**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»**

КАФЕДРА ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ И ПРОГРАММИРОВАНИЯ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЦИФРОВОГО ПРОСТРАНСТВА

Под редакцией Е.В. Стельмашонок, И.Н. Васильевой

**ИЗДАТЕЛЬСТВО
САНКТ-ПЕТЕРБУРГСКОГО ГОСУДАРСТВЕННОГО
ЭКОНОМИЧЕСКОГО УНИВЕРСИТЕТА
2019**

ББК 32.97
И74

Информационная безопасность цифрового пространства / под ред.
И74 Е.В. Стельмашонок, И.Н. Васильевой. – СПб. : Изд-во СПбГЭУ, 2019. – 155 с.

ISBN 978-5-7310-4465-3

В монографии исследуются проблемы информационной безопасности, сопровождающие процессы внедрения новых информационных технологий, цифровизации экономики и других областей человеческой жизни. Рассматриваются вопросы моделирования и построения защищенных информационных систем в различных сферах профессиональной деятельности. Приводится анализ современных технологий и средств защиты информации. Излагается опыт применения образовательных технологий в области информационной безопасности.

Монография может быть полезна преподавателям, студентам, магистрантам, аспирантам, занимающимся исследованием данных проблем и специалистам в области защиты информации, а также ИТ-специалистам и всем, кто интересуется вопросами формирования цифрового пространства и связанными вопросами информационной безопасности.

The monograph examines the problems of information security, accompanying the processes of introducing new information technologies, digitalization of the economy and other areas of human life. The issues of modeling and building secure information systems in various areas of professional activity are considered. The analysis of modern technologies and information security tools is provided. The experience of using educational technologies in the field of information security is presented.

The publication can be useful to teachers, students, undergraduates, graduate students who research these problems, to professionals in the field of information security, as well as IT professionals and anyone interested in questions of formation of digital space and related information security issues.

ББК 32.97

Коллектив авторов: И.Л. Андреевский, **И.Н. Васильева**, **И.Е. Галактионов**, **И.Г. Гниденко**, **Н.А. Дубских**, **А.П. Дурандина**, **И.В. Егорова**, **Л.А. Еникеева**, **А.Д. Игнатьев**, **Е.В. Майорова**, **О.Д. Мердина**, **М.А. Перминов**, **В.Г. Петров**, **А.М. Полегенько**, **М.А. Попов**, **Т.Г. Семёнова**, **С.О. Семёнова**, **М.В. Синько**, **Р.В. Соколов**, **С.А. Соколовская**, **А.В. Солодянников**, **В.Л. Стельмашонок**, **Е.В. Стельмашонок**, **В.В. Сухостат**, **Н.И. Сясин**, **Д.Ю. Федоров**, **Г.М. Чернокнижный**, **А.В. Черток**

Рецензенты: профессор СПб университета МВД России,
заслуженный деятель науки РФ, д-р техн. наук, проф. **В.И. Куватов**
зав. кафедрой информатики СПбГЭУ заслуженный деятель науки РФ,
д-р техн. наук, проф. **В.В. Трофимов**

ISBN 978-5-7310-4465-3

© СПбГЭУ, 2019

ОГЛАВЛЕНИЕ

Введение 4
Глава 1. ПРОБЛЕМЫ БЕЗОПАСНОСТИ ЦИФРОВОГО ПРОСТРАНСТВА 7
1.1. Цифровое пространство и проблемы информационной безопасности 7
1.2. Информационная безопасность цифрового пространства Интернета вещей 10
1.3. Проблема стандартизации в области Интернета вещей 16
1.4. Безопасность мессенджеров 20
1.5. Безопасность персональных данных в контексте европейского регламента GDPR 36
1.6. Информационная безопасность виртуальных предприятий 41
Глава 2. ПОСТРОЕНИЕ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 47
2.1. Построение онтологии информационной безопасности 47
2.2. Контроль функционирования комплексной системы защиты информации 56
2.3. Управление влиянием на проявления человеческого фактора при обеспечении информационной безопасности автоматизированной системы 67
2.4. Система обработки и обеспечения безопасности персональных данных в организации 74
2.5. Организация защиты персональных данных в банковских информационных системах 79
2.6. Выбор структуры предложения защищенных облачных сервисов в условиях неопределенности спроса 89
Глава 3. ТЕХНОЛОГИИ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ 98
3.1. Применение искусственного интеллекта в системах антивирусной защиты 98
3.2. Анализ эффективности применения технологии Threat Intelligence 102
3.3. Анализ криптографических средств операционных систем Windows ... 109
3.4. Исследование вопроса обеспечения конфиденциальности и целостности данных применением в базе данных механизма триггеров 124
3.5. Защита акустической речевой информации конфиденциального характера от утечки по техническим каналам 131
Глава 4. СОВРЕМЕННЫЕ ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 138
4.1. Разработка деловой игры «Построение системы защиты информации на предприятии» 138
4.2. Создание и использование лабораторного стенда для изучения DLP-системы InfoWatch Traffic Monitor 142
4.3. Административный доступ и обеспечение безопасности аппаратно-программного комплекса компьютерной аудитории 150
Заключение 155

Введение

В настоящее время информационные технологии стали движущей силой развития современного мира, прочно войдя во все сферы жизни человека, сформировав новое, цифровое пространство. Но наряду с инновационной составляющей процессы цифровизации несут в себе определенные угрозы, связанные, прежде всего, с проблемами информационной безопасности, обеспечением приватности и защитой личных (персональных) данных, защитой от деструктивных воздействий и злоупотреблений в цифровой среде.

Первая глава монографии посвящена рассмотрению актуальных проблем информационной безопасности цифрового пространства, связанных с влиянием человеческого фактора, развитием Интернета вещей, обеспечением приватности мобильных коммуникаций (мессенджеров), безопасностью персональных данных и развитием такой новой формы организации хозяйственной деятельности, как виртуальные предприятия.

Вопросам обеспечения информационной безопасности уделяется немало внимания как на государственном и международном уровне, так и на уровне отдельных хозяйствующих субъектов и участников информационных взаимоотношений. Информационная безопасность становится важной частью общей информационной культуры человека.

В Российской Федерации на законодательном уровне закреплена необходимость включения модели угроз информационной безопасности и требований к защите информации проектируемой или модифицируемой информационной системы уже на этапе формирования технического задания. Эти требования во многом определяют выбор используемых технологий и подходов к построению компьютерных систем. Должны быть разработаны соответствующие теоретические основы и модели с учетом актуальных угроз и положений информационной безопасности. Требования к защите информации определяют состав, функции и особенности реализации подсистемы защиты информации и должны выполняться, контролироваться и актуализироваться на всех этапах жизненного цикла информационных систем. Вопросы построения систем обеспечения информационной безопасности рассмотрены во второй главе монографии.

Рост объемов подлежащей защите информации, а также объемов данных, контролируемых и анализируемых системами защиты информации, демократизация доступа к новым информационным технологиям и системам, все большая изощренность и сложность технологий, применяемых атакующей стороной, требует применения новых защитных технологий, в том числе технологий интеллектуализации систем защиты информации. Вторая глава монографии посвящена исследованию отдельных технологий и средств защиты информации.

Немаловажной составляющей успеха как при внедрении отдельных систем защиты информации, так и процессов цифровизации в целом, является обучение и подготовка специалистов по вопросам информационной безопасности. Четвертая глава монографии отражает накопленный преподавателями кафедры вычислительных систем и программирования СПбГЭУ опыт использования современных образовательных технологий в области информационной безопасности.

Авторский коллектив монографии составляют преподаватели СПбГЭУ и других вузов, действующие специалисты в области информационной безопасности, а также студенты старших курсов, обучающиеся по направлению «Информационная безопасность». Вклад авторов распределился следующим образом:

- Андреевский И.Л. – доцент СПбГЭУ, к.э.н., доцент – п. 1.2, 2.6;
- Васильева И.Н. – доцент СПбГЭУ, доцент СПб университета МВД РФ, к.ф.-м.н., доцент – п. 1.4, 3.3;
- Галактионов И. Е. – директор службы безопасности ОАО «НПП «Радар ммс» − п. 2.4, 3.5;
- Гниденко И.Г. – доцент СПбГЭУ, к.э.н., доцент – п. 3.1;
- Дубских Н.А. – студент направления «Информационная безопасность» СПбГЭУ – п. 4.1;
- Дурандина А.П. – доцент СПб государственного архитектурно-строительного университета, к.э.н., доцент − п.2.5;
- Егорова И.В. – доцент СПбГЭУ, к.э.н., доцент − п. 3.1;
- Еникеева Л.А. – профессор СПб государственного института кино и телевидения, д.э.н., профессор – п. 2.5;
- Игнатьев А.Д. – студент направления «Информационная безопасность» СПбГЭУ – п. 4.1;
- Майорова Е.В. – доцент СПбГЭУ, к.т.н., доцент – п. 3.2;
- Мердина О.Д. – доцент СПбГЭУ, к.э.н., доцент – п. 3.4;
- Перминов М.А. – студент направления «Информационная безопасность» СПбГЭУ – п. 2.1;
- Петров В.Г. – заместитель директора УМЦ «ХимИнформЗащита» по учебно-методической работе, к.т.н., доцент – п. 2.4, 3.5;
- Полегенько А.М. – ведущий специалист по защите информации ЗАО «ТЕЛРОС» (г. Санкт-Петербург), аспирант университета ИТМО, ассистент кафедры вычислительных систем и программирования СПбГЭУ – п. 1.3;
- Попов М.А. – студент направления «Информационная безопасность» СПбГЭУ – п. 2.1;
- Семёнова Т.Г. – менеджер проектов SAM компании CSI Group (г. Москва) – п. 1.5;

- Семёнова С.О. – инженер испытательной лаборатории ЗАО «ТЕЛРОС» (г. Санкт-Петербург) – п. 1.5;
- Синько М.В. – студент направления «Информационная безопасность» СПбГЭУ – п. 2.1;
- Соколов Р.В. – профессор СПбГЭУ, д.э.н., профессор – п. 2.6;
- Соколовская С.А. – доцент СПбГЭУ, к.э.н., доцент – п. 1.6;
- Солодянников А.В. – доцент СПбГЭУ, генеральный директор ООО «АСБ» (г. Санкт-Петербург), к.т.н., доцент – п. 2.2;
- Стельмашонок В.Л. – доцент СПбГЭУ, к.э.н., доцент – п. 4.1;
- Стельмашонок Е.В. – профессор СПбГЭУ, д.э.н., профессор – п. 4.1;
- Сухостат В.В. – доцент СПбГЭУ, доцент Университета ИТМО, к.т.н., к.пед.н., доцент – п. 1.1, 2.3;
- Сясин Н.И. – доцент СПбГЭУ, к.б.н., доцент – п. 4.3;
- Федоров Д.Ю. – старший преподаватель СПбГЭУ, п. 2.1;
- Чернокнижный Г.М. – доцент СПбГЭУ, к.т.н., доцент – п. 4.2;
- Черток А.В. − специалист по информационной безопасности ЗАО «МоБильный Капитал» (г. Санкт-Петербург) – п. 3.2.

ГЛАВА 1. ПРОБЛЕМЫ БЕЗОПАСНОСТИ ЦИФРОВОГО ПРОСТРАНСТВА

1.1. Цифровое пространство и проблемы информационной безопасности

В настоящее время цифровое пространство (среда) становится движущей силой преобразований во всех сферах жизнедеятельности личности, общества и государства [1]. Радикальные изменения вызваны двумя основными факторами: быстрым прогрессом информационно-коммуникационных технологий (ИКТ) и их интеграцией в социотехнические системы наряду с массовой доступностью. Несомненно, проблемы информационной безопасности (ИБ), являются производными относительно более общих проблем цифрового пространства. При этом, в решении тех и других присутствует в явном или неявном виде «человеческий фактор» (ЧФ) как один из важнейших аспектов. Особенность заключается в том, что человек из оператора, т.е. средства, превратился в цель функционирования информационной системы, массовый пользователь практически беззащитен лично и невольно может стать вредоносным агентом. Поэтому содержание проблем ИБ должно формироваться в соответствии с содержанием проблем цифровизации.

Цифровое пространство как цифровая среда – «среда логических объектов, используемая для описания (моделирования) других сред (в частности, электронной и социальной) на основе математических законов» [2] создает проблему цифрового неравенства и цифрового суверенитета, сущность которых состоит в доминировании в различных сферах жизнедеятельности. Тогда как развитие сетевых технологий обусловливает проявление скрытого управления групповым и массовым поведением, то создание сетей со сложными и взаимосвязанными проблемами, такими как защита критической инфраструктуры на национальном уровне влечет за собой образование киберпространства [3]. В новых условиях только технические аспекты явно недостаточны для комплексного понимания проблематики ИБ. Поэтому роль человека в кибербезопасности является всеобъемлющей [4].

Вопросы о взаимоотношениях личности, общества и государства также рассматриваются в плоскости развития и совершенствования ИКТ. С одной стороны, расширяются права, возможности и свободы личности, а с другой – устанавливается контроль над ними в общественной жизни с позиций неявного корпоративного и государственного доминирования. При этом критериями потенциала государственного сектора и развития цифровой экономики являются прогресс технологий цифровой идентификации человека, создание электронных правительств, цифровых платеж-

ных систем, электронной торговли. Это все провоцирует рост киберпреступности, фальсификации [1].

Также повсеместное использование в организациях мобильных устройств в силу их уязвимости увеличивает возможность для доступа к корпоративным системам. Вместе с тем зависимость от информационных технологий делает систему безопасности более уязвимой. Предусмотреть и противостоять различным видам кибератак намного сложнее, чем противостоять традиционным видам угроз [3]. В этой связи можно полагать, что источником проблемы успешного «обнуления» усилий по обеспечению безопасности является ЧФ. А с другой стороны – только люди сегодня способны остановить киберугрозу – выявить, проанализировать и устранить ее даже в практически безнадежных ситуациях [4, 5].

Задачи хранения, интеграции и предоставления доступа к электронным ресурсам культурного и научного наследия основываются на противоречии между динамикой накопления цифровой информации и темпами технологического старения.

Эволюция цифрового пространства обусловливает распространение идей демократии, но одновременно порождает ряд проблем, связанных с неприкосновенностью личной жизни, киберпреступностью, разжиганием консциентальных войн в системе социальных коммуникаций. В этой связи следует отметить, что с развитием виртуальной и дополненной реальности прогнозируется рост атак, направленных на хищение личности [5].

Актуален вопрос о больших и открытых данных, экономическая составляющая которых оценивается сотнями миллиардов долларов в год. Однако аналитическая обработка информации становится катастрофической в мире. Избыточные объемы продуцирования информации негативно влияют на состояние общества и личности [1]. Происходящие трансформационные процессы в обществе продуцируют риск и неопределенность, тем самым оказывают серьезное влияние на обеспечение ИБ.

Для комплексного понимания проблематики ИБ в научно-технической сфере понятие «информационная безопасность» рассматривается как объединяющая метафора исследований вопросов технического характера наряду с гуманитарными аспектами.

Потому обеспечение информационной безопасности в современных условиях может быть достигнуто при реализации комплексного подхода к взаимоувязанному решению трех составляющих ее проблем:

- защиты информации;
- защиты от информации,
- в добывании информации о потенциальных угрозах.

Международный масштаб и стратегический характер второй составляющей как одной из ключевых проблем современности обусловливает три основных направления защиты от информационных воздействий: на

информационно-технические системы и средства, общество и личность наряду с добыванием информации о потенциальных угрозах [6].

Основанием для учета проявления человеческого фактора в обеспечении ИБ является стремительное усложнение психологической зависимости человека от коммуникаций, безопасности технологического оборудования, человеко-машинного взаимодействия, «социо-кибер-безопасности», безопасности в «Интернете вещей», а также обострение информационного противоборства, информационных войн как деформационных и трансформационных воздействий по информационным каналам. Постоянно меняющаяся динамика в современном ИТ-мире и разнообразный характер потенциальных угроз требует постоянного информирования о них управленческого и технического персонала организации [7].

В условиях глобального расширения цифрового пространства пути решения обозначенных проблем могут быть в плоскости вопросов по развитию способности противостояния современным угрозам посредством трансформатизации [3]. В этом плане подразумевается применение стратегического мышления, развитие возможностей, образование и обучение, сотрудничество и взаимодействие субъектов обеспечения информационной безопасности с учетом человеческого фактора.

Литература:

1. Марьина Е.Ю. Цифровое пространство: противоречия становления и развития // Young Scientist, № 9(36), september 2016 – С. 335-338 [Электронный ресурс]. URL: http://molodyvcheny.in.ua/files/journal/2016/9/116.pdf (дата обращения: 28.10.2018).
2. ГОСТ Р 52292–2004. Информационная технология. Электронный обмен информацией.
3. Курылев К.Л., Цаканян В.Т. Цифровая зависимость НАТО // Вестник Московского государственного областного университета. Серия: История и политические науки. – 2018. − №1. − С.45-51.
4. Кибербезопасность: человеческий фактор, 12.06.2018 [Электронный ресурс]. URL: https://legal-it.club/kiberbezopasnost-chelovecheskij-faktor (дата обращения: 28.10.2018).
5. Эксперты: Человеческий фактор – самый уязвимый аспект кибербезопасности, 30.11.2015 [Электронный ресурс]. URL: https://www.securitylab.ru/news/477095.php (дата обращения: 28.10.2018).
6. Сухостат В.В., Ульзетуева Д.Д. К вопросу об информационной защищенности оператора автоматизированных систем // Государство и бизнес. Современные проблемы экономики: Материалы X Международной научно-практической конференции. Санкт-Петербург, 25-27 апреля 2018 г./Северо-Западный институт управления РАНХиГС при Президенте РФ. Том I. – С. 235-238.
7. Солодянников А.В., Сухостат В.В., Антонова Л.С. Защита от атак методами социальной инженерии // Информационная безопасность регионов России (ИБРР-2017). Юбилейная X Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 1-3 ноября 2017 г.: Материалы конференции / СПОИСУ. – СПб., 2017. – С. 120-122.

1.2. Информационная безопасность цифрового пространства Интернета вещей

Понятие «Интернет вещей» (Internet of Things, IoT) появилось в 1999 году. Существует несколько определений, раскрывающих суть данного понятия.

По версии компании IDC «Интернет вещей − это сеть сетей с уникально идентифицируемыми конечными точками, которые общаются между собой в двух направлениях по протоколам Internet Protocol (IP) и обычно без человеческого вмешательства».

Специалисты компании Gartner дают следующее определение: «Интернет вещей − это сеть физических объектов, которые имеют встроенные технологии, позволяющие осуществлять взаимодействие с внешней средой, передавать сведения о своем состоянии и принимать данные из вне».

Существует еще более технологичное определение компании McKinsey − «Интернет вещей − это датчики и приводы (исполнительные устройства), встроенные в физические объекты и связанные через проводные или беспроводные сети с использованием протокола IP, который связывает Интернет».

Другими словами, «Интернет вещей − это необъятное скопление подключенных датчиков, камер, смартфонов, компьютеров и устройств, которые взаимодействуют с приложениями, веб-сайтами, социальными медиа и другими устройствами. Чтобы извлечь из этого максимальную пользу, необходимо обрабатывать и анализировать данные, которые генерируют все эти объекты, в реальном времени».

Можно вывести условную формулу, характеризующую Интернет вещей (IoT) [1], рис. 1.1.

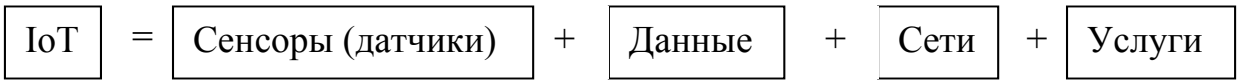


Рисунок 1.1. Образное представление интернета вещей

Решения для Интернета вещей базируются на использовании облачных технологий.

Под конкретной «Интернет вещью (thing)» принято понимать «любой натуральный или искусственный предмет, которому может быть присвоен IP-адрес и который обладает возможностью передачи данных по сети».

В 2009 году количество подключенных к сети предметов превысило количество людей, произошел переход от Интернета людей к Интернету вещей.

Ключевыми поставщиками для Интернета вещей, являются известные мировые компании: Alcatel-Lucent, Cisco, AT&T, Qualcomm, Amazon Web Services (AWS), Apple, ARM Holdings, Digi International, Atmel, Atos, Bosch Software Innovations, Broadcom, CTS, Dell, Echelon, Ericsson, Accenture, Freescale Google, Semiconductor, GE, Hitachi, HP, IBM, Huawei Technologies, Infosys и др.

Принято выделять решения Интернета вещей как для корпоративного сектора (B2B), так и для потребительского сектора (B2C). В потребительском секторе Интернета вещей преобладают бытовые (для дома) и носимые устройства (электроника), умная одежда, т.п. Корпоративный сектор решений для Интернета вещей представлен решениями для промышленного Интернета вещей (IIoT), умного города, электроэнергетики, здравоохранения, управления цепочками поставок, торговли, др. [2].

В настоящее время решения Интернета вещей наиболее активно используются в технологиях «умного дома»: удаленное управление через Интернет домашними устройствами, удаленный мониторинг и управление системами отопления, освещения, медиа − устройствами, электронными системами безопасности, оповещениями о вторжениях, противопожарными системами и пр.

Интернет вещей плотно вошел в нашу жизнь и миллиардов людей по всему миру. Рост количества подключенных устройств ведет к увеличению рисков безопасности: от причинения физического вреда людям до простоев и повреждения оборудования [3].

Заинтересованными сторонами в создании защищенных решений являются участники рынка, владельцы систем и производители средств защиты. Спрос на «реальную защиту» сложных систем и решений только начал формироваться. Внедрение средств безопасности увеличивает совокупную стоимость владения для конечного пользователя. Компании не спешат финансировать создание систем защиты, т.к. не видят экономической целесообразности, практической пользы и конкурентных преимуществ в краткосрочной перспективе.

Объем рынка в области безопасности Интернета вещей в 2019 г. прогнозируется по данным портала [4] на уровне 1,439 млн. долларов. С ростом сегмента рынка решений для Интернета вещей эта цифра будет только увеличиваться.

Традиционно принято выделять следующие направления в области технологий безопасности Интернета вещей [4]:

- безопасность устройств (физическая безопасность, безопасность данных, встроенная безопасность на базе микросхем, безопасная загрузка, аутентификация устройств, управление идентификацией устройств);
- безопасность сетевого взаимодействия (механизмы доступа, файрволлы, системы обнаружения и защиты от вторжений, End–2–End шифрование);

- облачная безопасность (безопасность данных, системы предотвращения утечек, интеграция платформ и приложений, управление угрозами);
- управление безопасностью в процессе жизненного цикла (управление рисками, политиками, аудит безопасности, мониторинг эксплуатации, обновления, управление ИТ-активами).

Вопросы информационной безопасности Интернета вещей носят комплексный характер и должны быть решены на всех уровнях архитектуры решения [5-9].

Концептуальные документы по архитектурам ведущих платформ Интернета вещей содержат раздел, посвященный безопасности:

- эталонная модель IoT (рекомендации Y.2060) [10];
- The Intel IoT Platform: Architecture Specification White Paper [11];
- Microsoft Azure IoT Reference Architecture [12];
- Industrial Internet Reference Architecture [13];
- и др.

Но в большинстве случаев данный раздел декларирует наиболее общие положения и не содержит практических рекомендаций по обеспечению информационной безопасности.

В то же время для 7 уровневой эталонной модели IoT, опубликованной в 2014 г. Комитетом по архитектуре Всемирного форума IoT, специалистами компании Cisco Systems был разработан фреймворк безопасности IoT [14], ставший дополнением эталонной модели.

Следует отдельно сказать, что в основе обеспечения информационной безопасности решений IoT в среде облачной платформы Microsoft Azure лежит методика моделирования угроз информационной безопасности STRIDE, рассматривающая все компоненты и уровни решения IoT с точки зрения возникновения различных угроз. Также предлагаются меры и способы противодействию негативным факторам.

Детальный сравнительный анализ встроенных возможностей по информационной безопасности популярных IoT фреймворков представлен в работе [15].

Объектами сравнения выступают следующие IoT фреймворки – AWS IoT от компании Amazon, ARM Bed от компании ARM, Azure IoT от компании Microsoft, Brillo/Weave от компании Google, Calvin от компании Ericsson, HomeKit от компании Apple, Kura от компании Eclipse и SmartThings от компании Samsung.

Традиционный подход в области информационной безопасности базируется на использовании 3 версии стандарта Common Vulnerability Scoring System (CVSS), который предполагает расчет числового показателя по десятибалльной шкале, на основе которого специалисты по безопасности оперативно принимают решение о том, как реагировать на ту или

иную уязвимость и в какой последовательности решать имеющиеся проблемы. Стандарт был разработан группой экспертов по безопасности National Infrastructure Advisory Council.

Российским аналогом перечня угроз можно считать банк данных угроз безопасности информации ФСТЭК РФ (http://bdu.fstec.ru/ubi).

Однако, для облачных технологий в целом, и технологий Интернета вещей данные подходы не всегда применимы или отсутствует наработанная практика применения. Решение данной проблемы актуально. Ощущается отставание в области обеспечения информационной безопасности.

Вопросам совершенствования методической базы в области информационной безопасности Интернета вещей посвящен ряд работ в этой сфере [3, 6, 7, 16, 17].

В таблице 1.1 [16] представлена классификация типов угроз и мер по их противодействию с учетом уровня архитектуры решения для Интернета вещей. Представленный набор угроз информационной безопасности, конечно же, далеко не полный, но данный набор характеризует концептуальный подход к данному вопросу.

Отдельным направлением для решений Интернета вещей является промышленный Интернет вещей (IIoT), имеющим свои особенности в части обеспечения информационной безопасности.

Анализу текущего положения в области обеспечения кибербезопасности для Индустрии 4.0 и IIoT посвящено большое количество исследований [13, 18, 19].

В основе классификации атак на кибер-производственные системы может лежать 4 признака классификации [20]: по способу атаки, по результату (ущербу) от атаки, по объекту (цели) атаки, по результату атаки. Для каждого признака принято также выделять два подмножества воздействий: кибернетических и физических.

Таблица 1.1. Типы угроз и меры противодействия для различных уровней архитектуры решения Интернета вещей

Уровень архитектуры IoT	Тип угрозы	Меры противодействия
Уровень восприятия (Perception Layer)	- Подмена оборудования; - Внедрение фальшивого узла; - Внедрение вредоносного кода; - Атака на отказ от сна; - Подавление сигнала в беспроводной сети; - Передача шумовых сигналов в беспроводной сети.	- Аутентификация; - Проверка целостности данных; - Безопасная загрузка; - Шифрование канала (IPSec); - Обезличивание персональных данных; - Использование качественных аппаратных компонентов.

Окончание табл. 1.1

Уровень архитектуры IoT	Тип угрозы	Меры противодействия
Сетевой уровень (Network Layer)	- Анализ траффика; - Подмена RFID; - Неавторизованный доступ RFID; - Атака по типу «Воронка»; - Атака по типу «Человек посередине»; - Нарушение маршрутизации.	- Конфиденциальность данных; - Безопасная маршрутизация; - Метрики безопасности для передаваемых пакетов; - Использование средств геолокации; - Механизмы проверки целостности данных.
Уровень обработки (Processing Layer)	- Нарушение модели безопасности приложений; - Несанкционированный доступ к данным; - Проблемы безопасности ИТ – инфраструктуры; - Проблемы с безопасностью при интеграции компонентов решения; - Безопасность для технологий виртуализации; - Безопасность используемых совместно ресурсов.	- Обезличивание данных; - Шифрование; - Сканеры веб-приложений; - Мониторинг и журналы аудита; - Декомпозиция компонентов; - Зоны безопасности.
Уровень приложений (Application Layer)	- Фишинг; - Вирусы, черви, шпионское ПО; - Вредоносные скрипты; - Отказ в обслуживании; - Потери данных; - Уязвимости программного обеспечения.	- Аутентификация; - Списки контроля доступа (ACL листы); - Антивирусы; - Сетевые экраны; - Методики оценки риска.

Существующие подходы к вопросам информационной безопасности промышленного Интернета вещей представлены в табл. 1.2.

Таблица 1.2. Подходы к вопросам информационной безопасности промышленного Интернета вещей (IIoT)

Наименование инициативы	Разработка вопросов кибербезопасности	Стандарты и инициативы
Industrie 4.0 Plattform	Отдельные разделы в рекомендациях по реализации инициатив Industry4.0 (2013)	Recommendations for implementing the strategic initiative INDUSTRIE 4.0

Окончание табл. 1.2

Наименование инициативы	Разработка вопросов кибербезопасности	Стандарты и инициативы
Industrial Internet Consortium (IIC)	Разделы по безопасности референсной Архитектуры Промышленного Интернета. Разработаны на основе стандартов безопасности ИТ и ICS, таких как ENISA, NIST, IEEE, ANSI, ISA, IEC(2015)	Industrial Internet Reference Architecture
Open Interconnect Consortium (OIC)	Набор спецификаций, разрабатываемых в качестве приложений к референсной архитектуре интернета вещей (2015)	OIC Specification - Smart Home Device Specification; - Security Specification; - Resource Specification; - Remote Access Specification; - Core Specification.
Internet Plus Strategy	Разрабатываются стратегические и прикладные инициативы для каждой критичной отрасли	Practical Application - Internet + Manufacturing Industry; - Internet + Finance; - Internet + Medical System; - Internet + Government; - Internet + Agriculture.

Основными элементами обеспечения информационной безопасности цифрового пространства Интернета вещей являются идентификация устройства и механизмы аутентификации.

Рассмотренные проблемы безопасности на каждом архитектурном уровне позволяют принять адекватные меры для повышения уровня безопасности решений Интернета вещей, повысить уровень защищенности.

Поскольку решения Интернета вещей станут частью повседневной жизни в ближайшем будущем, то необходимо предпринимать шаги для обеспечения доверия пользователей к данным информационным технологиям и цифровым платформам.

Литература:

1. Росляков А.В., Ваняшин С.В., Гребешков А.Ю. Интернет вещей: учебное пособие. − Самара: ПГУТИ, 2015. − 200 с.
2. Аналитический отчет компании Forrester Research «The Internet of Things Heat Map − 2018», [Электронный ресурс]. URL: https://www.forrester.com (дата обращения: 14.10.2018).
3. Singh S., Jeong Y., Park J. H. A survey on cloud computing security: Issues, threats, and solutions // Journal of Network and Computer Applications 75 (2016) − P. 200-222.

4. Аналитический отчет IOT Analytics: IoT security market report 2017-2022 [Электронный ресурс]. URL: https://iot-analytics.com/ (дата обращения: 14.10.2018).
5. Аналитический отчет «Industrial Internet Insights Report 2015» [Электронный ресурс]. URL: https://www.accenture.com (дата обращения: 14.10.2018).
6. Das A. K., Zeadally S., He D. Taxonomy and analysis of security protocols for Internet of Things // Future Generation Computer Systems 89 (2018) − P. 110-125.
7. Khan M.A., Khaled S. IoT security: Review, blockchain solutions, and open challenges // Future Generation Computer Systems 82 (2018) − P. 395-411.
8. Shancang Li Introduction: Securing the Internet of Things // Securing the Internet of Things, 2017 − P. 1-25.
9. Singh J., Pasquier T., Bacon J., Ko H., Eyers D. Twenty security considerations for cloud-supported Internet of Things // Internet Of Things Journal, IEEE Vol. 3, Iss. 3, June 2016.
10. Интернет вещей: сетевая архитектура и архитектура безопасности // Информационный сборник «Интернет изнутри» [Электронный ресурс]. URL: http://internetinside.ru/internet-veshhey-setevaya-arkhitektura-i/ (дата обращения: 14.10.2018).
11. The Intel IoT Platform: Architecture Specification White Paper [Электронный ресурс]. URL: https://www.intel.sg/content/www/xa/en/internet-of-things/white-papers/iot-platform-reference-architecture-paper.html (дата обращения: 14.10.2018).
12. Microsoft Azure IoT Reference Architecture [Электронный ресурс]. URL: https://aka.ms/iotrefarchitecture (дата обращения: 14.10.2018).
13. Industrial Internet Reference Architecture // Industrial Internet Consortium (IIRA) [Электронный ресурс]. URL: https://iiconsortium.org (дата обращения: 14.10.2018).
14. Securing the Internet of Things: A Proposed Framework [Электронный ресурс]. URL: https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html (дата обращения: 14.10.2018).
15. Ammar M., Russello G., Crispo B. Internet of Things: A survey on the security of IoT frameworks // Journal of Information Security and Applications 38 (2018) – P.8-27 [Электронный ресурс]. URL: https://doi.org/10.1016/j.jisa.2017.11.002 (дата обращения: 14.10.2018).
16. Ahemd M. M., Shah M. A., Wahid A. IoT Security: A Layered Approach for Attacks & Defenses // International Conference on Communication Technologies (ComTech), IEEE, 2017.
17. Alabaa F. A., Othmana M., Hashema I. A. T., Alotaibib F. Internet of Things security: A survey // Journal of Network and Computer Applications 88 (2017) − P. 10-28.
18. China Internet Plus Strategy (SESEC III Report) [Электронный ресурс]. URL: http://sesec.eu (дата обращения: 14.10.2018).
19. Lezzi M., Lazoi M., Corallo A. Cybersecurity for Industry 4.0 in the current literature: A reference framework // Computers in Industry 103 (2018). – P. 97-110.
20. Wu M., Moon Y. B. Taxonomy of Cross-Domain Attacks on Cyber Manufacturing System // Procedia Computer Science 114 (2017). − P. 367-374.

1.3. Проблема стандартизации в области Интернета вещей

Концепция Интернета вещей – активно развивающееся направление сегодня во всех странах, однако отставание российского рынка в этой области пока остается заметным. Долгое время «умные вещи» были дорого-

стоящими и, соответственно, мало распространенными. Последние несколько лет наблюдается тенденция развития доступных устройств, способных посредством объединения в сеть, обмениваться друг с другом информацией с участием пользователя или без него. И, если цены на устройства, которые являлись одним из сдерживающих факторов развития Интернета вещей, существенно снижаются, и устройства становятся более доступными, то по-прежнему остается актуальной другая проблема – отсутствие стандартизации в этой области.

Проблема отсутствия стандартов замедляет общее развитие концепции Интернета вещей как таковой. Это объясняется тем, что в условиях отсутствия стандартов каждая компания вынуждена тратить деньги на проработку одного и того же, и в итоге суммарный эффект в продвижении отрасли получается небольшим. Наличие стандартов позволяет усовершенствовать или использовать иначе то, что уже существует. Кроме этого, конечно же, наличие стандартов позволяет объединять в сеть устройства различных типов и видов, вне зависимости от производителя или форм-фактора.

Стоит отметить, что в условиях глобализации, страны, уделяющие внимание внедрению и разработке стандартов, обеспечивают себе технологическое лидерство. Наличие проработанных, качественных стандартов позволяет снизить издержки в рамках отрасли и страны, повысить конкуренцию.

Можно говорить о том, что все развитые страны участвуют во внедрении протоколов и стандартов Интернета вещей.

Привычной является практика объединения крупных компаний в ассоциации и альянсы, которые призваны решать, в том числе, и проблемы стандартизации. Наиболее известные среди них 4 крупнейших объединения [1].

1. The AllSeen Alliance (работает с 10 декабря 2013 года) – альянс направлен на решение вопросов, связанных с разработкой стандартов в области передачи данных между устройствами («вещами») и совместимостью устройств с существующими ОС.

2. The Open Interconnect Consortium (работает с 15 февраля 2014 года) – напрямую не занят в разработке стандартов, но работает над единой коммуникативной платформой, которая позволит объединить «умные вещи», принимает участие в доработке технологических стандартов после прохождения ими практических испытаний.

3. The Thread Group (работает с 25 июля 2014 года) – альянс делает ставку на разработку единого радиопротокола с низким уровнем потребления энергии. На данный момент работает над технологией 6LoWPAN.

4. Industrial Internet Consortium (работает с 27 марта 2014 года) – направлен на создание стандартов в области связи и безопасности.

В настоящие консорциумы входят крупные компании из сферы коммуникаций, разработки программного обеспечения, а также активно включаются компании, представляющие потребительский сектор. Такие компании, в первую очередь, привлекаются в качестве участников испытаний практической применимости разрабатываемых стандартов.

IETF (Internet Engineering Task Force) – открытое международное сообщество проектировщиков, ученых, сетевых операторов и провайдеров, которое уже больше десятилетия работает над выработкой спецификаций и документированием ключевых стандартов и рекомендаций в области Интернета вещей. Различные рабочие группы IETF занимаются вопросами адаптации и применимости существующих стандартов и протоколов в специфичных сетях «умных устройств», которые имеют свои ограничения. В последние несколько лет стали создаваться рабочие группы, направленные на проработку, в том числе, и стандартов безопасности в Интернете вещей.

В начале 2018 года Американский Национальный институт стандартов и технологий (NIST) представил проект документа «Статус международной стандартизации кибербезопасности Интернета вещей» («The Status of International Cybersecurity Standardization for IoT»), призванный помочь разработать международные стандарты безопасности для Интернета вещей. В рамках данного стандарта NIST предлагает разделить устройства Интернета вещей на пять функциональных областей: подключенные устройства, устройства потребительского класса, медицинское оборудование и устройства, используемые в сфере здравоохранения, умные здания, умное производство (в том числе, АСУ ТП) [2].

Исходя из того, что устройства из разных функциональных областей имеют свои особенности и призваны решать разные задачи, стандарты должны быть приняты для каждой из областей. Такой подход имеет ряд недостатков: во-первых – это время, требуемое на разработку, испытания и принятия каждого из стандартов в отдельной функциональной области. Кроме того, подход к стандартизации для разных функциональных областей не решает задачу полной унификации разрабатываемых решений для устройств Интернета вещей.

Возможно, упростить задачу стандартизации можно, используя подход к разделению устройств по ключевым свойствам безопасности, которые должны обеспечивать те или иные устройства.

Известно, что ключевыми свойствами безопасности являются конфиденциальность, целостность и доступность, при этом в Интернете вещей приоритетным, как правило, является обеспечение доступности. Безусловно, можно выделить и класс устройств, для которых на первом месте с точки зрения приоритетов будет находиться конфиденциальность. Однако обеспечение стандартизации по приоритетному свойству безопасности

можно предусмотреть на более высоком уровне модели взаимодействия, обеспечив унифицированную стандартизацию на более низких уровнях, таких как, например, физическом, канальном и транспортном.

Такой подход позволил бы принять унифицированный стандарт, регламентирующий разработку устройств Интернета вещей по общепринятым протоколам, адаптированным для данных устройств, а вопросы безопасности решались бы на прикладном уровне, являясь надстройкой в зависимости от назначения устройств.

В России ТК 194 «Кибер-физические системы» (Технический комитет «Кибер-физические системы) является ключевым участником реализации мероприятий в планах по направлению «Нормативное регулирование» программы «Цифровая экономика Российской Федерации» по разработке проектов национальных стандартов в области технологий «Большие данные», «Интернет вещей» и «Промышленный (индустриальный) интернет вещей», «Искусственный интеллект». На сегодняшний день ТК 194 уже разработал стандарт терминологии в сфере Интернета вещей, внедрение которого планируется синхронно с англоязычной версией. Ожидается, что внедрение данного стандарта позволит облегчить коммуникации между заказчиками, исполнителями и потребителями на рынке «интернета вещей», уменьшит вероятность ошибок при составлении технических заданий, проектировании систем и приемке работ.

Кроме этого в соответствии с программой разработки национальных стандартов на 2018 г. на официальном сайте ТК 194 «Кибер-физические системы» [3] была размещена первая редакция проекта ПНСТ «Информационные технологии. Интернет вещей. Протокол обмена для интернета вещей в узкополосном спектре (NB-Fi)». Настоящий стандарт предназначен для построения беспроводных сетей обмена данными между множеством конечных устройств (модемов) с одной стороны, и множеством устройств – с другой. Стандарт входит в линейку протоколов LPWAN и занимает особое место для средств телеметрии и управления киберфизическими объектами, благодаря своей простоте и дешевизне. Высокая энергоэффективность позволяет использовать для работы нелицензируемые диапазоны частот, в которых установлены ограничения на излучаемую передатчиками мощность.

Также ТК 194 представил проект международного стандарта в области промышленного Интернета вещей (IIoT), который направлен в адрес Международной организации по стандартизации ISO/IEC от имени Российской Федерации для международного голосования. Документ устанавливает единые требования к совместимости различных устройств и систем промышленного Интернета вещей. Принятие стандарта позволит заказчикам технологии IIoT использовать решения и оборудование от различных разработчиков и предприятий-изготовителей, а также проводить корректные испытания решений и оборудования на совместимость.

Таким образом, в связи с повсеместным развитием Интернет- технологий и устройств сети Интернета вещей, одной из актуальных проблем становится стандартизация в этой области. Участие стран в разработке, принятии и внедрении стандартов повышает конкурентоспособность и открывает возможности на мировом рынке. Несмотря на то, что развитие Интернета вещей в России в заметной степени отстает от уровня ведущих стран, на сегодняшний день комитеты по стандартизации в нашей стране ведут активную деятельность и участвуют в реализации проектов на мировом уровне.

Принимаемые стандарты подлежат публичному обсуждению, а также обязательной апробации в условиях функционирующих сетей. Стандартизация является ключевым фактором обеспечения унификации разрабатываемых устройств и поддерживающих их приложений, поэтому принимаемый стандарт должен охватывать как можно больше типов устройств, исключая необходимость принятия огромного количества смежных стандартов.

Литература:

1. Астахов М.И. Интернет вещей: роль стандартов //Техноспецназ, февраль 2017 [Электронный ресурс]. URL: техноспецназ.рф/2017/02/28/internet-veshhej-rol-standartov/. (Дата обращения: 02.11.2018).
2. NIST предложил принципы международной стандартизации безопасности в IoT, 20.02.2018 [Электронный ресурс]. URL: http://pro-iot.pro/materials/tekhnika-i-tekhnologii/news/nist-predlozhil-printsipy-mezhdunarodnoy-standartizatsii-v-iot-/ (Дата обращения: 04.11.2018).
3. ТК 194 «Кибер-физические системы» [сайт]. URL: http://tc194.ru/ (Дата обращения: 11.11.2018).

1.4. Безопасность мессенджеров

Широкое распространение и рост функциональности мобильных устройств (планшетных ПК, смартфонов), развитие мобильных операционных систем и разнообразие предоставляемых ими средств коммуникации в условиях относительной ограниченности аппаратных ресурсов остро ставит вопрос безопасности. Ниже будут более подробно рассмотрены проблемы и методы обеспечения безопасности мессенджеров, тесно связанные с общими вопросами обеспечения информационной безопасности мобильных платформ.

Под мессенджером (Instant Messenger, IM) будем понимать систему для обмена сообщениями в режиме реального времени через Интернет, голосовой и видеосвязи, обмена файлами, организации групповых видеоконференций (групповых чатов), и соответствующее программное

обеспечение (программы, мобильные приложения или веб-сервисы). Наибольшую известность в настоящее время получили мессенджеры WhatsApp, Viber, Skype, Telegram, ICQ, Facebook Messenger, Hangouts (являющийся стандартным сервисом Google) и др. В России отдают предпочтение первым четырем продуктам из этого списка, кроме того личная переписка ведется в рамках социальных сетей, таких как «ВКонтакте» и Facebook, востребованных также и пользователями десктопных систем через веб-сервисы. При этом в среднем каждый абонент пользуется 3 различными системами обмена сообщений [1].

Общий рост внимания к проблемам безопасности, наряду с обострением конкуренции среди мессенджеров, происходящее на фоне скандалов, связанных с продажей пользовательских данных компанией Facebook и блокированием мессенджера Telegram, использованное разработчиком последнего для продвижения идеи о защищенности своей системы, заставляет разработчиков внедрять дополнительные средства защиты, такие как end-to-end шифрование передаваемых данных.

Наряду с мессенджерами, которые изначально разрабатывались и позиционировались как защищенные (Signal Private Messenger, Threema, Wire, Wickr Me, Dust), в 2016 году включено полное шифрование сообщений, голосовых звонков и пересылаемых файлов в мессенджерах WhatsApp и Viber, в ICQ стали шифроваться не только текстовые сообщения, но аудио и видео, а в Facebook Messenger появились «секретные» чаты. В 2018 году систему оконечного шифрования чатов и звонков в рамках «личной беседы» ввел Skype, а «ВКонтакте» для iOS и Android запустил шифрование голосовых и видеозвонков.

«Секретные» чаты поддерживаются и в Telegram, однако в обычном режиме облачных чатов, используемом по умолчанию, данные «видны» серверам Telegram в открытом виде. При этом PR-компания мессенджера строилась на заверениях его владельцев, что никакие спецслужбы не смогут прочесть личные сообщения, и проводилась для англоязычной аудитории под лозунгом «Taking back our right to privacy» («вернем себе право на приватность»). По заявлениям Павла Дурова, «с самого первого дня мы не передали правительствам и третьим лицам ни байта приватных данных». Таким образом, защищенность мессенджера Telegram обеспечивается скорее не техническими мерами, а политикой компании. Однако в августе 2018 года Telegram был вынужден внести изменения в политику конфиденциальности мессенджера в рамках нового европейского закона о защите персональных данных GDPR (General Data Protection Regulation), добавив пункт о возможности раскрытия IP-адреса и номера телефона абонента на основании судебного решения, подтверждающего, что абонента подозревают в терроризме.

Это отражает еще одну тенденцию в обеспечении безопасности мессенджеров, обусловленную усилением регулирования со стороны госу-

дарства, стремящегося, по возможности, деанонимизировать коммуникации на случай необходимости их контроля. В этом ряду стоит и появившееся в августе 2018 года сообщение об отказе WhatsApp от используемой в настоящее время технологии оконечного шифрования. Новая версия приложения, реализующая ослабленное шифрование в соответствии с требованиями властей США, выйдет в 2019 году.

Мессенджеры используют собственные протоколы передачи данных, при этом шифрование сообщений обычно выполняется на прикладном уровне, а затем зашифрованные данные встраиваются в транспортный протокол. В качестве транспортного протокола, как правило (но необязательно), используется SSL/TLS, ставший де-факто стандартом для всех защищенных web-коммуникаций. Вместе с тем, реализация последнего на мобильных платформах бывает далека от совершенства [2, 3].

Для защиты передаваемых данных мессенджеры, как правило, используют end-to-end (E2E, оконечное или сквозное) шифрование. Это значит, что криптографические ключи генерируются и хранятся на конечном устройстве (устройстве пользователя), а не на серверах системы мгновенных сообщений. Поэтому никто, кроме адресата, даже сервер системы, не сможет прочитать содержимое зашифрованных сообщений. С другой стороны, переписка будет не доступна и самому абоненту, если он перейдет на другое устройство. Поэтому синхронизация устройств или восстановление в случае потери устройства (то есть получение доступа к архиву переписки) совместно с использованием оконечного шифрования невозможно без депонирования личного ключа вне устройства.

Поскольку оконечное шифрование реализуется на верхних уровнях сетевой архитектуры, адресные данные должны быть доступны в незашифрованном виде в промежуточных узлах (то есть, на серверах системы). А это значит, что метаданные коммуникаций пользователей (кто кому звонил или писал, и когда) остаются открытыми.

Многие мессенджеры в настоящее время реализуют оконечное шифрование на основе протокола Signal, разработанного некоммерческой организацией Open Whisper Systems (OWS) для одноименного мессенджера. Протокол тщательно документирован [4] и имеет реализующие его библиотеки с открытым исходным кодом на языках Java, C и JavaScript. На сегодняшний день протокол Signal используется мессенджерами WhatsApp, Google Allo, Facebook Messenger и Skype. Реализация шифрования Viber использует концепции протокола Signal, но другие криптографические алгоритмы. По заявлениям разработчиков Wire, используемый в этом мессенджере протокол шифрования Proteus также основан на протоколе Signal.

Протокол использует криптографию с открытым ключом на эллиптической кривой Curve25519 или Curve448 для цифровых подписей, со-

гласование ключей на основе модификации протокола Диффи-Хэллмана, шифрование сообщений с помощью симметричного алгоритма AES-256 в режиме CBC и проверку целостности с помощью кода аутентификации HMAC-SHA256. Кроме того, для изменения ключей шифрования в течение сеанса связи используется функция диверсификации ключа (KDF, Key Derivation Function) на основе HMAC-SHA256 и HMAC-SHA512 (HKDF). Все используемые протоколом криптографические примитивы хорошо известны и рекомендованы для применения в системах защиты информации. Безопасность протокола проанализирована в [5].

Основные особенности протокола Signal обусловлены тем, что вторая сторона коммуникаций может быть недоступна (находиться в автономном режиме, офлайн) в момент отправки сообщения. Поэтому стандартные протоколы аутентификации и обмена ключами (AKE, Authenticated Key Exchange) не могут быть непосредственно применены. Например, в классическом протоколе Диффи-Хэллмана (DH) в формировании общего секретного ключа принимают участие обе стороны, поскольку значение ключа вычисляется на основе секретных ключей обоих абонентов. При этом абоненты открыто обмениваются значениями, которые можно трактовать как открытые ключи криптосистемы DH.

Для решения проблемы автономности одной из сторон Signal реализует асинхронный протокол передачи X3DH, требуя предварительной отправки на промежуточный сервер партии предварительно вычисленных значений (открытых ключей). Такая отправка производится во время регистрации или позже (рис. 1.2). Когда абонент желает отправить сообщение, он получает необходимые для выполнения AKE-подобного протокола значения получателя с промежуточного сервера (который действует только как буфер) и вычисляет ключ шифрования сообщения.

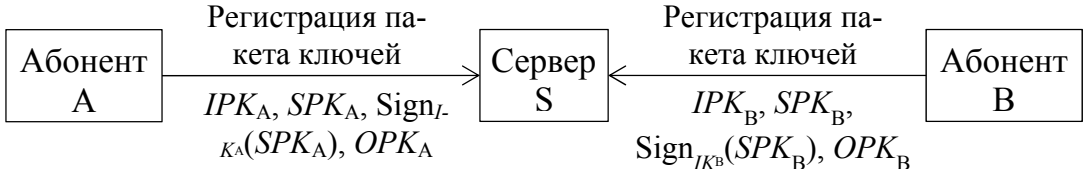


Рисунок 1.2. Первый этап протокола Signal – регистрация ключевой информации пользователей

На этапе регистрации до начала обмена сообщениями каждый абонент формирует 3 типа ключей асимметричной схемы: долговременный ключ *IK* (для подписи), среднесрочный предварительный ключ *SK* и набор одноразовых предварительных ключей *OK*. При этом на сервер отправляются только соответствующие им открытые ключи *IPK*, *SPK*, *OPK* и подпись ($Sign_{IK}(SPK)$ – среднесрочный открытый ключ *SPK* подписывается долговременным ключом *IK* абонента).

Абонент может периодически (например, раз в неделю или раз в месяц) обновлять свой среднесрочный открытый ключ *SPK* с подписью, а также в любое время загружать новый набор предварительных одноразовых открытых ключей *OPK* (например, когда сервер информирует Боба о том, что их запас на сервере снизился). Долговременный ключ *IPK* является идентификационным и регистрируется абонентом однократно.

Пусть абонент А хочет начать сеанс связи с абонентом В (рис. 1.3). Абонент А запрашивает у сервера и получает пакет ключей абонента В, а затем вычисляет секретный ключ *SK* из нескольких значений протокола DH, полученных на основе значений идентификационных ключей обоих абонентов IPK_A, IPK_B, среднесрочного открытого ключа получателя SPK_B и краткосрочного открытого ключа EPK_A из вновь сгенерированной отправителем пары ключей асимметричного шифрования.

$DH_1 = DH(IK_A, SPK_B)$

$DH_2 = DH(EPK_A, IK_B)$

$DH_3 = DH(EPK_A, SPK_B)$

$DH_4 = DH(EPK_A, OPK_B)$

$SK = \mathrm{KDF}(DH_1 \parallel DH_2 \parallel DH_3 \parallel DH_4)$

Если на сервере исчерпан запас одноразовых предварительных ключей OPK_B, то значение DH_4 опускается.

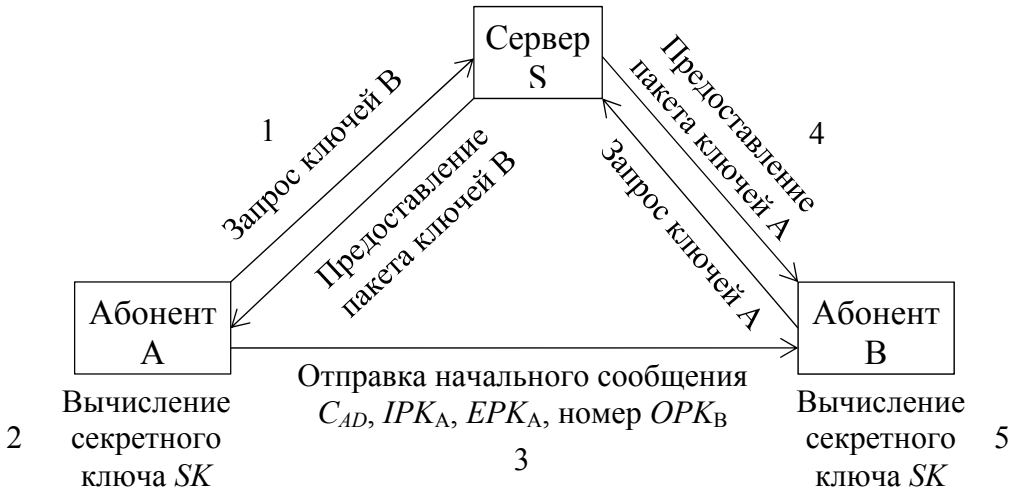


Рисунок 1.3. Второй этап протокола Signal – установка сеанса связи

SK служит основой для формирования цепочки ключей шифрования сообщений. Когда ключ шифрования создан, абонент А шифрует симметричным алгоритмом свое идентификационное сообщение *AD*, составленное из значений идентификационных ключей отправителя и получателя, а также любой дополнительной идентификационной информации – имен абонентов, сертификатов и т.п.

Затем A отправляет получателю B криптограмму C_{AD}, свой идентификационный ключ IPK_A, краткосрочный открытый ключ EPK_A, и информацию о том, какой из предварительных ключей OPK_B был использован для получения ключа шифрования сообщения.

Получив всю эту информацию, абонент B сможет сформировать ключ *SK* для расшифрования сообщения. Если сообщение расшифровано удачно и идентификационная информация корректна, B продолжает использовать цепочку ключей, полученных из *SK*, для шифрования своего сообщения.

Использованные одноразовые ключи OPK_B удаляются сервером, а соответствующие им OK_B – абонентом B.

Следует отметить, что если взаимодействие абонентов с сервером S и друг с другом происходит в недоверенной среде, то возможна реализация угрозы «человек посередине» (MITM, the man in the middle), позволяющей нарушителю подменять ключи при передаче и выдавать себя за любую из сторон коммуникации. Как правило, данная проблема решается с помощью цифровой сертификации и развертывания инфраструктуры открытых ключей PKI, однако протоколом Signal они не описываются, а промежуточный сервер не играет роли центра сертификации.

Защиту от реализации атак «человек посередине» призвано обеспечить использование на нижнем уровне защищенного транспортного протокола (SSL/TLS), однако на практике его реализации в мобильных приложениях зачастую уязвимы для этого типа атак [2, 3]. Кроме того, использование SSL/TLS сохраняет возможность реализации MITM атак на самом сервере (например, в случае контроля со стороны спецслужб и администраторов системы).

Для подтверждения подлинности второй стороны абоненты могут сравнивать полученный идентификационный ключ *IK* через некоторый аутентифицированный канал. Например, они могут сравнивать отпечатки цифровой подписи вручную или путем сканирования QR-кода. Методы создания такого аутентифицированного канала выходят за рамки описания протокола Signal. Проверка подлинности сторон по внешнему каналу может производиться до или после процедуры согласования ключа, однако, как указано в [5] в большинстве реализаций такая проверка может быть произведена лишь после обмена сообщениями.

Еще более остро стоит проблема подтверждение подлинности сервера распределения ключей S во время регистрации, никак не определенное в спецификации протокола Signal. Без обеспечения доверия к серверу существует возможность подмены личности любого абонента. Таким образом, решение вопроса взаимной аутентификации сервера и клиента ложится на конкретную реализацию мессенджера. Как правило, при установке приложение мессенджера привязывается к конкретному телефон-

ному номеру, и клиент аутентифицируется с помощью одноразовых SMS-паролей. Аутентификация сервера может проводиться на нижнем уровне с помощью цифровых сертификатов (как в браузерах), либо с помощью проверки отпечатков открытого ключа, данные о которых могут быть «защиты» в клиентском приложении (как это сделано, например, в Telegram).

Для снижения негативного эффекта от возможной компрометации ключей используется оригинальный Double Ratchet алгоритм, описывающий смену краткосрочного ключа асимметричной схемы *EK/EPK* с каждым ответным сообщением и смену симметричных ключей в порождаемой им ключевой цепочке (для шифрования каждого сообщения используется свой ключ). Согласованное с помощью DH значение секретного ключа *SK* служит основой для получения отправного ключа цепочки (*RK*, root key), ключа цепочки (*CK*, chaining key) и ключа шифрования сообщения (*MK*, message key). Ключ цепочки CK_{j+1} получаются из предыдущего CK_j с помощью конструкции HMAC.

Алгоритм формирования цепочки ключей симметричного шифрования на стороне одного из абонентов (абонента 1) показан на рис. 1.4.

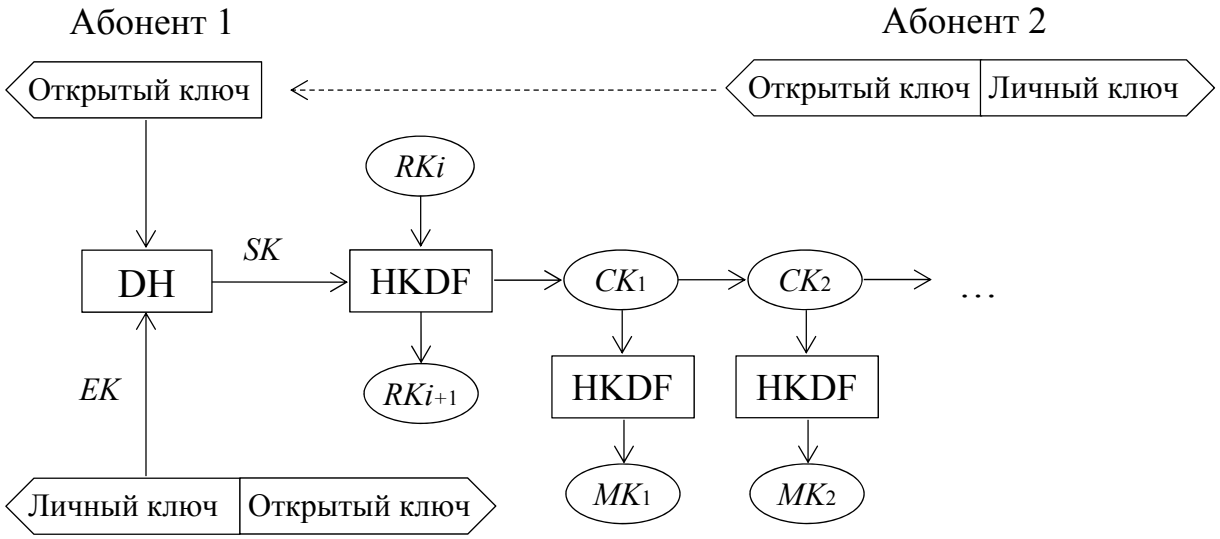


Рисунок 1.4. Формирование цепочек ключей шифрования сообщений

Когда абонент расшифровывает полученное сообщение, он использует для формирования цепочки свое старое значение личного ключа и присланное ему значение открытого ключа другого абонента. В результате ключи расшифрования совпадут с ключами, использованными для шифрования.

Если же абонент хочет послать ответное сообщение, он формирует новую пару кратковременных ключей *EK/EPK* асимметричной схемы, и использует ее для формирования новой цепочки, а открытый ключ *EPK* новой пары отсылает вместе с зашифрованным сообщением.

Если же абонент хочет послать следующее сообщение, не получив ответ на предыдущее, он использует следующий ключ шифрования сообщения из текущей цепочки, не обновляя ключи асимметричной схемы.

Таким образом, симметричные ключи в цепочках выводятся KDF на основе новых значений DH на каждом этапе, поэтому каждое обновление требует знания свежей информации. Поэтому даже если какой-то среднесрочный или краткосрочный ключ был скомпрометирован, он будет вскоре заменен новым, неизвестным нарушителю значением.

Такой подход позволяет обеспечить специфические свойства безопасности, такие как прямая секретность (forward secrecy) и безопасность после компрометации, или посткомпрометационная секретность (post-compromise security, post-compromise secrecy) [6].

Использование однонаправленных хэш-функций (или HMAC) для формирования цепочки ключей $x \to H(x) \to H(H(x)) \to \ldots$ позволяет обеспечить свойство прямой секретности. Это свойство означает, что если был скомпрометирован текущий ключ, предыдущие значения ключей не могут быть вычислены нарушителем. Это значит, что даже в случае компрометации текущего ключа, нарушитель не сможет расшифровать и прочитать сообщения, отправленные раньше.

Использование же для порождения цепочек обновляющихся согласованных значений DH обеспечивает свойство безопасности после компрометации (post-compromise security). Это свойство позволяет гарантировать безопасность протокола даже в том случае, если секреты одной из сторон ранее были скомпрометированы (рис. 1.5). Можно сказать, что гарантия прямой секретности защищает сеансы от компрометации, произошедшей в последующие моменты времени, а посткомпрометационная секретность защищает сеансы от компрометации, произошедшей ранее.

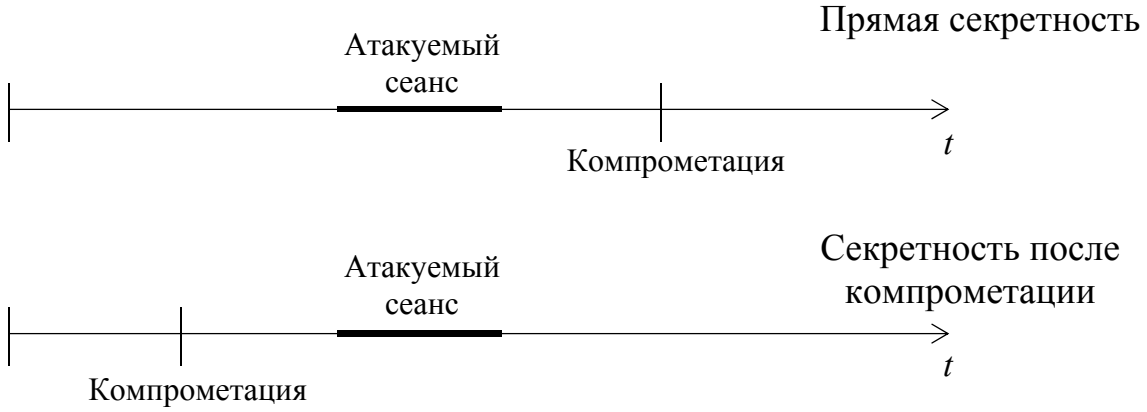


Рисунок 1.5. Сценарии атак, рассматриваемые в рамках будущей секретности и посткомпрометационной секретности

Алгоритм Double Ratchet позволяет учесть недоставленные сообщения за счет включения в каждый заголовок сообщения его номера в цепочке отправки и длину предыдущей цепочки отправки. Это позволяет получателю перейти к соответствующему ключу сообщения при сохранении значений пропущенных ключей на случай, если пропущенные сообщения поступят позже. Вместе с тем, сохранение устаревших ключей несколько ослабляет обеспечиваемое алгоритмом Double Ratchet свойство прямой секретности. X3DH также обладает свойством будущей секретности.

Авторами исследования [5], опиравшимися в том числе и на анализ кода протокола Signal, не было найдено у него существенных недостатков с точки зрения применения криптографии (при условии создания аутентифицированного канала обмена данными между абонентами и с сервером). Ошибки в коде протокола, связанные с нарушением граничных значений в протоколе (например, использование нулевых значений ключа), а также общие классы ошибок программного обеспечения рассмотрены в [7].

Реализации мессенджеров содержат наряду с кодом библиотек протокола Signal значительный объем стороннего кода. Вместе с тем, каждое применение протокола имеет свои особенности, что может существенно сказаться на надежности оконечного шифрования. При этом анализ большинства реализаций затруднен в связи с закрытостью их кода (WhatsApp, Viber, Skype, Wickr, Threema). Например, известны проблемы с реализацией протокола в системе WhatsApp, которое позволяет серверу принудительно менять ключи пользователя, что в свою очередь может привести к раскрытию недоставленных сообщений [8]. Подобная уязвимость отсутствует в мессенджере Signal. Несовершенна и защита групповых чатов WhatsApp, несмотря на использование сквозного шифрования [9-11].

Кроме того, протокол Signal был в дальнейшем дополнен алгоритмом управления сеансами пользователей для обеспечения синхронизации переписки на разных устройствах, управления параллельными сеансами и восстановления из резервных копий. В этом подпротоколе полномочия сервера существенно расширены, а компрометация хотя бы одного устройства ставит под угрозу безопасность всей коммуникации. Документация к алгоритму управления сеансами лишь указывает на то, что связь между устройствами и серверами должна быть зашифрована и аутентифицирована, по-прежнему не оговаривая способов решения этих задач.

Дополнительно источником проблем безопасности может быть некорректная реализация процедур, не имеющих прямого отношения к протоколу. Так, например, клиентская часть мессенджера Signal в процессе миграции от расширения для Chrome до полноценного десктопного кли-

ента экспортирует сообщения пользователя в незашифрованные текстовые файлы. При этом никаких предупреждений не выводится, а созданные файлы остаются на диске даже после завершения апгрейда [12].

В отличие от уже упомянутого WhatsApp, мессенджер Telegram использует собственный протокол MTProto, безопасность которого, несмотря на заявления разработчиков, является спорным вопросом [13]. Telegram позиционируется как система с открытым кодом, однако в свободном доступе отсутствует исходный код серверной части, кроме того, используемые решения не столь подробно документированы, как в Signal.

Протокол определяет 3 уровня: высокоуровневый слой, определяющий взаимодействие приложения с API, криптографический слой и компонент доставки, ответственный за выбор способа передачи сообщений (транспортного протокола).

Криптопротокол MTProto за время своего существования претерпел несколько изменений, и в настоящее время использует асимметричную криптосистему RSA-2048, согласование ключа Диффи-Хэллмана, симметричное шифрование с помощью алгоритма AES-256 в режиме IGE и хэш-функцию SHA-256.

На начальном этапе производится аутентификация клиента на основе обмена случайными значениями и регистрация сформированного им открытого ключа асимметричной пары на сервере (рис. 1.6). Аутентификация устройства клиента производится с помощью отправки SMS-кода на телефонный номер, указанный при регистрации. Если в дальнейшем пользователь осуществит вход с другого устройства, ему будет вновь выслан SMS-код.

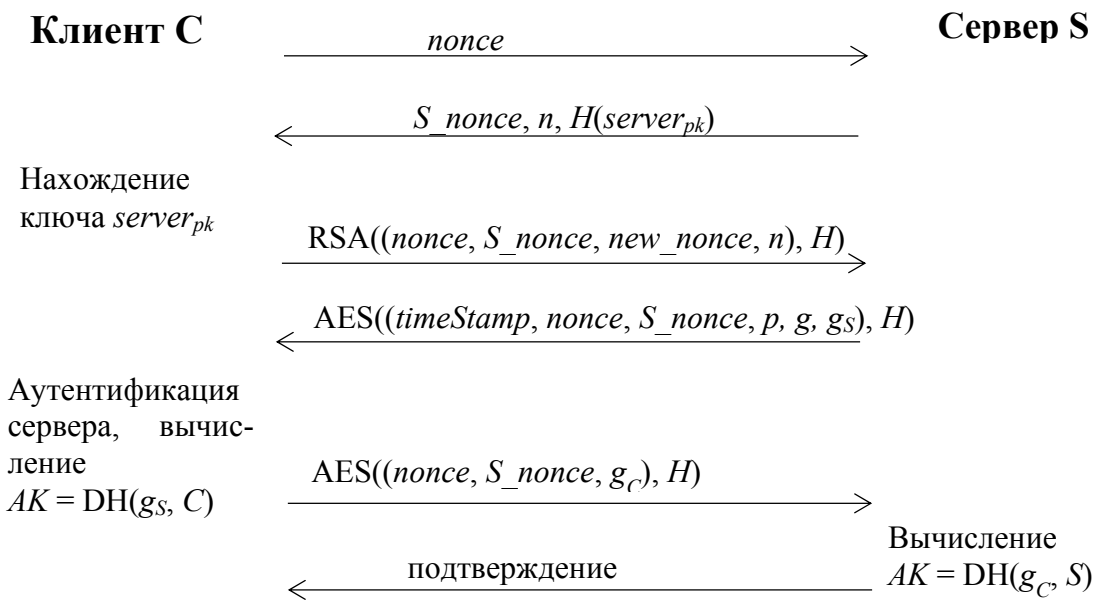


Рисунок 1.6. Регистрация клиента в протоколе MTProto

1. Клиент C отправляет запрос на сервер S со случайной строкой *nonce*.
2. S отправляет в ответ другую случайную последовательность *S_nonce*, целое число n (64 бита) и отпечаток открытого RSA-ключа сервера.
3. Клиент C раскладывает n на два простых числа p и q, $p < q$, и выбирает из набора публичных ключей сервера, хранящийся на устройстве, открытый ключ $server_{pk}$, который должен соответствовать пришедшему с сервера отпечатку.
4. C выбирает другую случайную строку *new_nonce*, отличающуюся от предыдущих строк *nonce* и *S_nonce*. Эта строка в открытом виде не передавалась. Затем клиент собирает набор из трех случайных строк, чисел n, p и q, вычисляет его хэш H и шифрует все это по алгоритму RSA с помощью ключа $server_{pk}$ и отправляет на сервер S.
5. В ответ сервер S передает свою метку времени, значения *nonce* и *S_nonce* (что позволяет клиенту аутентифицировать сервер), а также параметры криптосистемы Диффи-Хэллмана g, p и свой открытый DH ключ g_S, и хэш содержимого. Полученный пакет дополняется случайными значениями и передается в зашифрованном виде. Для шифрования используется алгоритм AES-256 на временном ключе и с вектором инициализации, полученным на основе *S_nonce* и *new_nonce* (рис. 1.7).
6. Клиент проверяет присланные значения, а затем выбирает секретное число C и вычисляет с помощью криптосистемы Диффи-Хэллмана общий секретный ключ $AK = \mathrm{DH}(g_S, C)$ и свой открытый ключ g_C. Затем g_C, значения *nonce* и *S_nonce* и хэш всего пакета шифруются AES и отправляются на сервер S.
7. Полученные S значения достаточны для формирования сервером общего секретного ключа AK. Если все присланные клиентом значения правильны, сервер посылает ответ с подтверждением (или с отказом в противном случае).

Общий секретный ключ AK теперь может использоваться для шифрования обмена данными между клиентом и сервером при использовании облачных чатов (без оконечного шифрования).

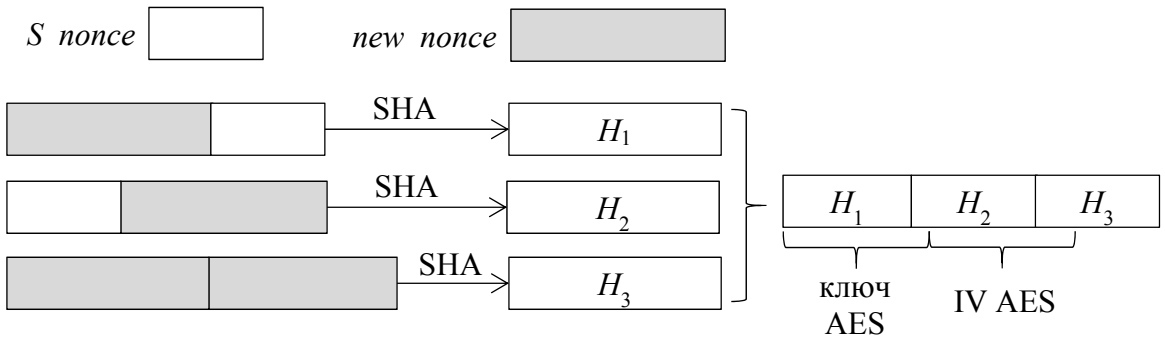


Рисунок 1.7. Формирование временного ключа
и вектора инициализации шифра AES во время регистрации MTProto

Оконечное шифрование в режиме секретных чатов выполняется следующим образом. При инициализации секретного чата пользователи А и В выполняют стандартный протокол Диффи-Хэллмана согласования общего ключа *AK* без предварительной аутентификации сторон. Согласование общего ключа периодически проводится заново. Как уже отмечалось, поскольку согласование ключа производится без аутентификации канала, это делает возможным реализацию классической атаки «человек посередине». Пользователям предлагается перед обменом сообщениями проводить визуальную сверку отпечатков *AK* в виде графического кода.

Само шифрование сообщений пользователя производится по схеме, представленной на рис. 1.8 (заливкой здесь отмечены секретные параметры шифрования). Дополнительная информация, добавляемая к сообщению при шифровании, включает исходящий и входящий номер сообщения, случайные значения соли и дополнения, общую длину и другие значения. В процедуре шифрования, используемой в облачных чатах, добавляемая к сообщению дополнительная информация несколько отличается, общая же структура процедуры шифрования остается неизменной.

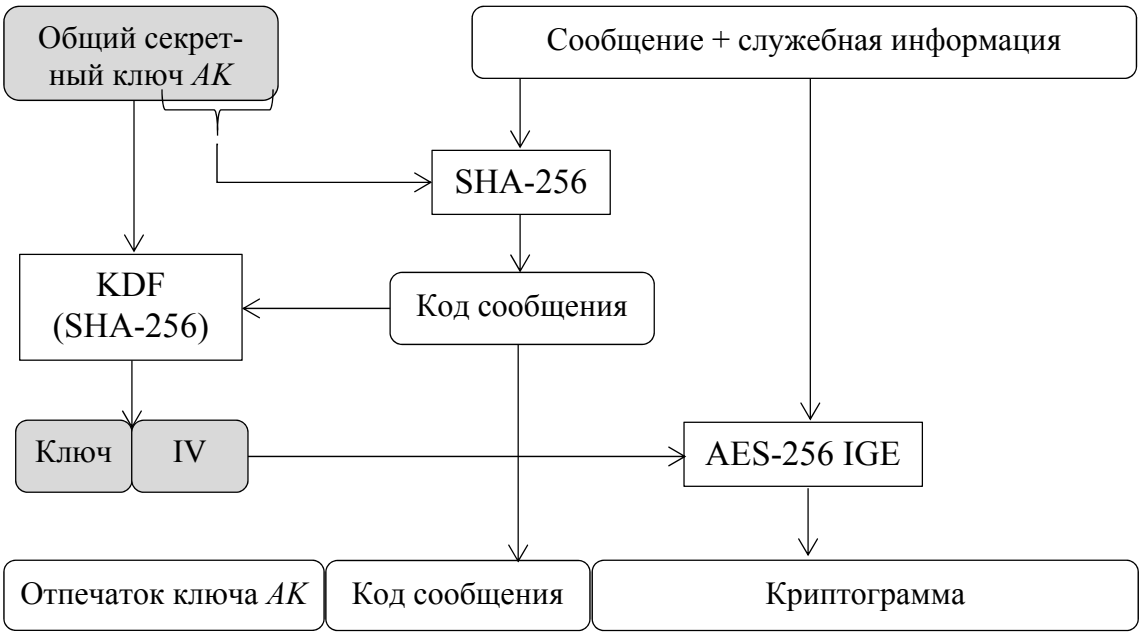


Рисунок 1.8. Общая схема шифрования сообщений в MTProto

На основе шифруемой информации (то есть самого сообщения с добавленной к нему дополнительной информацией) и части общего секретного ключа рассчитывается код сообщения, служащий для проверки целостности, а также позволяющий сформировать различные ключи шифрования для разных сообщений. Код сообщения передается вместе с криптограммой в открытом виде. Для вывода ключей шифрования используется

функция на основе SHA-256, построенная по принципу, сходному с KDF, представленной на рис. 1.7.

Поскольку отпечаток общего секретного ключа отсылается с каждым сообщением, при использовании оконечного шифрования абонент в любой момент может удостовериться в подлинности второй стороны коммуникации с помощью сверки графических кодов, однако это придется делать вручную.

Следует отметить, что сообщения об обнаружении уязвимостей в Telegram (например, [14]) появляются регулярно, и не менее регулярно они опровергаются владельцами мессенджера, заявляющими о его исключительной безопасности.

Знание особенностей оконечного шифрования позволяет прийти к пониманию существующих ограничений и возможных проблем безопасности. Так, основной проблемой является реализация аутентификации сторон коммуникации. Единственным действительно надежным способом связывания открытого ключа с абонентом, а значит, и обеспечения аутентификации стороны при децентрализованном (без участия сервера) распределении ключей в асимметричных схемах является использование цифровой сертификации. Последнее невозможно вне инфраструктуры открытого ключа (PKI). Вынужденный отказ от использования цифровых сертификатов приводит к перекладыванию решения проблемы аутентификации сторон общения на самих абонентов, которые должны осуществлять сверку отпечатков открытых ключей или их графических представлений каждый раз, когда производится процедура согласования общего ключа (в начале сеанса и в случае его изменения в дальнейшем). Это не самый удобный вариант аутентификации, поскольку:

- для снижения вероятности вскрытия шифра ключ может меняться достаточно часто;
- не все реализации мессенджеров осуществляют уведомление пользователей о смене ключа;
- пользователь должен быть достаточно информирован, чтобы осознавать необходимость сверки ключей, и обладать хорошей дисциплиной, чтобы производить ее регулярно;
- если сверка производится визуально (как в Telegram) велика вероятность ошибки для внешне «похожих» графических кодов.

Еще одна серьезная проблема связана с синхронизацией переписки для разных устройств при использовании оконечного шифрования. Системы обмена сообщениями решают эту проблему по-разному. Например, Telegram и Skype отказались от синхронизации переписки для секретных чатов (переписка будет доступна только на том устройстве, на котором начата); синхронизация выполняется только для обычных облачных чатов, не использующих оконечного шифрования. Другие системы поддержива-

ют возможность синхронизации и при использовании оконечного шифрования, например, протокол Signal содержит соответствующий алгоритм. Однако остаются вопросы к реализации этой функции. Например, Signal (как и многие другие мессенджеры) позволяет открыть параллельную сессию (и получить полный доступ к переписке) на другом устройстве, просто отсканировав QR-код, что дает пространство для злоупотреблений даже при кратковременном доступе нарушителя к устройству [15, 16]. Для синхронизации переписки на разных устройствах WhatsApp и Viber поддерживают механизм восстановления сообщений из облака, которые сохраняются в нем в незашифрованном виде [17]. Таким образом, появляется еще один возможный источник информации о переписке, защищенность которого обеспечивается средствами, отличными от сквозного шифрования. Несмотря на то, что создание резервных копий, как правило, может быть отключено в приложении, они могут создаваться автоматически также и самим устройством, и не всегда контролируются пользователем.

Еще одна проблема – возможность сбора метаинформации о контактах и действиях абонентов самой системой обмена сообщениями или третьими лицами (проблема защиты социального графа). Внимание к этому вопросу было привлечено во время скандала, связанного с компанией Facebook, которая занималась широкомасштабным сбором и продажей информации о пользователях. Как правило, возможность такого сбора оговаривается в пользовательском соглашении мессенджера. Например, в пользовательском соглашении WhatsApp – продукта, принадлежащего компании Facebook, указано, что мессенджер собирает информацию о деятельности абонентов (например, как абоненты используют услуги, как взаимодействуют с другими пользователями с помощью сервисов системы и т. п.), журналы веб-сайта, информацию о конкретном устройстве при установке, доступе или использовании сервиса системы (такие как модель телефона, его операционная система и информация из браузера, IP-адреса и мобильной сети, включая номер телефона). В то же время разработчики мессенджера Signal утверждают, что сервер системы сохраняет лишь номер телефона, указанный абонентом при регистрации, и дату последнего входа в систему (с точностью до дня). С другой стороны, как уже отмечалось выше, при использовании оконечного шифрования адресная информация передается в открытом виде и может быть доступна нарушителю.

Как видно, само по себе использование оконечного шифрования не является гарантией безусловной защищенности, как это представляют многочисленные публикации, сводя вопрос безопасности к тому, включено ли в мессенджере оконечное шифрование по умолчанию или нет. В [18] предложены следующие критерии для оценки безопасности мессенджеров и проведен анализ нескольких наиболее известных систем:

- степень централизации управления и архитектуры системы (возможность работы без поддержки серверной части системы, возможность прямых peer-to-peer соединений абонентов без участия сервера);
- возможность анонимной регистрации и использования;
- поддержка оконечного шифрования;
- поддержка синхронизации секретных чатов;
- уведомление о необходимости проверки отпечатков ключей собеседников в секретных чатах;
- запрет скриншотов в режиме секретного чата;
- поддержка групповых секретных чатов;
- уведомление о необходимости проверки отпечатков ключей собеседников в групповых секретных чатах;
- защита социального графа.

Укажем, не раскрывая подробно, еще ряд моментов, которые могут служить источником проблем безопасности при использовании систем обмена сообщениями на мобильных платформах.

Критическим с точки зрения безопасности является получение нарушителем физического доступа к устройству, в связи с этим встают вопросы о надежности удаления информации (старых сообщений), создании локальных резервных копий переписки (автоматическом сохранении сообщений на устройстве) и защите локального хранилища.

Создаваемый системой аккаунт пользователя, как правило, привязывается к номеру телефона, на который в ходе регистрации или при входе с другого устройства отправляется код подтверждения посредством SMS. Известная уязвимость в протоколе сотовой связи SS7 позволяет осуществлять перехват SMS-сообщений, как следствие, нарушитель может зайти в аккаунт абонента, зная лишь номер его телефона. Последнее позволяет, как минимум, отправлять сообщения от имени абонента, а в ряде случаев и получить доступ к его переписке [19].

Получение несанкционированного доступа к пользовательским данным из другого приложения или с помощью вредоносного кода. Данная угроза носит достаточно общий характер, однако она особенно актуальна для мобильных платформ, операционные системы которых имеют ограниченную модель безопасности.

Использование небезопасных клиентов. Если абонент загружает клиентское программное обеспечение не из официального магазина, а по прямой ссылке, велика вероятность использования поддельного клиента с неконтролируемыми возможностями.

Таким образом, наличие криптографических функций является важным, но далеко не единственным фактором обеспечения безопасности мобильных систем, и мессенджеров в частности.

Литература:

1. Названы любимые мессенджеры россиян //CNews. Издание о высоких технологиях, 28.02.2018 [Электронный ресурс]. URL: http://www.cnews.ru/news/top/2018-02-28_whatsapp_stal_samym_populyarnym_messendzheram_v (дата обращения: 31.10.2018).
2. Dennis Fisher. Исследователи обнаружили проблемы с SSL в WhatsApp, 24.02.2014 [Электронный ресурс]. URL: https://threatpost.ru/issledovateli-obnaruzhili-problemy-s-ssl-v-whatsapp/1626/ (дата обращения: 31.10.2018).
3. Карев Антон. Грандиозный факап. Разбираем уязвимости проверки сертификатов SSL и TLS в небраузерном софте // Хакер, 08.03.2018 [Электронный ресурс]. URL: https://xakep.ru/2018/03/08/ssl-tls-fuckup/, https://justpaste.it/1i089 (дата обращения: 31.10.2018).
4. Signal. Technical Information [Электронный ресурс]. URL: https://signal.org/docs/ (дата обращения: 31.10.2018).
5. Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowlingy, Luke Garratt, Douglas Stebila. A Formal Security Analysis of the Signal Messaging Protocol [Электронный ресурс]. URL: https://eprint.iacr.org/2016/1013.pdf (дата обращения: 31.10.2018).
6. Katriel Cohn-Gordon, Cas Cremers, Luke Garratt. On Post-Compromise Security. – Department of Computer Science, University of Oxford, 25.10.2016 [Электронный ресурс]. URL: https://eprint.iacr.org/2016/221.pdf (дата обращения: 01.11.2018).
7. JP Aumasson, Markus Vervier. Hunting for vulnerabilities in Signal – Hitbsecconf2017, Amsterdam [Электронный ресурс]. URL: https://conference.hitb.org/hitbsecconf2017 ams/materials/D2T1 – Markus Vervier – Hunting for Vulnerabilities in Signal.pdf (дата обращения: 01.11.2018).
8. Нефедова Мария. В WhatsApp найдена уязвимость, позволяющая читать чужие сообщения, 13.01.2017 [Электронный ресурс]. URL: https://xakep.ru/2017/01/13/ whatsapp-retransmission-problem/ (дата обращения: 01.11.2018).
9. Andy Greenberg. WhatsApp security flaws could allow snoops to slide into group chats, 10.01.2018 [Электронный ресурс]. URL: https://www.wired.com/story/whatsapp-security-flaws-encryption-group-chats/ (дата обращения: 01.11.2018).
10. Уязвимость в WhatsApp позволяет получить доступ к данным участников групповых чатов, 04.04.2018 [Электронный ресурс]. URL: https://www.securitylab.ru/ news/492456.php (дата обращения: 01.11.2018).
11. Уязвимость в WhatsApp позволяет изменять сообщения в групповых чатах. 09.08.2018 [Электронный ресурс]. URL: https://www.securitylab.ru/news/494962.php (дата обращения: 01.11.2018).
12. Самые защищенные и безопасные мессенджеры – обзор, 25.10.2018 [Электронный ресурс]. URL: http://www.voipoffice.ru/tags/zaschischennye_messendzhery/ (дата обращения: 01.11.2018).
13. Jakob Bjerre Jakobsen. A practical cryptanalysis of the Telegram messaging protocol. Master's thesis. – Aarhus University. Department of computer science, September 2015 [Электронный ресурс]. URL: https://nourbakhsh.ir/wp-content/uploads/2015/11/ jakobsen-master-thesis-telegram.pdf (дата обращения: 02.11.2018).
14. Hayk Saribekyan, Akaki Margvelashvili. Анализ безопасности Telegram, 11.01.2018 [Электронный ресурс]. URL: https://www.securitylab.ru/analytics/490726.php (дата обращения: 02.11.2018).
15. Калошин М. Как могут читать вашу/чужую переписку в WhatsApp, 01.10.2015 [Электронный ресурс]. URL: https://www.kaloshin.me/2015/10/how-to-read-whatsapp-messages-from-another-device.html (дата обращения: 02.11.2018).

16. Нефёдова М. Атака QRLJacking доказывает небезопасность авторизации с использованием SQRL, 02.08.2016 [Электронный ресурс]. URL: https://xakep.ru/2016/08/02/qrljacking/ (дата обращения: 02.11.2018).
17. Bill Budington, Gennie Gebhart. Where WhatsApp Went Wrong: EFF's Four Biggest Security Concerns, 26.01.2017 [Электронный ресурс]. URL: https://www.eff.org/deeplinks/2016/10/where-whatsapp-went-wrong-effs-four-biggest-security-concerns (дата обращения: 04.11.2018).
18. Губарева В., Колисниченко Д. Шифруйся грамотно! Выбираем мессенджер для безопасной и приватной переписки // Хакер, 03.07.2018 [Электронный ресурс]. URL: https://xakep.ru/2018/07/03/messengers/, https://teletype.in/@ht_vbok/ HJGdsTYGQ (дата обращения: 04.11.2018).
19. Как взломать Telegram и WhatsApp: спецслужбы не нужны, 06.05.2016 [Электронный ресурс]. URL: https://habr.com/company/pt/blog/283052/ (дата обращения: 04.11.2018).

1.5. Безопасность персональных данных в контексте европейского регламента GDPR

В условиях цифровизации информационного общества возрастают риски, связанные с кражей персональных данных. Компании, обрабатывающие личную и финансовую информацию клиентов, чаще всего подвержены хакерским атакам. Одним из наиболее крупных инцидентов, связанных с утечкой персональных данных 2017 года является случай с компанией Equifax. Одно из крупнейших в мире бюро кредитных историй заявило об утечке данных 147,9 миллионов своих клиентов. Украденная информация содержала имена, даты рождений, адреса и номера страховок.

Согласно данным Аналитического Центра группы компаний «InfoWatch», приведенным в отчете «Глобальное исследование утечек конфиденциальной информации в I полугодии 2018 года», более 60% от всех утечек составляют персональные данные [1] (рис. 1.9).

Постоянно возрастающие риски неправомерного использования персональных данных поспособствовали принятию различными странами нового закона, вводящего более четкие требования к обеспечению безопасности персональной информации граждан. В мае 2018 года вступил в силу «Общий регламент по защите персональных данных» (*General Data Protection Regulation*, GDPR) – это постановление Европейского Союза, с помощью которого Европейский парламент, Совет Европейского Союза и Европейская комиссия усиливают и унифицируют защиту персональных данных всех лиц, являющихся гражданами стран, входящих в Европейский Союз (ЕС) [2].

Рисунок 1.9. Процентное распределение утечек
по типам информации за 2017 и 2018 года

Общий регламент по защите данных представляет собой новый нормативный документ, действие которого распространяется на организации, предлагающие товары и услуги клиентам в Евросоюзе или собирающие и анализирующие персональные данные, относящиеся к гражданам и резидентам ЕС. Таким образом, российские организации, оказывающие услуги гражданам ЕС (транспортные компании, отели, хостелы и т.д.), обязаны соблюдать новые требования по обработке персональных данных. В случае нарушения настоящего регламента, с организаций может быть взыскан штраф в размере до 4 % от годового дохода.

Целью данного регламента является предоставление гражданам расширенных полномочий по контролю и управлению собственными персональными данными, которые обрабатываются организациями различных сфер деятельности.

Ключевые принципы GDPR [3]:

- законность, справедливость и прозрачность − основания для сбора и использования данных должны быть легальные; открытость всего процесса обработки персональных данных от начала и до этапа уничтожения данных;
- конкретность − все требования по защите персональных данных должны быть закреплены в политике безопасности, а также четко соблюдаться;

- минимизация использованных данных − использование адекватного количества данных для выполнения поставленных целей;
- достоверность − персональные данные должны быть достоверными, а ложные данные должны быть своевременно исправлены;
- ограничение хранения данных − не хранить данные дольше необходимого периода, проводить аудит данных и удалять неиспользуемые;
- целостность и конфиденциальность/безопасность − хранение данных в защищенном виде с ограничением прав доступа к ним посторонних лиц;
- подотчетность − ответственность за обработку персональных данных и выполнение всех остальных принципов GDPR: защиту, использование, проверку данных осуществляет специальное должностное лицо (англ. DPO, data protection officer) – оператор персональных данных (понятие «оператор» согласно ФЗ 152).

Следует учитывать, что понятие «персональные данные» согласно регламенту GDPR – это любая информация, которая позволяет идентифицировать личность: не только имя и фамилия, но и информация о местоположении (геолокация), онлайн-идентификаторы, адрес электронной почты. Данное определение является обширным, таким образом, к персональным данным также может быть отнесен, например, IP-адрес ПК, принадлежащего физическому лицу.

Типы организаций, попадающие под действие GDPR в России:

- дочерние и зависимые общества российских компаний, работающие в ЕС;
- российские компании, предлагающие физическим лицам в ЕС товары и услуги;
- российские компании, осуществляющие мониторинг действий лиц на территории ЕС;
- российские компании, которым контролеры (операторы) ЕС передали персональные данные для обработки (хостинг, резервное копирование, статистическая обработка и т.д.).

Согласно Регламенту, компании, имеющие бизнес-партнеров или ведущие иные бизнес-отношения с организациями, не отвечающими требованиям GDPR, также подвергаются денежному штрафу. Нарушения будут наказывать штрафом до 20 млн. евро или 4% от общего годового оборота компании. Например, если компания не получила согласие от пользователей на обработку персональных данных, ей грозит штраф до 20 млн. евро, а если персональные данные хранятся в незащищенном виде, штраф может составлять около 10 млн. евро [4].

Российские компании, которые не будут соответствовать GDPR, рискуют потерять многих европейских клиентов, а также клиентов из дру-

гих стран, не входящих в ЕС, но принявших решения соблюдать требования GDPR. С другой стороны, если своевременно внедрить требования GDPR и получить соответствующие сертификаты соответствия, можно получить неоспоримое конкурентное преимущество перед другими компаниями.

Все требования GDPR можно разделить на четыре больших блока:

1. Контроль: определять необходимое и достаточное количество информации, которое потребуется компании от клиентов для использования в работе, а также иметь достоверную информацию о том, где и в каком виде хранится данная информация;
2. Управление: выявление всех этапов обработки персональных данных; предоставление или уничтожение данных по запросу клиента;
3. Защита: должны быть внедрены механизмы контроля безопасности, позволяющие предотвращать возможные нарушения и заблаговременно устранять уязвимости;
4. Отчетность: должны быть задокументированы процедуры, используемые для выполнения требований всех трех предыдущих блоков; своевременные оповещения о нарушениях безопасности данных.

Выполнение требований регламента GDPR − это непростая задача для всей организации, которая потребует времени, инструментов, отлаженных процедур и опыта. Для того, чтобы определить основные направления, которые необходимо проработать в организации, можно провести экспресс-анализ уровня соответствия регламенту GDPR в рамках SAM-проекта (Software Asset Management), который выполняется компаниями, имеющими соответствующую специализацию. Реализация SAM-проекта обеспечивает ряд преимуществ, позволяющих повысить эффективность работы IT-инфраструктуры. Проведение проектов SAM базируется на методологии, выработанной на основе многолетней практики специалистов в области международной стандартизации ISO и ITIL.

Этапы выполнения SAM-проекта:

1. Подготовка:
   - определение целей и потребностей компании;
   - сбор информации об IT-инфраструктуре, организационной структуре предприятия;
   - обсуждение проекта, подготовка плана работ, выделение ресурсов.
2. Сбор данных:
   - инвентаризация IT-активов и технический анализ защищенности IT-инфраструктуры с использованием специализированных аппаратно-программных средств;
   - сбор информации о процессах и процедурах, связанных с получением, обработкой, хранением и защитой персональных данных путем интервьюирования сотрудников.

Область сбора данных для анализа [5]:

- базы данных;
- файловые серверы и общие папки;
- облачные компоненты Office 365;
- SharePoint On-Premise.

3. Анализ данных:
   - анализ и оценка полученной информации;
   - оценка соответствия процессов и IT-инфраструктуры требованиям законодательства;
   - разработка плана действий для обеспечения соответствия GDPR и соблюдению ФЗ 152.
4. Рекомендации.

Обсуждение рекомендаций для обеспечения соответствия требованиям GDPR и ФЗ 152, устранению выявленных уязвимостей, повышению эффективности IT-процессов.

Результатами выполнения SAM-проекта на соответствие требованиям GDPR являются:

- точное понимание текущего уровня соответствия процессов IT-системы требованиям законодательства по защите персональных данных: GDPR и 152 ФЗ;
- возможный план по улучшению и развитию системы обработки персональных данных, соответствующей принципам GDPR или 152 ФЗ;
- персональные рекомендации по улучшению общей кибербезопасности компании;
- повышение уровня контроля над программным обеспечением и рисками информационной безопасности;
- рекомендации по устранению текущих уязвимостей и слабых мест в IT-инфраструктуре.

SAM-проект по оценке соответствия требованиям GDPR позволяет выполнить исследования и анализ инфраструктуры обработки данных в компании. Его цель − обеспечить внедрение всех необходимых процессов, направленных на снижение уязвимости персональных данных, что, в свою очередь, позволит руководству компании сосредоточиться на продвижении и улучшении товаров или услуг, а не на работе по соблюдению регламента Евросоюза.

Литература:

1. Аналитический Центр группы компаний «InfoWatch» [Электронный ресурс]. URL: https://www.infowatch.ru/report2018_half (дата обращения: 02.11.2018).
2. Текст Регламента GDPR [Электронный ресурс]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (дата обращения: 02.11.2018).

3. Guide to the General Data Protection Regulation (GDPR) [Электронный ресурс]. URL: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ (дата обращения: 02.11.2018).
4. Институт исследований Интернета: Анализ возможных последствий и влияния Регламента General Data Protection Regulation (GDPR) [Электронный ресурс]. URL: https://internetinstitute.ru/gdpr/ (дата обращения: 02.11.2018).
5. Центр безопасности интернета [Электронный ресурс]. URL: https://www.cisecurity.org/controls/ (дата обращения: 02.11.2018).

1.6. Информационная безопасность виртуальных предприятий

Одной из причин появления концепции виртуальных предприятий (ВП) можно считать развитие и широкое распространение Интернет- технологий, позволяющее реализовать новые возможности для коммуникации и сотрудничества различных автономных, географически распределенных предприятий. ВП формируется как единое информационное пространство, позволяющее создать единую организационно – техническую базу за счет временного объединения ресурсов предприятий-агентов ВП для получения конечного продукта или услуги. Причем, каждый агент ВП имеет двоякое состояние − с одной стороны, это самостоятельная единица, а с другой, в ходе своей деятельности он должен учитывать интересы других агентов ВП.

Поэтому на протяжении всего жизненного цикла, как самого предприятия, так и продукта, выпуск которого происходит, между агентами ВП должен быть налажен обмен информацией для слаженной работы внутри предприятия. Создание единой информационной системы ВП позволит сократить временные и финансовые затраты на обработку, поиск и хранение информации, а также ускорит обмен между агентами ВП, что в конечном итоге позволит сократить себестоимость изделий и улучшить их качество. Так как информационная система содержит всю информацию о работе предприятия, то возникает вопрос о безопасности системы и принятию мер по защите информации.

Защиту информации на ВП традиционными методами осуществить невозможно, так новое предприятие имеет сложную инфраструктуру, характеризующуюся неопределенностью состояния внешней среды, несогласованностью действий локальных администраторов безопасности различных агентов ВП.

Информационная структура каждого агента ВП имеет свои информационные активы и периметр безопасности, свой набор функций защиты информации. Следовательно, при объединении возникает новая система со своим сложным и не всегда четким периметром безопасности. При этом общая стоимость информационных активов становится выше стои-

мости активов отдельных агентов и может меняться со временем, в зависимости от этапов жизненного цикла продукта.

Интегрированную информационную систему нового предприятия можно рассматривать как глобальную вычислительную сеть, узлами которой будут автоматизированные системы обработки данных агентов ВП жизненного цикла изделия, а коммуникация между этими узлами будет проходить через сеть передачи данных общего пользования. Таким образом, информационная система ВП представляет собой довольно масштабную и динамическую систему, в которой администраторы безопасности не способны эффективно управлять защитой информации, поскольку каждый из них контролирует лишь часть этой системы.

В структуру ВП можно разбить на блоки (табл. 1.3).

Таблица 1.3. Основные структурные блоки виртуального предприятия

Основные структурные блоки предприятия	Состав
базовая локальная вычислительная сеть	сетевое оборудование, рабочие станции пользователей, файловые серверы, серверы приложений PDM, серверы распределенных баз данных, архивные серверы, серверы электронной почты, web-серверы и рабочие станции пользователей
локальная вычислительная сеть	службы информационных, службы разработки/ проектирования, служба производства, службы испытаний
удаленных сегментов	фрагменты локальной вычислительной сети других участков ВП

Следует отметить, что взаимодействие географически удаленных агентов ВП осуществляется через сеть общего пользования.

Интегральную информационную среду (ИИС) можно разбить на подсистемы – агенты ВП, которые в свою очередь могут включать сервера приложений, сервера распределенных баз данных и рабочих станций пользователя. Связь между агентами ВП происходит по высокоскоростным каналам передачи данных.

С точки зрения теоретико-множественного описания, данная система может быть представлена направленным графом, нагруженным весами дуг, который можно представить в виде формулы:

$G = (X, \Gamma)$,

где X – множество вершин графа, представляющих рабочие станции и сервера агентов, Γ – множество ребер, определяющее сетевые соединения.

Причем обмен между агентами может быть в виде двустороннего обмена информацией между узлами, поэтому сетевое соединение можно преобразовать в два противоположно направленных ребра (рис. 1.10).

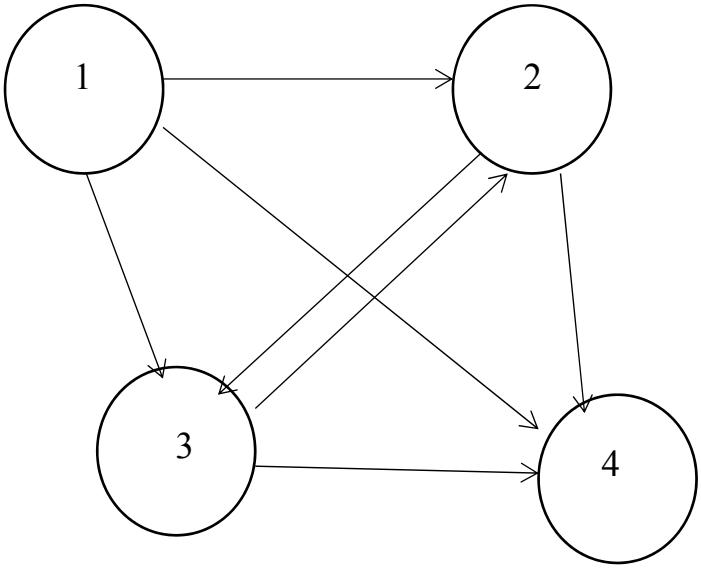


Рисунок 1.10. Схема обмена информацией между агентами ВП

Виды информации, которые используются ВП в ходе жизненного цикла:

- техническое задание;
- результаты научно-технических исследовательских работ;
- проектная информация;
- технологическая информация;
- испытательные тесты и отчеты;
- эксплуатационная документация.

Информацию, поступающую в интегрированную информационную среду ВП можно представить в виде элементов данных d_i − совокупности данных, обладающих законченным смысловым содержанием.

Такими элементами данных могут быть:

- электронные таблицы;
- схемы;
- чертежи;
- текстовые документы;
- модули программного обеспечения;
- другие осмысленные данные.

Все эти элементы данных проходят следующие стадии жизненного цикла (рис. 2): разработка, использование, старение, хранение.

Каждый элемент данных обладает свойством значимости (ценности), которая в течение жизненного цикла меняет свои характеристики от роста до ее падения. По мере создания изделия/услуги ценность возрастает и достигает максимума на момент завершения разработки. Этап использования документа, характеризуется высокой ценностью данных, поскольку именно в это время данные активно используются по назначению и приносят прибыль.

В фазе старения данных значимость их падает, а на этапе архивирования и хранения элементы данных выводятся из эксплуатации, упаковываются или уничтожаются с целью снижения затрат на хранение.

Значимость информации можно представить как функцию:

$c_i = F(k_i, t)$,

где: c_i − ценность, k_i − тип информации, t − время, i =1, 2,…, N.

Множеству элементов информации d_i можно сопоставить множество значимости информации c_i.

Элементы данных имеют неравномерное распределение в ВП, они перемещаются, изменяется их ценность в течение жизненного цикла продукта/услуги, причем и структура самого предприятия может меняться, поэтому становится чрезвычайно сложно вычислить данное значение.

Защиту информации ВП можно осуществить при помощи следующих подходов, которые рассмотрены в таблице 1.4.

Таблица 1.4. Подходы к организации системы защиты информации ВП

Подходы к организации системы защиты	Преимущество
Фрагментарный − каждый агент ВП организует защиту самостоятельно	- оптимальное распределение средств на защиту с точки зрения каждого агента; - выделение на защиту средств, пропорционально стоимости собственной информации.
Комплексный − единая система защиты интегрированной информационной среды	- создание метасистемы защиты информации и системы защищенных коммуникаций между географически удаленными частями интегрированной информационной среды.

Следует также отметить, что для информационных систем ВП следует провести анализ рисков и оценку защищенности, так как по многим угрозам отсутствует достоверная статистика, некоторые угрозы специфичны. Уязвимость информационных систем постоянно меняется – закрываются старые уязвимости и создаются новые. Только после проведения анализа рисков следует принимать решения о конфигурации системы защиты ВП. Такую защиту можно строить, применяя технологии искусственного интеллекта − нечеткую логику, нейронные сети, многоагентные технологии [3].

Организация же систем защиты информации организационно-технологического типа соответствует основным принципам управления, разработанных для данного типа систем.

Анализ позволил выделить следующие типы обрабатываемой информации табл. 1.5.

Таблица 1.5. Документопоток в информационных системах ВП

Тип информации	Характеристика
Периодическая	обмен данными, изменяющимися во время существования ВП
Обмен о жизненном цикле изделия	обмен данными, связанными непосредственно с выпуском продукта/услуги
Системная	информация, связанная с работой информационной системы ВП
Случайная	различного рода случайные воздействия на информацию

Информация первых трех типов является наиболее ценным ресурсом, поэтому требует эффективного уровня ее защиты, то есть контроль за перемещением и изменением. С этим помогут системы защиты, построенные с применением CALS-технологий, которые позволят контролировать системе состояние данных и планировать документопотоки и их ценность.

Следует отметить, что процедуры дополнительной защиты необходимо предусматривать и для случайной информации, если она представляет ценность.

Администраторы безопасности информационной системы ВП не всегда могут обрабатывать весь поток сведений об элементарных событиях и выявлять факты нарушения защиты, поэтому для решения этой задачи можно использовать автоматизацию функций сбора первичной обработки сведений о работе самой системы. Это позволяет администратору просмотреть решение автоматизированной системы, согласится с ним или изменить его. Автоматизировать можно следующие функции (табл. 1.6).

Таблица 1.6. Система автоматизации функций защиты

Функция	Автоматизация/недостаток
сбор первичных данных о функционировании ИИС	контроль событий; обнаружение изменений только под влиянием внешних событий
анализ данных	поиск алгоритмов сигнатур атак в зарегистрированных событиях; отсутствие в базе данных
принятие решения	получение прогнозов на основе алгоритмов многокритериальной оптимизации – величина ожидаемого ущерба от воздействия угрозы; неоднозначность ситуации
формирование управляющих воздействий и их реализация	выбор на основании полученного прогноза либо алгоритмов динамического формирования конфигураций средств защиты в зависимости от типа угроз; проверка на отсутствие противоречий в конфигурации
планирование требуемого уровня защиты	применение конфигураций защиты; определение уровня защиты

Автоматизированная система защиты информации предполагает решение следующих задач защиты информации ВП:

- разработка системы;
- разработка структуру и архитектуру этой системы;
- разработка оценки анализа рисков, основанная на плановых обработках данных;
- разработка алгоритмов анализа событий;
- разработка алгоритмов принятия решений.

Внедрение автоматизированной системы защиты информации ВП позволит повысить эффективность функционирования ВП, что приведет к снижению рисков повреждения и потери информации, а также к оптимизации затрат на мероприятия по защите информации. Таким образом, если значение величины снижения риска убытков превысит убытки, связанные со снижением эффективности функционирования, то внедрение системы автоматизации защиты информации можно резонной оправданной [3].

Литература:

1. Еникеева Л.А., Соколовская С.А. Методы управления виртуальными предприятиями (монография) СПб.: СПбГИЭУ, 2010. – 122 с.
2. Стельмашонок Е.В., Соколовская С.А. Стратегическое управление информационной безопасностью предприятия на основе сбалансированной системы показателей // Вестник ИНЖЭКОНа. Серия: Экономика. 2010. − № 6. − С. 112-117.
3. Информационная безопасность виртуального предприятия [Электронный ресурс]. URL: https://lektsii.org/8-15639.html (дата обращения: 28.10.2018).

ГЛАВА 2. ПОСТРОЕНИЕ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Построение онтологии информационной безопасности

Возросшие объемы перерабатываемой информации влекут за собой проблемы в области информационной безопасности (ИБ). Ключом к решению данных проблем может стать автоматизированная реакция на возникающие угрозы ИБ. Как известно, автоматизация требует формализации предметной области. В связи с этим рассматриваются примеры формализации, построенные на базе онтологий. В первой части параграфа приводится пример обобщенной онтологии в области ИБ, во второй − пример частной онтологии защиты информации.

Построение онтологии информационной безопасности на базе «Агасофии»

В качестве ключевых терминов для построения онтологии был взят тезаурус, предложенный Атамановым Г.А. [1, 2], который также носит название «АГАсофия» информационной безопасности. Остановимся на базовых предположениях, которые легли в основу онтологии.

Представить «опасность» и «безопасность» можно как два разных класса, находящихся на одном уровне иерархии. Безопасность при этом можно разделить на несколько подклассов, перечисленных ниже.

1. Подкласс «Условия безопасности», т.е. при каких условиях объект находится в состоянии безопасности.
2. Подкласс «Субъекты безопасности», т.е., кто обеспечивает безопасность.
3. Подкласс «Объекты безопасности», т.е., безопасность чего необходимо обеспечить.

Онтология будет иметь вид, представленный на рис. 2.1.

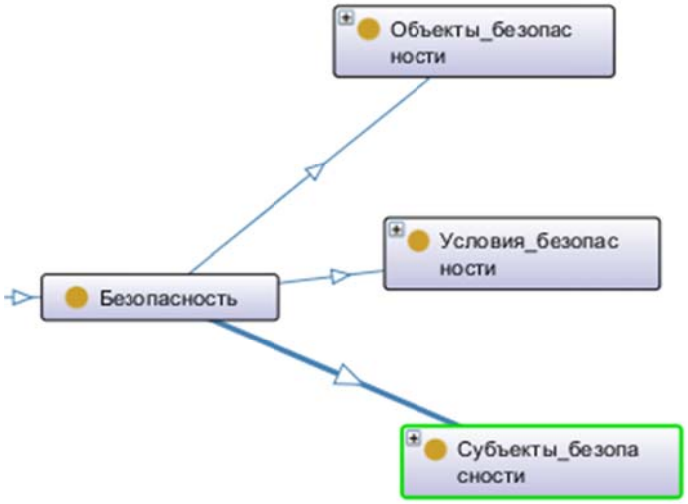


Рисунок 2.1. Онтология для класса «Безопасность»

К условиям безопасности, исходя из «АГАсофии», можно отнести следующие положения (см. рис. 2.2):

1. атаки не достигают цели;
2. атаки своевременно прерываются;
3. вред не превышает установленный порог;
4. угрозы не реализуются.

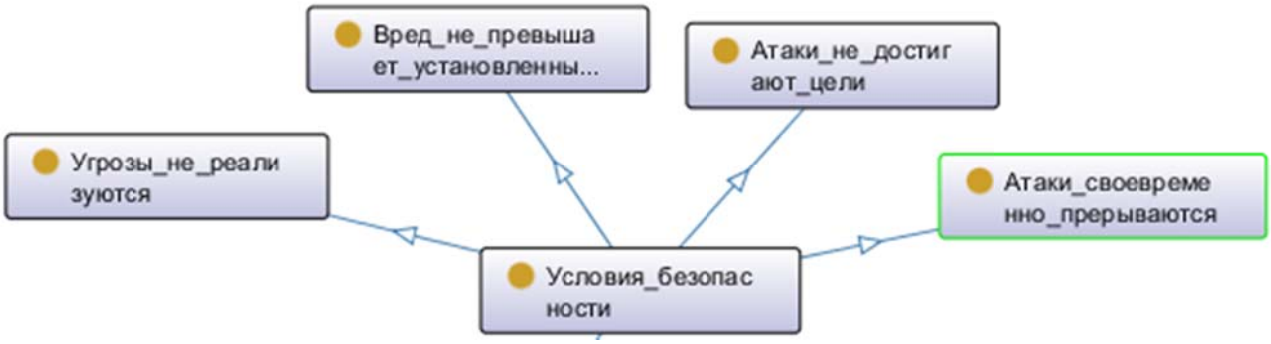


Рисунок 2.2. Онтология для подкласса «Условия безопасности»

Объектами, как и субъектами информационной безопасности, с точки зрения «АГАсофии» являются три класса (рис. 2.3):

1. класс «Индивид»;
2. класс «Корпорация»;
3. класс «Государство».

Каждый из обозначенных субъектов/объектов информационной безопасности может обеспечивать безопасность, требовать обеспечения безопасности или быть источником опасности.

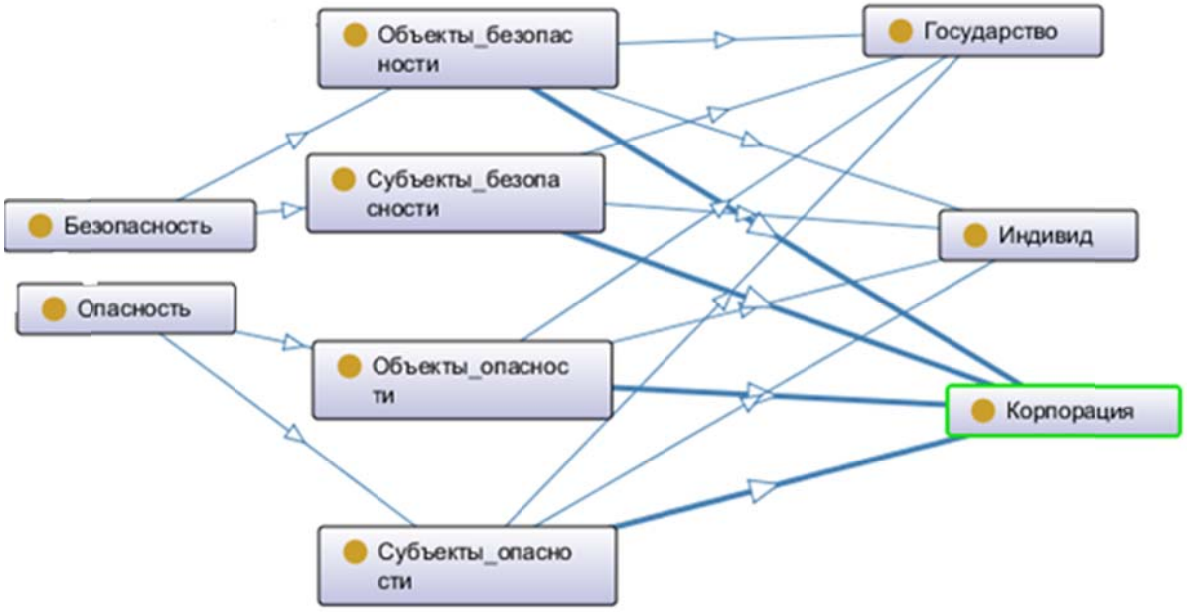


Рисунок 2.3. Онтология, включающая классы субъектов/объектов информационной безопасности

В объекты безопасности входит подкласс объекты защиты, включающий следующие подклассы (рис. 2.4):

1. подкласс «Связи»;
2. подкласс «Смыслы»;
3. подкласс «Элементы».

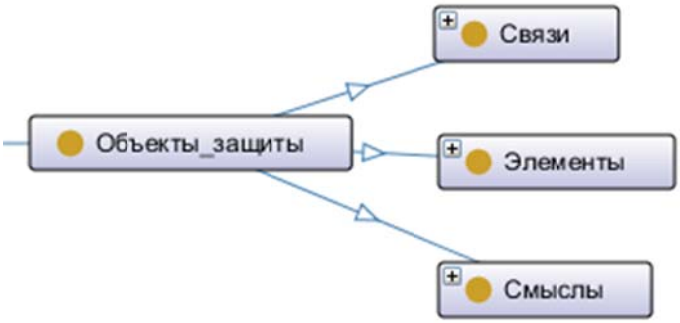


Рисунок 2.4. Онтология подкласса «Объекты защиты»

Опасность, в свою очередь, содержит следующие подклассы:

1. подкласс «Угрозы»;
2. подкласс «Субъекты опасности»;
3. подкласс «Объекты опасности».

Опасность появляется при наличии угрозы. При реализации угрозы возникает вред, поэтому подклассом угрозы является вред. Вред может состоять из следующих подклассов:

1. подкласс «Деструкция»;
2. подкласс «Дисфункция»;
3. подкласс «Значительное ухудшение условий существования».

Все эти классы содержат в себе подклассы объектов защиты, т.к. они направлены на них (рис. 2.5).

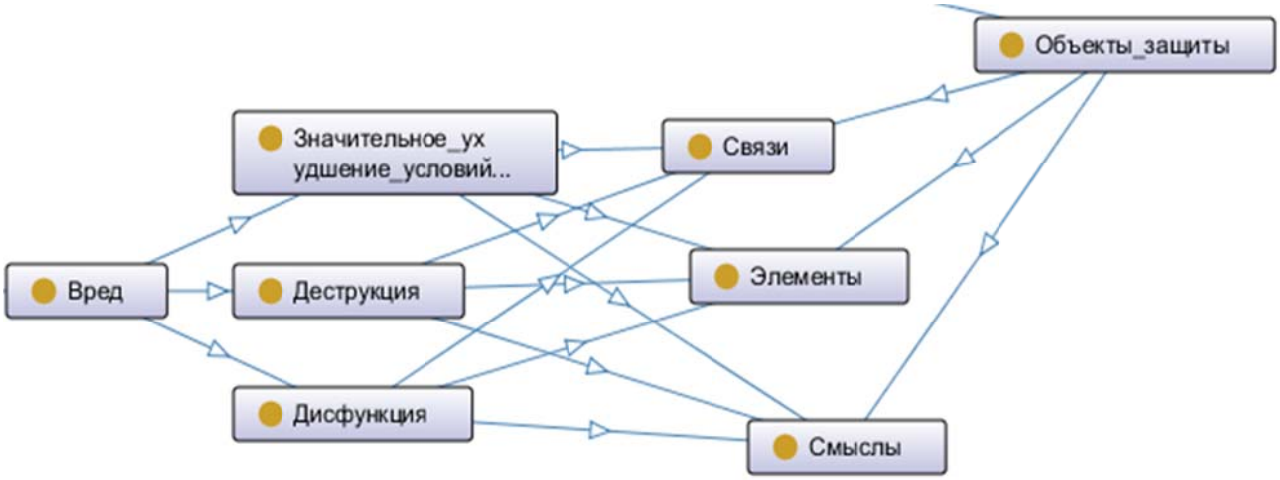


Рисунок 2.5. Онтология, связывающая объекты защиты и вред

Итоговая онтология в виде дерева представлена на рис. 2.6.

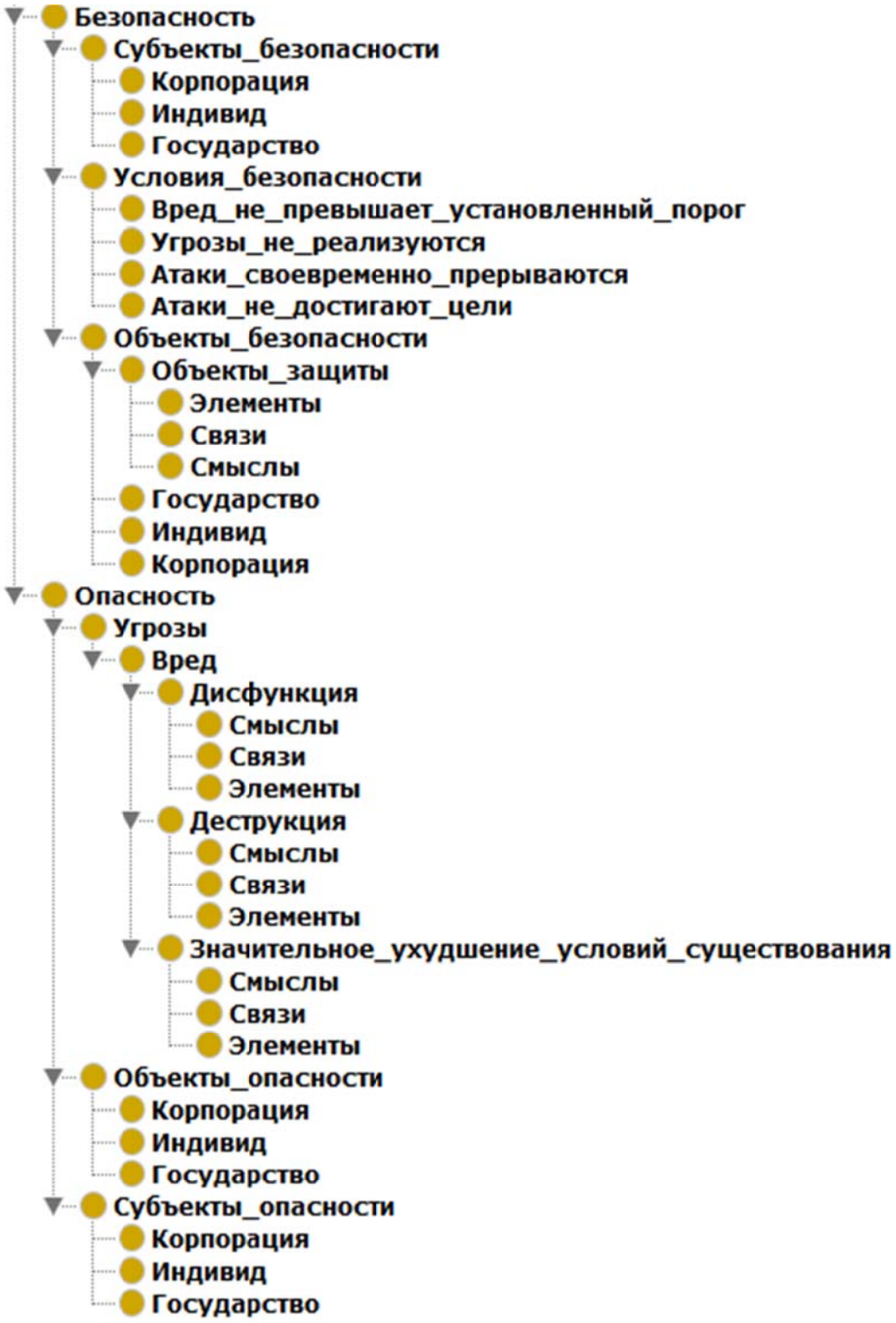


Рисунок 2.6. Итоговая онтология, представленная в виде дерева

Полученная онтология является первым эскизом, наращивая который можно построить полное представление предметной области «Информационная безопасность». Следующий шаг – установление связей с конкретными кейсами в области защиты информации.

Разработка базы знаний для интеллектуальной системы обнаружения и предотвращения вторжений

Ниже представлена онтология компьютерных угроз, которая достаточно полно описывает предметную область и может служить основой для разработки базы данных компьютерных угроз и основным источником информации для автоматизированной системы противодействия компьютерным угрозам.

Перечислим основные публикации на данную тему.

В работе [1] описывается метод разработки онтологий, основанный на загрузке существующей онтологии в качестве основного источника знаний по безопасности, который содержит список терминов в домене безопасности. Данный подход позволяет автоматически извлекать термины и понятия из источников, вводить отношения в соответствии с концепцией онтологии для каждого термина и классифицировать их в существующую онтологию. Этот подход основан на точных и приближенных совпадениях сходных понятий и информации, полученной из открытых источников.

В статье [2] описывается модельная онтология, которая направлена на интеграцию эмпирических знаний об уязвимостях, добавляемых во время разработки системы.

В [3] представлена система решения проблем, основанная на IRS, которая классифицирует информацию об атакующих векторах для облегчения использования внутри организации. IRS использует расширенную таксономию, как решение, устраняющее недостатки существующих таксономий. Цель такой системы – предоставить детальную информацию о векторе атаки: что включает себя атака и какое влияние она может оказать на целевую систему. Информация об атакующих векторах представлена в виде дерева, которое отображает весь путь атаки.

Статья [4] рассматривает концептуальные рамки безопасности для управления и аудита безопасности информационных систем. Предлагаемая структура основана на концептуальной модели в соответствии со стандартом ISO / IEC_JCT1, чтобы помочь организациям лучше контролировать безопасность своих информационных систем. В статье представлен подход для улучшения управления безопасностью с помощью концептуальных рамок, разработанных для оказания помощи организациям в классификации атак, определении активов и смягчении их уязвимостей и угроз. Предлагаемая структура основана на концептуальной модели с возможностью представления семантических концепций и их отношений в области информационной безопасности. Предлагаемая структура основана на концептуальной онтологии, которая моделирует основные понятия атак, угроз и уязвимостей, а также их отношения с другими концепциями

безопасности. Определенная концептуальная модель содержит 8 концепций и 16 отношений, основанных на стандарте безопасности ISO / IEC_JCT1.

Авторы [5] разработали онтологию инцидентов безопасности, которая учитывает особенности организации и ее общих систем, а не только программного обеспечения. Сюда относятся соответствующие защитные классы с категориями инцидентов, так как неблагоприятные результаты также необходимо рассматривать с точки зрения защитников с учетом их целей и конкретных обстоятельств. Была создана трехуровневая архитектура безопасности, состоящая из социального, логического и физического уровня, которая позволяет планировать комплексные меры защиты с общими атаками по площади, охватывающими все уровни. Эти идеи обеспечивают целостный анализ инцидентов не только по техническим аспектам, но и по человеческим и природным факторам, которые могут обеспечить всестороннюю защиту в целях предотвращения, обнаружения и восстановления после инцидентов.

Разработка и создание онтологии компьютерных угроз может лечь в основу базы данных компьютерных угроз и стать основным источником информации для автоматизированной системы противодействия компьютерным угрозам.

Основными составляющими любой онтологии являются:

- классы (понятия) – абстрактные термины, которые имеют атрибуты;
- атрибуты (свойства) – свойства, необходимые для установления связи между неиерархическими понятиями;
- связи (отношения) – отношения описывающие общие характеристики экземпляров класса или отношений классов;
- аксиомы – правила моделируемой области, которые ограничивают возможные интерпретации определенных классов;
- экземпляры – фактические представления абстрактных понятий.

Целью онтологий информационной безопасности является создание недвусмысленных семантических моделей концепций безопасности, которые могут служить для взаимодействия между программными агентами, что приводит к уменьшению языковой неоднозначности.

В основе онтологии предметной области должен лежать словарь терминов, которые необходимы для систематизации знаний в этой области. Для создания онтологии и составления словаря терминов были использованы источники, описывающие классификацию угроз информационной безопасности [6-10]. Выделены следующие основные термины: «Атака», «Угроза безопасности» (Threat), «Актив» (Asset), «Уязвимость актива» (Vulnerability), «Состояние защищенности системы» (State_of_security), «Инцидент безопасности», «Реакция системы»

(Reaction). Ядро сформированной концептуальной модели изображено на рисунке 2.7.

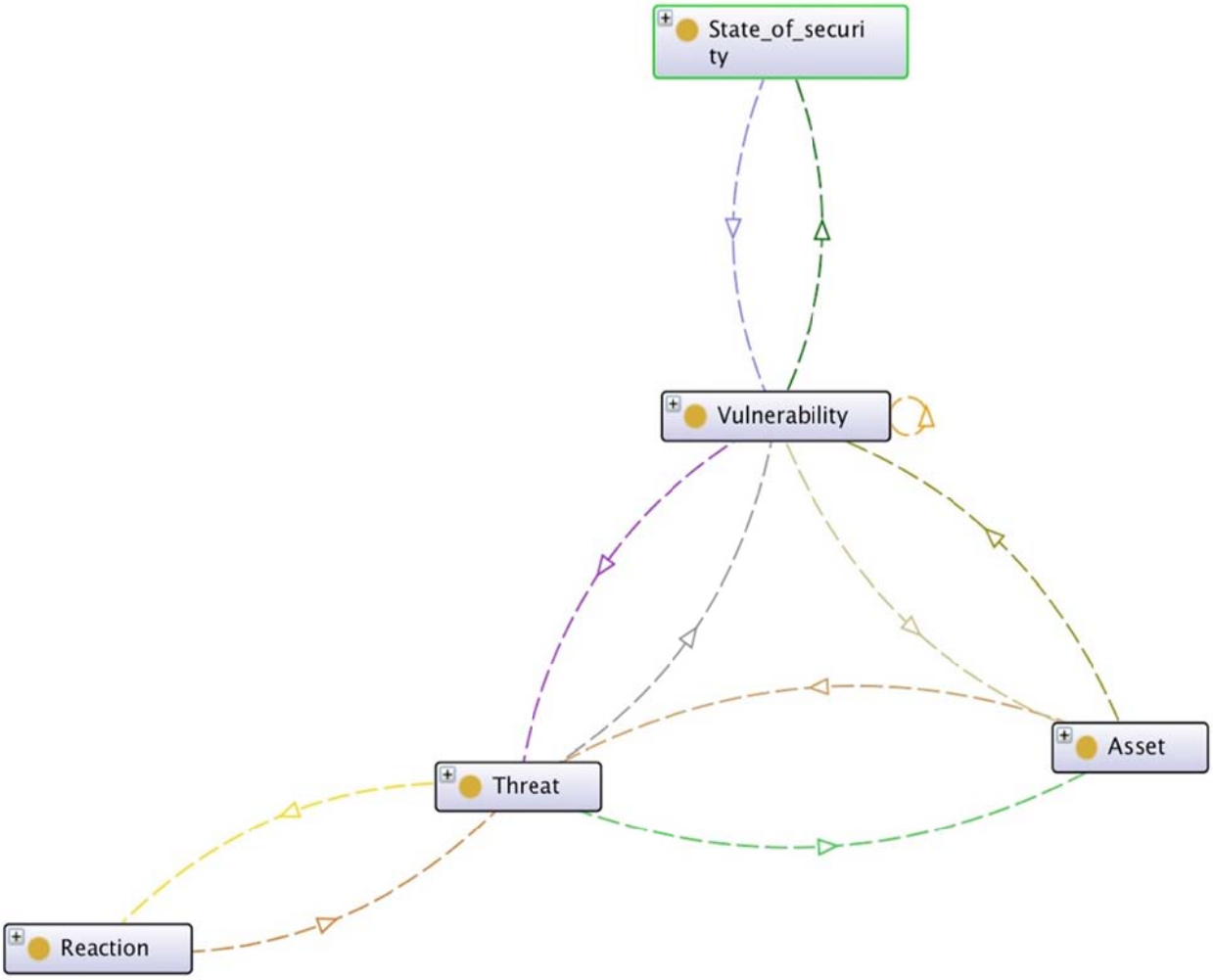


Рисунок 2.7. «Ядро концептуальной модели»

Были выделены следующие принципы, которые должны лежать в основе разрабатываемой онтологии.

1) На систему осуществляется «Атака», которая создает «Угрозу безопасности», которая влияет на «Состояние защищенности системы».
2) Атака использует «Уязвимость системы» и направлена на ее «Актив».
3) «Инцидент безопасности» подразумевает последствия, т.е. «Реакцию системы» на несанкционированные действия извне.
4) Использование какой-либо «Уязвимости» может открыть другую «Уязвимость».

Получившаяся онтология обладает внушительной иерархичностью и трудна для восприятия как пользователем, так и программой. Для решения этой проблемы был разработан дополнительный класс, который лег в основу глобальных классов ядра – класс «Прецедент» (рис. 2.8).

Рисунок 2.8. Структура класса «Прецедент»

Данный класс, с помощью своих атрибутов хранит ссылки на соответствующие объекты, тем самым связывая глобальные классы и отдельные объекты в паутину. Кроме того, класс «Прецедент» хранит ссылки на симптомы угроз и ссылки на реакции системы на данные угрозы, что значительно облегчает программный поиск по онтологии.

Можно выделить три причины для использования онтологии: возможность поделиться общими знаниями, возможность повторного использования знаний и эффективность взаимодействия онтологии и программных средств.

Большая часть предлагаемых на сегодняшний день онтологий информационной безопасности сосредоточены на освещении конкретных аспектов. Следовательно, требуется онтология, которая охватывает весь домен сетевой безопасности. Она должна быть гибкой, адаптируемой и обеспечивать повторное использование, обмен информацией и обмен знаниями, поддерживая масштабируемость сети.

Представлена попытка создать такую онтологию. В процессе работы спроектирована и разработана онтология предметной области информационной безопасности, основанная на прецедентном подходе.

Выделено несколько основных требований, используемых для дальнейшей доработки онтологии и создания программного средства.

- Реализация основана на правилах: используемый язык правил должен быть очень выразительным из-за сложности представления знаний.
- Поддержание работоспособности: необходимо постоянно обновлять и дополнять онтологию для сохранения ее актуальности. Четкое разделение компонентов (правил, бизнес-логики и интерфейсов) сильно облегчит данную задачу.
- База знаний OWL: структура должна работать непосредственно с файлами OWL, поскольку этот стандарт W3C имеет высокий потенциал и в настоящее время широко используется.
- Соблюдение стандартов: структура управления информационной безопасностью должна быть построена на языке OWL с целью ис-

пользования существующих онтологий угроз, уязвимостей, стандартов информационной безопасности и т.д.

В настоящее время рассматриваются два варианта разработки поддерживающего онтологию программного обеспечения:

- использование языка программирования Python в связке с библиотекой RDFlib, позволяющей отправлять запросы на языке SPARQL к онтологии;
- использование языка программирования Python в связке с библиотекой xml, позволяющей анализировать XML-документ.

В качестве ближайшей задачи ставится рассмотрение сильных и слабых сторон каждого из вариантов для определения и наиболее предпочтительного.

Литература:

1. Атаманов Г.А. Методология безопасности // Фонд содействия научным исследованиям проблем безопасности «Наука-XXI», 2011. – [Электронный ресурс]. URL: http://naukaxxi.ru/materials/302/, http://gatamanov.blogspot.ru/ (дата обращения: 01.11.2018)
2. Атаманов Г.А. Азбука безопасности. Объекты и субъекты безопасности вообще и информационной в частности // Защита информации. Инсайд. – 2013. – № 6. – С. 18-24.
3. Arwa Wali, Soon Ae Chun, James Geller. A Bootstrapping Approach for Developing a Cyber-Security Ontology Using Textbook Index Terms // International Conference on Availability, Reliability and Security, 2-6 Sept. 2013. [Электронный ресурс]. URL: https://ieeexplore.ieee.org/document/6657291 (дата обращения: 28.10.2018).
4. Elahi G., Yu E., Zannone N. (2009) A Modeling Ontology for Integrating Vulnerabilities into Security Requirements Conceptual Foundations. In: Laender A.H.F., Castano S., Dayal U., Casati F., de Oliveira J.P.M. (eds) Conceptual Modeling – ER 2009. ER 2009. Lecture Notes in Computer Science, vol 5829. Springer, Berlin, Heidelberg. – P. 99-114.
5. Simmons C.B., Shiva S.G., Simmons L.L. A qualitative analysis of an ontology based issue resolution system for cyber-attack management // The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent, 4-7 June 2014 [Электронный ресурс]. URL: https://ieeexplore.ieee.org/document/6917483 (дата обращения: 28.10.2018).
6. Teresa Pereira, Henrique Santos. A Security Framework for Audit and Manage Information System Security, Oct. 2010 [Электронный ресурс]. URL: https://www.researchgate.net/publication/224187157_A_Security_Framework_for_Audit_and_Manage_Information_System_Security (дата обращения: 28.10.2018).
7. Clive Blackwell. A Security Ontology for Incident Analysis, Jan. 2010. – 281 p.
8. Мирзагитов А.А., Пальчунов Д.Е. Методы разработки онтологии по информационной безопасности, основанные на прецедентном подходе // Вестник НГУ. Серия: Информационные технологии. – 2013. Т. 11, вып. 3. – С. 37-46.
9. Luciana Andréia Fondazzi Martimiano, Edson dos Santos Moreira. An OWL-based Security Incident Ontology, 2005 [Электронный ресурс]. URL: https://pdfs.semanticscholar.org/a010/96f282e267f99b3a78e15c4241ec03f9721a.pdf?_ga=2.259926217.2126079099.1542444029-1025335825.1542444029 (дата обращения: 28.10.2018).

10. Almut Herzog, Claudiu Duma, Nahid Shahmehri. An Ontology of Information Security, 2009. – 339 с.
11. Ontology-Based Decision Support for Information Security Risk Management by Xylem Technologies, Dec. 3, 2010 [Электронный ресурс]. URL: https://www.xylem-technologies.com/2010/12/ontology-based-decision-support-for-information-security-risk-management/ (дата обращения: 28.10.2018).
12. Danny Velasco Silva1, Glen Rodríguez. Ontologies for Network Security and Future Challenges, 2016. – 547 p.
13. Patel-Schneider P. F., Hayes P., Horrocks I. (Eds.) OWL Web Ontology Language Semantics and Abstract Syntax. W3C Recommendation 10 February 2004 [Электронный ресурс]. URL: https://www.w3.org/TR/owl-absyn/ (дата обращения: 28.10.2018).
14. Власов Д. Ю., Пальчунов Д. Е., Степанов П. А. Автоматизация извлечения отношений между понятиями из текстов естественного языка // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2010. Т. 8, вып. 3. – С. 23–33.
15. Stefan Fenz. Security Ontology [Электронный ресурс]. URL: http://stefan.fenz.at/research/security-ontology/ (дата обращения: 28.10.2018).

2.2. Контроль функционирования комплексной системы защиты информации

Виды контроля функционирования комплексной системы защиты информации (КСЗИ)

Контроль в общем виде является одной из основных функций управления, вызванной необходимостью обратной связи между субъектом и объектами управления для достижения поставленной цели.

В целом процесс контроля можно разбить на последовательные этапы: формулирование цели → формирование стандартов → разработка критериев оценки → разработка систем показателей → проведение процедуры сравнительного анализа → обобщение полученной информации и корректировка деятельности.

Основные требования к контролю: комплексность; своевременность; стандартизация; простота; доступность; гибкость; объективность; экономичность. Общие цели контроля: уменьшение отклонений от заданных норм; уменьшение неопределенной деятельности; предотвращение кризисных ситуаций.

Современные виды контроля: мониторинг − непрерывное поступление информации; контроллинг − оценка экономичности; бенчмаркинг (управленческое воздействие, заключающееся во внедрении в практику деятельности организации технологий, стандартов и методов деятельности более успешных организаций − аналогов).

Контроль функционирования КСЗИ можно разделить на два основных вида − внешний и внутренний. Внешний контроль функционирования КСЗИ осуществляется различного рода государственными органами, а также может осуществляться аудиторскими организациями.

Внутренний контроль осуществляется службой безопасности предприятия и подразделением зашиты информации предприятия. Внешний контроль отслеживает обеспечение защиты государственной тайны и персональных данных:

Контроль за обеспечением защиты государственной тайны подразделяется на межведомственный и ведомственный. Он осуществляется в органах государственной власти, на предприятиях, в учреждениях и организациях федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности; федеральным органом исполнительной власти, уполномоченным в области обороны; федеральным органом исполнительной власти, уполномоченным в области внешней разведки; федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, и их территориальными органами, на которые эта функция возложена законодательством Российской Федерации.

Органы государственной власти, наделенные полномочиями по распоряжению сведениями, составляющими государственную тайну, обязаны контролировать эффективность защиты этих сведений во всех подчиненных и подведомственных им органах государственной власти, на предприятиях, в учреждениях и организациях, осуществляющих работу с ними.

Контроль за обеспечением защиты персональных данных осуществляется федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической зашиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

Контроль и надзор за соответствием обработки персональных данных требованиям федерального закона осуществляет федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи.

Внутренний контроль осуществляется в отношении защиты всех видов информации с ограниченным доступом. Проводится руководством предприятия, внутренними проверочными комиссиями, службой безопасности и подразделением защиты информации. Подразделяется на текущий (постоянный), периодический (плановый) и внезапный.

Цель проведения контрольных мероприятий в КСЗИ

Целью контроля является установление степени соответствия принимаемых мер по защите информации требованиям законодательных и иных нормативных правовых актов, стандартов, норм, правил и инструкций, выявление возможных каналов утечки и несанкционированного (не-

правомерного, противоправного) доступа к информации, выработка рекомендаций по закрытию этих каналов.

Основные задачи контроля:

- оценка деятельности органов управления по методическому руководству и координации работ в области зашиты информации в подчиненных подразделениях;
- выявление каналов утечки информации об объектах защиты и несанкционированного доступа к информации (воздействия на информацию), анализ и оценка возможностей злоумышленников по ее получению;
- выявление работ с защищаемой информацией, выполняемых с нарушением установленных норм и требований по защите информации, и пресечение выявленных нарушений;
- анализ причин нарушений и недостатков в организации и обеспечении защиты информации, выработка рекомендаций по их устранению;
- анализ состояния зашиты информации в подразделениях предприятия, информирование руководства предприятия, подготовка предложений по совершенствованию защиты информации;
- предупреждение нарушений по защите информации при проведении работ с защищаемой информацией и ее носителями.

Направлениями контроля состояния защиты информации являются:

- контроль деятельности и состояния работ по противодействию ИТР и технической защите;
- контроль с применением технических средств эффективности мер защиты объектов, информационных систем, средств и систем связи и управления на всех стадиях их жизненного цикла;
- контроль эффективности защиты автоматизированных систем обработки информации от несанкционированного доступа, от специальных воздействий на информацию и средства ее обработки с целью разрушения, уничтожения, искажения и блокирования информации;
- контроль эффективности мероприятий по защите информации в системах связи автоматизированного управления;
- контроль за соблюдением установленного порядка передачи служебных сообщений должностными лицами предприятия, выполняющими работы, связанные со сведениями, составляющими государственную или служебную тайну, при использовании открытых каналов радио- и радиорелейных, тропосферных и спутниковых линий связи, доступных для радиоразведки.

Система контроля состояния защиты информации базируется на следующих основных принципах.

- наделение органов контроля необходимыми полномочиями, позволяющими им должным образом влиять на контролируемые объекты и обеспечивающими эффективность и действенность контроля;
- независимость органов контроля от должностных лиц контролируемых объектов при осуществлении полномочий;
- соблюдение законности в работе органов контроля и их должностных лиц;
- системность и регулярность в проведении контроля;
- профессионализм сотрудников органов контроля, применение ими методов и средств проведения проверок в соответствии с действующими нормативно-методическими документами, единая информационная база органов контроля по нормам, методикам и средствам контроля;
- объективность анализа обстоятельств и причин нарушений в состоянии защиты информации;
- наличие обратной связи с контролируемыми объектами, обеспечивающей объективность сведений о состоянии защиты информации и о ходе устранения вскрываемых нарушений и недостатков;
- экономическая целесообразность функционирования контрольных органов − оптимальное сочетание результативности деятельности органов с затратами на их содержание.

В функции органа контроля входят следующие обязанности:

- организация и осуществление контроля силами подразделений ЗИ и специализированных организаций;
- сбор, анализ и обобщение материалов о состоянии защиты информации по результатам проверок;
- информирование руководства предприятия об эффективности мер и состоянии работ по защите информации.

Проведение текущего (постоянного) контроля возлагается на объектовые органы в целях обеспечения установленного порядка функционирования средств защиты, соблюдения установленных режимов работы технических средств, в которых циркулирует защищаемая информация, выполнения установленных мер защиты, контроля за правильностью реализации правил разграничения доступа к информации в автоматизированных системах ее обработки, выявления и пресечения нарушений в области технической защиты информации.

В зависимости от объема работ по технической защите информации и контролю, функции объектового органа контроля по решению руководителя организации могут выполняться подразделением защиты информации либо специально созданными объектовыми органами контроля.

Основные методы контроля: проверка; изучение; испытания; наблюдения; зачеты, экзамены, тестирование; провокации; атаки; отзыв и изучение документов и др.

Анализ и использование результатов проведения контрольных мероприятий

Периодичность проведения проверок организаций определяется исходя из высшего грифа секретности обрабатываемой (циркулирующей) в ней информации или установленной категории по требованиям обеспечения защиты образцов вооружения и военной техники. Такая периодичность может указываться в руководстве по технической защите информации или в инструкциях по технической защите информации, касающейся изделия (образца).

Периодичность проведения проверок состояния технической защиты информации устанавливается:

- для организаций, работающих со сведениями «особой важности» (образцы 1-й категории) — не реже одного раза в два года;
- для организаций, работающих со сведениями, имеющими гриф «совершенно секретно» (образцы 2-й категории) — не реже одного раза в три года;
- для организаций, работающих со сведениями, имеющими гриф «секретно» (образцы 3-й категории) — не реже одного раза в пять лет.

Нарушения в области технической защиты информации представляют собой несоответствие мер технической защиты информации установленным требованиям или нормам.

По степени опасности нарушения делятся на три категории:

- первая категория − невыполнение требований или норм по технической защите информации, составляющей государственную тайну, подтвержденное протоколом технического контроля, в результате которого имелась или имеется реальная возможность утечки информации по техническим каналам, несанкционированный доступ к информации или воздействие на информацию;
- вторая категория − невыполнение требований по технической защите информации, в результате чего создаются предпосылки к утечке информации по техническим каналам или несанкционированному доступу к ней;
- третья категория − недостатки в оформлении документов по организации технической защиты информации, которые не ведут непосредственно к возникновению предпосылок к утечке информации по техническим каналам или к несанкционированному доступу к ней.

При обнаружении нарушений второй и третьей категорий руководитель проверяемой организации обязан принять необходимые меры по их устранению в сроки, согласованные с проверяющим органом. Контроль за устранением этих нарушений осуществляется подразделением контроля проверенной организации.

Содержание контроля состояния технической защиты информации составляет оценка деятельности (состояния работ) по противодействию ИТР и технической защите информации, а также эффективности мер (мероприятий) по защите государственных и промышленных объектов, образцов вооружения и военной техники, информационных систем, средств и систем связи и управления (далее − контроль эффективности защиты).

Контроль деятельности по технической защите информации заключается в проверке организации работ по защите информации, наличия органов (подразделений) технической зашиты информации, включения задач зашиты информации в положения о подразделениях и функциональных обязанностях должностных лиц, наличия и содержания внутренних организационно-распорядительных документов (приказов, руководств, положений, инструкций) на соответствие требованиям правовых и нормативных документов в области защиты информации, порядка и своевременности их доведения до исполнителей и подведомственных организаций, наличия и полноты планов работ по технической защите информации и контролю ее эффективности, а также состояния их выполнения.

Контроль эффективности защиты − это проверка соответствия качественных и количественных показателей эффективности мер (мероприятий) по противодействию ИТР и технической защите государственных и промышленных объектов, образцов вооружения и военной техники, информационных систем, средств и систем связи и управления требованиям или нормам эффективности защиты информации.

Состав видов технической разведки и их возможности, угрозы безопасности информации и каналы ее утечки, подлежащие контролю, определяются Гостехкомиссией России в соответствующих моделях технических разведок и концепциях защиты.

В зависимости от вида контроль эффективности защиты может быть организационным и техническим.

Организационный контроль − проверка соответствия полноты и обоснованности мероприятий по защите требованиям руководящих документов в области технической зашиты информации.

Технический контроль − это контроль эффективности зашиты, проводимый с использованием соответствующих средств. Целью технического контроля является получение объективной и достоверной информации о состоянии защиты объектов контроля. При проведении технического контроля оценивается соответствие объективных показателей состояния защиты объекта предельно допустимым значениям (нормам). Для проведения технического контроля эффективности зашиты информации могут использоваться космические, воздушные, наземные, морские, а также встроенные средства технического контроля.

Проведение объема технического контроля эффективности технической защиты информации может быть разным.

Комплексный контроль проводится по всем каналам возможной утечки информации (несанкционированного доступа к информации или воздействия на нее), характерным для контролируемого технического средства (образца, объекта информатизации), причем оценка эффективности технической зашиты информации осуществляется во взаимной увязке результатов обследования по всем указанным каналам.

Целевой контроль − это проверка по одному из каналов возможной утечки информации, характерных для контролируемого технического средства, в котором циркулирует защищаемая информация.

Для выборочного контроля из всего состава технических средств на объекте для проверки выбирают те из них, которые по результатам предварительной оценки с наибольшей вероятностью имеют технические каналы утечки защищаемой информации.

В зависимости от имеющихся условий проведения технический контроль эффективности технической зашиты информации может осуществляться тремя методами.

В ходе инструментального контроля используется техническое измерительное средство и моделируются реальные условия работы технического средства разведки.

При инструментально-расчетном контроле измерения проводятся в непосредственной близости от объекта контроля, а затем результаты измерений пересчитываются относительно предполагаемого места (условий) нахождения технического средства разведки.

Для проведения расчетного контроля эффективность защиты оценивается математически, исходя из реальных условий размещения и возможностей технического средства разведки и известных характеристик объекта контроля.

Технический контроль осуществляется в соответствии с методиками контроля состояния технической защиты информации, утвержденными или согласованными с ФСТЭК России. Не допускается физическое подключение технических средств контроля, а также формирование тестовых режимов, запуск тестовых программ на образцах, средствах и информационных системах в процессе выполнения ими обработки информации или технологического процесса.

Технический контроль состояния защиты информации в системах управления производствами, транспортом, связью, энергетикой и передачи финансовой и другой информации осуществляется в соответствии со специально разрабатываемыми программами и методиками контроля, согласованными Гостехкомиссией России, владельцем объекта и ведомством по подчиненности объекта контроля.

Во всех органах исполнительной власти и организациях проверяется:

- наличие должностных лиц, структурных подразделений или отдельных сотрудников по защите информации, уровень их подготовки (квалификации);
- наличие и полнота отработки Руководства по технической защите информации в соответствии с требованиями руководящих документов ФСТЭК России, правильность оценки опасности технических средств разведки применительно к данному объекту;
- наличие и достаточность руководящих и внутренних организационно-распорядительных документов по защите информации;
- наличие физической защиты территории и здания, где размещаются устройства и носители информации, с помощью технических средств охраны и специального персонала, обеспечение пропускного режима и специального оборудования помещений, где размещаются устройства и носители информации;
- своевременность и правильность категорирования выделенных помещений, соблюдение порядка их аттестации при вводе в эксплуатацию, оформление разрешения на проведение закрытых мероприятий и ведение переговоров по секретной тематике;
- эффективность мероприятий по защите информации, осуществляемых на объектах при посещении их иностранными представителями;
- организация и фактическое состояние доступа персонала к защищаемым информационным ресурсам, наличие и качество организационно-распорядительных документов по допуску персонала к защищаемым ресурсам;
- выполнение организационных и технических мер по технической защите информации при ее обработке средствами вычислительной и оргтехники;
- соответствие принятых мер по технической защите информации установленным нормам и требованиям.

В органах исполнительной власти и органах производственного управления (холдингах, аппаратах научно-производственных и производственных объединений, вышестоящих акционерных обществах по отношению к дочерним и зависимым организациям) проверяется:

- наличие в системе соответствующего органа исполнительной власти или производственного управления (далее − органа управления) необходимых руководящих документов по защите информации;
- своевременность доведения требований руководящих документов по технической защите информации до сотрудников аппарата и подведомственных организаций;
- состояние информационной безопасности в ведомственных (корпоративных) сетях связи и информатизации;

- деятельность аппарата органа управления по методическому руководству и координации работ по технической защите информации в отраслевых (дочерних, зависимых) организациях.

В научно-исследовательских и проектных организациях, на промышленных предприятиях и в испытательных организациях оборонного промышленного комплекса проверяется также:

- перечень проводимых работ и создаваемых образцов вооружения и военной техники, подлежащих защите от технических разведок, в соответствии с годовым планом (перечнем) работ по оборонной тематике;
- наличие в технических заданиях на разработку (создание) изделий (систем, средств, объектов) разделов по защите охраняемых сведений (характеристик) и конкретных требований по защите информации;
- качество проработки и обоснованность в эскизных и технических проектах мероприятий по защите информации, перечней охраняемых сведений и демаскирующих признаков, правильность определения технических каналов утечки информации и их опасности;
- наличие и полнота отработки «Инструкции по технической защите информации (противодействию техническим средствам разведки)» для различных этапов жизненного цикла объектов защиты (изделий);
- наличие и правильность ведения документов на рабочие места, где проводятся работы по закрытой тематике, а также журналов учета времени работы изделий;
- правильность оценки разведдоступности защищаемых работ (изделий) на объекте и основные результаты проведенного ранее на объекте технического контроля (аттестации);
- наличие и деятельность экспертных комиссий на предприятиях, осуществляющих поставки образцов вооружения и военной техники на экспорт, а также степень привлечения к их работе специалистов по технической защите информации и представителей заказчика;
- эффективность мер по защите охраняемых характеристик образцов вооружения и военной техники, их элементов − носителей защищаемой информации, охраняемых характеристик предприятия (как объекта защиты) по результатам технического контроля.

В информационных и автоматизированных системах обработки информации проверяется:

- наличие сведений, составляющих государственную или служебную тайну, циркулирующих в средствах обработки информации и помещениях в соответствии с принятой на объекте технологией обработки информации;
- правильность категорирования объектов информатизации, а также классификации автоматизированных систем в зависимости от степени секретности обрабатываемой информации;

- наличие и правильность оформления аттестатов соответствия на объекты информатизации, а также сертификатов на средства защиты информации, наличие материалов по специальным исследованиям и специальным проверкам технических средств (в необходимых случаях);
- организация и фактическое состояние доступа обслуживающего и эксплуатирующего персонала к защищаемым информационным ресурсам, наличие и качество организационно-распорядительных документов по допуску персонала к защищаемым ресурсам, организация учета, хранения и обращения с конфиденциальными машинными носителями информации;
- состояние учета всех технических и программных средств отечественного и иностранного производства, участвующих в обработке информации, подлежащей защите, наличие и правильность оформления документов по специальным исследованиям и проверкам технических средств информатизации, в том числе на наличие недекларированных возможностей программного обеспечения;
- правильность размещения технических средств информатизации (с привязкой к помещениям, в которых они установлены), трасс прокладки информационных и неинформационных цепей, выходящих за пределы контролируемой территории, в соответствии с предписаниями на эксплуатацию;
- обоснованность и полнота выполнения организационных и технических мер по защите информации, циркулирующей в средствах электронной вычислительной техники;
- наличие, правильность установки и порядка эксплуатации средств защиты от несанкционированного доступа и специальных программно-математических воздействий к информации;
- выполнение требований по технической защите информации при присоединении автоматизированных систем ее обработки к внешним и международным информационным системам общего пользования;
- оценка эффективности мер защиты по результатам проведения выборочного технического контроля.

В системах и сетях связи, автоматизированных системах управления и передачи данных проверяется:

- выполнение требований по технической защите информации при присоединении ведомственной (внутренней) сети связи к сети связи общего пользования, взаимоувязанной сети связи Российской Федерации;
- полнота и правильность оценки разведдоступности каналов и линий связи, анализ характера передаваемой по ним информации;
- наличие и правильность установки аппаратуры технической зашиты информации в каналах связи, а также ее исправность и работоспособность;

- обоснованность и полнота выполнения мероприятий по обеспечению защищенности от воздействий систем автоматизированного управления, а также систем передачи оперативно-диспетчерской информации;
- состояние технической защиты информации в ходе деятельности предприятий связи по обеспечению живучести и устойчивости магистральных сетей связи;
- обеспечение защищенности от программно-математических воздействий и несанкционированного доступа систем управления цифровым коммутационным оборудованием;
- эффективность мероприятий по защите оконечных устройств и коммутационного оборудования, размешенных в выделенных помещениях или передающих подлежащую защите информацию, наличие материалов по специальным исследованиям и специальным проверкам технических средств (в необходимых случаях).

В финансово-кредитных организациях, обслуживающих органы исполнительной власти и предприятия оборонного промышленного комплекса, проверяется:

- наличие требований по технической защите информации клиентов финансово-кредитной организации — органов исполнительной власти и предприятий оборонного промышленного комплекса;
- наличие специального участка (комплекса технических средств) для обработки информации, подлежащей защите;
- эффективность специального технологического процесса выделения подлежащей защите информации из общего массива финансовой информации.

В организациях, осуществляющих топографо-геодезическую и картографическую деятельность или использующих топографо-геодезическую информацию, проверяется:

- наличие лицензий и разрешений на выполнение топографогеодезических и картографических работ;
- технические мероприятия по защите информации при осуществлении цифровой обработки фотоматериалов и обоснованность грифа секретности производных материалов;
- технические мероприятия по защите информации при разработке и изготовлении тематических и специальных карт и планов на основе секретных топографических материалов;
- соответствие установленному порядку производства, реализации или эксплуатации аппаратуры для определения координат, работающей по сигналам космических аппаратов;
- порядок внедрения и использования геоинформационных систем для целей обработки подлежащей защите информации.

Литература:

1. Солодянников А.В. Комплексная система защиты объектов информатизации: учебное пособие. – СПб.: Изд-во СПбГЭУ, 2017. − 91 с.
2. Солодянников А.В. Международные и российские акты и стандарты по информационной безопасности : учебное пособие. – СПб.: Изд-во СПбГЭУ, 2017. − 87 с.

2.3. Управление влиянием на проявления человеческого фактора при обеспечении информационной безопасности автоматизированной системы

Одним из негативных факторов, влияющих на состояние информационной безопасности страны, является наращивание рядом зарубежных стран воздействий на информационную инфраструктуру с политическими и экономическими целями. Это влечет за собой постоянное повышение сложности и увеличение масштабности деструктивных воздействий на объекты критической информационной инфраструктуры. Поэтому жизненно важной задачей становится максимальная защищенность автоматизированных систем (АС) от киберугроз [1]. В этой связи следует отметить факторы, обусловливающие актуальность проблемы обеспечения информационной защищенности (ИЗ) оператора/операторов АС [2] с целью снижения влияния человеческого фактора.

Вытекающие факторы условно можно разделить на три группы.

К первой группе факторов относятся угрозы, воздействующие на оператора и вызывающие непреднамеренные (в ходе реализации этого воздействия непреднамеренные трансформируются в преднамеренные) действия оператора, приводящие к нарушению целостности и доступности информации, циркулирующей в автоматизированной системе управления (АСУ). В этой связи растут информационные нагрузки на оператора АС как со стороны среды (стрессовые, неблагоприятные состояния), так и со стороны профессиональной деятельности (сложность, большой объем информации).

Вторая группа факторов характеризуется современным представлением защиты информации как информационной безопасности (ИБ) [2-4]. Новое представление заключается в реализации комплексного подхода по двум основным направлениям:

- защиты информации;
- защиты от информации.

Второе направление сегодня приобретает международный масштаб и стратегический характер, становится одной из ключевых проблем современности. При этом выделяют три основных направления защиты от ин-

формационных воздействий: на информационно-технические системы и средства, на общество, на личность. Однако этот вид угроз в обеспечении ИБ в настоящее время недостаточно учитывается.

Факторы третьей группы включают определение АС [2, 5], согласно которому человек-оператор и технические средства являются единым конгломератом АС. Причем, оператор в силу специфики своей профессиональной деятельности подвержен внешним информационным воздействиям, последствия которых могут носить тяжелый деструктивный характер. Человек-оператор является уязвимым звеном АС, необходимым условием бесперебойного и эффективного ее функционирования.

Далее следует отметить, что характерной особенностью последних десятилетий является широкое внедрение средств информатизации в критически важные объекты, которые оказывают существенное влияние на национальную безопасность Российской Федерации, прекращение или нарушение функционирования которого приводит к чрезвычайной ситуации [2, 6].

Согласно официальному определению, ключевой системой информационной инфраструктуры (КСИИ) является информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление (или информационное обеспечение управления) критически важным объектом (процессом), в результате деструктивных воздействий на которую может сложиться чрезвычайная ситуация или будут нарушены выполняемые системой функции управления со значительными негативными последствиями. Критически важными являются объекты, прекращение или нарушение функционирования которых может привести к тяжелым последствиям для региона или государства в целом, в том числе и к человеческим жертвам.

При этом следует обратить внимание на то, к КСИИ в первую очередь относятся автоматизированные системы управления технологическими процессами (АСУ ТП) объектов атомной промышленности, топливно-энергетического комплекса, транспортной отрасли и т.д. Роль человека-оператора в таких системах и специфика его профессиональной деятельности, а в результате воздействия – не только уязвимый элемент АС, но и средство реализации угроз. Мировой опыт доказывает [7], что оператор является внутренним нарушителем, порождает угрозы, которые усиливают уязвимости организационно-технических мер, повышают риски, ведут к потере информации, нарушают конфиденциальность, доступность и целостность информации.

К сожалению, специалисты в сфере ИБ, недооценивают такой аспект в обеспечении ИБ как неосознаваемые реакции человека-оператора [2-4]. Зависимость информационной защищенности оператора от его состояния представлена на рис. 2.9.

Рисунок 2.9. Информационная защищенность оператора АС

Поэтому при организации работы на предприятии важно оценить профессионально-личностную готовность оператора/группы операторов АС к продолжению работы в конкретный момент времени. Решение данной задачи обусловливает обращение к методам оценки профессионально-личностной готовности и средствам математического моделирования.

Один из современных методов, позволяющих одновременно оценивать и физиологическое, и психологическое состояние человека – метод газоразрядной визуализации (ГРВ), основанный на эффекте Кирлиан. Данный эффект заключается в формировании характерного свечения живых тканей при их помещении в электромагнитное поле высокой напряженности. Простота применения, высокая скорость обработки полученных данных и автоматизированное формирование экспертного заключения [3, 4] обусловливает применение метода ГРВ в различных сферах жизнедеятельности человека.

Любой аппаратно-программный комплекс, работающий на основе методики ГРВ, после обработки полученных данных представляет ряд параметров, значения которых носят универсальный характер. В частности, к таким параметрам относятся площадь свечения (съемки), коэффициент активации и уровень симметрии.

В рамках исследования была разработана математическая модель, позволяющая на основе вышеуказанных параметров формировать заключение о профессионально-личностной готовности одного оператора АС и оценивать готовность группы операторов к продолжению работы [3]. Далее приводится описание математической модели.

Пусть n – число параметров, используемых для оценки состояния j-го оператора при $n \geq 2$, и вектор состояния A_j^n имеет вид:

$$A_j^n = \begin{pmatrix} a_{1j} \\ \dots \\ a_{nj} \end{pmatrix},$$

где a_{ij} – значение параметра, участвующего в анализе, $j \in [1, 2, \dots, k]$.

Тогда на вход алгоритму оценки текущего состояния оператора АС подается матрица параметров M_k^n:

$$M_k^n = \begin{pmatrix} a_{11} & \dots & a_{1k} \\ \dots & \ddots & \dots \\ a_{n1} & \dots & a_{nk} \end{pmatrix},$$

где k – число операторов.

По каждому вектору состояния A_j^n, где $j \in [1, 2, \dots, k]$, производятся вычисления общего суммарного балла S_j и максимальной абсолютной разности между всеми попарно взятыми параметрами $|\Delta_{\max}|_j$:

$$S_j = \sum_i^n a_i \ .$$

$$|\Delta_{\max}|_j = \max\left(|a_{1k} - a_{2k}|, |a_{1k} - a_{3k}|, \cdots, |a_{1k} - a_{nk}|, \cdots, |a_{2k} - a_{3k}|, \cdots, |a_{(n-1)k} - a_{nk}|\right)$$

Суммарный балл S_j характеризует текущее состояние оператора АС, максимальная абсолютная разность между всеми попарно взятыми параметрами $|\Delta_{\max}|_j$ позволяет проверить наличие противоречия между характеристиками параметров.

На основании значений суммарного балла S_j и абсолютной разности $|\Delta_{\max}|_j$ производится формирование экспертного заключения по решающим правилам. В таблице 1 [3] представлены решающие правила по формированию заключения о профессионально-личностной готовности оператора на основе параметров ГРВ. На рисунке 2.10 представлена структурная схема алгоритма оценки профессионально-личностной готовности оператора АС [3].

Таблица 2.1. Решающие правила по формированию заключения о профессионально-личностной готовности на основе параметров газоразрядной визуализации

S_j	$\lvert\Delta_{\max}\rvert_j$	Заключение о профессионально-личностной готовности оператора
$[-n;-0{,}7n)$	0	Снижение профессионально-личностной готовности
$[-0{,}7n;-0{,}4n)$	1	Снижения активности, возможно переутомление
$[-0{,}4n;0{,}4n]$	0; 1	Хорошая профессионально-личностная готовность
	2	Низкая профессионально-личностная готовность, необходимо дополнительное обследование
$(0{,}4n;0{,}7n]$	1	Повышение активности
$(0{,}7n;n]$	0	Повышение стрессового фона

Значения S_j и $\lvert\Delta_{\max}\rvert_j$ каждого оператора АС сводятся в матрицу параметров B_k^2:

$$B_k^2 = \begin{pmatrix} S_1 & \dots & S_k \\ \lvert\Delta_{\max}\rvert_1 & \dots & \lvert\Delta_{\max}\rvert_k \end{pmatrix}.$$

Рисунок 2.10. Структурная схема алгоритма оценки профессионально-личностной готовности оператора автоматизированной системы

По столбцам матрицы B_k^2 в соответствии с таблицей 2.1 формируются четыре интерпретатора (в процентах: от 0% – 100%) профессионально-личностной готовности группы операторов:

w (work) – готовы к работе: хорошая профессионально-личностная готовность,

p (pause) – требуется перерыв: снижение активности, возможно переутомление; состояние повышенной активности;

f (finish) – не готовы к работе: снижение профессионально-личностной готовности; повышение стрессового фона;

e (error) – значения не интерпретированы: низкая профессионально-личностная готовность, необходимо дополнительное обследование.

Полученные значения интерпретаторов *w, p, f* и *e,* используются для формирования заключения о готовности группы к продолжению работы в текущий момент времени по двум критериям: *T (tangible)* и *I (ideal)*, которые вычисляются по формулам:

$$T = \frac{w + p}{w + p + f + e},$$

$$I = \frac{w}{w + p + f + e}.$$

Значения критериев *T*, *I* и *e* интерпретируются в соответствии с решающими правилами по формированию заключения о профессионально-личностной готовности операторов (табл. 2.2). Для корректного формирования экспертного заключения о профессионально-личностной готовности группы операторов вводится коэффициент ν:

- 0,8 – внештатная ситуация;
- 1 – штатная ситуация.

Полученное соотношение критериев обрабатывается алгоритмом в соответствии с правилами принятия решения по формированию заключения о профессионально-личностной готовности операторов с учетом коэффициента оценки рабочей обстановки, значение которого также указывается при подаче на вход алгоритма матрицы параметров (табл. 2.2).

Таблица 2.2. Решающие правила по формированию заключения о профессионально-личностной готовности операторов

e	*T*	*I*	Заключение о профессионально-личностной готовности операторов
[0,2; 1]	любое	любое	Оценка профессионально-личностной готовности операторов невозможна
[0, 0,2)	$[0;0{,}75\nu]$	$[0, 0{,}75T]$	Низкая профессионально-личностная готовность операторов

Окончание табл. 2.2

e	T	I	Заключение о профессионально-личностной готовности операторов
		$[0{,}75T;T]$	Удовлетворительная профессионально-личностная готовность операторов
	$(0{,}75v;1]$	$[0;\ 0{,}75T]$	Средняя профессионально-личностная готовность операторов
		$(0{,}75T;T]$	Высокая профессионально-личностная готовность операторов

Созданный программный модуль реализует алгоритм анализа массива данных и входит в методику оценки профессионально-личностной готовности оператора/операторов автоматизированной системы, обобщающая схема которого представлена на рисунке 2.11.

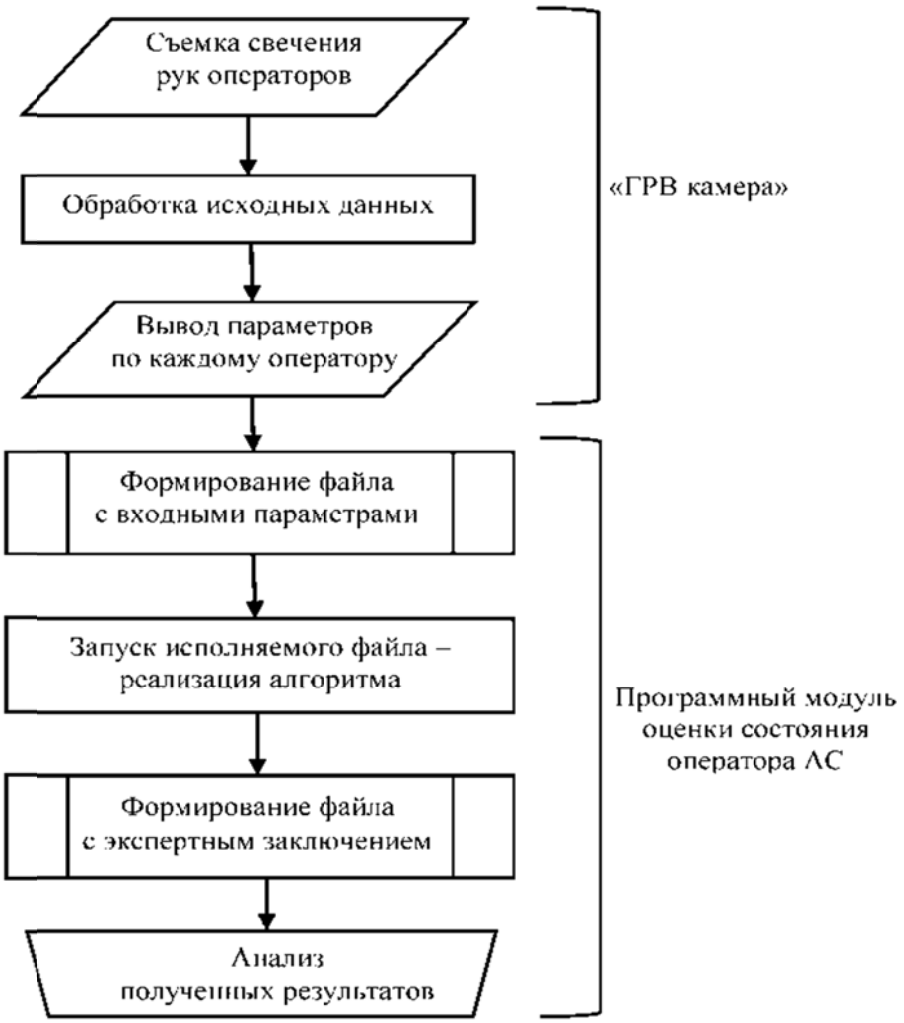


Рисунок 2.11. Обобщенная схема методики оценки профессионально-личностной готовности оператора/операторов автоматизированной системы

Таким образом, разработанная система и методика оценки на основе метода ГРВ позволяет определить текущее состояние оператора/операторов, может быть использована для снижения влияния человеческого фактора на ИБ АС, а также – при исследовании прогностической оценки профессионально-личностной готовности группы операторов к решению профессиональных задач.

Литература:

1. Информационная безопасность в России в современных условиях // Защита информации. Инсайд. – 2017. – №2 – С. 4-6.
2. Сухостат В.В., Ульзетуева Д.Д. К вопросу об информационной защищенности оператора автоматизированных систем // Государство и бизнес. Современные проблемы экономики: Материалы X Международной научно-практической конференции. Санкт-Петербург, 25-27 апреля 2018 г. / СЗИУ РАНХиГС при Президенте РФ. Том 1. – 293 с., С. 235-238.
3. Гатчин Ю.А., Поляков В.И., Сухостат В.В. Методика оценки информационной защищенности оператора автоматизированных систем на основе метода газоразрядной визуализации // Вестник компьютерных и информационных технологий – 2017. – № 6 (56). – С.45-49.
4. Гатчин Ю.А., Поляков В.И., Сухостат В.В. Методика оценки информационной защищенности оператора информационных систем в условиях деструктивных информационных воздействий//Вестник компьютерных и информационных технологий – 2015. – №2. – С.54-60.
5. ГОСТ 34.003–90. Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения [Электронный ресурс]. URL: http://www.internet-law.ru/gosts/gost/10673 (дата обращения 28.10.2018).
6. Приказ ФСТЭК России от 14.03.2014 N 31 (ред. от 09.08.2018 г.) 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. [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_165503/ (дата обращения 28.10.2018).
7. ГОСТ Р ИСО/МЭК 15408. Методы и средства обеспечения безопасности и критерии оценки безопасности информационных технологий. [Электронный ресурс]. URL: http://files.stroyinf.ru/data2/1/4293829/4293829823.pdf (дата обращения 28.10.2018).

2.4. Система обработки и обеспечения безопасности персональных данных в организации

В соответствие с требованиями ФЗ «О персональных данных» от 27.07.2006 года № 152 (в редакции ФЗ от 25.07.2011г. № 261) каждая организация (предприятие, учреждение, общество и др.), являющаяся юридическим лицом, относится к категории оператора персональных данных (далее ПДн). Указанным ФЗ определены обязанности и права оператора и субъек-

та ПДн. В частности, оператор обязан сформировать систему обработки и обеспечения безопасности персональных данных (далее СООБПДн).

Как известно, любая система содержит три главные компоненты: люди, документы, техника. Люди – сотрудники (работники) организации, подготовленные в профессиональном отношении к выполнению возложенных на них задач. Документы – организационно- распорядительные документы (ОРД), разработанные на основе нормативных правовых актов РФ, нормативных, руководящих и методических документов различного рода регуляторов, в том числе ГОСТы, и предназначенные для формирования и организации функционирования СООБПДн. Техника – средства вычислительной техники (СВТ) и технические средства защиты информации (СЗИ), которые составляют техническую основу информационных систем персональных данных (ИСПДн).

В соответствие с ОРД из числа работников организации назначается (ются) должностное лицо (лица), ответственное (ые) за формирование системы обработки и обеспечения безопасности ПДн, составляются и утверждаются установленным порядком списки должностных лиц, допущенных к обработке ПДн, списки сотрудников, обеспечивающих выполнение мероприятий по защите ПДн, списки сотрудников, осуществляющих эксплуатацию ИСПДн.

Одним из главных элементов СООБПДн являются ОРД. От их состава и содержания в значительной степени зависит успех функционирования всей системы в целом. Перед формированием пакета ОРД целесообразно провести комплекс предварительных мероприятий. В частности, в первую очередь следует четко определить потенциальные угрозы ПДн, которые могут быть реализованы в организации. С этой целью необходимо разработать частную модель угроз ПДн и, соответственно, модель нарушителя. Решение указанной задачи в настоящее время облегчается наличием «Банка данных угроз безопасности информации», разработанным ФСТЭК России и размещенным на ее сайте. Кроме этого следует создать комиссию по установке уровня защищенности ПДн, определению класса защищенности ИСПДн как автоматизированной системы, а также по оценке эффективности реализованных мер защиты.

Учитывая, что с ПДн выполняются два действия, а именно: обработка и обеспечение их безопасности, то с целью уменьшения общего количества документов целесообразно разработать один объединяющий документ, а именно − «Положение об обработке и обеспечении безопасности персональных данных в организации» (далее Положение). Как следует из 152 ФЗ, обработка персональных данных − любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хра-

нение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. Разработанное Положение должно содержать соответствующие разделы.

В частности, в качестве примера содержание Положения может иметь следующую структуру:

1. Общие положения
2. Основные термины и определения
3. Цели обработки и состав персональных данных работников
4. Сбор и порядок обработки персональных данных
5. Обеспечение безопасности персональных данных
6. Передача и хранение персональных данных
7. Доступ к персональным данным
8. Блокирование, уточнение, уничтожение и обезличивание персональных данных
9. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

Разработка каждого раздела должна быть проведена на основе положений нормативных правовых актов РФ и руководящих документов соотвевтствующих регуляторов. Так, обезличивание ПДн должно осуществляться в соответствии с Приказом Роскомнадзора от 05.09.2013 N 996 «Об утверждении требований и методов по обезличиванию персональных данных» (вместе с «Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ») (Зарегистрировано в Минюсте России 10.09.2013 N 29935).

Особое внимание следует уделить формированию «Перечня персональных данных организации». В организации (на Предприятии) могут обрабатываться персональные данные следующих категорий субъектов ПДн:

- работники Предприятия;
- бывшие работники Предприятия;
- лица, претендующие на трудоустройство на Предприятие;
- лица, которым оформляется разовый или временный пропуск на Предприятие;
- лица, являющиеся контрагентами Предприятия по гражданско-правовым договорам.

В качестве возможного варианта при формировании организационно-распорядительных, эксплуатационных документов и форм можно рассмотреть следующий комплект:

1. Приказ о назначении ответственного за обеспечение безопасности информации персональных данных в организации

2. Приказ о назначении администратора безопасности ИСПДн
3. Приказ о создании комиссии по установке уровня защищенности ПДн, определению класса защищенности ИСПДн как автоматизированной системы, а также по оценке эффективности реализованных мер защиты. ИСПДн
4. Правила рассмотрения запросов субъектов персональных данных или их представителей
5. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных
6. Приказ о проведении внутренней проверки
7. План внутренних проверок режима защиты персональных данных
8. Отчет о результатах проведения внутренней проверки
9. Приказ об утверждении списка лиц, которым необходим доступ к персональным данным, обрабатываемым в информационных системах персональных данных, для выполнения служебных (трудовых) обязанностей
10. Приказ о выделении помещения (помещений), в котором (ых) производится обработка персональных данных
11. Положение об организации режима безопасности помещений, где осуществляется работа с персональными данными
12. Порядок резервного копирования информации
13. Положение о порядке организации и проведения работ по защите персональных данных при их обработке
14. Положение об обработке и обеспечении безопасности персональных данных в организации
15. Разрешительную систему доступа (матрицу доступа пользователей к информационным ресурсам, программным и техническим средствам ИСПДн).
16. Положение о порядке хранения и уничтожения машинных носителей персональных данных
17. Положение о разграничении прав доступа к обрабатываемым персональным данным
18. План мероприятий по обеспечению защиты персональных данных
19. Журнал по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним
20. Руководство пользователя абонентскими пунктами ИСПДн
21. Руководство администратора безопасности ИСПДн
22. Инструкция системного администратора ИСПДн
23. Инструкция по антивирусной защите ИСПДн
24. Инструкция по парольной защите ИСПДн
25. Инструкция о порядке обращения с носителями конфиденциальной информации

26. Журнал учета машинных носителей информации
27. Журнал по учету мероприятий по контролю обеспечения защиты персональных данных
28. Приказ о ведении электронного журнала обращений пользователей информационных систем персональных данных
29. Перечень сведений конфиденциального характера
30. Перечень персональных данных, подлежащих защите
31. Перечень ИСПДн
32. Правила работы с обрабатываемыми обезличенными персональными данными
33. Перечень должностных лиц, ответственных за проведение мероприятий по обезличиванию персональных данных
34. Типовая форма согласия на обработку персональных данных
35. Типовая форма обязательства о неразглашении
36. Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои данные
37. Типовая форма Согласия субъекта на получение его персональных данных у третьей стороны
38. Типовая форма Согласия субъекта на передачу его персональных данных третьей стороне
39. Типовая форма Запроса о предоставлении персональных данных работников Предприятия (личных дел) для ознакомления
40. Типовая форма Заявления об отзыве согласия на обработку
41. Памятка по обеспечению режима безопасности в помещении, в котором осуществляется обработка персональных данных
42. Инструкция по обработке персональных данных без использования средств автоматизации

Кроме рассмотренного варианта комплекта ОРД необходимо разработать и ввести в действие документы на аттестованные ИСПДн, а именно − аттестаты соответствия с приложениями.

Таким образом, создание системы обработки и обеспечения безопасности персональных данных в организации, отвечающей действующим требованиям не простой и трудоемкий процесс, предполагающий инициативную и творческую деятельность значительного количества сотрудников организации.

Литература:

1. О персональных данных. Федеральный закон от 27 июля 2006 г. № 152-ФЗ.
2. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных. Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119.
3. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информаци-

онных системах персональных данных. Приказ ФСТЭК России от 18 февраля 2013 г. № 21.
4. Об утверждении требований и методов по обезличиванию персональных данных. Приказ Роскомнадзора от 05.09.2013 N 996.
5. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Приказ Гостехкомиссии России от 30.08.2002 №282.
6. Банк данных угроз безопасности информации. ФСТЭК России, ФАУ «ГНИИИ ПТЗИ ФСТЭК России», 2015 [Электронный ресурс]. URL: https://bdu.fstec.ru/ (дата обращения: 30.10.2018).
7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена 15.02.2008 заместителем директора ФСТЭК России.
8. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена 14.02.2008 заместителем директора ФСТЭК России.

2.5. Организация защиты персональных данных в банковских информационных системах

В организациях банковской системы Российской Федерации, согласно методическим рекомендациям по выполнению законодательных требований при обработке персональных данных, составленных на основе комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» для организаций банковской системы Российской Федерации (БС РФ) и общим требованиям по обеспечению информационной безопасности банковских технологических процессов, в рамках которых обрабатываются персональные данные (ПДн), предусматривается использование частных моделей угроз безопасности персональных данных, содержащих актуальные для организации БС РФ угрозы [1-3].

Отраслевая модель угроз безопасности персональных данных, содержащая актуальные для организации БС РФ угрозы безопасности персональных данных (УБПДн) действовала до 2014 года и была ориентиром для оценки рисков нарушения безопасности персональных данных, учитывающей особенности их обработки в конкретной организации БС РФ [1]. Сейчас модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн) может быть разработана на основе базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, банка данных угроз безопасности информации, потенциала нарушителя, рекомендованных ФСТЭК России или с использованием обучающих специальных сервисов [3-5].

Информационные системы персональных данных (ИСПДн) представляют собой совокупность информационных и программно-аппаратных элементов, а также информационных технологий, применяемых при обработке персональных данных. Приведем основные элементы ИСПДн [1]:

- Персональные данные, содержащиеся в базах данных, как совокупность информации и ее носителей, используемых в ИСПДн.
- Информационные технологии, применяемые при обработке ПДн.
- Технические средства, осуществляющие обработку ПДн (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн, средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации).
- Программные средства (операционные системы, системы управления базами данных и т.п.).
- Средства защиты информации.
- Вспомогательные технические средства и системы (ВТСС).
- Технические средства и системы, системы коммуникации, не предназначенные для обработки ПДн, но размещенные в служебных помещениях, где расположены ИСПДн, технические средства (различного рода телефонные средства и системы, средства вычислительной техники, средства и системы передачи данных в системе радиосвязи, средства и системы охранной и пожарной сигнализации, средства и системы оповещения и сигнализации, контрольно-измерительная аппаратура, средства и системы кондиционирования, средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения, средства электронной оргтехники и др.).

Классификационные признаки угроз для базовой модели угроз безопасности персональных данных при их обработке в ИСПДн:

- по виду защищаемой информации;
- по видам возможных источников угроз;
- по типу информационных систем персональных данных;
- по способу реализации угроз;
- по виду нарушаемого свойства информации (виду несанкционированных действий);
- по используемой уязвимости;
- по объекту воздействия.

Данные признаки являются базовыми для формирования систематизированного перечня УБПДн при их обработке в ИСПДн и разработке на

их основе частных моделей. Частная модель угроз безопасности персональных данных при их обработке в ИСПДн организации БС РФ учитывает также особенности обработки персональных данных в конкретной организации БС РФ [2, 6].

Ниже представлен возможный перечень персональных данных работников организации БС РФ:

- табельный номер работника;
- фамилия, имя, отчество (в т.ч. прежние), дата и место рождения;
- паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство;
- характеристики, идентифицирующие физиологические особенности человека и на основе которых можно установить его личность;
- адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания;
- номера телефонов (мобильного и домашнего), в случае их регистрации на субъекта персональных данных или по адресу его места жительства (по паспорту);
- сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки;
- сведения о повышении квалификации и переподготовке;
- сведения о трудовой деятельности;
- сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней;
- содержание и реквизиты трудового договора с работником Организации или гражданско-правового договора с гражданином;
- сведения о заработной плате;
- сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу;
- сведения о семейном положении;
- сведения об имуществе;
- сведения о номере и серии страхового свидетельства государственного пенсионного страхования;
- сведения об идентификационном номере налогоплательщика;
- сведения из страховых полисов обязательного (добровольного) медицинского страхования;
- сведения, указанные в оригиналах и копиях приказов по личному составу организации и материалах к ним;
- сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях;
- материалы по аттестации и оценке работников;

- материалы по внутренним служебным расследованиям в отношении работников;
- внутрибанковские материалы по расследованию и учету несчастных случаев на производстве и профессиональным заболеваниям;
- сведения о временной нетрудоспособности работника;
- сведения о социальных льготах и о социальном статусе.

Целями обработки персональных данных являются:

- осуществление функций, возложенных на организацию;
- организация учета служащих кредитной организации для обеспечения соблюдения законов и иных нормативно-правовых актов;
- содействие сотрудникам организации БС РФ в обучении, продвижении по службе, использовании различного вида льгот.

По данным портала персональных данных Уполномоченного органа по защите персональных данных, ПАО Сбербанк использует следующие и параметры ПДн физического лица в информационных системах [7]:

- фамилия, имя, отчество, год рождения, месяц рождения дата рождения, место рождения, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы;
- сведения о смене фамилии, имени или отчества;
- пол;
- гражданство;
- данные паспорта гражданина РФ или при его отсутствии иного документа, удостоверяющего личность в соответствии с законодательством РФ;
- данные заграничного паспорта;
- данные, включенные в документы воинского учета;
- данные водительского удостоверения;
- данные, включенные в свидетельство о браке;
- идентификационный номер налогоплательщика (ИНН);
- страховой номер индивидуального лицевого счета;
- сведения об обязательствах заемщика;
- сведения о близких родственниках;
- сведения о трудовом стаже и трудовой деятельности;
- номера городских и мобильных телефонов, номера факсов, адреса электронной почты;
- информация о транспортном средстве;
- номер банковской карты, номер банковского счета, номер ДЕПО счета;
- идентификатор клиента;
- IP-адрес пользователя сервиса, логин пользователя сервиса, файлы cookies, дата/время использования сервиса;
- номер участника программы лояльности «Аэрофлот Бонус»;

- персональные данные, относящиеся к специальной категории персональных данных: сведения о состоянии здоровья субъектов персональных данных (застрахованных лиц);
- персональные данные, относящиеся к биометрическим персональным данным (для сотрудников и их близких родственников, физических лиц, осуществляющим выполнение работ по оказанию услуг и заключивших с банком договор гражданско-правового характера и пр.): цифровое фотографическое изображение лица, использующееся банком для установления личности субъекта персональных данных, слепок голоса, оцифрованное изображение рисунка вен ладони.

Перечень типовых ошибок при реализации требований законодательства о ПДн, подлежащих защите в организации БС РФ:

1. в сфере компетенции Роскомнадзора:
- отсутствует согласие субъекта ПДн на обработку его ПДн;
- не уничтожены ПДн после обращения субъекта;
- не послано уведомление субъекту об уничтожении его ПДн;
- предоставление ПДн третьим лицам без согласия субъекта ПДн;
- несоответствие реальной обработки ПДн заявленным целям обработки;
- прямой маркетинг без получения предварительного согласия субъекта ПДн;
- обработка ПДн без уведомление Роскомнадзора;
- отсутствие в договоре с третьими лицами условия обеспечения конфиденциальности;
2. в сфере компетенции ФСТЭК России:
- отсутствие требований по технической защите персональных данных в ТЗ и проектной документации на ИСПДн;
- незавершенность классификации ИСПДн или ее ошибочность;
- невыполнение работ по анализу угроз информационной безопасности;
- незавершенность разработки необходимого комплекта организационно-распорядительной документации;
- отсутствие необходимых мер и сервисов защиты информации;
- непринятие мер по учету машинных носителей;
- отсутствие в должностных регламентах ответственных лиц за защиту ПДн и их полномочий по контролю за выполнением требований безопасности;
- отсутствие достаточного количества квалифицированных специалистов;
3. в сфере компетенции ФСБ России:
- использование средств криптографической защиты информации (СКЗИ), отличающихся от эталонных сертифицированных версий;

- невыполнение отдельных требований по порядку эксплуатации СКЗИ, предусмотренных технической документацией;
- несовершенство отдельных подготовленных оператором документов, регламентирующих вопросы обеспечения безопасности в конкретной организации.

Например, согласно принятой политики обработки персональных данных в ПАО Сбербанк, обеспечение безопасности обрабатываемых персональных данных осуществляется в рамках единой комплексной системы организационно-технических и правовых мероприятий по защите информации, составляющей банковскую и коммерческую тайну, с учетом требований законодательства о персональных данных и принятых в соответствии с ним нормативных правовых актов. Система информационной безопасности банка непрерывно развивается и совершенствуется на базе требований международных и национальных стандартов информационной безопасности, а также лучших мировых практик [8].

ПАО Сбербанк осуществляет автоматизированную и неавтоматизированную обработку персональных данных, передачу персональных данных по телекоммуникационным каналам связи международного информационного обмена «Интернет», корпоративной сети Банка и на материальных носителях персональных данных в многопользовательском режиме с разграничением прав доступа. Перечень основных операций, осуществляемых с персональными данными клиентов и работников Банка [7]: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), блокирование, обезличивание, уничтожение.

Правовое обоснование обработки персональных данных как один из методов их защиты в применяемых информационных системах персональных данных ПАО Сбербанк:

1. Законодательство РФ:

- ФЗ «О персональных данных»;
- Приказ ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСБ России от 10 июля 2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- Положение Центрального Банка России от 9 июня 2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»;

2. Внутренние нормативные документы:

- Стратегия информационной безопасности ОАО «Сбербанк России» от 20.10.2014 № 516 §1;
- Политика обработки персональных данных в ПАО «Сбербанк России» от 29.04.2014 № 3324;
- Политика кибербезопасности ПАО Сбербанк от 20.11.2017 № 4660;
- Политика управления процессами ОАО «Сбербанк России» от 28.02.2014 № 1995-2;
- Политика ОАО «Сбербанк России» по обмену данными с третьими лицами от 30.06.2015 № 3904;

3. Локальные акты:

- Положение о порядке обработки и защиты прав субъектов персональных данных в части организации управления персоналом ОАО «Сбербанк России» от 04.02.2013 № 2749;
- Порядок работы в ОАО «Сбербанк России» с документами, содержащими конфиденциальную информацию от 18.07.2005 № 1091-2-р;
- Сборник стандартов по обеспечению кибербезопасности от 24.01.2017 № 4456 (при использовании облачных интернет-сервисов, в автоматизированных системах, моделирование угроз кибербезопасности, при осуществлении к сервисам сети Интернет (на базе ПО Apache Hadoop), для обеспечения защиты от вредоносного кода, при размещения интернет-ресурсов ПАО Сбербанк на внешних площадках и организации массовых внутренних e-mail рассылок, при обезличивании данных).

4. Регламенты:

- Регламент процесса обработки персональных данных розничных клиентов ПАО Сбербанк от 17.12.2015 № 4065 (с учетом изменений от 20.04.2017 № 2);
- Регламент организации работы по предоставлению услуг с использованием системы «Клиент-Сбербанк» от 15.12.2011 № 1331-4-р (с учетом изменений от 26.05.2016 №4);
- Порядок предоставления услуг физическим лицам в рамках универсального договора банковского обслуживания от 25.06.2009 № 1718-р (с изменениями № 1-18);
- Порядок обеспечения безопасности информационных технологий в Сбербанке России от 28.12.2001 № 875;

- Порядок управления процессами обеспечения безопасности в ИТ инфраструктуре Сбербанка России от 12.01.2006 № 1410-р (с учетом изменений от 24.07.2009 № 2);
- Регламент ведения архивного дела в ПАО Сбербанк от 06.12.2016 № 3261-2 и Перечень документов со сроками хранения, образующихся в деятельности ПАО Сбербанк и его филиалов от 11.02.2015 № 1350-3;
- Порядок перевода информационных ресурсов в архивное состояние и разгрузки баз данных автоматизированных систем от 29.10.2002 № 1008-р.

Комплекс мер по технической защите персональных данных ПАО Сбербанк включает следующие компоненты.

1. Система защиты от несанкционированного доступа → доменная авторизация пользователей и доменная политика безопасности → Active Directory, служебная (инфраструктурная) система управления доступом к информационным ресурсам (СУД-ИР), proxy-сервер WebSEAL.

2. Блокирование внешних носителей информации на АРМ, включая носители с USB-интерфейсом и обеспечение антивирусной защиты на АРМ и серверах информационных систем → средства антивирусной защиты от утечек → ПО «Kaspersky Endpoint Security», ПО «Symantec Endpoint Protection».

3. Ограничения на программную среду, осуществляемое в соответствии с требованиями → управление ключами шифрования → ORACLE TDE.

4. Защита информационных систем и оборудования от внешних воздействий → подсистема межсетевого экранирования → ПАК СЗИ НСД «ФПСУ-IP» (разработчик − ООО «АМИКОН»), межсетевые экраны Cisco ASA.

5. Защита персональных данных в информационных системах при взаимодействии с клиентами, филиалами, внешними контрагентами → использование систем электронного документооборота → СКЗИ «Бикрипт-4.0-5.0», СКЗИ «Туннель 2.0», СКЗИ «Туннель-TLS», «VPN-Key-TLS Int». СКЗИ «ANET 5 Int», СКЗИ «Сигнатура-клиент», СКЗИ «Верба-OW».

6. Обнаружение и предотвращение вторжений → истопользование ПО предотвращения вторжений → ПО «StoneGate IPS (Intrusion Prevention System)».

7. Обнаружение фактов несанкционированного доступа к персональным данным, выявление и анализ уязвимостей → Средства контроля защищенности информации → MaxPatrol.

8. Контроль за утечками персональных данных и другой защищаемой информацией за периметр информационного обмена → Средства

DLP-системы (Data Leak Prevention) → «InfoWatch Traffic Monitor Enterprise» АО «ИнфоВотч».

Организационные меры (и ответственные лица) по защите персональных данных в ИСПДн, используемые в ПАО Сбербанк:

- непосредственный контроль за выполнением мер ИБ → администратор ИБ подразделений, эксплуатирующих СКЗИ;
- обеспечение безопасности функционирования СКЗИ → персонал эксплуатирующих и структурных подразделений, участвующих в электронном документообороте;
- организация работ по защите информации и проверке выполнения мер безопасности в подразделениях ТБ, эксплуатирующих СКЗИ → отдел по защите информационных технологий, входящий в состав Управлений безопасности филиалов ПАО Сбербанк;
- организация безопасности СКЗИ, криптографических ключей и их сохранность → клиент (по условиям Договора);
- организация регулярного контроля защищенности информационной инфраструктуры (внешний и внутренний инструментальный контроль защищенности на наличие уязвимостей, тестирование на проникновение на сетевом уровне и на уровне приложений → работники подразделения информационной безопасности с технологических рабочих мест, оборудованных сканером безопасности для серверов, СУБД, банковского ПО;
- организация контроля целостности программного обеспечения в информационных системах при выходе из строя оборудования, чрезвычайных ситуациях, стихийных бедствиях → процедуры резервного копирования и восстановления баз данных, системных и прикладных программ.

Начальник центра киберзащиты ПАО Сбербанк С. Валуйских отмечает, что модернизацию центра киберзащиты и управления противодействия кибермошенничеству (Security Operation Centre-SOC) ПАО Сбербанк называют одним из крупнейших в Европе и самым масштабным в России проектом трансформации SOC [9].

Основные подразделения распределенной структуры SOC ПАО Сбербанк расположены в Москве, но существуют ещё четыре региональных сервисных центра. Все они имеют следующую структуру [8-10]:

- круглосуточная дежурная смена → мониторинг событий кибербезопасности и реагирование на инциденты в режиме 24/7;
- отдел реагирования на инциденты кибербезопасности → реагирование на инциденты кибербезопасности в случаях, когда компетенций дежурной службы оказывается недостаточно;
- отдел киберугроз → аналитика в сфере киберугроз и раннее предупреждение рисков возникновения угроз и инцидентов;

- отдел средств защиты → администрирование систем, непосредственно влияющие на предоставление сервисов банка;
- отдел мониторинга → сопровождение средств и систем поддержки процессов SOC: SIEM, Ticketing, Reporting и др.

В ПАО Сбербанк достигнут высокий уровень надежности систем, обеспечивается их безопасность, несмотря на рост киберпреступлений в мире [11]. Так, время простоя автоматизированных систем к 2018 году снизилось до 0,3 часов /год, в то время как в 2013 году данный показатель был равен 7 часам/год. Объем транзакций возрос от 0,8 млрд операций в 2013 году до 4 млрд операций к 2018 году и запланирован к 2020 году уровень в 8 млрд операций. С использованием системы противодействия кибермошенничеству в 2016 году сохранены средства клиентов на сумму свыше 17 млрд руб. и с 2015 года отражается 100%DDoS атак [11].

В ПАО Сбербанк справедливо считают, что «данные о клиентах являются одним из наших ключевых активов» и будут продолжать заниматься их сохранностью [11, с.30].

В результате проведенного исследования определены особенности обеспечения информационной безопасности субъектов персональных данных организациями банковской системы РФ.

Литература:

1. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения [Электронный ресурс]. URL: https://www.cbr.ru/Content/Document/File/46921/st-10-14.pdf (дата обращения 13.11.2018).
2. Частная модель угроз и нарушителя безопасности персональных данных при их обработке в информационной системе персональных данных, 2015 [Электронный ресурс]. URL: https://isafety.ru/wp-content/uploads/2015/07/v10_Частная-модель.pdf (дата обращения 14.11.2018).
3. Банк данных угроз безопасности информации. [Электронный ресурс]. URL: http://bdu.fstec.ru (дата обращения 14.11.2018).
4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России [Электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god (дата обращения 13.11.2018).
5. Сервис создания моделей угроз [Электронный ресурс]. URL: http://www.threatmodel.com/#readme (дата обращения 14.11.2018).
6. Методические рекомендации по выполнению законодательных требований при обработке персональных данных в организациях банковской системы Российской Федерации" (утв. Банком России, АРБ, Ассоциацией региональных банков России (Ассоциация "Россия" 31 октября 2018 г.) [Электронный ресурс]. URL: http://legalacts.ru/doc/metodicheskie-rekomendatsii-po-vypolneniiu-zakonodatelnykh-trebovanii-pri/ (дата обращения 06.11.2018).

7. Портал персональных данных Уполномоченного органа по защите персональных данных: ПАО Сбербанк. [Электронный ресурс]. URL: http://pd.rkn.gov.ru/operators-registry/operators-list/?rid&id=11-0187199 (дата обращения 13.11.2018).
8. Политика обработки персональных данных в ПАО Сбербанк (с учетом изменений №1 от 17.11.2016, №2 от 04.07.2017, № 3 от 28.12.2017). [Электронный ресурс]. URL: https://www.sberbank.ru/common/img/uploaded/files/pdf/normative_docs/ politika_obrabotki_pd.pdf (дата обращения 13.11.2018).
9. Валуйских С. Второй SOC Сбербанка. Тюнинг или новая модель?// «BIS Journal – Информационная безопасность банков» №3(30), 2018. [Электронный ресурс]. URL: https://journal.ib-bank.ru/post/689 (дата обращения 13.11.2018).
10. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения [Электронный ресурс]. URL: https://www.cbr.ru/Content/Document/File/46921/st-10-14.pdf (дата обращения 13.11.2018).
11. Стратегия развития Сбербанка 2020 [Электронный ресурс]. – Режим доступа:https://www.sberbank.ru/common/img/uploaded/files/sberbankdevelopmentstrategyfor2018-2020.pdf (дата обращения 14.11.2018).

2.6. Выбор структуры предложения защищенных облачных сервисов в условиях неопределенности спроса

В Правительственных программах развития цифровой экономики Российской Федерации важная роль отводится использованию облачных сервисов [1].

Облачные услуги стали одной из самых динамично растущих областей ИТ-рынка России. Доля облачной инфраструктуры в крупных компаниях приближается к 60%, а у компаний малого и среднего бизнеса порядка 50% инфраструктуры уже находятся вне офиса [2, 3].

Номенклатура предлагаемых облачных сервисов обширна [4]. К числу наиболее популярных сервисов относятся:

- сдача в аренду виртуальных серверов и виртуальных центров обработки данных;
- размещение серверов в облачном дата-центре;
- создание гибридных облачных сегментов и широких пулов ресурсов для обработки задач с пиками вычислительных нагрузок, характерных для заказчиков из ритейла или банковского сектора;
- облачное хранилище;
- облачная база данных;
- различные платформы;
- организация виртуальных рабочих мест;
- решения для потоковой обработки данных;
- резервное копирование;
- корпоративная почта;

- сервисы технической поддержки;
- сервисы управления инфраструктурой;
- сервисы информационной безопасности и защиты данных;
- сервисы передачи данных и электронного документооборота;
- управление взаимоотношениями с клиентами.

Список облачных провайдеров в России насчитывает несколько десятков компаний [2, 3].

Ограниченность ресурсов компании-поставщика облачных сервисов проявляется через ограничение номенклатуры предлагаемых сервисов. При этом по каждой позиции номенклатуры ограничивается предельное количество выполнения возможных заказов.

Относительное количество возможных заказов по каждой позиции номенклатуры представляет собой структуру предложения облачных сервисов.

Компания-поставщик стремится к соответствию структуры своего предложения структуре спроса. Чем больше это соответствие, тем больше заключается договоров на предоставление облачных сервисов и больше выручка компании. Однако по ряду причин в краткосрочном периоде работы компании спрос носит неопределенный характер.

К факторам неопределенности спроса на облачные сервисы относятся:

- наличие потребности в функциональности сервиса;
- качество облачного сервиса;
- ценовая политика производителя на рынке облачных сервисов;
- обеспечение информационной безопасности при использовании облачных сервисов, то есть защищенность сервисов;
- реклама;
- качество технической поддержки;
- степень доступности;
- уровень быстродействия;
- государственная политика в области импортозамещения программных продуктов и облачных сервисов.

В связи с неопределенностью спроса перед компанией возникает задача выбора такой структуры предложения, которая обеспечивает гарантированную максимальную выручку.

Очевидно, что в долгосрочной перспективе с учетом появляющейся статистики заказов структура предложения должна уточняться.

При наличии статистических данных прогнозирование спроса на продукцию основывается обычно на известных методах временных рядов или корреляционно-регрессионного анализа [5, 6]. Однако в условиях отсутствия статистических данных, то есть в условиях неопределенности спроса, приходится использовать менее точные экспертные методы [7],

методы нечеткой логики [8] или же методы, основанные на решении матричных игровых моделей [9, 10].

Одним из подходов к обоснованию структуры предложения, обеспечивающим гарантированную максимальную выручку прибыли является подход, основанный на матричных игровых моделях.

Рассмотрим этот подход на примере выбора структуры предложения, максимизирующий гарантированную прибыль компании-поставщика защищенных облачных сервисов. При построении и исследовании модели должны быть решены следующие задачи [11].

1. Сформулирована цель.

Целью моделирования является получение максимальной гарантированной выручки поставщика сервисов предприятием в условиях неопределенности спроса. Поскольку требуется максимизировать объем выручки компании при самом неблагоприятном спросе, то данную игру можно рассматривать как антагонистическую.

2. Определены игроки.

Игроками являются: компания − поставщик облачных сервисов (игрок 1) и покупатель на рынке облачных сервисных услуг (игрок 2).

3. Установлен перечень стратегий.

Перечень стратегий соответствует номенклатуре продукции.

4. Построена матрица выигрышей.

Это квадратная матрица, имеющая следующий вид (рис. 2.12).

$$Q = \begin{bmatrix} q_{11} & q_{12} & \cdots & \cdots & \cdots & q_{1I} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ q_{i1} & q_{i2} & \cdots & q_{ij} & \cdots & q_{iI} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ q_{I1} & q_{I2} & \cdots & \cdots & \cdots & q_{II} \end{bmatrix}$$

Рисунок 2.12. Матрица выигрышей

В матрице выигрышей q_{ij} − выручка соответственно при продаже сервиса *i-го* наименования или издержки при несовпадении спроса и предложения. I − множество наименований предлагаемых сервисов.

5. Дана интерпретация экономического содержания процесса игры.

Процесс игры сводится к тому, что первый игрок выбирает i-ую стратегию, т.е. *i-ую* строку матрицы. Этот выбор означает, что первый игрок предлагает на рынок одну единицу сервиса i-го наименования. Второй игрок выбирает j-ый столбец, что означает, что покупатель готов купить одну единицу сервиса j-го наименования. Если $i = j$, то предложение соответствует спросу и сервис продается. Если $i \neq j$, то сервис не продается.

Следует заметить, что согласно постановке задачи матричной игровой модели спрос, на облачные сервисы ведет себя в установленных ограничениях, а именно:

- Номенклатура спроса соответствует номенклатуре предложения. То есть второй игрок заказывает сервисы из предлагаемой поставщиком номенклатуры.
- Суммарное количество сервисов, которое запрашивается в период игры в точности равно тому количеству сервиса, которое предлагается. То есть на один ход первого игрока следуют один ход второго игрока за период игры.

Компания-поставщик облачных сервисов осуществляет все свои ходы в начале игры. Потребитель сервисов осуществляет свои ходы постепенно в процессе игры. Количество ходов потребителя монотонно возрастает и в определенный момент времени достигает количества ходов поставщика сервисов, сделанных заранее. Этот момент времени является завершением периода игры. При этом на один ход поставщика приходится один ход потребителя.

Результат игры за период может быть оценен с помощью матричной игровой модели.

При оптимальном выборе смешанной стратегии ходов поставщик сервисов получает максимальную гарантированную выручку от продажи сервисов. Следует заметить, что она равняется минимальным необходимым затратам потребителя сервисов.

6. Предложен порядок расчета элементов матрицы выигрышей.

$$\text{При } i = j \quad q_{ij} = ц_i ,$$

где $ц_i$ − цена при продаже единицы сервиса *i-го* наименования.

$$\text{При } i \neq j \quad q_{ij} = c_i ,$$

где c_i − издержки, связанные с тем, что единица *i*-го сервиса не была продана. В этом случае матрица выигрышей приобретает следующий вид (рис. 2.13).

$$Ц = \begin{bmatrix} ц_1 & -c_1 & -c_1 & -c_1 & -c_1 \\ -c_2 & ц_2 & -c_2 & -c_2 & -c_2 \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ -c_I & -c_I & -c_I & -c_I & ц_I \end{bmatrix}$$

Рисунок 2.13. Матрица выигрышей с конкретизацией значений элементов, отражающих выручку или издержки в расчете на один экземпляр сервиса

Рассмотрим порядок расчета элементов матрицы.

Выручка от одиночной продажи *i-го* сервиса (цена *i-го* сервиса), может быть определена в соответствии с формулой:

$$ц_i = \frac{S_i}{N_i} + c_{уд.\ i} + p_i,$$

где S_i − совокупная стоимость владения *i-м* сервисом без учета переменных затрат, то есть затрат, зависящих от количества проданных сервисов;

N_i − ожидаемое суммарное количество продажи *i-го* сервиса в течение срока службы *i-го* сервиса (в долгосрочной перспективе), определяемое экспертным путем;

$c_{уд.\ i}$ − удельные затраты, связанные с продажей одного экземпляра *i-го* сервиса;

p_i − прибыль в составе цены однократной продажи экземпляра *i-го* сервиса.

Совокупная стоимость владения определяется по формуле [3]:

$$S_i = K_i + c_{пост.\ i}T$$

где K_i − капитальные (единовременные) затраты на создание *i-го* сервиса;

$c_{пост.\ i}$ − постоянные годовые эксплуатационные затраты на поддержание *i-го* сервиса в работоспособном состоянии, не зависящие от количества продаж сервиса;

T − предполагаемый срок службы сервиса в долгосрочной перспективе (в годах), ограниченный его моральным износом и зависящий от стратегии развития компании.

Потери компании при несовпадении предложения и спроса на *i-ый* сервис в расчете на один заказ любого сервиса, кроме *i-го,* составляет величину:

$$c_i = \frac{S_i}{N - N_i},$$

где *N* − общее количество экземпляров сервисов по всем наименованиям, которые предполагается продавать в долгосрочной перспективе.

$$N = \sum_{i \epsilon I} N_i.$$

Определяющим ограничением при выборе структуры предлагаемых сервисов в периоде игры является сумма удельных затрат $c_{уд.i}$ для всех проданных экземпляров сервисов.

Это ограничение имеет вид:

$$\sum_{i \epsilon I} n\, c_{уд.i}\, x_i \leq C_{пер.доп.}$$

где n − предполагаемое плановое суммарное количество сервисов, продаваемых в периоде игры;

x_i − доля экземпляров сервисов *i-го* наименования в общем количестве экземпляров сервисов n, предполагаемых к продаже в периоде игры;

$C_{\text{пер.доп.}}$ − допустимые переменные затраты компании в процессе игры.

Оптимальные значения x_i $(i \epsilon I)$, обеспечивающие гарантированную максимальную выручку компании, находятся на основании алгоритма решения матричной игровой модели.

В соответствии с предлагаемым порядком расчета элементов матрицы приводится пример таблицы выручки при продаже сервиса или издержек в случае несоответствия заказа покупателя предлагаемым сервисам (табл. 2.3).

Таблица 2.3. Пример таблицы выручки или издержек компании-поставщика облачных защищенных сервисов

№ п/п	Наименование сервиса	Единица измерения стоимости сервиса	Средняя стоимость заказа сервиса (ц) (руб.)	Издержки при несовпадении предложения и спроса (с) (руб.)
1	Облачные вычисления (использование виртуальных машин)	руб. / час	730	50
2	Хранение данных	руб. / Тб.	1300	13
3	Базы данных	руб. / час	730	50
4	Передача данных	руб./ Мб.	1	0,1
5	Управление доступом	руб. / пользователь	70	5

При определении значений затрат, присутствующих в приведенных формулах, следует учитывать затраты на обеспечение защищенности предлагаемых компанией сервисов.

Получая в свое распоряжение виртуальную машину в рамках сервиса облачных вычислений, потребитель сервиса имеет всю необходимую инфраструктуру для развертывания служб аутентификации и авторизации доступа внутри нее.

Сервис по хранению данных предоставляется с возможностью шифрации хранимых данных, поддерживаются решения по обеспечению высокой надежности и доступности данных.

Облачные базы данных пользователя имеют встроенные механизмы обеспечения безопасности для доступа к объектам базы данных, а при необходимости может быть обеспечено шифрование содержимого базы

данных как с использованием встроенных механизмов, так и средствами облачной операционной системы.

Передаваемый по сети траффик между структурными элементами распределенного приложения, базой данных может быть зашифрован с использованием штатных средств.

7. Выполнен анализ наличия «седловой точки» и обоснован выбор оптимальной стратегии.

Для установления наличия или отсутствия «седловой точки» требуется установить нижнюю и верхнюю цену игры.

Нижняя цена игры (критерий Вальда) равняется

$$\alpha = \max_i \min_j \left\{ q_{ij} \right\} = \max_i \left\{ -c_i \right\} < 0 .$$

Верхняя цена игры равняется $\beta = \min_j \max_i \left\{ q_{ij} \right\} = \min_j \left\{ u_i \right\} > 0$.

Поскольку $\alpha \neq \beta$, то «седловая точка» отсутствует. В этом случае оптимальная стратегия предполагает использование смешанной стратегии. Цена игры v лежит в пределах $\alpha \leq v \leq \beta$.

Смешанная стратегия игрока 1, то есть выбор структуры предложения, состоит в предложении различных единиц сервисов в определенных долях, пропорциях. Пропорции спроса игрока 2 могут отличаться от пропорции предложения. Смешанная стратегия представляет собой распределение вероятностей на множестве чистых стратегий игрока.

Выбор оптимальной стратегии основан на важнейшей в теории игр теореме: всякое конечная антагонистическая игра имеет хотя бы одну точку равновесия [9]. Это означает, что равновесие в смешанных стратегиях обеспечивает максимальный гарантированный выигрыш 1 игрока (выручку компании-поставщика сервисов), равный минимальным затратам 2 игрока на приобретение сервисов.

Доля предложения сервисов *i-го* наименования составляет величину

$$x_i = \frac{n_i}{\sum_{i \in I} n_i} ,$$

где n_i − количество предлагаемых единиц сервисов *i*-го наименования в периоде игры;

I − множество наименований сервисов, предлагаемых компанией.

Очевидно, что $\sum_{i \in I} x_i = 1$.

Доля или вероятность спроса единицы товара *i-го* наименования обозначим через y_j . Эта величина рассчитывается аналогично, т.е.

$$y_j = \frac{m_j}{\sum_{j \in J} m_j},$$

где m_j – величина спроса на сервисы *j-го* наименования.

J – множество наименований сервисов, запрошенных пользователем, $J \subseteq I$.

Очевидно, что $\sum_{j \in J} y_j = 1$

С учетом значений вероятностей x_i и y_j цена игры равняется:

$$v = \sum_{i \in I} \sum_{j \in J} q_{ij} x_i y_j$$

Как следует из этой формулы, цена игры представляет собой среднюю выручку компании-поставщика сервисов при продаже одного сервиса.

8. Обоснован выбор метода решения игровой задачи.

Имеется возможность сведения поставленной задачи к задаче линейного программирования. Для оптимальной стратегии 1 игрока должны выполняться условия:

$$\sum_{i \in I} x_i = 1$$

$$\sum_{i \in I} q_{ij} x_i \geq v, \ \forall j \in J$$

Обратим внимание, что указанных неравенств столько, сколько позиций в номенклатуре сервисов. Последнее условие говорит о том, что какой бы выбор ни сделал второй игрок, выручка первого игрока не должна быть ниже средней.

Поскольку значение v нам пока не известно, исключим эту величину в явном виде из условий задачи. Для этого введем новые переменные.

$$x_i^H = \frac{x_i}{v}, \ \forall i \in I$$

Тогда модель задачи линейного программирования примет вид:

$$\sum_{i \in I} x_i^H = \frac{1}{v} \to \min$$

$$\sum_{i \in I} q_{ij} x_i^H \geq 1, \quad \forall j \in J$$

$$x_i^H \geq 0, \quad \forall i \in I$$

После решения данной задачи цена игры находится по формуле

$$\nu = \frac{1}{\sum_{i \in I} x_i^H},$$

а доли предложения сервисов каждого наименования − по формуле:

$$x_i = x_i^H \nu, \ \forall i \in I$$

Если первый игрок хочет следовать оптимальной смешанной стратегии, то количество экземпляров, предложенных в процессе игры защищенных облачных сервисов должно быть достаточно велико, чтобы осуществить рекомендуемые пропорции предложения сервисов.

Литература:

1. Программа «Цифровая экономика Российской Федерации», утверждена распоряжением правительства Российской Федерации от 28 июля 2017 г. № 1632-р [Электронный ресурс]. URL http://static.government.ru/media/files/ 9gFM4FHj4PsB79I5v 7yLVuPgu4bvR7M0.pdf (дата обращения: 28.10.2018).
2. Облачные сервисы (рынок России) [Электронный ресурс]. URL: http://www.tadviser.ru/index.php/статья:Облачные_ сервисы_(рынок_России) (дата обращения: 28.10.2018).
3. Сравнение российских операторов предоставляющих облачные услуги [Электронный ресурс]. URL: https://habr.com/post/334044 (дата обращения: 28.10.2018).
4. Андреевский И.Л. Технологии облачных вычислений: учебное пособие. − СПб.: Изд-во СПбГЭУ, 2018. − 79 с.
5. Бережная Е.В., Бережной В.И. Математические методы моделирования экономических систем. − М.: Финансы и статистика, 2001. − 368 с.
6. Куприенко Н.В., Пономарева О.А., Тихонов Д.В. Статистические методы изучения связей. Корреляционно-регрессионный анализ. − СПб.: Изд-во Политехн. ун-та, 2008. − 118 с.
7. Гуцыкова С.В. Метод экспертных оценок. Теория и практика. − Изд-во: Институт психологии РАН, 2011. − 144 с.
8. Корячко В.П., Бакулева М.М., Орешков В.И. Интеллектуальные системы и нечеткая логика: учебник – М.: Изд-во «Курс», 2017. − 352 с.
9. Кузин Б.И., Широкова С.В. Теория игр. Матричные и биматричные игры, их приложения в экономике фирмы. − СПб.: Изд-во Политехн. ун-та, 2005. − 118 с.
10. Шуликовская В.В. Теория игр. − Ижевск: Информационно-издательский центр «БонАнца», 2009. − 304 с.
11. Андреевский И.Л., Соколов Р.В. Информационные системы управления производственной компанией: учебное пособие. − СПб.: СПбГЭУ, 2018. − 157 с.
12. Андреевский И.Л., Соколов Р.В. Проектирование и эксплуатация информационных систем: учебник. − СПб.: СПбГЭУ, 2017. − 422 с.

ГЛАВА 3. ТЕХНОЛОГИИ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

3.1. Применение искусственного интеллекта в системах антивирусной защиты

В последнее время все большее внимание уделяется исследованию возможностей применения методов искусственного интеллекта как для повышения уровня безопасности компьютерных систем, так и для организации хакерских атак. В данной статье сделана попытка разобраться в том, насколько оправдано применение методов искусственного интеллекта в сфере информационной безопасности в настоящее время.

Под искусственным интеллектом обычно понимается возможность системы выполнять некоторые функции, традиционно связанные с человеческим разумом, в частности способность к самообучению, к принятию решений, основанных на изучении ранее полученного опыта.

Нет сомнений, что сфера применения методов искусственного интеллекта будет расширяться. Интересно оценить какие преимущества может обеспечить этот подход в данный момент применительно к информационной безопасности, так как исследования в этой области не закончены и вероятно далеки от своего завершения.

Прежде всего, отметим, что за термином искусственный интеллект стоит несколько разнородных технологий и подходов.

Традиционно к методам искусственного интеллекта относят:

− экспертные системы, основанные на правилах. Такие системы имеют узкую направленность. Перед использованием экспертной системы правила должны быть «извлечены» и сохранены в базе знаний. Процесс извлечения знаний предполагает привлечение наиболее компетентных специалистов в той области, в которой предполагается применять экспертную систему. Эксперты, при помощи специалиста в области разработки экспертных систем, должны сформулировать правила поведения системы на основе собственного опыта;

− эволюционные вычисления. Эти системы охватывают круг теоретических и практических задач, связанных с использованием моделей автономного поведения, а также самосборки, самоконфигурирования и самовосстановления систем, состоящих из множества взаимосвязанных и совместно функционирующих узлов;

− причинно-следственные сети (байесовские сети доверия). Эти сети применяются для моделирования ситуаций, содержащих неопределенность, в которых случайные события соединены причинно-следственными связями. С математической точки зрения байесовская сеть представляет собой графическую модель, где узлы – это события, а дуги – возможные связи между событиями;

− нейронные сети. Это направление искусственного интеллекта связано с моделированием работы человеческого мозга. Исследования работы мозга привели к созданию модели его работы на основе нейронных сетей. Нейронные сети объясняют способность человека к обучению и самообучению. Нейронные сети могут быть успешно смоделированы на современных компьютерах, что позволяет создавать самообучающиеся компьютерные программ;

− системы нечеткой логики. В этих системах моделируется обработка лингвистических переменных, т.е. высказываний на естественном языке. При работе системы используется аппарат алгебры и правила логического вывода, установленные экспертом.

Постоянно возрастающее количество угроз информационной безопасности и связанные с этим потери делают проблему обеспечения информационной безопасности все более актуальной. По данным Национального агентства финансовых исследований (НАФИ) потери российских компаний от кибератак в 2017 году составили около 116 млрд рублей [1]. Использование методов искусственного интеллекта может повысить уровень безопасности информационных систем. Методы искусственного интеллекта могут использоваться для быстрого обнаружения угроз, что повышает защищенность информационной системы. Большое значение при этом имеет возможность систем искусственного интеллекта к самообучению.

Можно выделить следующие основные сферы применения методов искусственного интеллекта в области информационной безопасности [2]:

- быстрое распознавание угроз;
- оптимизация процесса поиска вредоносных источников;
- анализ поведения системы и выявление на основе этого анализа скрытых угроз;
- приобретение новых знаний в процессе обучения и построение на их основе более мощной системы защиты;
- борьба с вредоносным программным обеспечением, которое так же может являться самообучающимся;
- обслуживание средств управления идентификацией и аутентификации пользователей и доступом к ресурсам и средств администрирования доступа;
- совершенствование современного антивирусного программного обеспечения.

Остановимся подробнее на методах искусственного интеллекта, применяемых в области защиты от вирусов.

Стимулом для применения новых технологий при создании антивирусов является наличие ряда недостатков свойственных антивирусному программному обеспечению при традиционном подходе к разработке. Ос-

новными недостатками являются: необходимость частого обновления информационных баз, что обычно требует наличия подключения к интернету, относительно низкое быстродействие, не всегда оперативное реагирование на новые угрозы.

Необходимость обновления баз связана с тем, что вирусы распознаются по сигнатурам. Сигнатурой является часть кода вируса, достаточная для его распознавания и в тоже время уникальная. Она не должна встречаться в других программах, чтобы обеспечить отсутствие ложных срабатываний антивируса. Процесс поиска вредоносных программ сводится к перебору, имеющихся в базе сигнатур, и проверке того, что сигнатура встречается в программном коде.

Это упрощенная схема, часто антивирус должен распаковать код проверяемой программы, который может быть сжат архиватором. Также код может быть зашифрован и обработан обфускатором. Обфускатор – это специальная программа, которая не изменяет функции обрабатываемого кода, но снижает его читаемость после декомпиляции и поиск в нем сигнатур.

Проблемы с производительностью связаны как с ростом базы данных, содержащей сигнатуры вирусов, так и с необходимостью проверки большого числа файлов и фрагментов кода. Особенно это сказывается при оперативной проверке, осуществляемой при получении данных из внешних источников, таких как Интернет или переносные внешние диски. Внесение новых сигнатур выполняется производителями антивирусных средств после того как ими получен и исследован код нового вируса. Это означает, что каждый вирус может успеть инфицировать какое-то количество компьютерных систем. Чтобы повысить оперативность реагирования на новые угрозы разработчики встраивают возможность использования «эвристических методов».

Фактически возможность использования эвристических методов уже можно рассматривать как применение искусственного интеллекта. Так как набор эвристических методов является базой знаний, а их применение − это работа простой экспертной системы, построенной на применении правил. Недостатком применения этого подхода являются:

- необходимость затрат дополнительного времени и других ресурсов,
- не всегда точная диагностика.

При этом если пользователь антивируса использует эвристические методы, то обычно он может настроить работу своего антивируса так, чтобы информация о подозрительных файлах отправлялась разработчикам антивируса для дальнейшего анализа. Эта возможность позволяет повысить скорость реагирования на угрозы безопасности.

Антивирусные средства, основанные на применении машинного обучения, могут работать по иным принципам. Примером может служить

антивирус Cylance Protect американской фирмы Cylance [3]. Компания Cylance была создана в 2012 году как стартап, она владеет сайтом www.cylance.com. Одной из целей, которую поставила перед собой эта компания, является создание антивируса, который будет обнаруживать вирус или другое опасное программное обеспечение до того, как оно успеет нанести хоть какой-то вред. Cylance Protect не использует базы данных сигнатур и эвристические методы. Вместо этого она опирается на математическую модель, которая описывает работу программного обеспечения. На основе статистического анализа характеристик кода, определяются функции программы. Если среди них оказываются небезопасные, то использование программы блокируется. Основной упор делается не на лечение, а на предотвращение атак.

Модель может совершенствоваться, а антивирусное программное обеспечение может самостоятельно обучаться, чтобы приспособится к новым угрозам безопасности. Обновления не требуется выполнять часто, только при изменении математических моделей. Кроме того, в разы снижается нагрузка на системные ресурсы и время проверки не зависит от размера баз сигнатур, которых просто нет [4].

В компьютерных изданиях появлялась информация о разработке антивируса, который использует искусственный интеллект, сотрудниками и студентами Томского университета систем управления и радиоэлектроники (ТУСУР) [5]. Судя по приведенному описанию эта система, подобно Cylance Protect, также не использует сигнатуры и может самообучаться.

Этот проект упоминается на сайте разработчиков антивируса «Доктор Веб», в одном из выпусков информационного бюллетеня «Антивирусная правДА!» [6]. Мнение авторов антивируса о публикациях, об использовании искусственного интеллекта в борьбе с вирусами отрицательное, поскольку многие статьи и заметки пересказывают содержимое друг друга и содержат явные ошибки. Разработчики антивируса «Доктор Веб», судя по этой публикации, пока скептически относятся к возможности создания самообучающихся антивирусных программ, не опирающихся на применение баз данных сигнатур.

Что касается использования методов искусственного интеллекта во вредоносном программном обеспечении, то здесь возможно применение методов машинного обучения при разработке вредоносного кода. Так, в [7] приводятся данные о возможностях применения машинного обучения при выполнении обфускации. При обучении программа вносит небольшие изменения в двоичный код, не меняя его функций, затем проверяет его с помощью антивируса, оценивает результат и повторяет процесс с учетом полученных результатов. Предполагается, что такой подход может помочь обходить и антивирусные системы, которые используют машинное обуче-

ние. Исходный код примера такой программы изменения кода, без изменения его функциональности размещен на GitHub [7].

Также использование машинного обучения может помочь хакерам повысить эффективность подбора паролей и кражи личных данных пользователей сетевых сервисов.

Высказываются опасения относительно возможности появления вредоносных программ со встроенным искусственным интеллектом, хотя возможный механизм их действия не объясняется. Это пока представляется не невозможным, но не особенно нужным.

Литература:

1. Российские компании за год потеряли 116 миллиардов рублей из-за хакеров, 20.12.2007 [Электронный ресурс]. URL: https://ria.ru/economy/20171220/1511313238.html (дата обращения: 28.10.2018).
2. Олейникова Т.В. Применение методов искусственного интеллекта в задачах обеспечения информационной безопасности [Электронный ресурс]. URL: http://dom8a.ru/seminar-ib/05.06.2014/oleinikova/paper.pdf (дата обращения: 28.10.2018).
3. Уэйн Реш. Cylance выпускает продукт будущего для борьбы с вредоносным кодом, 28.04.2015 //ItWeek [Электронный ресурс]. URL: https://www.itweek.ru/security/article/detail.php?ID=174219 (дата обращения: 28.10.2018).
4. Антивирус с искусственным интеллектом не требует обновления баз и не нагружает систему, 14.06.2016 // Открытые системы. Open Systems Publications [Электронный ресурс]. URL: https://www.osp.ru/news/2016/0614/13033043 (дата обращения: 28.10.2018).
5. Антивирус с искусственным интеллектом – выходец из России, 15.08.2016 [Электронный ресурс]. URL: https://neuronus.com/news-tech/1132-antivirus-s-iskusstvennym-intellektom-vykhodets-iz-rossii.html (дата обращения: 28.10.2018).
6. ИИ против антивирусов, 06.09.2017 // Антивирусная правДА! [Электронный ресурс]. URL: https://www.drweb.ru/pravda/issue/?number=390 (дата обращения: 28.10.2018).
7. Георгиев Р. Искусственный интеллект научился писать трояны, невидимые для антивирусов. Платформа в открытом доступе, 02.08.2017 // CNews|безопасность [Электронный ресурс]. URL: http://safe.cnews.ru/news/top/2017-08-02_iskusstvennyj_intellekt_nauchilsya_pisat_troyany (дата обращения: 28.10.2018).

3.2. Анализ эффективности применения технологии Threat Intelligence

Каждые несколько лет в сфере информационной безопасности (ИБ) появляется технология, претендующая или возводимая в ранг панацеи. Такой технологией стала и Threat Intelligence (TI) − исследование угроз. Согласно Google Trends [1, 2], за последние пять лет интерес к этой технологии вырос многократно (рис. 3.1, 3.2).

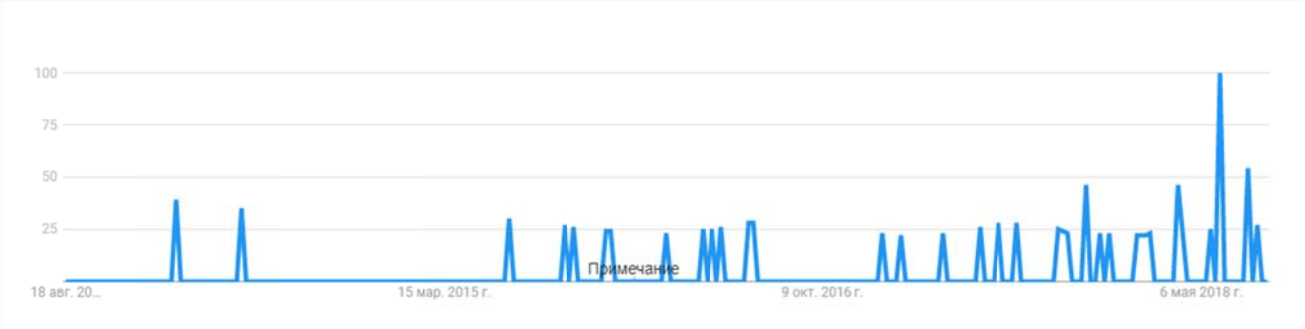


Рисунок 3.1. Динамика роста интереса к технологии Threat Intelligence в России

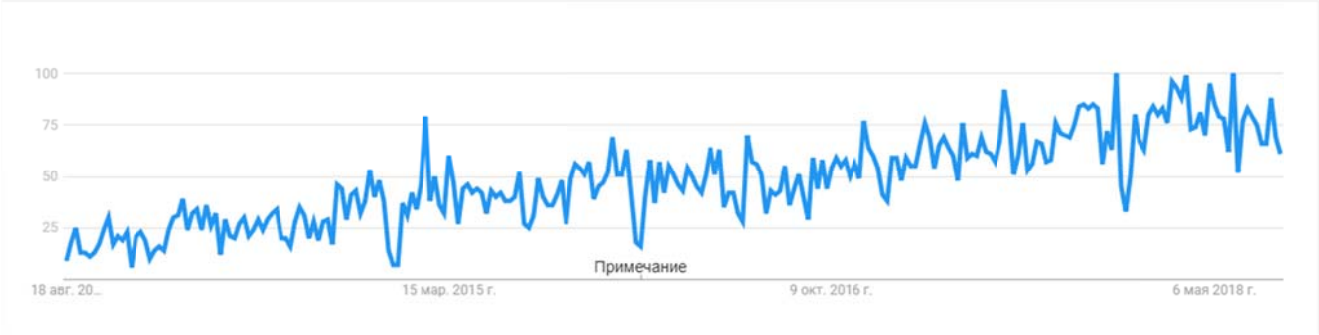


Рисунок 3. 2. Динамика роста интереса к технологии Threat Intelligence в мире

Из данных графика видно, что частота обсуждения данной технологии за последние 6 лет только растет. Рост внимания к Threat Intelligence, прежде всего, обусловлен ростом объема данных по угрозам и уязвимостям, которые уже не успевают и не могут самостоятельно обрабатывать команды аналитиков ИБ. Зачастую в компании просто нет необходимого количества специалистов для выполнения этой задачи.

По данным SANS на 2018 год (по сравнению с 2017) [3] число компаний, создавших свои системы TI, увеличилось на 8%; число компаний, которые используют сторонние данные об угрозах, выросло на 2%, в то время как производящих такие данные самостоятельно уменьшилось на 2%.

Цикл Threat Intelligence

Одним из основных факторов успешного функционирования системы ИБ, а следственно и минимизации рисков, как финансовых, так и репутационных, является своевременное обнаружение и закрытие угроз. Как было отмечено выше, современные решения, применяемые для обмена данными по киберугрозам, не могут обеспечить требуемый уровень работы аналитиков ИБ. Потому возникла необходимость внедрения процесса киберразведки (Threat Intelligence). Сам процесс можно описать следующим циклом (рис. 3.3): планирование – сбор данных – обработка – подготовка – оповещение.

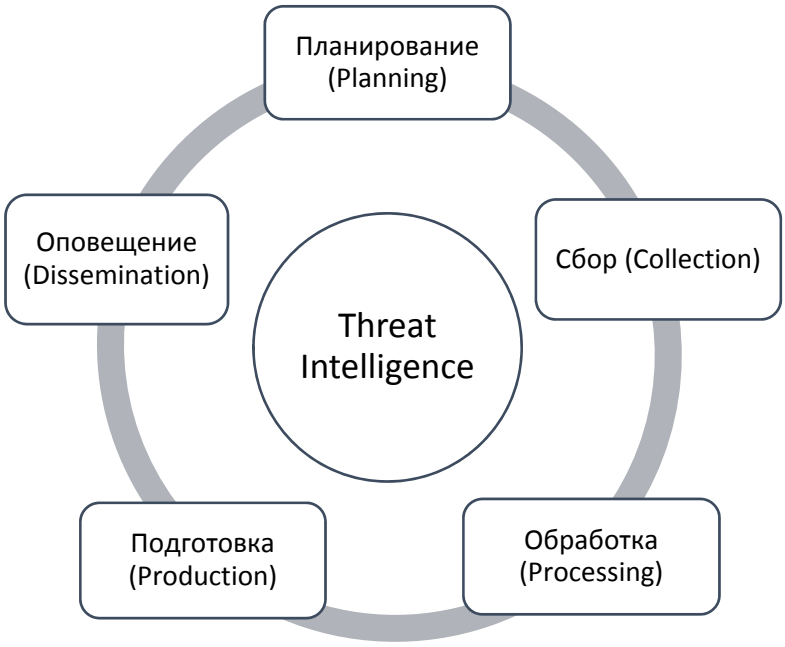


Рисунок 3.3. Цикл Threat Intelligence

1. На этапе планирования устанавливаются цели, требования к получаемой информации. Важно получать только необходимую и достаточную информацию и важно выбрать правильный источник информации.
2. Этап сбора включает в себя различные этапы деятельности по сбору информации для удовлетворения поставленных на первом этапе целей. Кроме собственных источников информации, на этом этапе используются и данные провайдеров Threat Intelligence, таких как Group-IB, Cisco, Palo Alto, ESET, Kaspersky Lab, Check Point и др (рис. 3.4). Для сбора данных об атаках используется множество источников: распределенные сети мониторинга, спам-ловушки, Proxy и VPN-сервисы, общедоступная информация (блоги, СМИ, социальные сети), общедоступные песочницы и др. Помимо этого, аналитики и исследователи собирают информацию из закрытых сообществ и даркнета.
3. На этапе обработки собранные исходные данные интерпретируются, транслируются и унифицируются. Многие компании начинают процесс внедрения киберразведки с использования открытых данных по угрозам из открытых фидов (Threat Intelligence Feeds).

Фиды – потоки данных, содержащие индикаторы компрометации, т.е. признаки, по которым можно распознать потенциальную угрозу, например, хэши вредоносных файлов, IP-адреса и домены или DNS-адреса, URL, CVE-записи, ключи реестра и т. д. Проблема фидов в том, что в них отсутствует контекст. Такие данные сами по себе на дают ответа на ключевые вопросы: какая связь этих индикаторов с конкретными атаками на организации из той или иной отрасли. Единственный способ по-

лучить важный контекст – заниматься анализом и выстраиванием взаимосвязей вручную, либо использовать платные платформы для анализа и обработки данных об угрозах.

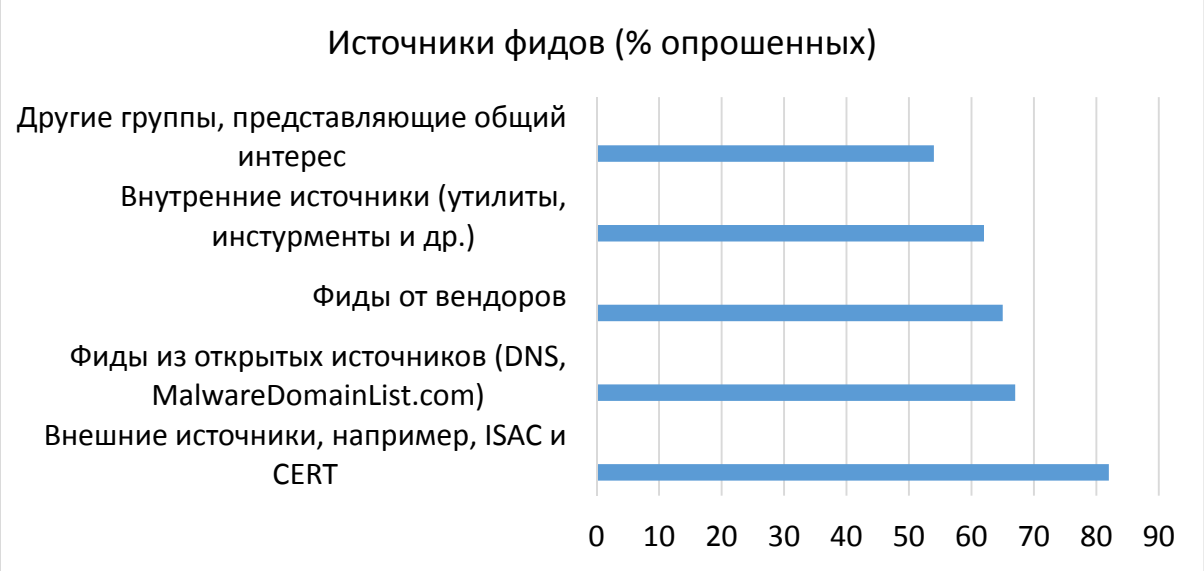


Рисунок 3.4. Источники информации Threat Intelligence

На основе проведенного анализа зависимости конкретных атак от индикаторов (фидов) были получены следующие данные (таблица 3.1).

Таблица 3.1. Примеры индикаторов компрометации

Категория	Индикатор компрометации	Пример
Сеть	- IP адрес - URLs - Доменные имена	Заражение вредоносными программами внутренних узлов, взаимодействующих с известными серверами злоумышленников
Почта	- Адрес почты нарушителя - Приложения к письму - Ссылки	Фишинг, когда пользователи, ничего не подозревая, нажимают на все что есть в письме, тем самым открывая для нарушителя двери во внутреннюю сеть
Конечные устройства	- Имена файлов и их хэши (SHA-1, MD5 и др.) - Ключи реестра - DLL	Атаки, проводимые зараженными хостами

4. Этап подготовки данных включает в себя процесс уточнения и слияния информации, обработанной на предыдущем этапе.
5. Заключающим этапом цикла становится распространение информации конечным потребителям. Это могут быть как собственные под-

разделения, так и другие компании. Так, согласно Указу Президента Российской Федерации от 15 января 2013 г. № 31, одной из основных задач государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) является «обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак». FinCERT Банка России обязан поддерживать обратную связь с клиентами с целью оповещения об угрозах информационной безопасности и рекомендациях по их устранению.

Проблема этого уровня заключается в отсутствии стандартов представления собранной информации. Российские поставщики Threat Intelligence используют стандарты STIX (Structured Threat Information eXpression) (https://stixproject.github.io) и TAXII (Trusted Automated eXchange of Indicator Information) (https://taxiiproject.github.io). Также рекомендуется [4] использовать CIF (Collective Intelligence Framework) (https://csirtgadgets.com/collective-intelligence-framework/), т.к. в России существует опыт эксплуатации данного стандарта, а также возможность интеграции CIF под нужды организации, например, генерация правил для Snort, Suricata и других средств защиты информации.

Эффективность применения технологии Threat Intelligence

Внедрение технологии Threat Intelligence позволяет организациям повысить уровень ИБ, не только создав систему в реальном времени, занимающуюся обработкой информации по угрозам и рискам, но и увеличивает КПД группы аналитиков ИБ, т.к. снижает на них нагрузку.

По данным SANS [3], 42 % опрошенных заявили, что имеют команду, занимающуюся TI, 12 % имеют хотя бы одного человека, ответственного за TI и 31 % респондентов сказали, что обязанности по TI распределены по разным группам (рис. 3.5). Эти данные в среднем выше, чем данные за 2017 год, что показывает положительную динамику развития TI. Чаще всего использующиеся для обнаружения угроз и атак технологии TI приведены на рис. 3.6.

Высокий процент обнаружения угроз и атак при использовании технологии TI закономерен, т.к. анализ угроз играет ключевую роль в дополнении и улучшении правил брандмауэра, списков контроля доступа к сети (ACL (Access Control List)) и списков репутации ресурсов. Также это позволяет быстро определить вредоносные ресурсы и заблокировать к ним доступ.

Рисунок 3.5. Распределение наличия персонала, ответственного за TI (данные на 2018 г.)

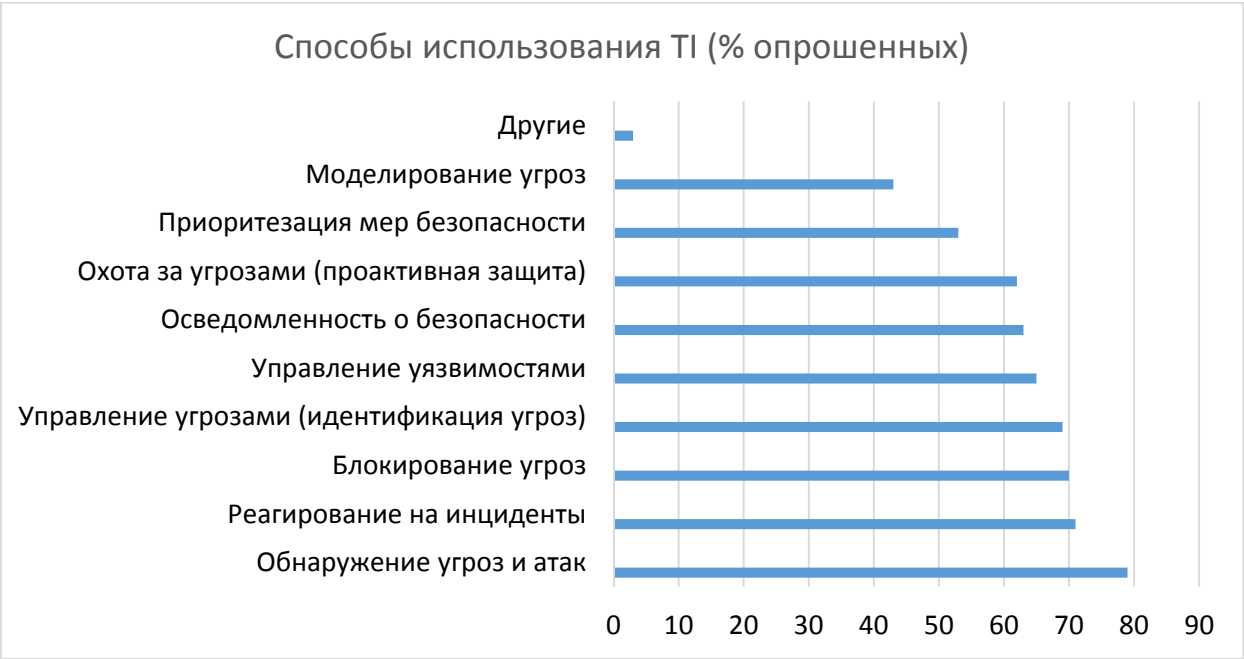


Рисунок 3.6. Способы использования TI

Чаще всего команды ИБ организаций, в которых используется TI, смотрят на индикаторы вредоносного ПО или ресурса, затем на информацию об уязвимостях, которые могут использовать злоумышленники.

Исходя из этого следует заключить, что организации ищут все более конкретную информацию о злоумышленниках, инструментах, вредоносном ПО. Крупномасштабная информация интересна и полезна, но технические специалисты и аналитики также нуждаются в конкретных данных, которые они могут немедленно применить к сценариям обнаружения и реагирования на инциденты.

Например, исследователи стараются детализировать следующие данные:

1. Данные полученные из новостей по поводу уязвимостей или ПО.
2. Данные, используемые для межсетевых экранов.
3. Данные по вредоносным ресурсам для создания черных списков и получению статистики по ним.
4. Данные полученные по API в SIEM от вендоров TI по вредоносному ПО.

Наглядный пример можно привести, связанный с вирусом Wannacry, эпидемия которого все еще свежа в памяти. С помощью TI-вендоров можно было вполне без усилий получать список серверов-источников и добавлять их в черный список, что сократило бы шансы заражения в разы.

Рассмотрим системы, в которые интегрируется TI:

1. Платформы SIEM.
2. Инструменты анализа сетевого трафика.
3. Сервера электронной почты.
4. Платформы мониторинга.
5. Платформа для управления угрозами.
6. Сторонние платформы отчетности.
7. Платформы для форензики и др.

Чаще всего интеграция происходит через API, также многие вендоры предлагают интегрировать данные при помощи форматов XML, STIX, CSV и др. Но недостаточно просто внедрить технологию. Для того чтобы она заработала, нужно проанализировать ситуацию и определить возможные угрозы, затем на основе собранных данных предусмотреть меры предосторожности (но это уже вопрос по организации работы SOC (Security operation center)).

На данный момент имеется ряд проблем с анализом огромного потока данных об угрозах, уязвимостях, вредоносных ресурсах и ПО, об атаках и злоумышленниках, но также имеется и реальное решение этой проблемы, которое развивается и с каждым годом все больше захватывает рынок ИБ − Threat Intelligence.

Литература:

1. Threat Intelligence – Анализ – Google Trends [Электронный ресурс]. URL: https://trends.google.ru/trends/ explore?date=today%205-y&geo=RU&q=Threat%20Intelligence (Дата обращения 16.08.2018).

2. Threat Intelligence – Анализ – Google Trends [Электронный ресурс]. URL: https://trends.google.ru/trends/explore?date=today%205-y&q=Threat%20Intelligence. (Дата обращения 16.08.2018).
3. Dave Shackleford. CTI in Security Operations: SANS 2018 Cyber Threat Intelligence Survey, Feb. 2018 [Электронный ресурс]. URL: https://www.sans.org/reading-room/whitepapers/threats/cti-security-operations-2018-cyber-threat-intelligence-survey-38285 (Дата обращения 16.02.2018).
4. Лукацкий А.В. Фиды – это еще не Threat Intelligence [Электронный ресурс]. URL: https://lukatsky.blogspot.com/2018/07/threat-intelligence.html (Дата обращения 12.08.2018).
5. Wang Wei. What is Threat Intelligence and How It Helps to Identify Security Threats [Электронный ресурс]. URL: https://thehackernews.com/2015/11/what-is-cyber-threat-intelligence.html (Дата обращения 02.09.2018).
6. Group-IB. Threat Intelligence. Выявляйте угрозы, утечки, взломы и хакерскую активность до того, как они смогут вам навредить [Электронный ресурс]. URL: https://www.group-ib.ru/intelligence.html (Дата обращения 10.02.2018).
7. Rob McMillan. Definition: Threat Intelligence [Электронный ресурс]. URL: https://www.gartner.com/doc/2487216/definition-threat-intelligence (Дата обращения 19.03.2018).
8. Ed Tittel. Comparing the top threat intelligence services [Электронный ресурс]. URL: https://searchsecurity.techtarget.com/feature/Comparing-the-top-threat-intelligence-services (Дата обращения 19.04.2018).
9. Threat Intelligence // KasperskyLab [Электронный ресурс]. URL: https://media.kaspersky.com/en/business-security/enterprise/ Kaspersky_Threat_Intelligence_Services.pdf. (Дата обращения 29.09.2018).
10. Откуда возникла необходимость в Threat Intelligence, Информзащита, 29.08.2017 [Электронный ресурс]. URL: https://habr.com/company/infosecurity/blog/336676/. (Дата обращения 10.09.2018).

3.3. Анализ криптографических средств операционных систем Windows

Большинство современных компьютерных систем, таких как операционные системы (ОС), web-серверы и СУБД, обладают встроенными средствами криптографической защиты информации (СКЗИ) для обеспечения безопасного хранения и защищенной передачи данных. В качестве примеров подобных средств можно привести функции шифрования файлов и папок Encryption File System (EFS) или средство шифрования диска BitLocker в операционных системах семейства Windows. При этом большинство пользователей уверено, что применяемые средства защиты обладают абсолютной надежностью за счет реализации стойких криптографических алгоритмов, таких как AES или отечественные криптоалгоритмы ГОСТ. Как правило, большое внимание уделяется выбору длины ключа алгоритма шифрования, например, даются рекомендации использовать алгоритм AES с длиной ключа 256 бит (AES-256) вместо AES-128.

Действительно, используемые современные криптографические алгоритмы, такие как AES, 3DES, отечественные ГОСТ Р 34.12–2015 «Кузнечик» и «Магма», обладают достаточной вычислительной стойкостью. Большие длины ключей (от 128 бит) исключают практическую возможность вскрытия методом полного перебора значений ключа. Вместе с тем, успешные атаки на зашифрованную информацию в ряде случаев все же возможны и обусловлены, прежде всего, непониманием особенностей и ограничений, некорректной настройкой или неправильным использованием, а иногда и уязвимостями реализации СКЗИ.

Представляет интерес исследование вопроса практической надежности популярных криптографических средств защиты информации с точки зрения форензики – компьютерной криминалистики, нацеленной на поиск и извлечение информации (доказательств) из компьютерных систем [1].

Требования безопасности приложений приводят к широкому использованию шифрования, которое зачастую осуществляется приложением автоматически, прозрачно для пользователя и не требует, а иногда и не допускает пользовательской настройки параметров. Так, например, популярные браузеры сохраняют данные учетных записей пользователей (логины и пароли) для доступа к сайтам, сессии и файлы cookies, служащие источником личной информации, в зашифрованном виде. Для защиты данных браузеры Chrome и Edge (IE) в операционной системе Windows используют интерфейс DPAPI (Data Protection API), позволяющий реализовать функции шифрования и расшифрования как данных, так и памяти. При этом, как правило, ключ шифрования генерируется на основе пользовательского пароля, используемого для входа в Windows. Механизмы DPAPI не обеспечивают абсолютно надежной защиты, что подтверждается опытом использования криминалистического программного обеспечения, например, Belcasoft Evidence Center [2].

Еще один пример – хранение синхронизированных данных и резервных копий информации с устройств, работающих под управлением операционных систем Android, iOS и Windows 10 в облачных хранилищах: Google Account, iCloud и Microsoft Account соответственно. Полученные с устройства облачные данные в ряде случаев никак не контролируются пользователем и могут содержать пароли, ключи доступа к зашифрованным томам, а также личную информацию (переписку, контакты, данные о звонках, геолокационные данные и прочее). Извлечение таких данных позволяет получить доступ к другим устройствам и хранилищам. Однако сама процедура извлечения данных из облака является нетривиальной, поскольку разработчики используют шифрование, причем некоторые данные, например, пароли в резервных копиях, дополнительно шифруются аппаратным ключом, другие допускают обращения только с доверенного устройства. Вместе с тем, суще-

ствуют криминалистические инструменты, справляющиеся с данной задачей, например, Elcomsoft Cloud Explorer, Elcomsoft Phone Breaker [3].

Для шифрования хранимых данных пользователем могут быть использованы встроенные СКЗИ, доступные в операционных системах Windows [4] и предназначенные для локального шифрования объектов файловой системы (EFS) и дисков (BitLocker, BitLocker Drive Encryption, BitLocker To Go). EFS фактически является надстройкой над файловой системой NTFS, позволяющей обеспечить защиту данных как во время работы ОС, так и в автономном режиме (при прямом физическом доступе к диску, с другого экземпляра ОС). EFS-шифрование прозрачно для пользователя, то есть при чтении файла данные автоматически расшифровываются, а при записи снова зашифровываются. Другие же пользователи в активной ОС не смогут открыть зашифрованный файл, а при прямом доступе к диску – прочитать его содержимое.

Поддержка EFS встроена в NTFS-драйвер. При обнаружении зашифрованного файла NTFS выполняет встроенные EFS-функции, осуществляющие шифрование и расшифровывание данных по мере обращения к ним (рис. 3.7). NTFS отправляет запросы к EFS-службе через подсистему локальной аутентификации (Local Security Authority Subsystem, LSASS).

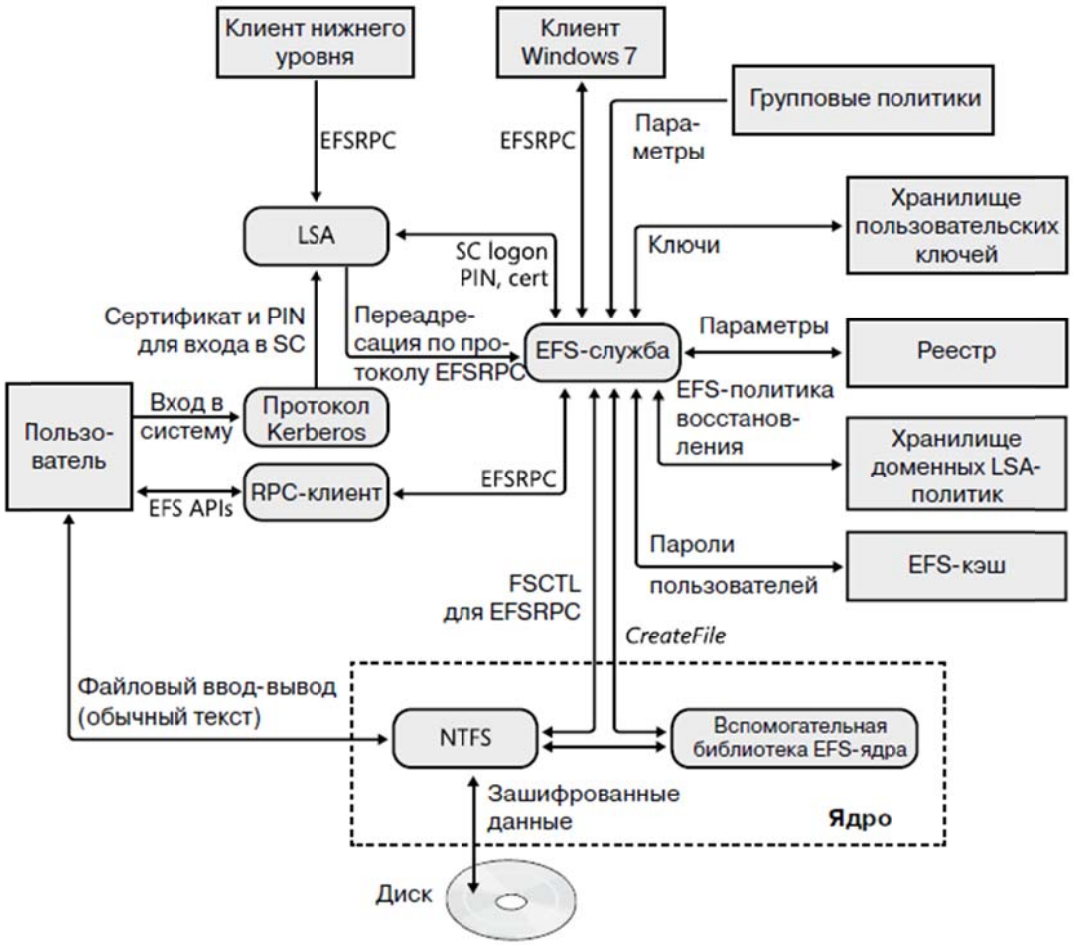


Рисунок 3.7. Архитектура EFS

EFS применяет симметричное шифрование, по умолчанию используется AES-256. Затем к ключу симметричного шифра применяется ассиметричное шифрование (RSA-2048). Начиная с Windows7 EFS наряду с RSA поддерживает использование шифрования на эллиптических кривых (для соответствия требованиям к криптосистемам для гос. учреждений США – Suite B). Для работы с EFS применяется API-интерфейс CNG (Cryptography Next Generation), соответственно, существует возможность воспользоваться любым криптографическим алгоритмом, поддерживаемым CSP, поставляемыми вместе с операционной системой, или сторонним криптопровайдером. Это означает, что EFS может использовать для шифрования локальных файлов и папок отечественные криптоалгоритмы (при установке поддерживающего криптопровайдера и расширения в систему и наличия соответствующего сертификата, например, КриптоПро CSP и КриптоПро EFS [5, С.72-79]).

Процесс шифрования выполняется следующим образом:

1. EFS-служба открывает файл для монопольного доступа.
2. Все потоки данных в файле копируются во временный текстовый файл, расположенный в системной папке.
3. Локальная подсистема безопасности LSA (Local Security Authority) генерирует случайное число – секретный ключ шифрования файла FEK (File Encryption Key), используемого для зашифровывания содержимого файла с помощью симметричного алгоритма.
4. Тот же секретный ключ потребуется и в процессе расшифровывания файла, поэтому ключ должен быть сохранен надежным способом (рис. 3.8). Для этих целей LSA выбирает открытый ключ сертификата пользователя и шифрует ключ FEK ассиметричным алгоритмом с использованием открытого ключа сертификата. Затем зашифрованный ключ записывается в специальное поле (Data Decryption Field, DDF) файла.

В качестве источника открытого ключа может быть административно указан сертификат формата X.509, который затем будет добавлен в хранилище сертификатов пользователя, смарт-карта (USB Token) или генератор случайных чисел. Если пользователю предварительно не был назначен подходящий сертификат и не используется центр сертификации (Certification Authority, CA) в домене, то локальная машина сгенерирует самоподписанный сертификат. Если в дальнейшем пользователю будет выдан EFS-сертификат (например, с помощью CA), шифрование все равно будет использовать созданный ранее самоподписанный сертификат. Этот сертификат не отображается в списке личных сертификатов, поэтому удалить его из системы через диспетчер сертификатов проблематично, но можно до начала шифрования EFS запретить использование самоподписанных сертификатов с помощью политики безопасности (на уровне домена).

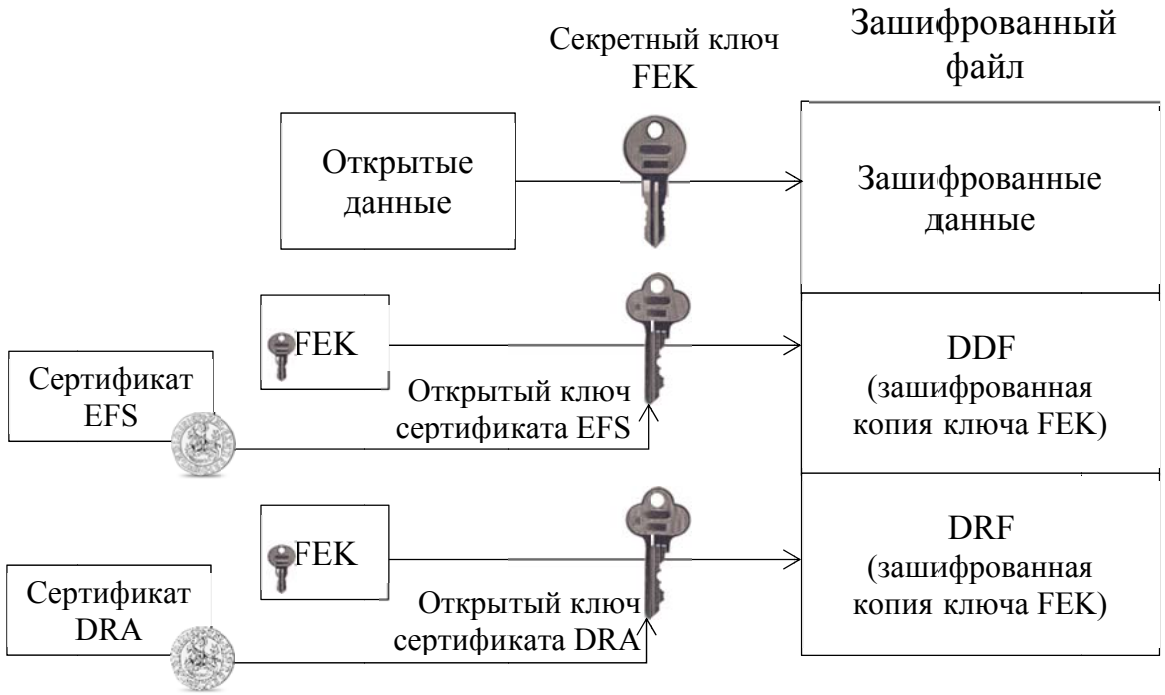


Рис. 3.8. Хранение секретного ключа шифрования EFS

5. Ключ FEK шифруется открытым ключом сертификата агента восстановления (Data Recovery Agent, DRA), который назначен локальной либо групповой политикой безопасности. Если политикой назначено несколько агентов восстановления, копия FEK шифруется с помощью открытого ключа каждого из них, после чего записывается в поле DRF (Data Recovery Field).

Чтобы воспользоваться зашифрованной копией ключа FEK потребуется закрытый ключ соответствующего сертификата. Таким образом гарантируется, что доступ к файлу получит только сам пользователь (владелец закрытого ключа EFS) или агенты восстановления.

6. Для полей DDF и DRF рассчитывается контрольная сумма (хэш-код), которая записывается в заголовок EFS-данных. При расшифровании она позволяет проверить целостность хранимых элементов ключей.
7. Зашифрованные данные (вместе с DDF и DRF) записывает обратно в файл.
8. Временный текстовый файл удаляется.

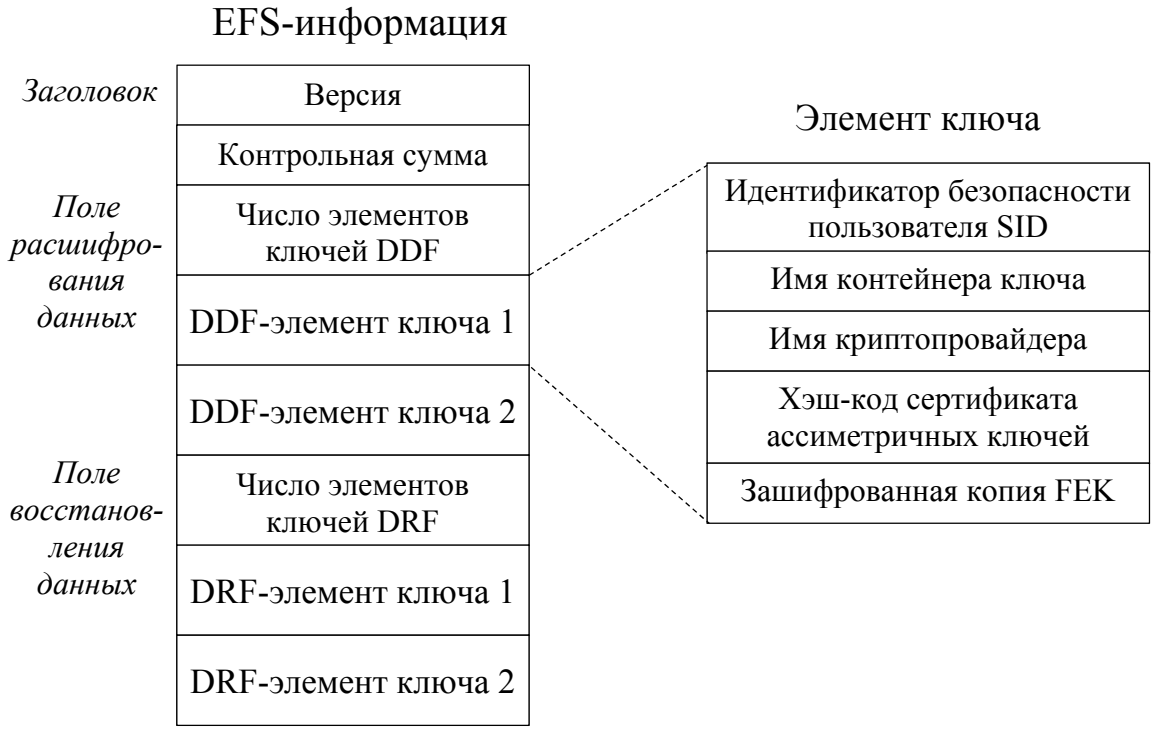
Начиная с Windows Server 2003, появилась возможность предоставлять локальные зашифрованные файлы в общий доступ с другими пользователями. При этом ключ FEK шифруется открытыми ключами сертификатов тех пользователей, которым разрешен доступ к зашифрованному файлу; сертификаты должны быть установлены на компьютере, на котором производится шифрование. Зашифрованный файл может быть предоставлен в общий доступ пользователям, но не группам, по-

скольку группы не могут иметь сертификатов. Предоставить файл в общий доступ может только тот, кто его зашифровал или агенты восстановления.

Записи обо всех имеющих доступ к файлу пользователях – совокупность элементов ключей (key entries) или связка ключей (key ring) − сохраняется в блоке DDF. Форматы EFS-данных файла и элементов ключа пеоказаны на рис. 3.9, элементы ключей DDF- и DRF- имеют единый формат.

Чтобы не допустить потенциальной кражи ключей, закрытый ключ асимметричного шифрования (сертификата EFS, агента восстановления) хранится в системе в зашифрованном виде. Шифрование закрытого ключа производится с помощью хэш-кода, полученного на основе пароля соответствующего пользователя. В свою очередь, хэш-коды паролей хранятся в системной базе пользователей, которая защищена при помощи ключа SYSKEY. Таким образом, надежность защита файла в конечном итоге определяется надежностью пользовательского пароля.

Для повышения надежности рекомендуется хранить контейнеры закрытого ключа на защищенных носителях, таких как смарт-карта или USB-токен. Сертификат может быть перенесен на защищенный носитель сразу же в процессе его создания. При отчуждении сертификата из системы доступ к зашифрованным данным становится невозможным даже в том случае, если был получен доступ к профилю пользователя.



Риснок 3.9. Формат EFS-информации и элементов ключа в зашифрованном файле

Доступ к данным, которые были зашифрованы пользователем, будет утрачен им и в случае сброса пароля пользователя. При плановой смене пароля (по сроку изменения пароля заданного в групповых политиках) или внеплановой смене с указанием предыдущего значения пароля, ключи шифрования обновляются (расшифровываются старым паролем и шифруются новым), и после смены пароля доступ к зашифрованным файлам не прекращается.

Доступ к зашифрованным EFS данным пропадает, если утрачена связь ОС с имеющимися физически на диске ключами. Существуют следующие типовые случаи, приводящие к потере доступа к зашифрованным файлам:

1. Система не загружается из-за смены или поломки комплектующих компьютера или нарушения работоспособности ОС (вышла из строя материнская плата, поврежден загрузочный сектор, испорчены системные файлы и т.п.).

2. Переустановка системы. Если имеется резервная копия системного диска, или профиля пользователя, доступ к зашифрованным данным может быть восстановлен с помощью специального программного обеспечения, но только в случае сохранности ключей.

3. Сброс пароля пользователя системным администратором или самим пользователем.

4. Удаление профиля пользователя.

5. Пользователь перенесен в другой домен (происходит его авторизация через другой сервер). Если при переносе сертификаты ключей хранились на сервере, то возможна потеря доступа к зашифрованным данным.

На случай физического удаления ключей с диска рекомендуется создать резервные копии сертификатов EFS/агента восстановления, содержащие закрытые ключи. Такие копии должны быть надежно защищены от кражи. Контейнер закрытого ключа защищается паролем, он должен быть сохранен на внешнем носителе, а физический доступ к последнему – ограничен.

Имея в своем распоряжении копию сертификата ключа, сотрудник, например, уезжая в отпуск, может удалить закрытый ключ из системы и предотвратить таким образом просмотр своих данных. После обратного импорта сертификата с закрытым ключом в систему доступ к зашифрованным файлам восстанавливается.

Вместе с тем, даже имея резервную копию ключа, не всегда можно восстановить доступ к данным. Например, если профиль пользователя был удален, то новый пользователь будет иметь другой SID, и связать импортированный сертификат ключа с новым пользователем будет невозможно. Если сертификаты ключей не были удалены с диска, для вос-

становления доступа к утраченным данным может быть использована утилита Advanced EFS Data Recovery от компании Elcomsoft, в процессе работы утилиты может потребоваться ввод параметров учетной записи пользователя – логина и пароля, от лица которого были зашифрованы файлы.

Таким образом, EFS шифрование является достаточно гибким и надежным средством защиты локально хранимых данных (при использовании надежных пользовательских паролей или аутентификации со смарт-картой/USB-токеном). Несомненными достоинствами EFS шифрования являются его прозрачность для пользователя, возможность поддержки российской криптографии, возможность управления на уровне домена, обеспечение защиты как при активной ОС, так в случае прямого доступа к диску.

Вместе с тем, EFS имеет существенные ограничения: не могут быть зашифрованы данные на разделе, отличном от NTFS (например, при копировании файла на флэш-накопитель с файловой системой FAT/ExFAT), не подлежат шифрованию системные файлы и области, что оставляет уязвимыми критичные данные ОС (такие, как реестр). Например, если разрешена авторизация доменного пользователя даже без подсоединения к домену, то средства проверки учетных данных в домене кэшируются в реестр компьютера. Поскольку эти данные не зашифрованы, нарушитель с помощью специальных инструментов сможет их извлечь и получить хэш-код пароля доменной учетной записи, что позволит ему производить офлайновую атаку на пароль при помощи взломщика паролей.

Для защиты от автономных атак Microsoft предлагает использовать шифрование на уровне тома с помощью инструмента BitLocker, доступного в версиях Windows Server и десктопных версиях Enterprise и Ultimate. Для съемных носителей (томов с файловой системой, отличной от NTFS) используется технология BitLocker To Go. BitLocker ориентирован, прежде всего, на совместное использование с аппаратным криптографическим сопроцессором – доверенным платформенным модулем (Trusted Platform Module, TPM) и глубоко привязан к конфигурации компьютера (рис. 3.10). Из-за импортных ограничений TPM на территории России недоступен, однако возможно использование шифрования BitLocker с ключом запуска, записанным на USB-накопитель.

BitLocker в стандартном режиме позволяет осуществлять полнодисковое шифрование тома NTFS, в том числе и системного тома с операционной системой Windows, а также осуществлять проверку целостности компонентов ранних стадий загрузки и конфигурационных загрузочных данных.

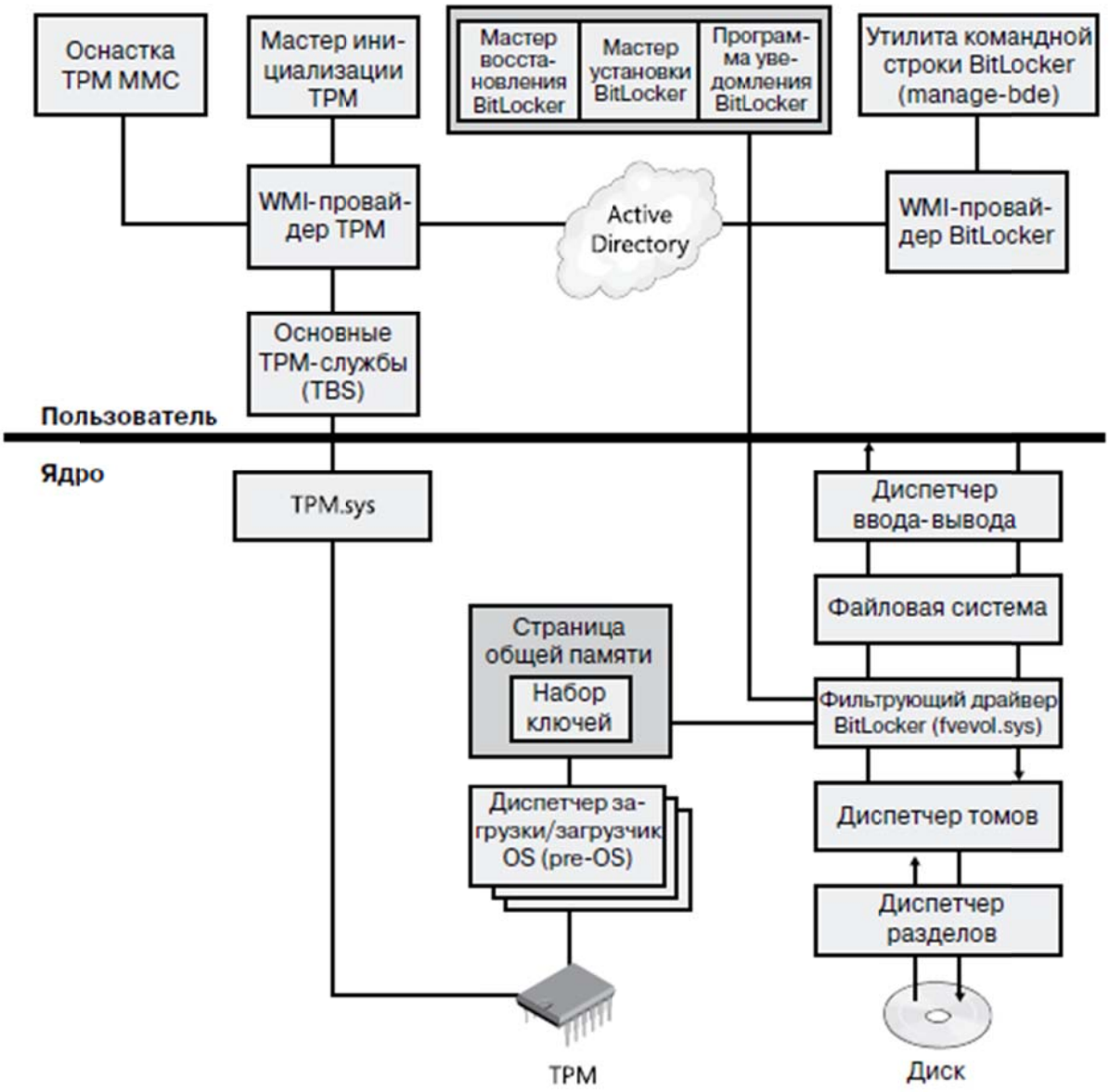


Рис. 3.10. Архитектура BitLocker

BitLocker использует фильтрующий драйвер шифрования всего тома (Full-Volume Encryption, FVE), который автоматически видит все запросы к тому на ввод и вывод, зашифровывая блоки при записи и расшифровывая в процессе чтения. В отличие от EFS, функционирующей на уровне файловой системы, BitLocker работает на уровне подсистемы ввода-вывода, находящейся ниже NTFS (рис. 3.11). Поэтому NTFS «не знает» о включении BitLocker и работает с томом как обычно. Однако при чтении данных с тома при прямом доступе к диску (минуя Windows) они окажутся зашифрованными. Это касается, в том числе, и системных файлов, если включено шифрование системного тома.

Такая низкоуровневая реализация BitLocker не позволяет задавать для шифрования альтернативные алгоритмы, например, определенные российскими криптографическими стандартами.

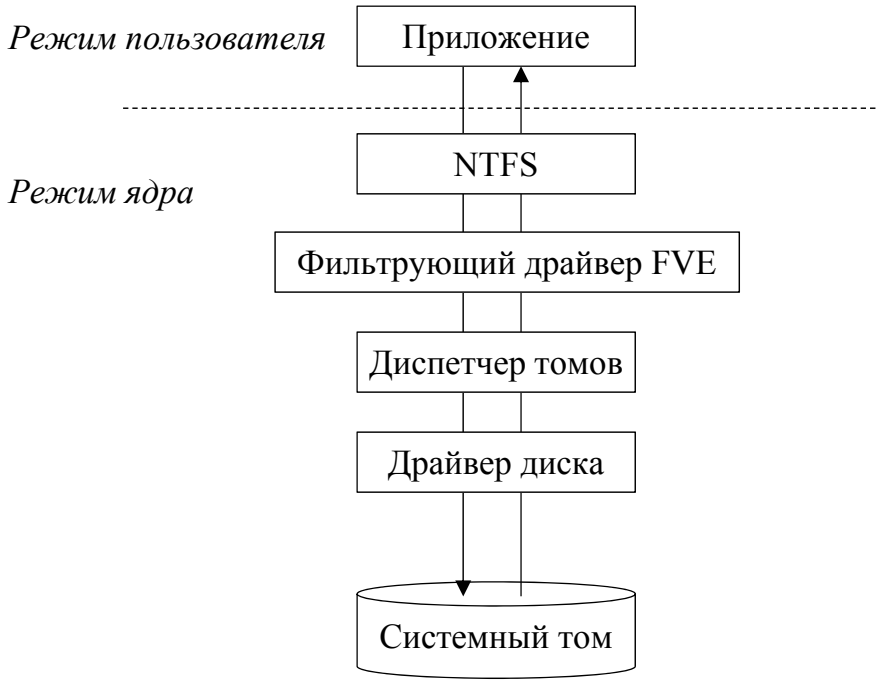


Рис. 3.11. Шифрование BitLocker

BitLocker автоматически шифрует все файлы, добавляемые на зашифрованный диск. Файлы будут зашифрованы только при хранении на зашифрованном диске, при их копировании на другой диск или компьютер они будут расшифрованы. Шифрование дисков BitLocker может использоваться совместно с шифрованием файловой системы EFS.
BitLocker оставляет незашифрованными:

- заголовок тома (совпадает с заголовком загрузочного сектора);
- поврежденные сектора, если они отмечены как нечитаемые;
- метаданные тома (зашифрованный том содержит три блока метаданных, для обеспечения избыточности).

Шифрование содержимого тома осуществляется BitLocker с помощью симметричного алгоритма AES128-CBC (по умолчанию), может быть выбран AES256-CBC с диффузором (Elephant Diffuser – расширение Microsoft) в ОС Windows 7 или AES256-XTS в ОС Windows 10. Поскольку режим CBC потенциально уязвим к атакам при известном изменении части шифруемого содержимого (то есть при изменении части содержимого тома, что является обычной ситуацией), рекомендуется менять установленный по умолчанию режим шифрования с помощью соответствующей политики безопасности. При шифровании используемый ключ FVEK (Full-Volume Encryption Key, ключ полнодиского шифрования всего тома), назначаемый тому в момент включения BitLocker, сохраняется в области метаданных на диске. В случае шифрования с диффузором Elephant Diffuser [6] используется дополнительный ключ TWEAK. До шифрования сектора

на основе TWEAK и содержимого сектора генерируется ключ сектора, который накладывается на исходное содержимое операцией побитового xor, а затем выполняются два бесключевых преобразования-диффузора (многократные повторения комбинации циклического сдвига, побитового xor и сложения по модулю 2^{32}).

Ключ TWEAK записывается в области метаданных сразу после FVEK. Ключи FVEK и TWEAK (если используется) хранятся в зашифрованном виде, для шифрования используется алгоритм AES в режиме CCM (Counter with CBC-MAC) и главный ключ тома (Volume Master Key, VMK). В свою очередь ключ VMK сохраняется на зашифрованном носителе в нескольких экземплярах, которые могут быть зашифрованы ключом восстановления, внешним ключом, пользовательским ключом или с помощью TPM (Trusted Platform Module).

Если TPM не используется, VMK зашифровывается внешним ключом (External Key, Startup key), который сохраняется на USB-накопителе. При защите несистемного тома может быть защищен пользовательский ключ на основе пароля (User key). Во время включения BitLocker кроме того будет создан ключ восстановления (Recovery Key). Обеспечение секретности ключа восстановления и его копий, а также защита ключевого носителя определяют надежность шифрования BitLocker.

Шифрование BitLocker может быть рассмотрено с точки зрения гарантированного уничтожения данных. После удалении ключей шифрования из области метаданных, чтение информации тома станет невозможным.

Шифрование BitLocker рассчитано лишь на автономные атаки при неактивной (выключенной) ОС. После загрузки операционной системы с использованием ключевого носителя (или ключа восстановления) ключи шифрования хранятся в оперативной памяти компьютера в открытом виде. Это значит, что сняв образ оперативной памяти, можно в дальнейшем получить доступ к зашифрованному тому. Следует отметить, что ключи шифрования EFS также могут находиться в оперативной памяти в случае недавнего обращения к зашифрованному файлу, однако здесь для каждого файла использован свой ключ, поэтому здесь компрометация ключа имеет несколько другой масштаб по сравнению с ключами полнодискового шифрования.

Снятие дампа оперативной памяти в ОС Windows не составляет большого труда, если пользователь не использует блокировку компьютера. Для этих целей могут быть использованы как встроенные механизмы самой ОС Windows, так и бесплатные утилиты, такие как Belkasoft Live RAM Capturer [7], или специальный Live-дистрибутив ОС linux (например, Ubuntu CyberPack). Такие средства загружаются в оперативную память атакуемого компьютера и, вообще говоря, изменяют ее содержимое, однако занимают,

как правило, очень немного места, что позволяет их использовать в криминалистической практике. В более сложном случае (если невозможен запуск программного обеспечения на атакуемом компьютере) криминалистами может быть использован метод холодной/горячей перезагрузки или получен непосредственный доступ к памяти с помощью специальных плат расширения, через порт FireWire и другие порты, использующие прямой доступ к памяти (DMA), в крайнем случае, возможно физическое изъятие оперативного запоминающего устройства с замораживанием [8, 9]. После получения снимка оперативной памяти возможно извлечение ключей BitLocker и получение доступа к зашифрованному диску с помощью утилиты Elcomsoft Forensic Disk Decryptor или Passware Kit Forensic [10]. Другой путь получения доступа к данным – использование копий ключей из облачного хранилища учетной записи Microsoft или хранилищ Active Directory, либо сохраненного пользователем ключа восстановления [7].

Дампы оперативной памяти, а также содержание файлов гибернации и подкачки, являются основным источником данных для извлечения паролей и ключевой информации. Анализ «вовремя» снятого образа оперативной памяти позволяет получить необходимые данные для дальнейшего дешифрования пользовательских данных. Подобный анализ и дешифрование могут быть реализованы с помощью таких криминалистических утилит, как Passware Kit Forensic, Elcomsoft Forensic Disk Decryptor (доступ к содержимому дисков, зашифрованных с помощью таких известных утилит, как BitLocker, TrueCrypt, PGP, FileVault 2), Elcomsoft Advanced EFS Data Recovery, Elcomsoft Advanced Office Password Recovery, Elcomsoft Advanced PDF Password Recovery и др.

Для защиты BitLocker и затруднения снятия дампа оперативной памяти следует:

- запретить загрузку ОС с внешнего носителя: USB-устройства и CD (или сделать первым загрузочным устройством жесткий диск), а также установить пароль на изменение настроек BIOS/UEFI;
- использовать режим безопасной загрузки UEFI;
- блокировать компьютер, если он временно не используется (с требованием введения пароля для разблокировки),
- заблокировать FireWire (и другие DMA-порты, если они установлены на компьютере) в BIOS/UEFI, с помощью групповой политики или специализированного программного обеспечения (например, Kaspersky Endpoint Security, DeviceLock и т.п.).

Отметим, что порты прямого доступа к памяти (FireWire, Thunderbolt, ExpressCard и др.) могут оставаться не заблокированными в процессе загрузки Windows в промежуток времени после разблокировки диска BitLocker и до применения связанных с этими портами политик или загрузки утилит контроля портов.

Рассмотрение особенностей шифрования BitLocker позволяет сделать следующие выводы:

- использование средства BitLocker оправдано в том случае, если необходимо обеспечить криптографическую защиту системных файлов (BitLocker должен быть включен на системном томе), либо требуется создать том, при записи на который данные подвергаются автоматическому шифрованию;
- низкоуровневая реализация и глубокая аппаратная привязка BitLocker повышают риски утраты зашифрованных данных в случае изменения или выхода из строя комплектующих компьютера либо нарушения работоспособности ОС;
- снятие шифрования BitLocker не приводит к расшифровыванию содержимого диска, а лишь раскрывает ключи шифрования, при этом процедура не всегда осуществляется корректно (например, может быть запрещена запись на диск);
- если все же принято решение об использовании BitLocker, рекомендуется сочетать его с EFS шифрованием критичных данных, следует придерживаться приведенных выше рекомендаций для защиты ключей BitLocker.

ОС семейства Windows обладают встроенными средствами криптографической защиты, передаваемой по сети – реализацией протоколов IPSec, Kerberos, а также позволяет осуществлять управление цифровыми сертификатами корпоративной сети с помощью серверной службы Certification Authority (CA). Протокол IPSec по умолчанию использует для защиты сетевого трафика 3DES и SHA-1, это наиболее сильные криптографические алгоритмы, поддерживаемые реализацией протокола. Аутентификация сторон выполняется в рамках протокола Kerberos [11, С.264-268], что обеспечивает соблюдение принципа единого входа. В качестве предраспределенного общего секретного ключа используется хэш-код пароля пользователя, первоначальное значение которого задается администратором домена во время регистрации доменного пользователя. В поздних версия ОС протоколом по умолчанию используются криптоалгоритмы AES-256 в режиме CTS (вариант CBC) и HMAC с хэш-функцией SHA-1. При аутентификации пользователя по смарт-карте, первоначальная аутентификация пользователя производится с помощью асимметричной криптографии (алгоритм зависит от используемого сертификата) в рамках расширения PKINIT.

Возможно использование отечественных реализаций протокола IPSec (например, КриптоПро IPSec с криптопровайдером КриптоПро CSP). При этом российская криптография в протоколе Kerberos может использоваться в рамках PKINIT, если имеется соответствующий сертификат пользователя со смарт-картой. Выпуск сертификатов с поддержкой

российских криптографических стандартов доступен при развертывании соответствующего программного обеспечения удостоверяющего центра (например, КриптоПро УЦ), либо с помощью службы CA [5, С.72-79]. Выпуск сертификатов с российской криптографией позволяет соответствующим образом настроить протокол TLS для обеспечения защиты Интернет-соединений (например, для подключения к корпоративному web-серверу по HTTPS).

Практика формирования ключей шифрования на основе пользовательского пароля (как правило, это пароль учетной записи пользователя для входа в ОС), с одной стороны, обеспечивает несомненное удобство работы с сервисами безопасности с соблюдением принципа единого входа, но с другой стороны, может способствовать решению задачи дешифрования. Фактическая безопасность построенных таким образом систем, в конечном счете, определяется надежностью пароля пользователя. Даже если пароль был задан специально, в ряде случаев при известной личной информации он может быть найден с высокой вероятностью, поскольку пользователи, как правило, используют легко запоминаемые, а значит, относительно несложные пароли [12].

Компании, работающие на рынке криминалистического программного обеспечения, предлагают утилиты для подбора паролей, такие, как Passware Kit Forensic, Elcomsoft Distributed Password Recovery. Повышение эффективности перебора достигается распараллеливанием вычислений за счет распределения их между различными устройствами (использование мультиагентных систем), использования мощных вычислительных систем с многоядерными (например, 32-ядерных) центральными процессорами (CPU), активного использования графических процессоров (GPU) видеокарт. Современные графические адаптеры могут иметь до нескольких тысяч процессоров, что позволяет проводить эффективные параллельные вычисления. При этом скорость подбора паролей может существенно варьироваться в зависимости от используемых форматов файлов данных, поскольку некоторые из них требуют значительной предварительной обработки традиционным способом, загружая центральный процессор.

Тем не менее, подбор пароля методом грубой силы практически неосуществим, поскольку функции формирования ключа по паролю используют многократные итерации хэширования с подмешиванием случайных данных, что значительно замедляет вычисление ключа и, как следствие, существенно снижает скорость опробования паролей. Например, процедура вычисления ключа, используемая при парольной защите документов Microsoft Office [5, С.80-81], допускает до 10 млн. итераций хэширования. Словарная атака с использование универсальных словарей, например, орфографического, либо словарей, предоставляемых разработчиками криминалистических средств (тем же Passware), также зачастую оказывается

неэффективной. Однако ситуация не является безвыходной. Решение, как это часто бывает, обусловлено наличием «человеческого фактора».

Как правило, пользователь использует не более трех различных паролей и их незначительные модификации (изменение регистра символов, замена отдельных букв на цифры или символы, добавление цифровой комбинации в начало/конец слова) для доступа к различным ресурсам. Это дает возможность реализации словарной атаки, эффективность которой существенно зависит от релевантности используемого для подбора словаря.

Общие рекомендации для криминалистов состоят в том, чтобы попытаться по возможности извлечь данные из всех устройств и облачных хранилищ, начиная с наиболее доступных, таких как данные браузеров, системные ресурсы (например, реестр Windows), файлы с наименее надежным типом шифрования. Извлеченная информация может быть использована для составления таргетированного словаря, ориентированного на конкретного пользователя. Результаты анализа снимков оперативной памяти, наряду с данными, полученными из хранилищ веб-браузеров и учетных записей почтовых клиентов могут быть использованы для создания такого словаря. Кроме того, извлеченная информация может дать представление о предпочтениях пользователя, в частности, о типе мутаций паролей, которые он, возможно, использовал. Современные средства вскрытия паролей, например, Passware Kit Forensic, Elcomsoft Distributed Password Recovery позволяют задавать определенные мутации при использовании словарной атаки. Подбор пароля с использованием таргетированного словаря, как правило, приводит к успешному вскрытию защищенной информации [13].

Широкая распространенность и доступность современных СКЗИ может создать у неспециалиста ложную уверенность в безопасности защищаемой информации. Использование стойких криптоалгоритмов само по себе не может гарантировать высокую надежность СКЗИ, при этом дополнительная настройка таких средств, включая увеличение длины используемых ключей шифрования, не играет первостепенной роли. Более важным является четкое понимание назначения, особенностей реализации и существующих ограничений того или иного СКЗИ, а также комплексное применение защитных мер и средств (например, обязательное включение блокировки Windows при использовании средства BitLocker). Подобные условия применения СКЗИ могут быть учтены специалистами при разработке политик безопасности. Особо стоит обратить внимание, как ни банально это звучит, на тщательный выбор паролей, в частности, пароля для входа в операционную систему. Альтернативой может служить аппаратная аутентификация с использованием смарт-карт/ USB-токенов с цифровыми сертификатами.

Только комплексный подход и строгое следование политикам безопасности может гарантировать необходимый уровень защищенности данных.

Литература:

1. Васильева И.Н. Вопросы практической надежности криптографических средств защиты информации // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 5 / СПОИСУ. – СПб., 2018. – С. 186-189.
2. Belcasoft. Forensics made easier: [сайт]. URL: https://belkasoft.com/ru/ (дата обращения: 09.11.2018).
3. Перебор паролей, восстановление доступа, расшифровка информации, мобильная криминалистика/ Elcomsoft Co.Ltd.: [сайт]. URL: https://www.elcomsoft.ru/ (дата обращения: 09.11.2018).
4. Руссинович М., Соломон Д., Ионеску А. Внутреннее устройство Microsoft Windows. 6-е изд. Основные подсистемы ОС. – СПб.: Питер, 2014. – 672 с.
5. Защита информации в компьютерных системах: монография; под ред. Е.В. Стельмашонок, И.Н. Васильевой – СПб.: Изд-во СПбГЭУ, 2017. – 163 с.
6. Niels Ferguson. AES-CBC + Elephant diffuser. A Disk Encryption Algorithm for Windows Vista, Microsoft, Aug. 2006 [Электронный ресурс]. URL: https://www.microsoft.com/en-us/download/confirmation.aspx?id=13866 (дата обращения 09.11.2018).
7. Возможен ли взлом Bitlocker? [Электронный ресурс]. URL: http://www.spy-soft.net/vzlom-bitlocker/ (дата обращения: 09.11.2018).
8. Использование метода «холодной» перезагрузки и других криминалистических техник в пентестах, 21.05.2014 [Электронный ресурс]. URL: https://www.security-lab.ru/analytics/452899.php (дата обращения 09.11.2018).
9. Типы атак для ключей шифрования томов, 13.08.2015 [Электронный ресурс]. URL: https://technet.microsoft.com/ru-ru/library/mt404683(v=vs.85).aspx (дата обращения 09.11.2018).
10. Windows Password Recovery tools by Passware: [сайт]. URL: https://www.passware.com (дата обращения: 09.11.2018).
11. Васильева И.Н. Криптографические методы защиты информации : учебник и практикум для академического бакалавриата – М.: Юрайт, 2016. − 349 с.
12. Афонин О. Использование утечек паролей для ускорения атак. 16.02.2017 [Электронный ресурс]. URL: https://blog.elcomsoft.com/ru/2017/02/ispolzovanie-utechek-paroley-dlya-uskoreniya-atak/ (дата обращения: 09.11.2018).
13. Афонин О. Как вскрыть до 70% паролей за несколько минут. 14.02.2017 [Электронный ресурс]. URL: https://blog.elcomsoft.com/ru/2017/02/kak-vskryit-do-70-paroley-za-neskolko-minut/ (дата обращения: 09.11.2018).

3.4. Исследование вопроса обеспечения конфиденциальности и целостности данных применением в базе данных механизма триггеров

Для любой базы данных актуальными остаются угрозы, связанные с потерей конфиденциальности, целостности и доступности данных.

Потеря конфиденциальности возникает в случае получения несанкционированного доступа как к серверу данных, так и к самой базе данных и ее объектам. А несанкционированная модификации объектов базы данных приведет к потери целостности. Отсутствие санкционированного доступа к базе данных указывает на потерю доступности к базе данных.

Современные системы управления базами данных имеют в своем арсенале средства, обеспечивающие реализацию методов защиты баз банных как от несанкционированного доступа, так и обеспечивающие целостность и доступность баз данных. Целью данной работы является исследования возможности применения механизма триггеров для обеспечения конфиденциальности и целостности данных на примере системы управления базами данных Microsoft SQL Server.

Как известно под целостностью базы данных понимается такое состояние базы данных, при котором все хранящиеся данные удовлетворяют заданным ограничениям и подчиняются правилам взаимной непротиворечивости. Большинство ограничений задаются на этапе определения данных и поэтому относятся к декларативным ограничениям целостности данных. В реляционных СУБД декларативными ограничениями являются:

- Ограничение NOT NULL − применяется к столбцу и указывает на недопустимость отсутствия значения в столбце.
- Ограничение DEFAULT – применяется к столбцу и позволяет задать для столбца значение по умолчанию. Ограничение DEFAULT может содержать значения констант, функции или значение NULL, если для столбца не задано ограничение NOT NULL.
- Ограничение уникальности UNIQUE гарантирует, что в определенных столбцах, не участвующих в первичном ключе, не будут встречаться повторяющиеся значения (допускается значение NULL только в одной строке).
- Ограничение PRIMARY KEY − это ограничение, которое гарантирует отсутствие в таблице одинаковых строк. Первичные ключи определяют для обеспечения уникальности значений, вводимых в указанные столбцы, не допускающих значений NULL. В таблице может быть только один первичный ключ.
- Ограничение FOREIGN KEY − это ограничение, которое обеспечивает целостность ссылочных данных. Главная задача ограничения FOREIGN KEY − управление данными, которые могут быть сохранены в таблице внешнего ключа, однако ограничение также контролирует изменение данных в таблице первичного ключа, на которую указывает ссылка. Ограничения FOREIGN KEY могут ссылаться только на таблицы в пределах той же базы данных на том же сервере.
- Ограничение CHECK задает условия для данных, помещаемых в столбец. Столбец может содержать любое количество ограничений CHECK, а условие может включать несколько логических выражений, соединенных операторами AND и OR. При указании нескольких ограничений CHECK для столбца их проверка производится в порядке их создания. Правила и ограничения CHECK выполняют

одну и ту же функцию проверки данных при выполнении команд INSERT и UPDATE.

Однако, вполне возможным является ситуация при которой изменение данных одной таблицы командами INSERT, UPDATE и DELETE может затрагивать данные других таблиц, возможно и не связанных друг с другом. Реализовать такое ограничение рассмотренными выше декларативными ограничениями не возможно. Эти ограничения называются пользовательскими, потому что их логика определяется исходя из алгоритма решения конкретных задач обработки данных (бизнес-логика). В СУБД для определения пользовательских ограничений реализован механизм триггеров.

Триггер − специальный тип хранимой процедуры, которая выполняется автоматически при возникновении события на сервере базы данных. В зависимости от того события, возникновение которого приведет к выполнению триггера различают:

- триггеры DML;
- триггеры DDL;
- триггеры входа.

Триггер DML является хранимой процедурой, выполнение которой осуществляется при изменении таблицы базы данных одной из трех команд модификации данных: UPDATE, INSERT, DELETE.

Эти операции по отношению к триггеру DML называют событиями модификации данных. Триггер DML создается с привязкой к одной таблице, но код триггера может выполнять доступ к данным и других таблиц. Создание триггера DML выполняется командой:

```
CREATE TRIGGER имя_триггера
ON имя_таблицы
{FOR|AFTER|INSTEAD OF}  {INSERT |UPDATE | DELETE}
AS
команды Transact-SQL
```

Могут быть созданы триггеры DML двух типов: AFTER и INSTEAD-OF триггеры.

Для создания AFTER – триггера следует указать параметр AFTER или FOR. Триггеры AFTER выполняются после успешного выполнения действий, обрабатываемых триггером. Триггеры этого типа могут создаваться только для базовых таблиц. И для каждой таблицы можно создавать множество AFTER триггеров для любого из указанных действий UPDATE, INSERT, DELETE, или для нескольких одновременно.

INSTEAD OF-триггер выполняется взамен действий, обрабатываемых триггером. Выполняются команды, указанные в коде триггера, а если действие, активизировавшее триггер должно выполниться, то команду его

выполнения необходимо указать в коде триггера. Для каждой таблицы можно создавать только по одному INSTEAD OF-триггеру для UPDATE, INSERT, DELETE.

Команда и триггер выполняются одной транзакцией. Если команда модификации не может быть выполнена, то триггер не получит управление. Если же команда успешно выполнена, а при выполнении триггера произошла исключительная ситуация, то будет произведен откат транзакции. И только в случае успешного выполнения команды и триггера, результаты транзакции будут зафиксированы в базе данных.

При активизации триггера создают две системные временные таблицы deleted и inserted. Структуры этих таблиц полностью соответствуют структуре таблицы триггера. Таблица *deleted* содержит копии строк, которые удаляются из таблицы. Эта таблица создается в триггерах для команд DELETE или UPDATE. Таблица *inserted* содержит копии строк, добавляемых к таблице триггера командами INSERT или UPDATE. Триггеру для команды UPDATE доступны обе временные таблицы: старые записи копируются в *deleted*, а новые – в *inserted*. Значения таблиц *deleted* и *inserted* доступны только из триггера.

Если для конкретного действия одной и той же таблицы создано несколько триггеров, то встает вопрос о том в каком порядке они будут выполняться. По умолчанию такого порядка не существует. С помощью системной процедуры sp_settriggerorder можно указать триггеры AFTER, срабатывающие первыми или последними. Порядок запуска триггеров AFTER, срабатывающих в промежутке между первым и последним триггерами, не может быть определен.

sp_settriggerorder [@triggername =] 'имя_триггера' , [@order =] 'значение'

Параметр @order может принимать три значения: first, last, none (порядок не определен).

Как уже было сказано выше, INSTEAD OF триггер выполняется вместо действия, обрабатываемого триггером.

Триггеры INSTEAD OF DELETE или UPDATE нельзя определить для таблицы, у которой есть внешний ключ, определенный для каскадного выполнения операции DELETE или UPDATE.

Сведения о триггере, такие как: *тип триггер, имя триггера и его владельца, даты, когда он был создан*. можно получить при помощи представления sys.triggers. Кроме этого можно:

- просмотреть определение триггера, если он не был зашифрован в процессе создания или модификации (представление sys.sql_modules и процедура sp_helptext);

- получить список объектов, используемых указанным триггером. Эти сведения могут быть использованы для выявления объектов, которые воздействуют на триггер, если они изменяются или удаляются из базы данных.

Все вышеизложенное позволяет сделать выводы о целесообразности применения триггеров DML в следующих случаях:

- реализация так называемых бизнес-правил, которые определяют, какие изменения должны осуществляться в таблицах базы данных в ответ на произошедшие изменения в данных базовой таблицы;
- реализация дополнительных ограничений целостности, которым должны удовлетворять данные базовых таблиц или связанные данные, действие которых могут осуществляться в соответствии с определенными условиями (например, действие ограничения в указанный период времени);
- организация контроля выполняющихся изменений в значениях особо контролируемых столбцов таблиц базы данных, и их сохранение для последующего анализа.

Триггеры DDL − это особый вид триггеров, которые запускаются при выполнении команд языка описания данных DDL. Это команды, начинающиеся ключевыми словами CREATE, ALTER или DROP. Также могут запускать триггеры DDL и системные хранимые процедуры, выполняющие операции создания, изменения или удаления объектов.

Триггеры DDL срабатывают только после выполнения соответствующих команд DDL и не могут быть INSTEAD OF триггерами. Команда создания триггера DDL имеет следующий синтаксис:

```
CREATE TRIGGER ИмяТриггера
ON { ALL SERVER | DATABASE }
[ WITH ENCRYPTION ] [EXECUTE AS ИмяВхода ] ]
{ FOR| AFTER } { ИмяСобытия|ИмяГруппыСобытий } [,...n ]
AS  sql_statement  [ ; ] [ ,...n ]
```

При определении триггера DDL необходимо указать:

- область действия триггера (сервер или база данных);
- команду запуска триггера.

Область действия триггера зависит от события. Например, триггер DDL, созданный для событие CREATE TABLE, может срабатывать каждый раз, когда в базе данных или в экземпляре сервера возникает событие CREATE_TABLE. Триггер DDL, созданный для события CREATE_LOGIN, может срабатывать только в случае, если на сервере возникает событие CREATE_LOGIN.

Триггеры DDL сервера являются объектами сервера и доступны, например, в среде администрирования SQL Server Management Studio в папке Триггеры (эта папка находится внутри папки Объекты сервера).

Триггеры DDL с областью действия база данных хранятся как объекты в базах данных и хранятся в папке Триггеры базы данных, которая находится в папке Программирование соответствующей базы данных.

Параметр WITH ENCRYPTION − затемняет (скрывает) текст инструкции CREATE TRIGGER.

Параметр EXECUTE AS − указывает контекст безопасности, в котором выполняется триггер. Позволяет управлять учетной записью пользователя, используемой экземпляром SQL Server для проверки разрешений на любые объекты базы данных, ссылаемые триггером.

ИмяСобытия это команды: CREATE, ALTER, DROP, GRANT, DENY, REVOKE и UPDATE STATISTICS

ИмяГруппыDDLСобытий – имя группы событий. Например, группа событий области сервера DDL_LOIN_EVENTS охватывает команды: CREATE LOGIN, ALTER LOGIN, DROP LOGIN, а имя группы DDL_ROLE_EVENTS области сервера и базы данных – команды CREATE ROLE, ALTER ROLE, DROP ROLE.

Приведем пример запроса на создание DDL-триггера, который контролирует событие удаления любой таблицы базы данных.

```
CREATE TRIGGER TrigDDL_DELETE_TABLE
ON DATABASE
FOR DROP_TABLE
AS
 PRINT 'Внимание! Попытка удаления таблицы'
 ROLLBACK ;
```

Порядок выполнения триггеров DDL для одного и того же события следующий:

1. Триггер сервера, обозначенный как First с помощью процедуры sp_settriggerorder.
2. Другие триггеры сервера.
3. Триггер сервера, обозначенный как Last.
4. Триггер базы данных, обозначенный как First.
5. Другие триггеры базы данных.
6. Триггер базы данных, обозначенный как Last.

Сведения о триггерах DDL можно получить при помощи представлений каталога sys.triggers, sys.server_triggers.

Сведения о событиях базы данных, вызывающих срабатывание триггеров − sys.trigger_events, sys.server_trigger_events.

Триггеры DDL могут быть использованы с целью:

- предотвратить внесение определенных изменений в схему базы данных;
- выполнить в базе данных некоторые действия в ответ на изменения в схеме базы данных;

- записать изменения или события схемы базы данных.

Таким образом триггеры DDL могут применяться при выполнении административных задач (например, для аудита безопасности и регулирования операций в базе данных).

Триггеры входа выполняют хранимые процедуры в ответ на событие LOGON. Это событие вызывается при установке пользовательского сеанса с экземпляром SQL Server.

Триггеры входа срабатывают после завершения этапа проверки подлинности при входе, но перед тем, как пользовательский сеанс реально устанавливается. Следовательно, все сообщения, которые возникают внутри триггера и обычно достигают пользователя, такие как сообщения об ошибках и сообщения от инструкции PRINT, перенаправляются в журнал ошибок SQL Server. Если проверка подлинности завершается сбоем, триггеры входа не срабатывают.

Синтаксис создания триггера входа:

```
CREATE TRIGGER ИмяТриггера
ON ALL SERVER
[ WITH [ ENCRYPTION ]   [ EXECUTE AS ИмяВхода ] ]
{ FOR| AFTER } LOGON
AS  sql_statement  [ ; ] [ ,...n ]
```

Триггеры входа можно использовать для отслеживания входов в систему, ограничения входов на сервер данных, или ограничения числа сеансов для конкретного имени входа.

Для события LOGON может быть определено несколько триггеров. Так же, как и для триггеров DML при помощи системной хранимой процедуры sp_settriggerorder для триггера входа можно указать, будет ли он срабатывать первым или последним. Остальные триггеров входа выполняются в неопределенном порядке.

Проведенный анализ механизма триггеров в СУБД позволяет сделать вывод об актуальности их использования в качестве дополнительного средства обеспечения конфиденциальности и целостности баз данных.

В базе данных *угроза целостности информации* может возникать во всех случаях, когда пользователю представляется разрешение на выполнение команд модификации данных INSERT, UPDATE, DELETE. В этом случае существует некоторая, пусть даже очень маленькая вероятность неумышленного изменения данных конечным пользователем при выполнении команд UPDATE и DELETE в результате халатного или невнимательного отношения при выполнении запросов. Применение триггеров DML позволит снизить подобные риски за счет расширения набора декларативных ограничений целостности данных в базе данных ограничениями, логика выполнения которых связана с бизнес-правилами решения задач,

возможностью организации оперативного аудита за изменениями данных базовых таблиц командами модификации данных и т.д.

*Угрозы конфиденциа*льности возникают при несанкционированном доступе к серверу, базе данных или ее объектам. Применение триггеров входа и DDL триггеров позволят расширить возможности имеющихся в СУБД средств аудита механизмом оперативного контроля за подключениями к серверу, выполнением команд DDL. Это, в свою очередь, позволит проводить дополнительный оперативный аудит учетных записей пользователя, усилить контроль за соблюдением политики безопасности пользователя и соблюдением принципа «наименьших прав доступа» (предоставления лишь необходимого уровня доступа к защищенному объекту участникам, нуждающимся в нем, и только на определенное время).

Литература:

1. Документации Майкрософт для пользователей, разработчиков и ИТ-специалистов [Электронный ресурс]. URL: https://docs.microsoft.com/ru-ru/sql/t-sql/statements/create-trigger-transact-sql?view=sql-server-2017 (дата обращения: 28.10.2018).
2. Десятка крупнейших угроз безопасности баз данных и борьба с ними [Электронный ресурс]. URL: https://www.dataarmor.ru/десятка-крупнейших-угроз-безопаснос (дата обращения: 28.10.2018).
3. Утебов Д.З., Белов С.В. Классификация угроз в системах управления базами данных [Электронный ресурс]. URL: http://cyberleninka.ru/article/n/klassifikatsiya-ugroz-v-sistemah-upravleniya-bazami-dannyh#ixzz2v4Ll6nE1 (дата обращения: 28.10.2018).

3.5. Защита акустической речевой информации конфиденциального характера от утечки по техническим каналам

Как известно, в последние годы информационные технологии внедрились в сферу жизни общества так широко, что без их использования любая деятельность представляется невозможной. Информация стала практически материальным ресурсом. Приходит понимание того, что любую информацию необходимо защищать, в первую очередь, информацию ограниченного доступа, не содержащую сведений, составляющих государственную тайну.

Указом Президента Российской Федерации от 6 марта 1997 года № 188 определен «Перечень сведений конфиденциального характера».

С одной стороны информатизация общества – великое благо. С другой стороны – количество преступлений в информационной сфере выросло в несколько сотен раз. Одним из основных источников угроз безопасности информации является деятельность иностранных разведывательных и специальных служб, преступных сообществ, организаций, групп и противозаконная деятельность отдельных лиц, направленная на

реализацию деструктивных воздействий на информацию, на сбор или хищение ценной информации, закрытой для доступа посторонних. Причем более чем в 90% случаях информация добывается злоумышленниками с применением технических средств разведки. Каждый обладатель информации должен отдавать себе отчет о необходимости обеспечения ее безопасности. Настоящая статья посвящена рассмотрению методов предотвращения утечки речевой информации по техническим каналам.

Классификация технических каналов утечки и угроз безопасности информации

Прежде чем рассматривать технические каналы утечки информации, следует ознакомиться с видами представления акустической информации (таблица 3.2). Под акустической понимается информация, носителями которой являются акустические сигналы. В том случае, если источником информации является человеческая речь, акустическая информация называется речевой.

Таблица 3.2. Виды представления акустической информации

Акустическая (речевая) информация		
информация, содержащаяся непосредственно в произносимой речи	информация, воспроизводимая акустическими средствами	информация, содержащаяся в электромагнитных полях и электрических сигналах, которые возникают за счет преобразований акустической информации

Основанием для добывания информации с применением технических средств является наличие технических каналов ее утечки.

Технический канал утечки информации (ТКУИ) – совокупность источника информации, физической среды, в которой распространяется информативный сигнал (циркулируют данные) и объектов разведки, которые с помощью технических средств разведки (ТСР) добывают информацию.

Наличие ТКУИ создают угрозы безопасности информации.

Как известно, под угрозой безопасности информации понимается возможность возникновения такого явления или события, следствием которого является нежелательное воздействие на носитель информации, частичная или полная утрата информации, либо ее утечка или разглашение.

Классификация технических каналов утечки акустической (речевой) информации

К техническим каналам утечки акустической (речевой) информации относятся:

1. *Воздушные*, позволяющие осуществлять перехват акустических сигналов микрофонами в комплексе с устройствами передачи информации:

– по радиоканалу;
– по сети электропитания;
– по оптическому каналу в инфракрасном диапазоне;
– по телефонным линиям;
– по трубам водоснабжения, отопления, металлоконструкциям;
– по сигналу вызова от внешнего телефонного абонента.

2. *Электроакустические*, позволяющие осуществлять перехват акустических колебаний через вспомогательные технические средства и системы (ВТСС):

– обладающие микрофонным эффектом, путем подключения их к соединительным линиям;
– путем ВЧ-навязывания.

3. *Вибрационные*, позволяющие осуществлять перехват акустических сигналов:

– с помощью электронных стетоскопов;
– электронными стетоскопами в комплексе с устройствами перехвата информации по радиоканалу, оптическому каналу в инфракрасном диапазоне, по трубам водоснабжения, отопления, металлоконструкциям и т. д.

4. *Параметрические*, осуществляющие перехват акустического сигнала:

– путем приема и детектирования ПЭМИ (на частотах ВЧ-генераторов) ВТСС при модуляции информативным сигналом;
– путем ВЧ-облучения специальных полуактивных закладочных устройств.

5. *Оптико-электронные* (*лазерные*), позволяющие осуществлять перехват акустического сигнала путем лазерного зондирования оконных стекол.

6. Каналы радио- и радиорелейной связи, позволяющие осуществлять перехват информации, передаваемой по ним.

7. Системы и средства связи, позволяющие осуществлять перехват электромагнитных излучений на частотах работы их передатчиков.

8. Кабельные линии связи, позволяющие осуществлять съем информации, передаваемой по ним:

– электрический – съем информации, передаваемой путем контактного подключения к кабельным линиям связи;
– индукционный – бесконтактный съем информации с кабельных линий связи.

Особенностью угроз безопасности информации при ее утечке по техническим каналам является реализация этих угроз непосредственно через элементы ТКУИ. Угрозы не существуют отдельно от каналов (так как они зависят от характеристик и параметров канала).

Технические каналы утечки речевой информации

Обеспечение безопасности информации конфиденциального характера в любой организации предполагает наличие в ней системы защиты. Успех создания и функционирования системы защиты информации зависит в первую очередь от принимаемых организационных и технических мер. С этой целью разрабатываются организационно-распорядительные документы, обязательные для исполнения всеми сотрудниками организации. Одним из таких документов является частная модель угроз (ЧМУ), разрабатываемая для каждого объекта защиты на основе руководящих и методических документов ФСТЭК России. В частности, ФСТЭК России разработан «Банк данных угроз безопасности информации», который размещен на ее сайте. Указанный документ целесообразно использовать с целью построения для своей организации адекватной модели угроз.

Практически во всех известных вариантах ЧМУ, разработанных различными структурами, в том числе и в «Методических рекомендациях по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости» технические каналы утечки речевой информации относятся, как ни странно, к неактуальным и не представляющим большой угрозы безопасности информации.

Однако недооценка потенциальной угрозы утечки речевой информации может привести к негативным последствиям, в первую очередь, это касается информации конфиденциального характера. В настоящее время создана современная, высокочувствительная аппаратура для ведения разведки (несанкционированного доступа (НСД) к информации) в акустическом диапазоне (акустическая речевая разведка − АРР). С помощью такой аппаратуры может контролироваться и записываться содержание закрытых совещаний, на которых происходит обсуждение, например, медицинских диагнозов физических лиц, вопросов усыновления, оригинальных технических решений на предприятиях оборонно-промышленного комплекса, планирование различного рода мероприятий органами власти, т.е. информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.

Классификация технических каналов утечки акустической речевой информации и возможности аппаратуры перехвата представлены в таблице 3.

Таблица 3.3. Технические каналы утечки речевой информации

Технический канал утечки информации	Наименование аппаратуры	Вид аппаратуры и технические характеристики
Акустический	Направленные микрофоны	Стационарная, портативная носимая, портативная возимая до 180 м
	Ненаправленные микрофоны	Портативная носимая, портативная возимая до 15 м.
Виброакустический	Вибродатчики («контактные микрофоны»)	Автономная автоматическая (совместно со средствами приема ретранслируемого сигнала) до 12 м (на поверхностях 150 см и более).
Виброакустический (лазерный)	«Лазерные микрофоны»	Стационарная, портативная носимая, портативная возимая до 450 м.
Акустоэлектрический	Средства съема электрических сигналов с гальваническим подключением	Стационарная, портативная возимая до 250 м.
ВЧ – навязывание	Средства съема электрических сигналов с гальваническим подключением	Стационарная, портативная возимая до 250 м.
ВЧ – облучение (параметрический	Приемники электромагнитного поля	Стационарная, портативная возимая до 800 м.

Как следует из таблицы 3.3, возможности добывания информации с помощью аппаратуры акустической речевой разведки довольно-таки значительные. Поэтому игнорировать наличие потенциального и эффективного в определенных случаях технического канала утечки акустической речевой информации было бы большой ошибкой. Следовательно, необходимо применять различные технические и организационные методы защиты акустической речевой информации.

Методы защиты акустической речевой информации от утечки по техническим каналам

Как было отмечено выше, основными методами защиты информации являются технические и организационные. Причем, как правило, первоначально отдается предпочтение техническим методам, а если их недостаточно или отсутствует возможность их использования, то в этих случаях применяются организационные методы. В настоящее время лицензиатами ФСТЭК России разработано значительное количество технических средств защиты акустической речевой информации от утечки по

техническим каналам. Указанные средства прошли сертификацию в системе сертификации ФСТЭК России, сведения о них размещены в реестре сертифицированных средств защиты информации (СЗИ). Часть из них предназначена для перекрытия одного, какого-либо конкретного, или нескольких каналов: система постановки акустических и виброакустических помех «ЛГШ-401», система виброакустической и акустической защиты «Соната-АВ» (модель 1М), комплекс виброакустической защиты «Шелест-4К», система виброакустической защиты «ВВ301», устройство виброакустической защиты речевой информации − ВП23-5П-Nk, которые сертифицированы на соответствие НМД АРР и Нормам защиты речевой информации, обрабатываемой техническими средствами, система защиты помещений по виброакустическому каналу SEL SP-55 с эквалайзером − на соответствие ТУ. Кроме этого разработаны и находятся в эксплуатации целые комплексы, как правило, автоматизированные, с помощью которых задача по предотвращению утечки акустической речевой информации по техническим каналам решается комплексно, например: система акустической и вибрационной защиты «Кабинет-С2», система акустической и вибрационной защиты «Кабинет-Д». Указанные средства устанавливаются на объектах защиты либо обладателями, либо организациями, имеющими лицензии ФСТЭК России на соответствующие виды деятельности. Одним из сравнительно дешевых, но при этом эффективных методов защиты акустической речевой информации от утечки по системам холодного и горячего водоснабжения, системам отопления является врезка в трубопроводы до границы контролируемой зоны резиновых или пластиковых вставок. Однако, в этом случае требуется проведение технического контроля эффективности реализованных методов защиты информации.

Учитывая, что защита информации – мероприятие затратное, то прежде чем принимать решение о создании системы технической защиты акустической речевой информации, следует провести тщательное обследование всех возможных каналов. Далее на этом основании следует принять рациональное решение, какие каналы перекрывать с помощью СЗИ, а какие с помощью организационных мер, а именно: разработкой соответствующих инструкций при проведении совещаний и неукоснительным выполнением их требований.

Таким образом, решение задач по обеспечению безопасности информации конфиденциального характера, циркулирующей в акустическом диапазоне, может быть успешно решено при использовании существующих сертифицированных средств защиты информации в сочетании с грамотно разработанными и введенными в действие организационно-распорядительными документами.

Литература:

1. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утверждены приказом Гостехкомиссии России от 30.08.2002 №282.
2. Банк данных угроз безопасности информации. СТЭК России, ФАУ «ГНИИИ ПТЗИ ФСТЭК России», 2015 [Электронный ресурс]. URL: https://bdu.fstec.ru/ (дата обращения: 30.10.2018).
3. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии − М.: Академия, 2009. – 415 с.
4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена 15.02.2008 заместителем директора ФСТЭК России.
5. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена 14.02.2008 заместителем директора ФСТЭК России;
6. ГОСТ Р 50.1.056-2005. Техническая защита информации. Основные термины и определения.

ГЛАВА 4. СОВРЕМЕННЫЕ ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Разработка деловой игры «Построение системы защиты информации на предприятии»

В условиях бурно развивающихся информационных технологий проблема информационной безопасности становится все более актуальной. Предприятия несут большие потери в результате преднамеренных и непреднамеренных действий, приводящих к краже, повреждению или уничтожению информации. Сбой в работе системы информационной безопасности может привести к утечке информации являющейся коммерческой, военной или иной тайной. Нестабильность работы поврежденных систем может привести к большим убыткам со стороны предприятия. Для предотвращения этих последствий необходимо выстроить качественную и что самое главное экономически эффективную систему защиты информации.

Деловая игра предназначена для обучения студентов принципам построения систем информационной безопасности. Несмотря на то, что игра носит обучающий характер, все механизмы, заложенные в ней, могут быть использованы и при построении реальной системы.

Целью деловой игры является построение экономически эффективной системы информационной безопасности, обеспечивающей не только требуемый уровень защищенности, но и не выходящей за рамки выделенного бюджета. Деловая игра проводится с использованием информационной системы, позволяющей автоматизировать процесс выбора решений, повышающих степень информационной защищенности предприятия. Основными задачами программы являются:

- агрегация всей справочной информации;
- автоматизация выбора возможных угроз и вероятности их реализации;
- выбор решений, повышающих уровень информационной безопасности;
- проверка соответствия выбранных решений исходным данным;
- генерация отчета.

В основе деловой игры лежат два базовых понятия: угрозы и решения. Под угрозами понимаются возможные действия, приводящие к нарушению информационной безопасности предприятия. В игре присутствуют следующие виды угроз:

1. угроза несанкционированного доступа;
2. угроза анализа сетевого трафика;
3. угроза удаленного администрирования;

4. угроза подмены доверенного объекта или субъекта распределенной вычислительной системы;
5. угроза внедрения в распределенную вычислительную систему ложного объекта;
6. угроза внедрения в распределенную вычислительную систему ложного объекта путем использования недостатков алгоритмов удаленного поиска;
7. угроза отказа в обслуживании;
8. угроза нарушения целостности;
9. угроза проникновения вредоносных разрушающих программ (компьютерных вирусов);
10. угроза от инсайдеров (несанкционированные действия нарушителей из числа сотрудников компаний).

Каждая угроза характеризуется возможными потерями и возможностью реализации. Возможные потери задаются лингвистической переменной, которой ставятся в соответствие числовые значения. Каждая угроза характеризуется расчетным значением и эталонным (табл. 4.1). Расчетное значение используется в расчетах итоговых показателей, а эталонное задает требуемый уровень защищенности.

Таблица 4.1. Возможные потери

№ п/п	Наименование	Расчетное значение	Эталонное значение
1	Очень низкие	0,07	0,4
2	Низкие	0,13	0,5
3	Средние	0,2	0,7
4	Высокие	0,267	0,8
5	Очень высокие	0,333	0,95

Для описания всех рассматриваемых угроз формируется таблица угроз (табл. 4.2).

Таблица 4.2. Угрозы

№ п/п	Наименование поля	Тип поля
1	№ п/п	Числовое
2	Наименование угрозы	Текстовое
3	Возможные потери	Список текстовых значений
4	Возможность реализации	Булево значение

Под решениями понимаются те или иные проекты, поднимающие уровень защищенности предприятия и препятствующие реализации угроз. Выбираемые решения могут защищать как от одной угрозы, так и от не-

скольких. Каждое решение характеризуется одним или несколькими коэффициентами, определяющими общий коэффициент защищенности, обеспечиваемый данным решением. Для описания возможных решений Таблица со списком решений формируется таблица решений (табл. 4.3).

Таблица 4.3. Решения

№ п/п	Наименование поля	Тип поля
1	№ п/п	Числовое
2	Наименование угрозы	Текстовое
3	Наименование решения	Текстовое
4	Коэффициенты	Текстовое
5	Стоимость решения	Денежное
6	Выбрано	Булево значение

Поле коэффициенты содержит отформатированный текст со значениями коэффициентов, характеризующих то или иное решение. Общий коэффициент защищенности для конкретного решения рассчитывается по формуле:

$$K_{ij} = \frac{\sum_{h=1}^{m} x_{hij}}{m}$$

где K_{ij} − общий коэффициент защищенности от i-ой угрозы, обеспечиваемой j-ым решением; m − количество коэффициентов, характеризующих j-ое решение; x_{hij} − значение h-ого коэффициента j-ого решения от i-ой угрозы.

По окончании игры рассчитывается коэффициент защищенности от каждой угрозы. Этот коэффициент рассчитывается по следующей формуле:

$$L_i = \frac{\sum_{j=1}^{b} K_{ij}}{b}$$

где L_i − общий коэффициент защищенности от i-ой угрозы; b − количество решений, защищающих от данной угрозы.

Общий коэффициент защищенности от всех видов информационных угроз может быть найден по формуле:

$$M = \frac{\sum_{i=1}^{n} L_i}{n}$$

где M − итоговый коэффициент защищенности, n − количество возможных угроз.

В процессе реализации игры также рассчитываются следующие показатели:

- Вероятность реализации *i*-ой угрозы:

$$P_i = 1 - L_i$$

- Возможные потери от одноразового воздействия угрозы:

$$G_i = C_i \times S$$

где:

G_i- −потери от реализации *i*-ой угрозы, C_i – −коэффициент потерь от реализации *i*-ой угрозы.

S – −ликвидная стоимость компании, задаваемая в исходных данных.

- Риск реализации *i*- ой угрозы рассчитывается в денежном выражении как произведение вероятности реализации угрозы на величину возможных потерь от ее реализации

$$R_i = G_i \times P_i$$

- Предотвращенные потери (величина, противоположная риску) в денежном выражении рассчитываются как произведение вероятности того, что неблагоприятное событие не произойдет, на величину возможных потерь в случае реализации риска.

$$D_i = (1 - P_i) \times G_i$$

- Коэффициент экономической эффективности выбранных средств защиты информации отражает объем предотвращенных потерь на единицу защищенности

$$E = \frac{\sum_{i=1}^{n} D_i}{M \times 100}$$

Все участники делятся на команды по 4-5 человек. Вся игра разворачивается между этими командами. Задачей каждой команды является предоставить свой оптимальный план построения системы информационной безопасности.

Стоит отметить, что игра учитывает также и временной фактор, т.е. программа по созданию системы информационной безопасности может быть рассчитана на несколько лет. Каждый год могут выделяться различные суммы на реализацию новых решений. Задача игроков уложиться в бюджет, при этом достигнув максимального повышения уровня информационной безопасности. Для этих целей командам предоставляется информация с подробным описанием каждого решения. Анализ этих данных должен помочь игрокам достичь поставленных целей.

По завершении основной части игры, команды могут сформировать отчет о созданной ими системе. Перед его созданием, программа автоматически проверяет, достигнут ли требуемый уровень защищенности. Если он не был достигнут, команда получает сообщение, после чего может по-

пробовать реализовать другую стратегию развития системы безопасности. В окончательный отчет включается список угроз со значениями возможных потерь от реализации угрозы, состояние бюджета на каждый год, список решений. Каждое решение сопровождается общим коэффициентом защищенности и списком угроз с рассчитанными значениями возможных потерь, вероятности реализации угроз, риска и экономической эффективности. Итоговым является показатель экономической эффективности выбранных средств защиты информации.

Проведение игры сводится к выполнению следующих этапов:

1. Игра начинается с анализа исходных данных, описывающих предприятие. Имея в своем распоряжении данные о фирме, игроки могут оценить вероятность возникновения угроз, оценить возможные потери в ходе реализации каждой угрозы.
2. После анализа входных данных выбирается список наиболее вероятных для данного предприятия угроз и определяются возможные потери, связанные с реализацией этих угроз.
3. На основном этапе игры команды выбирают те решения, которые предотвращают реализацию определенных ранее угроз или повышают уровень защищенности от их реализации.
4. Финальным этапом деловой игры является защита каждой командой своего проекта. На этом этапе каждая команда должна обосновать, почему ими были выбраны те или иные угрозы и средства защиты от них. Команды игроков создают отчеты со всеми рассчитанными показателями о спроектированных ими системах защиты и демонстрируют полученные результаты в форме презентации всем участникам игры.

Литература:

1. Стельмашонок Е.В. Моделирование коррелированых угроз информационной безопасности предприятия // Вестник ИНЖЭКОНА. − Экономика. − 2011.− № 5(48) − С.175-181.
2. Стельмашонок Е.В. Формирование облика системы защиты предприятия // Вестник ИНЖЭКОНА. − Экономика. − 2011. − № 6(49) − С.147-151.

4.2. Создание и использование лабораторного стенда для изучения DLP-системы InfoWatch Traffic Monitor

В первом полугодии 2018 года в СМИ и иных источниках обнародовано и зарегистрировано Аналитическим центром InfoWatch 1039 случаев утечки конфиденциальной информации, что на 12% больше, чем за аналогичный период 2017 года. Внешние атаки стали причиной 35,5% утечек

данных. В 64,5% случаев утечка данных произошла под воздействием внутреннего нарушителя и в 53,5% случаев виновными в утечку оказались штатные сотрудники компаний [1].

АО «Инфовотч» − российская компания, специализирующаяся на информационной безопасности в корпоративном секторе: защите корпораций от утечек информации и целевых атак извне. Контролирует около 50 % российского рынка систем защиты конфиденциальных данных. Компания образована в 2003 году как дочернее предприятие «Лаборатории Касперского», с 2007 года стала полностью самостоятельной [2]. На данный момент наиболее известными заказчиками в разных сегментах рынка у компании являются:

- банки и страховые компании − «Сбербанк», «Банк ВТБ», «Связь-банк», *Raiffeisen Bank*, «Банк Москвы», «Хоум Кредит», «Согаз», ВСК и др.;
- нефтегазодобывающие компании − «ЛУКойл», «Татнефть», «Сургутнефтегаз», «Новатэк», «Славнефть», подразделения «Газпрома», «E.ON Россия» и др.;
- энергетические компании − ТВЭЛ, «РусГидро», «Русэнергосбыт», «Русэнергоресурс», «Интер РАО» и др.;
- оборонные, промышленные предприятия − «Сухой», Московский вертолетный завод имени М. Л. Миля, «Оборонпром», Магнитогорский металлургический комбинат, Объединенную двигателестроительную корпорацию, Новороссийский морской торговый порт, «Мосводоканал» и др.;
- продовольственные компании, торговые сети, мобильную связь − «Магнит», *Magnum*, «Дикси», «Ударница», *KupiVIP*, «Билайн», МТС и др.;
- госструктуры − ФНС России, Фонд социального страхования, ФТС России, Минфин России, Минобороны России, МЧС России, Комитет по информатизации и связи Санкт-Петербурга, Правительство Тульской области, ВГТРК и др.

Наиболее важным для изучения в лабораторном практикуме по дисциплине «Защита сетевых информационных технологий» представляется основной продукт компании − InfoWatch Traffic Monitor (IWTM).

В связи с этим была поставлена задача создать на базе лаборатории программно-аппаратной защиты (ПАЗИ) кафедры вычислительных систем и программирования СПбГЭУ стенд для проведения лабораторных работ.

InfoWatch Traffic Monitor представляет собой автоматизированную систему контроля информационных потоков организации для выявления утечек информации, а также других внутренних угроз. Данный продукт компании представлен двумя версиями: Standard и Enterprise. Standard-версия продукта представляет собой упрощенную и местами урезанную

версию продукта. С целью более подробного изучения возможностей IWTM стенд решено создавать с использованием версии Enterprise.Архитектура продукта представлена на рис.1.

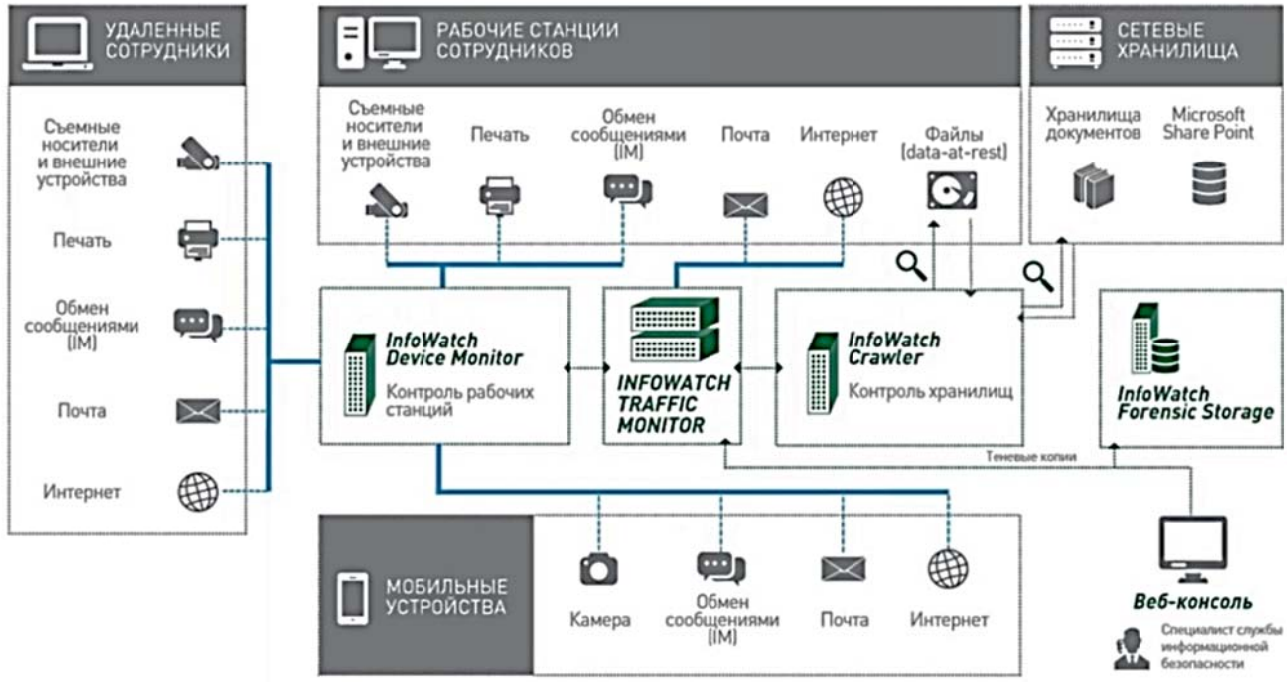


Рисунок 4.1. Архитектура IWTM

Коротко о каждой части продукта:

- InfoWatch Traffic monitor (TM) − главная часть продукта. Осуществляет связь между другими компонентами системы, контролирует интернет и почтовый траффик. Отвечает за блокировку и частичное теневое копирование всей исходящий от рабочей станции пользователя информации. Представлен решением в виде массива файлов, расположенных на ОС Red Hat. На данном компоненте так же реализована веб-консоль офицера безопасности—специальный интерфейс для настройки и отслеживания событий непосредственно при работе с системой;
- InfoWatch Device monitor (IWDM) − осуществляет контроль рабочих станций на физическом уровне. Способен анализировать буфер обмена, обмен информацией с внешними носителями, печать. Представляет собой приложение Windows. Также осуществляет задачу первичного распространения клиента монитора на все подконтрольные рабочие станции;
- InfoWatch Crawler − осуществляет сканирование хранилищ с целью выявления запрещенных документов. Установка, как наиболее популярное решение, осуществляется на тот же сервер, на котором находится DM (Device monitor);

- База Данных − важный компонент системы, представленный в виде дискового хранилища. Осуществляет хранение всего перехваченного трафика и всех присущих ему меток. При небольшом количестве пользователей и трафика, устанавливается вместе с ТМ и реализуется на Linux-совместимой БД (PostgresSQL или OracleSQL)

Основных режимов работы ТМ два: «в разрыв» и «режим копирования». Работа в режиме теневого копирования осуществляется в том случае, когда работа «в разрыв» невозможна. Например, когда ТМ не обладает подконтрольным ему коммутатором и не может полностью контролировать трафик, идущий по системе. При наличии прокси-сервера, к которому осуществлено подключение с помощью ТМ, становится возможно работать «в разрыв» и осуществлять контроль над трафиком рабочей станции. Также возможен комбинированный режим работы. В данном случае корпоративный почтовый сервер находится в локальной сети до коммутатора ТМ. Поэтому имеется возможность не только осуществлять контроль по пропуску трафика, но и снимать копию с каждого отправленного с рабочей станции письма.

Вот неполный список того, что возможно контролировать, используя данный продукт:

- почтовые протоколы SMTP, IMAP;
- веб-почта, социальные сети;
- загрузка в облачные хранилища;
- интернет трафик по таким протоколам как HTTP, HTTPS, FTP;
- контроль съемных носителей и т.п.

InfoWatch Traffic Monitor способен работать с разными объектами: текстовыми, сигнатурами файлов, классификациями по терминам и объекты защиты с использованием комбинированных технологий анализа:

- лингвистический анализ;
- детектор эталонных документов;
- детектор графических объектов;
- детектор выгрузок из баз данных;
- детектор заполненных анкет;
- оптическое распознавание символов;
- детектор печатей и факсимиле.

Не останавливаясь подробно на описании реализации перечисленных технологий в ТМ, перейдем непосредственно к проблемам создания стенда.

Системные требования к установке ТМ весьма высокие, особенно в части объема оперативной памяти сервера: не менее 8ГБ. Поэтому в условиях лаборатории ПАЗИ оказалось невозможным реализовать архитектуру стенда непосредственно на рабочих станциях с использованием виртуальных машин, как это было сделано ранее при создании подобного стенда

для изучения DLP Falcongaze. Установку было решено проводить на физическом сервере. Для этого был выделен сервер HP Proliant DL360 со следующими характеристиками:

- объем оперативной памяти 16ГБ;
- два процессора: Intel (R) Xeon (R) CPU E5504@ 2.0GHz, ядер 4, логических процессоров 4;
- объем диска 360 Гб;
- операционная система Windows Server 2016.

Для установки стенда были использованы следующие дистрибутивы:

- установочный файл IWTM с интегрированной в него 64х разрядной операционной системой Red Hat;
- Windows Server 2008R2 с AD и Microsoft SQL Server;
- рабочая станция с ОС Windows 7;
- установочный файл IWDM;
- установочный файл Crawler;
- лицензия для IWTM.

В лабораторном комплексе для виртуальной машины было выделено 4 процессорных ядра и почти 9Гб оперативной памяти. Особых требований к гипервизору со стороны системы не предъявлялось, и поэтому используется Oracle VM VirtualBox. Для корректной работы внутри сети должен быть включен режим «сетевой мост».

В силу ограничения ресурсов лаборатории ПАЗИ, с одной стороны, и использования IWTM исключительно в учебном процессе, с другой, была выполнена установка БД и IWTM на один сервер (так называемая система all-in-one). В качестве БД на ОС Red Hut выбрана PostgresSQL, являющаяся свободной объектно-реляционной СУБД.

Сетевые настройки выполнены в соответствии с параметрами ЛВС университета с использованием DNS и DHCP.

В работе с табличными пространствами выбран нормальный режим работы и включена архивация для всех типов ежедневных табличных пространств (ежедневные табличные пространства хранят в себе все события, которые перехватила система).

Установка DM производится на сервер с ОС Windows Server 2008R2 с развернутыми AD и Microsoft SQL (отметим, что IWTM 6 пока не ставится на Windows Server 2016). Большинство настроек выполняется по умолчанию, в том числе, создание нового ключа для защищенного канала.

После установки ТМ можно воспользоваться для настройки DM веб-консолью офицера безопасности (рис. 4.2).

Особенностью установки было то, что для нахождения токена авторизации для DM пришлось открыть просмотр кода страницы, в коде найти токен, скопировать его в поле установки DM и нажать Далее, после чего началась установка. В процессе установки необходимо ввести лицензию

на продукт, предоставленную вендором и провести синхронизацию политик безопасности на вкладке «Сихнронизация политик Traffic Monitor».

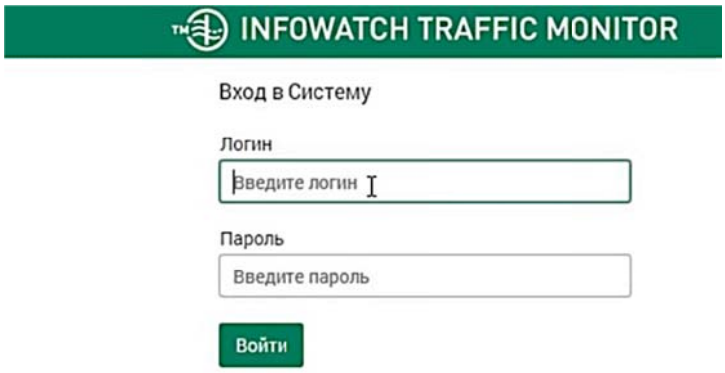


Рисунок 4.2. Окно входа в веб-консоль офицера безопасности

После установки связи между серверами в защитный периметр можно включать рабочие станции, используя AD. Установка (инсталляция) агентов на рабочие станции производится автоматически после выбора необходимых опций контроля в Мастере создания задачи. Для авторизации на сервере с рабочей станции используется форма server\user.

Установка утилиты Crawler вопросов не вызывает. Необходимо лишь корректно ввести параметры ТМ в окне Settings. Однако для активации Crawler требуется дополнительная настройка через веб-консоль офицера безопасности. Необходимо отредактировать файл web.conf, находящийся в папке opt/iw/tm5/etc, и в строке Crawler Enabled изменить 0 на 1. Затем следует перезапустить службу Kicker.

Созданный стенд позволяет проводить полноценный цикл работ, направленный на изучение студентами InfoWatch Traffic Monitor Enterprise.

Однако, в силу того, что система была установлена на выделенном сервере, организовать работу всей учебной группы одновременно не представляется возможным. Поэтому группа разбивается на бригады по 3-4 человека, каждый из которых может активно участвовать в выполнении заданий лабораторной работы. Время работы на стенде для бригады – четыре академических часа. Общий фонд времени, планируемый для проведения лабораторных работ по дисциплине «Защита сетевых информационных технологий» позволяет в течение семестра провести занятия на стенде для всех обучающихся. В проведении лабораторных работ активное участие принимают студенты, прошедшие обучение и получившие сертификаты как «Специалист внедрения и поддержки InfoWatch Traffic Monitor 6».

На стенде можно выполнять следующие практикумы.

1. Настройка уведомления офицера безопасности при перехвате системой защищаемого объекта при перехвате системой защищаемого объекта.

План решения задачи:
- указать адрес электронной почты для офицера безопасности;
- загрузить и настроить защищаемый объект;
- настроить периметр компании;
- настроить политику таким образом, чтобы в случае передачи данного защищаемого объекта за пределы компании, система генерировала уведомление;
- проверить правильность работы политик путем имитации передачи файлов за периметр и внутри его.

2. Настройка периметра организации для предотвращения утечек информации посредством выноса на физических носителях и переноса в облачные файловые хранилища.

   План решения задачи:
- добавить правила работы с облачными хранилищами и внешними устройствами;
- применить политики на группу рабочих станций;
- проверить работу политик путем имитации нарушения на нескольких рабочих станциях.

3. Нахождение определенного документа на жестком диске одной из рабочих станций сотрудников компании. Это позволяет инспектировать файловые хранилища и жесткие диски пользователей на предмет хранения на них документов или информации ограниченного доступа.

   План решения задачи:
- загрузить искомый документ в Traffic Monitor как эталонный и настроить объект защиты;
- создать задание на сканирование рабочих станций, на которых этот документ должен быть обнаружен;
- создать запрос, выводящий соответствующие события в БД
- проверить работу политики на одной рабочей станции.

4. Разрешение использовать заданный USB-носитель памяти на указанной рабочей станции.

   План решения задачи:
- создать новое правило в белых списках;
- ввести изменения в действия;
- проверить работу правила для конкретного USB-носителя на указанной рабочей станции.

5. Создание отчета, отображающего всех пользователей, которые копируют на внешние устройства информацию определенной категории.

   План решения задачи:
- создать и настроить защищаемую категорию, а также объект защиты;

- создать панель с виджетом, которая будет отображать все перехваченные события данной категории;
- создать отчет, который выводит информацию о нарушителях, которые копируют данную категорию.

6. Запретить использование приложений. Данный механизм позволяет исключить возможность запуска потенциально опасного ПО, в том числе такого, которое может позволить «обойти» существующие механизмы защиты информации.

   План решения задачи:

- создать список приложений;
- добавить в созданный список необходимые приложения;
- создать политику, добавить в политику правило работы с приложениями;
- применить политику на группу рабочих станций и ввести изменения в действие;
- проверить действие политики путем запуска запрещенного приложения на одной из рабочих станций.

7. Создать панель и отчет, на которой будет отображаться информация обо всех нарушениях группы пользователей.

   План решения задачи:

- создать группу и добавить в нее необходимых пользователей (можно использовать существующую группу AD);
- создать запрос, который выведет все нарушения политики безопасности, сгенерированные группой пользователей;
- создать панель с виджетом, выводящим события по данному запросу;
- создать отчет, выводящий диалоги группы пользователей, а также каналы передачи объектов защиты.

8. Запретить использование протоколов FTP, FTPS, POP3, SMTP, MAPI, IMAP4.

   План решения задачи:

- создать политику;
- добавить в созданную политику правила работы с FTP и почтой;
- применить политику на группу сотрудников и ввести изменения в действие;
- проверить работу политик путем имитации нарушения на нескольких рабочих станциях.

Все перечисленные практикумы обеспечены подробными методическими указаниями, основанными на рекомендациях вендора.

Проведенные занятия показали эффективность проведения практикумов в указанной постановке и хороший уровень знаний и навыков, получаемый студентами.

Литература:

1. Аналитический Центр InfoWatch представляет исследования утечек информации в мире [Электронный ресурс]. URL: https://www.infowatch.ru/analytics (дата обращения: 05.11.2018).
2. История компании InfoWatch [Электронный ресурс]. URL: https://www.infowatch.ru/about/history (дата обращения: 05.11.2018).

4.3. Административный доступ и обеспечение безопасности аппаратно-программного комплекса компьютерной аудитории

В государственном экономическом университете для нужд учебного процесса организовано более 90 компьютерных классов, в которых установлено более 1300 компьютеров и рабочих станций. На каждом персональном компьютере установлен большой пакет прикладных программ, необходимый для проведения лабораторного практикума на различных направлениях и специальностях университета. Многие из установленных в учебных классах программ имеют дорогостоящую лицензию и ограниченное число инсталляций.

Для обеспечения безопасности программного комплекса в 2015 г. все рабочие станции университета были введены в домен, и к ним была применена общая политика безопасности. Права пользователя с доменной учетной записью сильно ограничены, что, не мешая работе с программами, позволило защитить программный комплекс от случайного, непреднамеренного или умышленного повреждения при проведении компьютерного практикума [1].

Но для некоторых программных продуктов и циклов лабораторных работ требуется административный доступ к аппаратно-программным средствам компьютера. Такие циклы, обычно, проводятся в специализированных лабораториях, где развернута своя, изолированная от общей сети университета сеть. В такой лаборатории возможно проведение небезопасных для программно-аппаратного комплекса экспериментов.

В качестве примера можно привести преподаваемую в течение многих лет дисциплину «Компьютерные сети». В состав дисциплины входит лабораторный практикум, на котором студенты получают необходимые навыки и умения по настройке и подготовке компьютеров к соединению с другими компьютерами, обмену данными, использованию общих ресурсов и т.п. Для выполнения поставленных задач на компьютере (хосте) студенту предоставляется учетная запись с правами локального администратора. Проведение такого курса в специализированной лаборатории не представляет сложности.

Но та же дисциплина «Компьютерные сети» может быть и дисциплиной по выбору для студентов других направлений и специальностей,

которые базирующихся в других учебных корпусах. В таком случае проведение цикла лабораторного практикума в специализированной лаборатории не представляется возможным.

Получение прав локального администратора в обычных компьютерных классах и других учебных корпусах, как правило, невозможно или сопряжено с большими организационными трудностями. Не меньшую сложность представляет необходимость подключения дополнительного оборудования, используемого в практикуме. Выходом их этой сложной ситуации стало использование для проведения лабораторного практикума виртуальной машины (ВМ).

Виртуальная машина − программная и/или аппаратная система, эмулирующая аппаратное обеспечение некоторой платформы (target − гостевая платформа) и исполняющая программы для target-платформы на host-платформе (host − платформа-хозяин) или виртуализирующая некоторую платформу и создающая на ней среды, изолирующие друг от друга программы и даже операционные системы.

Виртуальная машина исполняет некоторый машинно-независимый код или машинный код реального процессора. Помимо процессора, ВМ может эмулировать работу как отдельных компонентов аппаратного обеспечения, так и целого реального компьютера (включая BIOS, оперативную память, жесткий диск и другие периферийные устройства). В последнем случае в ВМ, как и на реальный компьютер, можно устанавливать операционные системы. На одном компьютере может функционировать несколько виртуальных машин [2].

Основное удобство ВМ − отсутствие необходимости в переключении между ОС и доступ ко всем функциям воспроизводимой системы. Кроме того, все действия, совершаемые внутри виртуальной машины, не будут затрагивать работу основной системы, что предотвращает возможные сбои компьютера и повреждение программного обеспечения хоста.

Перевод лабораторного практикума на ВМ решает практически все сложные вопросы, перечисленные выше, почти не создавая новых трудностей [3].

При установке гостевой ОС пользователь получает права локального администратора, к ВМ можно подключать дополнительное оборудование (от носителя на флеш-памяти до принтера общего доступа).

Наиболее удобным менеджером виртуальных машин оказался ORACLE VirtualBox.

VirtualBox − простой, мощный и бесплатный инструмент для виртуализации. Он распространяется бесплатно, с открытым исходным кодом. VirtualBox позволяет устанавливать в качестве «гостевой» практически любую современную операционную систему, Windows, MacOS или любой из многочисленных представителей семейства Linux.

Преимуществом VirtualBox является простой и понятный пользовательский интерфейс. Хорошо сделан перевод на русский язык. Все основные функции вынесены в виде кнопок под меню. Создание виртуальных машин выполняется с помощью пошагового мастера [4, 5].

VirtualBox поддерживает работу с сетями, поэтому ваша виртуальная ОС может быть легко связана с локальной сетью или Интернетом. Очень полезной является функция «снимков» операционной системы.

Второе важное преимущество: предустановка по умолчанию на всех хоста в учебных корпусах университета.

Под лабораторный практикум был создан образ виртуального жесткого диска, в котором были проведены необходимые настройки прав пользователей и политики безопасности, а также установлен пакет офисных программ LibreOffice 4.1, необходимый для создания отчета. Файл образа был размещен на сетевом ресурсе университета и стал доступен для скачивания во всех учебных корпусах.

Первое практическое занятие почти полностью посвящено созданию, настройке и запуску виртуальной машины. Перед созданием ВМ студент запускает процесс скачивания образа виртуального жесткого диска с сетевого ресурса в новую папку на хосте (процесс может занимать от нескольких минут до полутора десятков минут). За это время студент успевает создать и настроить ВМ.

После успешного запуска ВМ и гостевой ОС для освоения работы с ВМ студент выполняет лабораторную работу «Основы работы в командной строке» (студенты, зачастую, не представляют как можно взаимодействовать с компьютером через «черный квадрат»).

На следующем практическом занятии настройка рабочей станции начинается с изменения имени компьютера. Необходимость присвоения уникального имени виртуальной рабочей станции обусловлена тем, что на всех ВМ используется один и тот же образ жесткого диска с именем Labs1. Студенты присваивают своим рабочим станциям уникальные номера, связанные с полным именем хост-компьютера. Это упрощает идентификацию компьютера в сети, а также поиск и исправление ошибок подключения.

Соединение виртуальных рабочих станций в одноранговую сеть, как правило, не вызывает затруднений, создание и использование общих папок и назначение разрешений требуют только скрупулезности и внимания. К одной из виртуальных рабочих станций подключается локальный принтер. Установка драйвера производится в ВМ, после чего принтер объявляется общим ресурсом и ему присваивается сетевое имя.

Для включения виртуальной рабочей станции в домен студенты должны хорошо понимать, что такое IP-адресация, сети, подсети и методику их создания. Поэтому практическая работа «Адресация в IP-сетях» должна быть выполнена до попытки включения рабочей станции в домен.

И вот, наконец, студенты «созрели» для включения своей рабочей станции в домен. Они произвели необходимые изменения в настройках виртуальной машины, изменили параметры протокола TCP/IP и даже получили отклик от сервера. Но от какого сервера был получен отклик? В специализированной лаборатории развернут сервер UNIVER, но он обслуживает потребности внутренней учебной сети. В учебных классах этот сервер не доступен, что опять же, связано с политикой безопасности.

Для проведения полноценных занятий на любой площадке университета было принято решение и сервер для организации двухранговой сети развернуть на виртуальной машине. Как и в случае с рабочей станцией, для развертывания сервера был создан образ виртуального жесткого диска с развернутым на нем Windows Server 2008 Enterprise [6, 7]. В сервере были созданы необходимые роли и службы, параметры сетевого подключения, а также 25 доменных учетных записей и сетевых профилей пользователя. На общедоступной папке размещены файлы различного назначения: программы, текстовые документы, графические изображения, аудио и видеофайлы.

На компьютере преподавателя (или на одном из студенческих) создается виртуальная машина с параметрами и характеристиками, позволяющими развернуть Server 2008. Для серверной ВМ желательно выделить два процессора (если позволяет аппаратная часть хоста) и 1300-1500 Мб оперативной памяти.

После запуска и развертывания сервера преподаватель может наблюдать попытки подключения рабочих станций с серверу, регистрацию с доменной учетной записью, создание сетевых профилей пользователя и т.п., а также корректировать эти процессы [8-10].

После выполнения основного задания студенты могут, просмотреть общие ресурсы, доступные на сервере, определить какие файлы они могут открыть и если нет, то почему, скопировать заинтересовавшие их файлы на свою рабочую станцию и, если файл невозможно открыть, т.к. на рабочей станции отсутствует необходимая программа, установить ее, скачав дистрибутив с сервера (возможность получения прав локального администратора остается).

Такие упражнения позволят студентам закрепить знания и умения, необходимые для овладения основами работы с компьютерными сетями различного назначения.

В заключении хочется отметить, что подавляющее большинство вышеперечисленных манипуляций невозможны на хостах учебных классов, а драйвер для принтера есть только в гостевой ОС. В виртуальной машине студенты могут проводить эксперименты с операционной системой «до посинения экрана». Работоспособность ВМ восстанавливается в течение нескольких минут. При этом аппаратно-программному комплексу хоста ничего не угрожает.

Литература:

1. Буйневич М.В., Васильева И.Н. Информационная безопасность и защита информации: учебное пособие. – СПб.: СПбГИЭУ, 2011. − 175 с.
2. Обзор виртуальных машин разных разработчиков [Электронный ресурс]. URL: https://ustanovkaos.ru/ustanovka-neskolkix-os/virtualnaya-mashina.html (дата обращения: 28.10.2018).
3. Васильева И.Н., Родин В.Н., Чернокнижный Г.М. Использование средств виртуализации в преподавании ИТ-дисциплин // Вестник Санкт-Петербургского университета МВД России − № 1 (77) январь – март 2018 г. – С. 148-154 [Электронный ресурс]. URL: http://www.univermvd.ru/files/other-files/№_1_(77)_2018_сжат.pdf (дата обращения: 28.10.2018).
4. Поисов Д.А. Начинаем работать с VirtualBox (для чайников), 12.12.2014 [Электронный ресурс]. URL: http://all-ht.ru/inf/vpc/VirtualBox.html (дата обращения: 28.10.2018).
5. Установка операционных систем на VirtualBox [Электронный ресурс]. URL: http://nastroyvse.ru/programs/review/kak-ustanavlivat-operacionnye-sistemy-na-virtualbox.html (дата обращения: 28.10.2018).
6. Установка Windows Server 2008 R2 на виртуальную машину, 05.01.2015 [Электронный ресурс]. URL: http://afirewall.ru/ustanovka-windows-server-2008-r2-na-virtualnuyu-mashinu (дата обращения: 28.10.2018).
7. WIN Sever 2008 на VirtualBox. Настройка сети и шары, 17.12.2015 [Электронный ресурс]. URL: http://slusar.su/win-sever-2008-na-virtualbox-nastroyka-seti-i-shary/ (дата обращения: 28.10.2018).
8. Чекмарев А.Н. Windows Server 2008. Настольная книга администратора – СПб.: БХВ-Петербург, 2009. – 512 с.
9. Поляк-Брагинский А.В. Администрирование сети на примерах. – СПб.: БХВ-Петербург, 2005. – 320 с.
10. Нестеров С.А. Администрирование в информационных системах: методические указания к лабораторным работам, 2010 [Электронный ресурс]. URL: http://saiu.icc.spbstu.ru/media/files/staff/nesterov/Administrirovanie_v_informacionnykh_sistemakh_lab_Nesterov.pdf (дата обращения: 28.10.2018).

Заключение

В монографии рассмотрены актуальные проблемы безопасности цифрового пространства, связанные с внедрением новых информационных технологий и форм организации хозяйствующих субъектов. Требования безопасности учитываются при моделировании различных аспектов функционирования информационных систем и построения систем защиты информации, которые требуют соответствующего теоретического обоснования, в частности в сфере понятийного аппарата. В монографии изложены подходы к построению онтологии информационной безопасности, управлению человеческим фактором и функцией контроля в системах защиты информации. Отдельное внимание посвящено обеспечению безопасности персональных данных при построении систем их обработки и защиты в организациях.

Проведен анализ отдельных технологий и средств защиты информации, в частности, рассмотрены вопросы интеллектуализации процессов поиска уязвимостей и антивирусной защиты. Рассмотрены криптографические функции, доступные в операционных системах Windows и в системах Интернет-коммуникации (мессенджерах), механизмы обеспечения целостности и конфиденциальности информации в системах управления базами данных, методы инженерно-технической защиты информации.

В заключении приведены методические разработки преподавателей кафедры вычислительных систем и программирования Санкт-петербургского государственного экономического университета, отражающие опыт использования современных образовательных технологий в области информационной безопасности.

Монография будет полезна преподавателям и специалистам по информационным технологиям и защите информации, аспирантам, магистрантам и студентам направлений «информационная безопасность», «информационные системы и технологии», «бизнес-информатика», а также других направлений при изучении дисциплин компьютерного цикла, экономическим специалистам, интересующимся применением современных информационных технологий и связанными вопросами информационной безопасности.

Научное издание

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЦИФРОВОГО ПРОСТРАНСТВА

Под редакцией Е.В. Стельмашонок, И.Н. Васильевой

Подписано в печать 26.12.18. Формат 60×84 1/16.
Усл. печ. л. 9,75. Тираж 500 экз. Заказ 1770.

Издательство СПбГЭУ. 191023, Санкт-Петербург, Садовая ул., д. 21.

Отпечатано на полиграфической базе СПбГЭУ