время.

По данным на 2013 год в 94% фишинговые письма содержат вредоносные вложения, и только в 6% случаев содержат вредоносные ссылки. [9]

Условно к разновидности фишинга можно отнести атаки вида спуфинг

Спуфинг – вид атаки, реализованной путем подмены адреса отправителя, либо передаваемых пакетов с целью обмана системы безопасности. В зависимости от целей, спуфинг может быть локальным и сетевым. При локальном атака направлена на операционную систему, сетевой спуфиг же направлен на информационную систему в целом.

Одним из основных видов спуфинга являются атаки на транспортный уровень, в частности на протоколы TCP/IP, UDP:

– NetBIOS/NBNS spoofing – метод, актуальный для ОС Windows, реализовывается во время резолвинга сетевого имени путем подмены DNS сервера на ложный. Если запрос к серверу оказался безуспешным, то операционная система попытается реализовать резолвинг с помощью NetBIOS. А злоумышленнику достаточно выдать себя за SOMEPC, во время широковещательного запроса.

– IP spoofing – атака, реализующаяся с помощью подмены IP-адреса отправителя с целью вызова ответных пакетов на ложный адрес. [10] На этом методе спуфинга построен ряд DoS-атак. Необходимо отметить, что наиболее подвержен атакам этого уровня протокол UDP, так как не имеет механизмов противодействия им. Для защиты от спуфинга IP – адреса является отправка ответного пакета на адрес отправителя, обычно злоумышленником используется недействительный (случайный) адрес, вследствие чего ответ не придет. [11]

– ARP спуфинг – вид атак в Ethernet сетях, направленный на перехват трафика между отдельными хостами, расположенными в пределах одного широковещательного домена. Базируется на уязвимостях протокола ARP и реализовывается путем подмены mac-адреса. Современные фаерволы способны распознавать данный вид атак. А также минимизировать возможность реализации данной угрозы способно использование arp-таблиц на ключевых частях сети.

– DNS Cache Poisoning (DNS-спуфинг) – атаки, направленные на изменение данных кэша доменных имен. Данный вид атак может быть предотвращен на стороне сервера путем уменьшения степени доверия сторонним данным, а также путем игнорирования любых DNS-записей, не относящихся изначальному запросу. [12].

Кроме этого, к фишинговым категориям спуфинга относится подмена e-mail адреса отправителя на ложный. Чаще всего применяется в массовом фишинге, и на сегодняшний день большинство почтовых сервисов оборудовано средствами «антиспама», что позволило минимизировать угрозу со стороны данной категории атак. [13]

Также известны случаи спуфинга номеров в VoIP-сетях, [14] номеров в SMS-сообщениях и подмены номеров в голосовой почте.[15]

Многие направления спуфинга является полноценной самостоятельной атакой, например GPS спуфинг – атака, направленная на GPS-приемники и реализуется путем использование более мощного передатчика, [16] и Referrer spoofing — подмена реферера. [17]

Вишигн – метод фишинговых атак через телефонные коммуникации. Злоумышленник совершает телефонный звонок жертве под видом другого физического, юридического или должностного лица, с которым у жертвы установлены доверительные отношения. Самым надежным способом защиты является не сообщать информацию ограниченного доступа во время телефонных разговоров. [18]

Таким образом, получение информации от пользователей возможно не только путем сложных технологических манипуляций, но путем использования банальной невнимательности или халатности субъектов. Что побуждает руководителей и сотрудников службы все большее внимание уделять человеческому фактору, ведь методы социальной инженерии работают везде, где хоть на одном этапе обработки информации присутствует человек.

СПИСОК ЛИТЕРАТУРЫ

1. Громыко И. А. Общая парадигма защиты информации: проблемы защиты информации в аспектах математического моделирования: монография / И. А. Громыко. — Х.: ХНУ имени В. Н. Каразина. 2014. — 216с.
2. Гридин А. Краткое введение в социальную инженерию, 2010. URL: https://habrahabr.ru/post/83415/ (дата обращения 15.09.2017).
3. Глобальное исследование утечек конфиденциальной информации в 2016 году // Аналитический центр InfoWatch, 2017. URL: https://www.infowatch.ru/report2016 (дата обращения 16.09.2017).
4. Утечки данных организаций в результате умышленных или неосторожных действий внутреннего нарушителя. Сравнительное исследование 2013-2015 гг. // Аналитический центр InfoWatch, 2017. URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_052016.pdf?rel=1 (дата обращения 16.09.2017).
5. Глобальное исследование утечек конфиденциальной информации в 2014 году // Аналитический центр InfoWatch, 2017. URL: http://ibsmol.ru/InfoWatch_global_report_2014.pdf (дата обращения 16.09.2017).
6. Кузнецов, М. В. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. — Санкт-Петербург: БХВ-Петербург, 2007. — 368 с.
7. Интернет-мошенничество фишинг: механизм, виды и способы противодействия - 2015. URL: https://www.exocur.ru/internet-moshennichestvo-fishing-mehanizm-vidyi-i-sposobyi-protivodeystviya/ (дата обращения 15.09.2017).
8. Кондураке В. П. Защита от фишинг-атак, 2009. URL: http://www.securrity.ru/articles/20-zashhita-ot-fishing-atak.html (дата обращения 17.09.2017).
9. Димов И. Фишинговые методы: сходства, различия и тенденции. Часть вторая: целевой фишинг – 2013 // URL: http://www.securitylab.ru/analytics/440663.php (дата обращения 14.09.2017).
10. Морозов А. В., Шахов В. Г. Анализ атак на беспроводные компьютерные интерфейсы // ОНВ. 2012. №3 (113). URL: http://cyberleninka.ru/article/n/analiz-atak-na-besprovodnye-kompyuternye-interfeysy (дата обращения: 17.09.2017).
11. Хохлов Н. С. Обзор уязвимостей Wi-Fi сигнализации в системах автоматизированного управления зданиями / Хохлов Николай Степанович, Михайлов Дмитрий Михайлович, Смирнов Александр Сергеевич // Вестник ВИ МВД России. 2014. №1. С.277-281.
12. Сапожников А. А. Наблюдение аномалий в сети // Вестник ЮУрГУ. Серия: Компьютерные технологии, управление, радиоэлектроника. 2009. №26 (159). С.62-65.
13. Облачный хостинг в Европе (vps/vds) Предотвращение спуфинга адресов и защита электронной почты при помощи SPF-записи. 2016. URL: https://www.8host.com/blog/predotvrashhenie-spufinga-adresov-i-zashhita-elektronnoj-pochty-pri-pomoshhi-spf-zapisi/ (дата обращения: 17.09.2017).
14. Johnny Gabel Hack a Voicemail Account Using SpoofApp. 2012. URL: https://computer-pranks.wonderhowto.com/how-to/hack-voicemail-account-using-spoofapp-0133304/ (дата обращения: 17.09.2017).
15. Абдеева З. Р. Проблемы безопасности электронной коммерции в сети Интернет // ПСЭ. 2012. №1. С.172-175.
16. GPS: глушилки, спуфинг и уязвимости // Блог компании Хакспейс Neuron. 2015. URL: https://habrahabr.ru/company/neuronspace/blog/254877/ (дата обращения: 17.09.2017).
17. Christopher Hadnagy Phishing Dark Waters: The Offensive and Defensive Sides of Malicious E-mails / Christopher Hadnagy, Michele Fincher – United States of America, Indiana, Indianapolis: John Wiley & Sons, Inc., 2015. 277 c.
18. Антонов И. О. Способы мошенничества с использованием платёжных карт как элемент криминалистической характеристики данного вида преступлений / Антонов Игорь Олегович, Шалимов Анатолий Николаевич // Учен. зап. Казан. ун-та. Сер. Гуманит. науки. 2013. №4. С.196-203.

УДК 001.812

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ОБУЧЕНИИ ХИМИИ

Колоколов Даниил Сергеевич
Санкт-Петербургский государственный университет,
Россия, Санкт-Петербург, Университетская наб., 7/9,
email: kolokolov.d@gmail.com

***Аннотация*:** В статье рассмотрены, как пример повышения эффективности обучения химии.

Ключевые слова: *компьютер, преподавание химии*

USE OF INFORMATION TECHNOLOGIES IN TRAINING CHEMISTRY

Daniil Kolokolov
St. Petersburg State Institute,
Russia, St. Petersburg, Universitetskaya Embankment, 7/9,,
email: kolokolov.d@gmail.com

Abstract: The article is considered as an example of increasing the effectiveness of teaching chemistry.

Keywords*: computer, teaching chemistry*

В настоящее время в Российском образовании идет процесс перехода к стандартам нового поколения, при этом определяется роль информатизации и подтверждается факт вхождения человечества в эпоху глобализации информационных процессов. Только за последнее десятилетие повсеместно стали использоваться новые информационные технологии: Интернет, мобильная связь, цифровые технологии. При этом разрабатываемый образовательный стандарт должен стать ответом на вызов современного глобального непрерывно меняющегося мира. Все новинки технологического прогресса с особым восторгом встречают именно дети. Поэтому очень важно использовать любознательность и высокую познавательную активность учащихся для целенаправленного развития их личности. Именно на уроках под руководством педагога школьники могут научиться использовать компьютерные технологии в образовательных целях, овладеть способами получения информации для

решения учебных, а впоследствии и более широкого круга задач, приобрести навыки, обеспечивающие возможность продолжать образование в течение всей жизни. Однако использование в настоящее время компьютерных технологий в процессе обучения, в том числе химии, скорее исключение, чем правило. Кроме того, надо признать, что за последние годы наблюдается снижение интереса учащихся к естествознанию вообще и к химии в частности, что представляет собой одну из проблем школьного образования. Причины негативных изменений, появившихся в обучении химии за последние годы, связаны с нарастанием сложности программного материала и сокращением учебного времени на его усвоение, а также недостаточным обеспечением учебного процесса специальным оборудованием. На современном этапе развития страны осуществляется модернизация среднего образования, в рамках которой и педагогами нашей школы активно ведутся поиски новых подходов, средств и методов обучения. Цель педагогической деятельности ориентирована на повышение качества образования через внедрение и интеграцию современных образовательных технологий, при этом информационным отводится ведущее место.

Для достижения поставленной цели в области преподавания химии определены следующие задачи: рассмотреть основные принципы и методические приемы построения компьютеризированных методик обучения химии; адаптировать применение информационных компьютерных технологий к условиям лечебно-образовательного процесса; создать условия для формирования ключевых компетенций обучающихся с акцентом на информационные; содействовать созданию здоровье сберегающей среды обучения. Реализация обозначенных цели и задач в нашем образовательном учреждении возможна благодаря наличию соответствующей материальной базы, созданной в рамках программы компьютеризации общеобразовательных учреждений. Для реализации нового подхода к преподаванию с применением информационных технологий необходимо знать возможности, предоставляемые компьютером для усовершенствования учебного процесса на каждом этапе урока. Так, на этапе подготовки к уроку компьютер предоставляет возможности: создавать компьютерные модели конспекта урока, темы, курса в целом; максимально целесообразно располагать материал; обеспечивать основной материал дополнительной информацией; подбирать и систематизировать материал с учетом особенностей класса и отдельных учащихся. На этапе проведения уроков компьютер позволяет: экономить время; красочно оформлять материал; повышать эмоциональную, эстетическую, научную убедительность преподавания; оптимизировать процесс усвоения знаний, воздействуя на различные анализаторы; индивидуализировать обучение; концентрировать внимание на важнейшей проблеме урока; в любой момент возвращаться к уже знакомому материалу; самостоятельно использовать учебный материал обучающимися. На этапе методической проработки процесса обучения у учителя появляются дополнительные возможности: аккумулировать совместные усилия учителей; развивать, модернизировать, корректировать электронные материалы; систематически накапливать материал; повышать мотивацию преподавания и обучения. Кроме того, компьютерная техника применяется и как средство контроля усвоения знаний учащимися, значительно расширяет доступ к источникам информации, дает возможность получения обратной связи. Для организации работы учителем могут быть применены различные модели использования компьютера на уроках. Они подразделяются на методологические и организационные. В практике преподавания химии мною применяются различные формы информационного сопровождения. Наиболее простым и эффективным приемом является использование готовых программных продуктов, которые обладают большим потенциалом и позволяют варьировать способы их применения исходя из содержательных и организационных особенностей образовательного процесса. Использование изобразительных средств (анимация, видеофрагмент, динамические рисунки, звук) значительно расширят возможности обучения, делает содержание учебного материала более наглядным, понятным, занимательным. Например, раздел “Химия на службе человека” позволяет приблизить получаемые сведения к реальности. Компьютерное моделирование оказывается незаменимым при изучении химических процессов, непосредственное наблюдение за которыми нереально или затруднено. Таким примером может служить рассмотрение процесса электролитической диссоциации, изучение реакций ионного обмена, где наглядно, в движении представлены процессы, происходящие в растворе между ионами. Компьютерные технологии дают возможность демонстрировать реакции с взрывчатыми или ядовитыми веществами, редкими или дорогостоящими реактивами, процессы, протекающие слишком быстро или медленно, что невозможно в школьных условиях. Например, при изучении электрохимической коррозии учащиеся в течение нескольких минут могут рассмотреть механизм этого крайне медленно протекающего процесса. Преподавание химии специфично по сравнению с другими дисциплинами, поскольку предполагает проведение практических работ. И в этом случае компьютер стал эффективным помощником учителя. Конечно, проведение опытов в лаборатории обладает неоспоримыми преимуществами, но при изучении токсичных веществ, например, галогенов, виртуальный мир дает возможность проводить химический эксперимент без риска для здоровья. Если в кабинете отсутствует необходимое оборудование, использование компьютера дает возможность компенсировать этот недостаток. Привлечение обучающих игр позволяет сделать процесс усвоения химической информации эмоционально насыщенным, а значит более продуктивным. Например, для

формирования умений различать принадлежность веществ к определенному классу можно использовать игру “Химическая защита” <Рисунок 7>. Обучающие игры можно применять и для внеклассной работы по предмету. Учитывая специфику санаторной школы и тот факт, что 80% обучающихся имеют домашний компьютер, появилась возможность использовать электронные носители информации в процессе индивидуальной работы с детьми, имеющими трудности в обучении, временно обучающимися на дому, и с одаренными детьми. Еще одним аргументом в пользу применения информационных технологий является возможность быстрого и эффективного контроля знаний учащихся. Большая часть электронных учебников содержит упражнения – тренажеры, задачи с решениями, тестовые задания. Отдельные программные продукты содержат электронный журнал, который позволяет фиксировать уровень знаний учащегося по каждой теме курса (учитывается не только отметка и число попыток решения, но и затраченное время на выполнение заданий). Система оценки результатов дает возможность определить рейтинг учащегося по каждой теме, проследить динамику успеваемости и скорректировать учебный процесс в соответствии с показанными результатами. Кроме того, использование контролирующих программ способствует формированию адекватной самооценки у учащихся. Несмотря на ряд преимуществ готовых программных продуктов, информация на некоторых из них излагается очень сухо, встречаются ошибки принципиального характера, некоторые задания чрезвычайно трудны для школьника. Поэтому возникает потребность в создании собственных информационных продуктов. Компьютерные презентации – эффективный метод представления и изучения любого материала.

Применение слайд – фильмов (Power Point) обеспечивает более высокий уровень проведения урока, его информационную насыщенность, динамичность, наглядность. При создании презентации использую данные электронных учебников, информацию сети Интернет, размещаю на слайдах необходимые формулы, схемы химических опытов в соответствии с последовательностью изучения материала на уроке. В целях своевременного устранения пробелов в знаниях и закрепления наиболее важных вопросов темы на последнем слайде помещаю контрольные задания. Если учащиеся не могут ответить, на какой - либо вопрос, то есть возможность вернуть слайд, содержащий сведения для правильного ответа. Таким образом, осуществляется разбор материала, вызвавшего затруднения. Наличие большого набора информационных объектов в презентации дает учителю возможность представить изучаемый объект или процесс во всем многообразии его проявлений и свойств, а также более четко и точно определить его место и значение в системе научных знаний об окружающем нас мире. Очень важно, что использование информационных технологий органично вписывается в структуру любого урока, дает возможность стимулировать поисковую деятельность учащихся на современном, качественно ином уровне, а также формировать учебную мотивацию и ключевые компетенции обучающихся.

СПИСОК ЛИТЕРАТУРЫ

1. Курдюмова Т. Н. Компьютерная технология обучения химии: достоинства и недостатки.// Химия в школе, 2002. - №8, с. 35 – 37.
2. Курдюмова Т. Н., Курдюмов Г. М. Компьютерные обучающие игры. //Химия. Методика преподавания, 2004. - №1, с. 75 – 77.

УДК 004.056.5

РЕАЛИЗАЦИЯ МЕТОДА КАНАЛЬНОЙ СТЕГАНОГРАФИИ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛА ICMP

Костырин Алексей Сергеевич, Красов Андрей Владимирович
Санкт-Петербургский государственный университет телекоммуникаций им.проф. М. А. Бонч-Бруевича
emails: alex.kostirin@ya.ru, krasov@inbox.ru

Аннотация: В данной работе рассматривается практическая реализация сокрытия информации в сетевом протоколе ICMP. Приведены сведения о спроектированном и написанном ПО для скрытого удаленного управления ЭВМ, представлены результаты эксперимента по удаленному управлению ЭВМ с сокрытием передачи управляющих данных в протоколе ICMP.

Ключевые слова: *Канальная стеганография, сокрытие информации, классификация видов стеганографии, защита информации, сети передачи данных*

IMPLEMENTATIONOF THE METOD OF CHANNEL STEGANOGRAPHY USING ICMP PROTOCOL

Kostyrin Alexey, Krasov Andrey
Saint-Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich
emails: alex.kostirin@ya.ru, krasov@inbox.ru

Abstract: Implementation of the method of channel steganography using ICMP Protocol. In this paper, we consider the practical realization of information hiding in the network Protocol ICMP. Provides information on designed and written for covert remote control of computers, experimental results are presented on remote management computers with concealment of transmitting control data in ICMP Protocol.

Keywords: *Channel steganography, information hiding, classification of types of steganography, data transmission network*

Стеганография - способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения). В отличие от криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования. Таким образом, стеганография потенциально обеспечивает не только безопасность, но также анонимность и конфиденциальность, которые очень важны в современном обществе[1]. Различные техники стеганографирования позволяют скрывать информацию в различных источниках – в изображениях, в тексте, в исполняемых файлах[2], а также в каналах связи.

Канальная стеганография – способ сокрытия факта передачи информации в сетях передачи данных

ПротоколICMP(Internet Control Message Protocol) – протоколстекаTCP/IP. Служит для передачи сообщений о сетевых ошибках и для обеспечения некоторых сервисных функций[3].

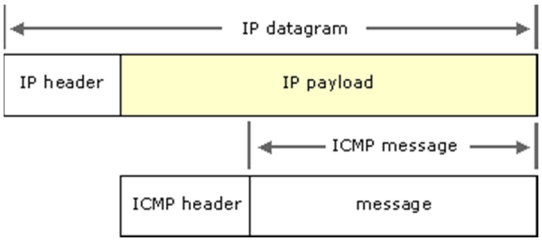


Рис. 1 – ICMP сообщение в IP пакете

ICMP принадлежит третьему (сетевому) уровню модели OSI.

ICMP сообщения инкапсулируются в пакеты IP (Рис. 1)

– ICMPпакет состоит из (Рис. 2):
– ICMPtype–тип сообщения ICMP
– Typecode–подтип сообщения ICMP
– ICMPchecksum – контрольная сумма пакета

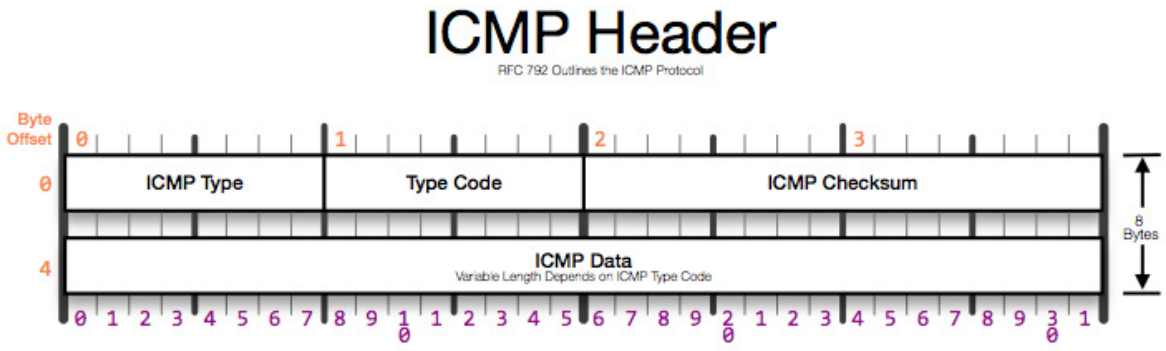


Рис. 2 – ICMPпакет

ICMP data– полезная нагрузка ICMPпакета (зависит от типа сообщения)

Часто используемые типы сообщений[4]:

– ICMP-сообщения (тип 12) генерируются при нахождении ошибок в заголовке IP-пакета (за исключением самих ICMP-пакетов, дабы не привести к бесконечно растущему потоку ICMP-сообщений об ICMP-сообщениях).

– Тип 3 - генерируются маршрутизатором при отсутствии маршрута к адресату.

– Утилита Ping, служащая для проверки возможности доставки IP-пакетов, использует ICMP-сообщения с типом 8 (эхо-запрос) и 0 (эхо-ответ).

– Утилита Traceroute, отображающая путь следования IP-пакетов, использует ICMP-сообщения с типом 11.

– ICMP-сообщения с типом 5 используются маршрутизаторами для обновления записей в таблице маршрутизации отправителя.

– ICMP-сообщения с типом 4 используются получателем (или маршрутизатором) для управления скоростью отправки сообщений отправителем.

ICMPтуннель (ICMPTX) – устанавливает скрытое соединение между двумя компьютерами, используя ICMPэхо запросы и ответы (типы 8 и 0 ICMPсообщений)[3]

ICMP туннелирование возможно потому, чтостандартRFC 792 позволяет задавать блок данных произвольной длинны для типов 0 (эхо-ответ) или 8 (эхо-запрос) ICMP-пакетов.

ICMPтуннелирование работает путем введения произвольных данных в эхо-пакет, отправленный на удаленный компьютер. Удаленный компьютер отвечает тем же самым способом, подставляя свои данные вэхо-ответ и отправляя его обратно. Клиент выполняет все коммуникации с использованием эхо-запросов, в то время как сервер может использовать как эхо-запросы, так и эхо-ответы[5].

ICMP-туннелирование может применятся для скрытия факта передачи данных и удаленного управления в обход правил брандмауэра. В зависимости от реализации программного обеспечения ICMP туннелирования, этот тип соединения также может быть классифицирован как зашифрованный канал связи между двумя компьютерами. Без применения систем DPI (DeepPacketInspection)[6], сетевые администраторы не имеют возможности обнаружить этот тип трафика в своей сети.

Цель: реализовать скрытое управление удаленным хостом путем передачи данных управления в ICMP–туннеле.

В качестве носителя информации будут применяться только тип 8 ICMPсообщений (эхо-запросы), как со стороны сервера, так и со стороны клиента. В данном случае сервер – управляемый хост, будет слушать ICMPсообщения на одном из своих интерфейсов, расшифровывать их и выполнять инструкции. Затем результат выполнения команды будет отправлен с помощью эхо-запроса клиенту. Клиент же в свою очередь принимает команды от пользователя, отправляет их удаленному серверу, упаковывая в эхо-запросы и принимает результат выполнения команды.

В качестве языка программирования выбран Python 3.6 для возможности наиболее быстрой разработки и портирования на другие платформы (однако целевой платформой является linux).

Программа не использует каких-либо дополнительных модулей, кроме стандартной библиотеки. Формирование пакетов ICMPпроисходит полностью «в ручном» режиме. Структура формируемого программой пакета:

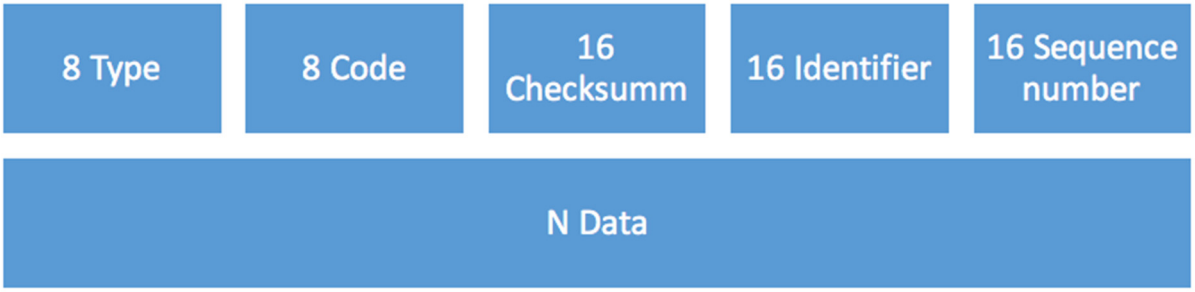


Рис.3 – Структура формируемого программой пакета

Где:

– Type – тип сообщения, 8 для эхо-запроса
– Code – подтип сообщения, 0 для эхо-запроса
– Checksum – Контрольная сумма пакета, алгоритм формирования контрольной суммы описан в стандарте RFC 1071
– Identifier – идентификатор, используется для определения пар пакетов эхо-запрос/эхо-ответ. В программе в качестве идентификатора используется текущий идентификатор процесса (PID)
– Sequencenumber–номер последовательности, используется для определения пар пакетов эхо-запрос/эхо-ответ. В программе в качестве номера последовательности используется 1.
– Data – данные, с помощью которых производится удаленное управление. Данные имеют формат “@@data” для удобства разборки полученных пакетов с использованием регулярных выражений. Данные передаются в открытом виде, шифрование данных не применяется.

Конфигурация хостов: для проведения эксперимента использовались два хоста – клиент и сервер. Клиент находился на виртуальной машине под управлением операционной системой Linux (Ubuntu16.10). Сервером выступал хост с гипервизором, операционная система – Linux (Ubuntu 16.10). В качестве гипервизора был выбран ParallelsDesktop.

Конфигурация сети: сеть была сконфигурирована таким образом, что клиент и сервер находились в одной подсети. IPадрессервера – 192.168.0.100, IPадресклиента – 192.168.0.105. Для контроля эксперимента на сервере запущенно ПО анализатор трафика – Wireshark.

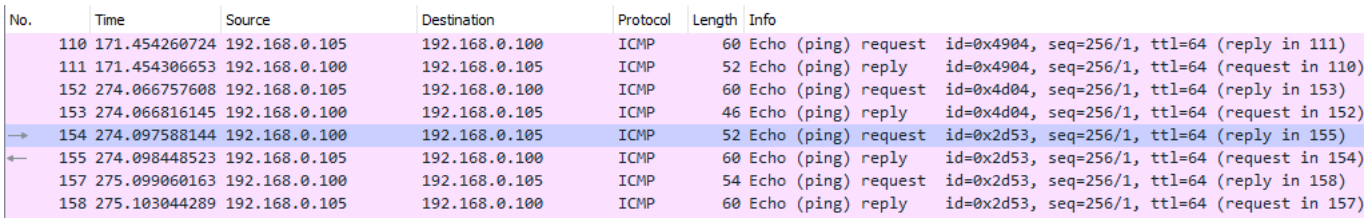
Сценарий проведения эксперимента:

– Запуск сервера и клиента с определенными согласно конфигурации сети
– Выполнение операций по управлению сервером с клиента через remoteshell
– Проверка результатов сеанса управления на сервере анализ захваченных с помощью Wireshark пакетов.
– В качестве операций по управлению сервером были выбраны:
– ls – операция листинга содержания текущего каталога
– pwd– вывод названия текущего каталога
– echotext>file.txt – выводвфайлfile.txt текста text

В результате проведения эксперимента, можем убедиться, что:

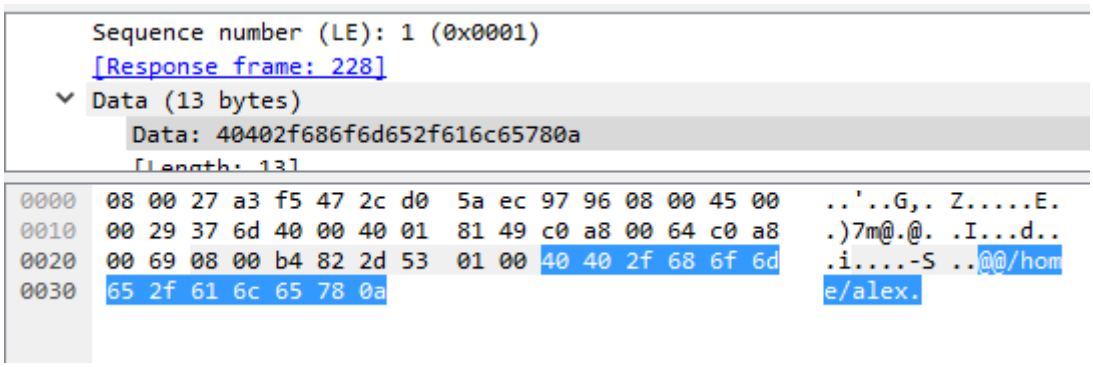
– На клиенте было отображено название и содержание текущего каталога на сервере
– Файл, созданный с помощью команды на клиенте, присутствует на сервере

Трафик управления инкапсулировался только в пакеты ICMPи данные управления передавались в открытом виде в пакетах ICMP, причем на каждый echo-requestследовал echo-reply(Рис 4, 5)



No.	Time	Source	Destination	Protocol	Length	Info
110	171.454260724	192.168.0.105	192.168.0.100	ICMP	60	Echo (ping) request id=0x4904, seq=256/1, ttl=64 (reply in 111)
111	171.454306653	192.168.0.100	192.168.0.105	ICMP	52	Echo (ping) reply id=0x4904, seq=256/1, ttl=64 (request in 110)
152	274.066757608	192.168.0.105	192.168.0.100	ICMP	60	Echo (ping) request id=0x4d04, seq=256/1, ttl=64 (reply in 153)
153	274.066816145	192.168.0.100	192.168.0.105	ICMP	46	Echo (ping) reply id=0x4d04, seq=256/1, ttl=64 (request in 152)
154	274.097588144	192.168.0.100	192.168.0.105	ICMP	52	Echo (ping) request id=0x2d53, seq=256/1, ttl=64 (reply in 155)
155	274.098448523	192.168.0.105	192.168.0.100	ICMP	60	Echo (ping) reply id=0x2d53, seq=256/1, ttl=64 (request in 154)
157	275.099060163	192.168.0.100	192.168.0.105	ICMP	54	Echo (ping) request id=0x2d53, seq=256/1, ttl=64 (reply in 158)
158	275.103044289	192.168.0.105	192.168.0.100	ICMP	60	Echo (ping) reply id=0x2d53, seq=256/1, ttl=64 (request in 157)

Рис. 4 – Перехват трафика управления в Wireshark



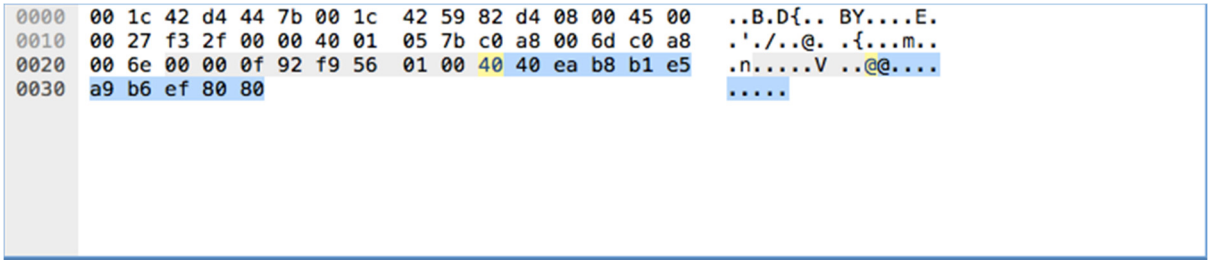
```
Sequence number (LE): 1 (0x0001)
[Response frame: 228]
Data (13 bytes)
    Data: 40402f686f6d652f616c65780a
    [Length: 13]
```

```
0000  08 00 27 a3 f5 47 2c d0  5a ec 97 96 08 00 45 00   ..'..G,. Z.....E.
0010  00 29 37 6d 40 00 40 01  81 49 c0 a8 00 64 c0 a8   .)7m@.@. .I...d..
0020  00 69 08 00 b4 82 2d 53  01 00 40 40 2f 68 6f 6d   .i....-S ..@@/hom
0030  65 2f 61 6c 65 78 0a                              e/alex.
```

Рис. 5 – Детальный разбор прихваченных ICMP пакетов

Так как данные могут быть перехвачены для ручного анализа, то было принято решение также использовать шифрование полезной нагрузки при передаче. В качестве алгоритма шифрования использован extendedtinyencryptionalgorithmc режимомCTR. Выбран он по следующим причинам:

– Компактность кода алгоритма. Клиент и сервер должны размещаться в одном руфайле
– Относительная криптоустойчивость при простоте реализации алгоритма
– Быстрота шифрования
– Режим CTRвыбран по причине отказа от блочного шифрования в пользу потокового для максимального использования пропускной способности вкладывания



```
0000  00 1c 42 d4 44 7b 00 1c  42 59 82 d4 08 00 45 00   ..B.D{.. BY....E.
0010  00 27 f3 2f 00 00 40 01  05 7b c0 a8 00 6d c0 a8   .'./..@. .{...m..
0020  00 6e 00 00 0f 92 f9 56  01 00 40 40 ea b8 b1 e5   .n.....V ..@@....
0030  a9 b6 ef 80 80                                    .....
```

Рис. 6 – Детальный разбор прихваченных *ICMP* пакетов с шифрованием

Как видно на рисунке 6, теперь вложенная в ICMP пакеты информация передается в зашифрованном виде.

Как результат данного эксперимента, можно сделать вывод, что возможность канальной стеганографии с применением протокола ICMPсоздает реальную угрозу передачи конфиденциальных данных без ведома пользователя. Возможный сценарий применения данной техники – это скрытая передача данных и управление сервером частной компании после успешной эксплуатации уязвимости в ПО и эскалации привилегий. Имеется возможность даже построить скрытую сеть поверх туннелей ICMPс использованием стека протоколов TCP/IP. Как уже было сказано, большинство современных межсетевых экранов не имеют защиты от использования ICMP-туннелирования, и обнаружение скрытой передачи информации возможно только с применением технологии DPI и тщательного контроля трафика администратором сети. Таким образом, разработка быстрых алгоритмов обнаружения ICMP-туннелирования в сети является перспективным направлением исследования.

СПИСОК ЛИТЕРАТУРЫ

1. Коржик В.И., Небаева К.А., Герлинг Е.Ю., Догиль П.С., Федянин И.А. Цифровая стеганография и цифровые водяные знаки. Под общей редакцией профессора В.И. Коржика. Санкт-Петербург, 2016.
2. Shterenberg S.I., Krasov A.V., Ushakov I.A. Analysis of using equivalent instructions at the hidden embedding of information into the executable files. Journal of Theoretical and Applied Information Technology. 2015. Т. 80. № 1. С. 28-34.

3. Postel, J.: RFC 792 (1981)
4. Алейников А.А., Билятдинов К.З., Красов А.В., Кривчун Е.А., Крысанов А.В. Технические аспекты управления с использованием сети Интернет Монография / Санкт-Петербург, 2016.
5. Daniel Stodle. Ping Tunnel: For those times when everything else is blocked. [сайт]. URL: http://www.cs.uit.no/~daniels/PingTunnel/
6. Алейников А.А., Билятдинов К.З., Красов А.В., Левин М.В. Контроль, измерение и интеллектуальное управление трафиком монография / Санкт-Петербург, 2016
7. Debasish Mandal. Covert Channel over ICMP. [Электронныйресурс] / Debasish Mandal's Blog. [сайт]. URL: http://www.debasish.in/

УДК 004.62

ИНФОРМАЦИОННОАЯ БЕЗОПАСНОСТЬ ОТКРЫТЫХ ДАННЫХ

Пешков Андрей Иванович , Тихонова Эльвира Никитична
Санкт-Петербургский государственный университет телекоммуникаций им.проф. М.А. Бонч-Бруевича,
Россия, Санкт-Петербург, проспект большевиков 22
emails: ap2000@yandex.ru, miss.tiny@mail.ru

Аннотация: совсем недавно открытые данные стали неотъемлемой частью повседневной жизни, вследствиечего они подвержены различного рода неправомерному и недобросовестному использованию. Авторы наблюдают состояние развития данного направления, анализируют угрозы, оценивают риски и исследуют способы обеспечения безопасности открытых данных.

Ключевые слова: *Открытые данные;общедоступные данные; публичные данные; открытые ресурсы; информационная безопасность*

INFORMATION SECURITY OF OPEN DATA

Vitkova Lidia, Peshkov Andrey, Tikhonova Elvir
The Bonch-Bruevich Saint - Petersburg State University of Telecommunications , Russia, Saint Petersburg,
Bolshevikov Prospekt 22
emails: ap2000@yandex.ru, miss.tiny@mail.ru

Annotation: Last time open data have been an integral part of everyday life, as a result of which they are subject to various kinds of misuse and illegal use**.** The authors observe the state of development of this area, analyze threat, analyze risks and explore ways to ensure the security of open data.

Keywords: *Open data; publicly available data; public data; open resources; Information Security*

Введение. Открытые данные (ОД) в широком смысле — это любая информация (документы, базы данных и т.д.) которая отвечает требованиям свободного доступа; свободы использования; автоматической обработки (машиночитаемость). Целью проекта «ОД» является реализация экономического и социального потенциала открытых данных, находящихся в распоряжении государства, путем вовлечения их в оборот негосударственного сектора. По сути, речь идет о содействии формированию информационного общества и экономики знаний. Такие задачи, как использование ОД в разработке программных приложений способствуют развитиюинновационного малого и среднего бизнеса.

Основным поставщиком наборов, открытых данных являются госорганы, но согласно статистике Портала, открытых данных порядка 3% наборов ОД поставляются негосударственными организациями и их число с каждым годом увеличивается.

Рассматривать ОД необходимо не только в качестве информации, предоставляемой государством. Среди интересов бизнеса существует потребность в раскрытии своих сформированных наборов, однако при это преследуются свои цели. Существует также потребность в предоставлении персональных и личных данных для последующей обработки в наборы. Поэтому важно разделять различные виды потребностей и целей потребителей ОД и выкладывающих их организаций[1].

Эксперты проекта «Инфометр» провели исследование уровня открытости федеральных органов исполнительной власти (ФОИВ), объединившее оценку трех основных механизмов открытости:

- Информационной открытости сайтов;
- Открытых данных;
- Общественных советов.

Каждый из этих механизмов уже оценивался экспертами проекта, что позволило отследить динамику работы органов власти по повышению открытости.

Аудит проводился в период с декабря 2013 по февраль 2014 года. С принятием Методических рекомендаций версии 3.0 существенно изменились технологические требования к публикации открытых данных на сайтах органов власти. Активизировался процесс принятия ведомствами самостоятельных дорожных карт по публикации массивов данных в машиночитаемых форматах(рисунок1,2).

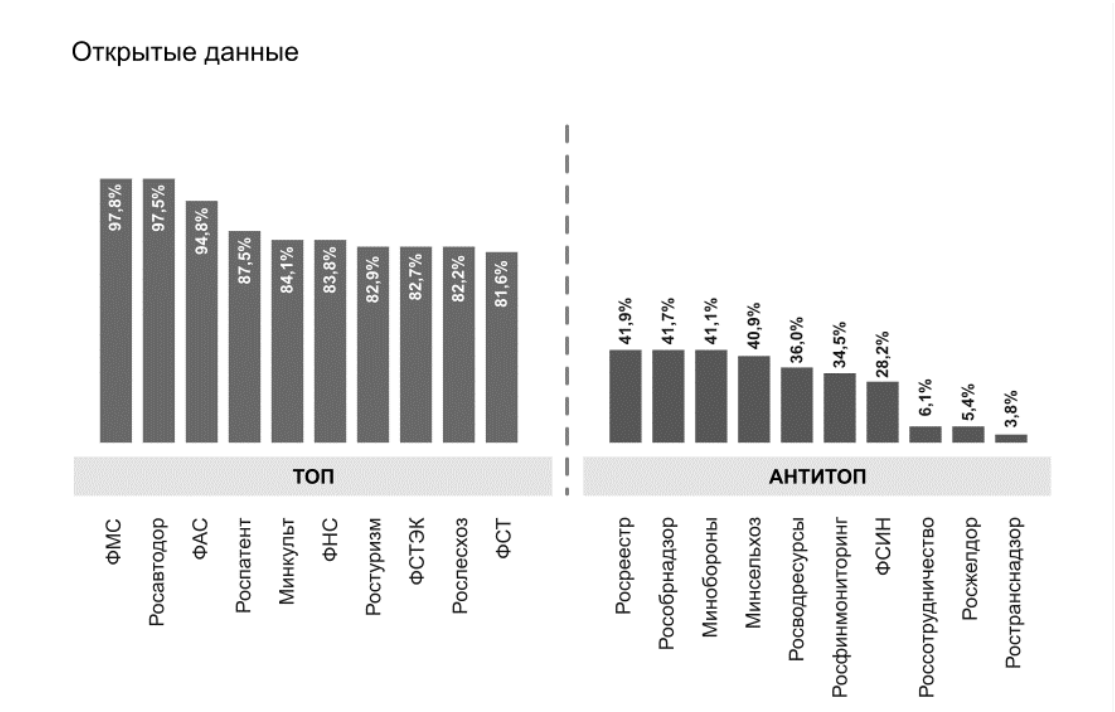


Рисунок1. Результаты аудита

infometer.org/analitika/foiv_2014/rating_2014

	Наименование органа власти	Информационная открытость	Открытые данные	Общественные советы	Сводный показатель
1	Федеральное дорожное агентство	68.82%	97.48%	80.03%	82.11%
2	Федеральная миграционная служба	74.72%	97.77%	63.14%	78.54%
3	Федеральная служба по интеллектуальной собственности	59.57%	87.45%	–	73.51%
4	Министерство транспорта Российской Федерации	50.62%	75.79%	90.67%	72.36%
5	Министерство культуры Российской Федерации	56.42%	84.07%	75.76%	72.08%
6	Федеральная антимонопольная служба	65.00%	94.77%	38.61%	66.13%
7	Федеральная служба по тарифам	66.07%	81.55%	50.07%	65.90%
8	Федеральная налоговая служба	63.36%	83.84%	50.00%	65.73%
9	Министерство труда и социальной защиты Российской Федерации	62.92%	72.82%	60.42%	65.39%
10	Министерство финансов Российской Федерации	38.14%	80.14%	60.21%	59.50%
11	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций	62.30%	80.82%	26.94%	56.69%
12	Федеральная служба по гидрометеорологии и мониторингу окружающей среды	60.41%	71.89%	23.21%	51.84%
13	Федеральное агентство по обустройству государственной границы Российской Федерации	49.82%	69.13%	34.49%	51.15%
14	Федеральная служба государственной регистрации, кадастра и картографии	46.72%	41.91%	58.20%	48.94%

Рисунок 2. Сводный рейтинг открытости федеральной исполнительной власти 2014 год

С увеличением числа вовлеченных в процесс открытия данных государственных органов и других организаций встает вопрос эффективной обработки большого массива информации, состоящей из зачастую неструктурированных и разнородных элементов[2].

Решением проблемы видится привлечение Инструменты и методы «BigData» могут быть применены не только для существенного ускорения сбора и обработки самих открытых данных, но и для решения проблем информационной безопасности, в частности – наблюдения и анализа использования в максимально автоматизированном режиме.

Одной из использующихся в сфере информационной безопасности технологий является «SIEM» (Securityinformationandeventmanagement). Средства «SIEM» в большей степени подходят организациям с крупной разветвленной структурой, обладающим временным ресурсом для накопления статистики, широкими финансовыми возможностями и высокими требованиями к защите от различных утечек данных. Таким образом, необходимостью применения и возможностью реализации обладают либо крупные компании, либо государственные органы, использующие в своей работе информацию, представляющую ценность для киберпреступников[3].

В нашей стране направление открытых данных появилось сравнительно недавно и вопросы информационной безопасности при их использовании еще недостаточно проработаны. Схематично процесс формирования открытых данных в органах власти приведен на рис. 3.

Рисунок 3. Формирование ОД в органах власти

На различных этапах развития находятся и ИС, целью которых является взаимодействие представителей власти между субъектами РФ и гражданами. В плане осуществления развития информационного общества были созданы основные предпосылки для дальнейшего совершенствования современной информационной инфраструктуры в масштабе страны. Самым распространенным видом ИС являются порталы и сайты органов государственной власти и местного самоуправления.

На каждом этапе обработки информации и формирования наборов ОД возможно возникновение угрозы безопасности информации. Они могут быть разделены на две большие группы: преднамеренные и не преднамеренные угрозы(рис.4). Часто атаки используются совместно для повышения эффективности, поэтому в ИС применяются комплексные методы защиты или в широком смысле "программы-антивирусы"[4].

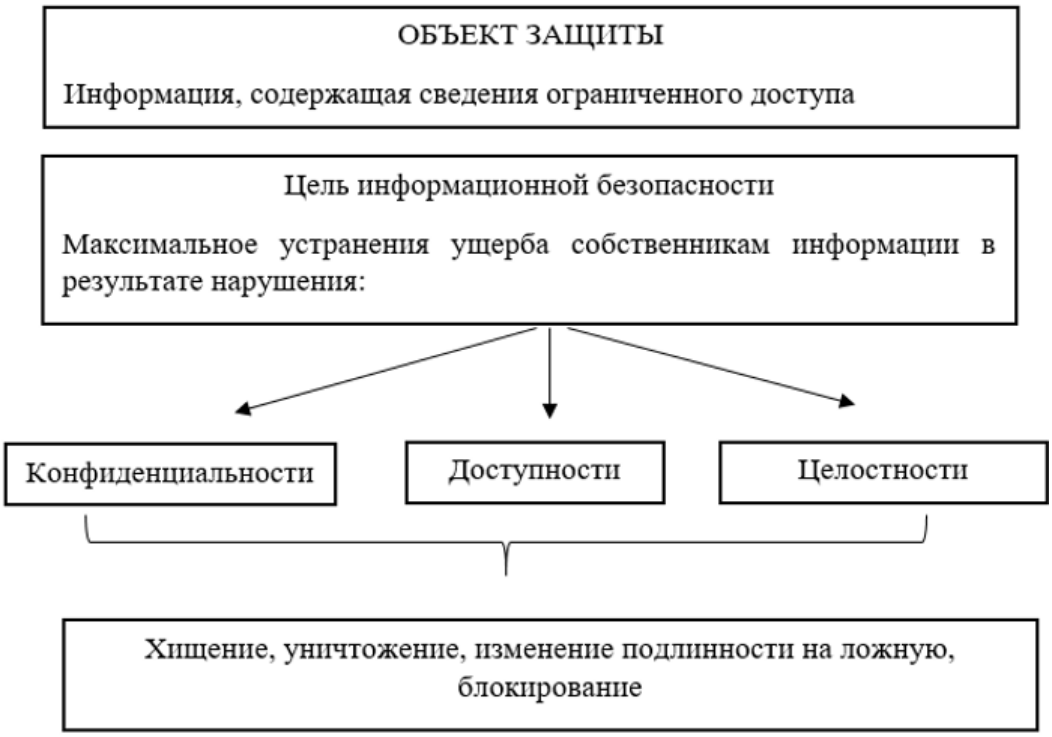


Рисунок 4. Цели и угрозы ИБ

Для автоматизации процесса сбора и анализа информации о событиях информационной безопасности используются специализированные системы мониторинга информации о событиях безопасности, поступающих из различных источников. В качестве таких источников могут выступать средства защиты информации, общесистемное и прикладное ПО [5]. Система мониторинга позволяет улучшить работу системы, заранее увидеть о возможных проблемах и устранить их.

Самый слабый и плохо исследованный аспект безопасного использования проектов на основе ОД– распространение наборов и приложений на их основе в сети Интернет. Приагрегации массивов информации, доступной для машинной обработки, возможно не только создание социально полезных продуктов, но и инструментов анализа, которые могут быть использованы такими видами нарушителей, как специальные службы иностранных государств, террористические, экстремистские группировки, конкурирующие организации.

Эти аспекты отражены в новой Доктрине информационной безопасности, принятой 5 декабря 2016 г. Доктрина создала политическую основу согласования деятельности органов государственной власти по реализации национальных интересов в информационной сфере и защите их от внешних и внутренних угроз [6].

В качестве одного из инструментов контроля можно использовать широко применяемые для создания вирусов исполняемые файлыLoader.exe. В базовом понятии под словом "лоадер" понимается некое программное обеспечение, выполняющее функции доставки файлов на компьютер пользователя. Форматы, определенные для публикации открытых данных - CSV, XML, JSON, ODS, допускают использование подобных структур. Загрузчики позволяют предварительно обрабатывать файлы, содержащие пошаговые инструкции, которым компьютер следует, чтобы выполнить ту или инуюфункцию.Loader.exe способен манипулировать другими программами, записывать ввод данных, при этом не обнаруживая своей деятельности для пользователя. Таким образом, можно получить информацию о распространении и использовании наборов открытых данных, через введенную метку типа лоадер.

Заключение. Дальнейшее развитие идеологии открытости невозможно без поиска новых средств и технологий как в области сбора, хранения, преобразования наборов открытых данных, автоматизации их обработки, так и с точки зрения обеспечения безопасности содержащейся в них информации. Только повышение безопасности технологий ОД позволит обеспечить эффективное достижение основной цели размещения открытых данных - создание условий для получения максимального международного, политического, социального и экономического эффекта.

СПИСОК ЛИТЕРАТУРЫ

1. Береснева Е.Е. opendata: зачем они нужны и что это такое [Электронный ресурс]//материалы портала «научная Россия» URL: https://scientificrussia.ru/articles/opendata-zachem-nam-nuzhny-otkrytye-dannye
2. Инструмент измерения и повышения информационной открытости [Электронный ресурс]// URL: http://infometer.org/analitika/foiv_2014#OD
3. Александр Бодрик, кибербезопасность ОД как предпосылка устойчивого развития экономической техники [Электронный ресурс]pcweekURL: https://www.itweek.ru/gover/article/detail.php?ID=189841
4. Касперски К., [книжный материал]// "Компьютерные вирусы изнутри и снаружи", Питер, 2006
5. Goldstein B., Dyson L., [книжныйматериал]//"Beyond Transparency: Open Data and the Future of Civic Innovation",2013
6. Проект Постановления Правительства Российской Федерации "О федеральной государственной информационной системе " [Электронный ресурс]// Минэкономразвития Росии 20.07.2016 URL: http://www.garant.ru/products/ipo/prime/doc/56577108/#ixzz4cBHkTXm4
7. Малков П.В. Реализация концепции ОД в РФ 15.12.2014 [Электронный ресурс]// Внедрение и использование ОД для экономического развитияURL:http://ac.gov.ru/events/04338.html
8. Доктрина информационной безопасности РФ от 5 декабря 2016 г [Электронный ресурс]// информационная безопасность РФ URL: http://www.femida.info/14/19002.htm
9. Антоненко Н.А. этапы развития и становления государственной политики в России в сфере информационной безопасности [Электронный ресурс]//новая наука: проблемы и перспективы,электрон.научн.журнал,г.2016 N 9-1 С.132-133 URL: http://elibrary.ru/item.asp?id=26711428
10. Виктор С.В. hparcsightэффективный инструмент для мониторинга событий ИБ [Электронный ресурс]// Информационная безопасность" №1, 2013 URL: https://dialognauka.ru/press-center/article/9999/
11. Протокол Правительственной комиссии по координации деятельности открытого правительства от 4 июня 2013 г. N 4 [Электронный ресурс]// требования к публикации открытых данных. С. 4-5. URL: https://www.nalog.ru/html/sites/www.new.nalog.ru/doc/met_opendata.docx
12. Методические рекомендации по реализации принципов открытости в федеральных органах исполнительной власти [Электронный ресурс]// портал открытых данных URL: http://data.gov.ru/metodicheskie-rekomendacii-po-realizacii-principov-otkrytosti-v-federalnyh-organah-ispolnitelnoy
13. Андрианов В.И., Красов А.В., Липатников В.А., Инновационное управление рисками информационной безопасности, учебное пособие: федеральное агенство связи, федеральное гос.образовательное бюджетное учреждение высш.проф.образования «СПБГУТ им.проф. М.А. бонч-бруевича»,2012
14. Андрианов В.И., Виткова Л.А., Сахаров Д.В., Исследование алгоритма защиты общедоступных персональных данных в информационных системах, сборник: Актуальные проблемы инфотелекоммуникаций в науке и образовании сборник научных статей V международной научно-технической и научно-методической конференции. 2016. С. 227-231.
15. Виткова Л.А., Рябова О.Н., Сахаров Д.В.,Проблемные вопросы создания и спользования наборов открытых данных органов государственной власти сборник: Актуальные проблемы инфотелекоммуникаций в науке и образовании сборник научных статей V международной научно-технической и научно-методической конференции. 2016. С. 271-276.

УДК 004.7

РАСШИРЕНИЕ ФОРМАЛИЗАЦИЙ ЖИЗНЕННОГО ЦИКЛА ЗАЩИЩЁННЫХ СЕРВИС-ОРИЕНТИРОВАННЫХ СИСТЕМ

Птицына Лариса Константиновна, Нежинский Виталий Владимирович
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
Россия, Санкт-Петербург, наб. р. Мойки д.61,
emails: ptitsina_lk@inbox.ru, seekerofconfessor@gmail.com

***Аннотация*:** В статье представлены преимущества защищённых сервис-ориентированных систем. Рассмотрены перспективы расширения формализаций жизненного цикла защищённых сервис-ориентированных систем. Актуализировано развитие формализмов для описания защищённых сервис-ориентированных систем с темпоральной логикой. Приведены базовые операции формирования описаний защищённых сервис-ориентированных систем с темпоральной логикой. Определены отличительные особенности рассмотренных спецификаций.

***Ключевые слова**: сервис; сервис-ориентированная система; защита информации; темпоральная логика; спецификация; модель.*

EXPANSION OF FORMALIZATIONS OF THE LIFE CYCLE OF PROTECTED SERVICE-ORIENTED SYSTEMS

Ptitsyna Larisa, Nezhinsky Vitaliy
Federal State Educational Budget-Financed Institution of Higher Education the Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
Russia, St. Petersburg, Moika River emb. 61,
emails: ptitsina_lk@inbox.ru, seekerofconfessor@gmail.com

Abstract: The article presents the advantages of secure service-oriented systems. Prospects for extending formalizations of the life cycle of secure service-oriented systems are considered. The development of formalisms for the description of protected service-oriented systems with temporal logic is actualized. The basic operations of forming descriptions of protected service-oriented systems with temporal logic are given. The distinctive features of the specifications considered are determined.

***Keywords**: service; service-oriented system; data protection; temporal logic; specification; model.*

Магистральное направление развития информационного общества ассоциируется с цифровой экономикой, при которой осуществляется непрерывное увеличение объёмов и ускорение темпов погружения взаимно-согласованных видов профессиональной деятельности в информационные инфраструктуры. В подобных условиях возрастает значимость обеспечения высокого уровня информационной безопасности при обширных масштабах априорной неопределённости, касающейся всевозможных ситуаций, сопровождающих профессиональную деятельность. В соответствии с указанными обстоятельствами проявляется объективная целесообразность сочетания в информационных инфраструктурах комплексных систем защиты информации, распределённых по ресурсам инфраструктуры, и защищённых сервис-ориентированных систем. При подобном сочетании удаётся воспользоваться представительным комплексом технологий их жизненного цикла, имеющих индустриальный характер, и арсеналом преимуществ сервис-ориентированных систем, основными из которых являются поддержка распределенности систем, независимость от технологий разработки и платформ, управляемое распределение нагрузки между сервисами, сжатые до разумной целесообразности длительности вывода на IT-рынок, высокая степень гибкости функциональной спецификации, согласуемая с современными запросами науки, образования промышленности, транспорта, медицины и социальной сферы.

С расширением многообразия комплексируемых сегментов профессиональной деятельности, погружаемых в информационные инфраструктуры цифровой экономики, повышается востребованность защищённых сервис-ориентированных систем, жизненный цикл которых разворачивается в контексте многокомпонентного программного обеспечения. Определение и оценивание качества функционирования многокомпонентного программного обеспечения, образуемого посредством интеграции сервисов, обеспечивается методологическим базисом, ключевые компоненты которого раскрываются в [1, 2, 3, 4, 5, 6, 7]. Задачи соблюдения требуемого уровня информационной защищённости возлагаются на подсистему сервисов защиты информации от потенциальных угроз, соответствующих комплексируемым сегментам профессиональной деятельности и сопровождающим информационным инфраструктурам. Определение и оценивание показателей различных профилей информационной защищённости обеспечивается методологическим базисом, основные составляющие которого представляются в [8]. При этом на основе сочетания двух указанных базисов может проводиться анализ информационной безопасности как на уровне собственно сервис-ориентированной системы, так и на уровне сложной системы, образуемой в

результате интеграции сервис-ориентированной системы и компонентов комплексных систем защиты информации, распределённых по ресурсам инфраструктуры.

В подобном направлении создания и развития технологических платформ цифровой экономики качество сложного многокомпонентного программного обеспечения становится одним из основных приоритетов развития индустрии информации, позволяющим планировать и достигать конкурентных преимуществ по целевым ориентирам корпоративных и национальных интересов социума. Условия жёсткой конкуренции компаний IT-сферы, стремящихся к ускорению процессов разработки инновационных сложных программных систем, являются дополнительным стимулом для расширения сферы цифровой экономики и создания различных высокоэффективных форм её реализации.

В динамично изменяющихся условиях рыночной экономики среда рассматриваемых систем сможет гибко и оперативно ориентироваться на успешное решение новых научно-технических и маркетинговых задач, среди которых:

– повышение качества сегментации партнёров и клиентов;

– повышение эффективности маркетинговых мероприятий по продвижению наукоёмкой продукции;

– интеграция различных каналов коммуникаций с клиентами для сбора необходимой информации о партнёрах и клиентах;

– повышение качества работы с наиболее успешными партнёрами и прибыльными клиентами для повышения их лояльности;

– персонализация общения с потенциальными клиентами и предложение им только тех услуг, которые соответствуют их потребностям и требованиям качества.

При обширном объёме тематики научных исследований, связанных с жизненным циклом сервис-ориентированных систем, методологические аспекты их формальной верификации остаются открытыми. Отмеченная особенность может являться одной из причин несогласованности составляющих жизненного цикла сложных многокомпонентных программных систем, обеспечивающих технологическое сопровождение цифровой экономики. К примеру, при создании систем с первым классом информационной защищённости позиционируется обязательность проведения верификации. В силу представленных оснований предлагается развитие системы формализаций методологии проектирования сервис-ориентированных систем посредством введения процедур их формальной верификации.

Согласно традиционным канонам [8] верификация модели осуществляется за три этапа: построение математической модели; представление проверяемых свойств в виде спецификации; формальное доказательство наличия или отсутствия проверяемого свойства и всех свойств в совокупности.

Математическая модель системы для верификации строится в виде графа. При этом состояниям системы (ситуациям или классам ситуаций, в которых может находиться система в различные моменты времени) ставятся в соответствие вершины графа, а действиям, выполняемым системой, – ребра графа.

Спецификация определяется как описание свойств системы в виде формального текста. Она представляется в формальном виде, зависящем от характера логики. В случае применения одной из самых известных логик CTL (Computational Tree Logic), соответствующей реальным условиям организации и функционирования распределённого программного обеспечения в гетерогенных активных инфокоммуникационных средах, спецификация записывается в терминах предикатов с использованием темпоральной логики.

Зависимость между свойствами интегрируемых сервисов и свойствами защищённой сервис-ориентированной системы определяется следующим выражением:

$$\bigcup_{i=1}^{N} (\text{свойство } i-\text{го сервиса}) \rightarrow (\text{все свойства системы}).$$

Во множество формализаций CTL логики вводится система переходов. Система переходов S описывается в виде кортежа

$$S = (P, Q, \delta, L, Q^0),$$

где P – множество, элементами которого являются утверждения;

Q – множество состояний системы перехода S;

δ – бинарное отношение на множестве Q

$$\delta \subseteq Q \times Q);$$

L (оценка) – функция

$$L: Q \times P \rightarrow \{0, 1\},$$

Функция L каждым q ϵ Q и p ϵ P ставит в соответствие 1, если утверждение p в состоянии q истинно, и 0, если утверждение p в состоянии q ложно;

$Q^0 \subseteq Q$ – множество начальных состояний.

Система переходов изображается в виде ориентированного графа, вершинами которого являются состояния и для каждой пары $(q', q)\ \epsilon\ \delta$ граф содержит ребро из q' в q.

Для каждого состояния q ϵ Q предусматривается $\delta(q) = \{q' \epsilon Q | (q, q') \epsilon \delta\}$. В ситеме выделяются пути. Путем в системе перехода является последовательность $\pi = (q_0, q_1, \dots)$, такая, что для $q_{i+1} \epsilon \delta(q_i)$ для любого i.

Пусть S = (P, Q, δ, L, Q^0) – система перехода. Для любого состояния q ϵ Q и любой CTL-формулы φ значением формулы q(φ) в состоянии q является булева константа 1 или 0, которая определяется индуктивно:

1. если φ = p ϵ P, то q(φ) уже определено в S.
2. q(1) $\stackrel{\text{def}}{=}$ 1, q(0) $\stackrel{\text{def}}{=}$ 0 .
3.

– $q(\overline{\varphi}) \stackrel{\text{def}}{=} \overline{q(\varphi)}$

– q(φ^η) $\stackrel{\text{def}}{=}$q(φ)^q(η)

– q(φ∨η) $\stackrel{\text{def}}{=}$ q(φ)∨q(η) .

В формулах CTL логики применяются кванторы пути и темпоральных операторов. Выделяют два квантора пути: A – квантор всеобщности, указывающий на то, что свойство выполнено для всех путей; E – квантор существования, указывающий на то, что свойство выполнено для некоторого пути. В типовых случаях рассматриваются два темпоральных оператора: G – унарный оператор, указывающий на то, что свойство выполняется для любого состояния; F – унарный оператор, указывающий на то, что свойство выполняется при некотором состоянии. В выбранной логике определяются CTL-операторы:

EF (ψ (q)) = 1,

если существует путь π из q и существует состояние $q' \epsilon$ π такое, что

ψ (q') = 1;

AG (ψ (q)) = 1,

если для каждого пути π из q и для каждого состояния $q' \epsilon$ π имеет место

ψ (q') = 1.

В случае доказательства наличия всех проверяемых свойств защищённая сервис-ориентированная система признаётся пригодной для дальнейшего исследования и реализации, в процессе которых определяются и оцениваются показатели качества её функционирования.

Посредством приведённой формальной верификации расширяется методологический базис проектирования защищённых сервис-ориентированных систем с требуемыми свойствами и качеством их функционирования для технологического сопровождения различных секторов цифровой экономики.

СПИСОК ЛИТЕРАТУРЫ

1. Птицына Л.К., Смирнов Н.Г. Разработка и анализ моделей интеграции сервис-ориентированных средств в гетерогенных сетях // Научно-технические ведомости СПбГПУ 6.1 (138). 2011. С. 71-80.
2. Птицына Л.К. Программное обеспечение компьютерных сетей. Управление крупно-гранулярными процессами на основе языка BPEL: учеб. пособие / Л.К. Птицына, Н.Г. Смирнов. – СПб. : Изд-во Политехн. ун-та, 2011. 105 с.
3. Птицына Л.К., Смирнов Н.Г. Системно-аналитическая основа интеграции сервис-ориентированных средств // Промышленные АСУ и контроллеры. 2011. № 5. С. 31-36.
4. Птицына Л.К., Веселов В.О. Анализ интеграции сервис-ориентированных средств в активных инфокоммуникационных средах // Наукоёмкие технологии в космических исследованиях Земли. 2015. Т. 7. № 2. С. 42-47.
5. Веселов В.О., Птицына Л.К. Моделирование интеграции сервис-ориентированных средств в активных инфокоммуникационных средах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2 т.; Т.1 / под ред. К.В. Дукельского, сост. А.Г. Владыко, Е.А. Аникевич, Л.М. Минаков. – СПб. : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2015. С. 465 – 470.
6. Птицына Л.К., Кондратьев Д.А., Эльсабаяр Шевченко Н. Моделирование интеллектуальных сервис-ориентированных систем // Информационные системы и технологии в моделировании и управлении: материалы всероссийской научно-практической конференции. Гуманитарно-педагогическая академия (филиал) ФГАОУ ВО «КФУ им. В.И. Вернадского» в г. Ялте; Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», 2016. С. 57-60.
7. Кондратьев Д.А., Птицына Л.К., Эльсабаяр Шевченко Н. Концептуальные модели интеллектуализации сервис-ориентированных архитектур // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3 т.; Т.2 / под ред. С.В. Бачевского, сост. А.Г. Владыко, Е.А. Аникевич, Л.М. Минаков. – СПб. : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2016. С. 108 – 113.
8. Птицын, А.В., Птицына, Л.К. Аналитическое моделирование комплексных систем защиты информации. Гамбург. Saarbrucken: LAP LAMBERT Academic Publishing, 2012. 293 с.
9. Миронов А.М. Верификация программ методом Model Checking [Электронный ресурс]. URL: http://intsys.msu.ru/staff/mironov/modelchk.pdf (дата обращения 10.02.2017).

УДК 004.72

ПРОБЛЕМА АНОНИМНОСТИ В СЕТИ ИНТЕРНЕТ СРАВНЕНИЕ МЕТОДОВ АНОНИМИЗАЦИИ ПОЛЬЗОВАТЕЛЯ

Титова Юлия Алексеевна[1], Садикова Анастасия Александровна[2], Савков Сергей Витальевич[3]
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики «ИТМО»,
Россия, Санкт-Петербург, пр-кт Кронверкский, 49
emails: titova.yulishna@mail.ru, nastya.sadkoo@mail.ru, sergsavkov@gmail.com

***Аннотация*:** Сейчас все большее количество людей беспокоит проблема анонимности в сети Интернет. К сожалению, полностью обезопасить себя нельзя, однако, используя методы анонимизации, риски можно свести к минимуму. В статье рассмотрены самые популярные методы, позволяющие обеспечивать анонимность и информационную безопасность в сети Интернет, такие как различные Proxy-серверы, VPN-серверы, сети Tor, I2P, и метод «крышевания» доменов. Рассмотрен принцип их работы, проанализированы основные преимущества и недостатки. Сделаны выводы, что каждый метод разработан для определённых целей, а значит, при выборе способа анонимизации следуют руководствоваться конкретными задачами, которые стоят перед пользователем.

***Ключевые слова*:** *анонимизация; proxy-сервер; VPN; Tor; I2P*

THE PROBLEM OF ANONYMITY IN THE INTERNET NETWORK COMPARISON OF METHODS OF USER ANONYMIZATION

Titova Yulia, Sadikova Anastasia, Savkov Sergei
Saint Petersburg National Research University of Information Technologies, Mechanics and Optics «ITMO»,
Russia, St. Petersburg, Kronverkskiy prospekt, 49
emails: titova.yulishna@mail.ru, nastya.sadkoo@mail.ru, sergsavkov@gmail.com

Abstract: Nowadays more and nore people are concerned about the problem of anonymity on the Internet. Unfortunately, one cannot completely protect onerself, however, using anonymization methods, risks can be minimized. The article covers the most popular methods that allow anonymity and information security on the Internet, such as various Proxy servers, VPN servers, Tor networks, I2P, and the method of domain "fronting". The principle of their work is considered, the main advantages and disadvantages are analyzed. It is concluded that each method is designed for certain purposes, and therefore, when choosing the method of anonymization, one should follow specific tasks that are faced to the user.

Keywords: *anonymization; proxy-server; VPN; Tor; I2P*

Введение. Ведущие специалисты в области информационной безопасности утверждают, что полной анонимности в сети Интернет добиться практически невозможно. Поэтому среднестатистический пользователь, считающий себя анонимом, является таковым лишь формально. Словарь Ожегова даёт следующее определение слову анонимность: Без указания имени того, кто пишет, сообщает о чем-либо [1]. Действительно, пользователи сети Интернет стараются не указывать свои личные данные на подозрительных сайтах, однако это не гарантирует анонимности в сети. Большинство Web-серверов ведёт контроль посещаемости, а значит IP адреса устройств, с которых был выполнен вход на сайт, остаются в базе данных, где также фиксируется активность пользователя на сайте. Помимо этого задействуются социальные сети. Так, к примеру, по официальным данным, Facebook, MySpace и несколько других социальных сетей продавали личные данные рекламным компаниям, которые в дальнейшем использовали их для поиска имён потребителей, контактных данных и другой личной информации [2]. Таким образом, осуществляется взаимодействие сайтов, в процессе которого происходит обмен информацией и составление полноценной характеристики о каждом клиенте. Более продвинутые пользователи пытаются оградить себя от этого и прибегают к различным изобретательным подходам для достижения анонимности. Но это им не всегда удается, поскольку в настоящее время со стороны, как государства, так и частных организаций активно ведется борьба с анонимностью в сети Интернет. Принимаются меры по деанонимизации: устанавливаются обязательная идентификация пользователей при использовании общественных точек доступа, блокируются proxy-серверы и анонимные сети, контролируется трафик с помощью технологии DPI и пр.

Методы анонимизации зачастую используются злоумышленниками, с целью избежать наказания за правовые нарушения. В борьбу с ними вступают правоохранительные органы, которые при помощи способов деанонимизации устанавливают реальную личность преступника, его место нахождения, активность в сети Интернет и прочую необходимую информацию.

В этом и заключается проблема анонимности в сети Интернет. Всегда будут люди, которые хотят защитить информацию о себе. А в противовес им будут существовать организации, которые пытаются извлечь выгоду из обладания личными данными пользователей, и правоохранительные органы, задача

которых деанонимизировать и наказать правонарушителя. Поэтому способы анонимизации в сети интернет будут рассмотрены с различных позиций.

Работа Proxy-серверов.

Одним из самых распространённых методов анонимизации является использование Proxy-серверов. Основным идентификатором в сети является IP адрес. Он служит обратным адресом, на который приходит ответ от Web-сервера. Поэтому избавиться от IP невозможно. Но с помощью Proxy-сервера его можно заменить.

Общий принцип работы таких методов заключается в появлении между пользователем и сетью Интернет связующего звена. Proxy-сервер получает запрос от клиента и перенаправляет его уже со своим IP адресом на Web-сервер. На рис. 1. представлена принципиальная схема работы Proxy-сервера. Таким образом у Web-сервера имеется адрес только Proxy-сервера. Ответ также проходит через Proxy-сервер и направляется обратно пользователю.

Рис. 1. Принципиальная схема работы Proxy-сервера

С точки зрения обеспечению анонимности различают три основных вида Proxy-серверов: HTTP(S) Proxy, CGI Proxy и Socks Proxy. HTTP(S) Proxy являются самыми распространёнными. Они позволяют скрыть IP пользователя, но в передаваемом трафике указывают, что был использован Proxy-сервер. Ещё одним недостатком такого сервера является работа только для HTTP протокола. Следующий вид это CGI Proxy, которые также называют анонимайзерами. Они привязаны к браузеру и представляют собой Web-сервер, в поле которого пользователь вводит URL. CGI Proxy выгружает запрашиваемую страницу себе, и пользователь может её посмотреть на сайте Proxy-сервера. Другой вид серверов это Socks Proxy. Они действуют по общему принципу, однако у них есть одно кардинальное отличие. Обмен информацией пользователь – proxy-сервер происходит с помощью специальных протоколов(socks4, socks5). В этом случае IP адрес клиента вообще не используется. Выявить такой сервер затруднительно, поскольку передаваемая информации проходит через него без изменений и не содержит в себе никаких данных об использовании связующего звена. Также стоит упомянуть о цепочках Proxy. Для их создания необходимы специальные программы, которые позволяют объединить сервера в так называемый виртуальный туннель и передавать по нему информацию от пользователя к конечному Web-серверу. При создании туннеля можно использовать Proxy-сервер одного вида или комбинировать их [3]. Однако цепочка Proxy-серверов считаются неэффективными, ввиду того, что в неё содержится информация обо всех серверах, которые в неё входят. Отличие заключается лишь в том, что для деанонимизации возникает необходимость получить ответ от каждого Proxy-сервера этой цепочки.

Основным недостатком такого метода является то, что протоколы всех действий хранятся на Proxy-серверах. Их владельцы могут подменить информацию или даже продать. Поэтому важно, пользоваться только надежными серверами. Если все же сервер надёжный, вычислить, что пользователь является анонимом, можно по cookies. Это происходит путём сравнивания данных cookies до использования proxy-сервер с новыми данными. Если cookies совпадают, а IP адреса различаются, сервер делает выводы и заносит данный адрес в чёрный список. Proxy-серверы не используют дополнительных методов шифрования, поэтому считается, что они не могут обеспечивать высокий уровень безопасности. Также на некоторых сайтах устанавливаются специальные java-скрипты, которые позволяют установить реальный IP адрес пользователя. Таким образом наиболее популярные серверы вычисляются и блокируются.

Работа VPN-серверов.

Следующий способ анонимизации, который будет рассмотрен, это VPN – Virtual Private Network. Такая логическая сеть организуется поверх другой сети, в общем случае поверх сети Интернет. По аналогии с Proxy-серверами трафик, поступающий от пользователя, проходит через частную сеть и, поступая на заданный Web-сервер, уже имеет IP адрес VPN-сервера. Тем самым пользователь скрывает свой реальный IP. Принципиальную схему работы VPN-сервера можно увидеть на рис.2. Преимуществом такого способа является шифрование. С помощью, установленной на компьютер программы, весь исходящий трафик скрывается с помощью выбранного алгоритма, и в зашифрованном виде передаётся на VPN-сервер. Далее на сервере информация дешифруется и передаётся адресату.

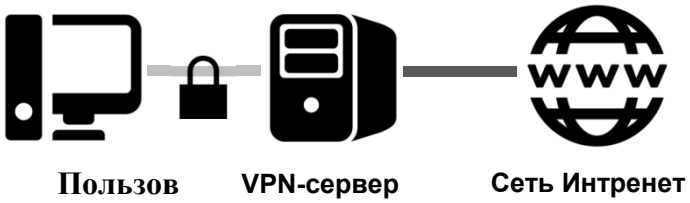


Рис. 2. Принципиальная схема работы VPN-сервера

Недостатки этого способа во многом схожи с рассмотренными ранее. Однако, в отличает от Proxy-серверов, способ VPN обеспечивает зашифрованный туннель между пользователем и VPN-сервером [4]. Это не гарантирует полной безопасности, поскольку на выходе из VPN-сервера трафик расшифровывается и, передаваясь в таком виде, он может быть перехвачен. Чтобы избежать этого, дополнительно используют SSL и TLS. Это криптографические протоколы, используемые для создания двустороннего защищенного канала. Они обеспечивают конфиденциальность, обнаружение подмены и аутентификацию узлов.

Работа сети Tor.

Более совершенный метод анонимизации представляет Tor. Его принципиальная схема работы представлена на рис. 3. Это программное обеспечение, осуществляющее распределение трафика по различным серверам с использованием так называемой «луковой» маршрутизации. Узлами системы Tor, помимо специальных серверов являются и устройства самих пользователей. В такой системе реализовано ступенчатое шифрование. Случайным образом выбирается количество промежуточных узлов. Затем производится соединение с каждым из них и передаётся личный ключ (для каждого узла свой). Многократно зашифрованные данные передаются на первый узел, который с помощью своего личного ключа открывает последний уровень шифрования и получает адрес следующего узла [5]. Следующий узел делает то же самое – расшифровывает очередной «слой» и, получив адрес, отправляет дальше. При этом на промежуточных звеньях передаваемая информация и конечный адресат являются невидимыми. Это обеспечивает отсутствие прямых связей. Завершающий узел цепочки Tor передаёт сообщение в сеть. Таким образом источник информации скрывается и запутывает обратный путь.

Рис. 3. Принципиальная схема работы сети Tor

В случае использования Tor следует разделять понятия анонимности и безопасности передаваемых данных, поскольку Tor позволяет защищать данные только внутри своей сети, а между конечным звеном и сетью Интернет такой защиты уже нет [6]. К примеру, даже на выходном узле цепи информация может подвергаться изменениям и мониторингу. Несмотря на это данный метод считается одним из наиболее эффективных способов анонимизации. Также сеть Tor имеет свои внутресетевые Web-сайты - onion сайты, доступные только внутри сети Tor. Это значит, что при пользовании внутренней сетью обеспечивается почти максимальная анонимизация. Более того, значительное преимущество Tor заключается в том, что заблокировать цепочку практически невозможно. Это обусловлено тем, что для блокировки Tor придётся блокировать целую подсеть, так как узлами цепи, помимо серверов являются и устройства пользователей. Кроме того следует отметить, что цепочка узлов, по которым передаётся трафик, является динамической. Она меняется через определённые промежутки времени. Несмотря на это анонимность, достигнутую с помощью рассмотренного способа, нельзя считать абсолютной, потому как на эту систему являются действенными атаки с использованием межсайтового скриптинга.

Комбинация Tor и VPN.

Для устранения утечек информации на входном и выходном узле цепочки Tor используются комбинации методов VPN и Tor. Существует два способа комбинации. Первый – когда VPN-сервер стоит перед сетью Tor в качестве входного узла. В этом случае трафик, поступающий на первый узел цепочки Tor, имеет IP адрес только VPN-сервера. Также эта комбинация позволяет скрыть от Интернет-провайдера сам факт использования системы Tor. И второй – где VPN-сервер используется в качестве выходного узла. Такой способ позволяет избежать прослушивания трафика на последнем узле цепочки

Tor. Однако методом анализа выходной узел может выявить использование VPN-сервера, поскольку клиент будет обращаться только к одному IP адресу. Несмотря на это, данные комбинации считаются неэффективными по сравнению с сетью Tor. Поскольку с применением данных комбинаций возникают дополнительные угрозы утечки данных с VPN-сервера.

Работа сети I2P.

Схожим по некоторым параметрам методом является построение сети I2P – Invisible internet project. В нём используется «чесночная» маршрутизация. Каждое сообщение многократно шифруется, как в описанной ранее «луковой». Затем объединяется с транзитными сообщениями в один пакет и передаётся по выстроенному туннелю. Когда же пользователю приходит пакет, он открывает его своим личным ключом и получает только адресованные ему сообщения. Остальной пакет является недоступным, потому как по отношению к нему пользователь лишь промежуточное звено [7]. Таким образом, пакет пересылается далее от узла к узлу. В отличает от сети Tor, маршруты Клиент – Web-сервер и Web-сервер – Клиент содержат разные узлы. На рис.4. изображена принципиальная схема построения маршрутов в сети I2P. Исходящий туннель позволяет скрыть данные об отправителе, а входящий – о получателе. Для связи этих туннелей используется сетевая База NetDb, в которой хранятся маршрутные данные клиентов. Следует отметить, что сеть I2P имеет свою адресацию. К каждому узлу привязывается, генерируемый случайным образом, I2P адрес, вместо IP, который используется в сети Интернет. IP адресом в такой цепи обладает только выходной узел, который обеспечивает связь с глобальной сетью. Вследствие этого узнать IP адрес пользователя весьма затруднительно. Также анонимность внутри сети обеспечивается за счёт того, что в ней не используется привычный DNS-сервер. Вместо него у каждого пользователя есть обновляемая адресная книга, в которой записаны доменные имена и соответствующие им I2P адреса. Из чего можно заключить, что вычислить пользователя по DNS запросам практически невозможно.

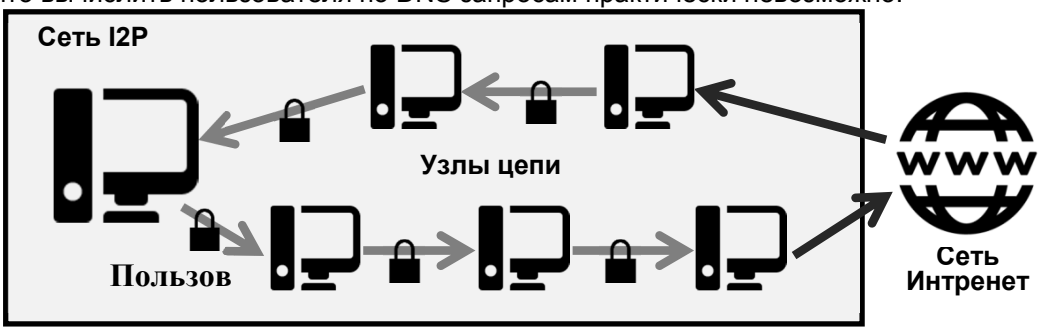


Рис. 4. Принципиальная схема построения маршрутов в сети I2P

Особенность сети I2P заключается в том, что она в основном используется, как полноценная и самостоятельная сеть, которая имеет свою адресацию и свои Web-сайты, называемые eepsites. В таком случае она действительно обеспечивает очень высокий уровень анонимизации. Если же её использовать для выхода в сеть Интернет, то возникает проблема безопасности, так как на выходном узле из сети I2P трафик может быть изменён или прослушан. Более того для пользователя предоставляется только один выходной узел, а это значит, что может возникнуть проблема с блокировкой на некоторых сайтах.

Метод «крышевания» доменов.

Методы и средства, обеспечивающие анонимность, постоянно развиваются. Сейчас активно набирает популярность описанный в 2015 году метод «крышевания доменов». В оригинальном источнике этот метод называется domain fronting. Рассмотрим его на примере известного мессенджера «Signal». Для обеспечения анонимности он использует широко признанное, авторитетное промежуточное звено между пользователем и Web-сервером. А именно службу хостинга сайтов «Google App Engine» [8]. На рис. 5. представлена принципиальная схема работы метода «крышевания» доменов. Особенность такого метода заключается в том, что средства анализирующие трафик воспринимают такие запросы, как обращение к различным доменам Google и рассматривают их в качестве конечного звена. На самом же деле реальное доменное имя зашифровано с помощью HTTPS шифрования и после прохождения промежуточного узла, трафик перенаправляется далее по необходимому адресу уже с IP адресом сервера Google. Для блокировки такого метода необходимо заблокировать все домены, которые предоставляет служба «Google App Engine», что является затруднительным.

Метод «крышевания доменов» зависит от промежуточного Web-сервера, а значит, вновь возникает проблема доверия. Недостаток рассмотренного мессенджера заключается в том, что к аккаунту привязывается номер мобильного телефона, а все контактные номера с устройства выгружаются на сервер, для того, чтобы организовать пересылку сообщений. Таким образом, информация о пользователе, которую можно найти в сети Интернет, привязывается к информации, которая храниться на серверах мобильных операторов.

Рис. 5. Принципиальная схема работы метода «крышевания» доменов

Как видно, ни один из разобранных в статье способов не может дать гарантию полной анонимности. Всегда остаются уязвимости систем, которыми могут воспользоваться с целью деанонимизации [9]. Поэтому прежде, чем выбирать способ скрытия личности в сети, необходимо чётко определить с какой целью он будет использован и оценить на какие затраты средств и времени будут готовы пойти злоумышленники, чтобы провести деанонимизацию. К примеру, если главная задача это не допустить утечку данных рекламным компаниям, то будет достаточно воспользоваться proxy-серверами и чистить файл cookies. При этом лучше избегать посещения социальных сетей. В условиях, когда провайдером блокируется часть Интернет ресурсов, особенно часто применяются средства анонимизации для получения доступа к запрещённым доменам. В таком случае помимо Proxy-серверов пользуются сетью Tor, поскольку она считается более надёжным методом достижения анонимности в сети. Если этот способ применяется с целью анонимного посещения Web-серверов сети Интернет, то, как правило, большинство атак будет сводиться к принципу «цель не оправдывает средства». Тем не менее, в настоящее время активно исследуются способы противодействия Tor. В качестве же системы для передачи личных данных лучше использовать I2P без выхода в сеть Интернет. Поскольку сеть I2P обеспечивает не только анонимность, но и безопасность передаваемых данных.

Заключение. В работе были рассмотрены подходы к обеспечению анонимности в сети. Ни один способ на сегодняшний день не может обеспечить полной анонимизации пользователя. Поэтому задача анонимизации сводится к тому, чтобы для деанонимизации требовались недостижимые вычислительные ресурсы или такой объем времени раскрытия, что по его истечению деанонимизация была бы уже не актуальной. Также при использовании различных методов возникают сопутствующие трудности. Поэтому, выбирая средства, следует учитывать, какой ценой будет обеспечиваться анонимность. Для того чтобы избавиться от некоторых недостатков того или иного метода анонимизации прибегают к комбинированию различных методов. Как показывает практика, на каждый метод анонимизации создаются средства, позволяющие обойти его. Поэтому, вероятнее всего, «панацеи» в средствах обеспечения анонимизации создано не будет. Со стороны нашего государства отношения в сфере информационной безопасности регулируются 23 и 24 статьей Конституции РФ. Каждый имеет право на неприкосновенность частной жизни, однако реализация этого права в руках каждого участника информационного обмена. Знание элементарных основ информационной безопасности решит большую часть проблем обеспечения анонимности.

СПИСОК ЛИТЕРАТУРЫ

1. Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка. – 4-е изд. – М., 1997.
2. Steel. E., Jessica E. Vascellaro. Facebook, MySpace Confront Privacy Loophole // www.wsj.com, 21.05.2010. Точный адрес статьи: http://www.wsj.com/articles/SB10001424052748704513104575256701215465596.
3. Радайкин М.Ф. Кратко о проблеме анонимности в сети интернет // Пробелы в российском законодательстве. Юридический журнал. 2013. №2 С. 25-28.
4. Денисова Т.Б. Безопасность услуги VPN // Вестник Самарского государственного технического университета. Серия: технические науки. 2005. №33 С. 168-171.
5. Иванов С.Н. Преступление в сфере высоких технологий: проблемы документирования компьютерных преступлений // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2012. № 18 С. 70-74.
6. Кузичкина О.А. Сеть Tor как способ подключения к «глубокому» интернету // Интеллектуальный потенциал XXI века: ступени познания. 2014. №25 С. 129-131.
7. Угрюмов Д.В., Хализев В.Н. Создание математической модели обеспечения достаточного уровня анонимности в системах электронного голосования с сохранением целостности и конфиденциальности передаваемых данных // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2013. №93 С. 1-16.
8. Fifield D., Lan C., Hynes R., Wegmann P., Paxon V. Blocking-resistant communication through domain fronting // Proceedings on Privacy Enhancing Technologies. 2015. N 2. P. 1-19.
9. Ахметшин Р.Г., Киселева Л.В. анонимность в глобальной сети // Вестник молодых ученых Самарского государственного экономического университета. 2016. № 1 (33). С. 265-269.

УДК 004.056

АНАЛИЗ АКТИВНЫХ СЕТЕВЫХ АТАК:ARP-SPOOFING ИDNS-SPOOFING

Ягудин Ильдар Рашидович, Волкогонов Владимир Никитич
Санкт-Петербургский государственный университет телекоммуникаций «СПБГУТ»,
Россия, Санкт-Петербург, ул. пр. Большевиков, 22, к. 1,
emails: Ildardag@gmail.ru

***Аннотация*:** в статье рассматриваютсянаиболеераспространённые виды активных сетевых атак, при реализациикоторых применяется перехват трафика между узлами и подмена сетевого адреса. Также, предложены различные методы защиты от определённых типов сетевых атак.

***Ключевые слова**: Активная сетевая атака, злоумышленник, подмен сетевого трафика, перенаправления трафика, локальная сеть.*

ANALYSIS OF ACTIVE NETWORK ATTACK: ARP SPOOFING AND DNS SPOOFING

Yagudin Ildar, Volkogonov Vladimir
Saint-Petersburg state University of telecommunications "SUT",
Russia, Saint-Petersburg, ul Bolshevikov, 22, building 1,
emails: Ildardag@gmail.ru, krasov@inbox.ru

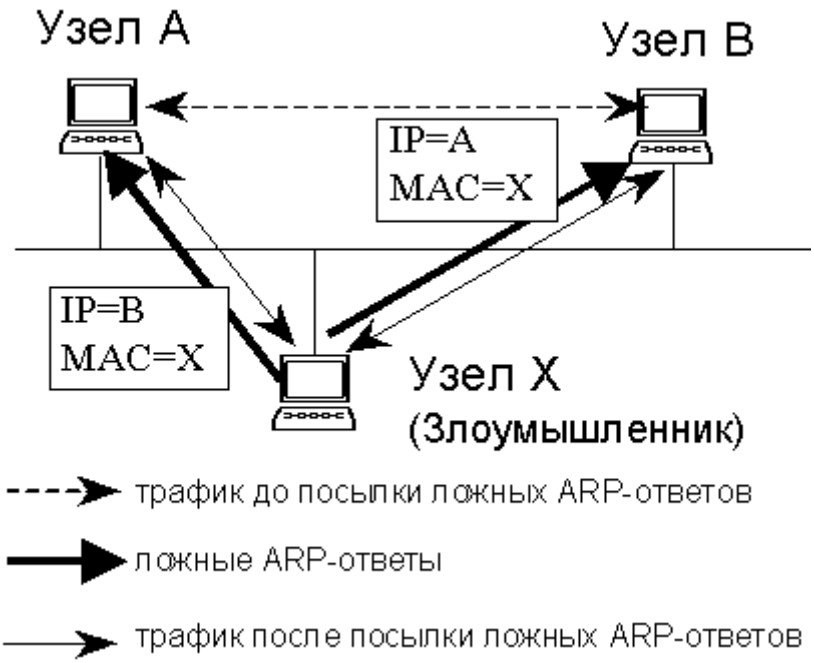
Abstract: this article discusses the most common types of network attacks, the implementation of which is used to intercept traffic between nodes, and the substitution of the network address. Also proposed various methods of protecting against certain types of network attacks.

***Keywords**: Active network attack, the attacker changes the network traffic, redirect traffic, and LAN.*

Введение. В настоящее время в мире существует огромное количество сетевых атак. В данной статье рассмотрены две сетевые атаки разновидностей атак MITM (англ. Maninthemiddle-человек посередине); ARP (англ. Address Resolution Protocol - протокол разрешения адреса) spoofing,DNS (англ. DomainNameSystem — система доменных имен)spoofing и рассматриваются возможности реализации их с использованием программного обеспечения. Обычно, для таких атак часто требуется использовать специализированное программное обеспечение. Как правило, все удалённые атаки, которые известны в нашем мире являются активными. Активные сетевые атаки оказывают непосредственное влияние на работу системы, то есть требуют от злоумышленника какие-то активные действия для того что бы попытаться нарушить принятую в системе политику безопасности. Они являются детектируемыми.

ARP–spoofing. На канальном уровне используютсяMAC- (от англ. Media Access Control — управление доступом к среде) адреса, на сетевом уровнеTCP/IP(от англ.TransmissionControlProtocol-протокол управления передачей)/(InternetProtocol -«межсетевой протокол») используютсяIP-адреса, так как для вычислительной техники IP-адрес — это набор байт, поэтому машине в локальной сети передают данные через MAC- адреса, который находится на канальном уровне, чтобы сопоставлять IP-адреса к MAC-адресам есть специальный протокол ARP (Address Resolution Protocol -протокол разрешения адреса) протокол позволяет сопоставить IP-адреса к адресам канального уровня. Протокол проектировался в 1992г и не предполагал механизмы защиты.Рассмотрим работупротокола. В нашей сети имеются 2компьютера со следующими характеристиками: компьютер А с IP-адресом напр.(10.55.55.2) и компьютер БсIP-адресом напр. (10.55.55.3). Они соединены между собой сетью Ethernet.КомпьютерА, отправляет пакет компьютеру Б у которого есть существующийIP-адрес, однако сеть Ethernet не работает с IP-адресам, а MAC-адрес ему неизвестен. Для этого он использует протокол ARP, он посылает широковещательный запрос всем компьютерам в локальной сети с таким сообщением «Компьютер с такимнапр. (10.55.55.3)IP-адресам сообщите свой MAC-адрес компьютеру, у которого такой MAC-адрес напр. (64:63:80:C9:64: F7)». Этот запрос доставляется всем устройствам в сети.Компьютер Б в ответ присылает компьютеру А свой MAC-адрес, в свою очередь они могут теперь пересылать данные.[7] Для того что бы не делать запрос каждый раз, MAC-адрес заносится в ARPтаблицу. Рассмотрим Атаку«ARP–spoofing». Анализ безопасности протокола ARP показывает, что еслиперехватить на атакующем хосте данного сегмента,широковещательныйARP запрос, то можно подменить ARP- ответ, тем самым объявить себя искомым хостом, и трафик будет идти через нас. Рассмотрим такую ситуацию, что злоумышленник, находясь в одной локальной сети с пользователем и ожидая его ARP запрос, то есть трафик, который злоумышленник хочет контролировать. Когда злоумышленник видит ARP запрос он старается ответить на этот запрос ложным ARP ответом, то есть подменить MAC-адрес хоста, который запрашивал пользователь, после этого узел, который будет атакован занесет в свою ARP-таблицу ложный Mac- адрес и будет слать пакеты злоумышленнику. Такую атаку производят, как и на пользователя так и на маршрутизатор.[1]/

На рис.1 показана схема контроля всего трафик атакуемого, атаки идут сразу на два узла на маршрутизатор и на атакуемый хост путем посылки ложныхARP ответов на ARP запросы которых как правило даже и не было. Рассмотрим пример реализации атаки в операционной системе «Kalilinux».



На рис.1 Показана атака на два узла.

Для реализации атаки используются специализированные программы. В основном написанные злоумышленниками. Для начала нужно проверить работает операционная система в режиме маршрутизатора.Для того что бы это проверить используется следующая команда: «Sysctlnet.ipv4.ip_forward». Если в ответ будет равен «0» это говорит о том, что режим выключен. Для включения используем эту команду«Sysctl -wnet.ipv4.ip_forward=1». Для проведения атаки ARP-spoof есть специальный инструменты, их много рассмотрим некоторые из них. Рассмотрим программу «Arpspoof» в консоли вводим «arpspoof -ieth0 -t[ip жертвы] -r [ip как правило маршрутизатора]» где -i — указывает интерфейс, -t — указывает IP-адрес хоста, -r указывает arpspoof «отравлять» arp-кэш обеих хостов.После этой команды посылаются ARP-пакеты на маршрутизатор в которых подменяются MAC адреса. В итоге мы получаем трафик чужого узла. Для просмотра пакетов можно использовать программу «wireshark». Неудобства утилиты «arpspoofing» в том, что программа умеет одновременно производить атаку только для двух хостов, для того чтобы производить атаку на несколько хостов надо открывать новый терминал и это неудобно. Рассмотрим другую программу под названием «Ettercap».[8] Очень мощное средство для проведения атак типа Man-in-the-Middle.Есть два интерфейса: консольный и графический. Поддержка плагинов, фильтров. Поддержка разных типов атак. Реализация в консоли, прописываем «Ettercap –Ieth0 –T –q –MARP /192.168.1.1// /192.168.1.36//» где, -i использоватьэтот сетевой интерфейс, -Tиспользовать только текстовый интерфейс, -q не показывать содержимое пакетов. –Мвыполнить атаку mitm. Другой вариант атаки «Ettercap –Ieth0 –T –q –MARP /192.168.1.1// ///» атака будет производиться по всей подсети, злоумышленник будет перехватывать трафик во всей подсети в которой он находится. В программе имеются очень полезные плагины. Рассмотрим плагин под названием «autoadd - автоматическое добавление новых жертв по мере их подключения к ARP». По умолчания утилита поддерживает 33 плагина, но это не предел так же можно написать свой плагин. Пример использования плагина. «Ettercap –Ieth0 –T –q –Pautoadd –MARP /192.168.1.1// ///» где -P запустить этот плагин.После того как мы запускаем атаку Ettercap сканирует все узлы, которые доступны и начинает их подменять, и если после некоторого времени появляется новый узел, то с этим плагином он будет добавлен в список к остальным узлам для подмены.[5] В программе также присутствуют так называемые «Фильтры». Фильтры нужны что бы;отсеивать только тот трафик, который нужен и в реальном времени вмешиваться в трафик (напр. Изменение картинок в веб страницы, понижение версии протокола такого как SSH(англ. SecureShell — «безопасная оболочка»).

Защита от атакиARP-spoofing. Рассмотрим два способа защиты от такого рода атак; введение статистической ARP таблицы и программно-аппаратный. Первый способ является одним из надежных решений по защите от ARP-spoofing. Заключается в введение статической ARP-таблицы. Задача очень трудная так как надо знать все узлы, IP-адреса и сопоставлять IP- адреса к MAC- адресам. Очень кропотливая работа, которая требует много времени, усилий и затрат. Так же надо отключиться динамическую поддержку ARP таблиц на ключевых узлах. Если говорить о программном способе, то это программа «arpwatch» единственная в своем роде которая позволяет наблюдать за такими атаками, обычно ставится на ключевые узлы напр. сервер. Существует и программно-аппаратный комплекс «Система обнаружения вторжений(СОВ) (англ. Intrusion detection system, IDS)» и

«Системапредотвращениявторжений (англ. IntrusionPreventionSystem, IPS)».Обычно ставится на критичные сегменты сети который выявляет атаки на сеть в том числе ARP-spoofingатаки. Различия IDS от IPS. IDS занимается только обнаружением атак, а IPS это более интеллектуальная система, она обнаруживает атаки и защищает от них.Атака детектируется, достаточно посмотреть в ARP таблицу и увидеть несоответствия. [6]

DNS-spoofingDNS-алгоритм удаленного поиска IP-адреса по имени в сети Internet.Хост посылает на IP-адрес ближайшего DNS-сервера (он, как правило, устанавливается при настройке сетевой ОС) DNS-запрос, в котором указывает имя сервера, IP-адрес которого необходимо найти.DNS-сервер, получив такое сообщение, ищет в своей базе «имен» указанное имя. Если указанное в запросе имя найдено, а, следовательно, найден и соответствующий ему IP-адрес, то DNS-сервер отправляет на хост DNS-ответ, в котором указывает искомый IP-адрес. Если же DNS-сервер не обнаружил такого имени в своей базе имен, то он пересылает DNS-запрос на один из ответственных за домены верхнего уровня DNS-серверов, адреса которых содержатся в файле настроек DNS-сервера, и описанная в этом пункте процедура повторяется, пока имя не будет найдено (или будет не найдено).[2] Существует 3 варианта удалённой атаки на DNS.Перехват DNS-запроса, направленный шторм ложных DNS-ответов на атакуемый хост, перехват DNS-запроса или создание направленного шторма ложных DNS-ответов на DNS-сервер. Рассмотрим перехват DNS запросов. Сначала злоумышленник ожидает DNS-запрос после получения запроса задача злоумышленника ответить на этот запрос где указать вместо реального IP-адреса хост ложного DNS-сервера (может быть узел атакующего, другой узел сети, несуществующий узел (чем может повлечь за собой ту самую «DOS (от англ. DenialofService — отказ в обслуживании)-атаку»)). Таким образом для атакующего хоста ложный DNS-сервер выглядит как настоящий сервер. Необходимые условия для проведения данной атаки; возможность перехвата DNS-запроса, знать с какого порта был послан запрос, transactionID (идентификатор в заголовке DNS ответов). Рассмотрим пример атаки DNS-spoofing. [4] Пользователь хочет попасть на сайт банка, в котором он обслуживается. Для этого в поисковой системе браузера он вводит наименования банка. После этого браузер пользователя посылает запрос на DNS-сервер: «на каком IP-адресе находится банк». В ответ на запрос DNS- сервер определяет на каком IP-адресе находится банк. В результате этого пользователь заходит на сайт и производит необходимые действия с банком: перевод средств, оплата счетовит.д.Представим ситуацию что пользователь находитесь в кафе, в котором существует открытая точкаWI-FI-сети. В одном кафе с пользователем сидит злоумышленник, и он организовал на негоARP-spoofing атаку и сделал ему подмену DNS. Он заходите 6на банк, которым пользуется, браузер отправляет запрос DNS –серверу «какой IP-адрес у банка» в ответ приходит IP-адрес, где злоумышленник уже развернул точную копию банка. Таким образом пользователь считает, что он находится на сайте банка, а в действительности сайт банка подменен и злоумышленник имеет возможность завладеть персональными данными пользователя и использовать по своему назначению. Рассмотрим реализация в Kalilinux: пример реализации с помощью утилита «dnsspoof» которая подменяет IP-адрес узла на свой.Для реализации атаки надо сначала произвести атаку ARP-spoofing. Также должен быть запущен сервер, например, «Apache HTTP-сервер». При попыткеперейти на любой сайт, пользователь будем перенаправлены на «Apache HTTP-сервер». Для удобства реализации атаки есть файл где мы можем указать IP-адрес и доменное имя какое нужно подменить, для того что бы перенаправлять только определённые сайты. Для начала атаки необходимо в консоли написать «dnsspoof» и атака запустится. Так же DNS –spoof можно реализовать в Ettercap с помощью плагина «dns_spoof». Рассмотрим второй вариант удаленной атаки «Шторм ложных DNS-ответов». Постоянная передача злоумышленником ложных DNS- ответов на различные UDP-запросы атакуемого хоста и с различными ID от имени (с IP-адреса) и будет происходить подмена настоящего IP-адреса на ложный, которым будет являться IP-адрес ложного сервера – хоста атакующего. Как говорилось ранее есть определенные требования к такому виду атаки, нужно направлять ответы на тот же порт с которого был отправлен запрос и знать transactionID. Рассмотрим третий вариант «перехват DNS-запроса или создание направленного шторма ложных DNS-ответов на DNS-сервер».[9]В этом варианте объедены первый и второй случай, атака может реализоваться не только когда мы находимся в клиентской сети, а, например, между двумя DNS –серверами. Когда пользователь обращается к DNS-серверу, а он не знает где находится IP-адрес сайта, то он обращается к другому DNS-серверу. Тут злоумышленник может перехватить DNS-запрос и ответить, подменив IP-адрес или также организовать шторм ложных DNS-ответов. DNS-сервер отправляет запрос другому DNS-серверу с 53 порта. Злоумышленнику заранее известен порт отправителя, ему только остается перебрать transaction ID.[3]

Защита от атаки DNS-spoofing.Если злоумышленник находится в локальной сети жертвы, то защититься от такой атаки очень тяжело. Так как нужно знать реальный IP-адрес сайтов.

Заключение. Таким образом в статье проведён анализ возможностей реализации сетевых атак. Рассмотрены примеры активных сетевых атак, а также методы защиты от них. В заключении стоит отметить что сетевые атаки реализуются достаточно просто, а защита от них не всегда представляется возможным. Результаты проведенного анализа могут быть полезны как для рядовых пользователей, так и для специалистов информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Медведовский И.Д., Семьянов П. В., Леонов Д.Г. Атака на Internet - Изд.Litres, 2017
2. Красов А.В., Левин М.В. Возможности управления трафиком в рамках концепции SDN// Актуальные проблемы инфотелекоммуникаций в науке и образовании IV. 2 тома, г.2015 с. 350-354
3. Алейников А.А., Билятдинов К.З., Красов А.В., Левин М.В. Контроль измерение и интеллектуальное управление трафиком. СПБ г.2016.
4. Красов А.В., Левин М.В., Штеренберг С.И., Исаченков П.А. Методология управления потоками трафика в программно-определяемой адаптивной сети. СПБ. Г.2016. № 4. С. 3-8.
5. Красов А.В., Левин М.В., Штеренберг С.И., Исаченков П.А. Модель управления потоками трафика в программно-определяемой сети с изменяющейся нагрузкой. 2016. Т. 8. № 4. С. 70-74.
6. Красов А.В., Сахаров Д.В., Ушаков И.А., Лосин Е.П. Обеспечения безопасности передачи MULTICAST-трафика в IP-сетях. // Защита информации. Инсайд г.2017. № 3 (75). С. 34-42.
7. Кунегина С.В. Обеспечение информационной безопасности в сетях IP[Электронный ресурс].http://kunegin.com/ref3/ip-sec/remote1.htm(дата обращения: 22.09.2017).
8. Алейников А.А., Билятдинов К.З., Красов А.В., Кривчун Е.А., Крысанов А.В. Технические аспекты управления с использованием сети интернет. СПБ г. 2016.
9. Красов А.В., Левин М.В., Цветков А.Ю. Управления сетями передачи данных с изменяющейся нагрузкой. 2015. № 1. С. 141-146.

МОЛОДЕЖНЫЕ НАУЧНЫЕ ШКОЛЫ: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОБЛЕМЫ УСТОЙЧИВОГО РАЗВИТИЯ

УДК 004.056.53

ИССЛЕДОВАНИЕ УЯЗВИМОСТИ СЕРИАЛИЗАЦИИ И ДЕСЕРИАЛИЗАЦИИ ДАННЫХ В JAVA

Шариков Павел Иванович[1], Красов Андрей Владимирович[2]
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича,
Россия, Санкт-Петербург, пр. Большевиков 22 к.1,
emails: sharikov.pavel@ro.ru, krasov@inbox.ru

***Аннотация*:** В статье данной статье исследована проблема уязвимости при сериализации и десериализации данных в Java. Дается общее представление о принципах работы сериализации в языке программирования. Рассмотрены реальные примеры, показывающие в какие моменты приложение использующее сериализацию уязвимо. Произведен разбор уязвимости, варианты в которых она возникает. Разработан алгоритм поиска уязвимых файлов в проекте, даны рекомендации по исправлению уязвимых мест приложения.

***Ключевые слова**: сериализация Java; десериализация Java; уязвимость; байт-код; исполняемые файл; защита авторских прав;*

INVESTIGATION OF VULNERABILITY OF SERILIZATION AND DESERIALIZATION OF DATA IN JAVA

Sharikov Pavel[1], Krasov Andrey[2]
St. Petersburg State University of Telecommunications of the prof. M. A. Bonch-Bruyevich,
Russia, St. Petersburg, prosp. Bolshevikov Street 22 building 1,
emails: sharikov.pavel@ro.ru, krasov@inbox.ru

Abstract: This article investigates the vulnerability in data serialization and deserialization in Java. We give a general idea of the principles of serialization in the programming language. Real examples are considered, showing at what moments the application using serialization is vulnerable. The vulnerability has been parsed, the variants in which it arises. The algorithm for searching for vulnerable files in the project is developed, recommendations for correcting vulnerabilities of the application are given.

***Keywords:** serilization Java; deserialization Java; vulnerability; bytecode; portable executable file; copyright protection;*

Введение. В данный момент Java один из самых популярных языков программирования. На этом языке написано огромное количество приложений и крупных коммерческих проектов. Например, таких как: Jenkins, Web Sphere, Web Logic, JBoss и другие. Java используется в банках, кассовых терминалах и еще во многих сферах жизни и бизнеса.

Десериализованные (unserialize) уязвимости – это класс уязвимостей. Большинство языков программирования предоставляют пользователям встроенные возможности для вывода данных приложения на локальный диск или передавать их по сети. Процесс преобразования данных приложения в другой формат (чаще всего двоичный), подходящий для транспортировки, называется сериализацией. Процесс чтения данных после того, как они были сериализованы, называется десериализация.

Уязвимости, которые мы далее будем исследовать, возникают, когда разработчики приложений на java пишут код, который принимает сериализованные данные от пользователей и производится попытка десериализации этих данных для дальнейшео использования их в программном продукте. В зависимости от языка программирования, это может привести различного рода последствиям.

Сереализация в Java. Десериализированные уязвимости полностью зависят от языка. В данном разделе мы рассмотрим примеры работы данных уязвимостей в Java. Также разберем, почему уязвимость, не подвергаемая кэшированию в любой из тысяч библиотек, загружаемых вашим приложением (даже библиотеки, которые вы не используете) может существенно повлиять на работоспособность вашего приложения.

Как описано выше, сериализация – это процесс, с помощью которого язык программирования, используемый вами для написания приложения, позволяет преобразовывать данные в статический двоичный формат, подходящий для сохранения данных на жесткий диск или отправки их по сети.

Десериализация – процесс противоположный. Данная функция принимает двоичные данные и преобразует их обратно в тот вид, в котором вы можете их использовать. Рассмотрим пример находящийся в Листинге 1, который показывает, как можно использовать сериализацию.

Листинг 1. Пример сериализации

```
public class SerializeTest{
   public static void main(String args[]) throws Exception{
      //Это объект, который мы хотим сериализовать
      String name = "bob";
      //Мы будем записывать сериализованные данные в файл "name.ser"
      FileOutputStream fos = new FileOutputStream("name.ser");
      ObjectOutputStream os = new ObjectOutputStream(fos);
      os.writeObject(name);
      os.close();

      //Чтение сериализованных данных из файла "name.ser"
      FileInputStream fis = new FileInputStream("name.ser");
      ObjectInputStream ois = new ObjectInputStream(fis);
      //Чтение объекта из потока данных и преобразование его обратно в строку
      String nameFromDisk = (String)ois.readObject();
      //Печать результатов в консоль
      System.out.println(nameFromDisk);
      ois.close();
   }
}
```

Код вышеприведенного листинга просто записывает строчку «bob» в файл на диск с помощью сериализуемого интерфейса java. Затем считывает его и выводит результат в консоль. Ниже в листинге 2, показан вывод в консоль после выполнения кода из листинга 1.

Листинг 2. Вывод результата работы кода

```
breens@us-l-breens:~/Desktop/SerialTest$ java SerializeTest
bob
breens@us-l-breens:~/Desktop/SerialTest$ xxd name.ser
0000000: aced 0005 7400 0362 6f62 ....t..bob
```

Обратите внимание, что файл на диске является двоичным и у него есть некоторые «непечатаемые» символы. В частности, байты «aced 0005» - это так называемые «magic byte», которые находятся вначале любого java-сериализованного объекта. Данный пример хорошо демонстрирует работу сериализации и десериализации в java.

Сериализация и объекты в Java. Java – это объектно-ориентированный язык программирования, поэтому в нем существует концепция объектов. Например, String является объектом, благодаря этому мы можем узнавать длину строки, которую хранит объект. Рассмотрим нижеприведенный код, находящийся в листинге 3.

Листинг 3. Пример более сложной сериализации

```
public class SerializeTest{

   public static void main(String args[]) throws Exception{
      //Это объект который мы хотим сериализовать
      MyObject myObj = new MyObject();
      myObj.name = "bob";

      //Запись сериализованных данных в файл "object.ser"
      FileOutputStream fos = new FileOutputStream("object.ser");
      ObjectOutputStream os = new ObjectOutputStream(fos);
      os.writeObject(myObj);
      os.close();

      //Чтение сериализованных данных из файла "object.ser"
      FileInputStream fis = new FileInputStream("object.ser");
      ObjectInputStream ois = new ObjectInputStream(fis);

      // Чтение объекта из потока данных и преобразование его обратно в строку
      MyObject objectFromDisk = (MyObject)ois.readObject();
```

```
            //Печать результата
            System.out.println(objectFromDisk.name);
            ois.close();
        }
    }

    class MyObject implements Serializable{
        public String name;
        private void readObject(java.io.ObjectInputStream in) throws IOException,
ClassNotFoundException{
            in.defaultReadObject();
            this.name = this.name+"!";
        }
    }
```

Теперь рассмотрим результат выполнения данного кода в листинге 4.

Листинг 4. Результат выполнения кода из листинга 3

```
breens@us-l-breens:~/Desktop/SerialTest$ java SerializeTest
bob!
breens@us-l-breens:~/Desktop/SerialTest$ xxd object.ser
0000000: aced 0005 7372 0008 4d79 4f62 6a65 6374 ....sr..MyObject
0000010: cf7a 75c5 5dba f698 0200 014c 0004 6e61 .zu.]......L..na
0000020: 6d65 7400 124c 6a61 7661 2f6c 616e 672f met..Ljava/lang/
0000030: 5374 7269 6e67 3b78 7074 0003 626f 62 String;xpt..bob
```

Разберем, что происходит в выводе после работы программы и почему уже на данном этапе можно говорить о «магии». Приведенный выше код очень похож на тот, который мы разбирали в листинге 1, за исключением того, что в данном примере сериализуемый объект определяется самим пользователем и называется «MyObject». Класс «MyObject» реализует интерфейс «serializable» java и определяет метод «readObject».

Теперь, изучая результат работы программы, мы можем увидеть, что в выводе находится находится информация, которая, как нам кажется, не соответствует действительности. Вместо имени, которое мы определили в строке «bob», программа напечатала в консоли «bob!». Кроме того, если мы читаем вывод из «xxd», чтобы увидеть, что было записано на диск, мы не видим никаких следов записи восклицательного знака. Так откуда же взялся восклицательный знак?

Ключевым моментом является метод readObject. Когда java читает сериализованный объект, первое, что она делает после чтения в необработанный байтах – это вызов пользовательского метода readObject, если он существует. В этом случае метод readObject добавляет восклицательный знак к имени, содержащемуся в строке.

Где используется сериализация. Java использует сериализацию практически повсеместно.

– В запросах HTTP – Параметры, ViewState, Cookies.
– RMI – широко используемый протокол java RMI на 100% основан на сериализации
– RMI через HTTP. Многие веб-приложения с «толмтым» клиентом используют это.
– JMX – Полностью полагается на сериализованные объекты
– Пользовательские протоколы. Отправка получаемых необработанных объектов Java является нормой, которую мы увидим в некоторых примерах.

Может ли приложение быть уязвимым.

Уязвимость была привнесена из-за того, что библиотека некорректно санирует вводимые пользователем данные. Атакующий может добавить вредоносный код, и он будет принят и выполнен.

Приложение уже может быть в списке уязвимых, если оно или одна из подключаемых библиотек использует библиотеку commons-collections.jar. Если библиотека просто присутствует в проекте, не находится в classpath и нигде не используется, риск уязвимости приложения снижается практически до минимума. Если библиотека есть и используется, то приложение в зоне риска. Для эксплуатации достаточно, чтобы библиотека была в classpath.

Поиск уязвимости. Защита. Итак, мы нашли приложение или сервер с приложениями, который поставляется в комплекте с уязвимой библиотекой.

Что мы ищем? Первое, что необходимо сделать – это найти ту часть приложения, в которой используется каким-либо образом сериализованный объект. Чтобы найти эту часть достаточно будет посмотреть на hexdump вашего приложения. Обычно существуют два отдельных объекта. Один из них шифруется base64, показывается в самом правом столбце и начинается с «rO0AB». Другой – это двоичный код, поэтому нам нужен шестнадцатеричный столбец. Он начинается с байтов «ac ed 00 05 73 72». Именно так выглядят сериализованные объекты java, они идентифицированы этими

заголовками и всегда начинаются с «ac ed 00 05 73 72», а после того, как это шифруется base64, то выдается как «rO0 ….». Необходимо следить за данными двумя строками. Также необходимо узнать, с какими портами работает ваше приложение или какие порты оно «слушает», ждет данных. Если среди используемых портов находится порт 1099, то это библиотека Java RMI, которая по определению использует сериализованные объекты для коммуникации. Это уязвимо.

Многие заграничные специалисты предлагают просто удалить уязвимые классы из библиотеки apache commons-collections и продолжать работать без них. Но это поверхностный подход. В среднем на проект подключается больше 10 библиотек и минимум 3-4 из них используют библиотеку с уязвимостью. А такие большие проекты, как Web Sphere, JBoss полностью завязаны на сериализации, поэтому необходимо делать исправления для каждой используемой библиотеки.

Первое, что необходимо сделать, если вы подозреваете, что ваше приложение уязвимо, необходимо развернуть его в тестовой среде, «песочнице».

Листинг 5. Команда для идентификации пакетов

```
root@us-l-breens:/opt/apache-tomcat-8.0.28# grep -Rl InvokerTransformer .
./webapps/ROOT/WEB-INF/lib/commons-collections-3.2.1.jar
```

Эта команда идентифицирует любые jar файлы или классы в вашем проекте, которые содержат уязвимую библиотеку. Можно удалить все связанные файлы, но после такого шага вашему приложению понадобится провести очень тщательное тестирование.

Другой подход для устранения уязвимости заключается в удалении класса «InvokeTransformer». Если мы удалим этот class-файл везде, где есть любые попытки его использования, то попытки использования уязвимости должны завершиться неудачей. Для этого необходимо открывать свои файлы jar с помощью таких утилит, как: Winzip, winrar и других. После это «пройти» в каталог «org/apache/commons/collections/functors/InvokerTransformer.class» и удалить необходимый class-файл.

Выводы. Необходимо крайне тщательно проверять использование сериализации и десериализации в вашем проекте.

Помнить, что при загрузке сериализованного объекта в приложение, десериализуется он в оперативной памяти и там может выполниться любой вредоносный код, который вы даже не заметите.

Проверить ваше приложение на использование библиотеки apache commons-collections. Если вы используете в вашем проекте продукты от таких гигантов, как Jenkins, Web Sphere, Web Logic, JBoss необходимо произвести поиск найти на их официальных сайтах «заплатки» или временного исправления данной уязвимости для их программного обеспечения.

Если вы все таки используете сериализацию в проекте, достаточно проверить весь проект на использование или любое обращение к классу InvokerTransformer.class. После переписать весь проект без использования данного класса и удалить этот класс из jar файла: «org/apache/commons/collections/functors/InvokerTransformer.class».

СПИСОК ЛИТЕРАТУРЫ

1. Красов А.В., Верещагин А.С., Цветков А.Ю. Аутентификация программного обеспечения при помощи вложения цифровых водяных знаков в исполняемый код // Телекоммуникации. 2013, №S7. С.27-29.
2. Shterenber S.I., Krasov A.V., Ushakov I.A. Analysis of using equivalent instructions at the hidden embedding of information into the executable files // Journal of Theoretical and Applied Information Technology. Т.80, 2015, №1. P.28-34.
3. 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.
4. Шариков П.И., Красов А.В., Штеренберг С.И. Методика создания и вложения цифрового водяного знака в исполняемые java файлы на основе замен опкодов // T-Comm: Телекоммуникации и транспорт. Т.11, 2017, №3. С. 66-70.
5. Красов А.В, Шариков П.И. Методика защиты байт-кода Java-программы от декомпиляции и хищения исходного кода злоумышленником // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. №1, 2017. С. 47-50.
6. Хомяков И.Н., Красов А.В. Возможность скрытого вложения информации в байт-код java // Информационные технологии моделирования и управления. №2(86), 2014. С. 185-191

ОГЛАВЛЕНИЕ

ГОСУДАРСТВЕННАЯ ПОЛИТИКА В СФЕРЕ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 5

ВЛИЯНИЕ СЕКЬЮРИТИЗАЦИИ НА ПОЛИТИКУ РОССИИ: ИНФОРМАЦИОННЫЙ АСПЕКТ
Баранов Николай Алексеевич 5

РЕЗУЛЬТАТИВНОСТЬ ИНСТРУМЕНТОВ ЭЛЕКТРОННОГО УЧАСТИЯ В РОССИИ ПРИ ФОРМИРОВАНИИ ПОЛИТИЧЕСКИХ РЕШЕНИЙ
Видясова Людмила Александровна, Тенсина Ярослава Дмитриевна 10

ГОСУДАРСТВЕННАЯ ПОЛИТИКА В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕВЕРО-ЗАПАДНОМ ФЕДЕРАЛЬНОМ ОКРУГЕ
Кучерявый Михаил Михайлович, Вовенда Юлия Владимировна 14

ОБЕСПЕЧЕНИЕ КАДРОВОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ ВЫСОКОТЕХНОЛОГИЧНЫХ ОТРАСЛЕЙ
Советов Борис Яковлевич, Касаткин Виктор Викторович 17

ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И ТЕХНОЛОГИИ 20

СИСТЕМАТИЧЕСКАЯ ПРОЦЕДУРА ПРИМЕНЕНИЯ МЕТОДА ДВУХМОМЕНТНОЙ АППРОКСИМАЦИИ ДЛЯ ОПРЕДЕЛЕНИЯ ФУНКЦИИ РАСПРЕДЕЛЕНИЯ ВРЕМЕНИ РЕАЛИЗАЦИИ СТОХАСТИЧЕСКОЙ СЕТИ
Канаев Андрей Константинович, Карабанов Юрий Сергеевич, Привалов Андрей Андреевич 20

ПРИМЕНЕНИЕ РОЛЕВОЙ МОДЕЛИ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ В МЕЖМАШИННЫХ СЕТЯХ ДИНАМИЧЕСКОЙ ТОПОЛОГИИ
Калинин Максим Олегович, Резединова Евгения Юрьевна 25

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ ИНФОРАСТРУКТУРЫ РФ ОТ КИБЕРАТАК
Мошак Николай Николаевич, Евсейко Константин Владиславович, Логинцев Александр Владимирович 31

МЕТОДЫ РАСЧЕТА КВАНТИЛЕЙ РАСПРЕДЕЛЕНИЯ СЛУЧАЙНОЙ СЕТЕВОЙ ЗАДЕРЖКИ ПАКЕТОВ ИЗОХРОННОГО ТРАФИКА В ЗАДАЧЕ АНАЛИЗА ИНФОКОММУНИКАЦИОННЫХ ТРАНСПОРТНЫХ СИСТЕМ
Мошак Николай Николаевич, Логинцев Александр Владимирович 36

ВАРИАНТ ФОРМИРОВАНИЯ АНСАМБЛЯ ДИСКРЕТНЫХ ОРТОГОНАЛЬНЫХ СИГНАЛОВ С ТРЕБУЕМЫМИ ПАРАМЕТРАМИ СТРУКТУРНОЙ СКРЫТНОСТИ
Сазонов Виктор Викторович, Беззубов Олег Владимирович,Мосягин Дмитрий Евгеньевич 42

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ
Пиюков Олег Юрьевич, Гвоздков Игорь Вячеславович 44

ВОПРОСЫ ВНЕДРЕНИЯ ТЕХНОЛОГИИ ЦИФРОВОГО ВИДЕО В ДЕЯТЕЛЬНОСТЬ ПОЛИЦИИ
Шалагинова Ольга Борисовна 46

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ 48

ДВУХМОДУЛЬНЫЕ КОДЫ С СУММИРОВАНИЕМ В ЭКСПЕРИМЕНТЕ ПО АНАЛИЗУ СТРУКТУРНОЙ ИЗБЫТОЧНОСТИ СИСТЕМ ФУНКЦИОНАЛЬНОГО КОНТРОЛЯ
Ефанов Дмитрий Викторович, Щагина Владислава Александровна 48

ЗАЩИТА ИНФОРМАЦИИ И ЧЕЛОВЕЧЕСКИЙ ФАКТОР
Карташов Павел Николаевич 54

ИНФОРМАЦИОННО-КОММУНИКАТИВНЫЕ ТЕХНОЛОГИИ КАК ИНСТРУМЕНТАЛЬНАЯ СРЕДА ПОДДЕРЖКИ УЧЕБНОГО ПРОЦЕССА
Колоколова Лидия Петровна 57

ФОРМИРОВАНИЕ ЭКЗЕМПЛЯРОВ ОНТОЛОГИЧЕСКИХ КЛАССОВ ПРИ ОБРАБОТКЕ НЕСТРУКТУРИРОВАННЫХ ДАННЫХ В РЕШЕНИИ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Полтавцева Мария Анатольевна, Печенкин Александр Игоревич 60

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СЕТИ ИНТЕРНЕТА ВЕЩЕЙ СРЕДСТВАМИ НИЗКОРЕСУРСНОЙ КРИПТОГРАФИИ
Супрун Александр Федорович, Царьков Игорь Сергеевич 64

ПЕДАГОГИЧЕСКИЕ И ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОГО ТЕСТИРОВАНИЯ НА РАЗНЫХ СТАДИЯХ ОБУЧЕНИЯ ДИСЦИПЛИНЕ
Титова Юлияна Францевна 68

МОДЕЛИРОВАНИЕ УЯЗВИМОСТЕЙ В СИСТЕМЕ БЕЗОПАСНОСТИ
Шипилева Алла Владимировна 74

СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ 77

ПРИМЕНЕНИЕ ПСЕВДОВЕРОЯТНОСТНОГО ЗАЩИТНОГО ПРЕОБРАЗОВАНИЯ В ТЕХНОЛОГИИ ТАЙНОГО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ
Вайчикаускас Мария Александровна, Татчина Яна Александровна, Синев Валерий Евгеньевич 77

КОНТРОЛЬ ФУНКЦИОНАЛЬНОГО СОСТОЯНИЯ ЧЕЛОВЕКА-ОПЕРАТОРА И ЕГО КОРРЕКЦИЯ КАК МЕТОД ПОВЫШЕНИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ НА РАБОЧЕМ МЕСТЕ
Колмаков Сергей Александрович 79

БЕЗОПАСНОСТЬ И ЮЗАБИЛИТИ СОВРЕМЕННЫХ ПОЛЬЗОВАТЕЛЬСКИХ ИНТЕРФЕЙСОВ
Леонов Антон Викторович 83

ПОДХОД К ФОРМИРОВАНИЮ МОТИВОВ ПЕРЕМЕЩЕНИЙ СОТРУДНИКОВ ВНУТРИ ОРГАНИЗАЦИИ
Новикова Евгения Сергеевна, Бекенева Яна Андреевна 86

МЕТОД РАНДОМИЗИРОВАННЫХ СВОДНЫХ ПОКАЗАТЕЛЕЙ ДЛЯ ЭКСПЕРТНОЙ ОЦЕНКИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ
Попова Елена Владимировна 89

ОРГАНИЗАЦИЯ ДРЕВОВИДНЫХ ХРАНИЛИЩ ДАННЫХ С УЧЁТОМ РАЗМЕЩЕНИЯ В НИХ ЭЛЕКТРОННЫХ ПОДПИСЕЙ
Романова Юлия Николаевна, Янюшкин Константин Александрович 92

СОЗДАНИЕ ПЕРИМЕТРА БЕЗОПАСНОСТИ В ОБЛАЧНОЙ СРЕДЕ
Рыжков Сергей Романович 94

МЕТОДИКИ И ИНСТРУМЕНТЫ АУДИТА СЕТЕВОЙ БЕЗОПАСНОСТИ
Садикова Анастасия Александровна, Титова Юлия Алексеевна, Савков Сергей Витальевич 97

КОМПЛЕКСНАЯ СИСТЕМА ИНЖЕНЕРНО ТЕХНИЧЕСКОЙ ЗАЩИТЫ КАБИНЕТА РУКОВОДИТЕЛЯ. ЭФФЕКТИВНОСТЬ РАБОТЫ ПРИБОРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ КОМПЛЕКСНОЙ СИСТЕМЫ ИНЖЕНЕРНО ТЕХНИЧЕСКОЙ ЗАЩИТЫ КАБИНЕТА РУКОВОДИТЕЛЯ
Фаязов Кобилджон Абдукаюмович 102

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 107

ИНСТРУМЕНТАЛЬНОЕ СРЕДСТВО ВИЗУАЛИЗАЦИИ МАРШРУТОВ ВЫПОЛНЕНИЯ КОМПЬЮТЕРНЫХ ПРОГРАММ
Безруков Вячеслав Алексеевич, Синещук Юрий Иванович,,, Синещук Максим Юрьевич 107

ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ СВЯЗИ
Вилков Валерий Борисович, Сычев Сергей Евгеньевичвич, Черных Андрей Климентьевич 111

О СОЦИАЛЬНЫХ СЕТЯХ ВУЗОВ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Кононов Олег Александрович, Кононова Ольга Васильевна 115

ПЕДАГОГИЧЕСКИЕ КОММУНИКАЦИИ В СОВРЕМЕННОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ
Костюк Анатолий Владимирович 119

МОДЕЛЬ ФОРМИРОВАНИЯ ТРЕБОВАНИЙ К КОНФИДЕНЦИАЛЬНОСТИ, ЦЕЛОСТНОСТИ И ДОСТУПНОСТИ ДАННЫХ В СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ
Куватов Валерий Ильич, Примакин Алексей Иванович 122

СУБЪЕКТНЫЙ СОСТАВ ПРАВООТНОШЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ
Лепёхин Александр Николаевич 126

О МЕТОДЕ ИДЕНТИФИКАЦИИ БЕСПИЛОТНЫХ ВОЗДУШНЫХ СУДОВ ПРИ РЕАЛИЗАЦИИ КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ
Беляев Сергей Алексеевич, Остапченко Юрий Борисович, Кудряков Сергей Алексеевич, Рубцов Евгений Андреевич 127

ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ 131

ФУНКЦИОНАЛЬНАЯ НАДЕЖНОСТЬ И УСТОЙЧИВОСТЬ ВЫЧИСЛИТЕЛЬНОГО ПРОЦЕССА
Богатырев Владимир Анатольевич, Богатырев Станислав Владимирович 131

АНАЛИЗ ОБЛАСТЕЙ ПРИМЕНЕНИЯ АРОМОСЕНСОРНЫХ СИСТЕМ БЕЗОПАСНОСТИ
Дмитрий Сергеевич Афанасьев, Елена Андреевна Бардакова, Денис Сергеевич Быстряков 133

ОПТИМИЗАЦИЯ ПЕРИОДИЧНОСТЬ ТЕСТОВОГО КОНТРОЛЯ ПРИ ОБЕСПЕЧЕНИИ ГОТОВНОСТИ СИСТЕМЫ К БЕЗОПАСНОМУ ФУНКЦИОНИРОВАНИЮ
Богатырев Владимир Анатольевич, Богатырев Станислав Владимирович 136

МОДЕЛЬ ДОСТУПА СЕНСОРНЫХ УСТРОЙСТВ В «ТУМАННЫХ ВЫЧИСЛЕНИЯХ» ИНТЕРНЕТА ВЕЩЕЙ
Елизаров Максим Андреевич 139

ОЦЕНКА И ПРОГНОЗИРОВАНИЯ РИСКОВ ДЛЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Капанов Алексей Александрович, Мещеряков Евгений Евгеньевич, Косолапов Владимир Викторович, Астахова Татьяна Николаевна 142

ПАРАДИГМЫ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ: ЕДИНСТВО И ОТЛИЧИЯ
Кутузов Олег Иванович, Татарникова Татьяна Михайловна 144

ФОРМИРОВАНИЕ И ИСПОЛЬЗОВАНИЕ В УЧЕБНОМ ПРОЦЕССЕ СИТУАЦИОННОГО ЦЕНТРА ДЕЛОВОЙ РАЗВЕДКИ
Левкин Игорь Михайлович, Микадзе Сергей Юрьевич 148

ОСОБЕННОСТИ МОДЕЛИРОВАНИЕ САМОПОДОБНОГО СЕТЕВОГО ТРАФИКА
Татарникова Татьяна Михайловна 151

МЕТОДИКА ПРОЕКТИРОВАНИЯ ГИС КОРАБЛЯ
Яготинцева Наталья Владимировна 155

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ИМПОРТОЗАМЕЩЕНИЕ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ 160

ФОРМИРОВАНИЕ ТРЕБОВАНИЙ К ОЦЕНКЕ ДОВЕРИЯ КРИТИЧНЫХ ОБЪЕКТОВ НА БАЗЕ СОВРЕМЕННЫХ СТАНДАРТОВ ИСО
Лившиц Илья Иосифович, Маликов Владимир Викторович 164

ОЦЕНКА ВЛИЯНИЯ СОВРЕМЕННЫХ РИСК-ОРИЕНТИРОВАННЫХ СТАНДАРТОВ НА ОБЕСПЕЧЕНИЕ ИБ КРИТИЧНЫХ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ
Лившиц Илья Иосифович, Маликов Владимир Викторович 167

МОДЕЛИРОВАНИЕ ГИБРИДНОГО ПРОТОКОЛА МАРШРУТИЗАЦИИ В БЕСПРОВОДНОЙ СЕТИ
Молокович Игорь Аркадьевич 170

СОВРЕМЕННЫЙ ПОДХОД К ВЫЯВЛЕНИЮ И УПРАВЛЕНИЮ МЕДИЦИНСКИМИ СИГНАЛАМИ В СИСТЕМЕ FLEX DATABASES
Сухов Родион.Владимирович 174

ПОДГОТОВКА И ПЕРЕПОДГОТОВКА ИТ-СПЕЦИАЛИСТОВ 177

ЛАБОРАТОРНЫЕ РАБОТЫ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»
Барабаш Павел Александрович, Панасенко Михаил Александрович 177

МЕТОДИКА ОЦЕНКИ КАЧЕСТВА ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ВЕРИФИКАЦИИ ИХ ЗНАНИЙ
Большакова Людмила Валентиновна, Яковлева Наталья Александровна 181

МНОГОУРОВНЕВЫЙ ПОДХОД В ПОДГОТОВКЕ И ПЕРЕПОДГОТОВКЕ КАДРОВ В СФЕРЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Бурлов Вячеслав Георгиевич, Грачев Михаил Иванович, Примакин Алексей Иванович 184

СЕТЕЦЕНТРИЧЕСКАЯ ПАРАДИГМА УПРАВЛЕНИЯ В ЦИФРОВОМ ОБЩЕСТВЕ
Верзун Наталья Аркадьевна, Колбанев Михаил Олегович, Касаткин Виктор Викторович 188

ЭВОЛЮЦИЯ СЕТЕЙ ЭЛЕКТРОСВЯЗИ И ПРИНЦИПОВ ИХ ПОСТРОЕНИЯ
Верзун Наталья Аркадьевна, Колбанев Михаил Олегович, Ипатов Олег Сергеевич 193

ПРИМЕРЫ РЕАЛИЗАЦИИ ОБОБЩЕННОЙ МОДЕЛИ ДЕЯТЕЛЬНОСТИ В ЦИФРОВОМ ОБЩЕСТВЕ
Верзун Наталья Аркадьевна, Колбанев Михаил Олегович,
Цехановский Владислав Владимирович 197

ДИСТАНЦИОННОЕ ОБУЧЕНИЕ КАК ОПЕРАЦИОННО-ДИДАКТИЧЕСКАЯ ФОРМА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ПЕДАГОГИЧЕСКИХ КАДРОВ В СИСТЕМЕ НЕПРЕРЫВНОГО ОБРАЗОВАНИЯ ВЗРОСЛЫХ
Каткова Ирина Васильевна, Цесаренко Ольга Петровна 199

СОЗДАНИЕ СОВРЕМЕННОЙ ЛАБОРАТОРНОЙ БАЗЫ ДЛЯ ПОВЫШЕНИЯ КАЧЕСТВА ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СООТВЕТСТВИИ С ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ В СФЕРЕ ОБРАЗОВАНИЯ
Соколов Сергей Сергеевич 203

МЕТОДЫ ЗАЩИТЫ ОТ АТАК МЕТОДАМИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ
Солодянников Александр Владимирович, Сухостат Валентина Василька,
Антонова Любовь Сергеевна 205

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ НА ТРАНСПОРТЕ 210

ТЕХНОЛОГИИ СЕТЕЙ НОВОГО ПОКОЛЕНИЯ (NGN) И ИХ ПРИМЕНЕНИЕ НА ВОДНОМ ТРАНСПОРТЕ
Алексеев Андрей Дмитриевич, Ерисова Анастасия Дмитриевна, Малов Сергей Сергеевич 210

О МЕТОДЕ ИДЕНТИФИКАЦИИ БЕСПИЛОТНЫХ ВОЗДУШНЫХ СУДОВ ПРИ РЕАЛИЗАЦИИ КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ
Беляев Сергей Алексеевич, Остапченко Юрий Борисович, Кудряков Сергей Алексеевич,
Рубцов Евгений Андреевич 214

НАУЧНО-МЕТОДИЧЕСКИЕ ПОДХОДЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ТРАНСПОРТЕ
Белов Андрей Сергеевич, Барабанов Владимир Викторович 218

ПРИМЕНЕНИЕ МЕТОДА АНАЛИЗА ИЕРАРХИЙ В ЗАДАЧЕ ОПТИМИЗАЦИИ САЙТА НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ КОМПАНИИ
Москалева Валерия Дмитриевна, Кривцов Александр Николаевич 222

ЭВРИСТИЧЕСКИЕ ПОДХОДЫ К РЕШЕНИЮ ЗАДАЧ МАРШРУТИЗАЦИИ С ВРЕМЕННЫМИ ОКНАМИ ДЛЯ ОПТИМИЗАЦИИ ПРОЦЕССОВ ОНЛАЙН-РИТЕЙЛА
Котляр Софья Денисовна, Кривцов Александр Николаевич 226

УГРОЗЫ БЕЗОПАСНОСТИ VOIP
Полугина Юлия Константиновна 230

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СОЦИОКОМПЬЮТИНГЕ 234

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ЗАЩИТЫ ОТ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ С ПОМОЩЬЮ РЕЗОНАТОРОВ
Копыльцов Александр Васильевич 234

АЛГОРИТМ ОЦЕНИВАНИЯ БЕЗОПАСНОСТИ СЛАБО ФОРМАЛИЗОВАННОЙ ИНФОРМАЦИИ
Копыльцов Антон Александрович 238

НАЦИОНАЛЬНЫЙ НАУЧНЫЙ ЯЗЫК КАК ОСНОВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Микони Станислав Витальевич 241

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ ОБЪЕКТАМИ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ 246

ПРОГНОЗИРОВАНИЕ РАЗВИТИЯ ОБСТАНОВКИ В ИНФОРМАЦИОННОЙ СФЕРЕ
Алексеев Анатолий Владимирович 246

ПРОБЛЕМЫ ПОДГОТОВКИ И ПЕРЕПОДГОТОВКИ КАДРОВ СИЛ ОБЕСПЕЧЕНИЯ ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ В СФЕРЕ МОРСКОГО И РЕЧНОГО ТРАНСПОРТА
Алимов Олег Михайлович 251

ДИСТАНЦИОННАЯ ДИАГНОСТИКА СУДОВЫХ МАШИН И ОБОРУДОВАНИЯ
Баркова Наталия Александровна, Барков Алексей Васильевич,
Грищенко Дмитрий Вячеславович, Федорищев Владимир Валерьевич 253

ДИВЕРСИОННОЕ ПРИКРЫТИЕ
Каторин Юрий Федорович, Юмашева Елена Сергеевна, Бач Марина Александровна 258

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ 262

СОЦИАЛЬНЫЙ ИНЖИНИРИНГ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
Хайруллов Артем Вадимович, Галлямова Миляуша Равильевна 262

МЕТОДЫ ВОЗДЕЙСТВИЯ И ЗАЩИТЫ ОТ ВИРУСНЫХ ВИДЕОРОЛИКОВ
Юмашева Елена Сергеевна, Ежгуров Василий Николаевич 266

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОЛОГИИ 270

ЗАТМЕННОЕ ЗОНДИРОВАНИЕ ВЕРХНЕЙ АТМОСФЕРЫ ЗЕМЛИ С ПИЛОТИРУЕМОЙ ОРБИТАЛЬНОЙ СТАНЦИИ: ПОЛУЧЕНИЕ И СОХРАНЕНИЕ ИНФОРМАЦИИ
Бузников Анатолий Алексеевич 270

ИНФОРМАЦИОННОЕ И ОПЕРАЦИОННОЕ ОБЕСПЕЧЕНИЕ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ДЕЯТЕЛЬНОСТИ СИЛОВЫХ СТРУКТУР И ОТРАСЛЕЙ ЭКОНОМИКИ РОССИИ
Доронин Александр Павлович, Щукин Георгий Георгиевич, Петроченко Вячеслав Михайлович, Козлова Наталья Александровна, Тимощук Александр Сергеевич, Шмалько Светлана Анатольевна, ... 272

ЭКОЛОГИЧЕСКИЙ КОНТРОЛЬ И РАЗВИТИЕ МОДЕЛЕЙ ПОПУЛЯЦИОННОГО РОСТА
Павлова Светлана Михайловна 276

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ 281

ПРОЕКТИРОВАНИЕ АППАРАТНО-ПРОГРАММНОГО КОМПЛЕКСА ИДЕНТИФИКАЦИИ СОСТОЯНИЯ ОБЪЕКТОВ И СУБЪЕКТОВ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ ИНТЕРНЕТ ВЕЩЕЙ
Дикий Дмитрий Игоревич, Артемьева Виктория Денисовна 281

МЕТОД РАЗРАБОТКИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ РЕГИОНАЛЬНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ
Козин Иван Сергеевич 283

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ МОДИФИКАЦИИ ПРОТОКОЛА АУТЕНТИФИКАЦИИ НА ОСНОВЕ СЛАБОГО ПАРОЛЯ
Шенец Николай Николаевич, Трухина Екатерина Евгеньевна 289

**МОЛОДЕЖНЫЕ НАУЧНЫЕ ШКОЛЫ:
БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ 294**

ПОСТРОЕНИЕ ИНФОРМАЦИОННО-МОНИТОРИНГОВОЙ СИСТЕМЫ АРОМОБЕЗОПАСНОСТИ НА АППАРАТНО-ПРОГРАММНЫХ СРЕДСТВАХ
Антонов Валерий Валентинович 294

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ ПОДХОДОВ ВИДЕОСТЕГОАНАЛИЗА
Ахрамеева Ксения Андреевна, Попов Леонид Геннадьевич 296

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ШИФРОВАНИЯ БАЗ ДАННЫХ В РАЗРАБОТКЕ СОВРЕМЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
Грибачев Виталий Петрович, Харитонов Георгий Дмитриевич 301

ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ НАЗЕМНОГО ГОРОДСКОГО ПАССАЖИРСКОГО ТРАНСПОРТА
Ильченко Лидия Михайловна, Зайцев Святослав Игоревич 303

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. ФИШИНГ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ ЕМУ
Ильченко Лидия Михайловна, Уваров Роман Валерьевич, Зайцев Святослав Игоревич 307

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ОБУЧЕНИИ ХИМИИ
Колоколов Даниил Сергеевич 310

РЕАЛИЗАЦИЯ МЕТОДА КАНАЛЬНОЙ СТЕГАНОГРАФИИ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛА ICMP
Костырин Алексей Сергеевич, Красов Андрей Владимирович 312

ИНФОРМАЦИОННОАЯ БЕЗОПАСНОСТЬ ОТКРЫТЫХ ДАННЫХ
Пешков Андрей Иванович , Тихонова Эльвира Никитична 316

РАСШИРЕНИЕ ФОРМАЛИЗАЦИЙ ЖИЗНЕННОГО ЦИКЛА ЗАЩИЩЁННЫХ СЕРВИС-ОРИЕНТИРОВАННЫХ СИСТЕМ
Птицына Лариса Константиновна, Нежинский Виталий Владимирович 320

ПРОБЛЕМА АНОНИМНОСТИ В СЕТИ ИНТЕРНЕТ СРАВНЕНИЕ МЕТОДОВ АНОНИМИЗАЦИИ ПОЛЬЗОВАТЕЛЯ
Титова Юлия Алексеевна, Садикова Анастасия Александровна, Савков Сергей Витальевич 323

АНАЛИЗ АКТИВНЫХ СЕТЕВЫХ АТАК:ARP-SPOOFING ИDNS-SPOOFING
Ягудин Ильдар Рашидович, Волкогонов Владимир Никитич 328

МОЛОДЕЖНЫЕ НАУЧНЫЕ ШКОЛЫ: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОБЛЕМЫ УСТОЙЧИВОГО РАЗВИТИЯ 332

ИССЛЕДОВАНИЕ УЯЗВИМОСТИ СЕРИАЛИЗАЦИИ И ДЕСЕРИАЛИЗАЦИИ ДАННЫХ В JAVA
Шариков Павел Иванович[1], Красов Андрей Владимирович[2] 332

ОГЛАВЛЕНИЕ 336

CONTENTS 342

CONTENTS

INFLUENCE OF SECURITIZATION ON POLICY OF RUSSIA: INFORMATION ASPECT
Baranov Nikolai 5

EFFECTIVENESS OF E-PARTICIPATION TOOLS IN RUSSIA IN POLICY-MAKING
Vidiasova Lyudmila, Tensina Iaroslava 10

STATE POLICY IN THE FIELD OF ENSURING INFORMATION SECURITY IN THE NORTH-WEST FEDERAL DISTRICT
Kucheryavyi Mikhail, Vovenda Julia 14

ENSURING PERSONNEL SAFETY OF THE INDUSTRIAL ENTERPRISES OF HIGH-TECH INDUSTRIES
Boris Sovetov, Victor Kasatkin 17

TWO-MOMENT APPROXIMATION METHOD APPLICATION SYSTEMATIC PROCEDURE FOR THE FUNCTION DETERMINATION OF STOCHASTIC NETWORK TIME DISTRIBUTION IMPLEMENTATION
Kanaev Andrey., Karabanov Yuriy., Privalov Andrey 20

APPLICATION OF ROLE-BASED ACCESS CONTROL IN MACHINE-TO-MACHINE NETWORKS WITH DYNAMIC TOPOLOGY
Kalinin Maxim, Evgenia Rezedinova 25

PROBLEMS OF PROTECTION OF INFORMATION AND TELECOMMUNICATION INFORASTRUKTURA OF THE RUSSIAN FEDERATION AGAINST CYBER ATTACKS
Moshak Nikolay Nikolaevich, Evseiko Konstantin Vladyslavovich 31

METHODS OF CALCULATION OF QUANTILES OF DISTRIBUTION OF THE CASUAL NETWORK DELAY OF PACKAGES OF ISOCHRONOUS TRAFFIC IN THE TASK OF THE ANALYSIS OF THE INFOCOMMUNICATION TRANSPORT SYSTEMS
Moshak Nikolay Nikolaevich, Logincev Aleksander Vladimirovich 36

OPTION FOR THE FORMATION OF THE ENSEMBLE OF DISCRETE ORTHOGONAL SIGNALS WITH THE REQUIRED PARAMETERS OF STRUCTURAL HIDDEN
Sazonov Viktor, Bezubov Oleg, Mosyagin Dmitry 42

SECURITY OF INFORMATION RESOURCES OF EDUCATIONAL INSTITUTIONS
Piyukov Oleg Yrievich., Gvozdkov Igor Vyacheslavovich 45

THE ISSUES OF INTRODUCTION OF DIGITAL VIDEO TECHNOLOGY IN POLICING
Shalaginova Olga Borisovna 46

TWO-MODULO CODES WITH SUMMATION IN EXPERIMENT ON THE ANALYSIS OF STRUCTURAL REDUNDANCY OF CONCURRENT ERROR DETECTION SYSTEMS
Efanov Dmitry, Schagina Vladislava 48

DATA PROTECTION AND THE HUMAN FACTOR
Kartashov Pavel 54

INFORMATION AND COMMUNICATION TECHNOLOGY AS AN INSTRUMENTAL ENVIRONMENT SUPPORT OF EDUCATIONAL PROCESS
Lidia Kolokolova 57

THE ONTOLOGICAL CLASSES INSTANCES GENERATION WHEN PROCESSING SEMISTRUCTURED DATA IN SOLVING INFORMATION SECURITY CHALLENGES
Poltavtseva Maria Anatolevna, Pechenkin Alexander Igorevich 60

THE NETWORK SECURITY OF THE INTERNET OF THINGS MEANS OF LOW-RESOURCE CRYPTOGRAPHY
Suprun Aleksandr, Tsarkov Igor 64

PEDAGOGICAL AND TECHNOLOGICAL ASPECTS OF THE USE OF COMPUTER-BASED TESTING AT DIFFERENT STAGES OF LEARNING THE DISCIPLINE
Titova Yuliayna Frantsevna 68

MODELING OF FLAWS WITHIN A SECURITY SYSTEM
Shipileva Alla 74

THE APPLICATION OF THE PSEUDOPROBABILISTIC PROTECTING DATA CONVERSION IN THE ELECTRONIC ELECTION TECHNOLOGY
Vaichikauskas Maria, Tatchina Yana, Sinev Valery ... 77

MONITORING OF THE FUNCTIONAL STATE OF THE HUMAN OPERATOR AND ITS CORRECTION AS A METHOD OF INCREASING THE INFORMATION-PSYCHOLOGICAL SAFETY IN THE WORKPLACE
Kolmakov Sergey ... 79

SECURITY AND USABILITY OF MODERN USER INTERFACES
Leonov Anton ... 83

APPROACH TO THE EXTRACTION OF THE MOTIVES IN EMPLOYEES MOVEMENT WITHIN ORGANIZATION
Novikova Evgenia, Bekeneva Yana ... 86

METHOD OF RANDOMIZED CONSOLIDATED INDICATORS FOR EXPERT EVALUATION OF INFORMATION PROTECTION SYSTEMS
Popova Elena ... 89

DESIGN OF TREE-BASED SERIAL DATA STORAGES WITH INCLUDED DIGITAL SIGNATURES
Romanova Yuliya Nikolaevna, Yanyushkin Konstantin Aleksandrovich ... 92

BUILDING CLOUD SECURITY PERIMETER
Ryzhkov Sergey ... 94

METHODS AND TOOLS OF THE AUDIT OF NETWORK SECURITY
Sadikova Anastasia, Titova Yulia, Savkov Sergei ... 97

INTEGRATED SYSTEM OF ENGINEERING AND TECHNICAL PROTECTION OF THE MANAGER'S OFFICE. THE EFFECTIVENESS OF THE WORK OF INFORMATION SECURITY DEVICES ON THE EXAMPLE OF AN INTEGRATED SYSTEM OF ENGINEERING AND TECHNICAL PROTECTION OF THE MANAGER'S OFFICE
Fayazov Kobiljon Abdukayumovich ... 102

THE PROBLEM OF VISUALIZING ROUTES RUN COMPUTER PROGRAMS
Bezrukov Vjacheslav, Sineshchuk Yuri, Sineshchuk Maxim ... 107

QUESTIONS OF INFORMATION SAFETY OF SYSTEMS OF COMMUNICATION
Vilkov Valeriy, Sychev Sergey, Chernykh Andrey ... 111

ABOUT SOCIAL NETWORKS OF UNIVERSITIES AND INFORMATION SECURITY
Oleg Kononov, Olga Kononova ... 115

PEDAGOGICAL COMMUNICATIONS IN THE MODERN EDUCATIONAL ENVIRONMENT
Kostyuk Anatoliy, Bobonets Sergey ... 119

MODEL FOR FORMATION OF REQUIREMENTS FOR CONFIDENTIALITY OF INTEGRITY AND ACCESSIBILITY OF DATA IN THE SYSTEM OF INFORMATION PROTECTION OF MEANS OF COMPUTER ENGINEERING AND AUTOMATED SYSTEMS
Kuvatov Valery, Primakin Alexey ... 122

SUBJECT COMPOSITION OF RELATIONSHIPS IN THE FIELD OF INFORMATION AND ANALYTICAL ENFORCEMENT OF LAW ENFORCEMENT ACTIVITY
Lepyokhin Alexander Nikolaevich ... 126

ABOUT THE METHOD OF UNMANNED AIRCRAFT IDENTIFICATION IN THE IMPLEMENTATION OF COMPLEX SAFETY SYSTEMS
Belyaev Sergey, Ostapchenko Yuriy, Kudryakov Sergey, Rubtsov Evgeny ... 127

FUNCTIONAL RELIABILITY AND STABILITY OF THE COMPUTATIONAL PROCESS
Vladimir Bogatyrev, Stanislav Bogatyrev ... 131

ANALYSIS OF AROMOSENSOR APPLICATION AREAS SYSTEMS OF SAFETY
Dmitry Afanasiev, Elena Bardakova, Denis Bystryakov ... 133

OPTIMIZATION OF THE FREQUENCY OF THE TEST CONTROL, WHILE ENSURING THE SYSTEM'S READINESS FOR SAFE OPERATION
Vladimir Bogatyrev, Stanislav Bogatyrev ... 136

MODEL ACCESS TO THE TOUCH DEVICES IN THE "FOG COMPUTING" OF IOT
Elizarov Maksim ... 139

ESTIMATION AND FORECASTING OF RISKS FOR INFORMATION SECURITY SYSTEMS
Alexey Kapanov, Evgeny Meshcheryakov, Vladimir Kosolapov, Tatyana Astakhova 142

SAFETY INFORMATION INTERACTION
Oleg Kutuzov, Tatiana Tatarnikova 144

FORMATION AND USE IN THE EDUCATIONAL PROCESS OF THE SITUATIONAL CENTER FOR BUSINESS INTELLIGENCE
Levkin Igor Mikhailovich, Mikadze Sergey 148

PECULIARITIES OF SIMULATING A SELF-SIMULATED NETWORK TRAFFIC
Tatiana Tatarnikova 151

METHODOLOGY OF DESIGNING A GIS SHIP
Natalia Yagotinceva 155

THE DEVELOPMENT OF IT-SECURITY MANAGEMENT SYSTEM FOR CRITICAL INDUSTRIAL OBJECT
Livshitz Ilya, Malikov Vladimir 160

THE FORmulation OF REQUIREMENTS FOR ASSESSMENT OF CRITICAL OBJECTS BASED ON MODERN ISO STANDARDS
Livshitz Ilya, Malikov Vladimir 164

EVALUATION OF THE IMPACT OF ACTUAL RISK-BASED STANDARDS FOR IT-SECURITY ASSURANCE FOR AN CRITICAL INFRASTRUCTURE FACILITIES
Livshitz Ilya [1], Malikov Vladimir [2] 167

SIMULATION HYBRID PROTOCOL ROUTING IN WIRELESS NETWORK
Molokovich Igor 170

MODERN APPROACH TO DETECTION AND MANAGEMENT, MEDICAL SIGNALS IN THE FLEX DATABASES SYSTEM
Rodion Sukhov 174

LABORATORY PRACTICUM ON EDUCATIONAL DISCIPLINE "SECURITY OF INFORMATION SYSTEMS"
Barabash Pavel, Panasenko Mikhail 177

METHODS OF EVALUATION THE QUALITY OF TRAINING IN THE FIELD OF ENSURING INFORMATION AND ECONOMIC SECURITY ON THE BASIS OF VERIFICATION OF THEIR KNOWLEDGE
Bolshakova Lyudmila, Yakovleva Natalia 181

MULTI-LEVEL APPROACH IN TRAINING AND TRAINING IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY
Burlov Vyacheslav Georgievich, Grachev Mikhail Ivanovich, Primakin Alexey Ivanovich 185

NETWORK-CENTRIC CONTROL PARADIGM IN A DIGITAL SOCIETY
Verzun Natalya, Kolbanev Mikhail, Kasatkin Victor 188

THE EVOLUTION OF TELECOMMUNICATION NETWORKS AND PRINCIPLES OF THEIR CONSTRUCTION
Verzun Natalya, Kolbanev Mikhail, Ipatov Oleg 193

EXAMPLES OF IMPLEMENTATION OF THE GENERALIZED MODEL ACTIVITIES IN A DIGITAL SOCIETY
Verzun Natalya, Kolbanev Mikhail, Cehanovsky Vladislav 197

DISTANCE EDUCATION AS OPERATIONALLY DIDACTIC FORM OF PROFESSIONAL DEVELOPMENT OF PEDAGOGICAL STAFF IN CONTINUING EDUCATION ADULTS
Katkova Irina, Cecarenko Olga 199

THE CREATION OF MODERN LABORATORY BASE FOR IMPROVEMENT OF QUALITY OF TRAINING IN THE FIELD OF INFORMATION SECURITY ACCORDING TO THE CURRENT LEGISLATION IN EDUCATION
Sokolov Sergey Sergeevich 203

METHODS OF PROTECTION FROM ATTACKS BY METHODS OF SOCIAL ENGINEERING
Solodyannikov Alexander, Sukhostat Valentina, Antonova Liubov 205

NEXT GENERATION NETWORK TECHNOLOGIES AND THEIR APPLICATION FOR THE WATER TRANSPORT
Andrey Alexeev, Anastasiya Erisova,Malov Sergey 210

ABOUT THE METHOD OF UNMANNED AIRCRAFT IDENTIFICATION IN THE IMPLEMENTATION OF COMPLEX SAFETY SYSTEMS
Belyaev Sergey, Ostapchenko Yuriy, Kudryakov Sergey, Rubtsov Evgeny 214

SCIENTIFIC AND METHODOLOGICAL APPROACHES TO ENSURE SAFETY OF INFORMATION SYSTEMS IN TRANSPORT
Belov Andrey, Barabanov Vladimir 218

APPLICATION OF THE HIERARCHY ANALYSIS METHOD IN THE PROBLEM OF OPTIMIZATION OF THE SITE OF THE SCIENTIFIC RESEARCH COMPANY
Moskaleva Valeriia, Krivtsov Alexander 222

CONSTRUCTION HEURISTIC FOR SOLVING VEHICLE ROUTING PROBLEM WITH TIME WINDOWS FOR E-FULFILLMENT PROCESS OPTIMIZATION
Kotliar Sofia, Krivtsov Aleksand 226

SECURITY THREATS OF VOIP
Polugina Julia 231

MATHEMATICAL MODELING OF PROTECTION AGAINST ELECTROMAGNETIC RADIATION BY MEANS OF RESONATORS
Alexander Kopyltsov 234

ALGORITHM OF SAFETY EVALUATION OF WEAKLY FORMALIZED INFORMATION
Anton Kopyltsov 239

NATIONAL SCIENTIFIC LANGUAGE AS BASIS OF INFORMATION SECURITY
Mikoni Stanislav 242

FORECASTING OF DEVELOPMENT OF SITUATION IN THE INFORMATION SPHERE
Alekseev Anatoly Vladimirovich 246

PROBLEMS OF TRAINING AND RETRAINING TRANSPORT SECURITY IN THE SPHERE OF MARITIME AND INLAND SHIPPING
Alimov Oleg Mihailovich 251

REMOTE DIAGNOSTICS OF SHIPBOARD MACHINERY AND EQUIPMENT
Nataliya Barkova, Alexey Barkov, Dmitriy Grishchenko, Vladimir Fedorishchev 254

DIVERSIONAL COVERAGE
Katorin Yuri , Yumasheva Elena, Bach Marina 258

SOCIAL ENGINEERING AND INFORMATION SECURITY
Khairullov Artem,Gallyamova Milyausha 262

METHODS OF EXPOSURE AND PROTECTION FROM VIRUS VIDEOS
Yumasheva Elena, Ezhgurov Vasily 266

ECLIPSING REMOTE SENSING OF THE EARTH'S UPPER ATMOSPHERE FROM MANNED SPACECRAFT: OBTAINING AND SAVING THE INFORMATION
Buznikov Anatoliy 270

ENVIRONMENTAL CONTROL AND DEVELOPMENT OF MODELS OF POPULATION GROWTH
Pavlova Svetlana Michailovna 276

DESIGN OF HARDWARE AND SOFTWARE IDENTIFY THE STATE OF OBJECTS AND SUBJECTS WITH APPLICATION OF TECHNOLOGIES OF INTERNET OF THINGS
Dikii Dmitrii[1], Artemeva Viktoriia[2] 281

METHOD OF DEVELOPMENT OF SECURITY INFORMATION AND EVENT MANAGEMENT COMPUTER-AIDED SYSTEM OF REGIONAL INFORMATION SYSTEM
Kozin Ivan 284

CONSTRUCTION OF THE INFORMATION-MONITORING SYSTEM OF AROMA-SAFETY ON HARDWARE AND SOFTWARE
Antonov Valery 294

COMPARATIVE ANALYSIS OF EFFICIENCY OF THE VIDEO STEGANALYSIS APPROACHES
Akhrameeva Ksenia, Popov Leonid 296

PROSPECTS OF APPLICATION OF DATABASE ENCRYPTION IN MODULAR SOFTWARE DEVELOPMENT
Gribachev Vitaly Petrovich, Kharitonov Georgiy Dmitrievich 301

PARTICULAR QUALITIES OF CONSTRUCTION OF INFORMATION PROTECTION SYSTEM IN INTELLECTUAL SYSTEMS OF GROUND CITY PASSENGER TRANSPORT
Ilchenko Lydia, Zaytsev Svyatoslav 303

SOCIAL ENGINEERING. PHISHING AND METHODS OF COUNTERING IT
Ilchenko Lydia, Uvarov Roman, Zaytsev Svyatoslav 307

USE OF INFORMATION TECHNOLOGIES IN TRAINING CHEMISTRY
Daniil Kolokolov 310

IMPLEMENTATIONOF THE METOD OF CHANNEL STEGANOGRAPHY USING ICMP PROTOCOL
Kostyrin Alexey, Krasov Andrey 312

INFORMATION SECURITY OF OPEN DATA
Vitkova Lidia, Peshkov Andrey, Tikhonova Elvir 316

EXPANSION OF FORMALIZATIONS OF THE LIFE CYCLE OF PROTECTED SERVICE-ORIENTED SYSTEMS
Ptitsyna Larisa, Nezhinsky Vitaliy 320

THE PROBLEM OF ANONYMITY IN THE INTERNET NETWORK COMPARISON OF METHODS OF USER ANONYMIZATION
Titova Yulia, Sadikova Anastasia, Savkov Sergei 323

ANALYSIS OF ACTIVE NETWORK ATTACK: ARP SPOOFING AND DNS SPOOFING
Yagudin Ildar, Volkogonov Vladimir 328

INVESTIGATION OF VULNERABILITY OF SERILIZATION AND DESERIALIZATION OF DATA IN JAVA
Sharikov Pavel, Krasov Andrey 332