



ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ УНИВЕРСИТЕТ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ ИМЕНИ В.Я. КИКОТЯ»

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Сборник научных трудов

Всероссийской конференции

**«ТЕХНОЛОГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ»**

28 февраля 2019 г.

Московский университет МВД России
имени В.Я. Кикотя, 2019

ISBN 978-5-9694-0811-1

Москва
2019

ББК 67.4
А-43

Рецензенты:

начальник кафедры информационно-компьютерных технологий в деятельности органов внутренних дел Белгородского юридического института МВД России имени И.Д. Путилина **А. Н. Прокопенко**;
начальник кафедры информатики и математики Краснодарского университета МВД России **И. Н. Старостенко**

А-43 ***Актуальные проблемы обеспечения кибербезопасности*** :
сборник научных трудов XVIII Всероссийской конференции «Технологии информационной безопасности в деятельности органов внутренних дел», 28 февраля 2019 года. – М. : Московский университет МВД России имени В.Я. Кикотя, 2019. – 255 с.
ISBN 978-5-9694-0811-1

XVIII Всероссийская конференция «Технологии информационной безопасности в деятельности органов внутренних дел» посвящена методологическим и отраслевым проблемам информационной безопасности, их выявлению, нахождению решений и контролю.

Методологические проблемы технологий информационной безопасности рассматриваются через призму внедрения современных новых информационных технологий, технологий защиты систем хранения, распространения, обработки и передачи данных, технологий расследования компьютерных преступлений.

В сборник вошли статьи курсантов, молодых ученых и преподавателей, специализирующихся в сфере обеспечения кибербезопасности Российской Федерации. В них отражены проблемные вопросы контроля и правового регулирования безопасности государства, анализа угроз обеспечения кибербезопасности страны, а также противодействия преступности в сфере информационных технологий.

ББК 67.4

ISBN 978-5-9694-0811-8

Научное электронное издание

В авторской редакции
Компьютерная верстка *Абилова Ф. А.*
14,82 усл. печ. л

Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12
<http://www.mosu.mvd.ru>, e-mail: support_mosu@mvd.ru

СОДЕРЖАНИЕ

<i>Е. А. Борздыко, В. И. Лустин</i> Информационно-аналитическая работа	8
<i>З. В. Василенко, В. И. Лустин</i> Преимущества наличия интегрированной системы безопасности	12
<i>Д. Е. Гришина, В. И. Лустин</i> Расследование преступлений в сети интернет	15
<i>А. А. Дуваа, А. В. Пузарин</i> Интегрированные системы безопасности: понятие, структура и задачи	18
<i>Д. Л. Кашипов, В. И. Лустин</i> Общая характеристика преступлений в сфере компьютерной информации	23
<i>И. А. Нуреева, В. И. Лустин</i> Анализ угроз безопасности информации, связанных с деятельностью сотрудников ОВД	27
<i>Е. Е. Петыхина, В. И. Лустин, Л. О. Евраев</i> Применение сотрудниками ОВД специальных средств борьбы со взрывами	29
<i>Н. К. Рудакова, В. И. Лустин</i> Правовой институт защиты детей от информации, причиняющей вред их здоровью и развитию	35
<i>М. В. Рябинин, В. И. Лустин</i> Назначение и особенности применения технических средств обнаружения пожара и технических средств пожаротушения	39
<i>П. Р. Саулина, В. И. Лустин</i> Организация защиты персональных данных в ОВД	44
<i>Ю. М. Сметанина, В. И. Лустин, В. Н. Бормотин</i> Функционирование системы обеспечения комплексной безопасности объекта в условиях нештатных и чрезвычайных ситуаций	49
<i>А. А. Тетюхин, В. И. Лустин</i> Защита информации	54
<i>А. С. Федорова, В. И. Лустин</i> Понятие автоматизированного рабочего места	57
<i>И. А. Братских, Г. Г. Плотников</i> Передача конфиденциальной информации графическими методами на основе принципа самореферентности	61

<i>И. А. Братских, Г. Г. Плотников</i> Альтернативные направления развития средств связи. IP-телефония	65
<i>Н. А. Капусткин, А. В. Пузарин</i> Техническая защита объектов информатизации, реализуемая с помощью беспилотных летательных аппаратов	68
<i>Е. А. Корноухов, Д. В. Галиев</i> Практические аспекты применения интегрированных систем безопасности	72
<i>А. Н. Кожурина, О. А. Дворянкин</i> Киберпреступность	77
<i>Е. А. Макарова, Г. Г. Плотников</i> Системы централизованного управления охраной объектов	82
<i>В. А. Косянчук, П. В. Орехов</i> Анализ уязвимостей NFC-технологий	85
<i>Д. И. Галаев, А. Г. Большунов, Г. В. Петров</i> Специальные информационные технологии и их роль в противоборстве с терроризмом	89
<i>А. А. Атанова, К. Р. Аветисян</i> Профайлинг в деятельности ОВД.....	91
<i>Н. В. Гринченко, В. И. Казанцев</i> Характеристика хищений денежных средств с помощью вредоносных компьютерных программ	94
<i>Л. Р. Абдрахманова, А. Г. Большунов</i> Умные гаджеты.....	97
<i>А. Г. Белкина, А. В. Пузарин</i> Анализ современных технических средств защиты информации в проводных линиях связи	100
<i>Д. Р. Бельдеубаева, Е. Н. Клочкова</i> Механизм биткойн-ключа и эллиптические кривые над конечными полями	106
<i>А. Г. Волков, А. В. Пузарин</i> Странности в алгоритмах ГОСТ Кузнечик и Стрибог.....	116
<i>Д. В. Глебко, О. В. Пименова</i> Нейронные сети.....	120
<i>А. А. Дутикова, А. В. Пузарин</i> Восстановление информации с USB-накопителей в целях проведения судебно-компьютерной экспертизы	123

К. И. Ершов, А. В. Пузарин

**Исследования в области проектирования
системы защиты информации 126**

В. И. Ильина, В. И. Лустин

**Применение киберразведки органами внутренних дел
в борьбе с преступностью в информационной сфере 132**

П. О. Каменев, Е. Н. Клочкова

**Возможности применения стандартных математических
пакетов для решения задач оптимизации 136**

Е. А. Кожинская, В. И. Лустин

**Проблемы противодействия правонарушениям
в сфере высоких технологий 141**

В. В. Селицкий, Г. Г. Плотников

Искусственный спутник 144

Н. А. Крупин, Е. Г. Белоглазов

**Специализированные технические средства
исследования компьютерных носителей информации 147**

Е. А. Кручок, Г. Г. Плотников

Централизованная охрана объектов 153

И. В. Лебедев, В. И. Лустин

**Совершенствование системы правового противодействия
разглашению сведений, составляющих тайну предварительного
расследования по уголовным делам 161**

В. И. Лустин

**Управление информационной безопасностью
в органах внутренних дел 163**

В. И. Лустин, И. С. Мельцева

**Назначение технических средств обеспечения
безопасности объектов 166**

В. В. Мандрикова, О. А. Дворянkin

Обзор фреймворков для цифровой форензики 169

Г. Р. Молчков, А. В. Пузарин

**Проблема интеграции специализированного ПТО в отделы
и подразделения правоохранительных органов
на районном уровне 173**

<i>А. Э. Покинен, В. В. Щерба</i> Анализ безопасности современных веб-сервисов	177
<i>О. Л. Ришилина, П. В. Орехов</i> Особенности проектирования системы видеонаблюдения на объекте информатизации и для объектов информации ОВД	180
<i>М. С. Курбатова, А. В. Серезевский</i> Современные тенденции развития пожарной сигнализации	187
<i>О. В. Симаков, В. И. Лустин</i> Видеонаблюдение: юридические аспекты	190
<i>А. И. Садовников, А. В. Пузарин</i> Перспективы развития систем автоматической противопожарной защиты объектов, предпосылки и задачи	194
<i>Н. С. Карнаухов, К. К. Борзунов</i> Компьютерные преступления: история и тенденция развития	199
<i>А. А. Жилкина, А. В. Пузарин</i> Техническая защита информации	202
<i>Г. В. Черногоров, А. Г. Большунов</i> Методы исследования файловых систем	206
<i>Н. Ю. Петухова, А. В. Пузарин</i> Cisco – средство обеспечения безопасности	210
<i>Н. С. Попов, В. И. Казанцев</i> Перспективы применения технологии SOC в МВД России	213
<i>А. Д. Распутина, К. Р. Аветисян</i> Использование информационно-аналитических ресурсов в деятельности ОВД	217
<i>Т. Э. Тараканова, А. В. Пузарин</i> Основные методы контроля цифрового радиозэфира	224
<i>Е. И. Таранина, О. В. Пименова, Д. Мусоев</i> Обработка изображений, используемых в дактилоскопии	227
<i>М. И. Титова, Е. Н. Клочкова</i> Организация защиты данных в современных информационных системах МВД России	230
<i>Ю. В. Филимонова, П. В. Орехов</i> Анализ уязвимостей комплексной системы безопасности	234
<i>Р. М. Червонюк, Е. Г. Белоглазов</i> ОРМ «наблюдение» как форма компьютерной разведки	235

К. М. Шарова, А. С. Овчинский

Применение методов и использование средств информационно-психологического воздействия правоохранительными органами..... 238

В. В. Эльканов, Д. В. Галиев

Программное обеспечение, используемое в стеганографии в операционной системе Linux..... 242

Ф. Ф. Мамедова, Е. Д. Мигачева, О. Н. Колокольчикова, В. И. Алескеров

О преступлениях, совершаемых в системе дистанционного банковского обслуживания..... 245

Н. Л. Денисов

Вопросы квалификации преступлений в сфере компьютерной информации, сопряженных с терроризмом и экстремизмом..... 250

Н. Ю. Ромашина, Н. Л. Денисов

Противодействие уголовно-правовыми средствами пропаганде терроризма и экстремизма в электронных СМИ 252

Борздыко Елизавета Александровна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Лустин Владимир Иванович²,
*старший преподаватель кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ РАБОТА

Успешное выполнение правоохранительных задач в условиях формирования новой социально-экономической и политической ситуации в стране неразрывно связано с обеспечением эффективности управляемыми органами внутренних дел, способствующие созданию нормальных условий для функционирования всей инфраструктуры общества.

Управление органами внутренних дел как разновидность социального управления должно осуществляться на уровне современных научных требований. Образование штабных подразделений и тылового обеспечения в структуре позволяет повысить эффективность управления и усовершенствовать работу по материально-техническому, финансовому и хозяйственному обеспечению.

Своевременными являются меры МВД России, направленные на сокращение документооборота путем решительного пресечения фактов истребования из органов сведений, не предусмотренных установленными формами статистической отчетности, ограничения количества истребуемых и направляемых управленческих документов структурным подразделениям МВД, ГУВД, УВД.

Информационные документы, предназначенные для начальника, должны быть краткими по содержанию, но отражающими все необходимые сведения, т. е. они должны быть информационно емкими.

Важное место в деятельности начальника ОВД занимают анализ и оценка оперативной обстановки. Информационной базой этой работы является главным образом статистическая информация о состоянии преступности и результате оперативно-служебной деятельности.

¹ © Борздыко Е. А., 2019.

² © Лустин В. И., 2019.

Накопителями указанной информации являются:

1. Единый журнал учета преступлений, уголовных дел (материалов, протоколов) и лиц, совершивших преступления. Информация в нем формируется на основании статистических карточек формы 1 – на выявленное преступление; формы 1.1 – о результатах расследования преступления; формы 1.2 – об установлении лица, совершившего преступление; формы 2 – на лицо, совершившее преступление; статистический талон формы 3 – о принятом решении по уголовному делу.

2. Журнал регистрации материалов, по которым вынесено постановление об отказе в возбуждении уголовного дела.

3. Книга учета заявлений и сообщений о преступлениях.

4. Журнал учета информации, поступившей в ОВД по телефону, телеграфу, в виде срабатывания приборов охранной сигнализации и иных сигналов о происшествиях.

5. Статистические отчеты о следственной работе (форма 1-Е, 1-ЕМ), о рассмотрении заявлений и сообщений о преступлениях (форма 2-Е).

С созданием штабов появилось возможность наиболее рационально организовать информационное обслуживание начальника внутренних дел.

Ежемесячно с нарастающим итогом штабом составляется для начальника справка о состоянии преступности, в которой предусматриваются данные по видам преступлений общеуголовной направленности, экономической направленности, совершенных в отчетном месяце. Также готовятся данные о раскрытии преступлений с учетом участия конкретных служб и подразделений. Наряду с этим, отдельно показывается работа по преступлениям, регистрируемым по линии аппаратов по борьбе с экономическими преступлениями.

Кроме общего анализа и оценки оперативной обстановки по городу (району) руководитель должен анализировать и оценивать конкретные направления борьбы с преступностью и охраны общественного порядка.

Источником для такого анализа в дополнение к цифровой статистической информации являются аналитические справки, подготавливаемые отраслевыми службами.

Совершенствование информационного обеспечения начальника связано также с применением технических средств, которые позволяют ускорить информационные процессы. Это достигается при помощи современных средств связи, использования промышленного телевидения в крупных ОВД.

Большие перспективы в совершенствовании информационного обеспечения деятельности руководителя открываются в связи с внедрением автоматизированных информационных систем на базе ЭВМ как на уровне МВД, ГУВД, УВД, так и на уровне ОВД.

На основе локальной сети были созданы и функционируют следующие системы и комплексы:

1. Информационная система «Поиск», которая ориентирована на сбор, хранение и обработку информации в рамках вычислительной сети в таких подразделениях, как начальник УВД, медвытрезвитель, дежурная часть муниципальных и городских отделений, дежурная часть ДПС, группа регистрации ГАИ, паспортный отдел, группа по лицензионно-разрешительной работе, служба участковых инспекторов, отдел дознания, ИВС.

В этой системе содержится информация в формализованном виде по следующим объектам:

- лица;
- уголовные дела;
- система учета;
- автотранспорт;
- оружие;
- вещи;
- объекты.

Система обеспечивает оперативный доступ пользователей к базам данных различного назначения непосредственно с рабочих мест сотрудников независимо от удаленности их рабочих мест сотрудников независимо от удаленности их рабочего места от места формирования и хранения данных.

Система предусматривает разграничение доступа пользователей к информации как средствами парольной защиты, так и средствами администратора данных. Последний позволяет создать на конкретном месте строго ограниченный набор функций, разрешенных к использованию.

2. Комплекс контроля дислокации и приданных сил УВД.

3. Комплекс ведения и контроля выполнения оперативно-тактических планов ОУВД.

4. Комплекс ввода и отображения оперативной информации по УВД и автоматизированного формирования оперативной сводки по УВД.

5. Комплекс ведения журнала инспекции и проверок УВД.

6. Комплекс накопления и использования неформализованной оперативной информации в подразделениях службы криминальной полиции УВД.

7. Комплекс «Финансовая часть ОВД». Помимо разработанного отделом совместно с другими фирмами программного обеспечения в ОУВД находятся в эксплуатации следующие системы, переданные отделу вышестоящими организациями:

- система проверки угнанного автотранспорта в рамках АСУ «Патруль»;
- дактилоскопический комплекс;
- программный комплекс для связи с ЗИЦ ГУВД;
- база данных абонентов Московской ГТС «Соната», позволяющая оперативному дежурному быстро узнать номер абонента МГТС;
- программный комплекс «Сводка ГУВД», благодаря которому оперативный дежурный формирует сводку происшествий в рамках требований ГУВД.

В настоящее время активно ведутся работы по созданию системы определения местоположения подвижного объекта и автоматизированного управления нарядами «Гранит», цифровой карты для нужд правоохранительных служб и информационного поля дежурной части УВД.

Василенко Зинаида Васильевна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Лустин Владимир Иванович²,
*старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ПРЕИМУЩЕСТВА НАЛИЧИЯ ИНТЕГРИРОВАННОЙ СИСТЕМЫ БЕЗОПАСНОСТИ

Каждый день владельцы различных предприятий и руководители организаций стремятся сделать необходимые шаги, чтобы вести свое дело в наиболее оптимальном направлении. В то время как прибыль, накладные расходы, персонал и различные улучшения занимают большую часть нашего внимания, мы склонны забывать один из самых важных аспектов: безопасность.

Безопасность – сложная проблема, которую мы склонны игнорировать, пока не стало слишком поздно. В современных условиях установка камер наблюдения или заключение контракта с поставщиком охранных услуг просто недостаточны с точки зрения безопасности.

Оптимальные решения безопасности могут быть достигнуты только путем интеграции систем безопасности, которые соответствуют уникальным требованиям каждого.

Что такое интегрированная система безопасности?

Интегрированная система безопасности принимает многоуровневые системы безопасности и объединяет их в одно решение. Примером можно привести следующие системы безопасности:

- видеонаблюдение;
- контроль доступа;
- тревога вторжения;
- служба охраны.

¹ © Василенко З. В., 2019.

² © Лустин В. И., 2019.

Перечислим положительные стороны интегрированных систем безопасности:

Эффективность

Управление в различных сферах сопряжено с огромным количеством задач высокого уровня, одной из которых является безопасность. Интегрированная система безопасности в любой отрасли позволит предприятиям и не только им процветать более эффективно и результативно.

Присвоение определенной роли конкретному человеку в отношении различных секторов интегрированной системы безопасности позволит члену команды использовать свои навыки более эффективно, что в конечном итоге гарантирует команде управления выполнение более обширных задач, что является грандиозным сдвигом в эффективности работы.

Централизация

Интегрированная система безопасности позволит централизовать операции по обеспечению безопасности. Команды управления и руководители теперь могут получать полный отчет из одной области, а не разговаривать со всеми областями своей интегрированной системы безопасности.

Это не только экономит время, но и обеспечивает более организованный рабочий процесс.

Предотвращение краж

Независимо от того в какой отрасли всегда есть вероятность неожиданной кражи. Будь то внутренняя или внешняя кража, она может нанести довольно значимый ущерб. Способы предотвращения подобных моментов – это интеграция специально разработанной системы безопасности.

Мониторинг в реальном времени

С несколькими системами безопасности, команды управления могут мгновенно видеть, что происходит на их объектах и в областях работы, если это необходимо.

Однако благодаря мониторингу в реальном времени эта задача превратилась в простую систему, доступную нажатием кнопки на телефоне, планшете или компьютере.

Разрешение конфликтов

Некоторые интегрированные системы безопасности поставляются с пакетом видеонаблюдения, контроля доступа, охранной сигнализации, систем охранного оповещения и службы охраны.

Все эти элементы проявятся, если на рабочем месте возникнет проблема, будь то внутренняя / внешняя кража со взломом, попытки взлома или любая угроза безопасности, которая может возникнуть.

Повышение производительности

В любой сфере интегрированная система безопасности является гарантией повышения производительности в рабочей области. Мониторинг сотрудников используется для повышения удовлетворенности клиентов, повышения производительности сотрудников и повышения производительности.

Это позволяет руководителям отслеживать деятельность своих сотрудников, поскольку это является одним из наиболее важных моментов в защите своего ведомства от нежелательных действий на рабочем месте.

Экономия

В конечном счете наличие интегрированной системы безопасности позволит сэкономить деньги и быть защищенным. В противном случае, в случае кражи, кражи со взломом или грабежа, руководители или команда управления будут нести ответственность за все убытки.

Благодаря интегрированной системе безопасности предприятия могут просматривать и выяснять, что произошло, почему это произошло или вероятность того, что эти события вообще не происходят.

Поэтому организациям необходимо проявлять инициативу в целях обеспечения безопасности своего бизнеса, так как отказ от интеграции новейшей системы безопасности может привести к повышенному риску серьезного нарушения безопасности.

Таким образом мы разобрали различные преимущества наличия интегральной системы безопасности.

Гришина Дарья Ефимовна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Лустин Владимир Иванович²,
*старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ В СЕТИ ИНТЕРНЕТ

С середины 1990-х годов киберпреступность резко возросла, а с 1995 г., интернет проник во все сферы жизнедеятельности человека, затронув и преступную сферу информационных технологий. Глобализация компьютерных сетей и информационных ресурсов привела к увеличению числа злоумышленников, которые используют свои навыки программирования, чтобы воровать деньги из банков и корпораций. Некоторые компании нанимают мошенников в качестве консультантов по безопасности, вместо того, чтобы отправлять их в тюрьму.

Каждый день тысячи людей во всем мире становятся жертвами компьютерной преступности. На сегодня увеличилось число случаев злоумышленничества с использованием виртуальных карт и переводов. Согласно данным МВД 70 % мошеннических попыток выманивания денег у людей происходит методом социальной инженерии. Так в 80 % случаев мошенники выводят денежные средства с банковских карт при помощи онлайн сервисов по переводу денег с карты на карту, представляясь при этом сотрудниками служб безопасности банков, а затем просят клиентов назвать код из СМС. Вот почему во всем мире правоохранительные органы занимаются проблемой кибербезопасности.

Любую форму кражи, мошенничества или эксплуатации, в настоящее время, можно осуществить с помощью компьютера и интернета. Самые распространенные компьютерные преступления включают в себя распространение детской порнографии, мошенничество с кредитными картами, промышленный шпионаж, преследование, взлом

¹ © Гришина Д. Е., 2019.

² © Лустин В. И., 2019.

и проникновение, вымогательство проституции, заговор, злонамеренные шалости и уничтожение имущества (вирусы), и это только малая часть преступлений, на которые способны злоумышленники.

Киберпреступность – это быстрорастущая область преступности. Все большее количество преступников используют сеть Интернет. Он получил свою популярность благодаря удобства использования, высокой скорости и, конечно же, анонимности. Такие преступления наносят серьезный вред и представляют собой настоящую угрозу для людей во всем мире.

Изначально киберпреступления осуществлялись отдельными людьми или небольшой группой. Сейчас существуют очень сложные и разнообразные кибер-криминальные сети, которые объединяют под своим началом множество людей со всего мира.

Криминальные организации все чаще используют всемирную паутину в своих злостных целях и, таким образом, максимально увеличивают свою прибыль в кратчайшие сроки. Сами преступления не обязательно новые (такие как кража, мошенничество, азартные игры, продажа наркотиков и запрещенных веществ), именно они наносят огромный ущерб всему человечеству, а распространение их происходит максимально быстро. Поэтому необходимость в следователях по киберпреступлениям неоспорима.

Как показывает практика, наиболее сложные преступления в сфере компьютерной информации совершаются с использованием возможностей, предоставляемых глобальными компьютерными сетями. Поэтому при раскрытии и расследовании данных преступлений исследуются следы, которые создаются не только в технических средствах пользователя (носителях), но формируются в каналах связи при передаче информации. Эта информация обычно состоит из двух частей: служебной (задающей маршрут передачи) и содержательной. Содержательная часть информации, несомненно, представляет основной интерес к расследованию и раскрытию преступлений, ведь именно эта часть включают сведения о преступной деятельности. Но служебная часть также важна, ведь она несет информацию о времени и месте совершения преступления, о связях преступника

Можно выделить следующие типичные следственные ситуации:

- компьютерное преступление произошло в условиях очевидности, характер и его обстоятельства известны (например, какую вирусную

программу и каким образом преступник загрузил в Интернет) и выявлены самими пострадавшими, кибер-преступник обнаружен и явился с повинной (задержан);

– известно, каким образом преступник совершил преступление, но механизм преступления в полном объеме неясен (например, произошел несанкционированный доступ к файлам законного пользователя через Интернет, через слабые места в защите компьютерной системы), преступник известен, но скрылся;

– налицо только преступный результат (например, дезорганизация компьютерной сети банка), механизм преступления и преступник неизвестны.

В случае возникновения первой ситуации, необходимо установить причинно-следственную связь между несанкционированным проникновением в компьютерную систему и наступившими последствиями (кража идентификационных данных, изменение настроек работы и т. д.), определить размеры ущерба¹.

В случае возникновения второй ситуации, необходимо объявить преступника в розыск и принять меры к задержанию преступника.

При условии, когда не известно ничего (третья ситуация), нужно установить механизм преступления.

Таким образом, с помощью всемирной паутины кибер-преступность вышла на новый уровень. Появляются новые виды преступлений, разрабатываются методы совершения старых. Необходимо совершенствовать методику и тактику раскрытия преступлений в сети Интернет, и конечно же, быть внимательным, чтобы самому не стать жертвой.

¹ Потапов С. А. Совершенствование расследования и раскрытия преступлений в сфере компьютерной информации // Социально-экономические явления и процессы. – 2016. – № 10 // URL: <http://cyberleninka.ru/article/n/sovershenstvovanie-rassledovaniya-i-raskrytiya-prestupleniy-v-sfere-kompyuternoy-informatsii> (дата обращения: 06.02.2018).

*Дуваа Антоний Анатольевич¹,
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

*Пузарин Андрей Валерьевич²,
начальник кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ИНТЕГРИРОВАННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ: ПОНЯТИЕ, СТРУКТУРА И ЗАДАЧИ

Тенденции современного развития систем безопасности неразрывно связаны с процессами широкой автоматизации и интеграции, которые касаются не только систем безопасности, но и всех остальных систем, предназначенных для автоматизации управления жизнеобеспечением и функционированием жилого здания, офиса, предприятия или любого другого объекта. Логическим развитием такой интеграции явилось создание интегрированных систем безопасности (ИСБ) с широкими функциональными возможностями, позволяющими автоматизировать также управление инженерными системами здания или объекта. Основой таких ИСБ служит единая аппаратно-программная платформа, представляющая собой автоматизированную систему управления (АСУ) с многоуровневой сетевой структурой, имеющую общий центр управления на базе локальной компьютерной сети и содержащую линии коммуникаций, контроллеры приема информации, управляющие контроллеры и другие периферийные устройства, предназначенные для сбора и обработки информации от различных датчиков (в том числе от извещателей пожарной и охранной сигнализации), а также для управления различными средствами автоматизации (оповещение, противопожарная автоматика и пожаротушение, инженерные системы и т. д.).

ИСБ представляют собой автоматизированную систему, обеспечивающую управление безопасностью различных объектов (жилых и офисных зданий, предприятий, комплексов сооружений и т. д.), сле-

¹ © Дуваа А. А., 2019.

² © Пузарин А. В., 2019.

довательно, на нее в полной мере распространяются положения «Комплекса стандартов и руководящих документов на автоматизированные системы». Например, ГОСТ 34.003 «Автоматизированные системы. Термины и определения» устанавливает следующие общие понятия.

Автоматизированная система; АС: Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Интегрированная автоматизированная система; ИАС: Совокупность двух или более взаимоувязанных АС, в которых функционирование одной из них зависит от результатов функционирования другой (других) так, что эту совокупность можно рассматривать как единую АС.

Интегрированная система безопасности (ИСБ) – совокупность технических средств (двух или более взаимоувязанных АС), предназначенных для построения систем охранной сигнализации, пожарной автоматики, контроля и управления доступом, и телевизионного наблюдения (охранного телевидения), которые обладают технической, информационной, программной и эксплуатационной совместимостью так, что эту совокупность можно рассматривать как единую АС.

Из этого определения также следует, что ИСБ это система, обеспечивающая защиту от нескольких видов угроз. В данном выше определении – ИСБ предназначена для защиты от пожара (пожарная сигнализация, оповещение, противопожарная автоматика) и от криминальных угроз (охранная сигнализация, контроль доступа, охранное телевидение).

Современные ИСБ строятся на основе иерархической сетевой структуры, в которую входят компьютерные сети, а также локальные сети различного уровня сложности специальных вычислительных устройств – контроллеров. Обобщенная структура ИСБ приведена на рисунке. В ней можно выделить четыре уровня сетевого взаимодействия.

Первый (верхний) уровень представляет собой компьютерную сеть типа клиент/сервер на основе сети интернет. Этот уровень обеспечивает связь между сервером и рабочими станциями операторов. Управление ИСБ на верхнем уровне обеспечивается посредством специализированного программного обеспечения (СПО). Современные возможности компьютерных сетей позволяют передавать информацию по различным каналам связи, тем самым на основе ИСБ можно создавать системы мониторинга безопасности удаленных объектов.

Второй уровень – уровень локальных контроллеров, основных компонентов управления ИСБ. Каждый контроллер должен обеспечивать выполнение функций в своей зоне контроля, даже при нарушении

связи с верхним уровнем ИСБ. Для связи между однородными контроллерами (горизонтальный уровень связи) используется интерфейс RS485 или другие интерфейсы, предназначенные для построения сетей промышленного уровня с хорошей помехозащищенностью и достаточной скоростью обмена данными.

Третий уровень – уровень адресных сетевых устройств, которые подключаются к каждому контроллеру второго уровня. Здесь, как правило, применяется интерфейс RS485. Количество сетевых устройств, подключаемых к одному контроллеру, может быть до 256. Номенклатура адресных сетевых устройств достаточно разнообразна, от простых расширителей для подключения радиальных ШС до сложных контроллеров третьего уровня, например, устройств управления пожаротушением или модулей подключения адресно-аналоговых пожарных извещателей.

Четвертый уровень – извещатели и оповещатели ОПС, считыватели и исполнительные устройства СКУД, датчики и устройства управления технологическим оборудованием и т. д. Здесь, как правило, применяются нестандартные специализированные интерфейсы и протоколы.

Технические возможности ИСБ позволяют определить дальнейшие перспективы их развития – интеграция с другими системами автоматизации и расширение видов и количества угроз, защита от которых обеспечивается с помощью ИСБ.

Тенденция дальнейшей интеграции – объединение ИСБ с системами автоматизации и управления инженерными системами здания или объекта связана с появлением термина – «интеллектуальное здание». Этот термин, по большей части, применяется к жилым и офисным зданиям. Для промышленных и производственных объектов интеграция систем дает возможность построения комплексов, в которых автоматизация производственного процесса или основного функционального назначения объекта тесно связана с обеспечением безопасности, как собственно объекта, так и человека от различных видов угроз, которые могут возникнуть на объекте в результате его функционирования. В этом случае более точно использовать понятие АСУ ФЖБ.

«Интеллектуальное здание» – комплекс проектных, организационных, инженерно-технических, программных решений, направленных на создание единой информационно-управляющей инфраструктуры, обеспечивающей гибкую и эффективную технологию обслуживания здания (объекта) и наиболее полно отвечающую потребностям

его владельцев и арендаторов с соблюдением современных требований обеспечения безопасности.

АСУ ФЖБ – автоматизированные системы управления функционированием, жизнеобеспечением и безопасностью объекта.

Процесс создания системы безопасности объекта включает в себя ряд этапов, основные из которых это проектирование, монтаж, пуско-наладочные работы, сдача в приемку заказчику. Так или иначе при создании системы безопасности на конкретном объекте приходится использовать принцип интеграции, так как на каждом объекте должны присутствовать системы защиты от нескольких угроз (как минимум, пожарная сигнализация и охранная сигнализация), соответственно проектирование обязательно включает в себя решение вопросов интеграции систем.

Принципы проектирования ИСБ во многом определяются способом интеграции, который можно разбить на четыре основных уровня (платформы интеграции):

- интеграция на проектном уровне (проектная платформа) – объединение разнородного оборудования, специально не предназначенного для построения ИСБ, только на этапе проектирования системы;

- интеграция на программном уровне (программная платформа) – объединение оборудования разных производителей, на базе специально разработанного для интеграции программного продукта и управления системой на базе ПЭВМ общего назначения или ЛВС ПЭВМ;

- интеграция на аппаратно-программном уровне (аппаратно-программная платформа) – объединение оборудования и программного продукта единого производителя и управления системой на базе ПЭВМ общего назначения или ЛВС ПЭВМ;

- интеграция на аппаратном уровне (аппаратная платформа) – объединение оборудования и программного продукта единого производителя и управления системой без использования ПЭВМ общего назначения, на основе специализированных высокопроизводительных контроллеров и ЛВС на их основе.

Каждый объект, на котором создается система безопасности, является уникальным, поэтому каждая проектируемая система представляет собой продукцию единичного производства, создаваемую заново для каждого конкретного объекта.

Процесс проектирования при создании системы играет важнейшую роль, так как именно на этапе проектирования закладываются все не-

обходимые качественные характеристики системы. При проектировании важнейшим вопросом является выбор технических средств, из которых будет создаваться система.

Здесь под техническими средствами ИСБ понимаются – технические изделия, представляющие продукцию серийного производства, специально предназначенную для построения ИСБ.

Таким образом при использовании термина ИСБ необходимо уточнение:

- ИСБ – это проектируемая система, продукт единичного производства для каждого конкретного объекта.
- ИСБ – это комплекс технических средств, продукт серийного производства.

ИСБ в любом случае представляет собой сложную техническую систему и при ее создании приходится использовать различное оборудование, как по функциональному назначению, так и оборудование разных производителей. При этом всегда встает задача совместимости оборудования. Причем она включает в себя две составляющие.

Первая – задача обеспечения взаимодействия оборудования различных подсистем, объединенных в ИСБ.

Вторая – совместимость оборудования разных производителей.

Эти задачи должны быть решены на этапе проектирования ИСБ и могут быть оптимизированы в рамках выбора способа (платформы) интеграции.

Кашипов Дмитрий Леонидович¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Лустин Владимир Иванович²,
*старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Понятие компьютерной информации

Технический прогресс неудержим. Современный компьютер превосходит своих крупногабаритных предков по множеству параметров. Изменилась и сфера применения компьютеров. Границы ее заметно расширились. С каждым днем во всем мире увеличивается число пользователей всемирной компьютерной сети Интернет, вместе с тем увеличивается и объем передаваемой между пользователями информации. Данная информация разнообразна. Она может быть, как открытой, так и конфиденциальной. Передаваться через различные источники.

Определение «информация» содержится в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». В ст. 2 «Основные понятия, используемые в настоящем Федеральном законе» поясняется, что информация – «сведения (сообщения, данные) независимо от формы их представления». Также в данной статье содержится и определение конфиденциальности информации – «обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя».

Следует отметить, что термина «компьютерная информация» в данном законе нет. Данный термин законодательство Российской Федерации установило в ст. 272 УК РФ примечание 1 «под компьютерной ин-

¹ © Кашипов Д. Л., 2019.

² © Лустин В. И., 2019.

формацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

Данную формулировку можно назвать несовершенной, так как для передачи информации возможно использование не только электрических сигналов, но и световых сигналов либо электромагнитное излучение.

Сигналом являться любой физический процесс, параметры которого могут изменяться в соответствии с передаваемым сообщением. «Говорить о «хранении» сигнала, в отличие от содержащейся в нем информации, с точки зрения физики абсурдно», – М. В. Старичков в своей работе «Понятие «компьютерная информация» в российском уголовном праве».

Осознавая несовершенство толкования, ученые выдвигают свои предложения, но они не решают главной задачи – разграничение компьютерной информации от других форм ее представления.

Понятие и виды преступлений в сфере компьютерной информации

Общей чертой для всех видов преступлений в сфере компьютерной информации является присутствие в них неправомерных действий, в которых используются компьютерные сети или вредоносные программы в корыстных целях. Данное вмешательство может нанести непоправимый вред здоровью человека, отрицательно влиять на экономику отдельной компании или даже страны, привести к открытому конфликту или политическому противостоянию между государствами.

В главе 28 УК РФ (преступления в сфере компьютерной информации) предусматривает четыре статьи, которые перечисляют виды неправомерной деятельности с использованием компьютеров и программного обеспечения, признаваемой правонарушающей в отношении государства, частных или юридических лиц.

Статья 272 рассматривает способы и формы неправомерной манипуляции с цифровыми сведениями, которые находятся в статусе охраняемых законом. В ней указаны те условия, которые смягчают или ужесточают конечный вердикт обвиняемой стороне.

Статья 273 содержит информацию о наказании в связи с неправомерной деятельностью, несущей опасность при использовании компьютерными программами.

Статья 274 перечисляет те действия, которые относятся противозаконным и возникают за несоблюдением регламента эксплуатации вспомогательных и основных средств для резервирования, обработки

или передачи охраняемой компьютерной информации между отдельными единицами ЭВМ и периферийной техники.

Статья 274.1. содержит характеристику действий, которые считаются неправомерным поведением по отношению к охраняемой критической информационной структуре Российской Федерации.

Анализируя главу 28 УК РФ, можно выделить следующие действия, которые являются правонарушениями:

- подмена вводимого пароля и доступ к защищенным сведениям;
- несанкционированный доступ в работу компьютерных сетей;
- действия по внедрению вредоносного программного обеспечения, с целью заражения средств хранения, обработки или передачи охраняемой законом информации;
- использование программного обеспечения без прав законного доступа;
- несанкционированный доступ к личной информации для ознакомления, удаления или использования в корыстных целях;
- модификация со злым умыслом действующих программных продуктов;
- подмена запросов, сетевых ресурсов с целью выведывания конфиденциальных данных;
- создание продуктов, мешающих другим пользователям применять принадлежащие им по праву компьютерные программы;
- распространение вредоносных программных продуктов для изменения работы действующих сервисов, похищения данных;
- уничтожение информации, которая не принадлежит лицу.

Выявление преступных деяний требует значительных усилий, так как правонарушителю легче всего уничтожить следы своего вмешательства и избежать судебного обвинения. Данные лица хорошо владеют компьютерными технологиями имеют технические и разрешительные возможности для негласного выхода к информации ограниченного доступа.

Для получения оснований для обвинения нужно:

- выявить местоположение доступа к информации;
- определить конкретное время совершения преступления;
- определить способ несанкционированного доступа;
- найти причастное лицо, определить двигавший ими мотив;
- определить данные о последствиях преступления.

Отдельно необходимо добавить применение компьютерной информации в мошенничестве. В частности, это может быть конфиденциальная, уникальная или опасная информация в виде файлов с текстом, графикой, аудио и видеоданными.

Правонарушитель может с корыстной целью использовать чужие или собственные данные, уничтожать их, нарушать работу компьютерных устройств или сетей.

Признаками компьютерного мошенничества являются:

1) ввод данных со злым умыслом и с помощью интерфейса либо путем использования шифра, записанного посредством копирования на съемный носитель информации;

2) преступная коррекция данных путем ручного ввода подменных сведений или с помощью вредоносных программ;

3) безвозвратное уничтожение данных, в том числе чужих личных сведений или алгоритмов, необходимых для корректной работы компьютерных программ;

4) внесение со злым умыслом или по незнанию изменений в работу программ, обеспечивающих доступ к продуктам на основании получения правильного разрешающего кода;

5) сознательное и умышленное вредоносное воздействие на рабочие характеристики чужих компьютеров, периферийной техники.

Стоит отметить, что обвинение и вынесение приговора за компьютерное мошенничество регламентируется ст. 159.6 УК РФ.

Непосредственным объектом в данных преступлениях с использованием компьютерной информации являются: определенная компьютерная информация, используемая на одном электронном носителе или имеющиеся общественные коммуникации, связанные с цифровыми данными, обеспечивающими взаимодействие отдельных элементов этой системы.

*Нуреева Ирина Альбертовна¹,
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

*Лустин Владимир Иванович²,
старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННЫХ С ДЕЯТЕЛЬНОСТЬЮ СОТРУДНИКОВ ОВД

Согласно «Доктрине информационной безопасности», утвержденной Президентом Российской Федерации от 09 сентября 2000 г. под угрозой информационной безопасности понимается потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности или секретности информации. Для полного анализа угроз защищаемой информации необходимо проанализировать источники угроз информационной безопасности ОВД, источники утечки и способы несанкционированного доступа к информации ограниченного доступа.

Потенциальными источниками угроз информационной безопасности ОВД являются лица или организации, заинтересованные в краже, копировании, разглашении, искажении или уничтожении конфиденциальной информации, принадлежащей ОВД³.

Средства массовой информации являются одними из самых заинтересованных лиц в получении информации ограниченного доступа. Для повышения своего рейтинга, получения дополнительных доходов средства массовой информации могут создать условия для разглашения информации ограниченного доступа, публикуя в своих изданиях, теле трансляциях данную информацию. Кроме того, в этот же источник можно отнести и специалистов, докладчиков на различных конференциях и выступлениях, которые так же являются потенциальным источником угрозы информационной безопасности ОВД.

¹ © Нуреева И. А., 2019.

² © Лустин В. И., 2019.

³ Степанов Е. А. Управление персоналом : персонал в системе защиты информации : учебное пособие. М. : ФОРУМ, ИНФРА-М, 2002.

Сотрудники ОВД, в своей непосредственной работе, сталкивающиеся с информацией ограниченного доступа, образуют второй источник угроз информационной безопасности ОВД. В данном случае имеется в виду такие методы как подкуп, шантаж, склонение к сотрудничеству, установка доверительных отношений и другие. Конечно же, для данного источника угроз информационной безопасности ОВД соответствует определенная категория сотрудников. К такой категории следует отнести сотрудников, имеющих определенные черты характера, такие как – обидчивость, тщеславие, излишняя разговорчивость, наглость и т. д.

Под противниками органов внутренних дел понимаются преступники, правонарушители, лица, ранее судимые, а также лица, заинтересованные в получении информации ограниченного доступа и в нанесении ущерба ОВД, мешающие правильной работе ОВД.

На безопасность информации посягают различного вида угрозы.

Если говорить об угрозах информационно-технического характера, можно выделить такие элементы, как кража информации, вредоносное программное обеспечение, хакерские атаки, спам, халатность сотрудников, аппаратные и программные сбои, финансовое мошенничество, кража оборудования.

Среди внутренних угроз безопасности информации выделяют нарушение конфиденциальности информации, искажение, утрата информации, сбои в работе оборудования и информационных систем, кража оборудования. И опять же, опираясь на статистику, наибольшее распростра

Технические средства обработки и передачи информации являются одним из распространенных источников и каналов утечки конфиденциальной информации. Так или иначе утечка информации зачастую происходит из-за «человеческого фактора».

В ОВД значительная часть документооборота осуществляется с помощью компьютерной техники, а это делает его уязвимым для шпионажа, если не принимать необходимые меры защиты.

Из проведенного анализа угроз защищаемой информации, исходящих от сотрудников, которые работают с информацией ограниченного доступа, следует, что основным направлением работы по совершенствованию информационной безопасности является организация деятельности сотрудников по защите информации.

Петыхина Екатерина Евгеньевна¹,
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя

Лустин Владимир Иванович²,
старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя

Евраев Леонид Олегович³,
доцент кафедры огневой подготовки
учебно-научного комплекса специальной подготовки
Московского университета
МВД России имени В.Я. Кикотя

ПРИМЕНЕНИЕ СОТРУДНИКАМИ ОВД СПЕЦИАЛЬНЫХ СРЕДСТВ БОРЬБЫ СО ВЗРЫВАМИ

В последние годы в Российской Федерации общественно опасные действия, связанные с использованием промышленных или самодельных взрывчатых веществ (ВВ), взрывных устройств (ВУ), часто приводят к совершению тяжких преступлений, сопряженных с посягательством на жизнь и здоровье граждан. Имеют место случаи гибели и ранения сотрудников правоохранительных органов, участвовавших в проведении работ, связанных с обнаружением и обезвреживанием взрывных устройств, а также в осмотрах мест взрывов и изъятии взрывоопасных объектов.

Причинами этого является отсутствие у большинства сотрудников навыков в обращении с ВУ, несоблюдение правил техники безопасности, неправильная организация осмотров мест происшествий и предварительных исследований.

¹ © Петыхина Е. Е., 2019.

² © Лустин В. И., 2019.

³ © Евраев Л. О., 2019.

Поступившая дежурному по ОВД информация о подобном происшествии, как правило, не содержит сведений, позволяющих сделать какие-либо выводы. Здесь возможно вести речь только о рациональной организации и обеспечении последующей работы исходя из условий безопасности граждан и участвующих в работе специалистов.

При выезде на место взрыва СОГ должна быть оснащена специализированными следственным чемоданом. Кроме того, в резерве необходимо иметь: оградительные ленты, наборы мелков (для изготовления предупредительных надписей и нумерации объектов); средства освещения (фонари, переносные лампы, удлинители); фото- и видеоборудование с достаточным запасом аккумуляторов и батарей; инструменты для разбора завалов мусора; инструменты для забора проб и изъятия образцов (включая стамески, шлямбуры, электроинструмент, наборы сит с ячейками разных размеров); навесы и укрывной материал для работы в неблагоприятных погодных условиях; упаковочные средства для изъятия и транспортировки вещественных доказательств, трупов и их фрагментов; спирт, ацетон, дистиллированную воду, стерильные бинты и марлю для производства смывов; достаточное количество пластиковых файлов, бумажных конвертов, планшеток, бланков протоколов, бумаги, шариковых ручек, карандашей, офицерских линеек, масштабных криминалистических линеек.

При работе на больших площадях и в многоэтажных зданиях важно иметь связь между участниками осмотра

Чтобы осмотр места взрыва был произведен качественно и эффективно, следует исходить из целого ряда условий:

1. Осмотр может производиться в зоне сильных разрушений и обрушений жилых и нежилых объектов, по итогам тушения возгораний и пожаров, при необходимости одновременного проведения неотложных аварийно-спасательных работ и при наличии пострадавших, нуждающихся в эвакуации и оказании медицинской помощи.

2. При осмотре на открытой местности возможны неблагоприятные погодные условия. Осмотр может происходить – при отсутствии электроснабжения, как на открытом пространстве, так и внутри зданий, помещений и т. д. В некоторых случаях возникает необходимость в проведении предварительных работ для обеспечения доступа к объектам осмотра.

3. Процесс осмотра места взрыва является длительным и трудоемким. Трудоемкость осмотров мест взрывов обуславливается тем, что они охватывают большие площади, определяемые расстоянием разлета

осколков и других элементов взорвавшегося устройства, предметов окружающей обстановки, максимальными дальностями проявления действия ударной волны, которые могут составлять сотни метров (а в случаях катастрофических взрывов – тысячи метров).

4. В ряде случаев, необходимо учитывать возможность наличия непрореагировавшего взрывчатого вещества, несработавших взрывных устройств, поврежденных систем электро-, газо-, тепло- и водоснабжения и т. д.

5. Сложность представляет обнаружение остатков ВУ и ВВ в зоне повреждений и разрушений. Орудия преступления – ВУ, ВВ – в значительной степени видоизменяются и разрушаются под воздействием взрыва, а их остатки часто присутствуют на месте взрыва в микро количествах. Для установления фактов и обстоятельств происшествия требуется фиксирование большого количества разрушений и перемещений окружающих объектов.

Взрыв, в зависимости от его мощности, вызывает те или иные, зачастую весьма существенные изменения окружающей обстановки, которые могут сопровождаться разрушениями, обрушениями, пожарами и т. д., что существенно осложняет производство осмотра места происшествия, отыскание следового материала и натуральных объектов для проведения экспертиз.

При возникновении пожара он должен быть ликвидирован до начала осмотра места происшествия, территория должна быть пролита, различные емкости с неизвестными наполнителями, сгоревшие и обгоревшие транспортные средства должны остыть.

При возникновении разрушений и обрушений зданий или сооружений и входящих в их состав помещений должны быть перекрыты ведущие к ним системы газо-, водо- и теплоснабжения, обесточены линии электроснабжения. Подключение этих систем или их части для обеспечения возможности качественного осмотра места происшествия возможно только после оценки ситуации и ликвидации опасности профильными специалистами. Причем подключение должно производиться тоже только профильными специалистами.

В случаях взрывов на химических производствах, в местах хранения и несанкционированного нахождения горюче-смазочных материалов, легковоспламеняющихся летучих жидкостей, ядовитых веществ и т. п. осмотр места происшествия может начинаться только после получения доклада сотрудников МЧС об их дезактивации.

При взрывах на магистральных газопроводах высокого давления не допускается начало осмотра до полного выгорания газа и остывания трубопровода.

При обнаружении на месте происшествия не среагировавших взрывчатых веществ, СВУ, боеприпасов, при возникшей утечке газа, при обнаружении масс летучих ГСМ и ЛВЖ, ядовитых и токсичных веществ и соединений необходимо немедленно эвакуировать всех людей с осматриваемой территории.

Основные задачи осмотра места происшествия, связанного со взрывом:

1. Исследование обстановки на месте происшествия в целях получения максимума информации о причинах, условиях возникновения, характере протекания взрыва и его последствиях, а также условиях, предшествующих взрыву.

2. Выявление, фиксация и изъятие материальных следов, определяющих непосредственную техническую причину взрыва и связанные с ним обстоятельства (объектов, несущих доказательственную информацию о событии взрыва).

3. Выявление, фиксация и изъятие следов, указывающих на конкретных лиц, причастных к происшествию.

4. Выявление условий, возникших после взрыва, угрожающих здоровью и жизни людей, для последующего принятия мер к их устранению.

По прибытии на место происшествия руководитель СОГ, прежде всего, предпринимает все меры для устранения опасности повторного взрыва. При наличии таковой все участники осмотра места происшествия должны быть удалены на безопасное расстояние. Радиус безопасного расстояния (с учетом максимальной ожидаемой мощности взрыва), возможность продления работ и степень опасности обнаруживаемых взрывоопасных объектов определяется специалистами в области взрывной техники.

Только после предварительного обследования места происшествия специалистом – взрывотехником, дающего возможность безопасного осмотра поврежденных сооружений, при отсутствии загазованности и химического либо радиоактивного заражения местности СОГ приступает к непосредственному осмотру.

Взрыв и его проявление всегда имеют только им присущие особенности и отличны друг от друга, что связано не только с большим многообразием используемых в преступных целях ВУ, но и с неповторяющимися обстоятельствами происшествия, а именно с условиями подготовки и осуществления взрыва. Выявление каких-либо конкретных

признаков взрыва на одном месте происшествия не означает их обязательного присутствия на другом месте взрыва. Однако выявление и фиксация наибольшего количества признаков – основная задача осмотра места происшествия, связанного со взрывом. Начальным этапом осмотра места взрыва являются обзор места происшествия, фиксация обстановки посредством фотографирования и видеозаписи, составление масштабного плана-схемы места происшествия. В процессе этого устанавливаются границы подлежащей осмотру территории или помещения, что определяется в каждом конкретном случае характером и степенью разрушений окружающих объектов и исходной информацией по обстоятельствам взрыва. С учетом проводимых спасательных и аварийно-восстановительных работ составляется дальнейший план действий СОГ. Только анализ общего характера разрушений и обобщение полученной информации на этом этапе позволяют перейти к более детальному осмотру отдельных участков места происшествия, и в частности зон наибольших разрушений объектов материальной обстановки (предполагаемого центра взрыва).

Именно центр взрыва определяет исходное положение разлетающихся осколков ВУ, не среагировавших частиц ВВ, распространение ударной волны и сжатых газов, оказывающих разрушающее и поражающее действие на окружающие объекты в радиальных направлениях. Поэтому установление центра взрыва, и его фиксация необходимы для облегчения последующего обнаружения следов взрыва, определения его природы, поиска частей ВУ, частиц ВВ и т. д., а также для определения схемы детального осмотра места происшествия.

Для извлечения металлических остатков ВУ из воронки (в грунте) используют магниты либо осыпавшийся грунт последовательно просеивают через сита с различными размерами ячеек. При наличии воронок в грунте, из нее должен изыматься материал массой не менее 1 кг, а также не менее одной сравнительной пробы на расстоянии нескольких метров от места взрыва и в том же количестве.

При взрыве в водоеме для исследования его дна на предмет обнаружения остатков ВУ применяются разного типа магнитные подъемники. Поиск остатков ВУ, внедренных в различные материалы, осуществляется с помощью металлоискателя, а их изъятие производится аналогично изъятию пуль и дроби. Однако при этом следует учитывать возможное наличие на остатках ВУ микроколичеств ВВ, сохранность которых необходимо обеспечить.

Отыскание частей непрореагировавших частиц ВВ бывает крайне осложнено имеющимися разрушениями. Практика показывает, что в следовых объемах они могут присутствовать на деталях обстановки вблизи центра взрыва, а также на деталях ВУ. Однако при взрыве порохов и пиротехнических составов разлет их непрореагировавшей части может составлять и несколько метров от центра взрыва. Отдельные частицы ВВ могут внедряться в мягкие ткани и материалы.

Изъятие следов ВВ с поверхностей некоторых пористых материалов (кирпич, бетон), обладающих способностью впитывать растворитель (ацетон, воду), целесообразно производить не с помощью смывов, а делая соскобы с них.

По официальным данным, ежегодно в России непосредственно от рук преступных элементов гибнет в среднем до 400 сотрудников. Учитывая смертность в дорожно-транспортных происшествиях, от несчастных случаев и других потерь, эта цифра возрастает до 1000 человек. До полутора тысяч сотрудников в год получают ранения при исполнении служебного долга. Вследствие длительных эмоционально-психологических перегрузок и стрессов количество самоубийств возросло до несколько сотен в год. Риск, как физический, так и психологический, является сегодня объективной составляющей в профессиональной деятельности сотрудников правоохранительных органов, и специальная работа по обеспечению их личной безопасности, то есть, целенаправленному уменьшению такого риска до реально возможного предела, чрезвычайно важна. Таким образом, обучение сотрудников органов внутренних дел тактике и методам обеспечения личной профессиональной безопасности, уверенным и грамотным действиям в экстремальных ситуациях выступает сейчас одним из важных направлений профессиональной подготовки кадров ОВД.

Рудакова Наталия Константиновна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Лустин Владимир Иванович²,
*старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ПРАВОВОЙ ИНСТИТУТ ЗАЩИТЫ ДЕТЕЙ ОТ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ИХ ЗДОРОВЬЮ И РАЗВИТИЮ

Актуальность вопроса защиты детей от информации, причиняющей вред их здоровью и развитию, обусловлена особой уязвимостью детей, которые в условиях интенсивного развития новых информационных технологий в наибольшей степени подвержены негативному информационному воздействию. Информация, распространяемая с использованием СМИ, информационно-телекоммуникационных сетей общего пользования все чаще оказывает на детей психотравмирующее и растлевающее влияние, побуждает их к агрессивному, жестокому, антиобщественному поведению, облегчает их вовлечение в преступления.

Во всем мире придается большое значение защите несовершеннолетних от вредной для них информации в целях обеспечения нормального физического и психического развития. Политика России в сфере обеспечения информационной безопасности несовершеннолетних является неотъемлемой составной частью общей политики государства в отношении детей. Именно поэтому цель моей статьи исследовать российское законодательство, регламентирующее право детей на защиту от информации, причиняющей вред их здоровью.

Под правами ребенка следует понимать принадлежащие ребенку от рождения неотъемлемые и неотчуждаемые основные права, и свободы человека и гражданина, установленные Конституцией Российской Федерации, а также специальные права, обеспечиваемые органами госу-

¹ © Рудакова Н. К., 2019.

² © Лустин В. И., 2019.

дарственной власти, органами государственной власти субъектов и органами местного самоуправления Российской Федерации в соответствии с действующим законодательством.

В настоящее время создана достаточная нормативно-правовая база, позволяющая контролировать информацию, получаемую детьми из средств связи. Рассмотрим подробнее ее составные элементы.

Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (далее в тексте – ФЗ-№ 436), (принят Государственной Думой Федерального собрания Российской Федерации в декабре 2010 г. и подписан Президентом в начале 2011 г.) и принятые к нему в дополнение поправки в отраслевое законодательство, а также подзаконные нормативные акты, распространяющиеся на оборот информации в средствах массовой информации, рекламе, интернете и других источниках, представляют собой реальные, высокоэффективные организационно-правовые механизмы защиты детей в современном информационном мире, такие как возрастная классификация и маркировка информационной продукции, введение временного раздела в теле-радиотрансляции взрослых и детских программ и передач, регламентация экспертизы информации, причиняющей вред здоровью и развитию детей, меры государственного и общественного контроля.

В ст. 2 ФЗ-№ 436 устанавливается особый термин, такой как информационная продукция для детей – информационная продукция, соответствующая по тематике, содержанию и художественному оформлению физическому, психическому, духовному и нравственному развитию детей. Такая продукция должна классифицироваться в зависимости от ее тематики, жанра, содержания и художественного оформления по возрастным категориям детей.

Под информационной безопасностью детей ФЗ-№ 436 предусматривает состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию. В вышеупомянутом законе введен дифференцированный подход к регулированию порядка распространения среди детей разных видов информационной продукции, способной нанести вред их здоровью и развитию, посредством регламентации мест ее реализации и предъявления специальных требований к ее оформлению.

Информационной продукцией называется предназначенные для оборота на территории Российской Федерации продукция средств массовой информации, печатная продукция, аудиовизуальная продукция

на любых видах носителей, программы для ЭВМ и базы данных, а также информация, распространяемая посредством зрелищных мероприятий, посредством информационно-телекоммуникационных сетей, в том числе сети Интернет, и сетей подвижной радиотелефонной связи.

Информация, причиняющая вред здоровью и (или) развитию детей, определена как информация (в том числе содержащаяся в информационной продукции для детей), распространение которой среди детей запрещено или ограничено в соответствии с данным законом.

К информации, запрещенной для распространения среди детей, относится информация:

- побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

- способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

- обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных данным Законом;

- отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;

- оправдывающая противоправное поведение;

- содержащая нецензурную брань;

- содержащая информацию порнографического характера;

- о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

Оборот информационной продукции, содержащей данную информацию в местах, доступных для детей, не допускается без применения

административных и организационных мер, технических и программно-аппаратных средств защиты детей от указанной информации.

К информации, распространение которой среди детей определенных возрастных категорий ограничено, относится информация:

- представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;

- вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;

- представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

- содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

Статья 6.17 КоАП РФ предусмотрена административная ответственность за нарушение законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, состоящая из трех составов.

Статья 13.21 КоАП РФ предусмотрена ответственность для средств массовой информации в случаях, если они нарушают установленный порядок распространения информационной продукции среди детей.

Кроме того, административная ответственность предусмотрена за изготовление юридическим лицом материалов или предметов с порнографическими изображениями несовершеннолетних и оборот таких материалов или предметов (ст. 6.20 КоАП РФ), пропаганду нетрадиционных сексуальных отношений среди несовершеннолетних (ст. 6.21 КоАП РФ), незаконное распространение информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), или нарушение предусмотренных федеральными законами требований к распространению такой информации, если эти действия (бездействие) не содержат уголовно наказуемого деяния (ч. 3 ст. 13.15).

В заключение хочу сказать, что необходимо усовершенствовать нормативную правовую базу и внести поправки в законодательные проекты, сужая рамки пропускаемой информации для детей и ужесточая административно-правовую ответственность.

Рябинин Михаил Владимирович¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Лустин Владимир Иванович²,
*старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

НАЗНАЧЕНИЕ И ОСОБЕННОСТИ ПРИМЕНЕНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ОБНАРУЖЕНИЯ ПОЖАРА И ТЕХНИЧЕСКИХ СРЕДСТВ ПОЖАРОТУШЕНИЯ

Пожарные датчики-извещатели являются основными элементами систем обнаружения очага пожара. Прежде всего, от их чувствительности и помехоустойчивости зависит эффективность работы системы. В частном жилье обычно используются дымовые, тепловые извещатели и приборы обнаружения открытого пламени. Как правило, все они являются «пороговыми», т. е. срабатывают в случае превышения контролируемым параметром заданного значения.

Дымовые извещатели. Дым – наиболее характерный признак пожара на самой ранней его стадии. Измерив концентрацию дыма в воздухе, датчик дает знать о наличии возгорания. Дымовые извещатели подразделяются на точечные и линейные.

Точечные производят замер в том месте, в котором установлены. В частном жилье из точечных извещателей используются только фотоэлектрические. Внутри такого устройства спрятана измерительная камера с источником света и фотоприемником. Частицы дыма, попавшие в камеру, изменяют светопрозрачность воздуха и рассеивают световой поток. Эти изменения и улавливает фотоприемник. Но в разных конструкциях по-разному. В одних он фиксирует общее ослабление светового потока (если расположен строго напротив источника света). В других – рассеяние потока (фотоприемник расположен под прямым углом к источнику света). Первые из описанных приборов более чувствительны, но зато менее устойчивы к помехам (например, к пыли)

¹ © Рябинин М. В., 2019.

² © Лустин В. И., 2019.

и нуждаются в частом техническом обслуживании. Вторые чуть менее чувствительны, зато более помехоустойчивы. Именно они в основном и используются при создании СПС в частном жилье. Крепятся обычно под потолком, поскольку горячие газы и дым поднимаются вверх. Контролируемая одним дымовым извещателем площадь может составлять до 80 м². Даже если метраж помещения, в котором устанавливается датчик, намного меньше этой величины, для повышения достоверности обнаружения возгорания следует устанавливать в нем не менее двух пожарных извещателей. При использовании подвесных потолков и прокладке за ними силовой электропроводки необходимо защитить запотолочное пространство отдельными дымовыми датчиками.

Обсудим эти вопросы на примере точечных дымовых извещателей. Чувствительность датчиков может быть высокой, средней и низкой, но обязательно должна находиться в пределах от 0,05 до 0,2 дБ/м (именно в таких единицах, пересчитываемых по довольно непростой формуле в объемные проценты, принято измерять чувствительность – стандартный дымовой датчик должен сработать, если задымление в месте его установки вызывает ослабление света на расстоянии 1 м на 1,1–4,5 %). В некоторых извещателях есть возможность регулировки чувствительности, которая производится специальным переключателем, устанавливаемым на задней стенке. Он может быть, как двухпозиционным (переключает с верхнего сразу на нижний предел), так и трехпозиционным (переключает с верхнего предела на нижний через средний, например, в сериях «Профи» и Leonardo от System Sensor). Лучше выбрать извещатель с трехпозиционным регулятором. Почему? Настроенный на верхний предел чувствительности, прибор реагирует на минимальное содержание дыма в воздухе и может «сработать» не только при курении в комнате, но и при жарке мяса или работе тостера на кухне (это «ложные срабатывания»). Минимальной чувствительности может оказаться недостаточно. Вам кажется, что датчик должен бы сработать, а он упорно «молчит». Вероятнее всего, вас устроит средний уровень чувствительности. А датчик с двухпозиционным регулятором именно его и лишен. Датчики любого типа нуждаются в периодическом уходе, точнее, техническом обслуживании. Почему оно необходимо? Понятно, что на находящихся под потолком приборах будут оседать испарения и пыль, оседают они не только на корпусах, но и внутри измерительной камеры, ослабляя световой поток, на который настроен прибор, и вызывая так называемое ложное срабатывание. На не осевшие (витающие в воздухе внутри камеры) частицы пыли датчик реагирует так же, как на дым. «Ложное срабатывание» неприятное явление для хозяев: ничего не горит, а датчик упорно сигнализирует. Хозяева же

при этом нервничают и ломают голову: «А вдруг в доме действительно что-то горит, а мы не замечаем?! Надо бы все еще раз проверить!» Чтобы предотвратить попадание пыли внутрь измерительной камеры, изготовители ограждают ее довольно сложной, почти лабиринтной конструкцией и усложняют геометрию корпуса, снижая тем самым вероятность «ложных срабатываний». Осевшую пыль, естественно, надо периодически удалять. Но если стереть пыль с корпуса ничего не стоит, то из ограждающего измерительную камеру «лабиринта» удалить ее бывает довольно непросто, протирая оптику, можно нарушить юстировку (оптика в данном случае используется весьма миниатюрная). В общем лучше поручить уход специалистам, которые будут периодически приезжать на дом.

Линейные дымовые извещатели. состоят из двух элементов, внешне напоминающих камеры видеонаблюдения, - излучателя и приемника-преобразователя. Они устанавливаются друг против друга на противоположных стенах комнаты («ИПДЛ» от «Полисервис», цена – 95 долл.; «СПЭК-2210» от «СПЭК», цена – 230 долл.; «6424» от System Sensor, цена 540 долл.). В последнее время появились модели, в которых оба элемента объединены в общем корпусе, в этом случае напротив излучателя находится отражатель («6200» и «6500» от System Sensor). Излучатель может быть либо инфракрасным, либо лазерным, работающим в видимом диапазоне красного света. Появление дыма в пространстве между передатчиком и приемником (или между приемопередатчиком и отражателем) вызывает ослабление принимаемого светового потока. Величину этого ослабления и фиксирует приемник – преобразователь, в случае превышения установленного порога формирует сигнал «Пожар».

Выгодны такие датчики исключительно для больших помещений, поскольку обнаруживают дым в зоне длиной от 10 до 100 м и шириной от 9 до 18 м (то есть обеспечивают контроль площади от 90 до 1 000 – 2 000 м²). Один линейный извещатель вполне способен заменить десяток точечных, что может оказаться выгодно не только экономически, но и с точки зрения дизайна помещения. Но есть и недостатки. Время срабатывания устройств зависит от объема и даже конфигурации помещения. «Ложное срабатывание» могут вызывать резкие изменения прямого и отраженного света, вспышки молний, а также изменение взаимного положения частей.

Тепловые пожарные извещатели. Чувствительными элементами тепловых извещателей могут быть: биметаллические пластины (например, в «ИП-103-5» от «КомплектсТройсервис»; «ИП 101-1А» от «Сибирского Арсенала»), полупроводниковые терморезисторы и т. п.

По принципу действия тепловые извещатели делятся на пассивные (контактные) и активные (электронные). Пассивные не потребляют электричества и функционируют следующим образом: когда температура в помещении достигает критической (порядка 70°C), чувствительный элемент либо вырабатывает определенный сигнал (за счет термоэлектрического эффекта), либо разрывает/замыкает контакт электрической цепи, подавая тем самым сигнал тревоги. Активные устройства потребляют электричество, зато выдают информацию не только о достижении критической температуры в охраняемой зоне, но, главное, и об изменении скорости повышения температуры. Их принято называть дифференциальными извещателями. Внутри их корпуса находится не один чувствительный элемент, а два- один непосредственно соприкасается с внешней средой, другой спрятан внутри корпуса. Если температура при возгорании растет быстро, прибор фиксирует разницу в показаниях чувствительных элементов и посылает на ПКП сигнал тревоги («МАК–ДМ» от НПП «Специнформатика», г. Москва, цена – 215 руб.; «ИП 115–1» от «Магнито-Контакт», г. Рязань, цена – 315 руб.; «5451 Е» от System Sensor). Если температура растет медленно (тогда температура элементов изменяется одинаково), прибор фиксирует превышение ею порогового значения и тоже посылает сигнал тревоги.

В результате, если пассивные тепловые извещатели подходят только для обнаружения пожаров с открытым пламенем, сопровождающихся резким превышением порогового значения температуры (срабатывают, когда уже точно что-то горит), то дифференциальные подают сигнал тревоги, когда еще нет открытого пламени, а температура лишь начала расти, но с недопустимой скоростью. Этим и объясняется то, что пассивные датчики в последнее время используются в системах сигнализации все реже (несмотря на цену, равную 15–20 руб.). Потребители предпочитают датчики пусть и более дорогие, но срабатывающие на более ранней стадии пожара- дифференциальные. Используются они обычно там, где дымовые пожарные извещатели выдавали бы ложные сигналы тревоги, например, на кухнях, в душевых, курительных комнатах и т. д. Для таких помещений, как котельные, где быстрое повышение температуры является обычным явлением, больше подходят пороговые детекторы на температуру 70°C – дифференциальные детекторы здесь будут давать ложные сигналы тревоги.

Оптические извещатели открытого пламени. Понятно, что любой очаг горения является источником оптического излучения в диапазоне от инфракрасного до ультрафиолетового. Обнаружение такого излучения с помощью фотоприемного устройства, имеющего высокую спек-

тральную чувствительность в ультрафиолетовой или инфракрасной области, но нечувствительного к видимой части спектра, и является задачей оптических извещателей открытого пламени.

В продаже можно найти в основном инфракрасные оптические приборы (например, серия датчиков «Пульсар» от КБ «Прибор», г. Екатеринбург, цена – от 1 360 до 2 200 р.; «Спектрон» от «НПО СПЕКТРОН»). Датчик в них может быть вмонтированным в приемник-преобразователь и выносным. В последнем случае датчик устанавливается непосредственно в контролируемой зоне и соединяется с приемником, устанавливаемым вне ее, оптоволоконным кабелем (длина до 20 м).

Оптические извещатели – малоинерционные устройства с минимальным временем обнаружения очага пожара. Угол обнаружения приравняется 90–120 м, дальность от 13 до 32 м. Они могут обнаруживать как тлеющие очаги, так и открытое пламя. Их недостаток состоит в том, что, если очаг горения заслоняют строительные элементы или мебель, извещатель его не зафиксирует. Незаменимы такие приборы там, где возможно быстрое возникновение пламени без дыма (гаражи, кладовые, помещения с электробытовой аппаратурой). Например, в гаражах, где возможно возгорание бензина и прочих нефтепродуктов, следует установить, как минимум два таких прибора, чтобы находящийся в центре автомобиль не загорел пламя.

Комбинированные извещатели представляют собой совмещенное устройство из двух датчиков в одном корпусе, управляемых одной микросхемой. Например, извещатель «ИП212/101–2» серии «Эко» от SYSTEM SENSOR (цена – 320 руб.) сочетает функции дымового оптико-электронного и теплового максимально дифференциального извещателя, благодаря чему срабатывает при любом возгорании (как при сопровождающемся задымлении, так и в бездымном, но с повышением температуры). Надо отметить, что комбинированные извещатели такого типа пользуются в последнее время популярностью, поскольку избавляют потребителей от необходимости монтировать в одном помещении два типа датчиков дымовой и тепловой (например, такая потребность возникает при установке извещателей в гаражах).

Саулина Полина Романовна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Лустин Владимир Иванович²,
*старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОВД

Необходимость обеспечения безопасности персональных данных в наше время объективная реальность. Информация о человеке всегда имела большую ценность, но сегодня она превратилась в самый дорогой товар. Информация в руках мошенника превращается в орудие преступления, в руках уволенного сотрудника – в средство мщения. Именно поэтому персональные данные нуждаются в самой серьезной защите.

Необходимость принятия мер по защите персональных данных вызвана также возросшими техническими возможностями по копированию и распространению информации. Уровень информационных технологий достиг того предела, когда самозащита информационных прав уже не является эффективным средством против посягательств на частную жизнь. Современный человек уже физически не способен скрыться от всего многообразия явно или неявно применяемых в отношении него технических устройств сбора и технологий обработки данных о людях.

С развитием средств электронной коммерции и доступных средств массовых коммуникаций возросли также и возможности злоупотреблений, связанных с использованием собранной и накопленной информации о человеке. Появились и эффективно используются злоумышленниками средства интеграции и быстрой обработки персональных данных, создающие угрозу правам и законным интересам человека. В настоящее время большое внимание в органах внутренних дел уделяется вопросам обеспечения информационной безопасности. Но если

¹ © Саулина П. Р., 2019.

² © Лустин В. И., 2019.

вопросы защиты государственной и служебной тайны регламентированы большим количеством нормативных методических документов и ведомственных приказов, то нормативное обеспечение защиты персональных данных недостаточно¹.

Конституция Российской Федерации 1993 г. в качестве высшей ценности провозгласила человека, его права и свободы, где соблюдение, защита прав и свобод человека и гражданина объявлены важнейшей обязанностью государства.

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее в тексте – ФЗ-№ 152)² определил высокоуровневые требования, которые затем были конкретизированы в подзаконных актах Правительства Российской Федерации и Министерства связи, нормативно-методических документах регуляторов Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Федеральной службы по надзору в сфере связи и массовых коммуникаций.

В соответствии с ФЗ-№ 152 персональными данными является любая информация, с помощью которой можно однозначно идентифицировать физическое лицо. К персональным данным относятся фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, принадлежащая субъекту.

В соответствии со ст. 3 ФЗ-№ 152 МВД России является оператором персональных данных, который организует и осуществляет обработку персональных данных, а также определяет цели их обработки, состав, подлежащий обработке.

Координацию и контроль деятельности по защите персональных данных при их автоматизированной обработке в МВД России осуществляет Департамент информационных технологий, связи и защиты информации МВД России, который является единым координирующим и контролирующим органом в системе МВД России по вопросам защиты персональных данных при их автоматизированной обработке.

¹ Методические рекомендации по обеспечению безопасности персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации.

² Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. – 2006. – № 31, ч. 1, ст. 3451.

Координацию и контроль деятельности по защите персональных данных при их автоматизированной обработке в МВД России осуществляет Департамент информационных технологий, связи и защиты информации МВД России, который является единым координирующим и контролирующим органом в системе МВД России по данным вопросам.

Определение угроз безопасности персональных данных при их обработке

Под угрозами безопасности персональных данных при их обработке в информационной системе персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе.

Персональные данные должны быть защищены от неправомерного или случайного доступа к ним, копирования, изменения, уничтожения, блокирования, распространения персональных данных, а также от иных неправомерных действий. Угрозы безопасности персональных данных могут быть связаны как с непреднамеренными действиями персонала информационной системы персональных данных и потребителей, пользующихся услугами, предоставляемыми информационной системой персональных данных в соответствии с ее назначением, так и со специально осуществляемыми неправомерными действиями иностранных государств, криминальных сообществ, отдельных организаций и граждан, а также иными источниками угроз.

Угрозы безопасности могут быть реализованы за счет утечки данных по техническим каналам (технические каналы перехвата информации при ее передаче по каналам связи, технические каналы утечки информации, обрабатываемой в технических средствах информационной системы, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа к персональным данным с использованием соответствующего программного обеспечения.

При формировании модели угроз особое внимание следует обратить на оценку актуальности угроз, связанных с наличием недокументированных возможностей в системном и прикладном программном обеспечении, используемом в информационной системе и определить тип угроз, так как в дальнейшем эти исходные данные позволят определить уровень защищенности персональных данных.

К актуальным относятся угрозы, которые могут быть реализованы в информационной системе персональных данных и представляют опасность для персональных данных. Уровень значимости информации, обрабатываемой в анализируемой информационной системе, определяется в зависимости от степени возможного ущерба для обладателя информации и оператора вследствие нарушения основных характеристик безопасности информации – конфиденциальности, целостности или доступности персональных данных.

Степень возможного ущерба определяется обладателем информации или оператором самостоятельно экспертным методом.

Уровень защищенности персональных данных – это комплексный показатель, который характеризует выполнение требований, способных нейтрализовать угрозы безопасности информационных систем персональных данных.

Защита информации в информационной системе персональных данных является составной частью работ по созданию и эксплуатации информационной системы персональных данных обеспечивается на всех стадиях ее создания и эксплуатации путем принятия организационных и технических мер защиты информации в рамках системы защиты персональных данных с учетом класса информационной системы, уровня защищенности и определенных актуальных угроз. Обеспечение защиты персональных данных, содержащихся в информационной системе персональных данных, осуществляется в соответствии с разделом III Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах с учетом раздела II Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Кроме того, формирование требований к системе защиты персональных данных необходимо осуществлять с учетом «Системного проекта подсистемы информационной безопасности единой системы информационно-аналитического обеспечения деятельности МВД России с учетом особенностей «облачной архитектуры»», утвержденного заместителем Министра внутренних дел Российской Федерации С. А. Герасимовым и постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

При адаптации базового набора допускается исключение мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе.

Практически каждая мера по защите персональных данных или их совокупность реализуется благодаря использованию какого-либо технического, программного или программно-аппаратного средства защиты информации. Применяемые средства защиты информации должны проходить оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации. Сертификацию средств защиты информации осуществляют федеральные органы: ФСТЭК России и ФСБ России.

Объекты информатизации МВД России, имеющие в своем составе информационные системы персональных данных, должны быть аттестованы по требованиям безопасности.

Обеспечение безопасности персональных данных

В соответствии со ст. 19 ФЗ-№ 152 оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для их защиты от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

Государство возложило на операторов персональных данных определенные обязанности. Важнейшим из них является обеспечение безопасности персональных данных. Это означает, что оператор персональных данных обязан принять все необходимые меры для обеспечения конфиденциальности сведений о субъектах персональных данных. Уполномоченные государством органы разработали требования по созданию системы защиты персональных данных и конкретизировали их в нормативно-методических документах.

В заключение следует подчеркнуть, современные методы по обеспечению безопасности информационных технологий в сфере защиты персональных данных базируются на первоисточнике проблемы, а именно возникновении угроз, создаваемых из корыстных целей. Основная задача – бороться с атаками, утечкой, несанкционированным доступом к персональным данным наиболее эффективно, соответствуя каждой характеристике вида угроз, чтобы данные мероприятия по защите проводились выгоднее как в трудоемком плане, так и в материальной составляющей.

Сметанина Юлия Михайловна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Лустин Владимир Иванович²,
*старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

Бормотин Владимир Николаевич³,
*преподаватель кафедры огневой подготовки
учебно-научного комплекса специальной подготовки
Московского университета
МВД России имени В.Я. Кикотя*

ФУНКЦИОНИРОВАНИЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ОБЪЕКТА В УСЛОВИЯХ НЕШТАТНЫХ И ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

Системы обеспечения комплексной безопасности создаются на объекте защиты с целью предупреждения и пресечения угроз, а также оперативной ликвидации их последствий.

Рассмотрим как должна функционировать система обеспечения комплексной безопасности в условиях нештатных и чрезвычайных ситуаций на объекте.

При возникновении на объекте чрезвычайной или нештатной ситуации основными задачами являются:

1. Оперативное выявление источника угрозы и получение максимально возможной и достоверной информации о том ущербе, который уже причинен или может быть причинен элементам защиты и объекту в целом.

2. Проведение анализа полученной информации, оценка ситуации, принятие решения о составе и объеме привлекаемых сил и средств,

¹ © Сметанина Ю. М., 2019.

² © Лустин В. И., 2019.

³ © Бормотин В. Н., 2019.

необходимых для пресечения или ликвидации последствий нештатной или чрезвычайной ситуации.

3. Организация оповещения и передача информации о чрезвычайном происшествии или нештатной ситуации привлекаемым силам.

4. Организация оперативных действий сил реагирования на объекте.

5. Привлечение средств для ликвидации последствий чрезвычайных и нештатных ситуаций, организация их взаимодействия для оперативного приведения объекта в штатный режим функционирования.

На первом этапе основное внимание следует уделять вопросу раннего обнаружения источника угрозы и выявления возможного ущерба. Если это пожар, следует применять адресно-аналоговые пожарные извещатели, которые не только обнаруживают возгорание на ранней стадии, но еще и выдают информацию о конкретном месте возгорания. Если это несанкционированное проникновение на объект, то желательно не только мгновенно получить сигнал тревоги от установленной сигнализации, но и также увидеть и зафиксировать нарушителя с помощью охранного телевидения, следует отметить, что очень важно не только своевременно получить тревожную информацию, но и получить ее в максимально возможном объеме для того, чтобы принять адекватные меры противодействия.

Чрезвычайная ситуация на объекте может развиваться быстро, и чтобы пресечь ее с минимальными потерями время реагирования должно составлять даже не минуты, а секунды, в этом случае без автоматических систем обеспечения безопасности не обойтись. Автоматические системы безопасности в обязательном порядке применяются на сложном и технологически опасном производстве, в системах обеспечения пожаробезопасности, а также в технологических установках систем жизнеобеспечения объектов. Если на объекте отключается электроэнергия, автоматика должна переключить электроснабжение на резервную линию или на автономный источник питания. Если на объекте возник пожар, по команде пожарной сигнализации должна включаться система оповещения и срабатывать автоматическое пожаротушение.

На втором этапе анализа нештатной или чрезвычайной ситуации необходимо оценить источник причинения ущерба с точки зрения возможного развития сценария. Если вооруженный нарушитель проник на объект, можно предположить, что он планирует совершить

ограбление или убийство. Если на пятом этаже прорвало трубу отопления, можно спрогнозировать, что за пол часа зальет горячей водой все нижние этажи. Оценка ситуации и проигрыш сценария необходим для выработки и принятия управленческого решения по пресечению дальнейшего развития НС или ЧС.

Приведенные примеры иллюстрируют достаточно простые ЧС на объекте, и принятие решения, в данных случаях, не является сложной задачей. Если происходит авария в тоннеле или взрыв на атомной электростанции анализ ситуации представляет собой очень сложную задачу, из вышесказанного можно сделать два вывода:

- чем сложнее объект и потенциально подвержен воздействию различного спектра угроз, тем серьезнее должна быть подготовка персонала;

- для принятия правильного решения по пресечению НС и ЧС на сложных, с точки зрения обеспечения безопасности, объектах внедряются автоматизированные системы принятия управленческого решения на основе использования компьютерных программ предусматривающих варианты действий при различных нештатных и чрезвычайных ситуациях и реализующие эти действия после команды ввода оператора.

Третий этап – это организация оповещения сил реагирования для пресечения нештатной или чрезвычайной ситуации на объекте. После оценки ситуации необходимо принять решение о привлечении сил и средств необходимых для пресечения НС или ЧС. Всем известны телефоны экстренной помощи 01,02,03 и 04, в крупных городах в настоящее время вводятся единые телефоны экстренной помощи (в г. Москве – 01). Однако для привлечения экстренной помощи необходимо еще знать телефоны служб, отвечающих за энергоснабжение, обслуживание лифтов, водоснабжение и канализацию, и другие, связанные со спецификой объекта. Для уменьшения времени прибытия оперативных и аварийно-спасательных служб на объекте должны быть прямые телефоны именно тех служб, которые обслуживают район, на территории которого расположен объект. На объекте должна быть схема оповещения руководства и ведущих сотрудников организации, для того чтобы вызвать их в нужное время.

Чем быстрее оперативные и аварийно-спасательные службы получают информацию о НС или ЧС на объекте, тем быстрее они придут на место и потери могут быть сведены к минимальным. Поэтому рекомендуется на объекте иметь схемы оповещения о НС

и ЧС, резервные и дополнительные средства связи, а также утвержденные должностные обязанности по оповещению и действиям в условиях НС или ЧС дежурных или лиц их заменяющих.

На четвертом этапе организации оперативного реагирования по пресечению НС или ЧС на объекте – наиболее важным является обеспечение скорейшего доступа сил реагирования к источнику угрозы на объекте и создание необходимых условий по его локализации. Если на объекте пожар, то необходимо обеспечить проезд пожарных машин на территорию, вскрыть нужные помещения, показать, где находятся гидранты, обеспечить эвакуацию людей и автотранспорта из опасной зоны. Если поступило сообщение о закладке взрывного устройства, еще до прибытия саперов необходимо эвакуировать людей из зоны действия возможного взрывного устройства. Существуют определенные нормативы, регламентирующие, на каком расстоянии должны находиться люди, в зависимости от массы и типа взрывчатого вещества.

В случае воздействия криминальных угроз на объект защиты больше внимания должно уделяться сохранению следов взлома или кражи, отпечатков пальцев, следов ног, крови и других вещественных доказательств, которые могут способствовать поиску преступников, служить доказательной базой для привлечения к ответственности. Лучше всего до прибытия оперативной группы оградить доступ людей на место преступления. После прибытия оперативной группы следует оказать помощь: по осмотру объекта, поиску преступников или похищенного «по горячим следам», опросу свидетелей и потерпевших, сбору другой информации, необходимой для раскрытия преступления.

Для того чтобы обеспечить грамотное и оперативное воздействие сил реагирования на источники угроз и минимизировать возможный или реальный ущерб, на объекте должны быть разработаны планы действий в нештатных и чрезвычайных ситуациях основанные на анализе наибольших рисков и оптимальном перечне мероприятий по обеспечению безопасности. Такие планы утверждаются руководителем объекта, являются неотъемлемой частью системы обеспечения комплексной безопасности и должны отрабатываться руководителями и персоналом объекта в ходе проведения обучения, тренировок и учений. По результатам тренировок и учений в эти планы вносят соответствующие корректировки до тех пор, пока планы действий не будут оптимальны, и соответствовать реальным возможностям по обеспечению безопасности на объекте.

Пятый этап включает в себя ликвидацию последствий НС и ЧС, приведение объекта в штатный режим работы.

Как уже было отмечено ранее, имидж фирмы, состоящий в основном из его материального положения, зависит от способности объекта защиты выходить из кризисных ситуаций с наименьшими потерями и в кратчайшие сроки. Одним из распространенных способов сохранения имиджа в кризисных ситуациях служит преднамеренное занижение реального ущерба. Однако эта мера носит временный характер, необходимо спланировать работу по ликвидации последствий так, чтобы она реально минимизировала ущерб.

В связи с этим рекомендуется не ждать катаклизмов, а заранее составить планы выходов организации из кризисных ситуаций. При формировании этих планов необходимо использовать анализ рисков, возможных потерь и эффективности мер по ликвидации последствий. На основе такого анализа создаются резервные фонды, проводится страхование рисков, разрабатываются запасные варианты организации предпринимательской деятельности, планируется привлечение дополнительных ресурсов. К разработке таких планов привлекают в первую очередь специалистов по экономической безопасности, но при участии руководителей и ведущих специалистов организации. Для проведения восстановительных работ непосредственно на объекте составляются планы-графики, в которых по дням расписывают перечень и объемы выполняемых работ и ответственных за их проведение. Завершением восстановительных работ и антикризисных мероприятий является приведение объекта в штатный режим работы, проведение полного анализа причин возникновения и последствий НС и ЧС, а также внесение соответствующих изменений в существующую систему безопасности с целью не допущения подобных ситуаций.

Тетюхин Артем Андреевич¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Лустин Владимир Иванович²,
*старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ЗАЩИТА ИНФОРМАЦИИ

XXI в. стал веком информационных технологий, в середине XX в. развитые капиталистические страны вступают в постиндустриальную фазу развития, происходят изменения в структуре общества, в сфере экономики и производства. Объем знаний и их производство постоянно растет, так возникает рынок информационных услуг и на повестку дня выходит вопрос информационной безопасности.

Для более детального разбора данной темы необходимо обратиться к определению понятий «информационная безопасность» и «безопасность информации». Первое включает в себя сохранность информационных ресурсов и защищенности законных прав личности и общества в информационной сфере. Второе подразумевает сохранность самой информации принадлежащей пользователю. Стоит отметить, что данные понятия взаимосвязаны. Формирование нашего современного информационного общества является важнейшим этапом в эволюции современной жизни людей, характеризующимся глобальным развитием информационных технологий, сетей, а также расширением глобального информационного пространства. Тут стоит обратить внимание на термин «информационные технологии» (ИТ), включающий в себя процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов. Информационная среда, которая создается за счет внедрения ИТ, определяет качество функционирования жизнедеятельности общества,

¹ © Тетюхин А. А., 2019.

² © Лустин В. И., 2019.

его уровень развития и безопасность, общество начинает функционировать на новом уровне благодаря информационному взаимодействию. Но для всего необходимо обеспечить должный уровень защиты информации, чтобы предотвратить появления угроз, связанных с искажением и раскрытием данных принадлежащих конечным пользователям.

Важнейшим аспектом информационной безопасности является выявление и классификация угроз. Угрозы информационной безопасности представляют собой совокупность факторов и условий, представляющих опасность для защищенной информации.

Методы воздействия на информацию подразделяются на два вида: искусственные и естественные. В свою очередь, человеческие угрозы включают преднамеренные и непреднамеренные.

К естественным угрозам относят: стихийные бедствия, пожары, наводнения, техногенные аварии и другие явления, не зависящие от человека.

К искусственным преднамеренным угрозам относится: кража (копирование) документов, подслушивание переговоров, несанкционированный доступ к информации, перехват информации, внедрение (вербовка) инсайдеров, фальсификация, подделка документов, диверсии, хакерские атаки и т. д.

К искусственным непреднамеренным угрозам относят: ошибки пользователей, неосторожность, невнимательность, любопытство и т. д.

Проблема защиты информации существовала долгое время до развития компьютерных технологий, а появление компьютеров только подняло ее на новый уровень. И, как показывает практика: лучший способ защиты от атак – это предотвращение атак. Защита информации не ограничивается только техническими методами. Основным недостатком защиты является человеческий фактор, поэтому надежность системы безопасности зависит от ее отношения к ней.

Чтобы поддерживать высокий уровень защиты, необходимо постоянно улучшать развитие современных технологий и технологий, можно сказать, что они идут в ногу со временем.

Сегодня формирование информационного общества является важнейшим этапом развития современного социума, превосходя по значимости остальные области функционирования человека. Информационные технологии, рассматриваемые, как фактор, оказывающий огромное влияние на глобальное развитие социума и формирование современной реальности, повлияли на жизнь и восприятие окружающего

мира обществом, расширили его возможности, поменяли приоритеты и ценности. Информационная среда определяет качество функционирования жизнедеятельности общества, его уровень развития и безопасность. При формировании данного направления необходимо обеспечивать должный уровень защищаемой информации для безопасного функционирования общемирового взаимодействия. Как сказал Натан Майер Ротшильд, кто владеет информацией, тот владеет миром.

Федорова Алина Сергеевна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Лустин Владимир Иванович²,
*старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ПОНЯТИЕ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА

Термин «автоматизированное рабочее место» (АРМ) возник в 70-е гг. прошлого столетия с появлением вычислительных средств, позволяющих вести автоматизированную обработку символьной информации (ЭВМ «Минск-32», ЕС ЭВМ 9003 и т. д.), трактовался как средство для создания систем автоматизации процесса проектирования и рассматривался в качестве одного из возможных вариантов разработки программных интегрированных пакетов. На начальных этапах автоматизированной обработки данных понятие это ассоциировалось с графическими проектными комплексами на базе мини-ЭВМ. Задачи в основном сводились к построению сложных схем, их модификации и отображению результатов проектирования с помощью различных графопостроителей. При таком подходе область применения АРМ была крайне узкой и касалась в основном машиностроения, радиоэлектроники, микроэлектроники и т. д., тех отраслей, где необходимо было выполнять графические и чертежные работы.

Ситуация коренным образом изменилась с начала массового выпуска персональных компьютеров. Сейчас уже трудно представить какие бы то ни были производство, организацию, функционирующие без применения персональных компьютеров, этим и обуславливается актуальность данной курсовой работы.

АРМ с персональным компьютером можно рассматривать как объект защиты, то есть необходимо понимание того, каким образом организовать его защиту для эффективного и безопасного использования, но в данной статье АРМ рассматривается как способ обеспечения ин-

¹ © Федорова А. С., 2019.

² © Лустин В. И., 2019.

формационной безопасности объектов. Возрастающие темпы информатизации общества повышают значение вычислительной техники в управленческих процессах. Использование возможностей современной вычислительной техники для автоматизации процесса обработки информации позволяет увеличить производительность труда, повысить эффективность работы с документами и ускорить обмен управленческой информацией.

Автоматизированное рабочее место – это комплекс среди вычислительной техники и программного обеспечения, располагающийся, непосредственно на рабочем месте сотрудника и предназначенный для инженера, проектировщика, бухгалтера и т. д.

Автоматизированные рабочие места должны создаваться строго в соответствии с их предполагаемым функциональным назначением. Однако общие принципы создания АРМ остаются неизменными, к ним относят: системность, гибкость, устойчивость, эффективность.

Под принципом системности понимается автоматизированное рабочее место должно представлять собой систему взаимосвязанных компонентов. При этом структура АРМ должна четко соответствовать тем функциям, для выполнения которых создается данное автоматизированное рабочее место.

Принцип гибкости имеет огромное значение при создании современных и эффективно работающих автоматизированных рабочих мест. Данный принцип означает возможность приспособления АРМ к предполагаемой модернизации как программного обеспечения, так и технических средств. В настоящее время, когда скорость устаревания программных и технических средств постоянно растет, соблюдение данного принципа становится одним из важнейших условий при создании АРМ. Для обеспечения принципа гибкости в реально работающих автоматизированных рабочих местах все подсистемы отдельно взятого АРМ выполняются в виде отдельных легко заменяемых модулей. Чтобы при замене не возникало проблем несовместимости, все элементы должны быть стандартизированы.

Большое значение имеет принцип устойчивости. Он заключается в выполнении заложенных в АРМ функций, независимо от воздействия как внутренних, так и внешних факторов. При возникновении сбоев работоспособность системы должна быстро восстанавливаться, неполадки отдельных элементов должны легко устраняться.

Принцип эффективности подразумевает, что затраты на создание и эксплуатацию системы не должны превышать экономическую выгоду от ее реализации. Кроме того, при создании АРМ надо учитывать, что

его эффективность будет во многом определяться правильным распределением функций и нагрузки между работником и машинными средствами обработки информации, ядром которых является ПЭВМ. Только при соблюдении этих условий АРМ становится средством повышения не только производительности труда и эффективности управления, но и социальной комфортности специалистов.

Практический опыт использования АРМ как одного из элементов распределенных систем управления позволяет выделить следующие требования к эффективно и полноценно функционирующему автоматизированному рабочему месту:

- своевременное удовлетворение информационных потребностей пользователя;
- минимальное время ответа на запросы пользователя;
- адаптация к уровню подготовки пользователя и специфике выполняемых им функций;
- возможность быстрого обучения пользователя основным приемам работы;
- надежность и простота обслуживания;
- дружественный интерфейс;
- возможность работы в составе вычислительной сети.

Задачи, решаемые на АРМ, условно можно разделить на информационные и вычислительные.

К информационным задачам относятся кодирование, классификация, сбор, структурная организация, корректировка, хранение, поиск и выдача информации. Часто информационные задачи включают несложные вычислительные и логические процедуры арифметического и текстового характера и отношения (связи). Информационные задачи являются, как правило, наиболее трудоемкими и занимают большую часть рабочего времени специалистов.

Вычислительные задачи являются как формализуемыми, так и не полностью формализуемыми. Формализуемые задачи решаются на базе формальных алгоритмов и делятся на две группы: задачи прямого счета и задачи на основе математических моделей. Задачи прямого счета решаются с помощью простейших алгоритмов. Для более сложных задач требуется применять различные математические модели.

Техническое обеспечение представляет собой комплекс технических средств, основой которого служит профессиональный персональный компьютер, предусматривающий работу специалиста без посредников (программистов, операторов и т. д.). У групповых АРМ таким компьютером могут пользоваться от четырех до шести человек. В ком-

плект профессионального персонального компьютера входят процессор, дисплей, клавиатура, магнитные накопители информации, печатающие устройства и графопостроители.

К комплексу технических средств следует отнести и средства коммуникаций для связи различных АРМ в сетях, а также средства телефонной связи.

Информационное обеспечение – это массивы информации, хранящиеся в локальных базах данных. Информация организуется и хранится, в основном, на магнитных дисках. Управление ею осуществляется с помощью программной системы управления базами данных, которая производит запись информации, поиск, считывание, корректировку и решение информационных задач. В АРМ может быть несколько баз данных.

Организационное обеспечение включает средства и методы организации функционирования, совершенствования и развития АРМ, а также подготовки и повышения квалификации кадров.

Для групповых и коллективных АРМ в подсистему организационного обеспечения включаются функции администрирования АРМ: проектирование, планирование, учет, контроль, анализ, регулирование, организационные связи с инфрасистемами и т. д.

Программное обеспечение состоит из системного программного обеспечения и прикладного. Основой системного обеспечения является операционная система и системы программирования. Системные программы обеспечивают рациональную технологию обработки информации. Так называемые сервисные программы, которыми АРМ комплектуется в зависимости от потребности в них, расширяют возможности операционной системы.

Технологии не стоят на месте, каждый год придумываются новые преступления, связанные с информационной безопасностью, и приходится придумывать новые способы борьбы с ними. АРМ с персональным компьютером – хорошее решение для защиты объекта. Во-первых, все процессы автоматизируются, минимизируется человеческий фактор. Во-вторых, так как само АРМ надежно защищается и существуют способы безопасного доступа к нему, то все процессы, осуществляемые при помощи него будут максимально надежны, а это повышает информационную безопасность на объекте. Иначе говоря, поскольку АРМ можно рассматривать как объект защиты и оно хорошо защищается, то АРМ как способ защиты работает максимально надежно.

Братских Илья Александрович¹,
*курсант факультета подготовки специалистов
 в области информационной безопасности
 Московского университета
 МВД России имени В.Я. Кикотя*

Плотников Герман Геннадьевич²,
*доцент кафедры информационной безопасности
 учебно-научного комплекса информационных технологий
 Московского университета
 МВД России имени В.Я. Кикотя*

ПЕРЕДАЧА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ГРАФИЧЕСКИМИ МЕТОДАМИ НА ОСНОВЕ ПРИНЦИПА САМОРЕФЕРЕНТНОСТИ

В 2001 году Джефф Таппер, профессор информатики Университета города Торонто (Канада), в своем докладе для ежегодной конференции по вопросам компьютерной графики (SIGGRAPH), организуемой по инициативе организации ACM SIGGRAPH, впервые представил научному сообществу самореферентную формулу автоматического построения изображений (впоследствии – формула Таппера) и разработанную им программу рисования графиков GrafEq.

Вот так выглядит формула Таппера:

$$\frac{1}{2} < \left[\text{mod} \left(\left\lfloor \frac{y}{17} \right\rfloor 2^{-17[x] - \text{mod}([y], 17)}, 2 \right) \right]$$

Так выглядит график формулы:

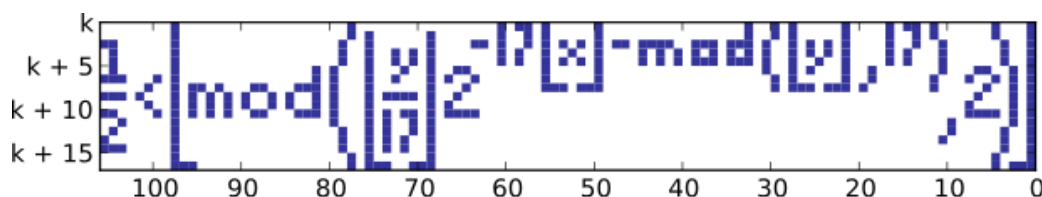


Рис. 1. График функции Таппера

Что же здесь поразительного? График формулы – это сама формула на графике. Она называется самореферентной формулой Таппера. На самом деле в этом графике есть небольшое жульничество. Это жульничество заключается в букве «к». Невозможно понять, что это за ордината, в отличие от абсциссы, которая охватывает область от 0 до 106.

¹ © Братских И. А., 2019.

² © Плотников Г. Г., 2019.

Чтобы увидеть данную картинку, нам нужно подняться на высоту «k» и не обращать внимание на все, что находится выше $k+17$ и ниже k , где $k = 4858450636189713423582095962494202044581400587983-244549483093085061934704708809928450644769865524364849997247024915119110411605739177407856919754326571855442057210445735883681829823754139634338225199452191651284348332905131193199953502413758765239264874613394906870130562295813219481113685339535565290850023875092856892694555974281546386510730049106723058933586052544096664351265349363643957125565695936815184334857605266940161251266951421550539554519153785457525756590740540157929001765967965480064427829131488548259914721248506352686630476300.$

Это где-то очень высоко на оси ординат. Но самое потрясающее в формуле Таппера, так это то, что она может строить не только себя, а то что она строит все. Если пройти вдоль оси ординат, то она построит каждый возможный рисунок из черных и белых пикселей размерами 106×17 .

Формула Таппера, по задумке, должна строить абсолютно любое растровое изображение, которое только может существовать в размерности 106×17 . Если использовать данную формулу в практической кодировке изображений, то получится, что конкретное изображение кодируется в так называемой «k», которая по своей сути является ординатой данного изображения, и чтобы его закодировать, нужно найти это самое «k» (таков смысл кодировки растрового изображения по формуле Таппера). При этом изображение будет располагаться при $y \in [k; k+17)$ и при $x \in [0; 106]$.

Как закодировать сообщение в картинке, но большего размера? Если внимательно рассмотреть формулу, заметим, что высота кодируемого изображения зависит от числа 17 в этой формуле, а ширина может быть любой. Все что меняется это сама цифра «k». Она становится больше, если больше ширина, и меньше, если наоборот. Скажем, если нужно выбрать картинку любого размера, необходимо 17 заменить на $h(16 \rightarrow h-1)$, а 106 на $w(105 \rightarrow w-1)$ ($w-1$ и $h-1$ нужны, так как в массивах нумерация элементов идет от 0 до $n-1$ элементов).

Тогда получить «k» изображения произвольного размера можно по следующему алгоритму:

- получаем двоичный код и переводим в десятичную систему счисления;
- умножаем на h ;
- изображение будет лежать в границах $[k; k+h)$.

В данном алгоритме, можно заметить, что одно и то же «k» может подходить для разных изображений, поэтому, чтобы раскодировать необходимое изображение по этой формуле, нужно знать размер этого изображения (пусть это будет приватный ключ для кодируемого изображения).

Формулу Таппера можно обобщить следующим образом.

$$\frac{1}{2} < \left\lfloor \text{mod} \left(\left\lfloor \frac{y}{h} \right\rfloor * 2^{-h * \lfloor x \rfloor - \text{mod}(\lfloor y \rfloor, h)}, 2 \right) \right\rfloor$$

Рис. 2. Обобщенная формула

```

1  from PIL import Image
2
3  def get_our_picture():
4      our_picture = Image.open('cypher.jpg')
5      our_picture = our_picture.convert('1')
6      our_picture = our_picture.save('cypher after decode.jpg')
7      return our_picture
8
9  def get_bits_from_our_picture(w,h):
10     picture = get_our_picture()
11     our_bits_from_image = ""
12     for x in range(w-1,-1,-1):
13         for y in range(h):
14             if picture.getpixel((x,y)) > 127:
15                 our_bits_from_image += '0'
16             else:
17                 our_bits_from_image += '1'
18     return our_bits_from_image
19
20 def get_our_k(w,h):
21     k = int(get_bits_from_our_picture(w,h),2)
22     k *= h
23     return k
24
25 if __name__ == '__main__':
26     file = open('cypher_k','w')
27     main_w = input("width: ")
28     main_h = input("height: ")
29     file.write(str(get_our_k(main_w,main_h)))
30     file.close()
31     file_size.close()

```

Рис. 3. Код программы, который записывает полученное k в файл

```

1  from PIL import Image, ImageDraw
2
3  def get_k(k):
4      return str(bin(k//h))[2:]
5
6  def decode(w,h,k):
7      k=get_k(k)
8      image = Image.new("1", (w,h), (0))
9      draw = image.load()
10     bin_k = ""
11     if len(k)<w*h:
12         for i in range(w*h-1,len(k),-1):
13             bin_k += '0'
14     bin_k += k
15     lists = [[] for i in range(h)]
16     for i in range(w*h):
17         lists[i%h].append(bin_k[i-1])
18     for x in range(w):
19         for y in range(h):
20             if int(lists[y][x]) == 0:
21                 image.putpixel(xy = (w-1-x,y), value = (1))
22             else:
23                 image.putpixel(xy = (w-1-x,y), value = (0))
24     image.save('encvpher.png')
25
26 if __name__ == '__main__':
27     main_w = input("width: ")
28     main_h = input("height: ")
29     k = input("k: ")
30     decode(main_w,main_h,k)

```

Рис. 4. Код программы на питоне для декодирования

Скрипты кодирования и декодирования написаны на Python 3. Однако обычному пользователю будет ими неудобно пользоваться, поэтому можно написать удобный клиент(интерфейс) для работы с данными скриптами на языке программирования C#.



Рис. 5. Схема работы приложения

Братских Илья Александрович¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Плотников Герман Геннадьевич²,
*доцент кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя,*

АЛЬТЕРНАТИВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ СРЕДСТВ СВЯЗИ. IP-ТЕЛЕФОНИЯ

IP-телефония – телефонная связь по протоколу IP. Под IP-телефонией подразумевается набор коммуникационных протоколов, технологий и методов, обеспечивающих традиционные для телефонии набор номера, дозвон и двустороннее голосовое общение, а также видеообщение по сети Интернет или любым другим IP-сетям. Сигнал по каналу связи передается в цифровом виде и, как правило, перед передачей преобразовывается (сжимается) с тем, чтобы удалить избыточность информации и снизить нагрузку на сеть передачи данных.

IP-телефония реализует задачи и решения, которые с помощью технологии телефонной сети общего пользования реализовать будет труднее либо дороже.

К примеру, возможность передавать более одного телефонного звонка в рамках высокоскоростного телефонного подключения. Поэтому IP-телефония используется в качестве простого способа для добавления дополнительной телефонной линии дома или в офисе.

Свойства (например, конференция, переадресация звонка, автоматическое повторение номера, определение номера звонящего) предоставляются бесплатно, тогда как в традиционных телекоммуникационных компаниях обычно выставляются в счет.

Безопасные звонки со стандартизованным протоколом (такие как SRTP). Большинство трудностей для включения безопасных телефонных соединений по традиционным телефонным линиям, такие как оцифровка сигнала, передача цифрового сигнала, уже решены в рамках

¹ © Братских И. А., 2019.

² © Плотников Г. Г., 2019.

IP-телефонии. Необходимо лишь произвести шифрование сигнала и его идентификацию для существующего потока данных.

Независимость от месторасположения. Нужно только интернет-соединение для подключения к провайдеру IP-телефонии. Например, операторы центра звонков с помощью IP-телефонов могут работать из любого офиса, где есть в наличии эффективное, быстрое и стабильное интернет-подключение.

Доступна интеграция с другими сервисами через Интернет, включая видеозвонок, обмен сообщениями и данными во время разговора, аудиоконференции, управление адресной книгой и получение информации о том, доступны ли для звонка другие абоненты.

Дополнительные телефонные свойства – такие как маршрутизация звонка, всплывающие окна, альтернативный GSM-роуминг и внедрение IVR – легче и дешевле внедрить и интегрировать. Тот факт, что телефонный звонок находится в той же самой сети передачи данных, что и персональный компьютер пользователя, открывает путь ко многим новым возможностям.

Дополнительно: возможность подключения прямых номеров в любой стране мира (DID).

Для передачи голоса по IP-сети человеческий голос оцифровывается при помощи импульсно-кодовой модуляции, сжимается (кодируется) и разбивается на пакеты. На принимающей стороне происходит обратная процедура, данные извлекаются из пакетов, декодируются и преобразуются обратно в аналоговый сигнал.

Кодирование вносит дополнительную задержку порядка 15–45 мс, возникающую по следующим причинам:

- использование буфера для накопления сигнала и учета статистики последующих отсчетов (алгоритмическая задержка);

- математические преобразования, выполняемые над речевым сигналом, требуют процессорного времени (вычислительная задержка).

Подобная задержка появляется и при декодировании речи на другой стороне. Задержку кодека необходимо учитывать при расчете сквозных задержек. Кроме того, сложные алгоритмы кодирования/декодирования требуют более серьезных затрат вычислительных ресурсов системы.

Проведенный в различных исследовательских группах анализ качества передачи речевых данных через Интернет показывает, что основным источником возникновения искажений, снижения качества и разборчивости синтезированной речи является прерывание потока речевых данных, вызванное:

- потерями пакетов при передаче по сети связи;
- превышением допустимого времени доставки пакета с речевыми данными.

Это требует решения задачи оптимизации задержек в сети и создание алгоритмов компрессии речи, устойчивых к потерям пакетов (восстановления потерянных пакетов).

При передаче телефонного трафика по IP-технологии должны учитываться жесткие требования стандарта TL9000 к качеству услуг, характеризующие:

- качество установления соединения, определяемое в основном быстротой установления соединения,
- качество соединения, показателем которого являются сквозные (воспринимаемые пользователем) задержки и качество воспринимаемой речи.

Многие потребительские реализации IP-телефонии не поддерживают криптографическое шифрование, несмотря на то, что наличие безопасного телефонного соединения намного проще внедрить в рамках IP-технологии, чем в традиционных телефонных линиях. В результате, при помощи анализатора трафика относительно несложно установить прослушивание IP-звонков, а при некоторых ухищрениях даже изменить их содержание.

*Капусткин Никита Алексеевич¹,
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

*Пузарин Андрей Валерьевич²,
начальник кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ТЕХНИЧЕСКАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ, РЕАЛИЗУЕМАЯ С ПОМОЩЬЮ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Информационная безопасность объекта информатизации – это состояние защищенности объекта информатизации, при котором обеспечивается безопасность информации и автоматизированных средств ее обработки. Объект информатизации – это совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или посещения и объекты, предназначенные для ведения конфиденциальных переговоров.

Техническая защита объектов информатизации, в свою очередь, – это деятельность, направленная на обеспечение некриптографическими методами безопасности объекта информатизации, подлежащего защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Одним из технических средств защиты объектов информатизации может служить беспилотный летательный аппарат – летательный аппарат без экипажа на борту. БПЛА могут обладать разной степенью автономности – от управляемых дистанционно до полностью автоматических, а также различаться по конструкции, назначению и множеству других параметров. Управление БПЛА может осуществляться эпизодической

¹ © Капусткин Н. А., 2019.

² © Пузарин А. В., 2019.

подачей команд или непрерывно – в последнем случае БПЛА называют дистанционно-пилотируемым летательным аппаратом (ДПЛА). Таким образом, можно задавать данным средствам определенный перечень команд, которые он будет выполнять полностью автоматизировано и даже возможна реализация обработки собранных данных и предоставления отчета об уязвимостях объекта информатизации.

К примеру, обычный квадрокоптер с камерой и тепловизором можно использовать для обнаружения возможных приборов слежения, прослушивания и иных приборов сбора информации посредством определения разницы температур, ведь как известно, любые приборы во время работы имеют свойство нагреваться. Таким образом дрон может пилотировать вокруг объекта информатизации и передавать картинку в реальном времени, с помощью которой мы можем наблюдать наличие различных средств сбора информации.

В настоящее время наблюдается резкое увеличение применения различных беспилотных авиационных комплексов (БАК) во всех сферах жизнедеятельности человека – от торговли до военного дела. Беспилотные авиационные комплексы, как правило, включают в себя оператора (пилот-оператор, пункт управления), беспилотный летательный аппарат (БЛА) и каналы связи, однако их защите от внешних программно-аппаратных воздействий, не смотря на рост количества инцидентов, не уделяется достаточного внимания.

Атаки могут быть направлены на перехват управления, вывод из строя БЛА, получение разведывательной информации или для дальнейшей атаки на пилота-оператора и взаимодействующие с ним системы.

К уязвимым местам БЛА можно отнести:

- наличие резервных каналов передачи данных, как правило, открытых для доступа и работающих исключительно на прием, при этом, при выполнении ряда условий, имеющих приоритет перед основными каналами;
- использование спутниковых каналов, а также других беспроводных каналов связи (Wi-Fi, GSM, Bluetooth), имеющих свои характерные уязвимости;
- использование систем спутниковой навигации GPS/Глонасс совместно с инерциальной системой для позиционирования в процессе полета.

В настоящее время существует множество средств обнаружения и защиты информации от программно-аппаратных воздействий, однако, ни одно из них не предназначено для защиты роботизированных комплексов и БАК (БЛА) соответственно.

Возможности источников угроз безопасности информационной системы обусловлены совокупностью способов несанкционированного и (или) случайного доступа к системам БАК, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) информации.

Угроза безопасности информации реализуется в результате образования канала реализации угроз между источником угрозы и БАК, что создает условия для проведения атакующего воздействия.

Основными элементами канала реализации угроз являются:

- источник угрозы – субъект, материальный объект или физическое явление, создающие угрозы;
- среда (путь) распространения информации или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) БАК;
- носитель информации – составная часть БАК, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

В настоящее время частичная защита информации, циркулирующей в БЛА, осуществляется только в БАК военного назначения – информация, передаваемая по каналу управления, информационному каналу, а также информация, содержащая сведения о задании, и информация, хранящаяся в устройстве хранения видовой информации.

Для защиты информации применяются следующие средства:

- средства шифрования – аппаратные и (или) аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

– средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.

Общий сценарий подготовки и применения внешних программно-аппаратных воздействий на систему управления БЛА, элементы БАК и взаимодействующие сети и системы может включать следующие этапы.

Обязательные компоненты атаки:

- проведение технической компьютерной разведки;
- выбор цели атаки;
- подготовка к проведению атаки.

Дополнительные компоненты атаки:

- «заражение»¹ системы БЛА;
- осуществление по заданному алгоритму воздействия;
- «заражение» системы АРМ пилота-оператора;
- осуществление по заданному алгоритму воздействия;
- «заражение» сети, в которую может быть интегрирована АРМ пилота-оператора;
- осуществление по заданному алгоритму воздействия.

¹ Под «заражением» понимают различные угрозы безопасности информации, определенные в разделе 3.2 ГОСТ Р.50.1.053-2005 «Основные термины и определения в области технической защиты информации».

Корноухов Егор Алексеевич¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Галиев Денис Вадимович²,
*преподаватель кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ПРАКТИЧЕСКИЕ АСПЕКТЫ ПРИМЕНЕНИЯ ИНТЕГРИРОВАННЫХ СИСТЕМ БЕЗОПАСНОСТИ

Обеспечение безопасности страны с более чем 146 миллионным населением является необходимым условием обеспечения жизни и деятельности ее граждан, соблюдения их законных прав и свобод, эффективного функционирования системы управления, экономики, хозяйства, транспорта и связи, сохранения на необходимом уровне среды обитания, развития социальной и духовной сфер общества.

Исследование вопросов эффективного обеспечения безопасности населения и промышленных объектов в современных условиях является особенно актуальным в связи с активизацией угроз международного терроризма и техногенных катастроф, а также ростом криминальности, экономической нестабильностью, компьютерными преступлениями, промышленным шпионажем.

Особое значение в современных условиях имеет обеспечение безопасности объектов особой важности, повышенной опасности и жизнеобеспечения (критически важных объектов – КВО) на фоне роста криминальных и террористических угроз. Захват, вывод из строя или нарушение функционирования таких объектов и перевозимых специальных грузов чреваты крайне негативными последствиями и могут нанести крупный или невосполнимый ущерб государству и обществу.

К таким объектам могут относиться:

– объекты высших органов власти, правительственные учреждения, крупные объекты кредитно-финансовой сферы;

¹ © Корноухов Е. А., 2019.

² © Галиев Д. В., 2019.

– объекты особо важного административного, общественного и промышленного значения с высокими требованиями к системам жизнеобеспечения и безопасности;

– объекты топливно-энергетического комплекса, ядерно, радиационно, химически и биологически опасные объекты, электростанции, в том числе атомные, гидротехнические сооружения, тоннели, мосты, газонефтепроводы, склады горюче-смазочных материалов и т. д.;

– объекты микробиологической и фармацевтической промышленности, объекты по переработке и хранению наркотических веществ, сильнодействующих ядов и химикатов, психотропных веществ и препаратов;

– объекты, являющиеся архитектурными памятниками, музеи, здания для хранения архивов, художественных и других подобного рода культурных и материальных ценностей, объекты культа;

– объекты (территории) жизнеобеспечения;

– метрополитен, подземные сооружения особо важного значения;

– жилые многоэтажные дома;

– объекты массового пребывания людей: школы и больницы, театры, стадионы, вокзалы, аэропорты и т. д.;

– специальные грузы, перевозимые автомобильным, железнодорожным транспортом, судами речного и морского флота.

Обеспечение безопасности различных объектов требует комплекса мер, направленных на предупреждение, пресечение и устранение угрозы или опасной ситуации. Комплекс мер должен основываться на принципах системного подхода к деятельности по обеспечению безопасности как на этапах организации, подготовки, проектирования, так и в процессе эксплуатации и включать совокупность организационных и технических мероприятий.

В последнее время в целях повышения технической оснащенности охраняемых объектов активно внедряются интегрированные системы безопасности (ИСБ). Это связано с тем, что требования к уровню обеспечения безопасности постоянно растут и для их наиболее полного удовлетворения необходимо широко использовать средства автоматизации, автоматизированные системы управления, новые информационные технологии, которые позволяют интегрировать организационные и технические ресурсы для решения этих задач.

Использование ИСБ позволяет решить на новом качественном уровне задачи по обеспечению безопасности граждан и объектов. Сле-

дует отметить, что применение ИСБ не устраняет необходимость контроля со стороны человека, но значительно повышает эффективность работы служб безопасности, особенно при наличии многочисленных зон и факторов риска.

Преимущества использования интегрированных охранных систем и создание комплексных систем безопасности стало новым этапом в сфере обеспечения охраны объектов.

В области обеспечения безопасности, как и в любой другой, технологии устаревают очень быстро. Наиболее продвинутой характеристикой ИСБ на данный момент является решение не только вопросов безопасности, но и задач по управлению системами жизнеобеспечения здания. Предпочтительно применение оборудования от одного производителя, так как в этом случае есть гарантия, что все элементы будут одинакового класса качества и согласованы по параметрам, что эта система будет работать нормально.

Необходимо отметить, что работоспособные ИСБ появились на нашем рынке лишь несколько лет назад. Но несмотря на стереотип об отсталости нашей страны от того же Запада, разработки отечественных инженеров ничуть не хуже. К тому же отечественные технические средства имеют ряд преимуществ – относительную дешевизну, адаптированность к отечественным нормам и стандартам, хорошую ремонтно-сервисную базу, возможность поставки доработанных средств или программного обеспечения по особому заказу. Импортные технические средства имеют более высокие потребительские характеристики и надежность в эксплуатации, но и с ними может возникнуть целый ряд проблем. Это оборудование может не иметь сертификата, не быть адаптировано к российским условиям, а это неизбежно приведет к повышению эксплуатационных расходов при его обслуживании или даже к невозможности его длительной эксплуатации.

Итак, для построения интегрированной системы безопасности современного технического уровня, эффективной по критерию «цена – качество», не следует:

- применять оборудование, имеющее только локальные функции;
- применять оборудование, не имеющее стандартного цифрового интерфейса для передачи данных и управления функциями;
- применять оборудование и системы, работа которых не может отображаться и управляться стандартными средствами графического интерфейса персонального компьютера;

- применять системы и оборудование, не имеющие четкого технического описания команд и состояний устройств.

Процесс развитие интегрированных систем безопасности не стоит на месте и в дальнейшем можно выделить такие перспективы развития ИСБ, как:

- повышение «интеллектуальности» системы. Сведение роли человека в процессе принятия решений по реагированию на поступившие сообщения о тревогах и неисправностях от специализированных подсистем ИСБ, к минимуму;

- создание распределенных систем безопасности, не имеющих ограничений по масштабу, количеству пользователей и подсистем, что в свою очередь позволит создать единую систему безопасности и мониторинга стратегически важных объектов в масштабах страны, континента, планеты. Единая система мониторинга позволит обеспечить высокий уровень прозрачности, управляемости и защиты распределенных объектов;

- повышение уровня интеграции ИСБ с различными специализированными системами. Например, объединение с юридическими, информационными системами, системами управления бизнесом и др., работа которых не направлена на физическую защиту объекта;

- широкое распространение технологии «умный дом». Повсеместная интеграция ИСБ с системами, предназначенными для автоматизации управления функционированием и жизнеобеспечением (технология «умный дом»), как на малых, средних и крупных объектах промышленности, так и на объектах социальной направленности (школы, больницы, гос. организации);

- распространение и внедрение программы «Безопасный город» для всех субъектов Российской Федерации. В настоящее время ИСБ широко используются для реализации программы «Безопасный город». Такие системы могут объединять в себе: центр оперативного управления, подсистему видеонаблюдения, подсистему инженерной инфраструктуры, подсистему защиты информации, подсистему оповещения и др. Данная программа принята для разработки только в некоторых крупных городах России. Принятие на реализацию программы «Безопасный город» во всех субъектах Российской Федерации, позволит обеспечить комплексную безопасность населения и объектов на территории России, с единым центром мониторинга верхнего уровня, объединяющего в себе центры мониторинга нижнего уровня. Такая единая система будет

направлена на предупреждение чрезвычайных ситуаций, развитие гражданской обороны, защиту населения на территории субъекта Российской Федерации от чрезвычайных ситуаций природного и техногенного характера, обеспечение пожарной безопасности и личной безопасности людей на всей территории Российской Федерации;

– возможность интеграции роботов в систему безопасности. В настоящее время на развитие робототехники и роботостроения выделяется много сил и средств. Роботы являются незаменимыми помощниками там, где человек уже обойтись без них не сможет. Например, использование для разминирования опасных объектов специальных роботов-саперов является уже обычной практикой, сохраняющей жизнь людей. Роботы также не восприимчивы к газам и могут работать при таких условиях, при каких обычный человек без специального оборудования не сможет долго находиться на потенциально опасной территории. Наличие таких роботов на крупных и опасных объектах промышленности, функционирование которых координировалось бы с единого центра ИСБ объекта, позволило бы ликвидировать различного рода нештатные ситуации без участия оперативных сотрудников.

Следует отметить, что интеграция – это новый этап в построении систем безопасности. Актуальность применения интегрированных систем безопасности определяется слиянием всех автоматизированных систем в единый комплекс. При интеграции систем увеличиться возможность анализа тех или иных воздействий на основе единого информационного поля. Применение интеграции обеспечит простоту получения новой информации и внедрение сложных алгоритмов функционирования отдельных элементов системы, а также повысит безопасность технико-экономических показателей.

*Кожурина Анастасия Николаевна¹,
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

*Дворянкин Олег Александрович²,
старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

КИБЕРПРЕСТУПНОСТЬ

Киберпреступность – это одна из главных проблем XXI в. Под данным понятием подразумевается совершение преступлений в сфере высоких технологий. Это весьма обширный термин, включающий в себя множество незаконных деяний.

На территории России раскрываемость преступлений в сети чрезвычайно невысока. Причиной можно назвать существенное отставание технологий и оборудования, находящегося в арсенале правоохранительных органов. Преступники на этот счет экипированы значительно сильнее. Киберпреступность представляет собой не только техническую и правовую, но и социальную проблему, эффективное решение которой требует, прежде всего, системного подхода к разработке основ обеспечения безопасности жизненно важных интересов гражданина, общества и государства в киберпространстве.

Цель компьютерно-технической экспертизы – найти цифровые следы, связанные с деятельностью человека или группы людей, оценить соответствие этих следов какой-то конкретной ситуации и выделить из них те, которые являются криминалистически значимыми, то есть могут и должны лечь в основу расследования. Важная проблема, представление результатов исследования в таком виде, чтобы они были понятны специалистам с чисто юридическими знаниями, не знакомым с тонкостями судьям, прокурорам, адвокатам и другим участникам судопроизводства. Современное общество невозможно представить без

¹ © Кожурина А. Н., 2019.

² © Дворянкин О. А., 2019.

современных компьютерных технологий. Более того, общество по праву признается информационным. Вряд ли найдется представитель такого общества, который не сталкивался бы с передачей и получением информации через компьютерные сети. Напротив, согласно данным, ожидается, что глобальный трафик будет ежегодно увеличиваться, так что к настоящему времени количество битов пересылаемых через интернет каждый день, возможно, уже превысило приблизительное число песчинок на всех пляжах в мире. Впрочем, примерно с такой же стремительностью растет и киберпреступность и количество так называемых ИТ-инцидентов.

На сегодняшний день значительная доля компьютерных преступлений приходится на не правомерные посягательства на информацию, которая в последующем используется в личных, корыстных целях. Когда начали пользоваться первыми цифровыми сетями, очень мало усилий затрачивалось на то, чтобы защитить их от вторжения. Вскоре стало очевидным, что методология цифровой безопасности абсолютно необходима. Методология цифровой безопасности заключается в добавлении в цифровую сеть дополнительных слоев, которые предотвращают несанкционированный доступ, а также могут обнаружить и сохранить довольно длинную историю всех доступов и определенных точек входа. Тем более выяснилось, что при проведении сетевого криминалистического анализа, исследования, экспертизы, часто приходится работать в системе, которую нельзя выключать, маршрутизаторы, переключатели и другие виды сетевых устройств, в том числе и критические серверы. Наконец, стало совершенно ясно только цифровые следователи и специалисты в компьютерной криминалистике используют эти и многие другие системы, чтобы расследовать цифровые преступления. Для выполнения подобных задач необходимы отдельные человеческие ресурсы и их вовлечение в процесс. При этом необходима высокая квалификация специалистов, владение методиками и процедурами сбора и представления доказательств, их подачи в компетентные инстанции, знание законодательных нормативов и тонкостей для формирования понятного состава обвинения в условиях работы со случаями нарушения законодательства в узкоспециализированной сфере, которая обычно недостаточно понятна судам.

Разведка – это теория и практика сбора информации о противнике или конкуренте для обеспечения своей безопасности и получения преимуществ в области вооруженных сил, политики или экономики.

Разведка может применять как законные методы получения информации (например, получение и исследование сведения из открытых источников, прослушивание радиоканалов, слежка с помощью спутников), так и незаконные операции, трактующиеся как «шпионаж» или «кража информации».

Внешняя разведка – получение информации об зарубежных странах и о том, что происходит на их территории.

В России термин внутренняя разведка входит в понимание оперативно-розыскной деятельности, что представляет собой сбор сведений о преступной деятельности в своей стране.

Военная разведка – комплекс мероприятий по получению и обработке данных о действующем или вероятном противнике, его военных ресурсах, боевых возможностях и уязвимости, а также о театре военных действий. Она делится на тактическую разведку и стратегическую разведку.

Политическая разведка – это деятельность, направленная на добычу сведений о внутренней и внешней политике иностранного государства.

Экономическая разведка – это вид внешней разведки, объектами которой являются промышленность, транспорт, торговля, финансовые и денежно-кредитные системы, природные ресурсы и т. п.

Внешняя контрразведка – вид внешней разведки, объектами которой являются разведывательные службы иностранных государств, добытие сведений об их деятельности:

- добывание сведений о международных террористических организациях и подготавливаемых за рубежом государственных переворотах в своей стране;

- добывание сведений о международной организованной преступности.

Агентурная разведка включает деятельность разведчиков, действующих под видом дипломатов и обладающих поэтому дипломатической неприкосновенностью, и нелегальную разведку.

Видовая разведка включает воздушную разведку и космическую разведку.

Радиоэлектронная разведка включает перехват переговоров – радиоразведку и перехват систем связи между техническими системами и обнаружение источников радиоизлучения – радиотехническую разведку.

Разведывательная деятельность включает сбор информации, оценку ее достоверности и объединение отдельных фактов в общую картину. При этом большое значение имеет оценка достоверности полученной информации.

Киберразведка может производиться как удаленно, с помощью сети Интернет, так и путем осуществления взлома компьютеров и компьютерных сетей компаний обыкновенными шпионами («крысами») и хакерами. С недавнего времени киберразведка включает в себя анализ спецподразделениями поведения пользователей в социальных сетях, таких как В Контакте и Instagram с целью выявления экстремистской, террористической или антиправительственной деятельности.

Киберразведка организуется и ведется в интересах решения двух групп задач – добывание разведывательных сведений из компьютерных систем или сетей и их обработка с помощью аппаратно-программных средств (компьютерная разведка), а также сбор и систематизация данных о потенциальных источниках киберугрозы и самих угрозах (разведка киберугроз).

Первая группа задач решается путем проведения комплекса согласованных мероприятий по несанкционированному проникновению в сети и компьютеры иностранных государственных и неправительственных организаций, а также представляющих интерес частных лиц. Решение второй группы задач (сбор информации о киберугрозах) предполагает использование совершенно новых источников, технологий и технических приемов.

Киберпреступление – это любое незаконное действие в электронной сфере, которое совершено с использованием компьютерных технологий либо против них. Главные особенности таких преступлений – максимальная скрытность деяний. Это достигается благодаря совершенным методам обеспечения анонимности любых совершаемых в интернете действий. Использование анонимайзеров (пример – браузер TOR) либо выход в сеть через «подставные компьютеры» (например, в интернет-кафе) делает практически невозможным определение личности преступника. Трансграничность – преступник и его «жертва» могут

быть разделены гигантскими расстояниями. Возможность совершения преступлений в автоматизированном режиме. Известны случаи, когда хакеры разрабатывали программы, которые самостоятельно (без их участия) снимали деньги с кредитных карт, либо совершали другие противозаконные действия. Нестандартность действий преступников. В отличие от «обычных» преступлений в данной стезе практически невозможно предугадать действия злоумышленников. Обратите внимание: основным средством спецслужб по выявлению местоположения преступника является установление ip-адреса устройства. Однако использование шифровальных программ, либо подключение динамического ip-адреса (он меняется в случайном порядке, такую услугу предоставляют многие российские провайдеры) делает такой метод не эффективным. Поэтому сегодня активно разрабатываются более совершенные технологии для определения фактического адреса устройства, с которого было совершено киберпреступление.

*Макарова Екатерина Андреевна¹,
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

*Плотников Герман Геннадьевич²,
доцент кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

СИСТЕМЫ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ОХРАНОЙ ОБЪЕКТОВ

Развитие систем централизованного управления охраной объектов напрямую зависит от развития информационных технологий.

Благодаря развитию телефонных сетей, появились уникальные условия для создания специализированных систем, способных обеспечить централизованный контроль за проникновением и возникновением пожара на охраняемых объектах. К примеру, система передачи извещений о проникновении и пожаре (СПИ) «Ахтуба» предназначена для централизованной охраны квартир граждан и объектов. Система используется в городах, поселках и прочих населенных пунктах, где между группой охраняемых объектов, автоматической телефонной станцией (АТС) и пунктами централизованной охраны имеются занятые или выделенные телефонные линии, сеть сотовой связи GSM/GPRS, Ethernet/Internet и другие каналы связи. СПИ «Ахтуба» – это полностью цифровая, компьютеризированная система повышенной надежности.

В системе все процессы управления, контроля, самодиагностики и восстановления максимально автоматизированы. Система разработана по заданию и при поддержке Главного управления вневедомственной охраны МВД России и включена в «Перечень средств, рекомендованных для применения в подразделениях вневедомственной охраны ГУВО МВД России». СПИ «Ахтуба» успешно эксплуатируется отделами вневедомственной охраны МВД России разных регионов России, а также службами безопасности предприятий.

¹ © Макарова Е. А., 2019.

² © Плотников Г. Г., 2019.

С дальнейшим развитием технологий появились системы, использующие открытый эфир. Например, системы видеонаблюдения интегрированные с системой охранной сигнализации. С их помощью может осуществляться визуальное наблюдение за охраняемым объектом в прямом эфире, либо же данные могут записываться на жесткий диск или другой вид носителей до их востребования. Видеонаблюдение в офисах, на торговых и производственных площадях позволяет следить за всем что происходит в них. При осуществлении денежных расчетов в супермаркетах, в пунктах обмена валют и в других помещениях уже стало обычной практикой фиксировать все расчеты на камеры наблюдения высокого разрешения и записывать данные на магнитные и оптические накопители.

Развитие сотовой связи в начале XXI в. дало новый толчок в развитии централизованной охраны объектов. Уже сейчас мы отмечаем значительный рост охраняемых объектов системами, использующих в качестве канала передачи извещений сотовую связь. Само по себе это упростило создание охранной техники. Для сотовых сетей нет необходимости разрабатывать специальные передатчики и приемники. Теперь производители просто приобретают модули сотовой связи иностранного производства и интегрируют их в уже существующие охранные приборы.

В настоящее время существуют уже беспроводные системы сигнализации с цветной видеофиксацией, например система Videofied, которая не только посылает сигнал тревоги на пульт оператора охраны, но и дает возможность ее обладателю управлять системой через приложение на смартфоне (постановка/снятие с охраны, запрос фото, видео), что исключает вероятность «ложной» тревоги. Также с помощью Videofied возможно управление системой активного воздействия на нарушителя (дымообразование, светозвуковые устройства, подача определенных голосовых команд нарушителю, электрозамковые устройства и т. п.).

Рассмотрим акустические, световые и дезориентирующие средства.

Начнем с акустических средств воздействия. При несанкционированном проникновении в помещение сирена издает звук высокой громкости (акустическая мощность – до 127 дБ), создавая звуковой «барьер» и вынуждая злоумышленника покинуть охраняемое помещение. Кроме того, нарушитель понимает, что его обнаружили.

Световая система активной защиты представляет собой мощный стробоскопический источник света с изменяемой частотой световой пульсации.

Комбинированные свето-акустические системы – это сочетание двух описанных средств воздействия, нарушитель ослепляется и оглушается одновременно.

Система генерации сухого тумана предназначена для предотвращения краж из помещения в промежуток от момента проникновения до приезда полиции. При активации системы все пространство помещения почти мгновенно (со скоростью $28 \text{ м}^3/\text{с}$) заполняется безвредным для человека составом, снижающим видимость до нуля. Заполняющий помещение дым является взвесью, получаемой при испарении раствора гликоля, и он абсолютно безвреден, однако даже это знание на какой-то момент вводит в замешательство и не позволяет свободно вздохнуть. Этот эффект не только оказывает психологическое воздействие на преступника, но и физически препятствует его дальнейшим действиям: в густом и непроницаемом тумане затруднительно передвигаться, вскрывать хранилища, искать ценности и деньги. Защищенное таким способом помещение остается заполненным туманом в течение длительного времени (около 40 мин), что вполне достаточно для прибытия группы как быстрого, так и медленного реагирования.

Дополнительный психологический эффект достигается с помощью применения генератора тумана совместно с акустическими средствами воздействия. Работает эффект мультипликации, когда человек перестает получать информацию от органов зрения, он начинает сильнее прислушиваться к происходящему, в этот момент, включается сирена, которая помогает системе еще сильнее дезориентировать злоумышленника.

Несмотря на все разнообразие и надежность охранных систем, преступный мир тоже не стоит на месте. Сейчас возникла необходимость в переходе к следующему поколению систем, способных благодаря высокой информативности обеспечить надежную централизованную охрану объектов.

Косянчук Вениамин Андреевич¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Орехов Павел Васильевич²,
*преподаватель кафедры специальных
информационных технологий учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

АНАЛИЗ УЯЗВИМОСТЕЙ NFC-ТЕХНОЛОГИЙ

Near field communication – NFC («коммуникация ближнего поля», «ближняя бесконтактная связь») – технология беспроводной передачи данных малого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на расстоянии около 10 см. Эта технология – простое расширение стандарта бесконтактных карт (ISO 14443), которое объединяет интерфейс смарт-карты и считывателя в единое устройство. Устройство NFC может поддерживать связь и с существующими смарт-картами, и со считывателями стандарта ISO 14443, и с другими устройствами NFC и, таким образом, совместимо с существующей инфраструктурой бесконтактных карт, уже использующейся в общественном транспорте и платежных системах. NFC нацелена, прежде всего, на использование в цифровых мобильных устройствах.

Принцип работы NFC заключается в индукции магнитного поля, где две рамочные антенны располагаются в пределах ближнего поля друг друга, эффективно формируя трансформатор с воздушным сердечником. Этот стандарт работает в пределах общественно доступных и нелицензируемых радиочастот ISM band – промышленные, научные и медицинские радиочастоты около 13,56 МГц, с шириной полосы пропускания почти 2 МГц. Далее в статье рассмотрим возможность его использования.

Во-первых, бесконтактные платежи, при чем не важно, с карты, с телефона или же с часов (если они имеют модуль NFC и соответствующее ПО).

¹ © Косянчук В. А., 2019.

² © Орехов П. В., 2019.

Во-вторых, создание NFC-меток для оптимизации каких-либо процессов.

В-третьих, для передачи информации напрямую между двумя активными модулями телефон/телефон – телефон/пк и наоборот. Для получения информации с пассивной NFC-метки (получение информации о товаре к примеру)

Для авторизации в системе, необходимо знать следующие режимы работы:

- *пассивный режим связи*: устройство-инициатор обеспечивает несущее поле, а целевое устройство отвечает посредством модулирования имеющегося поля. В этом режиме целевое устройство может вытягивать свою рабочую мощность из предоставленной Инициатором электромагнитной области, таким образом делая целевое устройство ретранслятором;

- *активный режим связи*: и инициатор, и целевое устройство взаимодействуют путем поочередного создания своих собственных полей. Устройство деактивирует свое радиочастотное поле в то время, как оно ожидает данных. В этом режиме у обоих устройств должно быть электропитание.

Для передачи данных NFC использует два различных вида кодирования. Если активное устройство передает данные со скоростью 106 кбод, тогда используется модифицированный код Миллера со 100 % модуляцией. Во всех других случаях используется манчестерское кодирование с коэффициентом модуляции 10 %.

Устройства NFC в состоянии одновременно и получать, и передавать данные. Таким образом, они могут контролировать радиочастотное поле и обнаруживать противоречия, если полученный сигнал не соответствует переданному.

На конференции EuSecWest по вопросам безопасности, прошедшей 19–20 сентября 2012 г., компанией MWR Labs был представлен эксплойт 0day, показавший уязвимость технологии NFC в мобильных устройствах. Специалистам по безопасности удалось передать через NFC-соединение вредоносный файл и получить полный контроль над принимающим устройством. Таким образом, конфиденциальные данные и денежные средства «жертвы» оказались под угрозой. Для предотвращения захвата контроля необходимо внесение доработок разработчиками устройств с целью ограничения активности данных, принятых посредством NFC. Хотя радиус связи NFC ограничен несколькими сантиметрами, NFC сама по себе не гарантирует безопасности соединений.

Подслушивание. Радиочастотный сигнал беспроводной передачи данных может быть перехвачен антеннами. Расстояние, с которого атакующий в состоянии подслушать радиочастотный сигнал, зависит от многочисленных параметров, но в любом случае — это всего несколько метров. Кроме того, на подслушивание чрезвычайно влияет режим связи. Устройство без собственного источника питания, которое производит очень слабый радиосигнал, намного тяжелее подслушать, чем устройство с источником питания. Стандарт NFC сам по себе не предлагает защиты против подслушивания. По идее, стек протоколов должен использовать криптоалгоритмы поверх NFC для защиты данных.

Модификация данных. Разрушение данных относительно легко осуществить средствами радиоэлектронной борьбы (РЭБ), т. е. глушилками RFID. Нет способа предотвратить такое нападение, однако единственным его результатом будет невозможность установить связь. Несанкционированная модификация данных внутри сообщения атакующим устройством нереализуема на практике в связи с невозможностью предсказать амплитуду и сдвиг фазы наведенного сигнала на приемном устройстве. RFID-приемник чувствителен к внезапной смене амплитуды и фазы несущего сигнала.

Поскольку NFC-устройства обычно также обеспечивают функциональность ISO 14443, описанная Relay attack также выполнима и для NFC. Для этого нападения злоумышленник должен отправить жертве запрос считывателя и ее ответ в режиме реального времени передать дальше на считывающее устройство. Это делается для того, чтобы выполнить задачу, симулирующую владение смарт-картой жертвы. Однако на практике такая атака довольно затруднительна в связи с жесткими ограничениями по времени на ответ запрашиваемого устройства. В некоторых случаях речь может идти о микросекундных допусках (например, при выполнении обязательной процедуры антиколлизии), также ввиду маленького расстояния взаимодействия атаки с использованием ретрансляторов очень проблематичны.

Сегодня актуален вопрос создания карты клона при помощи NFC: Да, вашу банковскую карту могут откопировать (ее NFC составляющую), но информация на ней закодирована потребует очень мощный декриптор, чтобы ей воспользоваться. При копировании карты мы получаем всю информацию карты, но поскольку она зашифрована, мы видим в блоках только нули. Как только мы расшифруем эту информацию, мы сможем перезаписать карту на любой NFC-носитель и пользоваться ею. Как бы это ни считалось невозможным, такое ПО есть, и в

данный момент можно найти в теневой части Интернета за немалые деньги.

Следующую опасность для пользователей бесконтактных платежей представляют терминалы оплаты. Представим: вы едете в метро и любое лицо, у которого есть терминал, подносит его к вашей карте, деньги спишутся, но каждый терминал регистрируется на определенный счет, который можно отследить, значит, такой способ мошенничества и краж по идее не рентабелен для неблюстителей закона. Но, в том же Даркнете мы можем найти ПО, позволяющее делать терминал оплаты из обычного считывателя NFC, который можно купить на каждом углу, можно запрограммировать NFC-считыватель так, что он будет производить покупку криптовалюты, и отследить такие платежи и кражи невозможно (данный вид мошенничества не распространен в Российской Федерации, но набирает популярность).

Как мы знаем, NFC используется в системе СКУД (система контроля и учета доступа). К примеру, злоумышленнику нужно проникнуть на охраняемый объект. Выбирается жертва, которая имеет доступ к этому объекту, немного социальной инженерии, слежки и карту СКУД можно откопировать за доли секунды, далее – проникновение на объект и т. п.

В данный момент роль NFC в повседневной жизни сильно принижена, использование NFC-меток может ненамного, но облегчить жизнь обычного человека. Самые простые примеры – программирование меток на контакт с телефоном (например, вы пришли домой – ставим параметры на включение WIFI, отключение GPS и т. п.). NFC может служить и для авторизации в системе «умный дом».

Галаев Даниил Игоревич¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Большунов Александр Геннадьевич²,
*преподаватель кафедры специальных информационных
технологий учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

Петров Герман Владимирович³,
*преподаватель кафедры огневой подготовки
учебно-научного комплекса специальной подготовки
Московского университета
МВД России имени В.Я. Кикотя*

СПЕЦИАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИХ РОЛЬ В ПРОТИВОБОРСТВЕ С ТЕРРОРИЗМОМ

Интенсивное использование Интернета группами, занимающимися террористической деятельностью, вызывает все больше вопросов. Именно через Интернет транслируются фотографии и видеоматериалы групп джихадистов по часто меняющимся адресам и размещаются на форумах. Интернет становится очень ценным средством международного общения для террористов всех мастей, дает возможность распространять информацию практически без затрат для миллионов людей одновременно. Пропагандисты используют YouTube, Twitter, социальные сети и чат-платформы, чтобы праздновать свои победы, терроризировать, публикуя видеоролики обезглавливания журналистов, и призывать молодых людей присоединиться. По статистическим данным, около 2 000 жителей Запада совершивших поездку в Сирию, чтобы сражаться в рядах ИГИЛ были завербованы в интернете.

В период с 2009 г. по 2010 г. Китай, член Совета Безопасности, на 10 месяцев ограничил доступ в интернет по всей провинции Синьцзян

¹ © Галаев Д. И., 2019.

² © Большунов А. Г., 2019.

³ © Петров Г. В., 2019.

в результате этнического насилия на его западной территории, где проживает уйгурское сепаратистское движение. Другие страны – от Эфиопии до России и Египта предложили или использовали законы для контроля за свободой выражения мнений под предлогом пресечения терроризма и защиты национальной безопасности.

Терроризм также побудил демократические страны предпринять действия, которые могут оказывать влияние на свободу мысли. Между правительствами европейских стран и специалистами по сетевым технологиям была организована частная встреча по вопросу экстремистского содержания. Если компании могут свободно распоряжаться своим пространством по своему усмотрению и часто удаляют контент в результате правовых требований, предъявляемых правительствами и правоохранительными органами, такие частные сделки между государственным и частным секторами меняют логику, преобладающую в сфере интернета.

Информационные фильтры позволяют запретить нецензурный контент. Так контент-фильтр работает по статистическому принципу заранее считывает определенные слова текста, определяет категорию к которой относится содержимое сайта и позволяет блокировать веб-сайты с содержимым не предназначенным для просмотра.

С терроризмом необходимо бороться, сотрудничая в области правовой взаимопомощи и обмена разведывательными данными между странами. Для этого необходимо изучить истоки терроризма, его проявления в интернете, определить существующие террористические сайты, их цель, к чему приводит участие в подобных группировках. Знание равно оружию. Человека знающего и осведомленного не так просто сбить с пути.

*Атанова Александра Андреевна¹,
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

*Аветисян Карэн Рафаелович²,
преподаватель кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ПРОФАЙЛИНГ В ДЕЯТЕЛЬНОСТИ ОВД

Профайлинг – система предотвращения противоречащих закону действий путем профилирования, что означает выявление потенциально опасных лиц путем оперативной невербальной диагностики.

Технология профайлинга взяла свое начало в авиационной безопасности еще во второй половине XX века. В то время эта технология была устремлена на снижение вероятности появления возможных рисков, связанных с авиаперевозками пассажиров. Это были простейшие вопросы, позволяющие пассажирам без затруднений ответить на них, а сотрудникам полиции выявить нестандартные реакции опрашиваемых лиц. Эта технология имела в своем содержании небольшое количество стандартных типов поведения, и напоминала собой процедуру психологического тестирования.

Профайлинг является новым направлением в психологической науке, появившимся сравнительно недавно и позволяющим расшифровывать невербальные компоненты, используемые в межличностном общении. По мнению специалистов, профайлинг дает возможность получать самую объективную информацию о потенциальной опасности субъекта и может быть эффективно использован для превентивных мер по предупреждению террористических актов на транспорте и местах массового скопления людей.

¹ © Атанова А. А., 2019.

² © Аветисян К. Р., 2019.

Решение проблемы выявления и предотвращения противоправных действий с максимальной эффективностью во многом зависит от применения широкого спектра научно-практических методик, охватывающих различные области человеческих знаний.

Опыт осуществления защиты от актов незаконного вмешательства на транспорте свидетельствует, что применение только высокотехнологичной досмотровой техники не может решить проблему выявления потенциального террориста. В этой связи одним из ведущих направлений является применение технологии профайлинга, позволяющей выявить потенциально опасных граждан на ранних этапах.

В настоящее время в крупных аэропортах мира наряду с применением современных технических средств досмотра пассажиров, их ручной клади и багажа уже используется технология профайлинга.

Так, в мировой правоохранительной практике, профайлинг является системой специальных мероприятий по выявлению потенциально опасных пассажиров и ситуаций методом наблюдения и специального опроса.

Существует перечень, так называемых критических признаков. К ним можно отнести: подделку паспорта и иных документов; «мешковатость» одежды на теле; «распахнутость» или же «застегнутость» одежды в местах возможного ношения оружия; наличие одежды, которая скрывает контуры фигуры; произвольный контроль за оружием, находящимся при пассажире; бесцельное перемещение по помещению; наличие скрытого оружия; поведение террориста-смертника. Последнему критическому признаку необходимо уделить особое внимание. Чаще всего, террорист-смертник выражает свои эмоции в скрытом гневе или же, наоборот, в явно выраженной агрессии. Соответственно, нельзя оставлять без внимания и неестественно бледный цвет лица, перекосы одежды, «одеревенение», так называемая, «походка Буратино». Необходимо следить и за полной нейтрализацией пассажира, так называемой «суицидальной маской», выражающейся отсутствием эмоций, трансом.

Таким образом, выделим следующие этапы профилирования в обеспечении безопасности по итогу профайлинга:

- начальное наблюдение;
- проверка личных документов и ручной клади;
- беседа;

- опросы по подозрительным признакам;
- наблюдение и взаимодействие с другими сотрудниками полиции, в частности, и правоохранительных органов, в целом.

Следует обратить особое внимание на первый этап. Здесь представляется возможным для удобства и обеспечения наилучшего результата работы профайлера создать так называемые «безопасные коридоры». Например, им может являться досмотровая рамка, позволяющая упорядочить большой поток людей и разделить его на маленькие группы, что позволит лучше видеть каждого гражданина, что позволит профайлеру выделить среди людей подозрительных лиц. Решение по созданию таких коридоров, на мой взгляд, является правильным и целесообразным, так как это не только создает удобства для граждан, обеспечивая им безопасность, но и сотрудникам, работающим в местах массового скопления людей, становится проще выполнять свои профессиональные обязанности.

Сегодня одной из важнейших задач для системы образования сотрудников ОВД является организация обучения технологии профайлинга. Эффективность применения технологии профайлинга во многом будет зависеть от уровня подготовленности и профессионального опыта самого сотрудника.

Соединение теоретической подготовки по системе профайлинга с практическим опытом сотрудников ОВД и других силовых ведомств может стать серьезным оружием в борьбе с терроризмом.

Гринченко Никита Вячеславович¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Казанцев Владимир Иванович²,
*старший преподаватель кафедры огневой подготовки
учебно-научного комплекса специальной подготовки
Московского университета
МВД России имени В.Я. Кикотя*

ХАРАКТЕРИСТИКА ХИЩЕНИЙ ДЕНЕЖНЫХ СРЕДСТВ С ПОМОЩЬЮ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ

В работе освещаются относительно новые, технически и организационно сложные преступления – хищения денежных средств с банковских счетов, а также электронных денежных средств, совершаемые с использованием специализированного вредоносного компьютерного программного обеспечения, массово распространяемого в сети Интернет. В настоящее время такие преступления квалифицируются как мошенничество в сфере компьютерной информации, предусмотренное ст. 159.6 УК РФ, введенной в действие Федеральным законом от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации».

Появление и рост количества данных преступлений объясняется интенсивным развитием в последние десятилетия множества систем переводов денежных средств (платежей), осуществляемых с использованием компьютерных технологии и сетей передачи данных, и широким распространением доступа к сети Интернет.

Глобальное распространение электронных средств платежа предопределило как появление обособленной разновидности и без того специфической компьютерной преступности, так и возникновение своеобразной криминальной индустрии, необходимой для совершения хищений денежных средств с использованием вредоносных программ. Похищение денежных средств со счета жертвы дистанционным способом

¹ © Гринченко Н. В., 2019.

² © Казанцев В. И., 2019.

является технически трудной задачей, выполнение которой невозможно без специального программного и аппаратного инструментария и использования многочисленных регулярно поставляемых криминальных «товаров» и «услуг». Постоянно растущий спрос на такие товары и услуги естественным образом приводит к формированию их полноценного рынка, разумеется, черного, подпольного и одновременно к появлению слаженных преступных групп. Последние разделены по обособленным профессиям и криминальным интересам: компьютерные мошенники, непосредственно атакующие владельцев денежных средств, их многочисленные пособники, помощники и обслуживающий персонал, производители вредоносных программ и поставщики услуг: разнородные торговцы и посредники. Результаты их деятельности, причиняя существенный ущерб гражданам и организациям, остаются в основном неочевидными для потерпевших и не находят должного отображения в уголовной статистике.

Латентность данных преступлений настолько высока, что сейчас не представляется возможным оценить их общее количество, объемы причиняемого ущерба, а также детально изучить их качественные характеристики. В официальную статистику правоохранительных органов попадают сведения лишь о незначительной части таких преступлений, тогда как большинство их остается не только не раскрытым, но и не выявленным. Преувеличивать негативное влияние хищений на устойчивость финансового сектора экономики, вероятно, не следует, однако они, безусловно, являются фактором риска. Снижающим привлекательность высокотехнологичных платежных систем для клиентов и повышающим сложность и стоимость их создания и эксплуатации для операторов. Тем самым преступность в определенном смысле тормозит развитие современных финансовых технологий в нашей стране.

Несмотря на практическую значимость разработки данной проблематики, в научной литературе ей уделяется пока еще недостаточно внимания, в том числе в связи с относительной новизной, неочевидностью и повышенной сложностью проблем борьбы с данным видом преступных посягательств (хищениями, совершаемыми с использованием вредоносных компьютерных программ). Так рассматриваются те элементы национальной платежной системы, которые наиболее подвержены преступным посягательствам и описываются специализированные вредоносные компьютерные программы, дается характеристика организации преступной деятельности и криминальных профессий, поэтапно рассматривается совершение типового преступления.

Способ совершения хищений с использованием вредоносных компьютерных программ является технически сложным и требует предварительного внедрения на компьютеры и мобильные устройства пользователей электронных средств платежа специализированных (тройных) вредоносных компьютерных программ. Преступления совершаются группами, участники которых обладают обособленными криминальными профессиями. Структуры действующих преступных групп отличаются непостоянством и могут изменяться непосредственно в процессе совершения преступления по различным тактическим причинам. Относительно стабильным является только ядро группы, в то время как многочисленные пособники и соисполнители привлекаются на непостоянной основе. В интересах обеспечения преступной деятельности функционирует масштабный подпольный рынок криминальных товаров и услуг, представленный в основном в сети интернет на специализированных ресурсах.

Абдрахманова Лидия Ринатовна¹,
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя

Большунов Александр Геннадьевич²,
преподаватель кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя

УМНЫЕ ГАДЖЕТЫ

Пользователями всех умных гаджетов являются люди. Некоторые из этих пользователей становятся на путь преступной деятельности. При этом «интернет-вещи» могут стать «невольными свидетелями» действий злоумышленников. Они накапливают информацию, которая может в дальнейшем быть расшифрована правоохранительными органами и использована для целей уголовного судопроизводства.

Однако вопрос о нормативно-правовом регулировании данной области остается открытым и вызывает дискуссии среди правоприменителей. Несомненно, IoT могут использоваться в сфере правоохранительной деятельности.

Что нужно знать об этих предметах следователю или дознавателю?

Устройства, входящие в «интернет-вещи» – это любые автономные устройства, подключенные к Интернету, которые могут отслеживаться и/или управляться удаленно.

Экосистема IoT, или интернет-вещи – это все компоненты, которые позволяют бизнесу, правительствам и пользователям присоединять свои устройства IoT, включая пульта управления, панели инструментов, сети, шлюзы, аналитику, хранение данных и безопасность.

Безусловно, без использования специальных знаний и приглашения специалиста в данной сфере, сложно определить тактику проведения следственных действия и методику расследования в целом.

¹ © Абдрахманова Л. Р., 2019.

² © Большунов А. Г., 2019.

После изъятия объектов они исследуются экспертом, который получит дополнительную информацию об объекте исследования. При проведении исследования для каждого объекта используется свое программное обеспечение.

Также для эксперта важно использовать специальные программно-аппаратные комплексы, имеющие следующие возможности:

- блокировка записи информации на исследуемый носитель, для этого используется «блокиратор», который активируется перед проведением экспертизы;
- посекторное копирование, например, необходимо создать резервную копию исследуемого жесткого диска (для последующего исследования), чтобы предотвратить возможность изменения данных в оригинале;
- доступ к файловой системе носителя;
- просмотр типа файлов;
- просмотр реестра (просмотр всех подключений к устройству);
- оформление результатов исследования.

Если рассматривать исследование «интернет-вещей», то из приведенных выше программных обеспечений можно использовать «Мобильный криминалист» и «Tizen Studio» так как большинство «интернет-вещей», таких как SmartWatch («умные часы»), подключаются к мобильному устройству. При помощи данного ПО возможно выяснить BluetoothID (уникальный номер устройства) «умных часов», которые были подключены к исследуемому смартфону. Если при проведении осмотра, обыска или выемки были изъяты другие СВТ, то выясненный BluetoothID сравнивается с идентификатором «интернет-вещи».

Существует недостаток при снятии информации с «интернет вещи»: возможно, что все данные, которые передавались между устройствами, зашифрованы. Расшифровка этих данных будет затруднительна.

При рассмотрении продукции Apple и Samsung, которые выпускают SmartWatch («умные часы»), было выяснено, что при проведении исследования подобных часов будет невозможно найти какой-либо информации о мобильном устройстве, которое было подключено к Smart-Watch.

iWatch не дадут никакой информации о себе, а также о подключенном ранее к ним мобильном устройстве, так как на них существует блокировка путем пароля, который проблематично обойти. Также данные часы не подключаются к iTunes и вся информация, которая проходила через них, осталась на мобильном устройстве, т. е., при исследовании

данного продукта от Apple эксперт не получит никакой нужной информации для дела.

С часами от Samsung работать немного проще, так как они выдадут только те данные и настройки, которые установил сам пользователь, а также данные о его здоровье и передвижении, т. е., работая только с «умными часами» от Samsung, получить нужную информацию для уголовного или административного дела не удастся. Существует синхронизация SmartWatch на личном аккаунте Samsung пользователя, где можно найти данные, которые передавались на «интернет-вещь», так как часы просто копируют информацию с мобильного устройства и переносят ее на свой экран.

Для упрощения работы эксперта предлагается использовать учетную запись злоумышленника, для входа в его учетную запись, чтобы установить действительность использования «Интернет-вещи» для совершения преступления.

Но с практической точки зрения, предложенные действия вызовут вопросы у защитника подозреваемого/обвиняемого, так как данные, описанные выше, могут храниться в облачном хранилище и присутствует возможность «исчезновения» данных, которые могли бы служить доказательством в уголовном деле. Сегодня данные о соединении двух устройств, которые использовались для совершения преступления присутствуют в облачном хранилище, а завтра – нет. Адвокат может заявить, что этих данных раньше не было, и эксперт, проводящий исследование данного объекта, дает ложное заключение.

*Белкина Анна Геннадьевна¹,
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

*Пузарин Андрей Валерьевич²,
начальник кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

АНАЛИЗ СОВРЕМЕННЫХ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ПРОВОДНЫХ ЛИНИЯХ СВЯЗИ

Одним из наиболее распространенных и доступных видов связи и передачи информации в настоящее время являются проводные телефонные линии. В силу отсутствия специальных штатных технических средств защиты информации на городских и междугородних автоматических телефонных станциях, перед абонентами, желающими осуществить передачу конфиденциальной информации, возникает проблема выбора устройств данного класса из всего имеющегося многообразия.

Имеющиеся на сегодняшний момент устройства противодействия снятию информации с проводных линий связи можно классифицировать следующим образом:

- блокираторы телефонов;
- устройства защиты от ВЧ-навязывания и микрофонного эффекта;
- анализаторы телефонных линий;
- устройства активной защиты телефонных линий;
- универсальные устройства защиты телефонных линий;
- скремблеры;
- выжигатели средств съема.

Основным назначением блокираторов телефонных аппаратов является пресечение попыток использования платных сервисов доступных через данную телефонную линию, а также прослушивания разговора с помощью параллельно включенного телефона.

¹ © Белкина А. Г., 2019.

² © Пузарин А. В., 2019.

Таким образом, блокираторы в большей степени защищают телефон от пиратских покушений на защищаемую линию. Защита от методов снятия конфиденциальной информации по заранее проверенную линию и служат для контроля параметров телефонной пары. Часто такие сигнализаторы называют «телефонными стражами». Телефонный страж обычно выполняется в виде розетки с двумя светодиодами: зеленый – «Линия чиста», красный – «Тревога! Параметры линии изменились».

Плюсом таких стражей является простота эксплуатации, минусом – высокая вероятность «ложной тревоги». Тестовые комплекты предназначены для проверки линии специалистами. Такой комплект посылает в линию зондирующий сигнал и анализирует ответный сигнал, по которому определяет наличие в линии каких-либо радиоэлементов, присущих цепям съема и передачи информации.

На российском рынке представлен широкий спектр анализаторов, цена которых колеблется от десятков до нескольких тысяч и даже десятков тысяч долларов.

Устройства постановки маскирующей помехи (УПМП) используют следующие способы нарушения нормальной работы средств несанкционированного съема информации:

- синусоидальный сигнал с диапазоном частот 20–70 кГц и амплитудой 12–50 В, который подается в телефонную линию при разговоре и нарушает работу телефонных передатчиков, «размывая» спектр передаваемого сигнала и нарушая режим работы выходного каскада передатчика;

- шумовой сигнал с диапазоном частот 6–10 кГц и амплитудой ~ 5 В (метод высокочастотной маскирующей помехи);

- шумовой сигнал с диапазоном частот 300–3400 Гц и амплитудой ~ 2 В (метод низкочастотной маскирующей помехи). Данный сигнал подается в телефонную линию при положенной трубке и, воздействуя на систему активации записи диктофонов, заставляет их записывать только шум в промежутках между переговорами.

Кроме того, препятствует работе выносных микрофонов, использующих телефонную линию для передачи информации при положенной трубке, маскирует сигналы, возникающие из-за микрофонного эффекта. Телефонный подавитель осуществляет зашумление верхнего звукового диапазона, ухудшая тем самым соотношение сигнал/шум на входе устройств съема информации.

Преимущества анализаторов, подавителей и блокираторов гармонично сочетают в себе универсальные устройства защиты телефонных

линий. Они также устанавливаются на «чистую» линию, работают в двух режимах: обнаружение и подавление. При любом контактном подключении к линии прибор подаст сигнал тревоги, после чего можно включить режим подавления. Помеха, подаваемая в линию, действует на участке от прибора до АТС, выводя все средства съема из рабочего состояния.

Данный класс устройств защиты является наиболее приемлемым для обеспечения безопасности телефонных переговоров. В большинстве устройств данного класса реализован метод высокочастотной маскирующей помехи (SP-17/D, КТЛ-3, КТЛ-400, «Ком-32», «Прокруст», «Прокруст2000», «Гром-ЗИ-6», «Протон» и т. д.).

Метод низкочастотной маскирующей помехи применяется в приборах «Прокруст», «Протон», «Кзот-06» и т. д.

Недостатки устройств постановки маскирующей помехи:

- наличие шумов в телефонной трубке;
- защита речевой информации только того абонента, у которого установлено УППИ;
- отсутствие сертификата Министерства связи Российской Федерации у большинства устройств;
- высокая стоимость.

Аппаратура уничтожения средств съема информации с телефонной линии (выжигатели) выдает в телефонную линию один или несколько импульсов высокого напряжения (1400–2000 В). Воздействие такого напряжения на полупроводниковые элементы выводит их из строя, в результате чего схемы средств съема информации перестают функционировать.

Следует отметить, что аппаратура данного класса представлена только на российском рынке, среди продукции зарубежных компаний такие устройства отсутствуют.

Особо следует отметить аппаратуру криптографической защиты (скремблеры). Все рассмотренные выше устройства способны защитить телефонные переговоры только на участке от абонента до АТС. Для обеспечения конфиденциальности на всем пути прохождения речевого сигнала применяются специальные устройства криптографической защиты.

Под криптографической защитой, или засекречиванием, понимается изменение характеристик речевого сигнала таким образом, чтобы речевой сигнал, переданный в канал связи, был неразборчивым и занимал

такую же полосу частот спектра, что и исходный открытый сигнал в речепреобразующем устройстве.

В зависимости от способа передачи информации можно выделить два основных метода закрытия речевого сигнала: аналоговое засекречивание и дискретизация, или выделение параметров речевого сигнала, представленных в цифровом виде, с последующим шифрованием.

В первом случае в канале связи – сигнал с фрагментами речевого сигнала, во втором – сигнал с выхода модема, использующего один из стандартных видов модуляции и скорости передачи 2400, 4800, 7200 или 9600 бит/с.

При аналоговом засекречивании реализуется два основных способа преобразования речевых сигналов: частотные и временные перестановки. Наиболее высокий уровень закрытия получается при использовании одновременно обоих способов в сочетании с частотной инверсией. При этом характеристики речевого сигнала меняются таким образом, что преобразованный сигнал занимает ту же частотную полосу (0,3–3,4 кГц). Это позволяет передавать его по каналам связи в обычном режиме.

На российском рынке отечественные фирмы предлагают целый ряд устройств криптографической защиты. Широкое распространение получили устройства аналогового типа с частотными и временными перестановками серии SCR–М 1.2, скремблеры семейства «Грот», мозаичные скремблеры М28800 и «Орех-А», а также приборы динамической инверсии спектра ACS-2.

Порядок действий со скремблером такой: необходимо дозвонится до абонента, включить свои скремблеры, подождать пока они настроятся друг на друга, и после этого начинать разговор.

Преимущества аппаратуры аналогового типа:

- высокая степень защиты информации, передаваемой как на всем протяжении линии связи («абонент / абонент»), так и на участке «последней мили» («абонент / АТС»);
- защита как речевых, так и факсимильных сообщений;
- возможность работы с любыми телефонными аппаратами и различными АТС;
- простота в управлении при переходе в закрытый режим связи.

Цифровой способ кодирования информации более устойчив к раскрытию. Сигнал предварительно преобразуется в цифровой вид, а затем кодируется с использованием специальных криптографических алгоритмов. Главная проблема, которую приходится решать при работе с

аппаратами данного класса, состоит в достижении высокого качества синтезированного Р.С. при реальных скоростях его передачи по каналу связи, составляющих 2400–9600 бит/с. Эти факторы, а также условие обязательной сертификации в ФАПСИ затрудняют распространение данных устройств на российском рынке.

На сегодняшний день можно выделить следующие продукты коммерческого применения стоимостью от 500 до 1500 долл.: VoiceCoder-2400, СКР-511 «РЕФЕРЕНТ».

На зарубежном рынке аппаратура данного класса занимает доминирующую позицию, так как структура ТфОП, их качество и наличие специальных сетей телефонных аппаратов, таких как Secure Telephone Unit, объединяющей в США более 700 тыс. абонентов, делают возможным ее полноценное использование для закрытия телефонных переговоров.

К преимуществам аппаратуры дискретного типа относится высокая степень защиты и гарантированная криптографическая стойкость. Недостатком устройств данного класса является неустойчивая работа на двухпроводных телефонных линиях среднего и низкого качества. Таким образом, на сегодняшний день для коммерческого применения в условиях России оптимально использование аналоговых засекречивающих устройств мозаичного типа. Для эффективного противодействия несанкционированному доступу к речевой информации необходимо создание четкой модели «телефонных угроз» в каждом конкретном случае. Она должна учитывать ценность передаваемой информации, особенности построения линии ТфОП не только от абонента до АТС, но и далее до конкретного абонента на другом конце канала связи. Эта модель также должна включать в себя анализ других, в частности технических, каналов утечки информации. Только на основе такого подхода, опираясь на знание реальных возможностей средств защиты, можно разработать и предложить заказчику рациональный комплекс мер по предотвращению несанкционированного доступа к его речевой информации и обеспечить необходимый уровень конфиденциальности.

Список литературы

1. Хорев, А. А. Защита информации от утечки по техническим каналам. – М. : Гостехкомиссия России, 1998. – 320 с.
2. Демидов, В. А. Техника связи ОВД : учебное пособие / В. А. Демидов, Н. В. Сильников, А. В. Шайтанов. – СПб. : Фонд «Университет», 2000. – 95с.
3. Галкин, А. П. Защита технических каналов связи предприятий и учреждений от несанкционированного доступа : учебное пособие / А. П. Галкин, В. С. Эмдин. – СПб. : СПбГУТ, 2001. – 321с.
4. Лагутин, В.С. Утечка и защита информации в телефонных каналах. / В.С.Лагутин, А. В. Петраков. – 2-е изд., испр. и доп. – М. : Энергоатомиздат, 1997. – 298 с.

Бельдеубаева Даяна Ренатовна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Клочкова Екатерина Николаевна²,
*доцент кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

МЕХАНИЗМ БИТКОЙН-КЛЮЧА И ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ НАД КОНЕЧНЫМИ ПОЛЯМИ

Сегодня биткойн продолжает набирать популярность, а индустрия разрабатывать все новые приложения для работы с криптовалютой. Одной из причин такой популярности является строгая математическая база, на которой строится биткойн. Благодаря этому система функционирует в условиях полного отсутствия доверия между участниками сети, исключая воздействие человеческого фактора. Биткойны не хранятся ни централизованно, ни локально, поэтому никто не является их хранителем. Они существуют в виде записей в распределенной книге, называемой блочной цепочкой, копии которой совместно используются волонтерской сетью подключенных компьютеров. «Владеть» биткойном просто означает иметь возможность передавать контроль над ним кому-то другому, создавая запись передачи в блок-цепочке. Что дает эту способность? Доступ к паре закрытого и открытого ключей. Что это значит и как это защищает биткойн? В данной научной статье я бы хотела поговорить о математических основах биткойн-блокчейна – эллиптических кривых, ECDSA и ключах.

В Bitcoin используется так называемая криптография на эллиптических кривых (*Elliptic curve cryptography, ECC*). Она основана на некоторой особой функции – эллиптической кривой. Это процесс, который использует эллиптическую кривую и конечное поле для «подписи» данных таким образом, что третьи стороны могут проверить подлинность подписи, в то время как подписавший сохраняет исключительную способность создавать подпись. С биткойном данные, которые

¹ © Бельдеубаева Д. Р., 2019.

² © Клочкова Е. Н., 2019.

подписаны, являются транзакцией, которая передает право собственности.

ECDSA имеет отдельные процедуры подписания и проверки. Каждая процедура представляет собой алгоритм, состоящий из нескольких арифметических операций. Алгоритм подписи использует закрытый ключ, а процесс проверки использует открытый ключ.

Эллиптическая кривая

Эллиптическая кривая представляется алгебраически как уравнение формы:

$$y^2 = x^3 + ax + b.$$

Для $A = 0$ и $b = 7$ (версия, используемая биткойном, рис. 1).

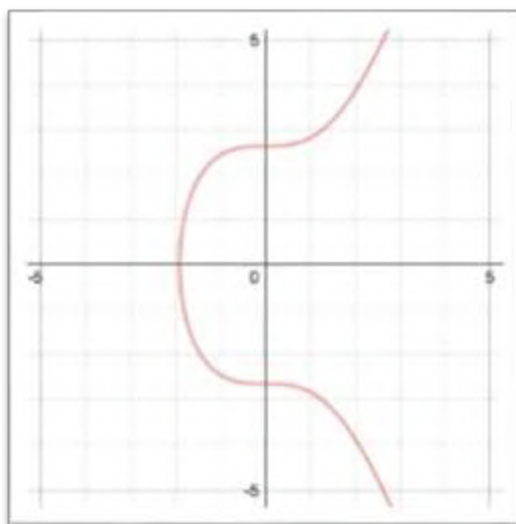


Рис. 1. Эллиптическая кривая уравнения $y^2 = x^3 + 7$

Эллиптические кривые обладают полезными свойствами. Например, не вертикальная линия, пересекающая две некасательные точки на кривой, всегда пересекает третью точку на кривой. Еще одним свойством является то, что не вертикальная линия, касательная к кривой в одной точке, будет точно пересекать другую точку на кривой.

Мы можем использовать эти свойства для определения двух операций: добавление точек и удвоение точек.

Добавление точки, $P + Q = R$, определяется как отражение через ось x третьей пересекающейся точки R' на линии, которая включает P и Q . Проще всего понять это, используя схему (рис. 2):

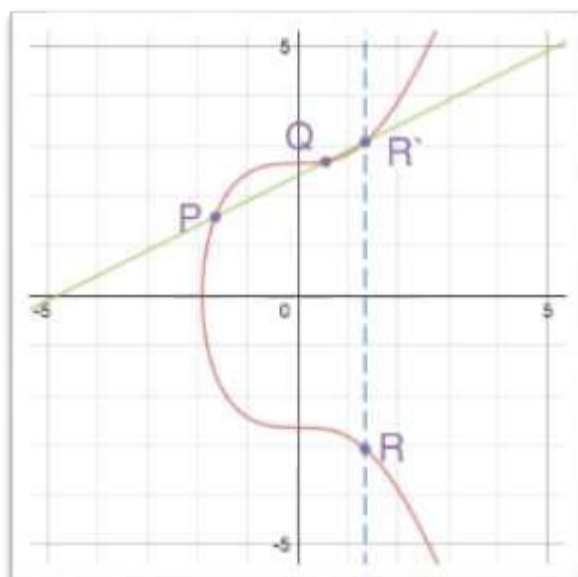


Рис. 2. Схема «добавление точки»
на эллиптической кривой уравнения $y^2 = x^3 + 7$

Удвоение точки, $P + P = R$, определяется путем нахождения линии, касательной к точке, которая будет удвоена, P , и принимая отражение через ось x пересекающейся точки R на кривой, чтобы получить R . Вот пример того, как это будет выглядеть (рис. 3):

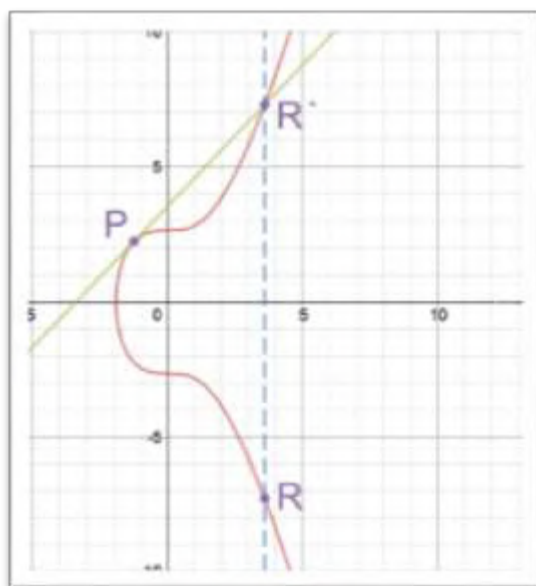


Рис. 3. Схема «удвоение точки» на эллиптической кривой уравнения $y^2 = x^3 + 7$

Вместе эти две операции используются для скалярного умножения, $R = A P$, определяемого путем добавления точки P в себя a раз, например:

$$R = 7P \quad -R = P + (P + (P + (P + (P + P)).$$

Процесс скалярного умножения обычно упрощается с помощью комбинации операций добавления и удвоения точек. например:

$$R = 7P \quad -R = P + 6P \quad -R = P + 2(3P) \quad -R = P + 2(P + 2P).$$

Здесь $7P$ был разбит на два шага удвоения точек и два шага сложения точек.

Конечное поле в контексте ECDSA можно рассматривать как predetermined диапазон положительных чисел, в пределах которого каждый расчет должен падать. Любое число вне этого диапазона «оборачивается» так, чтобы попасть в диапазон.

Самый простой способ подумать об этом-вычислить остатки, представленные оператором модуля (mod). Например, $9/7$ дает 1 с остатком 2:

$$9 \bmod 7 = 2.$$

Здесь наше конечное поле по модулю 7, и все операции по модулю над этим полем дают результат, падающий в диапазоне от 0 до 6.

ECDSA использует эллиптические кривые в контексте конечного поля, что значительно изменяет их внешний вид, но нележащие в их основе уравнения или специальные свойства. То же самое уравнение, построенное выше, в конечном поле по модулю 67, выглядит следующим образом (рис. 4):

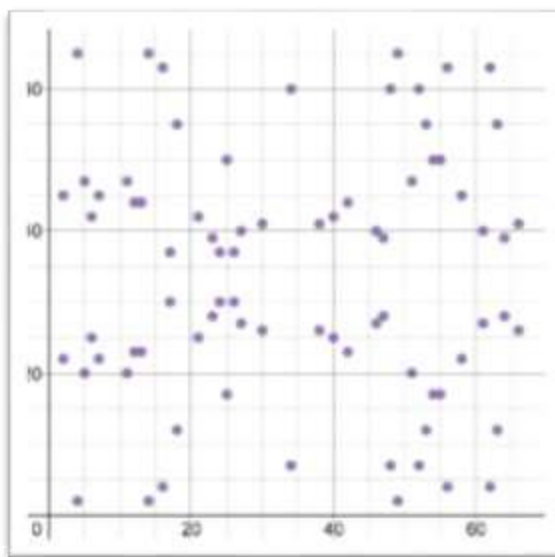


Рис. 4. Эллиптическая кривая уравнения $y^2 = x^3 + 7$ в конечном поле по модулю 67

Теперь это набор точек, в котором все x и значения являются целыми числами от 0 до 66. Заметим, что «кривая» все еще сохраняет свою горизонтальную симметрию.

Добавление и удвоение точек теперь немного отличаются визуально. Линии, нарисованные на этом графике, будут обтекать горизонтальные и вертикальные направления, так же, как и в игре астероидов, сохраняя тот же наклон. Таким образом, добавление точек (2, 22) и (6, 25) выглядит так (рис. 5):

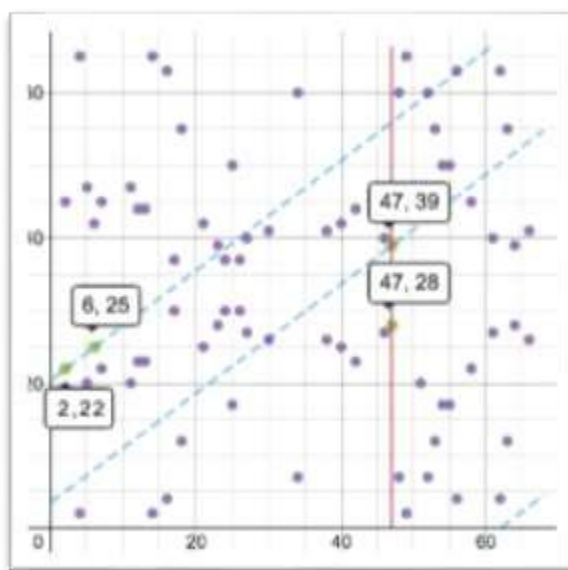


Рис. 5. Эллиптическая кривая уравнения $y^2 = x^3 + 7$ в конечном поле по модулю 67 после добавления и удвоения точек (2, 22) и (6, 25)

Третья точка пересечения (47, 39) и ее точка отражения (47, 28).

Такой протокол, как биткойн, выбирает набор параметров эллиптической кривой и ее конечное представление поля, фиксированное для всех пользователей протокола. Параметры включают используемое, простое по модулю поле и базовую точку, которая попадает на кривую. Порядок базовой точки, который не является независимо выбранным, но является функцией других параметров, можно представить графически, как количество раз, когда точка может быть добавлена к себе, пока ее наклон не будет бесконечным, или вертикальная линия. Базовая точка выбирается таким образом, что порядок является большим простым числом.

Биткойн использует очень большие числа для своей базовой точки, простого по модулю и порядка. В действительности, все практические применения ECDSA используют преогромные значения. Безопасность

алгоритма зависит от того, что эти значения являются большими и поэтому нецелесообразны для грубой силы или обратного проектирования.

В случае биткоина уравнение эллиптической кривой: $y^2 = x^3 + 7$.

Простое по модулю $= 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1 =$
 $FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF$
 $FFFFFFFFE FFFFFFFC2F$.

Базовая точка = $04\ 79BE667E\ F9DCBBAC\ 55A06295\ CE870B07$
 $029BFCDB\ 2DCE28D9\ 59F2815B\ 16F81798\ 483ADA77\ 26A3C465$
 $5DA4FBFC\ 0E1108A817B448\ A6855419\ 9C47D08F\ FB10D4B8$.

Заказ = $FFFFFFFF FFFFFFFF FFFFFFFF BAAEDCE6$
 $AF48A03B\ BFD25E8C\ D0364141$.

Кто выбрал эти номера, и почему? Большое количество и изрядное количество интриг окружает подбор соответствующих параметров. В конце концов, большое, казалось бы, случайное число может скрыть метод бэкдора восстановления закрытого ключа. Вкратце, эта конкретная реализация идет именем `secp256k1` и является частью семейства решений эллиптической кривой над конечными полями, предложенными для использования в криптографии.

С этими формальностями мы теперь в состоянии понять частные и открытые ключи и то, как они связаны. Вот в двух словах: в ECDSA, закрытый ключ – это непредсказуемо выбранное число между 1 и заказом. Открытый ключ является производным от закрытого ключа путем скалярного умножения базовой точки в несколько раз равное значению закрытого ключа. Выражается как уравнение:

*открытый ключ = закрытый ключ * базовая точка.*

Это показывает, что максимально возможное количество приватных ключей (а значит и биткоин-адресов) равно порядку.

В непрерывном поле мы могли бы построить касательную линию и определить открытый ключ на графике, но есть некоторые уравнения, которые выполняют то же самое в контексте конечных полей. Добавление точки $p + q$ для поиска r определяется по компоненту следующим образом:

$$c = (q_y - p_y) / (q_x - p_x) \quad -r_x = c^2 - p_x - q_x \quad -r_y = c(p_x - r_x) - p_y.$$

И удвоение точки p , чтобы найти r , выглядит следующим образом:

$$c = (3p_x^2 + a) / 2p_y \quad -r_x = c^2 - 2p_x \quad -r_y = c(p_x - r_x) - p_y.$$

На практике вычисление открытого ключа разбивается на несколько операций удвоения и добавления точек, начиная с базовой точки.

Давайте запустим пример конверта, используя небольшие числа, чтобы получить интуицию о том, как ключи строятся и используются при подписании и проверке. Параметры, которые мы будем использовать:

уравнение: $y^2 = x^3 + 7$ (т. е. $a = 0$ и $b = 7$) – простое по модулю: 67 – базовая точка: (2, 22) – заказ: 79 – секретный ключ: 2.

Во-первых, давайте найдем открытый ключ. Так как мы выбрали самый простой возможный закрытый ключ со значением = 2, потребуется только одноточечная операция удвоения от базовой точки. Расчет выглядит так: $c = (3 * 2^2 + 0) / (2 * 22) \bmod 67$ – $c = (3 * 4) / (44) \bmod 67$ – $c = 12 / 44 \bmod 67$.

Здесь мы должны остановиться на немного ловкости: как мы выполняем деление в контексте конечного поля, где результатом всегда должно быть целое число? Мы должны умножить на обратное, которое пространство не позволяет нам определить здесь (мы отсылаем вас сюда и сюда, если это интересно). В случае под рукой, вы должны довериться нам на данный момент, что: $44^{-1} = 32$.

Двигаясь прямо вперед:

$$c = 12 * 32 \bmod 67 \quad -c = 384 \bmod 67 \quad -c = 49;$$

$$r_x = (49^2 - 2 * 2) \bmod 67 \quad -r_x = (2401 - 4) \bmod 67 \quad -r_x = 2397 \bmod 67 \quad -r_x = 52;$$

$$r_y = (49 * (2 - 52) - 22) \bmod 67 \quad -r_y = (49 * (-50) - 22) \bmod 67 \quad -R_y = (-2450 - 22) \bmod 67 \quad -R_y = -2472 \bmod 67 \quad -r_y = 7.$$

Таким образом, наш открытый ключ соответствует точке (52, 7). Все это работает на приватный ключ 2.

Эта операция – переход от частного к открытому ключу-вычислительно проста по сравнению с попыткой работать назад, чтобы вывести закрытый ключ из открытого ключа, который, хотя теоретически возможен, является неосуществимым из-за больших параметров, используемых в фактической эллиптической криптографии.

Таким образом, переход от закрытого ключа к публичному ключу – это путешествие в один конец.

Как и в случае с закрытым ключом, открытый ключ обычно представляется шестнадцатеричной строкой. Но подождите, как мы можем добраться от точки на плоскости, описанной двумя числами, до одного числа? В несжатом открытом ключе два 256-битных числа, представляющие координаты x и y , просто склеиваются в одну длинную строку. Мы также можем использовать симметрию эллиптической кривой для создания сжатого открытого ключа, сохраняя только значение x и отмечая, на какой половине кривой находится точка. Из этой частичной информации мы можем восстановить обе координаты.

Подписание данных закрытым ключом

Теперь, когда у нас есть пара закрытых и открытых ключей, подпишем некоторые данные.

Данные могут быть любой длины. Обычно первым шагом является хэширование данных для создания числа, содержащего такое же количество битов (256), что и порядок кривой. Для простоты мы пропустим шаг хэширования и просто подпишем raw data z . Назовем G базовой точкой, N порядком и D закрытым ключом. Рецепт подписания выглядит следующим образом:

1. Выберите некоторое целое число k между 1 и $n - 1$.
2. Вычислить точку $(x, y) = k * G$, используя скалярное умножение.
3. Найти $r = x \bmod n$. Если $r = 0$, вернитесь к шагу 1.
4. Найти $s = (z + r * d) / K \bmod n$. Если $s = 0$, вернитесь к шагу 1.
5. Сигнатура-пара (r, s) .

В качестве напоминания, в шаге 4, если числа приводят к дроби (что в реальной жизни они почти всегда будут), числитель должен быть умножен на обратный знаменатель. На шаге 1 важно, чтобы k не повторялись в разных подписях и чтобы третья сторона не предполагала, что это будет возможно, т. е., k должен быть либо случайным, либо порожденным детерминированными средствами, которые хранятся в тайне от третьих сторон. В противном случае можно было бы извлечь закрытый ключ из шага 4, поскольку s, z, r, k и n все известны.

Выбираем номер 17.

Наша переменная:

$z = 17$ (данные) – $N = 79$ (заказ) – $G = (2, 22)$ (базовая точка) – $d = 2$ (закрытый ключ).

1. Выберите случайное число:

$k = \text{rand}(1, n-1)$ – $k = \text{rand}(1, 79-1)$ – $k = 3$ (это действительно случайно? Хорошо вы получили нас, но это сделает наш пример проще!).

2. Вычислить точку. Это делается так же, как и определение открытого ключа, но для краткости опустите арифметику для сложения точек и удвоения точек.

$(x, y) = 3G$ – $(x, y) = G + 2G$ – $(x, y) = (2, 22) + (52, 7)$ – $(x, y) = (62, 63)$ – $x = 62$ – $y = 63$.

3. Найти r :

$r = x \bmod n$ – $R = 62 \bmod 79$ – $r = 62$.

4. Найти s :

$$s = (z + r * d) / K \bmod n \quad - s = (17 + 62 * 2) / 3 \bmod 79 \quad - s = (17 + 124) / 3 \bmod 79 \quad - s = 141 / 3 \bmod 79 \quad - s = 47 \bmod 79 \quad - s = 47.$$

Обратите внимание, что выше мы смогли разделить на 3, так как результат был целым числом. В реальных случаях мы будем использовать обратное k (как и раньше, мы скрыли некоторые детали goгу, вычисляя его в другом месте):

$$s = (z + r * d) / K \bmod n \quad - s = (17 + 62 * 2) / 3 \bmod 79 \quad - s = (17 + 124) / 3 \bmod 79 \quad - s = 141 / 3 \bmod 79 \quad - s = 141 * 3^{-1} \bmod 79 \quad - s = 141 * 53 \bmod 79 \quad - s = 7473 \bmod 79 \quad - s = 47.$$

5. Наша подпись-пара $(r, s) = (62, 47)$.

Как и в случае с закрытым и открытым ключами, эта подпись обычно представлена шестнадцатеричной строкой.

Проверка подписи открытым ключом

Теперь у нас есть некоторые данные и подпись для этих данных. Третья сторона, у которой есть наш открытый ключ, может получить наши данные и подпись и проверить, что мы являемся отправителями. Давайте посмотрим, как это работает.

Поскольку Q является открытым ключом и другими переменными, определенными как раньше, шаги для проверки подписи следующие:

1. Убедитесь, что r и s находятся в диапазоне от 1 до $n - 1$.
2. Вычислить $w = s^{-1} \bmod n$.
3. Вычислить $U = Z * W \bmod n$.
4. Вычислить $v = r * w \bmod n$.
5. Вычислить точку $(x, y) = uG + vQ$.
6. Убедитесь, что $r = x \bmod n$. Подпись недействительна, если она не является.

Почему эти шаги работают? Наши переменные, еще раз:

$$z = 17 \text{ (данные)} \quad - (R, s) = (62, 47) \text{ (подпись)} \quad - N = 79 \text{ (заказ)} \quad - G = (2, 22) \text{ (базовая точка)} \quad - Q = (52, 7) \text{ (открытый ключ)}.$$

1. Убедитесь, что r и s находятся в диапазоне от 1 до $n - 1$. Проверьте и проверьте.

$$r: 1 <= 62 < 79 \quad - s: 1 <= 47.$$

2. Вычислить w :

$$w = s^{-1} \bmod n \quad - W = 47^{-1} \bmod 79 \quad - w = 37.$$

3. Вычислить u :

$$U = ZW \bmod n \quad - U = 17 * 37 \bmod 79 \quad - U = 629 \bmod 79 \quad - u = 76.$$

4. Вычислить v :

$$v = RW \bmod n \quad - V = 62 * 37 \bmod 79 \quad - V = 2294 \bmod 79 \quad - v = 3.$$

5. Вычислить точку (x, y) :

$$(x, y) = uG + vQ.$$

Давайте разберем точки удвоения и сложения в uG и vQ отдельно.

$$\begin{aligned} uG &= 76G \quad - uG = 2(38G) \quad - uG = 2(2(19G)) \quad - uG = 2(2(G + 18G)) \\ - uG &= 2(2(G + 2(9G))) \quad - uG = 2(2(G + 2(G + 8G))) \quad - uG = 2(2(G + 2(G + 2(4G)))) \\ - uG &= 2(2(G + 2(G + 2(2G)))) \end{aligned}$$

Используя трюк группировки, мы уменьшаем 75 последовательных операций сложения только до шести операций удвоения точки и двух операций сложения точки. Эти трюки пригодятся, когда цифры станут действительно большими.

Наш путь изнутри:

$$\begin{aligned} uG &= 2(2(G + 2(G + 2(2(2(2, 22)))))) \quad - uG = 2(2(G + 2(G + 2(2(52, 7)))))) \\ - uG &= 2(2(G + 2(G + 2(25, 17)))) \quad - uG = 2(2(G + 2((2, 22) + (21, 42)))) \\ - uG &= 2(2(G + 2(13, 44))) \quad - uG = 2(2((2, 22) + (66, 26))) \\ - uG &= 2(2(38, 26)) \quad - uG = 2(27, 40) \quad - uG = (62, 4). \end{aligned}$$

А теперь для vQ :

$$\begin{aligned} vQ &= 3Q \quad - vQ = Q + 2Q \quad - vQ = Q + 2(52, 7) \quad - vQ = (52, 7) + (25, 17) \\ - vQ &= (11, 20). \end{aligned}$$

Объединяя их:

$$(x, y) = uG + vQ \quad - (x, y) = (62, 4) + (11, 20) \quad - (x, y) = (62, 63).$$

Ясно, что этап 5 составляет основную часть работы. Для заключительного шага, убедитесь, что:

6. $r = x \bmod n$, где

$$r = x \bmod n \quad - 62 = 62 \bmod 79 \quad - 62 = 62.$$

Мы разработали некоторую интуицию о глубоких математических отношениях, которые существуют между публичными и частными ключами. Мы видели, как даже в простейших примерах математика за сигнатурами и верификацией быстро усложняется, и мы можем оценить огромную сложность, которая должна быть задействована, когда параметры являются 256-битными числами. Мы видели, как умное применение простейших математических процедур может создать односторонние функции «ловушки», необходимые для сохранения информационной асимметрии, которая определяет владение биткоином. И у нас есть новая уверенность в надежности системы, при условии, что мы тщательно охраняем знание наших закрытых ключей.

Другими словами, именно поэтому обычно говорят, что биткойн «поддерживается математикой».

Волков Антон Григорьевич¹,
*курсант факультета подготовки специалистов
 в области информационной безопасности
 Московского университета
 МВД России имени В.Я. Кикотя*

Пузарин Андрей Валерьевич²,
*начальник кафедры специальных информационных технологий
 учебно-научного комплекса информационных технологий
 Московского университета
 МВД России имени В.Я. Кикотя*

СТРАННОСТИ В АЛГОРИТМАХ ГОСТ КУЗНЕЧИК И СТИБОГ

В 2016 г. исследователи показали, что таблица перестановки в российских алгоритмах хеширования и шифрования Кузнечик и Стрибог имеет определенную структуру, после того, как в Стрибоге была найдена тривиальная ошибка, уменьшающая его стойкость с 2^{512} до 2^{266} .

29 января 2019 г. было опубликовано новое исследование «Partitions in the S-Box of Streebog and Kuznyechik», которое недвусмысленно намекает на теоретическую возможность бекдора в этих алгоритмах.

Итак, S-Box или таблица замены, ключевой элемент безопасности во многих алгоритмах симметричного шифрования и хеширования. Пример такой таблицы приведен ниже.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

¹ © Волков А. Г., 2019.

² © Пузарин А. В., 2019.

В общем случае эта таблица сопоставляет одной последовательности бит другую, а вот по какому принципу всегда большой вопрос.

Государственные структуры нередко ограничиваются их публикацией без какого-либо рационального объяснения. В случае с DES АНБ предложило изменить S-Box до того, как алгоритм стал стандартом. Только через много лет выяснилось, что это изменение на самом деле повышало стойкость DES к дифференциальному криптоанализу.

Согласно новым ГОСТам, авторы декларировали, что таблица замен выбрана случайным образом. Вот слайд из презентации алгоритма, на котором указано, что авторы выбирали таблицу случайным образом. Так, чтобы у нее не было явной структуры, которая помогла бы произвести эффективный криптоанализ (красным отмечено то, что выбрали).

Методика разработки Принципы синтеза Краткое описание базовых операций

Синтез нелинейного преобразования

Выбор из известных классов

- близкие к оптимальным значения некоторых криптографических параметров
- очевидная аналитическая структура
- обращение элемента в поле

Случайный поиск с заданным ограничением на параметры

- не оптимальны по совокупности значений основных криптографических характеристик
- не обладают выраженным аналитическим строением

Борислав Шенников ФСБ России
Принципы синтеза переносимого алгоритма базового шифрования [18/74]

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$\mathcal{I}$	0	1	c	8	6	f	4	e	3	d	b	a	2	9	7	5
ν_0	2	5	3	b	6	9	e	a	0	4	f	1	8	d	c	7
ν_1	7	6	c	9	0	f	8	1	4	5	b	e	d	2	3	a
ϕ	b	2	b	8	c	4	1	c	6	3	5	8	e	3	6	b
σ	c	d	0	4	8	b	a	e	3	9	5	2	f	1	6	7

Table 1: The non-linear functions needed to compute π .

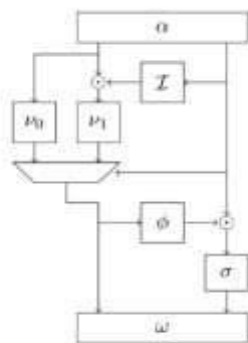


Figure 1: Our decomposition of π . The “wires” transmit 4 bit.

Но, во-первых, как оказалось, она сгенерирована не случайным образом, а с помощью хитрого алгоритма, который был определен еще в 2015 г.

Во-вторых, авторы не оставили попыток выяснить причину такого подхода к конструированию S-Box и натолкнулись на очень интересные результаты.

Оказалось, что алгоритмов, которые формируют таблицу замены, больше чем один. Разные группы исследователей описали абсолютно разные алгоритмы, которые не имеют почти ничего общего, но приходят к одной и той же таблице.

Это навело авторов оригинального исследования на мысль покопаться в структуре этих алгоритмов поглубже и найти общие элементы, что им с успехом удалось.

TKlog. TKlog – это конструкция перестановки, которую авторы криптоанализа называли в честь российской конторы ТК-26, где и были созданы Кузнечик со Стрибогом. Ключевым свойством TKlog является использование дискретного логарифмирования, прямо как в асимметричной криптографии.

Что важно, так это тот факт, что оба варианта функции замены из ГОСТовских алгоритмов являются частным случаем конструкции TKlog. Как и еще одна функция замены из белорусского алгоритма BelT. Функции разные, но сводятся к одной.

Скрытый текст. Тот факт, что разных вариантов преобразования TKlog крайне мало, говорит о преднамеренном использовании именно этой, нерандомизированной структуры вместо случайной, показанной нам на слайде.

Разбиения на смежные классы. Ключевым свойством преобразования TKlog является то, что оно работает с так называемыми смежными классами (cosets). И сопоставляет одни другим.

Проблема в том, что эти смежные классы бывают мультипликативными, как во всех обычных алгоритмах, и бывают аддитивными. Так вот,

единственный известный случай, когда аддитивные смежные классы использовались в функции замены блочных шифров – специальное создание бекдора. Информация об этом находится в работе 2016 г., такие бекдоры называются NOBUS (сокр. от *nobody but us*) – это уязвимости, которые могут эксплуатировать только сами авторы алгоритмов.

Авторы криптоанализа не представили новых атак на существующие алгоритмы ГОСТ, но задались справедливым вопросом целесообразности всего этого цирка с якобы случайной таблицей перестановки. АНБ не так давно попыталось протолкнуть в стандарты свои легковесные симметричные алгоритмы Simon и Speck. И самого факта наличия таблиц замены с дизайном, описания которого предоставлено не было, хватило чтоб их прогнали.

Глебо Дарья Владимировна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Пименова Оксана Владимировна²,
*доцент кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

НЕЙРОННЫЕ СЕТИ

Избегая сложных формулировок и нагромождений терминов, нейронную сеть проще всего описать как устройство, функционирующее по принципу головного мозга человека. Нейронные сети могут быть самых разных видов (сверточные, рекуррентные, прямого распространения и т. д.), отличаться по типу поставленной задачи (анализ, прогнозирование, распознавание образов и т. д.) и по своей структуре, однако в любом случае это некая математическая модель, представленная в виде программного и аппаратного обеспечения и имеющая целью обучиться делать выводы из обновляемых данных подобно человеку, принимающему то или иное жизненное решение.

Главное отличие нейронной сети от обычной компьютерной программы способность обучаться, т. е., результат работы нейронной сети может быть основан на данных, которых не существовало на стадии обучения. Нейронные сети могут решать широкий круг задач обработки и анализа данных – распознавание и классификация образов, прогнозирование, управление и т. д.

Конкурентами у нейросетей являются классические методы статистического прогнозирования/распознавания/классификации (некоторое сравнение с методами статистики уже было проведено при обсуждении преимуществ нейронных сетей), методы идентификации систем и автоматического управления, алгоритмы идентификации зависимостей и «машинного обучения» (machine learning), а также технологии искусственного интеллекта.

¹ © Глебо Д. В., 2019.

² © Пименова О. В., 2019.

Поэтому там, где задачи уже решаются этими конкурирующими методами – там возможно и применение нейросетей, практически без необходимости переформулировать или как-то по-иному ставить задачу. И по причине бОльшей гибкости нейротехнологий результаты (точность решения и т. д.) могут оказаться значительно лучше.

Возможные способы использования или программирования

Чаще всего используются программы-нейроимитаторы, которые работают на обычных компьютерах, а современные нейроалгоритмы позволяют быстро обрабатывать значительные объемы информации, т. е. использовать нейросети для решения сложных реальных задач. Программы включают в себя как набор базовых операций по созданию, обучению и манипулированию нейронными сетями, исходными данными, свойствами нейросетей и нейрорешений, так и автоматизированные процедуры выполнения наиболее рутинных цепочек действий, например, для определения оптимальных настроек сети и алгоритма обучения.

Универсальные современные нейропрограммы имеют возможности сгенерировать описание обученной нейросети на некотором языке программирования, чтобы полученный программный модуль можно было вставить в программу пользователя. Также программа пользователя может использовать стандартные средства межпрограммной коммуникации (DDE, OLE, COM в среде Windows) для организации доступа к нейросетям в универсальных нейропрограммах (нейросеть остается работать в той среде, которая создала ее нейросетевые программы, а программа пользователя только отдает нужные команды-данные и получает результаты).

На специфические вычислительные архитектуры (например, сигнальные процессоры) обычно переносят сгенерированное программой-нейроимитатором описание обученной нейронной сети на языке программирования (например, на языке C). Для ПЛИС/PLM/FPGA-кристаллов существуют и CAD-системы, в которых номенклатуру нейроэлементов можно создать-описать в виде набора модулей и потом из этих модулей путем выбора и «перетаскивания» мышкой собрать нужную топологию-архитектуру нейросети, затем проект скомпилировать и «прошить» кристалл. В настоящее время возможно создавать нейрокомпьютеры на базе видеокарт (графических процессоров), используя технологии CUDA и OpenCL.

Естественно, остается возможность не пользоваться чем-то готовым, а запрограммировать все вручную. Ну, или можно взять готовое

нейроядро (программную библиотеку) и добавить нужные механизмы доступа к своим данным, интерфейс для манипулирования данными и/или настройками методов их обработки, и средства отображения/визуализации результатов. Так что существует широкий спектр достаточно универсальных способов организации инструментальных средств и процесса применения нейронных сетей на различной программно-аппаратной базе. Всегда можно подобрать наиболее оптимальный для некоторой задачи вариант, ведь многое определяется свойствами задачи и требованиями к решению, а также компетентностью пользователя или разработчика.

*Дутикова Анастасия Александровна¹,
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

*Пузарин Андрей Валерьевич²,
начальник кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ С USB-НАКОПИТЕЛЕЙ В ЦЕЛЯХ ПРОВЕДЕНИЯ СУДЕБНО-КОМПЬЮТЕРНОЙ ЭКСПЕРТИЗЫ

Развитие информационных технологий привели к тому, что почти вся информация приобрела цифровой вид. Теперь мы можем хранить, переносить информацию на различных накопителях. В данной работе речь пойдет о так называемых флешках. Хороши ли они? Какие бывают у них повреждения?

Тема восстановления данных с usb-накопителей очень актуальна и всесторонняя. Целью статьи является проведение исследования по программам восстановления данных. Но прежде чем до этого дойти, необходимо выяснить предназначение флешек, какие чипы памяти и файловые системы используют данные накопители, а также выявить причины удаления данных и изучить приемы восстановления данных.

Usb- накопители имеют некоторые преимущества перед другими носителями: мобильное хранение занимает мало места (в отличие от внешнего HDD, которые не всегда удобно переносить), довольно-таки дешево (в принципе, как и внешние HDD). Но у накопителей данного вида есть огромный минус – непредсказуемая надежность.

Что же сказать о чипах? По реализации и своей простоте SLC память более экономична и сложна, но она имеет уникальный плюс - долговечность. Срок службы SLC твердотельных накопителей превосходит срок службы накопителей на чипах MLC. Тем не менее, нынешний уровень технологий достиг того уровня, что долговечность MLC чипов памяти стала сопоставимой с выигрышем в цене, которую пользователь получает при приобретении данных решений.

¹ © Дутикова А. А., 2019.

² © Пузарин А. В., 2019.

Если рассматривать файловые системы, то FAT32 не такая прочная, как NTFS, так как она не использует журналирование. Из-за сбоя, например, выключения электричества, прерывания записи, информация может просто напросто исчезнуть, при этом у NTFS потерянная информация будет стремиться к минимуму. Среди рассмотренных USB флеш-накопителей самым удачным оказался SanDisk Ultra Dual Type-C. Именно он показывает лучшие результаты по скоростным показателям, оснащен двумя разъемами и выполнен в красивом качественном корпусе.

Если вы используете смартфон с разъемом microUSB, то ваш выбор падет на SanDisk Ultra Dual Drive m3.0. Данный накопитель позволит подключить его к вашему смартфону и перенести на него (или с него на компьютер) данные. Скорость записи в данном случае будет ниже, но скорость чтения остается очень высокой, а это главное.

SanDisk Ultra USB Type-C заслуживает звание очень смелого решения. И дело даже не в том, что скоростные показатели оказались самыми низкими среди рассматриваемых образцов, а в том, что накопитель оснащен единственным разъемом USB Type-C. Остается еще слишком много компьютеров и мобильных устройств, не оснащенных USB Type-C, а значит это сильно сузит круг потенциальных потребителей.

USB-накопители хранят файлы во флэш-памяти и подключаются к ПК посредством интерфейса USB. Можно отметить, что наиболее скоростным и долговечным типом флэш-памяти является SLC. Однако из-за высокой цены, эту память вытеснили более дешевые типы. Бюджетным, и в тоже время, менее скоростным является тип TLC. И, наконец, золотой серединой является тип MLC, который обеспечивает более высокую скорость и надежность по сравнению с обычными дисками и при этом является не слишком дорогим типом. Ну а что касается файловых систем: FAT32 или NTFS для флешки? Если мы будем хранить документы и фотографии, то однозначно FAT32. Если на флешке содержатся файлы огромного размера, то необходимо использовать NTFS. USB 2.0 и 3.0: отличия в первую очередь в качестве работы – более новая версия лучше, хоть и немного дороже. Современное оборудование выпускается с интерфейсом 3.0, поэтому приобретать компьютер целесообразно тоже с такой версией. Устройства разных версий совместимы друг с другом и работают приемлемо, хоть и производительность их падает. Среди рассмотренных USB флеш-накопителей

самым удачным оказался SanDisk Ultra Dual Type-C. Именно он показывает лучшие результаты по скоростным показателям, оснащен двумя разъемами и выполнен в красивом качественном корпусе.

К плюсам можно отнести: стильный дизайн, высокую скорость чтения и удобное подключение к мобильным устройствам. Из минусов можно отметить низкую скорость записи (кроме SanDisk Ultra Dual Type-C).

M.2 – это новый, используемый для плат расширения разъем, устанавливаемый в компьютеры. Разъем M.2 взаимодействует с шинами PCI Express 3.0, SATA 3 и USB 3.0. Благодаря этому производит

Также флеш карты могут иметь разные повреждения: от механических до логических, вследствие чего потребуется восстановление. Чтобы избежать неприятностей, как вариант, можно архивировать информацию с помощью программ резервного копирования. Они позволяют выбирать папки и файлы для регулярного сохранения. Ну, а если же файлы все-таки исчезли, то рекомендую применять программы для восстановления файлов Recuva, Easy Recuva, R-studio и другие. Я использовала Recuva. Чем удобна данная утилита? В первую очередь, – понятный интерфейс и русская версия. Это позволяет быстро разобраться в функциональной части даже новичкам. Так же данная программа бесплатна.

Как же восстановление данных помогает ОВД при расследовании и раскрытии преступления в органах внутренних дел? При поиске информации мы пользуемся всеми способами, и выше перечисленный – один из них. Восстановление информации помогает в раскрытии и расследовании преступления. Главное, чтобы эксперт обладал специальными знаниями, выбирал правильные инструменты, средства для восстановления, мог разобраться какое повреждение у накопителя, а также использовать подходящие режим восстановления, которые помогут достигнуть определенных задач и целей.

Ершов Константин Игоревич¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Пузарин Андрей Валерьевич²,
*начальник кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ИССЛЕДОВАНИЯ В ОБЛАСТИ ПРОЕКТИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Архитектура системы защиты информации (СЗИ) должна базироваться на следующих принципах:

- СЗИ рассматривается как комплекс средств защиты, направленных на обеспечение безопасности информационной системы и обрабатываемой в ней информации;
- каждое средство защиты информации является комплексом механизмов защиты, реализованных в данном средстве;
- механизмы защиты должны присутствовать на каждом из возможных информационных потоков типа «объект–субъект» и «субъект–субъект»;
- каждый механизм защиты призван нейтрализовать конкретную угрозу, существующую на заданном информационном потоке.

При построении СЗИ специалисты по информационной безопасности (ИБ) формируют перечень внедряемых средств защиты, основываясь на собственном опыте. На сегодняшний день не существует четкого перечня механизмов защиты, реализованных в отдельно взятом средстве защиты, и их сопоставления с конкретными угрозами. Описываемая в данном разделе методика позволяет представить средства защиты в виде перечня механизмов защиты информации.

Для анализа и оценки существующей в организации СЗИ необходимо:

- построить схему защищаемых информационных потоков (схему документооборота);

¹ © Ершов К. И., 2019.

² © Пузарин А. В., 2019.

- для каждого информационного потока определить перечень установленных средств защиты информации (СрЗИ);

- перечень угроз информации для каждого информационного потока.

Для составления схемы документооборота необходима модель документооборота, включающая перечень типовых информационных потоков. Таким образом, схема документооборота – это описание реальных информационных потоков в организации в виде структуры, состоящей из типовых элементов (объектов, хранящих или передающих информацию, и субъектов, обрабатывающих информацию) и типовых каналов связи между ними. Модель угроз содержит типовые угрозы для типовых информационных потоков. Классификация механизмов защиты напрямую зависит от угроз. При этом для каждой типовой угрозы существует собственный механизм защиты.

В рамках методики необходима конкретизация состава механизмов защиты, реализованных во внедренных и потенциально рекомендуемых специалистом по ИБ СрЗИ. Бизнес-процесс «Формирование рекомендуемого перечня СрЗИ» представлен в нотации IDEF0 (рис. 1).



Рис. 1. Методика формирования рекомендованного перечня средств защиты информации

Формирование рекомендуемого перечня СрЗИ происходит в три этапа (рис. 2):

- определение перечня угроз для каждого существующего в организации информационного потока;

-) определение для каждого существующего информационного потока функционирующих в организации механизмов защиты и их достаточности;

– выбор для каждого существующего информационного потока рекомендуемых СрЗИ, позволяющих нейтрализовать «незакрытые» угрозы.

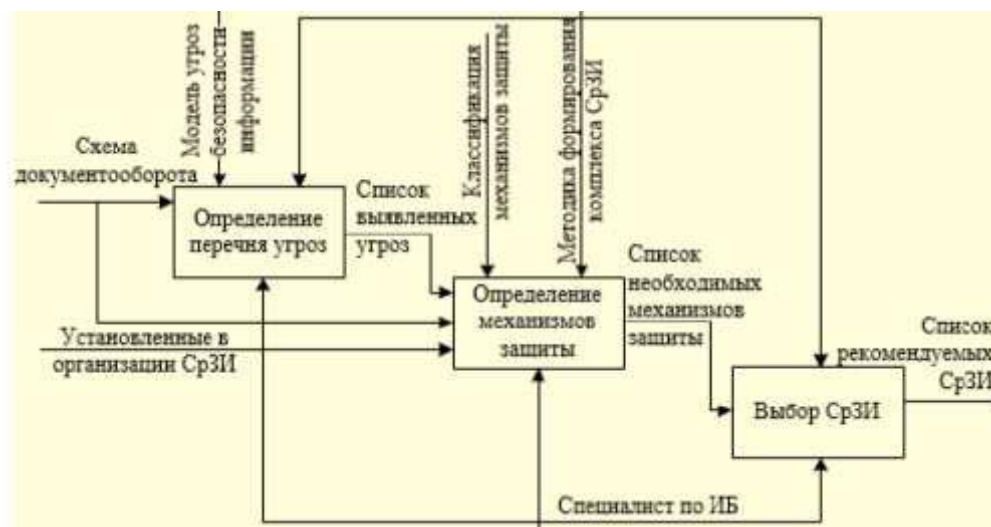


Рис. 2. Декомпозиция методики формирования рекомендуемого перечня средств защиты информации

Модель документооборота

При построении модели документооборота за основу было принято то, что действия, направленные на информацию и ее носители, могут происходить в разных средах. Среди них можно выделить такие среды, как:

- видовая – среда, где существует угроза визуального получения информации, т.е. возможность получения информации из документа без использования дополнительных преобразований;
- физическая – среда, где существует угроза получения доступа непосредственно к самому носителю информации;
- акустическая/виброакустическая – среда, где существует угроза утечки речевой информации;
- среда сигналов – среда, где существует угроза получения информации через побочные электромагнитные излучения носителей и средств ее передачи;
- виртуальная – среда, где существует угроза получения информации непосредственно из оперативной памяти.

На рис. 3 представлена разработанная модель документооборота. Элементы полученного графа представлены ниже.

Носители информации:

- V1 – объект, хранящий аналоговую информацию, в том числе печатные документы;
- V2 – человек;
- V3 – объект, хранящий цифровую информацию;

V4 – процесс.

Каналы передачи информации:

e1 – в визуальной среде;

e2 – в акустической среде;

e3 – в электромагнитной среде;

e4 – в виртуальной среде.

Каналы удаленной передачи информации:

e3' – в электромагнитной среде;

e4' – в виртуальной среде.

На данной модели документооборота было построено множество документопотоков:

$G = \{V, e\}$,

где $V = \{V1, V2, V3, V4\}$ – это множество состояний, $e = \{e1, e2, e3, e4\}$ – множество каналов передачи информации.

Под документопотоком понимается поток документов между пунктами обработки и создания информации (руководителями организации и структурных подразделений, специалистами) и пунктами технической обработки документов: экспедицией, секретариатом, канцелярией.

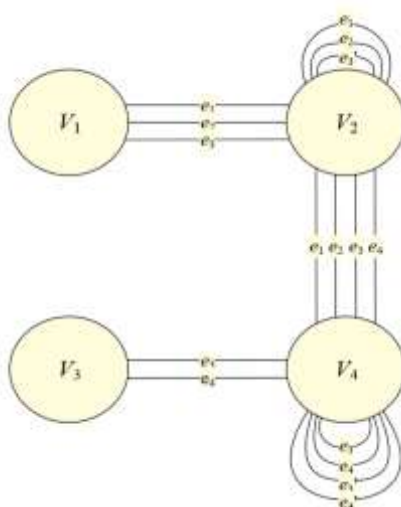


Рис. 3. Модель документооборота

Модель угроз обрабатываемой информации

Комплексная модель угроз информационной безопасности состоит из трех элементов:

- модель угроз обрабатываемой информации и ее носителям;
- модель угроз безопасности информационной системы;
- модель угроз безопасности СЗИ.

При этом ко всем трем элементам существуют угрозы конфиденциальности и целостности, а к обрабатываемой информации – дополнительно угрозы доступности. Например, применительно к обрабатываемой информации можно выделить 4 типовые угрозы конфиденциальности, применимые к каждому документопотоку:

- подмена получателя V_i ;
- подмена получателя V_j ;
- использование несанкционированного канала e_z ;
- контроль злоумышленником канала e_z .

Примером подобных типовых угроз могут являться соответственно:

- отправка защищаемой информации ложному объекту в сети (из-за подмены IP-адреса, адреса вебсайта, электронной почты получателя при типе документопотока $\{V_4, e_4', V_4\}$) или запись информации ограниченного доступа в незащищенный файл (при типе документопотока $\{V_3, e_4', V_4\}$);
- несанкционированное считывание информации из защищаемого файла (при типе документопотока $\{V_3, e_4', V_4\}$); □
- использование сетевых протоколов, не поддерживающих шифрование (при типе документопотока $\{V_4, e_4', V_4\}$);
- перехват сетевых пакетов за счет анализа сетевого трафика (при типе документопотока $\{V_4, e_4', V_4\}$).

Таким образом, при использовании разработанной модели можно получить типовой набор угроз для каждого элементарного документопотока в схеме документооборота, что приводит к формализации процесса составления перечня угроз и ликвидации субъективизма при получении искомого результата.

Модель системы защиты информации

Построение модели системы защиты информации основано на классификации механизмов защиты в зависимости от элементарного документопотока и типа угрозы. Для каждого документопотока в каждой из сред были выбраны типовые механизмы защиты информации в соответствии с типовыми угрозами. Результаты классификации механизмов защиты от угроз конфиденциальности информации в виртуальной среде представлены в табл. 1. Типы механизмов защиты, обозначенных в табл. 1:

- идентификация и аутентификация (ИА);
- управление доступом (УД);
- очистка памяти (ОП);
- регистрация событий (РС);
- шифрование (ШИ).

Если рассматривать элементарный документопоток между человеком (пользователем) и любым прикладным процессом по виртуальному каналу, то подобным каналом будут являться драйверы устройств ввода/вывода. Перечень угроз конфиденциальности передаваемой информации и соответствующих механизмов защиты представлен в табл. 2.

Типы угроз	Типы механизмов защиты		
	Виды документопотоков		
	Человек – процесс $\{V_2, e_4, V_4\}$	Носитель шифровой информации – процесс $\{V_3, e_4, V_4\}$	Процесс – процесс $\{V_4, e_4, V_4\}$
1-й тип	ИА УД РС ШИ	ИА УД РС ШИ	ИА УД РС ШИ
2-й тип	ИА УД РС ШИ	ИА УД РС ШИ	ИА УД РС ШИ
3-й тип	ИА УД РС	ИА УД РС	ИА УД РС
4-й тип	ОП РС	ОП РС	ОП РС

Табл. 1. Соответствие механизмов защиты типовым угрозам в виртуальной среде

Угроза	Механизмы защиты
Получение несанкционированным пользователем данных, обрабатываемых прикладным процессом	ИА – аутентификация пользователя при запуске программы. УД – разграничение доступа пользователей к запуску программ. РС – регистрация работы пользователя с программой. ШИ – вывод пользователю только закодированной информации
Ввод защищаемой информации в несанкционированную программу	ИА – проверка аутентичности исполняемого файла. УД – реализация замкнутой программной среды. РС – регистрация работы пользователя с программой. ШИ – ввод пользователем только закодированной информации
Использование несанкционированного (некорректного) драйвера устройства при вводе/выводе данных	ИА – проверка аутентичности драйвера при запуске. УД – разграничение доступа пользователей к устройствам ввода/вывода в операционной системе. РС – регистрация событий, связанных с работой драйвера
Считывание обрабатываемой информации из буферов в оперативной памяти, закрепленных за устройством ввода/вывода	ОП – очистка буферов оперативной памяти. РС – регистрация событий, связанных с очисткой памяти

Таблица 2. Пример механизмов защиты для документопотока $\{V_2, e_4, V_4\}$

Ильина Валерия Игоревна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Лустин Владимир Иванович²,
*старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ПРИМЕНЕНИЕ КИБЕРРАЗВЕДКИ ОРГАНАМИ ВНУТРЕННИХ ДЕЛ В БОРЬБЕ С ПРЕСТУПНОСТЬЮ В ИНФОРМАЦИОННОЙ СФЕРЕ

Прогресс в науке и технике в современном мире порождает и новые виды преступлений в различных сферах жизнедеятельности общества. Всеобщая информатизация, активное внедрение современных информационных технологий в экономике и культуре образа жизни человека вынуждают различные институты разрабатывать новые средства и методы защиты их интересов в информационной сфере.

В условиях быстро меняющейся криминогенной обстановки в стране и качественного изменения видов преступности требуется принятие комплексных мер, направленных на установление надежного правопорядка в стране, обеспечение защиты жизни, здоровья граждан, собственности, безопасности общества и государства от преступных посягательств, особенно, в информационной сфере.

Одной из социальных проблем современного технократического общества стало появление компьютерной преступности, причиняющей колоссальный вред существующим информационным отношениям.

Масштабы ущерба, причиняемого компьютерными преступлениями в Российской Федерации, впечатляют. Так, по оценкам аналитиков компании Group-IB объем рынка киберпреступности в Российской Федерации в 2012 г. составил 1,93 млрд долл.³, а с середины 2013 г. по

¹ © Ильина В. И., 2019.

² © Лустин В. И., 2019.

³ URL : <http://digit.ru/business/20130910/405335397>.

середину 2014 г. в России и СНГ русскоговорящие хакеры «заработали» 2,5 млрд долл., что составляет 2 % от глобального рынка¹.

Американская корпорация Symantec оценила ущерб от киберпреступности в России за 2013 г. в 1 млрд долл., а в 2012 г. в 1,48 млрд долл. При этом общий ущерб от киберпреступности в мире в 2013 г. составил 113 млрд долл.².

Анализ специальной и научной литературы показывает, что вопросам противодействия компьютерным преступлениям в Российской Федерации уделяется достаточно пристальное внимание со стороны научного сообщества³.

Однако, что же следует понимать под компьютерной преступностью? На этот, казалось бы, простой вопрос в криминологической науке нет однозначного ответа, и до сих пор ведутся многочисленные дискуссии о содержании и значении этого юридического понятия. В настоящее время в отечественной науке сложилось несколько подходов к определению рассматриваемого понятия. Помимо определений компьютерных преступлений, их видов, также существуют и методы борьбы с ними. Использование высоких технологий предоставляет нам (правоохранителям) широкий спектр различных средств в вопросах противодействия «киберпреступности». В качестве инструмента по расследованию преступлений в сфере высоких технологий выступает киберразведка.

На основе выполненного исследования выявлены возможности и направления использования результатов киберразведки органами внутренних дел в борьбе с преступностью в информационной сфере

Вопрос применения результатов киберразведки в доказывании по уголовным делам остается открытым, так как для этого отсутствует законодательная основа. Законодательно термин «киберразведка» не определен и рассматривать его как один из видов оперативно-розыскного мероприятия не представляется возможным.

Предварительное расследование, включающее в себя проведение следственных действий и оперативно-розыскных мероприятий, имеет в своем распоряжении широкий инструментарий, способствующий на

¹ URL : <http://www.group-ib.ru/index.php/investigation/1063-link-nezavisimye>

² URL : <http://go.symantec.com/norton-report-2013/>

³ Евдокимов К. Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации // Академический юридический журнал. – 2015. – № 1 (59). – С. 21–31.

должном уровне выполнять задачи уголовного судопроизводства. Применение такого инструмента, как киберразведка, дает правоохранителю возможность раскрывать и расследовать преступления в сфере высоких технологий. Но для этого необходимо развивать соответствующую законодательную базу.

Анализ средств и методов ведения киберразведки позволил определить различные этапы КР и выявить состав информации, подлежащей защите на предварительном этапе КР: данные о характере и режиме работы, АСОД; о составе и структуре самой АСОД; об используемом программном обеспечении; о протоколах управления и взаимодействия, о квалификации персонала.

Предлагается осуществлять защиту сведений о функционировании АСОД и квалификации персонала, начиная с этапа предпроектной стадии СЗИ. На последующих этапах при разработке технического задания и на стадиях проектирования, реализации объекта информатизации организационно-технические мероприятия по защите информации строятся с учетом обеспечения конфиденциальности ОИ.

Предложены организационно-технические и технические мероприятия по защите информации от предварительной киберразведки на разных стадиях создания системы защиты информации.

Темпы развития современных информационных технологий опережают темпы разработки рекомендательной и нормативно-правовой базы и руководящих документов области защиты информации. Поэтому решение вопроса об оценке уровня безопасности в той или иной организации обязательно связано с проблемой выбора критериев оценки информационных рисков организации и эффективности защиты информации.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.) // Российская газета. – 1993. – № 237.
2. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности».
3. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (с изменениями от 18 июля 1997 г., 21 июля 1998 г., 5 января, 30 декабря 1999 г., 20 марта 2001 г., 10 января, 30 июня 2003 г., 29 июня, 22 августа 2004 г., 2 декабря 2005 г.).
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

5. Постановление Правительства Российской Федерации от 1 июля 1996 г. № 770 «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы оперативно-технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и перечня видов оперативно-технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности».

6. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 31 декабря 2015 г. № 683).

7. Доктрина информационной безопасности Российской Федерации. (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646).

8. Доктрина информационной безопасности Российской Федерации. (утв. Указом Президента Российской Федерации от 9 сентября 2000 г. № Пр-1895).

9. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Защита информации.

10. Белоглазов, Е. Г. Макаренков, Д. Е., Каретников М. К. Практикум, по компьютерной разведке : учебное пособие. Применение информационных технологий в аналитической разведке : курс лекций. – М. : Московский университет МВД России, 2006.

11. Курушин, В. Д., Минаев, В. А. Компьютерные преступления и информационная безопасность. – М. : Новый Юрист, 1998.

12. Меньшаков, Ю. К. Защита объектов и информации от технических средств разведки. – М. : Российский государственный гуманитарный университет, 2002.

Каменев Павел Олегович¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Клочкова Екатерина Николаевна²,
*доцент кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ СТАНДАРТНЫХ МАТЕМАТИЧЕСКИХ ПАКЕТОВ ДЛЯ РЕШЕНИЯ ЗАДАЧ ОПТИМИЗАЦИИ

Люди всегда были в поисках оптимальных решений, именно это привело к созданию первых математических методов и уже в XVIII в. были заложены основы математической оптимизации. До второй половины XX в. методы оптимизации применялись очень редко, поскольку требовало большой математической работы, которую было очень трудно, а порой невозможно реализовать без вычислительных приборов. Если отвлечься от экономического, физического, химического или иного содержания этих задач, то все они сводятся к оптимизационной задаче: найти минимум или максимум функции на некотором множестве некоторого пространства.

В зависимости постановки задачи, любая из них может решаться разными методами, и наоборот, любой метод может применяться для решения разных задач. Методы оптимизации могут быть скалярными (оптимизация проводится по одному критерию), векторными (оптимизация проводится по многим критериям), поисковыми (включают методы регулярного и методы случайного поиска), аналитическими (методы дифференциального исчисления, методы вариационного исчисления и т. д.), вычислительными (основаны на математическом программировании, которое может быть линейным, нелинейным, целочисленным, динамическим и т. д.). Подвергаться оптимизации могут задачи, как с ограничениями, так и без них.

¹ © Каменев П. О., 2019.

² © Клочкова Е. Н., 2019.

Математические пакеты – это программы, включающие в себя средства для выполнения математических расчетов, начиная от простых арифметических вычислений, и заканчивая решением математических моделей, проверки различных гипотез и решением задач оптимизации.

Математические пакеты можно использовать как в обычном калькуляторе для решения простейших задач, так и в сложных программах, при генерировании графики или даже звука. В настоящее время практически все современные пакеты математического моделирования имеют встроенные функции символьных вычислений. Благодаря математическим пакетам, встроенным в программы можно сэкономить массу времени и избежать многих ошибок при вычислениях.

Задачи, решаемые с помощью математических пакетов:

- проведение математических исследований, требующих вычислений и аналитических выкладок;
- разработка и анализ алгоритмов;
- математическое моделирование и компьютерный эксперимент;
- анализ и обработка данных;
- визуализация, научная и инженерная графика;
- разработка графических и расчетных приложений.

Данные программы имеют обширную и удобную справочную систему, а также средства оформления отчетов. К математическим пакетам можно отнести программы типа Matlab, Mathcad, Mathematica, MS Excel и другие.

Оптимизация (от лат. optimum – наилучшее), процесс нахождения выбора наилучшего (оптимального) варианта из множества возможных. Одним из самых надежных способов нахождения наилучшего варианта является сравнительная оценка всех возможных вариантов (альтернатив). Зачастую, количество альтернатив бесконечно велико, поэтому, при поиске наилучшего варианта используются методы математического программирования (математические пакеты).

Применить эти методы можно, если есть строгая постановка задачи: задан набор переменных, установлена область их возможного изменения (заданы ограничения) и определен вид целевой функции (функции, экстремум которой нужно найти) от этих переменных.

Математические пакеты используют для решения реальных задач, помогая предприятиям оптимизировать свое производство. Возможность произведения сложных вычислений позволяет выбрать наиболее рациональный вариант, позволяющий увеличить выпуск той или иной

продукции. Выстраивание успешной стратегии является одним из главных факторов производства, с чем успешно справляются программы, использующие математические пакеты.

Различные математические пакеты

Mathematica. Пакет Mathematica зачастую применяется при расчетах в современных научных исследованиях, данный пакет является одним из самых крупных программных систем и реализует наиболее эффективные алгоритмы вычислений (например, исключение появления в программах побочных эффектов), благодаря чему и получил широкую известность в научной и образовательной среде.

Система Mathematica позволяет упрощать алгебраические выражения, дифференцировать, вычислять определенные и неопределенные интегралы, вычислять конечные и бесконечные суммы и произведения, решать алгебраические и дифференциальные уравнения и системы, а также раскладывать функции в ряды и находить пределы.

Mathematica решает численными методами (т. е. приближенными методами) задачи, которые не поддаются аналитическому решению. Она позволяет решать задачи оптимизации (линейного программирования, нахождения экстремумов функций), задачи математической статистики.

Система снабжена базой помощи. Богатые численные и символьные возможности системы Mathematica, мощные графические возможности (включая анимацию), встроенный язык программирования и удобные средства построения гипертекстовых связей между документами делают эту систему привлекательной как для исследовательской и практической деятельности, так и для обучения студентов.

Maple. Данный пакет называют системой символьных вычислений или системой компьютерной алгебры. Может вычислять как численные, так и аналитические расчеты. Помимо выполнения функций математического пакета, данная программа является довольно мощным научным графическим редактором.

Плюсы данной программы в простом и эффективном языке - интерпретаторе, а возможность преобразования кодов Maple в коды С делает его очень эффективным средством создания новых алгоритмов. Maple является первым универсальным математическим пакетом, который предлагает встроенную поддержку протокола TCP/IP для обеспечения динамического доступ к информации из других интернет ресурсов, например, к данным для финансового анализа в реальном времени или к данным о погоде.

MS Excel. Дополнительные возможности программы облегчают решение сложных прикладных задач. В программу MS Excel встроена удобная подсистема помощи, которая в любой момент готова выдать необходимую справку.

Применение электронных таблиц упрощает работу с данными и позволяет получать результаты без проведения расчетов вручную или специального программирования.

Программа MS Excel позволяет решать сложные задачи, связанные с финансовой и бухгалтерской работой предприятий: проводить широкий круг сложных вычислений в электронных таблицах, легко и быстро анализировать большой объем данных.

При альтернативном использовании математических пакетов возможно применение таких программ как: MSEquationEditor, MicrosoftAccess, SmallBusinessTools и т. д.

Применение математических пакетов

Целью любого производства является получение максимально возможной прибыли. На практике производство и сбыт продукции имеют большое количество ограничений, учет которых влияет на планирование ассортимента и количественные показатели. В математической модели производства можно учесть лишь часть этих показателей. В данном параграфе рассмотрены следующие задачи: составление оптимального производственного плана, оптимизация составления смесей.

Структура производственных моделей

Производственная математическая модель предназначена для формирования оптимального производственного плана или технологических операций при ограниченных временных, материальных, трудовых и производственных ресурсах. Критерием оптимальности является получение максимума прибыли или минимума издержек. Обычно планирование состоит из определения количества выпускаемой продукции или составляющих в пределах заданного ассортимента. Для того, чтобы создать математическую модель производственной фирмы, необходимо определить следующие параметры:

- постоянные нормативных затрат материалов, труда и финансов;
- переменные решения;
- целевую функцию;
- запас ресурсов или продукции;
- параметры спроса на данную продукцию.

Оптимизация модели производственного плана состоит в поиске максимальной прибыли или минимальных затрат целевой функции при

ограничении на спрос и ресурсы. Кроме того, возникают вопросы о минимализации производственных отходов. При некоторых видах производства часто требуется выполнить ограничение сверху и снизу концентрации составляющих компонент.

Математическое программирование занимается исследованием определенных и одноцелевых задач. «Программирование» в данном случае приравнивается к значению слова «планирование». Существуют различные методы математического программирования:

1. Линейное программирование: нахождение экстремального значения линейной функции многих переменных при наличии линейных ограничений, связывающих эти переменные. Достоинством этого метода является то, что от целевой функции не требуется дифференцируемости, более того, она может быть не заданна в аналитическом виде. Алгоритмы прямых методов минимализации основаны на возможности определения значений в заданных точках.

2. Нелинейное программирование: целевая функция и ограничения могут быть нелинейными функциями. Это задачи с нелинейной целевой функцией и линейными ограничениями.

3. Целочисленное программирование: встречается как в линейном, так и в нелинейном программировании, когда на оптимальные решения накладывается условие целочисленности искомых параметров.

4. Динамическое программирование: для отыскания оптимального решения планируемая операция разбивается на ряд шагов (этапов) и планирование осуществляется последовательно от этапа к этапу. Однако выбор метода решения на каждом этапе производится с учетом интересов операции в целом.

5. Теория графов, с помощью которой решаются многие сетевые задачи, связанные с минимальным протяжением сети, построение кольцевого маршрута и т. д.

Кожинская Евгения Александровна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Лустин Владимир Иванович²,
*старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ПРАВОНАРУШЕНИЯМ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

«Информационная революция» застигла нашу страну в сложный экономический и политический период и потребовала срочного нормативного регулирования проблем, возникающих в данной области. Вместе с тем, как известно, правовые механизмы включаются и становятся эффективными лишь после того, как общественные отношения, подлежащие регулированию, в достаточной мере стабилизируются. В последнее время в результате принятия ряда базовых нормативных актов в области регулирования информационных отношений наступил относительно благоприятный период для применения этих механизмов на практике.

Любые формы завладения сведениями ограниченного доступа без непосредственно выраженного согласия обладателя последних и их несанкционированного использования (за исключением случаев, прямо указанных в законе) являются неправомерными, поскольку уровень доступности информации определяется законом или непосредственно самим ее обладателем. Неправомерное использование информации наказуемо. Причем, наряду с гражданско-правовыми и административно-правовыми мерами к нарушителям информационных отношений могут быть применены и уголовно-правовые санкции. Таким образом, информация и информационные отношения становятся соответственно предметом и объектом преступления. Преступные деяния данной категории охватываются общим понятием – информационных преступлений.

¹ © Кожинская Е. А., 2019.

² © Лустин В. И., 2019.

Следует напомнить, что уголовно-правовые санкции предусмотрены для защиты целого ряда сведений ограниченного доступа и результатов интеллектуальной деятельности: государственной тайны (ст.ст. 275, 276, 283, 284 УК РФ), тайны частной жизни (ст. 137 УК РФ), тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ), тайны усыновления (ст. 155 УК РФ), коммерческой, банковской, налоговой тайн (ст. 183 УК РФ), объектов авторского права и смежных прав, объектов патентного права, средств индивидуализации юридических лиц, товаров, работ, услуг и предприятий (ст.ст. 146, 147, 180 УК РФ), и т. д. Все составы преступлений, предусмотренные указанными статьями УК РФ, носят информационный характер.

Одной из разновидностей информационных преступлений являются компьютерные преступления, имеющие на этом общем фоне особую специфику. В настоящее время среди российских ученых дискутируются различные точки зрения относительно классификации компьютерных преступлений. Сложности, связанные с однозначной формулировкой этих понятий, возникают, по-видимому, как по причине невозможности выделения единого объекта преступного посягательства, так и ввиду множественности предметов преступных посягательств с точки зрения их уголовно-правовой охраны.

Действующее российское законодательство в сфере противодействия компьютерной преступности под компьютерными преступлениями понимает предусмотренные уголовным законом общественно опасные деяния, при осуществлении которых предметом преступного посягательства оказывается машинная информация, используемая в различных сферах деятельности. Одновременно машинная информация рассматривается и в качестве орудия преступления. Наряду с ней в разряд орудий совершения подобных преступлений попадают сам компьютер, а также информационно-телекоммуникационная сеть (вычислительная среда, в которой эта информация циркулирует). Причем, машинная информация, циркулирующая в вычислительной среде, должна быть зафиксирована на соответствующем носителе в форме, доступной для восприятия ЭВМ или передачи по телекоммуникационным каналам.

Можно выделить следующие характерные особенности компьютерного преступления:

- неоднородность предмета посягательства;

- особенности машинной информации, рассматриваемой как в качестве предмета, так и в качестве средства (орудия) совершения преступления;
- многообразие предметов и средств преступного посягательства;
- особенности компьютера и компьютерной сети в целом, рассматриваемых и в качестве предметов, и в качестве средств совершения преступления.

Таким образом, с точки зрения криминалистических аспектов проблемы, под компьютерными преступлениями следует понимать предусмотренные уголовным законом общественно опасные деяния, совершенные с использованием средств электронно-вычислительной (компьютерной) техники.

Особое место среди прочих компьютерных преступлений занимают преступления в области компьютерной информации, которым посвящена отдельная гл 28 УК РФ. На сегодняшний день к ним отнесены неправомерный доступ к компьютерной информации (ст. 272); создание, использование и распространение вредоносных компьютерных программ (ст. 273); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274) и неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274).

Список литературы

1. Арутюнов, В. В. Современные проблемы и задачи обеспечения информационной безопасности. // Вестник Московского финансово-юридического университета. – 2016. – № 2. – С. 213–222.
2. Степанов, Е. А. Информационная безопасность и защита информации : учебное пособие / Е. А. Степанов, И. К. Корнеев. – М. : ИНФРА-М, 2014.
3. Яковец, Е. Н. Правовые основы обеспечения информационной безопасности Российской Федерации : учебное пособие. – 2-е изд., доп. и перераб. – М. : Юрлитинформ, 2014. – С. 182–256.

Селицкий Владимир Васильевич¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Плотников Герман Геннадьевич²
*доцент кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ИСКУССТВЕННЫЙ СПУТНИК

Впервые идею спутниковой связи представил в 1945 г. англичанин Артур Кларк. В радиотехническом журнале он опубликовал статью о перспективах ракет, подобных «Фау-2», для запуска спутников земли в научных и практических целях. Знаменателен последний абзац той статьи: «Искусственный спутник на определенном расстоянии от Земли будет совершать один оборот за 24 ч. Он будет оставаться неподвижным над определенным местом и в пределах оптической видимости почти с половины земной поверхности. Три ретранслятора, размещенные на правильно выбранной орбите с угловым разнесением на 120°, смогут покрыть телевидением и УКВ-радиовещанием всю планету; я боюсь, что те, кто планирует послевоенные работы, не сочтут это дело простым, но я считаю именно этот путь окончательным решением проблемы».

В 1967 г. через спутник связи «Молния-1»³ создана разветвленная телевизионная сеть приемных земных станций «Орбита» с центральной передающей станцией под Москвой. Это позволило организовать первые каналы связи между Москвой и Дальним Востоком, Сибирью, Средней Азией, передавать программу Центрального телевидения в отдаленные районы нашей Родины и дополнительно охватить более 30 млн телезрителей.

¹ © Селицкий В. В., 2019.

² © Плотников Г. Г., 2019.

³ URL : [https://ru.wikipedia.org/wiki/Молния-1_\(КА\)](https://ru.wikipedia.org/wiki/Молния-1_(КА))

В 80-е годы прошлого века эффективно функционировали работающие на стационарных орбитах спутники связи «Радуга» и телевизионные спутники «Экран». Для приема их сигналов не нужны были сложные наземные станции. Телевизионные передачи с таких спутников принимаются прямо на несложные коллективные, и даже индивидуальные антенны.

Первые спутниковые линии связи и вещания через ИСЗ «Молния-1»

В лаборатории спутниковой связи были подготовлены несколько системных проектов, а затем она приняла участие в разработке первой отечественной системы спутниковой связи «Молния-1» в диапазоне частот ниже 1 ГГц. Головной организацией по созданию этой системы был Московский научно-исследовательский институт радиосвязи (МНИИРС). Главным конструктором системы «Молния-1» является М. Р. Капланов, заместитель руководителя МНИИРС.

Первая в мире спутниковая система «Орбита» была создана для распределения ТВ-программ. После завершения исследований технических возможностей ИСЗ «Молния-1» специалистами НИИР Н. В. Талызиным и Л. Я. Кантором было предложено решить проблему подачи ТВ-программ центрального телевидения в восточные районы страны путем создания первой в мире системы спутникового вещания «Орбита» в диапазоне 1 ГГц на базе аппаратуры «Горизонт-К». Это предложение было одобрено, и решением правительства СССР НИИР был определен головной организацией по созданию в стране аппаратуры ЗС спутниковых систем связи и вещания.

Первая в мире система непосредственного ТВ-вещания «Экран»

Первый спутник системы «Экран» был запущен 26 октября 1976 г. на геостационарную орбиту в точку 99° в. д. Несколько позднее в Красноярске были выпущены станции коллективного приема «Экран-КР-1» и «Экран-КР-10» с мощностью выходного телевизионного передатчика 1 и 10 Вт. Земная станция, передающая сигналы на ИСЗ «Экран», имела антенну с диаметром зеркала 12 м, она была оборудована передатчиком «Градиент» мощностью 5 кВт, работающим в диапазоне 6 ГГц. Приемные установки этой системы, разработанные специалистами НИИР, были наиболее простыми и дешевыми приемными станциями из всех, реализованных в те годы. К концу 1987 г. число установленных станций «Экран» достигло 4 500 шт.

Список литературы

1. URL : https://ru.wikipedia.org/wiki/Спутник_связи.
2. URL : https://studopedia.ru/12_8862_istoriya-sozdaniya-sputnikovih-sistem-svyazi.html.
3. URL : http://sernam.ru/book_history.php.
4. URL : https://ru.wikipedia.org/wiki/Спутниковая_связь.
5. URL: <http://statehistory.ru/3899/Istoriya-sozdaniya-sovetskogo-sputnikovogo-televeshchaniya>.
6. URL : <http://www.astronautica.ru/polety-v-kosmos/osvoenie-kosmosa/319.html>.
7. URL : <https://www.space-ru.com/russian-satellites/satellite-raduga-1>.
8. URL : <http://www.computer-museum.ru/connect/sputnik.htm>.

Крупин Николай Алексеевич¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Белоглазов Евгений Григорьевич²,
*профессор кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

СПЕЦИАЛИЗИРОВАННЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА ИССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

Исследование компьютерной (машиной) информации является одним из самых молодых направлений в криминалистической технике. Оно начало складываться в первой половине 90-х гг. XX в. Наиболее часто исследования компьютерной, в том числе документированной информации, проводятся при расследовании следующих видов преступлений: в сфере компьютерной информации; экономические и налоговые преступления, в том числе совершенные путем нарушения правил бухгалтерского учета; связанные с изготовлением различной печатной продукции, в том числе бланков документов, денежных знаков, ценных бумаг и других; преступные нарушения авторских и смежных прав.

На современном этапе в криминалистике окончательно не сформировались теоретические и методологические основы криминалистического исследования компьютерной информации. В частности, среди криминалистов нет единства взглядов на предмет, задачи и объекты криминалистического исследования компьютерной информации.

Криминалистическое исследование компьютерной информации отнесено к криминалистическому исследованию документов, но в дальнейшем возможно данное направление сформируется в самостоятельную отрасль криминалистической техники.

Для целей технико-криминалистического исследования компьютерной информации определяющее значение имеет физическая природа данного вида информации.

¹ © Крупин Н. А., 2019.

² © Белоглазов Е. Г., 2019.

Компьютерная информация является объектом материального мира, элементом искусственной среды, созданным человеком. Она может существовать только с помощью специально приспособленных технических средств: электронно-вычислительной техники и электронных средств связи (системы телекоммуникаций).

Компьютерная информация, как и любой другой вид информации, состоит из двух элементов:

- содержания информации, сведений о каком-либо явлении объективной реальности;
- материального носителя данных сведений.

В рассматриваемом направлении криминалистической техники изучается компьютерная информация, содержание которой представлено в форме, пригодной для обработки ЭВМ, а ее материальным носителем является электромагнитное поле.

Физическая природа компьютерной информации обуславливает следующие ее свойства, делающие данный вид информации весьма сложным объектом криминалистического исследования: компьютерная информация не доступна для непосредственного человеческого восприятия; определенное содержание информации не может быть однозначно закреплено за конкретным материальным носителем; материальный носитель компьютерной информации (электромагнитное поле) невозможно индивидуализировать; как содержание информации, так и ее материальный носитель могут быть отделены друг от друга без их изменений; возможность быстрого изменения и удаления информации, в том числе путем удаленного доступа и вне контроля лиц, правомерно пользующихся данной информацией; невозможность выделения точных и допускающих единую трактовку признаков, присущих компьютерной информации, позволяющих восстанавливать содержание измененной или удаленной информации.

В предмет криминалистического исследования компьютерной информации входит:

- разработка приемов, способов, рекомендаций по обнаружению, фиксации, изъятию и хранению компьютерной информации и электронно-вычислительной техники;
- изучение состояния и процессов обработки компьютерной информации; состояния и функционирования электронно-вычислительной техники.

Компьютерная техника и иное электронное оборудование (далее – компьютерная техника) изучается в рамках данного раздела, главным

образом, поскольку и в связи с тем, что эти технические средства использовались для создания, обработки и изменения компьютерной информации. Даже в тех случаях, когда компьютерная техника является самостоятельным объектом исследования, например, при решении вопроса, является ли определенное устройство ЭВМ. В конечном итоге такое исследование является промежуточным шагом в решении задач, связанных с изучением компьютерной информации или процессов ее обработки.

В тех случаях, когда правоохранительные органы и суд интересуют свойства собственно компьютерной техники (потребительские свойства) вне связи с обрабатываемой этой техникой информацией, может назначаться судебно-товароведческая экспертиза, которая будет проводиться специалистами в области компьютерной техники или с участием таких специалистов.

В рамках криминалистического исследования компьютерной информации решаются идентификационные, классификационные и диагностические задачи.

Идентификационные и классификационные задачи. Объединение этих задач сделано по двум причинам. Во-первых, на современном этапе в большинстве случаев криминалисты не располагают инструментарием, позволяющим провести идентификацию единичных материальных объектов, изучаемых при криминалистическом исследовании компьютерной информации, а также использовать эти объекты для индивидуальной идентификации других объектов. Это обусловлено названными выше свойствами, присущими компьютерной информации. Во-вторых, при решении классификационных задач исследователи стремятся выйти на уровень как можно более узкой классификационной группы, выделить отдельные индивидуализирующие признаки, пусть и недостаточные для индивидуальной идентификации. Поэтому решение классификационных задач осуществляется по идентификационным методикам.

Наиболее часто решаются следующие идентификационные и классификационные задачи:

- изготавливалась (обработывалась, передавалась, изменялась) ли данная информация с помощью определенного типа или конкретного технического устройства;
- какой тип (вид, модель, марка) аппаратных и программных средств применялся при операциях с машинной информацией;
- к какому типу (текстовые файлы, программы, вирусы и т. д.) или более узкой классификационной группе (системное или прикладное

программное обеспечение, версия программы, редакция тестового файла) относится представленная компьютерная информация;

- к какому типу (вид, модель, марка) относится представленная компьютерная техника;

- определение общего источника происхождения содержания информации, представленной на разных носителях (создание ее определенной программой и т. д.).

Пока нет достаточно надежных методик установления автора или изготовителя компьютерной информации. Встречающиеся в литературе предложения использовать в этих целях методики, применяемые для решения аналогичных задач в других отраслях криминалистической техники (например, в автороведении или технико-криминалистическом исследовании документов) не имеют экспериментального подтверждения.

В литературе широко обсуждается возможность идентификации технических комплексов (единичный компьютер, сеть ЭВМ). В настоящее время в криминалистике нет апробированных методик, которые позволили бы провести такую идентификацию. Представляется, что решить задачу идентификации компьютера или сети ЭВМ в настоящее время только технико-криминалистическим путем в большинстве случаев невозможно. Поскольку это требует установления временных, организационных факторов, что нельзя сделать в рамках экспертных идентификационных исследований. Установление единичной ЭВМ или компьютерной сети является задачей процессуального доказывания. Экспертная идентификация выступает как один из методов, используемых для достижения конечной цели.

Идентификация некоторых электронных печатающих устройств (принтеров, телефаксимильных аппаратов и т. д.) проводится по их признакам, отобразившимся в текстовой информации на бумажных носителях. Поэтому чаще всего идентификация данных устройств проводится в рамках технико-криминалистического исследования документов. При этом эксперт должен обладать знаниями в области вычислительной техники или привлекать специалиста в данной области.

Типовыми диагностическими задачами являются следующие:

- установление свойств и состояния компьютерной информации и компьютерной техники;

- установление факта внесения изменений в компьютерную информацию после ее создания, выявление признаков такого изменения;

- установление первоначального состояния машинной информации;

- установление времени создания (удаления, изменения) информации, хронологической последовательности функционирования компьютера, компьютерной системы или сети;
- установление способа доступа к компьютерной информации и/или техники;
- определение фактического состояния и исправности компьютерной техники;
- установление соответствия реквизитов машинных документов требованиям, предъявляемым к ним, выявление признаков изменения данных реквизитов;
- установление порядка соблюдения технических правил при работе с машинной информацией, в том числе правил, обеспечивающих ее защиту;
- установление причинной связи между действиями с компьютерной техникой, машинной информации (например, программным обеспечением) и наступившими последствиями, например, удалением какой-либо информации, прекращением работы компьютера и т. д.

Основными объектами криминалистического исследования компьютерной информации являются: компьютерная информация и компьютерная техника.

В криминалистике встречаются различные классификации компьютерной информации. Для целей технико-криминалистического исследования основное значение имеет три основания классификации: по физической природе носителя, на котором находится компьютерная информация, по ее функциональному назначению и по правовому статусу.

В соответствии с физической природой носителя, на котором находится компьютерная информация, можно выделить следующие виды машинной информации:

- жесткий магнитный диск (винчестер, НЖМД, HDD). Это устройство, которое может находиться как внутри компьютера, так и в отдельном блоке. Существует отдельный вид устройств, построенных на основе жестких дисков, который называется RAID (Redundant Arrays of Independent Disks), массив независимых дисков с избыточностью;
- оперативное запоминающее устройство (ОЗУ-RAM) и постоянное запоминающее устройство (ПЗУ-ROM) обеспечивающие все преобразования информации в компьютере и периферийных устройствах;
- гибкие магнитные диски или дискеты (НГМД, FDD – floppy disk drive). Существует два типа таких устройств: дискеты размером 5,25

дьюма (пятидюймовая дискета) и объемом памяти до 1,2 Мбайт, практически вышедшие из употребления, и дискеты размером 3,5 дюйма и объемом до 2,88 Мбайт;

- накопители на магнитных лентах (стримеры). Стримеры часто используются для дублирования других носителей информации (архивирования информации), так как обладают значительной емкостью;

- оптические и магнитооптические диски. Принцип их работы основан на считывании и, в некоторых видах, записи информации с помощью луча лазера. Наиболее распространенным устройством данного типа является накопитель на компакт-дисках (CD-ROM). К этой группе относятся магнитооптические дисководы, ZIP-устройства и некоторые другие;

- существуют и другие реже употребляемые носители информации, такие как модули памяти на цилиндрических магнитных доменах (ЦМД), перепрограммируемые карты памяти (Flesh-card), дисководы типа Бернулли и т. д.

В число носителей компьютерной информации часто включаются современные средства связи, например, линии электросвязи, компьютерные сети и другие, в которых машинная информация находится при ее передаче.

По правовому статусу компьютерная информация подразделяется на два вида, имеющих разный правовой режим: документированная информация (документ) и информация, не имеющая документированной формы. Сравнивая понятия «информация» и «документированная информация (документ)», можно выделить признак, который, по мнению законодателя, присущ документу как виду информации – это реквизиты, позволяющие идентифицировать информацию, содержащуюся в документе.

Реквизитами компьютерной документированной информации (машинного документа) в соответствии с действующим законодательством могут быть различные коды, пароли, электронно-цифровая подпись, иные аналоги собственноручной подписи.

Таким образом, если при изучении экспертами «простой» компьютерной информации объектами исследования являются содержание информации и ее материальный носитель, то при изучении машинных документов самостоятельным объектом исследования могут стать и их реквизиты, а также программные и аппаратные средства, используемые при их создании.

Кручок Елена Андреевна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Плотников Герман Геннадьевич²,
*доцент кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ЦЕНТРАЛИЗОВАННАЯ ОХРАНА ОБЪЕКТОВ

Пульт централизованной охраны (ПЦО) – это диспетчерский пункт для централизованной охраны ряда рассредоточенных объектов от проникновения и пожара с использованием систем передачи извещений.

Проводные системы передачи извещений (СПИ) давно зарекомендовали себя как простые и надежные решения для централизованной охраны объектов. Привлекательность подобных систем обусловлена низкой стоимостью пультового и объектового оборудования, невысокими затратами на монтаж и эксплуатацию. Учитывая повсеместную телефонизацию объектов, а также возрастающую плотность застройки в крупных и средних городах, использование проводного канала, несомненно, предпочтительнее радиоканала. Немаловажно и то, что эксплуатация проводных систем не требует специалистов высокой квалификации и наличия дорогого проверочного оборудования.

Переход на двухсторонний канал связи позволил системе передачи извещений выйти на качественно новый уровень. За счет небольшого усложнения аппаратуры и протокола обмена появились следующие возможности:

- полная автоматизация процедуры шифрования канала связи;
- запись/чтение ключей электронного идентификатора (ЭИ) непосредственно с пунктом централизованной охраны (ПЦО);
- возможность взятия/снятия объектового устройства с ПЦО;
- удаленная конфигурация объектовых устройств;
- контроль канала связи с объектом;
- визуализация наличия связи с ПЦО на объекте;

¹ © Кручок Е. А., 2019.

² © Плотников Г. Г., 2019.

- передача на объект/с объекта текстовых сообщений;
- удаленное управление исполнительными механизмами.

Отдельно взятая система передачи информации, в зависимости от целевого назначения, может и не иметь каких-либо из вышеупомянутых функций, однако важно понимать, что для этого нет препятствий технического плана. Объективности ради зададимся вопросом: есть ли недостатки у систем с двухсторонним протоколом? И да, и нет. В качестве одного из них можно указать несколько более высокую цену оборудования, однако это с легкостью компенсируется высокой надежностью и богатым функционалом. Также, существует мнение о том, что двухсторонние системы более чувствительны к помехам. Тут тоже нельзя дать однозначного ответа. Цикл обмена, как правило, состоит из двух фаз: пакет передачи в сторону УО; ответный пакет в сторону ретранслятора. При наличии шумов в линии вероятность потери сообщения будет определяться суммой вероятностей неприема пакета УО и вероятностью неприема пакета ретранслятором. В соответствии с этим двухсторонняя система теоретически уступает односторонней, однако на практике реальная помехоустойчивость будет зависеть, в большей степени, от качества приемного узла и программной устойчивости алгоритмов цифровой обработки.

Заканчивая обзор плюсов и минусов применения одно- и двухстороннего проводного канала связи, хотелось бы подчеркнуть, что возрастающая сложность технических средств охраны должна компенсироваться, в первую очередь, надежностью оборудования и простотой технического обслуживания на объектах. В качестве примера сочетания простоты и надежности системы передачи извещений можно рассмотреть одну из новых разработок – СПИ «Атлас 7».

СПИ «Атлас-7»

СПИ «Атлас-7» предназначена для централизованного сбора информации с объектов оборудованных охранной сигнализацией с автоматической и ручной тактикой взятия/снятия и выдачи информации на автоматизированное рабочее место дежурного пульта централизованной охраны. Область применения-организация централизованной охраны рассредоточенных объектов, квартир, офисов, торговых помещений и т. д.

Основными техническими характеристиками СПИ «Атлас-7» являются:

- формационная емкость СПИ (для ПК) – 57 600;
- максимальное количество линий связи – 4;
- максимальное количество ретрансляторов на одной линии связи – 15;

- максимальное количество обслуживаемых направлений ретрансляторов приравнивается к 64;
- максимальное количество приборов на одном направлении приравнивается к 15.

Ретрансляционное оборудование СПИ «Атлас-7» группируются на АТС в локальную сеть посредством витой пары с учетом полярности интерфейса RS-485. Для обеспечения связи сети ретрансляторов с сервером пункта централизованной охраны используется аппаратура уплотнения на базе преобразователей интерфейсов ПИ-4М различных исполнений. Несмотря на относительно небольшое количество обслуживаемых направлений (не более 64), ретранслятор в состоянии обслуживать в общей сложности до 960 объектовых приборов. Это достигается за счет использования концентраторов объектовых «К-15». Один концентратор в состоянии контролировать работу 15 объектовых устройств и, соответственно, передавать ретранслятору информацию о состоянии 15х4 шлейфов сигнализации (ШС) по одной телефонной линии.

При использовании занятой линии дополнительно требуется установка двух блоков подключения с обоих концов линии. Абонентские и станционные линии должны быть скроссированы на два вертикально расположенных разъема ретранслятора (по 32 направления в каждом). Максимальное количество АТС, связанных с 1 линией связи, не может превышать 5, максимальное количество ретрансляторов не может превышать 15. Как видим, в общем случае на АТС не требуется установка какого-либо другого оборудования за исключением собственно ретрансляторов и преобразователей интерфейса. Здесь отметим, что иногда возникает ситуация, когда между АТС и так называемым «выносом» нет проводной линии связи. В таких случаях обычно имеется возможность организовать связь по оптоволоконной линии в составе группового цифрового канала Е1, либо по локальной ТСР/ІР сети. С этой целью можно использовать стандартное каналообразующее оборудование известных фирм «Моха» и НПП «Полигон». При этом надо помнить, что использование подобного оборудования вносит существенные задержки в канал связи, что может стать причиной замедления обмена с ретрансляционным оборудованием.

Связь ретрансляторов с объектовыми устройствами может осуществляться как по проводным линиям, так и с использованием радиоканала. В первом случае, в части подключения УО на объекте, СПИ не имеет отличий от большинства существующих систем. Второй случай рассмотрим более подробно. Иногда возникает ситуация, когда на охраняемом

объекте отсутствует телефонная линия связи, однако в радиусе 1 км есть несколько телефонизированных объектов, на которых можно установить соответствующее радиоканальное оборудование. В качестве последнего используется преобразователь интерфейса: «занятая линия - радиоканал ПИ-4Р». Устройство размещается в стандартном корпусе для объектового прибора, комплектуется внешней направленной антенной и встроенным аккумулятором 2,2 А/ч. Объектовое радиоканальное устройство устанавливается на охраняемом объекте в непосредственной близости от окна. Внешнюю антенну желательно укрепить на внешней стене здания, направив ее на антенну блока ПИ-4Р. В условиях прямой видимости и небольшом расстоянии между устройствами можно использовать встроенные антенны. Эксплуатация радиоканальных объектовых устройств не требуют получения лицензии, максимальная мощность передатчиков для обоих устройств не превышает 10 мВт, рабочая частота – 433 МГц, количество частотных каналов – 30. При обнаружении помехи оба устройства автоматически переходят на резервный канал связи. В качестве радиоканального объектового устройства можно также использовать радиоконцентратор К-15-Р. В этом случае можно контролировать состояние до 15 и четырехшлейфных объектовых приборов на одно направление.

Особенностью объектовых устройств СПИ «Атлас-7» является то, что в ее состав входят охранные и охранно-пожарные объектовые устройства (УО). Каждый тип УО имеет исполнения в зависимости от наличия или отсутствия встроенного источника питания, аккумулятора и дополнительных реле. УО обеспечивают следующие функции:

- контроль, звуковую и световую индикацию состояний 2 или 4 охранно-пожарных шлейфов;
- контроль датчика вскрытия корпуса;
- индикацию и контроль ЦКН;
- контроль состояния источника питания;
- контроль наличия связи ПЦО;
- криптозащиту протокола обмена (32 бита), защиту от подмена устройства;
- автоматическое взятие/снятие с помощи ЭИ или с ПЦО;
- удаленное программирование настроек;
- дополнительного источника питания 12 В для питания активных извещателей.

Максимальное время выполнения любой команды ПЦО не более секунды, при использовании концентратора – не более двух. Все

объектовые устройства с питанием от сети 220 В имеют возможность установки внутрь корпуса аккумулятора 2,2 А/ч, время непрерывной работы устройства при питании от аккумулятора составляет не менее 18 часов.

В процессе разработки СПИ «Атлас-7» особое внимание было уделено помехозащищенности каналов связи на участках «Сервер ПЦО – РО, РО – УО», а также целостности информации в узлах системы в случае кратковременного или длительного отсутствия связи. Так применение современных алгоритмов цифровой фильтрации позволило увеличить чувствительность приемных узлов до 10–15 мВ, что позволяет ретранслятору поддерживать устойчивый обмен с оконечными устройствами на линиях связи протяженностью до 10 км. Параметры приемопередающих узлов рассчитаны для совместной работы с аппаратурой абонентского доступа ADSL Annex A (B). Устранение взаимного влияния аппаратуры ОПС и ADSL достигается за счет использования дополнительных абонентских фильтров БФ.

Устройства ZigBee

В последнее время все большее распространение и значение приобретают беспроводные сенсорные сети. Сети, которые по своему назначению, параметрам, спецификациям существенно отличаются от сетей связи – WiFi, GSM, LTE и т. д. Среди прочих, используемых в сенсорных сетях, выделяется спецификация ZigBee – наиболее продвинутая надстройка к стандарту IEEE 802.15.4.

Zigbee – это стандарт беспроводной связи, подобный Wi-Fi и Bluetooth, но созданный специально для интернета-вещей и «умного дома».

Существовавшие 15 лет назад стандарты беспроводных сетей, например WiFi и Bluetooth, не подходили для новых возникших потребностей таких как «умный дом». Эти стандарты были недостаточно надежны, а их модули были слишком дорогими. Для разработки нового сетевого протокола была создана ассоциация из ведущих технологических компаний (Philips, Samsung, LG, Siemens и другие) под названием Zigbee Alliance. В 2004 г. был принят международный стандарт, регламентирующий новый протокол Zigbee, работающий на частотах, не требующих специального разрешения.

Характеристика протоколов связи

Технология	Wi-Fi	Bluetooth	ZigBee
Стандарт связи	IEEE 802.11	IEEE 802.15.4	IEEE 802.15.4
Скорость передачи данных	300+ мбит/с	до 3 мбит/с	250 к/с
Энергопотребление	высокое	низкое	низкое
Частотный диапазон	2.4 ГГц	2.4 ГГц	2.4 ГГц
Поддержка IP	+	—	—
Топология	«звезда»	«звезда»	«mesh»

Сети ZigBee строятся из базовых станций трех основных типов: координаторов, маршрутизаторов и конечных устройств.

Координатор запускает сеть и управляет ею. Он формирует сеть, выполняет функции центра управления сетью и доверительного центра (trust-центра), также устанавливает политику безопасности, задает настройки в процессе присоединения устройств к сети, ведет ключами безопасности.

Маршрутизатор транслирует пакеты, осуществляет динамическую маршрутизацию, восстанавливает маршруты при перегрузках в сети или отказе какого-либо устройства. При формировании сети маршрутизаторы присоединяются к координатору или другим маршрутизаторам, и могут присоединять дочерние устройства - маршрутизаторы и конечные устройства. Маршрутизаторы работают в непрерывном режиме, имеют стационарное питание и могут обслуживать «спящие» устройства. Маршрутизатор может обслуживать до 32 спящих устройств.

Конечное устройство может принимать и отправлять пакеты, но не занимается их трансляцией и маршрутизацией. Конечные устройства могут подключаться к координатору или маршрутизатору, но не могут иметь дочерних устройств. Конечные устройства могут переводиться в спящий режим для экономии заряда аккумуляторов. Именно конечные устройства имеют дело с датчиками, локальными контроллерами и исполнительными механизмами.

Сеть ZigBee – самоорганизующаяся, и ее работа начинается с формирования. Устройство, назначенное при проектировании координатором персональной сети (PAN координатор), определяет канал, свободный от помех, и ожидает запросов на подключение.

Устройства, пытающиеся присоединиться к сети, рассылают широковещательный запрос. Пока PAN-координатор – это единственное устройство в сети, отвечает на запрос и предоставляет присоединение к сети только он. В дальнейшем присоединение к сети могут предоставлять также присоединившиеся к сети маршрутизаторы.

Устройство, получившее ответ на широковещательный запрос, обменивается с присоединяющим устройством сообщениями, чтобы определить возможность присоединения. Возможность определяется способностью присоединяющего маршрутизатора обслужить новые устройства в дополнение к ранее подключенным.

Сети ZigBee полностью соответствуют следующим требованиям, а именно:

- благодаря ячеистой (mesh) топологии сети и использованию специальных алгоритмов маршрутизации сеть ZigBee обеспечивает самовосстановление и гарантированную доставку пакетов в случаях обрыва связи между отдельными узлами (появления препятствия), перегрузки или отказа какого-то элемента;

- спецификация ZigBee предусматривает криптографическую защиту данных, передаваемых по беспроводным каналам, и гибкую политику безопасности;

- устройства ZigBee отличаются низким электропотреблением, в особенности конечные устройства, для которых предусмотрен режим «сна», что позволяет этим устройствам работать до трех лет от одной обычной батарейки AA и даже AAA;

- сеть ZigBee – самоорганизующаяся, ее структура задается параметрами профиля стека конфигурируется и формируется автоматически путем присоединения (повторного присоединения) к сети образующих ее устройств, что обеспечивает простоту развертывания и легкость масштабирования путем простого присоединения дополнительных устройств;

- устройства ZigBee компактны и имеют относительно невысокую стоимость.

Связь в сети ZigBee осуществляется путем последовательной ретрансляции пакетов от узла источника до узла адресата. В сети ZigBee

предусмотрено несколько альтернативных алгоритмов маршрутизации, выбор которых происходит автоматически.

Стандарт предусматривает возможность использования каналов в нескольких частотных диапазонах. Наибольшая скорость передачи и наилучшая помехоустойчивость достигается в диапазоне от 2,4 до 2,48 ГГц. В этом диапазоне предусмотрено 16 каналов по 5 МГц.

Цена, которую пришлось заплатить в сетях ZigBee за минимизацию энергопотребления, компактность и дешевизну – относительно низкая скорость передачи данных.

Средняя скорость передачи полезных данных, в зависимости от загрузки сети и числа ретрансляций, составляет от 5 до 40 кбит/с.

Расстояние между рабочими станциями сети составляет десятки метров внутри помещений и сотни метров на открытом воздухе. За счет ретрансляций покрываемая сетью зона может быть весьма значительной: до нескольких тысяч квадратных метров в помещении и до нескольких гектар на открытом пространстве. Более того, сеть ZigBee в любой момент может быть расширена добавлением новых элементов или наоборот разбита на несколько зон простым назначением соответствующего числа новых конфигураторов сети. Это бывает полезно для снижения нагрузки и соответственно повышения скорости передачи данных.

Лебедев Игорь Викторович¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Лустин Владимир Иванович²,
*старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ПРАВОВОГО ПРОТИВОДЕЙСТВИЯ РАЗГЛАШЕНИЮ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ТАЙНУ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ ПО УГОЛОВНЫМ ДЕЛАМ

Уголовный закон, употребляя в статьях особенной части термин «тайна», не раскрывает его содержание. В русском языке он традиционно означает «все сокрытое, неизвестное, неведомое», а также «нечто скрытно хранимое, что скрывают от кого-либо». Таким образом, «тайна» имеет два смысловых значения: нечто абсолютно неизвестное всем и нечто относительно неизвестное для какого-либо круга лиц. Очевидно, что уголовно-правовой смысл имеет только второе значение.

В соответствии со ст. 2 Федерального закона от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» (далее в тексте – ФЗ-№ 24) под информацией понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Сведения должны быть известны или доверены узкому кругу лиц. При этом основанием известности сведений тому или иному лицу может быть профессиональная или служебная деятельность последних, семейно-брачные отношения и пр. Общим для всех видов конфиденциальных сведений является тот факт, что свободный доступ к ним ограничен в силу предписаний федерального законодательства.

Несанкционированное нарушение неприкосновенности охраняемой законом тайны влечет юридическую и уголовную ответственность. На лицах, которым доверена такая информация, лежит правовая обязанность не нарушать ее конфиденциальность.

¹ © Лебедев И. В., 2019.

² © Лустин В. И., 2019.

Исходя из сказанного тайну в уголовном праве можно определить как сведения, доступ к которым ограничен в соответствии с положениями федерального законодательства и за несанкционированное нарушение конфиденциальности которых установлена уголовная ответственность.

В уголовно-правовой литературе обычно утверждается, что сведения (информация), составляющие ту или иную тайну, являются предметами соответствующих преступлений. При этом традиционно считается, что предмет преступления – это, в первую очередь, вещь материального мира, имеющая определенные физические характеристики. Очевидно, что такими характеристиками может обладать какой-либо носитель информации. В ФЗ-№ 24 под информацией понимаются и не материализованные сведения о лицах, предметах, фактах, событиях, явлениях и процессах, отраженные в образах, в том числе и вербальных. Действительно, вполне возможно нарушение охраняемой уголовным законом тайны, которая не отражена в материальном носителе. Более того, в ряде составов УК РФ подразумевается уголовное преследование как раз за нарушение тайны определенной информации, не отраженной в материальном носителе.

Однако более всего важен факт, как действующее законодательство определяет юридическое существо тайны. Так, в преамбуле Закона Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» указывается, что настоящий закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Следовательно, юридически значимая тайна лежит в основе возникающих определенных отношений. Представляется, что взятые под специальную охрану тайные сведения являются первопричиной возникающих на их основании отношений между субъектами, в нашем случае – уголовного правоотношения, возникающего по поводу несанкционированного нарушения неприкосновенности той или иной тайны. Именно поэтому сведения (информация), составляющие ту или иную тайну, должны расцениваться в уголовном праве как объект, т. е. как интерес (благо) уголовно-правовой охраны, реализующийся и существующий в форме общественного отношения по его защите.

Именно характер общественных отношений, возникающих по поводу интересов охраны той или иной тайны, должен лежать в основе видовой классификации тайны в уголовном праве. Анализ непосредственных объектов составов преступлений, предусмотренных статьями УК РФ, позволяет выделить виды уголовно-правовой тайны.

*Лустин Владимир Иванович¹,
старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Проблема управления информационной безопасностью становится все более сложной и практически значимой ввиду активного перехода информационных технологий на автоматизированную основу без использования традиционных бумажных документов во всех сферах человеческой деятельности. Информационная безопасность носит концептуальный характер и предполагает создание комплексной системы безопасности, включающей правовые, организационные, инженерно-технические, криптографические и программно-аппаратные методы и средства защиты информации. Организационные методы являются главным звеном, объединяющим вышеупомянутые компоненты в единую комплексную систему защиты информации, которая должна удовлетворять критериям эффективности.

Общие методы обеспечения информационной безопасности Российской Федерации разделяются на правовые, организационно-технические и экономические.

К правовым методам обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации. Наиболее важными направлениями этой деятельности являются:

- внесение изменений и дополнений в законодательство Российской Федерации, регулирующее отношения в области обеспечения информационной безопасности;
- законодательное разграничение полномочий в области обеспечения информационной безопасности Российской Федерации между федеральными органами государственной власти и органами государственной власти субъектов Российской Федерации, определение целей,

¹ © Лустин В. И., 2019.

задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;

- разработка и принятие нормативных правовых актов Российской Федерации, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации;

- создание правовой базы для формирования в Российской Федерации региональных структур обеспечения информационной безопасности.

Основными организационно-техническими методами обеспечения информационной безопасности Российской Федерации являются:

- создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;

- усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, в том числе предупреждение и пресечение правонарушений в информационной сфере;

- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;

- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации;

- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль выполнения специальных требований по защите информации;

- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;

- формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

Так, основными организационно-техническими мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах определены:

- лицензирование деятельности организаций в области защиты информации;
- аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ, связанных с использованием сведений, составляющих государственную тайну;
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи;
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;
- создание и применение информационных и автоматизированных систем управления в защищенном исполнении;
- регулярное проведение специальных проверок и специальных исследований объектов информатизации.

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя:

- разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;
- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Информационная безопасность является одной из составляющих национальной безопасности страны и оказывает влияние на защищенность национальных интересов Российской Федерации в различных сферах жизнедеятельности общества и государства. Угрозы информационной безопасности Российской Федерации и методы ее обеспечения являются общими для этих сфер.

*Лустин Владимир Иванович¹,
старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

*Мельцева Ирина Сергеевна²,
старший научный сотрудник учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

НАЗНАЧЕНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ

В настоящее время трудно себе представить какой-либо объект, организацию, учреждение или предприятие, не использующее технические средства безопасности. Начиная с периметра объекта, его территории, фасадов зданий, и заканчивая внутренними помещениями, складами, офисными помещениями, архивами, кассами, сейфами и т. д., все, в зависимости от спектра рисков объекта защиты, может быть оборудовано техническими средствами обеспечения безопасности. Применение технических средств позволяет в полной темноте обнаружить нарушителя, выявить утечку газа, определить фальшивую купюру, защитить информацию, создать непреодолимое препятствие для проникновения и многое другое, чего без технических средств сделать просто невозможно.

Основным назначением технических средств и систем безопасности является:

- создание препятствий для возникновения факторов, дестабилизирующих нормальное функционирование объекта защиты;
- обнаружение источников угроз объекту защиты;
- формирование наиболее полной информации по каждому тревожному событию;
- передача, отображение и регистрация этой информации для принятия решения;
- обеспечение эффективного реагирования.

¹ © Лустин В. И., 2019.

² © Мельцева И. С., 2019.

Поскольку системы обеспечения комплексной безопасности объекта, фирмы предпринимательской деятельности предусматривают не только создание препятствий и обнаружение различных видов угроз, но, а также принятие адекватных мер по их недопущению, пресечению, а в случае реализации оперативной ликвидации последствий с наименьшим ущербом для объекта защиты. Следует отметить, что не количество и не характеристики технических средств определяют эффективность системы безопасности.

Эффективность системы безопасности определяется правильным использованием технических средств, в соответствии с конкретными задачами по обеспечению безопасности, их функциональным назначением и возможностями.

Если все помещения объекта оборудовать охранной сигнализацией, это не спасет объект от пожара. Если на объекте стоит самая современная противопожарная система, то нет никаких гарантий, что его не зальет прорвавшаяся труба. Следовательно, применение технических средств, в первую очередь обусловлено вероятностью реализации и конкретными видами угроз, которые могут воздействовать на объект защиты. Если объект подвержен кражам, необходимы инженерно-технические средства защиты и охранная сигнализация, если он пожароопасный, то основное внимание следует уделить пожарной сигнализации и средствам пожаротушения. На особо важных объектах, как правило, применяются комплексы технических средств безопасности или интегрированные системы безопасности.

При разработке концепции и системы безопасности объекта, фирмы, в результате анализа элементов защиты, вероятности и перечня угроз, степени рисков, формируется перечень организационных и технических мероприятий, которые предполагают использование технических средств и систем безопасности. Количество видов и типов технических средств безопасности настолько велико, что проблема заключается не в сравнении их технических характеристик, а в правильном выборе вида технического средства или системы для решения конкретной задачи. Для того чтобы было легче решать эту проблему, перейдем к классификации технических средств безопасности.

Существует несколько подходов при классификации технических средств и систем безопасности.

1. Классификация технических средств безопасности по их физическому принципу действия. Например, извещатели делятся на: магнито-контактные, оптикоэлектронные, акустические, пьезоэлектрические и т. п. Средства активного противодействия составляют: огнестрельное оружие, электрошоковые средства, газовые и т. д.

2. Наиболее распространенной является классификация технических средств безопасности по способности противодействия отдельным видам угроз. Например, антитеррористические, противоугонные (для защиты автомобилей), для защиты информации, противопожарные, обнаружения проникновения и другие.

3. Наиболее рациональной для выбора технических средств и систем безопасности при создании системы обеспечения комплексной безопасности представляется смешанная классификация, в которой «общий ствол дерева» в классификации представлен функциональным назначением, а по мере разветвления идет разделение по физическим принципам действия и конкретным типам. Именно такая классификация дает наиболее полное представление о многообразии технических средств безопасности и позволяет выбрать конкретный вид или тип изделий для использования в системе обеспечения комплексной безопасности.

Мандрикова Валерия Вячеславовна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Дворянкин Олег Александрович²,
*старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ОБЗОР ФРЕЙМВОРКОВ ДЛЯ ЦИФРОВОЙ ФОРЕНЗИКИ

Форензика, или компьютерная криминалистика – это прикладная наука о расследовании и раскрытии преступлений, связанных с компьютерной информацией, об исследовании цифровых доказательств в виде компьютерной информации, методах поиска, получения и закрепления таких доказательств. Для решения задач, поставленных перед компьютерной криминалистикой, необходим специализированный инструментарий, частью которого является фреймворк – программное обеспечение, позволяющее объединять различные модули и компоненты.

Основное достоинство фреймворков – это гибкость разработки, которая выражается в том, что их архитектура основана на декомпозиции нескольких отдельных модулей или приложения, что позволяет расширять функциональность, исходя из потребностей, и использовать измененную версию вместе с кодом фреймворка или использовать сторонние приложения. При этом на начальном этапе разработки приложения фреймворк накладывает определенные правила построения его архитектуры.

Специалисты, осуществляющие экспертизы, используют специализированное программное обеспечение, которое обычно недоступно рядовому пользователю, однако, существует достаточно большое количество бесплатных и общедоступных инструментов, например, SANS Investigative Forensic Toolkit (SIFT), ExifTool, Sleuth Kit, Computer Aided Investigative Environment (CAINE), Free Hex Editor Neo, DEFT, DSI USB Write Blocker, обладающих не меньшими возможностями.

¹ © Мандрикова В. В., 2019.

² © Дворянкин О. А., 2019.

CrowdResponse – это консольное приложение, которое можно использовать для сбора контекстной информации, такой как список процессов, запланированные задачи или кэш-память Shim. С помощью встроенных подписей YARA – сканировать хост на наличие вредоносных программ и сообщать о наличии каких-либо признаков компрометации.

FTK Imager – это инструмент, который позволяет просматривать файлы и папки на локальных жестких дисках, сетевых дисках, компакт-дисках и DVD-дисках, содержимое криминалистических изображений или дампов памяти, создавать хэши файлов SHA1 или MD5, просматривать и восстанавливать файлы, которые были удалены из корзины (при условии, что их блоки данных не были перезаписаны), и монтировать криминалистическое изображение для просмотра его содержимого в проводнике Windows.

Linux «dd» – криминалистическая очистка диска (обнуление диска) и создание необработанного образа диска.

DEFT – это Linux Live CD, который содержит инструменты для мобильной криминалистики, сетевой криминалистики, восстановления данных и хеширования.

Xplico – инструмент сетевого криминалистического анализа с открытым исходным кодом (NFAT), который предназначен для извлечения данных приложений из интернет-трафика (сообщения электронной почты из трафика POP, IMAP или SMTP); поддержка протоколов HTTP, SIP, IMAP, TCP, UDP, повторная сборка TCP и возможность вывода данных в базу данных MySQL или SQLite.

LastActivityView – это инструмент, позволяющий просматривать события и действия пользователя. Информация может быть экспортирована в файл CSV/XML/HTML.

DSi USB Write Blocker - это программный блокировщик записи, который предотвращает доступ на запись к USB-устройствам.

FireEye RedLine предоставляет возможность анализа памяти и файлов конкретного хоста для создания общего профиля оценки угроз: собирает информацию о запущенных процессах и драйверах из памяти, метаданные файловой системы, данные реестра, журналы событий, информацию о сети, сервисы, задачи и историю Интернета.

PlainSight – это Live CD, основанный на Knoppix (дистрибутив Linux), который позволяет выполнять цифровые криминалистические задачи, такие как просмотр истории Интернета, вырезание данных,

сбор информации об использовании USB-устройств, проверка дампов физической памяти, извлечение хэшей паролей и многое другое.

Volatility – это криминалистическая структура памяти для реагирования на инциденты и анализа вредоносных программ, которая позволяет извлекать цифровые артефакты из дампов энергозависимой памяти (RAM). Имеется возможность анализировать сырые дампы памяти, аварийные дампы, снимки виртуальных машин, дампы VMware (.vmem), аварийные дампы Microsoft, файлы гибернации, дампы виртуальных ящиков и многое другое. Используя Volatility, возможно извлекать информацию о запущенных процессах, открытых сетевых сокетах и сетевых подключениях, DLL-файлах, загруженных для каждого процесса, частях кэшированного реестра, идентификаторах процессов.

Rekall предоставляет комплексное решение для реагирования на инциденты и судебных аналитиков. Подход Rekall к анализу памяти уникален, так как использует точную информацию отладки, предоставляемую поставщиками операционной системы, для точного определения существенных структур данных ядра, в то время как другие инструменты основаны на эвристике и сигнатурах. Фреймворк может полностью использоваться как библиотека. Одна из основных целей Rekall сделать возможным внедрение Rekall в виде библиотеки в другой проект.

Рассмотренные фреймворки реализует самые передовые методы анализа в области компьютерной криминалистики, хотя и разрабатываются в открытом доступе с бесплатной лицензией с открытым исходным кодом.

Фреймворки могут быть полезны сотрудникам правоохранительных органов, относящихся к экспертно-криминалистическим подразделениям, в качестве готовых средств, для установления и выявления сведений в виде цифровых следов, оставленных в результате преступной деятельности.

Список литературы

Алексеев, Д. М. Расследование инцидента информационной безопасности с использованием Volatility Framework // Международный студенческий вестник. – 2017. – № 4, ч. 4.

Федотов, Н. Н. Форензика – компьютерная криминалистика. – М., Юридический Мир, 2007. – 432 с.

Brian Carrier. File System Forensic Analysis. Addison Wesley Professional, 2005. – 600 p.

Harlan Carvey Windows Registry Forensics. Advanced Digital Forensic Analysis of the Windows Registry. Esevier, Inc. 2007. – 206 p.

Яковлев, А. Н. Цифровая криминалистика и ее значение для расследования преступлений в современном информационном обществе. // URL : https://www.eforensics.ru/publ/eforensics/significance_of_eforensics/1-1-0-7 (дата обращения: 10.01.2019).

URL : <https://habr.com/post/327740/> (дата обращения: 11.01.2019).

Forensic Control // URL : <https://forensiccontrol.com/resources/beginners-guide-computer-forensics/#stages> (дата обращения: 10.01.2019).

Volatility Foundation // URL : <https://www.volatilityfoundation.org> (дата обращения: 10.01.2019).

OpenSourceForU // URL : <https://opensourceforu.com/2016/10/volatility/> (дата обращения: 10.01.2019).

Rekall Forensic // URL : <http://www.rekall-forensic.com> (дата обращения: 17.01.2019).

GFI TechTak // URL : <https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/> (дата обращения: 17.01.2019).

Молчков Григорий Романович¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Пузарин Андрей Валерьевич²,
*начальник кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ПРОБЛЕМА ИНТЕГРАЦИИ СПЕЦИАЛИЗИРОВАННОГО ПТО В ОТДЕЛЫ И ПОДРАЗДЕЛЕНИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ НА РАЙОННОМ УРОВНЕ

Не секрет, что во время глобальной эволюции в области информационных технологий, районные уровни, которые, по моему мнению, являются наиболее важными и незаменимыми в правоохранительной сфере, полностью обделены специализированных программно-техническим обеспечением.

Страшно даже подумать, что если в крупных городах такие отделы обеспечиваются по своему допустимому минимуму, то в малых городах, рабочих поселках, отдаленных регионах сотрудники отделов районного уровня могут даже и не знать, что кроме Microsoft office Word существует еще много абсолютно допустимого, удобного и полезного программно-технического обеспечения.

К примеру, такое ПТО, как АИС «Синергет Розыск» SYN-DTC. Эта система предназначена для идентификации граждан по лицу и поиска лиц, находящихся в Розыске.

Система позволяет анализировать видеоканалы с целью поиска лиц людей и распознавать их в режиме «Один-ко-многим» или «Один-к-одному».

Технология распознавания, используемая в системе, обеспечивает высокую (не менее 99 %) вероятность распознавания лица, в том числе, при изменении физических характеристик: старении, появлении бороды и усов, изменении прически.

¹ © Молчков Г. Р., 2019.

² © Пузарин А. В., 2019.

Поиск лица в базе данных по готовому шаблону занимает не более одной секунды для базы данных из миллионов лиц. Умный алгоритм системы обеспечивает возможность параллельного выполнения запросов по поиску различных лиц в одной базе данных.

В зависимости от производительности сервера возможно анализировать 25 видеок кадров в секунду с целью поиска лиц людей, причем одновременно может производиться поиск лица в базе данных с производительностью от 40 млн сравнений шаблонов лиц в секунду (на серверных платформах до 1 млрд лиц в секунду).

Система имеет возможность вывода всех похожих лиц из базы данных, с установленным пороговым процентом соответствия с биометрическим шаблоном.

Ключевые особенности системы:

- применяется в системах, предназначенных для антитеррористической деятельности;
- для сравнения лица с базой используется метод «один-к-одному» или «один-ко-многим»;
- количество серверов, обрабатывающих одну базу неограниченно.

Применяемый в специальном программном обеспечении «Синергет Розыск» алгоритм распознавания осуществляет анализ лица для выявления уникальных особенностей, выполняет преобразование найденных особенностей в набор численных характеристик (признаков), производит сравнение наборов признаков разных изображений и информирует оператора о сходстве и различии лиц. Применение в алгоритме распознавания методов математического моделирования позволяет обрабатывать фотоизображения различного качества: минимальный размер лица – 20 пикселей, оптимально – 150; поворот головы до $\pm 60^\circ$ по горизонтали, до $\pm 30^\circ$ по вертикали; любой фон; глаза могут быть закрыты, объект может быть в очках; устойчивость к бороде и усам; разница в возрасте до 20 лет.

Эта оперативная база данных и учета состоит из комплекса «Коридор безопасности», который прослеживает видеопотоки от видеокамер, подключенных к этому комплексу и видеосерверов «Синергет», основанных на специализированных программных обеспечениях, предназначенных для распознавания и поиска лиц в видеопотоках. Принцип работы состоит из:

- анализа видеопотока в реальном времени;
- поиска лиц, находящихся в розыске;
- передачи сообщений об обнаружении в единую базу данных.

Единая база данных доступна с любого количества рабочих мест и производительность ограничивается только мощностью сервера.

Удобство данного программного обеспечения не только в простом, а главное функциональном интерфейсе, но и в логической структуре, которым является управляющий web-сервер.

Web-сервер представляет собой базу данных лиц, которые находятся в розыске, а также функциональный интерфейс, позволяющий управлять офлайн-сервером распознавания и осуществлять поиск по фото в базе данных лиц.

Офлайн-сервер распознавания. Сравнивает лица на фотографиях, полученных из комплекса «Коридор безопасности», указанного оператором, с указанной оператором фотографией человека. Сервер поиска по фотографии. Сравнивает лица на фотографии, полученной от оператора, с базой данных.

Так в структуре НТЦ «Вулкан» есть подразделения, которые выполняют прикладные исследования и разработки в сфере защиты информации и в смежных областях.

Между тем в ФГУП «ГлавНИВЦ» Управления делами Президента Российской Федерации разрабатывается и реализуется единая техническая политика по построению информационно-телекоммуникационной системы, которая обеспечивает разработку и внедрение специальных баз данных и автоматизированных информационных систем.

В связи с вышесказанным можно отметить, что разрабатываемые аналитические программы, интегрируются в вузы, где проходят обработку. В то же время ознакомиться со специальными ПТО можно на научно-практических конференциях.

В заключение можно сказать, что необходимо внедрять программное обеспечение в подразделениях и отделах на районном уровне. Всем органам внутренних дел требуется та или иная информация, автоматизированные ПО облегчают поиск и могут повысить скорость и качество работы органов следствия или дознания, а также изменить состояние районных отделов, сначала в Москве, а затем и в других городах нашей страны.

Так, в районных отделах и участках, было бы гораздо удобнее собирать, хранить и анализировать информацию с помощью такого прикладного математического программного обеспечения как (УПМО) ИБД-Регион. Удобство в введении учета, поиске и анализе информации о лицах, совершивших преступление или административные правона-

рушения, ведение статистических карточек. Такое программное обеспечение как «Синергет Розыск» и программный комплекс «Сова» помогли бы в действительности отразить возможности эффективной работы этих подразделений и отделов. С таким ПО было бы гораздо проще осуществлять поиск лиц и транспортных средств, находящихся в розыске. И в целом работа стала бы продуктивнее, чем сейчас. Зачастую отделы и подразделения отправляют запросы в различные ведомства ведения баз данных, можно было бы внедрить сервисы Интегрированной аналитической системы ИСОД в отделы, для повышения качества и эффективности обработки и передачи данных.

Следует отметить, что для отделов и подразделений полиции эффективность и качество работы два самых главных и значимых качества, именно поэтому стоит пересмотреть состояние технического и программного обеспечения данных отделов и подразделений, с целью утверждения данной проблемы, и в последующем внедрении специализированного программного обеспечения в подразделения и отделы на районном уровне.

Покинен Андрей Эдуардович¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Щерба Вадим Викторович²,
*старший преподаватель кафедры специальных
информационных технологий
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

АНАЛИЗ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ ВЕБ-СЕРВИСОВ

Web-сервис (служба) – программа, которая организывает взаимодействие между сайтами. Информация с одного портала передается на другой. Прежде всего, веб-сервисы (или веб-службы) – это технология. Как и любая другая технология, они имеют довольно четко очерченную среду применения. Если посмотреть на веб-сервисы в разрезе стека сетевых протоколов, мы увидим, что это, в классическом случае, не что иное, как еще одна надстройка поверх протокола HTTP.

Интернет – разнороден, т. е. различные приложения на различных узлах сети функционируют на разных аппаратно-программных платформах, и используют различные технологии и языки. Чтобы связать все это и предоставить возможность одним приложениям обмениваться данными с другими, и были придуманы веб-сервисы. По сути, веб-сервисы – это реализация абсолютно четких интерфейсов обмена данными между различными приложениями, которые написаны не только на разных языках, но и распределены на разных узлах сети.

Именно с появлением веб-сервисов развилась идея SOA – сервис-ориентированной архитектуры веб-приложений (Service Oriented Architecture).

На сегодняшний день наибольшее распространение получили следующие протоколы реализации веб-сервисов:

– SOAP (Simple Object Access Protocol) – по сути это тройка стандартов SOAP/WSDL/UDDI;

¹ © Покинен А. Э., 2019.

² © Щерба В. В., 2019.

- REST (Representational State Transfer);
- XML-RPC (XML Remote Procedure Call).

На самом деле, SOAP произошел от XML-RPC и является следующей ступенью его развития. В то время как REST – это концепция, в основе которой лежит скорее архитектурный стиль, нежели новая технология, основанный на теории манипуляции объектами CRUD (Create Read Update Delete) в контексте концепций WWW. Безусловно, существуют и иные протоколы, но, поскольку они не получили широкого распространения, мы остановимся в этом кратком обзоре на двух основных – SOAP и REST. XML-RPC ввиду того, что является несколько «устаревшим», мы рассматривать подробно не будем. Нас в первую очередь интересуют вопросы создания новых веб-служб, а не реализация клиентов к существующим (как правило поставщики веб-сервисов поставляют пакеты с функциями API и документацией, поэтому вопрос построения клиентов к существующим веб-службам менее интересен с точки зрения автора).

Преимущества:

- создание необходимых условий для взаимодействия программных компонентов вне зависимости от платформы;
- веб-сервисы основываются на открытых стандартных протоколах. За счет внедрения XML обеспечивается простота формирования и настройки веб-сервисов;
- применение HTTP гарантирует взаимодействие систем посредством межсетевого доступа.

Недостатки:

- невысокая производительность и большой объем трафика, в сравнении с системами RMI, CORBA, DCOM, за счет использования XML-сообщений в разрезе текста;
- уровень безопасности. Все современные веб-сервисы должны внедрять кодирование, и требовать авторизации пользователя. Хватит ли здесь наличия HTTPS или необходимы более надежные протоколы, как XML Encryption, SAML и т.д., решается в ходе разработки.

Сервисы используются, чтобы настроить работу клиента и сервера. Это дает следующие преимущества:

- можно продавать не само программное обеспечение, а делать платным доступ к веб-сервису;
- легче решать проблемы с использованием стороннего ПО;
- проще организовывать доступ к контенту и материалам сервера.

Ниже представлены основные способы аутентификации в веб-сервисах в зависимости от способа ее безопасной реализации.

Способ	Основное применение	Протоколы
По паролю	Аутентификация пользователей	HTTP, Forms
По сертификатам	Аутентификация пользователей в безопасных приложениях; аутентификация сервисов	SSL/TLS
По одноразовым паролям	Дополнительная аутентификация пользователей (для достижения two-factor authentication)	Forms
По ключам доступа	Аутентификация сервисов и приложений	—
По токенам	Делегированная аутентификация пользователей; делегированная авторизация приложений	SAML, WS-Federation, OAuth, OpenID Connect

Ришилина Ольга Леонидовна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Орехов Павел Васильевич²,
*преподаватель кафедры специальных информационных
технологий учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ И ДЛЯ ОБЪЕКТОВ ИНФОРМАЦИИ ОВД

При проектировании крупной системы видеонаблюдения, важно учитывать особенности, которые касаются как технических вопросов выбора оборудования и проектных решений, так и непосредственно работы специалиста над проектом.

Проект на объекте информатизации считается довольно крупным и сложным. Так как много нюансов свойственных только данному объекту.

Во-первых, крупный объект большой по площади, для него характерны большие расстояния, и для которого может быть критичным время реагирования из-за тех же расстояний. К примеру, проект охраны периметра предприятия на 100 камер, будем считать крупным.

Во-вторых, это большое количество оборудования в одном проекте. Если площадь объекта не очень большая, но в нем несколько сотен камер – это крупный проект. Но здесь уже несколько иные факторы будут иметь значение при проектировании. Так, например, организация работы оператора, большие потоки, и просто много рутинной работы.

Помимо размеров и масштабов, крупный объект имеет ряд особенностей, которые важно учитывать при проектировании систем видеонаблюдения:

– долгий срок реализации проекта, так как крупный объект – это большой срок между выпуском проектной документации и строительной готовностью к монтажу;

¹ © Ришилина О. Л., 2019.

² © Орехов П. В., 2019.

– перманентное расширение и модернизация, крупный проект постоянно расширяется, модернизируется, перестраивается.

Рассмотрим подробнее все те факторы, которые следует учитывать при проектировании большой системы.

Технические аспекты проектирования крупных систем видеонаблюдения

Выбор оборудования. Стоимость

Причем не важно о каком именно оборудовании идет речь. Это могут быть камеры, коммутаторы, или же серверы. Мы говорим о подходе. Представим себе завод площадью несколько десятков гектар и камеры по периметру. Сколько будет стоить организовать сеть для 100 камер по периметру? Миллионы, если не десятки миллионов рублей. А сколько будут стоить камеры, серверы, коммутаторы? Да на самом то деле в несколько раз меньше.

И вот теперь важная мысль! Доля стоимости станционного и объектового оборудования в крупном проекте меньше, чем в небольшом. И цена здесь имеет уже второстепенное, если не третьестепенное значение. Экономия в рамках проекта выливается в проценты или даже доли процентов.

Выбор оборудования. Надежность

Когда оборудования много, много компонентов системы, количество точек отказа может быть огромным. Это касается не только оборудования, но и всех компонентов системы, в том числе тех или иных кабелей, разъемов, фурнитуры. Но даже, если взять только камеры, то для нескольких сотен камер, если одна будет давать сбой раз в год, получится, что каждый день происходит сбой.

Именно поэтому, для крупных систем, актуально использование оборудования известных брендов, которое зарекомендовало себя как надежное и безотказное. Поскольку, надежность для крупного проекта имеет существенное значение.

Здесь стоит отметить, что еще более правильным, при защите стоимости проекта и обоснования применения качественного оборудования, будет рассчитать TCO (Total Cost of Ownership – совокупная стоимость владения). Нередко расчеты показывают, что более качественное и дорогое оборудование окупается в перспективе нескольких лет его эксплуатации.

Повысить надежность, а точнее отказоустойчивость можно еще за счет резервирования.

Выбор оборудования. Доступность

Доступность к приобретению – это пример важного аспекта проектирования крупной системы видеонаблюдения.

Долгий срок внедрения и старта реализации проектов может привести к тому, что заложенное оборудование уже будет устаревшим, а проектные решения не актуальными. Здесь простая рекомендация: при проектировании, выбирать новинки, и самые прогрессивные решения.

Однако стоит учитывать один тонкий момент. Нужно сохранить баланс с тем, что решение должно быть не только прогрессивным, но и рабочим. Бывает и такое, что новинка вспыхивает ярко, но на поверку оказывается нежизнеспособной. Здесь потребуется высокий уровень экспертизы специалистов, либо консультация авторитетный профессионалов.

По поводу срока жизни конкретной модели оборудования, стоит отметить, что крупные производители, ориентированные на проекты, проектные бренды, могут выпускать одну и ту же модель много лет, и даже если та или иная модель снимается с производства, то всегда предлагают замену.

Контроль состояния компонентов системы означает, что выбор качественного оборудования не гарантирует полное отсутствие поломок – это лишь способствует снижению частоты отказов. В виду того, что оборудования много, а работоспособность системы критична для защиты объекта и срок простоя должен быть минимальным, необходимо оперативное реагирование на поломки.

Резервирование. Мы с вами говорим о крупном объекте, где цена реализации угрозы достаточно велика, где критично время простоя. Для большинства крупных проектов и систем ситуационного наблюдения бесперебойная работа системы является определяющей в тактике охраны.

Чтобы этого избежать можно организовать резервирование. Резервирование доступно на всех уровнях, за исключением камер. Да и камер, теоретически, можно поставить две. Резервирование можно реализовать на уровне коммутаторов, серверов, систем хранения данных, и даже на уровне резервирования резервных источников питания. Все это вполне доступно и несложно.

На уровне серверов систем видеонаблюдения это легко реализовать на программном уровне, нужно заложить софт с поддержкой этой функции и избыточное количество серверных мощностей для резервирования.

Мониторинг, оперативное реагирование

В случае отображения на 6 мониторах 150 камер, следует отметить, что формально и технически это возможно, но что оператор на них увидит? Безусловно, восприятие информации снизится, так если оператору вывести 6 камер на 6 мониторах будет получено больше информации. Для продуктивной работы следует задуматься об эффективном восприятии информации оператором, а также об организации рабочего места оператора и тактике охраны объекта.

Ограничения в скорости записи на HDD

Если тактика охраны объекта предполагает возможность ситуации, что несколько операторов одновременно начнут активно работать с архивом, то в этот момент возможна конкуренция между процессами записи и чтения с дисков подсистемы хранения. С высокой долей вероятности запись выиграет, но тем не менее следует избегать таких ситуаций на этапе проектирования системы, обеспечив запас. Это все довольно тонкие моменты и каждый конкретный проект и сервер записи нужно рассматривать отдельно, но граничные значения для ориентира мы можем дать:

- в системе, где просмотр архива осуществляется редко, граничным для одного сервера можно считать поток на запись 1300 Мбит/с;
- если предполагается активная работа с архивом одновременно с нескольких ПК, то в самом напряженном режиме граничным значением будет 240 Мбит/с.

Нужно понимать, что это не запретные значения. Есть способы увеличения пропускной способности в зависимости от того как пишет архив ПО видеонаблюдения.

Открытые платформы. Масштабируемые решения. Запас

Во-первых, при выборе стационарного оборудования следует использовать открытые интеграционные платформы с широкими возможностями. В любой момент заказчику может потребоваться принятие или изменение того или иного вертикального решения. В таком случае, чтобы не менять систему, следует изначально использовать ПО видеонаблюдения с возможностями расширения, в том числе и вертикальными решениями. К примеру, видеорегистраторам DVR и NVR не место в крупном проекте видеонаблюдения.

Второй аспект расширения системы – это готовность инфраструктуры. Не следует экономить на магистральных каналах. Перезаложитесь и пропускной способностью, и количеством каналов, чтобы в любой момент вы смогли подключить к этой общей магистрали новые участки си-

стемы. Все эти запасы не вносят значительной дополнительной стоимости, если потом не хватит, придется тратить значительные средства и производить модернизацию магистральных информационных каналов.

Информационная защита

На крупных проектах, зачастую, заказчик настаивает на использовании магистральных каналов информационной защиты системы. Если даже вам выделили свободные пары оптики, то все равно придется подключаться к общей сети заказчика. Есть разные службы и руководители, которые могут быть заинтересованы в просмотре камер и работе с архивом: АХО, главные инженеры, начальники секторов и производств, заведующие складами, не говоря уже о руководстве предприятия. В этих случаях стоит побеспокоиться об организации защиты. Как минимум, для соединений с внешним миром использовать управляемые коммутаторы, маршрутизаторы со встроенным фаерволом, с поддержкой шифрования и создания VPN туннелей.

В особенностях работы проектировщика над крупным проектом видеонаблюдения особое место занимает специфика работы проектировщика с крупной системой безопасности, при работе с крупным проектом и серьезным заказчиком нужно учитывать все аспекты деятельности, чтобы успешно завершить проект.

Цена ошибки. Соответствие нормам

Начнем с ошибок. Одна и та же ошибка в небольшом и крупном проекте системы видеонаблюдения, очевидно, имеет разную стоимость. Первые ошибки совершают, игнорируя нормативную базу.

Приступая к крупному проекту изучите существующую нормативную документацию для этого объекта, для этого заказчика, для проектируемых систем. Не забываем и о внутрикорпоративных или ведомственных нормах заказчика. То, что влияет на параметры будущей системы вносите в договор, в техническое задание, в проектную документацию. О проблеме нормативной документации для видеонаблюдения мы рассказывали в нашей статье.

Вторая ошибка – это работа по шаблонам, не учитывая особенности объекта и решаемые задачи. По нашему мнению, работа над крупным проектом должна начинаться даже не с подготовки технического задания, а с создания концепции системы безопасности, модели угроз и т. п. Если этого нет, то велика вероятность создать систему, которая не будет защищать объект или функции которой будут не востребованы. В крупном проекте проектировщик должен понимать цели системы ставиться, и то какие задачи она решает.

Крупная система – это большие объемы рутинной работы. Любые изменения влекут большие трудозатраты по переделке проекта. Поэтому, сохраняем исходники расчетов, чтобы в случае необходимости можно было легко пересчитать. Элементарный список расчетов включает следующие пункты:

- расчет зон обзора камер и разрешения;
- расчет архива и пропускной способности подсистемы хранения;
- расчет системы бесперебойного питания;
- мощности серверов;
- количества рабочих мест операторов и мониторов для отображения.

Для расчета станционной части системы видеонаблюдения мы рекомендуем пользоваться калькулятором серверов для IP-видеонаблюдения.

Программы для проектирования системы видеонаблюдения

VideoCAD – небольшая многофункциональная программа с удобным интерфейсом, предназначенная для проектирования видеонаблюдения на профессиональном уровне.

Программа проектирования видеонаблюдения – *VideoCAD* – упрощенная версия. Если версия *Professional* кажется вам слишком сложной или дорогой, попробуйте версию *Lite*. Версия *Lite* содержит все необходимое для большинства проектов систем видеонаблюдения.

IP Video System Design Tool – это хорошая программа с большим набором функций, которые включают решение тригонометрических задач расположение и формы зона обзора. Виртуально моделирует получаемые с видеокамеры изображения, осуществляет разделение зон обзора на участки с различной функциональностью: идентификация объекта, распознавание лица, выявление нарушителя. Программа довольно проста в использовании, интерфейс разбит на логические блоки, есть возможность формирования различных отчетов.

Проектировщик CCTV – одна из лучших программ для создания проектно-сметной документации и расчета систем видеонаблюдения. Разработчики систематически выпускают новые версии и обновляют базы данных оборудования (все обновления платные). Имеет ряд функциональных возможностей отсутствующих или недостаточно проработанных в других программных комплексах:

- реализована возможность определения разрешающей способности матрицы видеокамеры и фиксированного фокусного расстояния объектива по фотографии зоны наблюдения;

- рассчитывается оптимальная скорость потока видеозаписи и величина файла видеорегистратора с учетом емкости используемого жесткого диска и пропускной способности конкретной модели;
- наличие подпрограммы, определяющей величину выдержки камеры видеонаблюдения, которая необходима для получения четкого изображения автомобильного номера от транспортного средства, находящегося в движении;
- возможность экспорта базы выбранного оборудования в Excel таблицу.

В заключение статьи, мы хотим дать ряд рекомендаций для проектирования системы видеонаблюдения. Так следует выбирать качественное и надежное оборудование из новых линеек, в рамках проекта стоимость не существенна, оборудования должно иметь возможность мониторинга. По максимуму все резервируем. Для ситуационного наблюдения уделяем внимание тактике охраны и организации рабочего места оператора, активно интегрируемся с ОПС и СКУД, а также внедряем видеоаналитику. Оборудование выбираем самое современное и прогрессивное, выбираем открытые платформы и помним про ограничение записи архива. Магистральные линии и центральное оборудование проектируем со значительным запасом на расширение и не забываем про информационную защиту.

Курбатова Мария Сергеевна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Серезевский Алексей Вадимович²,
*доцент кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ПОЖАРНОЙ СИГНАЛИЗАЦИИ

В настоящее время наблюдается совершенствование средств пожарной автоматики и сигнализации. Наблюдается тенденция к увеличению сертифицированной продукции, а также улучшение качества данных изделий отечественного производителя. В настоящее время по статистическим данным МЧС наблюдается тенденция снижения общего числа пожаров в стране. Однако, в 2018 г. число пожаров на объектах с массовым пребыванием людей выросло на 29,4 %. Пожар в ТРЦ «Зимняя вишня» г. Кемерово унес жизни 64 человек. По материалам уголовного дела обвиняемым вменяется в вину халатность, нарушение требований пожарной безопасности, оказание услуг, не отвечающих требованиям безопасности. В момент возникновения пожара в помещении ТРЦ пожарная сигнализация была отключена, в результате чего голосового оповещения о начале пожара не было, в тоже время автоматические системы, которые включаются при появлении дыма не сработали.

Объекты массового пребывания людей должны по правилам быть оборудованы такими основными системами противопожарной защиты как: автоматической системой сигнализации и системой оповещения, спринклерной системой водяного пожаротушения, система внутреннего противопожарного водопровода, огнетушители, системы газового, порошкового пожаротушения.

Система пожарная сигнализации охраняемого объекта – совокупность технических средств пожарной сигнализации, установленных на объекте и передающих сигналы на пункт охраны объекта.

¹ © Курбатова М. С., 2019.

² © Серезевский А. В., 2019.

Для контроля состояния данных систем предлагается создать дистанционный онлайн-мониторинг всего комплекса противопожарных систем. С помощью него появится возможность наблюдения за системой пожарной безопасности. Данные о состоянии объекта будут отправляться в ближайшие пожарные части МЧС, наблюдение в таком случае осуществляется в онлайн-режиме.

Основные этапы развития систем пожарной безопасности объекта

1-е поколение систем – построение отдельных автоматических систем пожарной сигнализации без функции управления системой противодымной защиты и пожаротушения.

2-е поколение систем – построение интегрированных автоматических систем пожарной сигнализации и управления с функцией прямого автоматизированного управления системой комплексной противодымной защиты и пожаротушения.

3-е поколение систем – построение автоматизированных систем управления активной противопожарной защиты.

Сегодня одним из наиболее перспективных направлений обнаружения возгорания можно считать современные видеотехнологии. Выделяются два направления – создание видеодетекторов, способных обнаружить пожар по специфическим признакам; системы видеомониторинга с функциями обнаружения пожара. На лидирующих позициях находятся устройства обнаруживающие такой фактор пожара как дым, далее устройства, обнаруживающие тепло, пламя или газ. Стоит отметить, что существуют устройства использующие различные сочетания признаков (к примеру, дым и газ).

Основными направления в развитии пожарной сигнализации являются:

- использование новых термочувствительных элементов;
- совершенствование конструкции термочувствительного элемента, уменьшение воздействия на него внешних факторов, к примеру, повышенная влажность;
- совершенствование метода обработки сигнала, в результате чего повышается скорость обнаружения пожара и достоверность срабатывания пожарной сигнализации;
- использование различных эффектов, сопровождающих возникновение пожара (звуковых);
- разработка датчиков, контролирующих нагрузку на электросеть. Такие устройства, в отличие от иных датчиков, отслеживают состояние электропроводки, а именно реагируют на превышение заданного уров-

ня нагрузки электропроводки, далее выключение неисправного участка цепи и звуковое сообщение о неисправности. Таким образом, сократилось бы количество пожаров, возникших в результате неисправности электросети;

– разработка датчиков резкого возрастания давления. Широкое применение данных устройств было бы распространено в связи с использованием газов и легковоспламеняющихся жидкостей на производстве, а также в случае террористического акта;

– разработка комбинированных устройств пожарного извещения.

В заключение стоит отметить, что перспективными направлениями развития средств пожарной автоматики и сигнализации является разработка самостоятельно адаптирующихся и обучающихся систем в условиях пожара. Повышение эффективности контроля за окружающей средой, а также самостоятельный выбор системой действий в условиях чрезвычайной ситуации, минимизация ложных срабатываний и передача данных о состоянии объекта в ближайшие пожарные части МЧС – это основные характеристики, которые должны содержать современные технические средства подобного рода.

Список литературы

1. URL : <https://ombudsmanbiz.ru/2018/11/po-statistike-mchs-v-2018-godu-chislo-pozharov-na-obektah-s-massovym-prebyvaniem-ljudej-vyroslo-na-tret>.
2. URL: <https://www.kommersant.ru/doc/3585935>.
- 2.7.103. Национальный стандарт РФ ГОСТ Р 52551-2006 «Системы охраны и безопасности. Термины и определения».
3. Соколов, В. П. Общие тенденции развития автоматической системы пожарной сигнализации // URL : https://www.tinko.ru/files/library7-8-04_1.pdf.
4. Буцынская, Т. А., Землянухин, М. В. Анализ патентной информации в области пожарной сигнализации. – Вестник Академии Государственной противопожарной службы МЧС России. – 2005. – № 3. – С. 174.
5. Кривенко, Н. Н., Ануфриев Ф. Е. Перспективы развития систем пожарной сигнализации // URL : <https://www.cyberleninka.ru/article/n/perspektivy-razvitiya-sistem-pozharnoy-signalizatsii/viewer>.

Симаков Олег Витальевич¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Лустин Владимир Иванович²,
*старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ВИДЕОНАБЛЮДЕНИЕ: ЮРИДИЧЕСКИЕ АСПЕКТЫ

В действующем российском законодательстве нет самостоятельного нормативного акта, регулирующего деятельность по организации и осуществлению видеонаблюдения. Регулирования, касающиеся различных отдельных правовых аспектов видеонаблюдения, содержатся фрагментарно в кодифицированных актах (к примеру, ГК РФ, ТК РФ, КоАП РФ), а также в специальных законодательных актах:

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее –ФЗ-№ 152);
- Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» и другие.

Осуществление видеонаблюдения в местах общего доступа

Осуществление видеонаблюдения в местах общего доступа предполагает, что появление любого физического лица или объекта может быть зафиксировано системой видеонаблюдения. Это значит, что невозможно заранее определить круг лиц, которые попадут в камеры.

Ст. 152.1 ГК РФ устанавливает правовую охрану изображения гражданина как нематериального блага. Соответственно, каждый гражданин вправе запретить получение своего изображения или записи видео с его изображением, но, если видеонаблюдение осуществляется в таких местах, как, например, общие коридоры, холлы, торговые залы, гостевые парковки – это невозможно.

¹ © Симаков О. В., 2019.

² © Лустин В. И., 2019.

Как правило, это связано с тем, что в указанных зонах видеонаблюдение осуществляется с целью документальной фиксации возможных противоправных действий, которые могут нанести вред имуществу. Предполагается, что в случае необходимости материалы видеозаписей, полученных камерами видеонаблюдения, будут использованы в качестве доказательства в уголовном или гражданском судопроизводстве.

В ч. 1 ст. 22 ФЗ-№ 152 среди общих требований к обработке персональных данных устанавливает необходимость предварительного уведомления Федерального агентства по надзору в сфере связи, информационных технологий, массовых коммуникаций (далее – Роскомнадзор), за исключением случаев, предусмотренных ч. 2 данной статьи, например, обработка персональных данных в рамках трудовых отношений и т. д.

Таким образом, прежде чем приступать к установке системы видеонаблюдения и предполагая использовать ее для получения доказательств совершения неправомерных действий, работодателю необходимо уведомить Роскомнадзор.

Информация, полученная с камер системы видеонаблюдения в отсутствие предварительного уведомления Роскомнадзора, не будет иметь юридической силы по смыслу ч. 2 ст. 55 ГПК РФ, ч. 2 ст. 50 Конституции Российской Федерации.

Обязательно уведомление посетителей о том, что в помещениях производится видеонаблюдение в силу п. 3 ст. 12 Закона Российской Федерации от 11 марта 1992 г. № 2487-І «О частной детективной и охранной деятельности в Российской Федерации». Для выполнения такого требования достаточно установить хорошо читаемые таблички в наиболее доступных для посетителей местах. Каких-либо дополнительных специальных требований к содержанию либо формату таких табличек действующее законодательство не устанавливает.

*Видеонаблюдение в зонах, закрытых для свободного доступа
(вход только для сотрудников)*

Согласно п. 2 ст. 3 ФЗ-№ 152 под персональными данными понимается любая информация, позволяющая, прямо или косвенно идентифицировать конкретное лицо.

Соответственно, в том случае, если система видеонаблюдения позволяет отслеживать деятельность сотрудников на рабочем месте или иных помещениях, закрытых для общего доступа, такое наблюдение будет считаться обработкой персональных данных.

Таким образом, при осуществлении видеонаблюдения за объектами, имеющими режим ограниченного доступа, работодателю необходимо

руководствоваться не только соображениями обеспечения законности получения доказательств, но и дополнительно соблюдать ограничения, связанные с регулированием процесса обработки персональных данных.

Исключение, пожалуй, составляют лишь случаи несанкционированного проникновения в помещения, имеющие режим ограниченного доступа. Основываясь на системном толковании норм закона «О персональных данных», можно установить, что для обработки персональных данных работника, работодателю необходимо:

- заключить с работниками соглашение о сборе и обработке персональных данных (или включить соответствующие положения в трудовой договор) с указанием целей обработки, предполагаемыми источниками получения персональных данных, способами ее получения, последствиями отказа работников от дачи согласия на ее получение;
- принять локальный нормативный акт, устанавливающий порядок обработки персональных данных работников и связанные с этим права работников;
- осуществлять надлежащую охрану полученных данных;
- указать работников, ответственных за обработку персональных данных в данном локальном нормативном акте.

Следовательно, если на предприятии впервые вводится система видеонаблюдения, потребуется внесение соответствующих изменений в положение о персональных данных. Указанное справедливо и в случае осуществления видеонаблюдения силами частной охранной организации.

Срок хранения записей системы видеонаблюдения

Ст. 5 ФЗ-№ 152, однако, устанавливает применительно к персональным данным, что они должны храниться не более срока, необходимого для выполнения целей обработки (подразумевается, что после выполнения таких целей все персональные данные будут автоматически уничтожены).

Соответственно в случае обработки персональных данных работника срок хранения таких данных ограничен периодом действия трудового договора: с увольнением соответствующего работника прекращает существовать цель обработки его персональных данных работодателем (за исключением случаев необходимости использования данных в судебном разбирательстве против такого работника).

Возможная ответственность

Говоря о мерах ответственности в рассматриваемом случае, мы главным образом подразумеваем административную и гражданско-правовую ответственность.

Кодекс об административных правонарушениях устанавливает ответственность за нарушение порядка обработки персональных данных в ст. 13.11 – штраф для граждан в размере от 300 до 500 р.; должностных лиц – от 500 до 1000 р.; юридических лиц – от 5 до 10 тыс. р., который может быть наложен по итогам проверки Роскомнадзором соблюдения законодательства о персональных данных.

В свою очередь, ч. 2 ст. 24 ФЗ-№ 152 налагает обязанность возместить причиненный ущерб (включая моральный вред) лицу, пострадавшему в результате разглашения персональных данных, в нарушение положений данного закона по иску такого лица. Доказыванию в данном случае подлежат обстоятельства, установленные ст. 151 ГК РФ.

Скрытое видеонаблюдение

Отдельно следует рассмотреть вопрос организации скрытого видеонаблюдения. Данный вид наблюдения представляет собой форму получения информации с помощью устройств, предназначенных для ее негласного получения. Осуществление такого наблюдения в принципе запрещено физическим и юридическим лицам в соответствии с ч. 6 ст. 6 Закона Российской Федерации от 12 августа 1995 г. № 144-ФЗ «Об оперативной и розыскной деятельности».

Кроме того, ст. 138.1 УК РФ воспрещает приобретение и использование устройств, предназначенных для негласного получения информации под страхом лишения свободы сроком до 4 лет.

Итак, действующее российское законодательство в принципе позволяет осуществлять видеонаблюдение без необходимости получения какой-либо разрешительной документации.

В то же время обработка материалов системы видеонаблюдения прочно связана с обработкой персональных данных, охрана которых обеспечивается ФЗ-№ 152.

Соответственно для целей обработки персональных данных работодателю необходимо соблюдать требования ТК РФ, ФЗ-№ 152 и иных нормативных источников.

Садовников Артем Игоревич¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Пузарин Андрей Валерьевич²,
*начальник кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМ АВТОМАТИЧЕСКОЙ ПРОТИВОПОЖАРНОЙ ЗАЩИТЫ ОБЪЕКТОВ, ПРЕДПОСЫЛКИ И ЗАДАЧИ

Первая и главная задача любой противопожарной системы – это сохранение жизни и здоровья людей. Вторая – сохранение материальных ценностей. При этом система должна быть проста в обслуживании и быть как можно более «незаметной» в штатном режиме работы объекта. Она также не должна становиться новым источником опасности, при ложном срабатывании или при работе в режиме слежения за состоянием объекта защиты. Желательно, чтобы она была проста в установке и настройке, а оборудование объекта системами противопожарной защиты не приводило к неоправданно высоким затратам.

Одна из важнейших задач совершенствования противопожарных систем – это минимизация вероятности их ложных срабатываний, которые в настоящее время являются серьезной проблемой. Систематические ложные срабатывания систем, как правило, приводят к тому, что установку отключают, или пытаются симитировать ее нормальную работу, вводя в заблуждение обслуживающий персонал и ответственных за пожарную безопасность объекта.

В связи с этим в последнее время наметилась определенная тенденция в пользу выбора более дорогих и качественных систем противопожарной автоматики, применяемых для защиты объектов. Все чаще стали применяться адресно-аналоговые извещатели, позволяющие не просто определить состояние контролируемого объекта по принципу «где-то что-то произошло» и сильно зависящие от мастерства инсталлятора, а дающие возможность увидеть конкретную динамику развития контролируемого

¹ © Садовников А. И., 2019.

² © Пузарин А. В., 2019.

параметра среды в конкретной точке помещения объекта или выдать сигнал о неисправности какого-либо элемента системы. При управлении установкой пожаротушения данные системы позволяют запустить огнетушащее вещество в автоматическом режиме в конкретную точку. Данный принцип работы позволяет в кратчайшие сроки локализовать очаг возгорания без перерасхода огнетушащего вещества.

Кроме того, в настоящее время идет работа по совершенствованию самого устройства извещателей. Например, в камерах дымовых оптико-электронных извещателей традиционно используются светодиоды ИК-диапазона с длиной волны порядка 945 нм, что ограничивает регистрируемые частицы дыма, не позволяя регистрировать мелкие частицы. Появление синего светодиода с длиной волны 470 нм, позволяет обнаруживать более мелкие частицы дыма. В новом поколении двухдиапазонных дымовых извещателей применяются оба светодиода, выдающих сигналы на микропроцессор с интеллектуальной обработкой сигнала (ISP), алгоритмы которого позволяют различить частицы дыма, пыли или пара. Это приводит к более раннему и более надежному обнаружению возгораний и снижению вероятности ложных срабатываний.

Контролируемый параметр среды определяется выбором типа извещателя. Для сложных технологических сред, выбираются извещатели, контролирующие и анализирующие сразу несколько параметров. Многие производители делают упор на разработку комбинированных извещателей. Чаще всего это извещатели, контролирующие одновременно температуру и оптическую плотность среды. Также это могут быть ивещатели, контролирующие сразу три фактора: СО+дым+тепло. Применение их в адресно-аналоговых системах дает очень большую достоверность обнаружения возгорания, а пожарные извещатели реагирующие на уровень СО, отличаются также и большим быстродействием.

Все чаще находят свое применение извещатели пламени, в ряде случаев они способны обнаружить очаг возгорания намного раньше извещателей других типов. Любой извещатель пламени содержит чувствительный элемент – преобразователь электромагнитного излучения в электрический сигнал – реагирующий на электромагнитное излучение пламени соответственно в инфракрасном, видимом или ультрафиолетовом диапазоне длин волн. Современные извещатели обрабатывают излучение сразу в инфракрасном (тепловом) и ультрафиолетовом диапазонах, практически не затрагивая область видимого, что вместе со

специальными алгоритмами обработки сигнала, позволяет многократно повысить надежность обнаружения очага возгорания без ложных срабатываний.

Кроме ложных срабатываний, полное отсутствие срабатываний и возможности получить какие-либо данные о контролируемых параметрах среды длительное время также приводит к снижению бдительности, и к необходимости проведения дополнительных работ по обслуживанию, для проверки работоспособности систем. Этого недостатка лишены адресно-аналоговые системы с выводом данных на монитор и возможностью удаленно проконтролировать все параметры и элементы систем. Разрабатывается программное обеспечение, позволяющее получить, например, динамично меняющееся тепловое поле объекта на основе показаний тепловых пожарных извещателей. Использование сенсорного экрана позволяет оперативно на планах помещений получить требуемую информацию и, при необходимости, корректировать работу систем пожарной автоматики для эффективного тушения возгораний или управления эвакуацией людей.

Данные алгоритмы работы можно применить для работы спринклерной системы водяного пожаротушения с принудительным пуском. Система такого типа объединяет достоинства традиционных спринклерных и дренчерных систем пожаротушения. Достоинством традиционной спринклерной системы является малый расход воды и подача огнетушащего вещества непосредственно в очаг возгорания, недостатком же считается большая инерционность срабатывания, что может привести к отставанию роста орошаемой площади по отношению к увеличению площади развивающегося пожара. При дренчерном способе тушения, огнетушащее вещество подается на площадь заведомо большую, чем площадь возможного возгорания, что приводит к гарантированному тушению очага возгорания, однако влечет за собой значительный перерасход воды, а как следствие и увеличение ущерба от воздействия нее. Применение спринклеров с принудительной термической активацией с контролем факта вскрытия позволяет создавать алгоритмы для подачи огнетушащего вещества по площади немного большей, чем площадь очага возгорания, и также следить за динамикой развития пожара и корректировать работу всех систем.

Еще одним перспективным направлением развития противопожарных систем, является совершенствование интерфейсов передачи данных: от извещателей к приемно-контрольному прибору, между объек-

тами, или между объектом и пожарным постом. Использование беспроводных технологий позволяет в разы сократить работы по монтажу и обслуживанию противопожарных систем. С каждым годом увеличивается количество и качество выпускаемого радиоканального оборудования, что приводит к общему снижению стоимости установки беспроводных противопожарных систем.

Другое направления для развития это – Ip-технологии, объединяющие в себе регламент передачи пакетов от одного ip-адреса к другому, физические интерфейсы, каналы передачи данных, протоколы прикладного уровня и т. д. Данная технология является массовой, все основные протоколы открыты, существует множество open-source разработок, множество провайдеров для предоставления каналов связи, размещения серверов и хостинга, повсеместно доступная сегодня возможность туннелирования транспортных потоков стека ТСР/IP в сетях мобильной связи. Дешевизна современных интегральных схем и их компактность позволяет встраивать Ip-транспорт в самые простые устройства. Все это позволяет контролировать множество распределенных объектов и связывать их в единую сеть, для удаленного контроля и администрирования, и объединить данные противопожарных систем с другими системами безопасности независимо от производителя оборудования. Это позволяет влить системы противопожарной защиты в единую информационную сеть, став такими же подсетями, какими стали корпоративные сети современных предприятий.

Следующим направлением развития противопожарных систем является их объединение с другими инженерными системами и системами безопасности здания в блок, под управлением единого контроллера (по принципу «умного дома»). Это позволяет уменьшить время реакции системы объекта на возникновение возгорания, за счет наличия единого управляющего и информационного центра объекта, а также задать правильный алгоритм работы других слаботочных, электрических и инженерных систем в случае пожара. Охранные извещатели или система видеонаблюдения также может зафиксировать раннее возникновение очага пожара, в некоторых ситуациях даже раньше системы пожарной сигнализации, что можно использовать, например, для выдачи команды на уменьшение порога чувствительности пожарных извещателей, по поступившему тревожному сигналу от других систем объекта.

Примерами такой единой системы могут служить пожарные роботы, активно применяющиеся в 2000-е годы. Они оснащены ИК-сканерами для автоматического обнаружения загорания и ТВ-камерами для видеоконтроля. Их чувствительность позволяет обнаружить очаг возгорания площадью 30х30 см и быстродействие составляет считанные секунды, в течение которых определяются места возгорания в трехмерной системе координат, по сигналам от адресных извещателей пламени или термокабеля контролирующего перегрев несущих конструкций. Заранее созданные алгоритмы работы позволяют орошать несущие конструкции зданий, предотвращая их обрушение. На базе пожарных роботов, объединенных единой магистралью, формируются роботизированные пожарные комплексы. Такие системы все чаще находят применение для противопожарной защиты сооружений с массовым пребыванием людей. Подобные системы могут найти свое применение и для защиты объекта от несанкционированного доступа, используя гидромеханическое воздействие воды. Пожарные роботы также устанавливаются в нишах, укрытых декоративными панелями, и выходят на боевую позицию по сигналу «тревога», а в дежурном режиме переходят обратно в нишу, закрывая за собой проем.

Оборудование объекта единой системой, способной принимать и анализировать информацию от всех инженерных подсистем, передавать ее в единый центр мониторинга, при возникновении внештатной ситуации, отключать или включать необходимое противопожарное оборудование, электрооборудование, включать систему оповещения, с указанием безопасных путей эвакуации и пускать огнетушащее вещество непосредственно в очаг возгорания еще на ранней стадии развития пожара, что на сегодняшний день является приоритетным направлением развития систем автоматической противопожарной защиты. При этом система, по возможности, должна фиксировать и передавать все изменения состояний инженерных систем и наличие людей на объекте, для облегчения работы пожарных расчетов и последующего анализа причин возгорания.

Карнаухов Никита Сергеевич¹,

курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя

Борзунов Константин Константинович²,

доцент кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ: ИСТОРИЯ И ТЕНДЕНЦИЯ РАЗВИТИЯ

Компьютерные преступления – это преступления, которые совершаются в сфере информационных технологий. Специалисты технического профиля знают, что пару десятков лет тому назад тема компьютерных преступлений и киберпреступности только зарождалась. Считается, что компьютер следует отнести к важнейшим изобретениям XX в. С 1973 г., когда первый персональный компьютер ALTAIR 8000 был запущен в производство, жизнь человека начала кардинально меняться. Умная электронная машина не только стала надежным товарищем, но и помощником людей в каждой сфере их деятельности. Она упростила их жизнь, сделала интереснее, уничтожив границы информационного пространства. Впредь любой человек, в любое время, в любой точке Земли с помощью компьютера способен получить различную интересующую его информацию.

Но компьютер породил альтернативный тип преступления. В новом российском уголовном кодексе для них была выделена отдельная глава «Преступления в сфере компьютерной информации». С 1997 г. такие действия, как «незаконный доступ к компьютерной информации», «создание, использование и распространение компьютерных вредоносных программ» и «нарушение правил эксплуатации компьютеров, компьютерных систем или их сетей» чреваты уголовной ответственностью. Для защиты от преступлений в сфере высоких технологий в конце 1990-х годов в системе органов внутренних дел были созданы подразделения «Р».

¹ © Карнаухов Н. С., 2019.

² © Борзунов К.К., 2019.

Компьютер не только прочно вошел во все сферы жизнедеятельности человека, но и сформировал свой особый вид людей, который можно назвать компьютерщиками. Эти люди имеют свою структуру и иерархию. Их называют «хакерами». Хакер – это человек, который породнился с машиной и в совершенстве овладел работой на ней.

Изучив определение «компьютерные преступления», мы поняли, что проблема актуальна, так как преступления в сфере информационных технологий очень часто являются международными, то есть преступники действуют в одном государстве, а их жертвы находятся в другом государстве.

Так 23 ноября 2001 г. в Будапеште была подписана Конвенция Совета Европы о компьютерной преступности ETS № 185. Она открыта для подписания как государствами-членами Совета Европы, так и государствами, не являющимися членами. В частности, конвенция была подписана США и Японией. Россия еще не подписала Конвенцию.

Конвенция Совета Европы о киберпреступности разделяет преступления в киберпространстве на четыре группы.

Первая группа включает: конфиденциальность, целостность и доступность компьютерных данных, незаконный доступ (ст. 2), незаконная кража (ст. 3), компьютерные данные (незаконный ущерб, удаление, повреждение, ст. 4) или система (ст. 5). Эта преступная группа также включает несанкционированное использование специальных технологических устройств (ст. 6) – компьютерных программ, разработанных или адаптированных для совершения преступлений в соответствии со ст.ст. 2–5, а также пароли компьютеров, коды доступа и аналогичные продукты, которые можно использовать для доступа ко всей или части компьютерной системы). Ст. 6 применяется только в том случае, если использование (распространение) специального технического устройства является незаконным.

Вторая группа включает преступления, связанные с использованием компьютерных инструментов. К ним относятся подделка и мошенничество с использованием компьютерных технологий (ст.ст. 7, 8). Подделка, использующая компьютерную технологию, включает в себя злонамеренное и незаконное внесение, изменение, удаление или блокирование компьютерных данных, нарушающих подлинность данных, с намерением их рассматривать или использовать в качестве законных целей.

Третья группа – производство (с целью распространения через компьютерную систему), предложение и (или) предоставления использования, распространения и приобретения детской порнографии, а также хранение детской порнографии в памяти компьютера (ст. 9).

Четвертую группу составляют преступления, связанные с нарушением авторского права и смежных прав.

В соответствии с Конвенцией каждая сторона обязана предоставить компетентным органам правовые условия, необходимые для определения следующих прав и обязанностей в отношении киберпреступности:

- обнаружение компьютерных систем, их частей или операторов, создание и захват компьютерных данных;
- обеспечение целостности и безопасности соответствующих компьютерных данных;
- уничтожение или блокирование компьютерных данных.

Конвенция также требует создания необходимых правовых условий для обязанности интернет-провайдеров собирать и регистрировать или перехватывать необходимую информацию с использованием имеющихся технических средств, а также помогать правоохранительным органам в этом. Рекомендуются обязать поставщиков поддерживать полную конфиденциальность фактов такого сотрудничества.

В начале 2002 г. был принят Протокол № 1 к Конвенции, согласно которому в перечень преступлений было добавлено распространение информации расистского и иного характера, возбуждающей насилие, ненависть или дискриминацию, отдельного лица или группы по признаку расы, национальности, религии или этнической принадлежности.

*Жилкина Алина Алексеевна¹,
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

*Пузарин Андрей Валерьевич²,
начальник кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Информация, подобно экономическим ресурсам человеческого общества, подвергается накоплению, хранению для дальнейшего использования и распространению. Технические изобретения, представляя собой овеществленный труд, являются одновременно и овеществленной информацией. Формирование информационного общества является закономерным этапом эволюции современного социума, характеризующегося, в первую очередь, масштабным внедрением информационных технологий и развитием глобального информационного пространства. Процесс становления нового общества, обусловленный внедрением информационных технологий, нуждается в верном осознании его информационной специфики и конструктивном развитии заложенного в нем потенциала. Проблема защиты от проявившихся в третьем тысячелетии новых видов опасностей и угроз, порожденных информатизацией, беспокоит исследователей современного общества.

Сложность освещения проблемы информационной безопасности до настоящего времени, как отмечают специалисты, связана с отсутствием общепринятого толкования терминов, описывающих рассматриваемую предметную область. Наряду с термином «информационная безопасность», активно используется термин «безопасность информации». Не вызывает сомнений тот факт, что данные понятия взаимосвязаны. Информационная среда определяет качество функционирования жизнедеятельности общества, его уровень развития и безопасность.

Информационное взаимодействие, его своевременность, полнота и интенсивность регулируют все процессы жизнеобеспечения общества.

¹ © Жилкина А. А., 2019.

² © Пузарин А. В., 2019.

Оттого информационная инфраструктура представляет собой основную цель информационного оружия. Мишенью «асимметричной» войны являются жизненно важные точки государства. Эти точки называются критическими инфраструктурами, потому что их дееспособность или уничтожение будет иметь пагубные последствия для национальной безопасности и экономического и социального благополучия нации.

Изобретательность человека в орудиях разрушения превышает изобретательность в технике, например, медицинской, а также то, что «небольшая кучка людей, обладающая секретом технических изобретений, сможет тиранически держать в своей власти все человечество». Рост модификации информационного оружия далеко опередил развитие технологий защиты, в результате чего нейтрализация данного оружия становится приоритетной задачей национальной безопасности государства.

Информационная революция начинается с создания электронно-вычислительных машин в конце 40-х гг. XX в. с того времени исчисляется эра развития информационной технологии, материальное ядро которой образует микроэлектроника. Процесс развития современных технологий отражает качественную перестройку информационной среды человека. Информационные технологии повлияли на сознание человека и возможности, изменили его образ жизни. Современные информационные технологии поменяли приоритеты и ценности.

Сегодня используемые в обществе информационные технологии рассматриваются как фактор, оказывающий огромное влияние на глобальное развитие социума и формирование информационной реальности. В настоящее время информационная сфера оказалась сердцевинной экономических, социальных, политических и других конфликтов в обществе. Проявившиеся впоследствии использования современных технологий основные опасности и угрозы систематизированы в зависимости от сфер жизнедеятельности общества. Так, в социальной сфере возникла опасность нового неравенства в обществе: реальная угроза «информационного расслоения», ведущая к потенциальной угрозе формирования информационной элиты общества.

Система глобальной информационной безопасности отражает важный фактор перехода к устойчивому развитию. Необходимо определить основные направления развития информационной безопасности:

- обеспечение состояния защиты информационной среды от угроз и опасностей реального и потенциального характера;

- развитие в безопасном направлении для общества, человека и биосферы информационного пространства;
- справедливое распределение благ и ресурсов информационной среды между народами и всеми мировыми государствами;
- содействие процессу перехода к устойчивому развитию формирующейся информационной среды.

На пути реализации указанной стратегии важно не забывать, что мировое информационное пространство не имеет географических и государственных границ, в результате чего его защита и укрепление зависят одновременно от всего мирового сообщества, равнозначно как уязвимость и ущерб его развитию отражается на разных странах.

Первое направление технической защиты информации – это защита объекта информатизации. Такая защита осуществляется за счет использования инженерных сооружений: различных преград, ограждений, турникетов, специальных хранилищ и т. д.

Данный вид защиты реализуется с помощью технических систем охраны объектов: охранной и пожарной сигнализации, охранного видеонаблюдения, управления доступом в выделенные зоны или к защищаемым ресурсам объекта информатизации, применением интегрированных систем охраны.

Техническая защита объекта информатизации позволяет предотвратить доступ противника к средствам информатизации и носителям информации с целью предупреждения преднамеренных деструктивных воздействий на защищаемую информацию и нейтрализовать негативные воздействия стихийных бедствий или техногенных катастроф на средства информатизации и носители информации.

Также защита объекта препятствует созданию противником необходимых оперативно-технических позиций для скрытого ведения разведки, а значит, предупреждение потенциальной утечки информации ограниченного доступа.

Второе направление технической защиты информации – это защита информации от утечки по техническим каналам:

- энергетическое скрывание опасных сигналов, препятствующего их распознаванию, регистрации и декодированию с помощью технических средств разведки противника за счет уменьшения соотношения «уровень опасного сигнала – уровень шума» в точке потенциального перехвата сигналов;

– поиск и нейтрализация технических средств разведки – закладных устройств, скрытно установленных противником на объектах информатизации; при этом в процессе поисковых операций осуществляется выявление, как работающих закладных устройств, так и закладных устройств, исчерпавших ресурс автономных источников питания или находящихся в выключенном состоянии;

– двойное преобразование формы опасных сигналов, как правило, используемое для защиты от декодирования речевых сообщений различных систем связи, которые могут быть перехвачены противником; прямое преобразование выполняется над отправляемым сообщением, затем, обратное преобразование над принимаемым сообщением.

Черногоров Георгий Викторович¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Большунов Александр Геннадьевич²,
*преподаватель кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

МЕТОДЫ ИССЛЕДОВАНИЯ ФАЙЛОВЫХ СИСТЕМ

Чтобы носитель компьютерной информации мог содержать файлы, он должен быть размечен и отформатирован под определенную файловую систему. Разметка состоит в создании на носителе разделов, внутри которых могут быть образованы логические диски (тома). Форматирование логического диска (тома) состоит в создании на нем пустой файловой системы. Некоторые виды носителей способны содержать единственный раздел, например дискеты.

Файловая система – это структура для организации хранения информации в виде файлов и доступа к ней. Файл обязательно предусматривает заголовок и тело. В заголовке содержится имя файла, другие его атрибуты и указание на расположение тела файла. В теле файла записываются данные, т. е. содержимое файла. Практически все файловые системы предусматривают древовидную структуру: файлы включаются в состав директорий (каталогов), которые, в свою очередь, могут включаться в другие директории. Минимальная единица хранения определяется параметрами носителя (например, размером сектора) и файловой системой; обычно она именуется блоком или кластером. Тело файла всегда занимает целое число таких блоков. Наиболее распространенные файловые системы таковы: FAT16, FAT32, EXFAT, NTFS, HFS+, APFS, EXT3, EXT4, F2FS, BTRFS. Для того, чтобы четко понимать, как и каким методом исследовать файловую систему, необходимо знать всю информацию о файловой системе, ее структуре.

Рассмотрим следующий вариант: интересующие нас файлы не были обнаружены. Но точно известно, что они были на данной ЭВМ. Допу-

¹ © Черногоров Г. В., 2019.

² © Большунов А. Г., 2019.

стиф файлы были удалены и не находятся в «промежуточном хранилище», именуемом «Корзина» в системе Windows. Безвозвратное удаление файлов осуществляется только с использованием специального программного обеспечения (утилиты очистки PGP, BestCrypt и др.). Если же удаление информации осуществлялось путем очистки «Корзины» или из иной программы, например файлового менеджера, минуя корзину, то всегда существует вероятность полного или частичного восстановления этих данных. Для восстановления удаленных файлов используются специальные программы. Процедура восстановления должна осуществляться на другой носитель (предпочтительно НЖД, использование съемных носителей – дискет, FLASH-дисков, CD-дисков – не целесообразно ввиду значительного объема восстанавливаемой информации).

Все программы, предназначенные для этих целей, можно разделить по их функциональности на простые «восстановители», действующие по принципу «найти все, что удалено и восстановить» и более мощные программы, позволяющие делать прогноз восстановления, работать с поврежденными носителями и обладающие другими опциями. Программ восстановления много.

Примером первого типа подобных продуктов (достаточно удачным в силу своей простоты, скорости работы и неплохой результативности) является программа Handy Recovery. Примером программ второго типа является Easy Recovery Pro.

При удалении файлов средствами операционной системы или файловыми менеджерами возможно обратное восстановление удаленной информации.

При удалении файлов физического уничтожения информации не производится. Операционная система заменяет первый символ в заголовке файла, размещенного в таблице FAT, на специальный символ. В дальнейшем система считает, что кластера дисков, на которые ссылается такой модифицированный заголовок, являются свободными. Поэтому возможно восстановить удаленные файлы.

Теперь проведем исследование на примере файловой системы FAT используя изучение HEX-кода с подробным отчетом.

Загрузочный сектор представляет собой таблицу параметров и программу загрузчик. Размер загрузочного сектора обычно 512 байт, но он может быть больше. В загрузочном секторе хранится информация не актуальная для флеш-накопителей: число секторов на треке, число головок.

Так, что не все параметры для нас представляют интерес. Если посмотреть HEX-код какого-нибудь носителя информации отформатированного в формате FAT, то мы увидим значение полей.

Значение каждой ячейки считываются справа налево, где два заполненных элемента (по 32 байта). В данном случае для примера в корне хранятся два файла «1.txt» и «test.txt».

Допустим, мы имеем в нашем образе FAT16 директорию «TEST_DIR» с файлом «in_dir.txt». Тогда в корневом каталоге появиться новый элемент (32 байта), он описывает директорию как и файл, но с небольшими отличиями.

Содержимое «файла» TEST_DIR - тот же корневой каталог, т. е. набор элементов (по 32 байта).

Вышеописанный метод очень трудоемкий и занимает очень много времени. Так же он требует большого количества знаний. Приведенные выше файловые системы можно исследовать таким методом, но опять же все зависит от подготовленности специалиста.

Воспользуемся программой *AVSearch*. Данная программа позволяет производить поиск файлов по текстовому фрагменту по указанному адресу (адресам). При этом есть возможность наложения условий поиска.

Скорость работы указанной программы зависит от параметров компьютера, эффективность поиска равна 100 %. После задания области поиска, в главном окне в поле задания текстового фрагмента указывается искомое слово (или фраза).

Теперь воспользуемся программой для поиска графических файлов *ACDSee Pro*, затем перейдем к поиску файлов в заданной области. В результате будут показаны миниатюры найденных графических файлов.

Теперь можно ознакомиться со свойствами данных файлов. Рассмотрим такой вариант: интересующие нас файлы не были обнаружены. Но точно известно, что они были на данной ЭВМ. Допустим файлы были удалены и не находятся в «промежуточном хранилище», именуемом «Корзина» в системе Windows. Безвозвратное удаление файлов осуществляется только с использованием специального программного обеспечения (утилиты очистки PGP, BestCrypt и т. д.). Если же удаление информации осуществлялось путем очистки «Корзины» или из иной программы, например, файлового менеджера, минуя корзину, то всегда существует вероятность полного или частичного восстановления этих данных. Для восстановления удаленных файлов используются специальные программы. Процедура восстановления должна осуществляться на другой носитель.

Рассмотрим возможности программы *Easy Recovery*. Программа представляет пример «продвинутой» утилиты, обладающей достаточно мощными возможностями по восстановлению информации.

Показывать и описывать процесс восстановления данных не представляет интереса, так как все что требуется – это умение пользоваться компьютером и читать инструкцию к данному программному обеспечению.

В файловой системе могут находиться скрытые файлы. Используем простую в использовании, но очень мощную и полезную программу *Total Commander*. В настройках включаем «отображать скрытые файлы и папки», в окошках появятся файлы и папки, которые были скрыты, и помечаются восклицательным знаком на самом значке.

Петухова Наталья Юрьевна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Пузарин Андрей Валерьевич²,
*начальник кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

CISCO – СРЕДСТВО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Для защиты организации нужна соответствующая архитектура безопасности и постоянная бдительность, хакерство в настоящее время превратилось в полноценный бизнес, направленный на огромную прибыль.

Хакеры стали очень организованными, они действуют с размахом и масштабы их вредоносной деятельности только растут. Подготовка атак ведется продуманно и профессионально, они имеют хорошее финансирование и в будущем атак станет намного больше.

Сейчас цепочка атаки представляет собой не просто отдельные атаки, а целую теневую индустрию, которая поставила на конвейер кражу конфиденциальных данных для их дальнейшей продажи либо незаконного использования с целью обогащения.

Так что же делать до обнаружения атаки, во время атаки и после нее? Как заявляют представители cisco, при любом сценарии развития атаки и любых последствиях, они предоставляют все необходимые инструменты для успешной борьбы с кибератакой и защиты от нее на всех этапах. Модель, ориентированная на защиту от угроз – это лучшее решение для борьбы с киберзлом, которое ежедневно угрожает безопасности организаций.

Технологии фирмы Cisco Systems широко используются для построения защищенных компьютерных сетей. Аппаратно-программные комплексы Cisco можно встретить в сетях практически любых организаций. Соответственно, растет потребность в специалистах, способных не только эксплуатировать данное оборудование, но и разрабатывать

¹ © Петухова Н. Ю., 2019.

² © Пузарин А. В., 2019.

на его базе сложные защищенные сетевые проекты, а также осуществлять анализ информационной безопасности таких сетей. Известно, что подобные специалисты весьма ценятся и могут рассчитывать на высокооплачиваемую работу.

Списки доступа (access lists) представляют собой общие критерии отбора, которые можно впоследствии применять при фильтрации дейтаграмм, для отбора маршрутов, определения приоритетного трафика и в других задачах. Списки доступа, производящие отбор по IP-адресам, создаются командами access-list в режиме глобальной конфигурации, каждый список определяется номером – числом в диапазоне от 0 до 99. Каждая такая команда добавляет новый критерий отбора в список.

Недостатком списков доступа, применяемых для фильтрации трафика, является то, что они формируются администратором статически до начала работы. В итоге администратор вынужден закладывать в них разрешения «на все случаи жизни».

Систему разграничения компьютерных сетей с различными политиками безопасности, реализующую правила информационного обмена между ними, называют межсетевым экраном (МЭ).

Межсетевой экран – это локальное (однокомпонентное) или функционально-распределенное (многокомпонентное) программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему (АС) и/или исходящей из нее.

NAT (Network Address Translation) – трансляция адресов, позволяющая скрывать адреса сети от узлов, находящихся за Cisco PIX. При прохождении пакетов через Cisco PIX внутренние адреса сети перед выходом с внешнего интерфейса транслируются в другие адреса. NAT конфигурируется с помощью команд nat и global.

IPSec предлагает стандартные способы аутентификации и шифрования соединений. В IPSec применяются открытые стандарты согласования ключей шифрования и управления соединениями. Технология IPSec предлагает методы, позволяющие сторонам «договориться» о согласованном использовании сервисов. Для указания согласуемых параметров в IPSec существуют ассоциации защиты.

Ассоциация защиты (SA) представляет собой согласованную политику или способ обработки данных, обмен которыми предполагается осуществлять между двумя устройствами.

Система обнаружения атак (англ. Intrusion Detection System) – это программный или программно-аппаратный комплекс, предназначенный для выявления и по возможности предупреждения действий, угрожающих безопасности информационной системы.

Основными задачами, решаемыми с помощью систем обнаружения атак (СОА), являются:

- обнаружение атак (вторжений);
- прогнозирование возможных сценариев развития комплексных атак на основе выявления признаков начальных этапов атакующего воздействия;
- фиксация информации об источниках компьютерного нападения;
- получение информации об уязвимостях, использованных для компьютерного нападения.

Попов Никита Сергеевич¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Казанцев Владимир Иванович²,
*старший преподаватель кафедры огневой подготовки
учебно-научного комплекса специальной подготовки
Московского университета
МВД России имени В.Я. Кикотя*

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ SOC В МВД РОССИИ

Центр оперативного реагирования на инциденты информационной безопасности, SOC (Security Operations Center) – организационная единица подразделения информационной безопасности, которая включает в себя людские единицы, процессы и технологии, предназначенные для получения ситуационной осведомленности в процессе обнаружения, локализации и предотвращения угроз информационной безопасности. SOC включает в себя множество элементов, например Big Data или DLP-система.

Большие данные (англ. big data) – это разновидность подходов, инструментов и методов обработки структурированных и неструктурированных данных огромных объемов и значительного разнообразия для получения «читаемых» человеком результатов, наиболее эффективных в сочетании непрерывного прироста, распределения по многочисленным узлам вычислительной сети, которая может находиться как поблизости, так и задействовать через облачные технологии в пределах одного или нескольких государств, но «отработанную» информацию передавать на только один вычислительный центр.

Для чего нужен такой субъект как big data:

- сбор и обработка больших данных;
- аналитика;
- инженерия больших данных;
- архитектура больших данных и системная интеграция;
- разработка продуктов и услуг на основе больших данных;

¹ © Попов Н. С., 2019.

² © Казанцев В. И., 2019.

- управление большими данными и системами;
- проведение исследований с целью получения новых математических и технических решений для работы с большими данными.

Big Data кратко описывается с помощью четырех Vs: volume (объем), velocity (скорость), variety (разнообразие), veracity (достоверность), теперь о каждом поподробнее.

Объем. Реально большие объемы данных в физическом смысле. Тот объем данных, который раньше накапливался годами, теперь генерируется каждую минуту. Новые инструменты больших данных используют распределенные системы, так что данные можно хранить и анализировать в нескольких географически распределенных базах данных.

Скорость. Сообщения в социальных сетях расходятся по всему интернету в считанные секунды. Современные технологии позволяют анализировать данные на лету, даже не размещая их в базах данных.

Разнообразие. Недавно рассматривались только структурированные данные, аккуратно встроенные в таблицы реляционных баз данных, например, финансовые данные. Но, фактически, 80 % мирового объема данных являются неструктурированными (текст, изображения, видео, голос и т. д.). С технологиями больших данных теперь есть возможность проанализировать и свести воедино данные разных типов, такие как сообщения, разговоры в социальных сетях, фотографии, данные с датчиков, видео или голосовые записи.

Достоверность. Для значительного множества данных их качество и точность являются слабо контролируемыми (сообщения в Твиттере, сокращения и ошибки в разговорной речи, ненадежность и неточности контента). Новая технология позволяет теперь работать и с этим типом данных.

Системы защиты от утечек конфиденциальной информации (Data Loss Prevention – DLP) предназначены для отслеживания и блокирования попыток несанкционированной передачи данных за пределы корпоративной сети. Помимо предотвращения утечек информации DLP система может выполнять функции по отслеживанию действий пользователей, записи и анализу их коммуникаций через e-mail, социальные сети, чаты и т. д. Основная задача систем DLP – обеспечение выполнения принятой в организации политики конфиденциальности (защита информации от утечки).

Использование DLP системы наиболее актуально для организаций, где риск утечки конфиденциальной информации повлечет серьезный финансовый или репутационный ущерб, а также для организаций, ко-

торые настороженно относятся к лояльности своих сотрудников. Решения класса DLP по предотвращению утечек информации обеспечивают защиту такой конфиденциальной информации, как условия тендеров, заказы на услуги и решения, номера пластиковых карт, сведения о счетах клиентов, персональные данные сотрудников и клиентов, финансовые данные и т. д.

К основным функциям DLP-систем относят:

- контроль передачи информации через Интернет с использованием E-Mail, HTTP, HTTPS, FTP, Skype, ICQ и других приложений и протоколов;
- контроль сохранения информации на внешние носители – CD, DVD, flash, мобильные телефоны и т. п.;
- защита информации от утечки путем контроля вывода данных на печать;
- блокирование попыток пересылки/сохранения конфиденциальных данных, информирование администраторов ИБ об инцидентах, создание теневых копий, использование карантинной папки;
- поиск конфиденциальной информации на рабочих станциях и файловых серверах по ключевым словам, меткам документов, атрибутам файлов и цифровым отпечаткам;
- предотвращение утечек информации путем контроля жизненного цикла и движения конфиденциальных сведений.

Обычно система класса DLP включает следующие компоненты:

- центр управления и мониторинга;
- агенты на рабочих станциях пользователей;
- сетевой шлюз DLP, устанавливаемый на Интернет-периметр.

Для чего нужно создание SOC?

Следует заметить, что SOC находит уязвимые места и предотвращает атаки на них; SOC автоматизирует функции, которые и так уже сейчас есть в организации, что позволяет снижать те или иные расходы, к примеру, часть подразделений готовы отдать свои функции в SOC и таким образом минимизировать свои расходы, вкладывая часть своих ресурсов в его построение.

Между тем предоставление услуг SOC другим организациям окупит все вложения (так работают провайдеры сервисов по управлению безопасностью – Manager Security Services Providers – MSSP).

Предпосылкой создания SOC был Fusion Center. Отличительной чертой является то, что Fusion Center был предназначен для обмена информацией, а не круглосуточного мониторинга информационной безопасности. Более того, первоначально, да и сейчас, эти центры не имели ничего общего с кибербезопасностью. Они создавались под эгидой Министерства национальной безопасности или Министерства юстиции Российской Федерации, и позволяли обмениваться стратегической информацией между ФБС, Министерством обороны Российской Федерации, МЧС и т. д. В первые годы Fusion Center, а их насчитывалось только несколько десятков, были неэффективны: они обменивались плохо структурированной информацией, которую сложно было анализировать, искать в ней взаимозависимости и строить на ее основе какие-то выводы и принимать решения. Например, в 2011-м г. Fusion Center сообщил о взломе насосной станции системы водоснабжения в Подмосковье. Позже сотрудники ФБС опровергли данное заявление, доказав, что речь шла о легальном удаленном доступе администратора насосной станции.

Что же касается широкомасштабного применения SOC в Российской Федерации, то первым был Сбербанк России. Первый этап по созданию SOC, включал в себя внедрение SIEM-системы, ориентированной на сбор и корреляцию событий безопасности и был завершен в апреле 2016 г. В 2018 г. по окончании второго этапа строительства центра безопасности ИТ-системы стали рассматривать миллионы подозрительных финансовых «событий» в день, для анализа которых были внедрены средства искусственного интеллекта¹.

¹ В результате количество рассмотренных в день подозрительных «событий» в работе систем организации увеличилось до нескольких миллионов (сейчас этот показатель составляет 4 млн в сутки). В общей сложности работу центра безопасности обеспечивают более сотни сотрудников. Точное количество специалистов и местоположение SOC в Сбербанке не уточняют. Совокупный ИБ-бюджет банка в 2015 г. (включая строительство SOC) составил 1,5 млрд.

*Распутина Анастасия Дмитриевна¹,
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

*Аветисян Карэн Рафаелович²,
преподаватель кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ РЕСУРСОВ В ДЕЯТЕЛЬНОСТИ ОВД

Анализ состава информационных ресурсов МВД России позволяет разделить их на ряд групп.

Информационные ресурсы управленческого и справочного характера

В деятельности ОВД создается значительное количество нормативных и ненормативных управленческих документов. Документы создаются и пересылаются в «бумажном» и электронном виде. Причем электронный документооборот в последние годы значительно возрос.

Одной из ключевых целей документооборота является создание информационных ресурсов управленческих документов. Для этого в органах внутренних дел организовано текущее и архивное хранение документов. После исполнения документы объединяются в дела. Сформированные дела хранятся установленные сроки и используются в деятельности органов внутренних дел, а в отдельных случаях в деятельности других правоохранительных и государственных органов.

Основой электронного документооборота в МВД России является Положение о системе передачи информации с ограниченным доступом (СПИОД), не содержащей сведений, составляющих государственную тайну, в технических каналах связи в системе МВД России. Указанное Положение устанавливает возможность передачи информации, в том числе заверенной электронной цифровой подписью, через защищенную систему передачи данных, а также регламентирует порядок обмена информацией конфиденциального характера в электронной форме.

¹ © Распутина А. Д., 2019.

² © Аветисян К. Р., 2019.

Кроме того, к информационным ресурсам управленческого и справочного характера относятся следующие информационные ресурсы:

- информационные ресурсы нормативно-правового характера, объединенные в базы данных «Нормативно-правовые акты», «Судебная практика», «Международные договора», «Юридическая консультация» в рамках СТРАС «Юрист»;
- информационные ресурсы о сотрудниках ОВД, объединенные в базу данных «Кадры», информационные ресурсы об информации штатного характера, объединенные в АИС «Штаты»;
- информационные ресурсы о финансировании МВД России, объединенные в автоматизированную систему управления.

Оперативно-справочные и розыскные информационные ресурсы

Информационные ресурсы оперативно-справочного и розыскного характера создаются в дежурных частях, оперативными работниками, участковыми инспекторами полиции, следователями, сотрудниками экспертно-криминалистических и лицензионно-разрешительных подразделений, сотрудниками паспортно-визовых служб и других подразделений. Указанные информационные ресурсы создаются на основе документов первичного учета, в учетных журналах и на других носителях. Они включают в себя сведения о: людях, в том числе совершивших преступления и правонарушения; предметах, в том числе оружии и автотранспорте; помещениях (адресах); нераскрытых преступлениях; происхождении и принадлежности обнаруженных вещественных доказательств и т. д.

Информация оперативно-справочного и розыскного характера объединяется в информационные ресурсы в информационных центрах МВД республик, региональных УМВД, УМВДТ. На федеральном уровне информационные ресурсы оперативно-справочного и розыскного характера концентрируются в Главном информационно-аналитическом центре МВД России.

Внедрение навигационно-мониторинговых систем для позиционирования служебного автотранспорта (с использованием ГЛОНАСС), а также формирование в муниципальных образованиях элементов аппаратно-программного комплекса «Безопасный город» и введение в эксплуатацию стационарных и удаленных рабочих мест доступа к ин-

формационным ресурсам позволит добиться четкого и слаженного взаимодействия нарядов ППС, ДПС ГИБДД, вневедомственной охраны под руководством дежурной части ОВД¹.

Экспертно-криминалистические информационные ресурсы

Для производства экспертиз и исследований правоохранные органы используют огромное количество разнообразной как чисто криминалистической, так и справочно-вспомогательной информации. Для хранения и использования указанной информации в экспертных учреждениях МВД России созданы экспертные автоматизированные информационные системы и автоматизированные банки данных практически по любому виду экспертиз. Основными информационными ресурсами экспертной информации являются автоматизированные дактилоскопические информационные системы (АДИС) и автоматизированные баллистические идентификационные системы (АБИС).

АДИС применяются при ведении дактилоскопических автоматизированных учетов, в целях осуществления оперативной проверки следов пальцев рук, изымаемых с места происшествия, по массивам дактилокарт ранее осужденных или определенного круга подозреваемых лиц. Информационные ресурсы о дактилоскопических учетах являются одними из основных информационных ресурсов МВД России. Необходимо отметить, что формирование и ведение подавляющего большинства дактилоскопических учетов осуществляет МВД России.

АБИС позволяют идентифицировать оружие по стреляным пулям и гильзам. Посредством АБИС возникла возможность автоматизировать всю технологическую цепочку трасологических исследований пуль, гильз и их фрагментов: от ввода информации и создания электронной базы данных, проверок и сравнительных исследований, до получения экспертного заключения.

Также к информационным ресурсам экспертно-криминалистической направленности относятся информационные ресурсы автоматизированных лабораторий ДНК-анализа, лабораторий, занимающихся фотоскопическими исследованиями².

¹ Кузнецова Л. В., Миронов Е. В., Бояркин А. Б. Аналитическая работа в территориальных органах МВД России на районном уровне : учебно-методическое пособие. Барнаул : БЮИ МВД России, 2017.

² Прокопенко А. Н. Информационные ресурсы МВД России на современном этапе // URL : <https://www.cyberleninka.ru/article/n/2-7-infrmatsionnye-resursy-mvd-rossii-a-sovremennom-etape>.

Статистические информационные ресурсы

В них входит информация о преступлениях, лицах, их совершивших, о материальном ущербе и изъятии предметов преступной деятельности, о потерпевших, о движении уголовных дел и результатах их рассмотрения судом первой инстанции. Статистические информационные ресурсы о преступности в настоящий момент представляют собой единую систему учета преступлений, формирование которой осуществляется разными правоохранительными ведомствами, а ведение и использование поручено МВД России.

Информационные ресурсы Интерпола и используемые органами внутренних дел информационные ресурсы других правоохранительных и иных государственных органов Российской Федерации

Национальное центральное бюро Интерпола формирует информационные ресурсы о лицах, организациях, событиях, предметах и документах, связанных с преступлениями, носящими международный характер, а также справочно-информационный фонд.

Формирование информационных ресурсов НЦБ Интерпола осуществляется всеми правоохранительными ведомствами и зарубежными партнерами. МВД России активно взаимодействует с другими правоохранительными органами в области формирования и использования информационных ресурсов. В первую очередь, необходимо отметить формирование информационных ресурсов о гражданах Российской Федерации, иностранных гражданах и лицах без гражданства, осуществляемое Федеральной миграционной службой. Указанные информационные ресурсы включены в состав оперативно-справочных и розыскных информационных ресурсов МВД России. Также МВД России взаимодействует с Министерством юстиции, Министерством обороны, Федеральной налоговой службой и другими правоохранительными ведомствами.

Информационные ресурсы образовательных учреждений МВД России и системы научно-технической информации

К информационным ресурсам образовательных учреждений относятся, в частности, фонды библиотек образовательных учреждений. Кроме того, в каждом вузе создан информационный образовательный центр, в котором формируются электронные информационные ресурсы для самостоятельной работы курсантов и слушателей. Информатизация образовательных учреждений МВД России является составной частью информатизации органов внутренних дел и включает в себя информатизацию:

- учебно-воспитательного процесса;
- научных исследований;
- служб, обеспечивающих учебный процесс и жизнедеятельность образовательного учреждения;
- процесса координации деятельности образовательных учреждений.

Система научно-технической информации МВД России предназначена для информационного обеспечения оперативно-служебной и иной деятельности органов, подразделений, учреждений внутренних дел, проводимых в МВД России научно-исследовательских и опытно-конструкторских работ, учебного процесса в образовательных и научно-исследовательских учреждениях МВД России на базе информационных ресурсов, накапливаемых в результате обработки сведений о достижениях науки и техники, положительном опыте деятельности органов внутренних дел Российской Федерации и зарубежных правоохранительных органов.

Информационные ресурсы СНТИ содержат материалы об опыте работы органов внутренних дел России, деятельности правоохранительных органов зарубежных стран, а также сведения о результатах проводимых в системе МВД России научно-исследовательских и опытно-конструкторских работ и диссертационных исследований.

Необходимо отметить, что внедренная в последние годы система дистанционных образовательных технологий (СДОТ) на базе комплекса «Стеллус» также предназначена для накопления информационных ресурсов образовательных учреждений и организации дистанционного обучения сотрудников МВД России¹.

Совершенствование аналитической работы органов внутренних дел

Сегодня информационно-аналитическая работа в органах внутренних дел не должна оставаться на том уровне. Прежде всего, она призвана своевременно выявлять назревающие негативные тенденции в сфере правопорядка, для чего необходимы соответствующая коррекция ранее разработанных оперативных и профилактических мероприятий, перераспределение имеющихся сил и средств, принятие иных упреждающих мер.

¹ Кузнецова Л. В., Миронов Е. В., Бояркин А. Б. Аналитическая работа в территориальных органах МВД России на районном уровне : учебно-методическое пособие. Барнаул : БЮИ МВД России, 2017.

В связи с этим и в целях совершенствования информационно-аналитической работы можно предложить осуществление следующих мероприятий:

В первую очередь, необходимо расширение идеологии, содержания аналитической работы. Это обусловлено тем, что аналитическая работа сводится не только к регулярному написанию аналитических справок и оценок обстановки, а включает в себя проведение научных изысканий, особенно по новым проблемам, с которыми ранее правоохранительным органам не приходилось сталкиваться.

Для решения этой ключевой задачи информационного обеспечения необходимо пересмотреть и скорректировать существующую систему формирования и ведения важнейшей информации в виде схемы взаимосвязи возникающих проблем и принимаемых решений. В ней во взаимосвязанном виде должна содержаться сводная аналитическая информация по ключевым проблемам развития политической и экономической ситуации, процессам и тенденциям в состоянии правопорядка и преступности, деятельности ОВД и иных государственных и негосударственных структур, обеспечивающих общественную безопасность и борьбу с преступностью, условия эффективной реализации проблем, предлагаемые и осуществляемые решения. При этом возникает принципиально важное условие – возможность рассмотрения основополагающих проблем и решений не изолированно, а комплексно, что, в свою очередь, позволит руководителю осуществлять управление и контроль не по отдельным задачам, а с точки зрения реализации проводимой политики в целом.

Во-вторых, необходимо распространение перспективных форм и методов информационно-аналитической работы. Это либо создание самостоятельного ведомственного научно-практического издания по проблемам информационно-аналитической работы, либо использование для этого постоянной рубрики в уже существующих ведомственных изданиях, или регулярное проведение кустовых и всероссийских научно-практических семинаров по проблемам информационно-аналитического обеспечения деятельности ОВД с публикацией их результатов.

В-третьих, необходимо интегрировать усилия разрозненных научных коллективов и отдельных ученых на решении проблем оценки анализа и прогнозирования преступности. С этой целью целесообразно разработать и утвердить отраслевую программу научно-исследовательских работ по проблемам информационно-аналитической деятельности ОВД, с использованием системного метода, который позволит изучить влияние

социально-экономической ситуации на состояние криминогенной обстановки как взаимодействие системных образований.

Между тем, реализация приведенных в данной статье предложений должна обеспечить координацию при решении сложных проблем, например, таких как:

а) разработка методики оценки криминогенной ситуации по линиям служб: создание постоянной системы мониторинга преступности и системы мониторинга деятельности подразделений по различным направлениям оперативно-служебной деятельности, с использованием возможностей Организационно-аналитического управления ОВД, ГИАЦ и главных управлений МВД России;

б) анализ статистических материалов по различным, отдельно взятым направлениям, к примеру, о влиянии социально-экономической ситуации на состояние оперативной обстановки в конкретном регионе, открывает в настоящее время широкие, принципиально новые возможности в информационно-аналитическом обеспечении деятельности ОВД. Связано это и с возможностью эффективного использования современных компьютерных технологий в информационно-аналитической работе органов внутренних дел;

в) совершенствование правового регулирования организации информационно-аналитического обеспечения деятельности ОВД, что в настоящее время также остается одной из важных нерешенных проблем. Информационные фонды, предназначенные для обеспечения деятельности органов внутренних дел, ведутся на основе большого числа нормативных актов, которые зачастую противоречат друг другу. Существующие же ведомственные правовые акты касаются лишь отдельных аспектов данной проблемы, что облегчит взаимодействие органов, усовершенствует работу информационно-аналитического обеспечения, а также будет способствовать пресечению преступлений и их прогнозированию.

Тараканова Татьяна Эдуардовна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Пузарин Андрей Валерьевич²,
*начальник кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ОСНОВНЫЕ МЕТОДЫ КОНТРОЛЯ ЦИФРОВОГО РАДИОЭФИРА

Цифровое радио – это технология беспроводной передачи цифровой информации посредством электромагнитных волн радиодиапазона. Сейчас в мире постепенно начинается переход к «цифре», но он гораздо медленнее, чем у телевидения так как в отличие от аналогового вещания, где уменьшение уровня сигнала ниже определенного уровня приводит к ухудшению соотношения сигнал-шум, в цифровом – трансляция пропадает вовсе.

Актуальность данной статьи обусловлена необходимостью перевода вещания от аналогового режима к цифровому, а также мировым прогрессом в области цифровой техники и нарастающим процессом слияния компьютерных технологий, средств связи, вещания и информационных служб в единую интерактивную цифровую систему. Под действием этих процессов уже сейчас становится вполне очевидно, что вскоре общество будет иметь совсем другое радиовещание, совершенно не такое, каким мы его знаем теперь. Радиоканалы уже сейчас входят в мультиплексы цифрового телевидения, как эфирного, так и спутникового.

Индикаторы электромагнитного поля, несомненно, являются самыми доступными и простыми приборами для поиска радиопередающих устройств. Индикаторы успешно применяются не только в качестве средств экспресс-анализа, но и в качестве дополнения к более сложным средствам радиомониторинга.

¹ © Тараканова Т. Э., 2019.

² © Пузарин А. В., 2019.

Классический индикатор поля представляет собой всеволновой измеритель мощности электромагнитного поля, наводимого на его приемную антенну.

Основные проблемы при работе с индикаторами поля связаны с большим разбросом по мощности фоновых источников и сложности пространственного распределения этих полей.

Математическое описание полей позволяет рассчитать радиус ближнего поля источника, как функцию излучаемой длины волны и геометрических размеров излучающей антенны.

Современные специальные технические средства (СТС), использующие для передачи перехваченной информации радиоканал (далее – радиозакладки), за последние несколько лет шагнули в своем развитии настолько далеко вперед, что многие комплексы радиомониторинга просто не в состоянии их обнаружить с приемлемой вероятностью.

В настоящее время активно развиваются несколько направлений создания радиозакладок. Выделим основные – сложные типы сигналов для передачи перехваченной информации (широкополосных, шумоподобных, ППРЧ и т. д.), затрудняющие обнаружение их средствами радиомониторинга.

С нашей точки зрения, наиболее опасное направление – использование легальных каналов связи (DECT, Bluetooth, Wi-Fi, GSM и т. д.) для передачи перехваченной информации. В данном случае многие специалисты, используя имеющуюся у них аппаратуру, не в состоянии отличить работающее по своему прямому назначению легальное радиоизлучающее устройство от используемого для негласного съема информации. Сделать это без применения специальных средств анализа цифровых пакетов в реальном масштабе времени, невозможно.

Если рассматривать вопрос использования легальных каналов связи для работы радиозакладок, в качестве примера возьмем радиотелефонию стандарта DECT и сложности, связанные с выявлением радиозакладок на его основе. При существующей в настоящее время плотности использования беспроводной связи стандарта DECT и активном применении при производстве специальных технических средств перехвата акустической информации (СТС) этого вида передачи, уже недостаточно просто фиксировать факт работы данного стандарта связи.

С помощью различных комплексов можно выявлять нестандартную работу сети – фактически, обнаруживать работу средств перехвата мобильной связи. Видя все каналы, оператор получает следующие пара-

метры топологии сети: принадлежность к стране, к оператору, идентификатор базовой станции, код сектора, Location Area (LA – идентификатор группы сот, объединенных по географическому признаку). Комплекс видит все служебные каналы, каналы трафика и привязку их друг к другу.

При возникновении подмены базовой станции (БС) оператор может увидеть или новый идентификатор БС с мощным уровнем сигнала, или просто значительное увеличение мощности сигнала одной из БС. Также может измениться привязка служебных каналов к трафиковым.

Существующее на данный момент программное обеспечение позволяет в любой момент можно посмотреть необходимый материал в нужном промежутке времени: хоть день назад, хоть годы. И для этого нет необходимости работать на отдельном компьютере – анализировать накопленную информацию можно на том же ноутбуке, где работает комплекс, причем даже без его остановки. Можно проанализировать любую интересующую полосу – когда сигнал работал в эфире, когда его не было.

С учетом анализа методов радиомониторинга и особенностей цифрового радиоэфира, можно отметить, что важную роль в комплексах радиоконтроля стала играть функция отображения спектра сигналов в виде так называемого «водопада», позволяющего наблюдать за изменениями радиочастотного спектра с привязкой ко времени. Появляется возможность вести базу данных непрерывно и круглосуточно, не теряя ни один принятый комплексом сигнал. Иногда достаточно взглянуть на «водопад», чтобы визуально обнаружить работу закладки.

В заключение следует выделить, что только круглосуточный радиоконтроль позволяет наблюдать за тем, как «живет» сигнал, как он соотносится с различными важными событиями на охраняемом объекте, обнаруживать закономерности во времени появления в эфире, сравнивать текущие спектры сигналов с ранее полученными. Наличие перечисленных возможностей является необходимым и обязательным требованием к современному поисковому комплексу радиомониторингу.

Таранина Екатерина Игоревна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Пименова Оксана Владимировна²,
*доцент кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

Мусоев Давлахмад³,
*старший преподаватель кафедры огневой подготовки
учебно-научного комплекса специальной подготовки
Московского университета
МВД России имени В.Я. Кикотя*

ОБРАБОТКА ИЗОБРАЖЕНИЙ, ИСПОЛЬЗУЕМЫХ В ДАКТИЛОСКОПИИ

Дерматоглифика – научная дисциплина, которая изучает рельеф кожи на пальцах, ладонных и подошвенных поверхностях человека. Обычно дерматоглифические исследования производят на основе визуального анализа, что является монотонной работой и, как следствие, они не могут удовлетворить требованиям получения своевременной и точной информации, которые имеются на сегодняшний день.

Чтобы свести на ноль неудобства, связанные с исследованием папиллярных узоров, необходимо разработать программное обеспечение для обработки изображений и отпечатков пальцев.

В основу алгоритма обработки изображений, предназначенных для дактилоскопических исследований, должен быть включен расчет коэффициента корреляции между двумя матрицами изображений.

Корреляцией называется статистическая взаимосвязь двух или нескольких случайных величин. При этом изменения значений одной или нескольких из этих величин сопутствуют систематическому изменению значений другой величины.

¹ © Таранина Е. И., 2019.

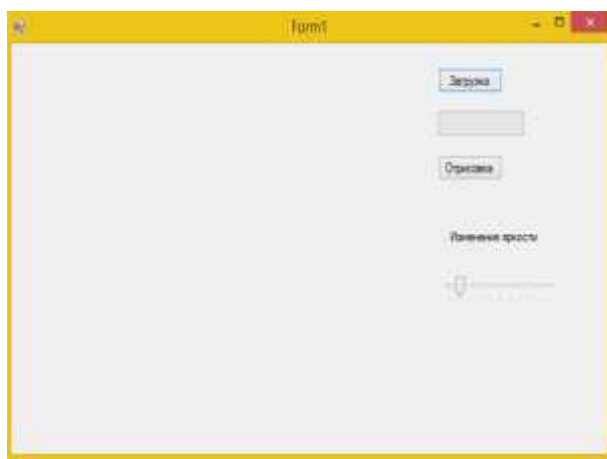
² © Пименова О. В., 2019.

³ © Мусоев Д., 2019.

Таким образом, главная цель корреляционного анализа – обеспечить получение некоторой информации об одной переменной с помощью другой переменной.

При изменении роста и веса разных людей каждое измерение представляется точкой в двухмерном пространстве.

Для реализации алгоритма обработки изображений, мною была создана программа, предназначенная для просмотра изображения в формате RAW, редактирования яркости и контрастности. Данная программа написана на языке программирования C# в консольном приложении Microsoft Visual Studio 2015. Программа состоит из двух форм: формы входа и основной формы (рис. «Форма входа в приложение»).



Форма входа в приложение

Перед входом в данную программу необходимо пройти процедуру аутентификации – проверку подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базах данных пользователей. Если пароли совпадают, то процедура аутентификации успешно пройдена, и пользователю предоставляется доступ для работы с программой.

Основная форма состоит из кнопки загрузки входного изображения, индикатора процесса, кнопки попиксельной отрисовки загруженного изображения и ползунка изменения яркости.

При загрузке входного изображения в программу, происходит запись изображения в массив и дальнейшая попиксельная отрисовка, где пиксель – это минимальная единица изображения.

Изменение яркости изображения происходит путем прибавления одинакового значения. Изменение контраста происходит путем увеличения разности между черным и белым элементом изображения.

На данном этапе разработки, программа предназначена для изменения яркости и контрастности, что необходимо для анализа изображений, используемых при дактилоскопии.

Планируется дальнейшее совершенствование программы путем добавления кнопок загрузки эталонного изображения и создания диалогового окна для выбора нескольких изображений для загрузки.

Для сравнения исследуемого объекта с эталонным планируется произвести корреляционное сравнение выбранного изображения с серией эталонных изображений и зафиксировать максимальные значения коэффициента корреляции. Работа по совершенствованию новых алгоритмов корреляционного анализа изображений является попыткой решения не только проблем, существующих в дактилоскопии, но и проблем, входящих в одну из областей информационных технологий – цифровую обработку изображений

Титова Мария Игоревна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Клочкова Екатерина Николаевна²,
*доцент кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ОРГАНИЗАЦИЯ ЗАЩИТЫ ДАННЫХ В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ МВД РОССИИ

Использование компьютеров играет огромную роль в современной жизни, так как на данном этапе развития практически все основывается на информационных технологиях. Эта тенденция не миновала и органы внутренних дел МВД России. Для организации слаженной работы органов внутренних дел МВД России широко применяются различные информационные системы (далее – ИС). Там, где присутствуют ИС, существуют и угрозы для них.

Актуальные угрозы безопасности персональных данных, в соответствии с постановлением от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах» – это такая совокупность условий и факторов, которые создают риск несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, что может привести к уничтожению, изменению, блокированию, копированию, предоставлению, распространению персональных данных, а также иные неправомерные действия. Существуют угрозы четырех типов, которые возможны на прикладном, системном и системном и прикладном программных обеспечениях. При обработке персональных данных в информационных системах устанавливаются четыре уровня защищенности, на каждом из которых необходимо выполнение хотя бы одного условия, чтобы защита была организована верно.

¹ © Титова М. И., 2019.

² © Клочкова Е. Н., 2019.

Для организации эффективной защита информационной системы необходимо проанализировать модель угроз информационной безопасности.

Для построения модели угроз информационной безопасности необходимо выполнить несколько последовательных шагов (однако составляются они на основе постоянно меняющихся данных):

- определение источников угроз;
- выявление критических объектов информационной системы;
- определение перечня угроз для каждого критического объекта;
- выявление способов реализации угроз;
- оценка материального ущерба и других последствий возможной реализации угроз.

Грамотный анализ существующих угроз и дальнейшее их моделирование, верное определение уровня защиты информации занимают основную долю защиты информационных систем, это касается и информационных систем, которые используются в ОВД.

В настоящее время происходит активное объединение всех ИС в ИСОД МВД России, для того чтобы всем подразделениям из разных регионов было возможным их использование. Однако некоторые системы остались самостоятельными, и каждая из них отвечает за разные функции:

- автоматизированная информационная система «Синергет-Розыск» – используется для идентификации граждан по лицу и поиска лиц, которые находятся в розыске;
- информационная база данных федерального уровня ИБДФ МВД России – база, предназначенная для предоставления информации по судимостям, уголовным правонарушениям, паспортным данным, сведений о зарегистрированном оружии граждан РФ и иностранных граждан;
- информационная база данных федерального уровня ИБДР МВД России – фактически тоже самое, что и ИБДФ, только поиск происходит по регионам, а не по всей России;
- программно-технический комплекс «Розыск-Магистраль» – программно-технический комплекс МВД России по выявлению лиц, которые находятся в розыске;
- Федеральная миграционная служба России «Территория» – база данных, в которой содержатся данные о регистрации лиц в Москве;

- база данных «Записная книжка» – база данных, в которой происходит идентификация лиц и нахождение связей по номерам телефонов, ФИО, кличкам;

- ИСОД МВД России — это совокупность используемых в МВД России автоматизированных систем обработки информации, программно-аппаратных комплексов и программно-технических средств, систем связи и передачи данных, функционирующая на принципе работы облачных технологий.

Для того чтобы максимально снизить человеческий фактор при работе с ИС, необходимо выполнять следующие правила:

- хранить свой ПИН-код в тайне, а именно нельзя хранить его возле рабочего места, в ящиках, на мониторе, на столе и т. д., а идентификатор рутокен – в недоступном для других месте;

- не использовать посторонние носители информации;

- не отключать средства защиты информации, установленные на рабочем месте;

- при убытии с рабочего места на продолжительное время отключать компьютер;

- минимум раз в месяц менять пароль доступа в ИСОД. Пароль должен быть сложным для угадывания злоумышленниками, а именно: с использованием букв верхнего и нижнего регистра, цифр, символов, латинских букв. Пароль не должен состоять из логических фраз и каких-либо слов, и быть длиннее 6 символов, но при этом запоминаемым для сотрудника.

Говоря об организации защиты информации в ИС, нельзя ограничиваться только программными и техническими мерами. Одним из ключевых аспектов обеспечения защищенности системы является организационная защита. Сотрудник органов внутренних дел может оказаться самым уязвимым звеном в обеспечении защиты информации в ИСОД МВД России. Из этого следует, что по степени реализации технических мер, основной акцент должен концентрироваться и усиливаться на неукоснительном соблюдении культуры обеспечения информационной безопасности на этапе эксплуатации ИСОД МВД России, сущностью которой является не только личная ответственность руководителя всех уровней за организацию защиты информационных ресурсов, а также строгое выполнение установленных правил обеспечения безопасности информации каждым отдельным сотрудником.

Список литературы

1. Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
2. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 (ред. от 23.03.2017) «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
3. Методический документ ФСТЭК «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.).
4. Стандарт ЦБР СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (принят и введен в действие распоряжением ЦБР от 21 июня 2010 г. № Р-705).
5. Горский, В. Г., Королев, Д. Г. О перспективах развития информационных систем в МВД России на основе «облачных» технологий. // Совершенствование и внедрение IT-технологий в деятельности органов внутренних дел Российской Федерации. – 2012. – С. 44–45.
6. Кадулин, В. Е., Потехин, В. С. Об уточнении понятия и классификации автоматизированных рабочих мест, используемых в информационных системах и компьютерных технологиях. – Вестник Санкт-Петербургского университета МВД России. – 2015. – № 4 (68). – С. 207–210.

Филимонова Юлия Витальевна¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Орехов Павел Васильевич²,
*преподаватель кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

АНАЛИЗ УЯЗВИМОСТЕЙ КОМПЛЕКСНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ

В современном мире подход к проектированию автоматизированной системы безопасности того или иного объекта предполагает взаимное интегрирование различных подсистем безопасности, вне зависимости от того, когда идет речь о крупном объекте или об офисе, состоящем из нескольких кабинетов. Рассмотрим функции и элементы системы безопасности.

Безопасность организации, компании, офиса, производственного или иного помещения обеспечивается целым комплексом мер. К важной составляющей выявления угроз и их нейтрализации относятся системы безопасности. Они нужны на любом коммерческом объекте. Системы безопасности обеспечивают стабильность работы организации, выполняя различные функции защиты и контроля.

Первоочередная задача любого комплекса – это охрана организации от внешних и внутренних угроз таких. В качестве таких угроз, в основном, рассматривают следующее:

- перехват управления предприятием;
- подрыв деловой репутации компании;
- материальный ущерб;
- попытка хищения имущества или коммерческой тайны;
- возникновение пожара, аварии и других опасных для жизни и здоровья людей ситуаций.

Именно системы безопасности способны справиться с предупреждением подобных угроз путем обеспечения контроля доступа на территорию предприятия и охраняемых объектов, мониторингом ситуации в режиме реального времени и принятием срочных мер в случае возникновения чрезвычайных ситуаций.

¹ © Филимонова Ю. В., 2019.

² © Орехов П. В., 2019.

Червонюк Руслан Михайлович¹,
*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Белоглазов Евгений Григорьевич²,
*профессор кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ОРМ «НАБЛЮДЕНИЕ» КАК ФОРМА КОМПЬЮТЕРНОЙ РАЗВЕДКИ

Наблюдение – это ОРМ, направленное на получение оперативно-разыскной или иной юридически значимой информации путем непосредственного или опосредованного с помощью технических средств, визуального и(или) слухового контроля за физическими лицами, а также ее фиксация и регистрация.

Наблюдение может осуществляться визуально, при помощи технических средств, а также комплексно. В процессе наблюдения может применяться аудиозапись, видео-, фотосъемка и средства слухового контроля.

В процессе наблюдения в порядке хронологии фиксируются все действия объекта наблюдения.

Наблюдение, ограничивающие конституционные права граждан, допускаются на основании судебного решения только при наличии у оперативного сотрудника информации, предусмотренной Законом об оперативно-розыскной деятельности.

Наблюдение, не ограничивающее конституционные права граждан, осуществляются по решению оперативного сотрудника, а в случае привлечения дополнительных сил и средств – по решению руководителя соответствующего подразделения.

С учетом того, что преступные действия лиц не ограничиваются пределами одного государства, наблюдение может осуществляться и за пределами Российской Федерации:

– сотрудниками правоохранительных органов государств – участников СНГ по запросам российских органов;

¹ © Червонюк Р. М., 2019.

² © Белоглазов Е. Г., 2019.

– оперативными сотрудниками российских органов в течение пяти часов с момента пересечения границы государства – члена Европейского союза с правом задержания лица до прибытия местной полиции.

Результаты наблюдения отражаются в составляемых оперативным сотрудником рапорте или справке, к которым прилагается аудио – и видеозаписи, фотографии.

Объектами компьютерной разведки в рамках ОРМ «наблюдение» являются информация о признаках преступной деятельности, возможных участниках, местах хранения орудий совершения преступлений и похищенного имущества, а также материальные носители информации, представляющей оперативный интерес.

Наблюдение может осуществляться оперативными работниками, агентами и иными лицами, оказывающими содействие, т. е. основным субъектом наблюдения является оперативный работник или по его заданию – сотрудники специальных оперативно-поисковых подразделений правоохранительных органов, дополнительным субъектом – лицо, оказывающее содействие в осуществлении ОРД открыто и на конфиденциальной основе.

Выделяют два основных вида наблюдения: физическое визуальное и электронное(техническое). Наблюдение может быть комплексным, т. е. сочетающим в себе элементы физического и электронного наблюдения.

Физическое наблюдение – метод визуального получения информации, выражающийся в негласном, направленном, непосредственном восприятии деятельности объекта оперативной заинтересованности наблюдателем.

Техническое(электронное) наблюдение – опосредованный метод получения информации с помощью оперативно-технических средств, заключающийся в негласном направленном восприятии деятельности объекта оперативной заинтересованности.

Электронное наблюдение – метод, основанный на применении специальных технических средств для слежения за действиями подозреваемого в помещениях и транспортных средствах; оно осуществляется сотрудниками специальных оперативно-технических подразделений. Электронное наблюдение может осуществляться с помощью фото-, киносъемки или видео- и аудиозаписи, которая применяется с целью слухового контроля и записи разговоров подозреваемых.

Техническое(электронное) наблюдение позволяет установить лиц, участвующих в общении, кто, где и с кем встречается, цель их контактов, содержание разговоров.

Целью компьютерной разведки является получение информации, имеющей оперативное значение

Задачами компьютерной разведки является получение и обработка данных с линий связи, компьютеров, компьютерных систем, материальных носителей и преобразование информации в удобную форму.

Для их выполнения требуется получение характеристик программно – аппаратных средств и телекоммуникационного оборудования, реализуемое в ходе обследования помещений, зданий, сооружений, участков местности, транспортных средств.

История борьбы с преступностью показывает, что для своевременного обнаружения, предупреждения, пресечения и раскрытия тяжких преступлений, розыска скрывшихся преступников одних только гласных уголовно-процессуальных и иных средств не достаточно, необходимы и иные средства борьбы с преступностью.

Важнейшей задачей для правоохранительных органов является не только расследование уже совершенных преступлений, но и контроль за развитием криминальных явлений и процессов. Лучше, если этот контроль будет негласным, то есть не известным самим объектам контроля. Использование специальных средств разрешено только правоохранительным органам для осуществления оперативно-разыскных, контрразведывательных мероприятий и решения задач органов досудебного расследования.

К специальной технике относятся специально сконструированные радиотехнические, оптические, видеотехнические, звукозаписывающие и другие научно-технические средства, основным назначением которых является негласное получение и фиксация информации.

*Шарова Ксения Михайловна¹,
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

*Овчинский Анатолий Семенович²,
профессор кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ПРИМЕНЕНИЕ МЕТОДОВ И ИСПОЛЬЗОВАНИЕ СРЕДСТВ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ ПРАВООХРАНИТЕЛЬНЫМИ ОРГАНАМИ

С развитием информационных технологий появляются новые методы воздействия на сознание и подсознание людей, называемые информационно-психологическими, которые представляют собой комплекс специальных психологических операций, мероприятий, акций, информационного, психотронного или психофизического воздействия на психику человека, оказывающего влияние на восприятие им реальной действительности, в том числе на его поведенческие функции, а также в некоторых случаях на функционирование органов и систем человеческого организма, которое проводится с помощью информации, пропаганды и агитации, подготовленной соответствующим образом и доводимой до объекта (групп объектов), осуществляемый с помощью различных форм психологического воздействия (печатными средствами, радио- и телевидением, изобразительными средствами, через непосредственное общение, материальными акциями, через информационные компьютерные сети и различные информационно-технологические средства). Среди них обычно выделяют аудиальное, визуальное, психофизическое и другие виды воздействий.

В настоящее время органы внутренних дел уже используют некоторые методы и средства, которые воздействуют не только на физический уровень (например, временная слепота или глухота), но и на психику человека в целом. В ст. 21 Федерального закона от 7 февраля

¹ © Шарова К. М., 2019.

² © Овчинский А. С., 2019.

2011 г. № 3-ФЗ «О полиции» в качестве специальных средств, используемых сотрудниками, закреплены специальные акустические и световые средства.

Существуют более перспективные и эффективные разработки средств информационно-психологического воздействия, но возникает вопрос: используются ли они правонарушителями? Считается, что использование средств мультимедиа и иного сопровождения каких-либо массовых мероприятий, воздействуя на органы чувств человека, может вызывать определенные эмоциональные отношения к окружающей действительности и мотивировать поступки. Так, в Конституции Российской Федерации обозначено: «Права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства» (ч. 3, ст. 55). Поэтому, в случае проявления агрессии на массовых мероприятиях или при массовых беспорядках применяются средства звукоусиления сигнала высокой интенсивности, что, как раз, позволяет воздействовать на группы людей и их сознание, эмоциональное состояние в целях изменения их поведения. Однако применение таких средств должно соответствовать требованиям «Санитарных норм допустимой громкости звучания звуковоспроизводящих и звукоусилительных устройств в закрытых помещениях и на открытых площадках» (СанПиН 42-128-4396-87).

Деятельность ОВД направлена в основном на пресечение и предупреждение преступлений и правонарушений. Исходя из этого, отметим, что аудиальные и визуальные методы воздействия в деятельности сотрудников могут использоваться как способ предупреждения, а иногда и пресечения правонарушений. Рассмотрим их подробнее.

Для начала дадим определение аудиальных и визуальных воздействий. Аудиальное воздействие – это воздействие звуковых волн различной частоты и интенсивности. Визуальное воздействие представляет собой воздействие световых волн на сенсорное восприятие живых существ. Часто такие воздействия используют в целях изменения отношения человека к тем или иным вещам, привычкам. Фразы суггестивного воздействия и особая обработка видеофайла помогают человеку бросить курить, вылечить бессонницу, улучшить состояние психики и т. д. Сегодня данные методы широко используются в лечебных целях. Учитывая этот

факт, можно предложить их использование и в деятельности правоохранительных органов как один из способов предупреждения правонарушений, который представляет собой не физическое, а мягкое психологическое воздействие на источник правонарушения.

Рассматривая средства визуального воздействия выделяют неосознаваемые воздействия (вставки расщепленных кадров по всему видеоряду), цветовоздействие и ритмовоздействие, когда чередуются цвета определенной частотой, эти цвета вызывают в подсознании людей определенные настроения, например, возбуждение, активность (красный, оранжевый, желтый), спокойствие (голубой, синий), подавленность (фиолетовый).

Аудиальное воздействие может быть представлено теми аудиофайлами которые своим ритмом, громкостью воздействуют на человека, а также фразами суггестивного воздействия на неслышимом человеческим ухом диапазоне частот, но воспринимаемым подсознанием, которые накладываются на основное аудио. Если запустить в толпе фоном ритмичную агрессивную музыку, то, соответственно, в сознании людей возникнут такие же настроения.

При проведении массовых мероприятий, спортивных, культурных и иных видов, организаторы не осознают того факта, что при использовании определенных мультимедийных средств сопровождения таких мероприятий несут деструктивный характер людям. Так, мультимедийное сопровождение, которое содержит в себе музыкальное и визуальное сопровождение, агрессивно воздействующее на участников массовых мероприятий, может привести к негативным последствиям (например, массовым беспорядкам).

Учитывая такое положение дел, предлагается создать комиссию по проверке организации массовых мероприятий, которая будет давать заключения по тем или иным техническим оборудованьям, заявленным в регламенте мероприятия, а также используемых средств мультимедиа, осуществлять передачу этих данных в правоохранительные органы для последующего от ОВД разрешения о проведении мероприятия.

Список литературы

1. Словарь терминов МЧС. – 2010.
2. Аветисян, К. Р. Правовые основы применения аудиальных информационно-психологических воздействий как специальных средств органов внутренних дел // Студенческий вестник. Ростовский филиал Российской таможенной академии. – 2010. – № 1.
3. СанПиН 4396-87 «Санитарные нормы допустимой громкости звучания звуковоспроизводящих и звукоусилительных устройств в закрытых помещениях и на открытых площадках» (утвержден 07.07.1987 г.).
4. Прокофьев, В. Ф. Объект атаки – подсознание человека // Сборник научных статей посвящен двадцатилетию со дня создания ЦВСИ Генерального штаба Вооруженных Сил Российской Федерации / под ред. Ю.Н. Балуевского. – М., 2004.
5. ИМБИТ «Профессиональный психологический инструментарий «Саната» комплект аудиовизуальных психокоррекционных программ» // А. И. Кучинов.
6. Беспалько, И. Г. О соотношении между цветовыми порогами, соматотипом и эмоциональным состоянием // Математические методы в психиатрии и неврологии. – Л., 1972.
7. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» // СПС «КонсультантПлюс». URL: <https://www.consultant.ru>.

*Эльканов Виктор Витальевич¹,
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

*Галиев Денис Вадимович²,
преподаватель кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ИСПОЛЬЗУЕМОЕ В СТЕГАНОГРАФИИ В ОПЕРАЦИОННОЙ СИСТЕМЕ LINUX

Проблема сокрытия данных волнует человечество с древних времен. Для защиты информации обычно используют шифры. Надежность их может быть разной, но к тому моменту, когда врагу все же удастся его взломать, информация будет уже старой.

В эпоху цифровых технологий положение несколько изменилось: вычислительные возможности компьютеров непрерывно увеличиваются, а кроме того, появилось огромное количество каналов связи, по которым можно передавать информацию. При этом красть данные стало значительно легче. Стеганография (от греч. «тайнопись») – это наука о скрытой передаче информации путем сохранения в тайне самого факта передачи. В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает сам факт его существования. Хотя обычно эти две технологии используют совместно.

Современная стеганография – цифровая и компьютерная. Последнюю можно разделить на три больших направления. Первое – это собственно тайнопись, или методы сокрытия одних файлов (которые принято называть сообщением) внутри других («контейнера»). После заполнения сообщением контейнер внешне меняется незаметно и полностью сохраняет свою функциональность.

Стеганографию используют для всевозможных целей. Нередко ее используют не для воровства, а для борьбы с похитителями.

Одним из методов может быть добавление к сообщению скрытых или стеганографических меток (stegomarks). Это незаметные без специальной обработки метки, идентичные для всех файлов одного человека или

¹ © Эльканов В. В., 2019.

² © Галиев Д. В., 2019.

устройства. Например, такие стегометки записываются в цифровые фотографии для того, чтобы можно было доказать их авторство. Крэкеры иногда оставляют стегометки в лицензионных ключах. Они защищены на уровне алгоритма генерации, а потому сохраняются при попытке изменить интерфейс кейгена и выдать его за свой.

Второй метод – это внедрение в сообщение цифровых отпечатков (digital fingerprints). В отличие от стегометок, эти скрытые знаки уникальны для каждого сообщения. Они служат в основном для защиты интересов правообладателей, позволяя отследить распространение контента. К примеру, многие интернет-магазины внедряют цифровые отпечатки в продаваемые книги и музыкальные композиции. В них кодируется информация о дате продажи и аккаунте купившего (имя, IP-адрес). Если купленные файлы позже появятся среди торрентов или на файлообменниках, то правообладатели смогут установить распространителя нелегального контента.

Суть методов типа LSB (Least Significant Bit, наименьший значащий бит) и аналогичных заключается в замене последних значащих битов в контейнере (изображения, аудио или видеозаписи) на биты скрываемого сообщения. Возьмем в качестве примера графический файл. Наглядно это выглядит следующим образом: мы меняем младшие биты в коде цвета пикселя на картинке. Если считать, что код цвета имеет 32-битное значение, то замена 0 на 1 или наоборот, не приведет к сколько-нибудь существенному искажению картинки, ощутимому для органов восприятия человека, между тем в этих битах для большой картинки можно что-то спрятать.

Рассмотрим небольшой пример. Допустим, имеется 8-битное изображение в градациях серого. 00h (00000000B) обозначает черный цвет, FFh (11111111B) – белый. Всего имеется 256 градаций. Также предположим, что сообщение состоит из 1 байта, например, 01101011B. При использовании 2 младших бит в описаниях пикселей нам потребуется 4 пикселя. Допустим, они черного цвета. Тогда пиксели, содержащие скрытое сообщение, будут выглядеть следующим образом: 00000001 00000010 00000010 00000011. Тогда цвет пикселей изменится: первого – на $1/255$, второго и третьего – на $2/255$ и четвертого – на $3/255$. Такие градации, мало того, что незаметны для человека, могут вообще не отобразиться при использовании низкокачественных устройств вывода.

Стоит отметить, что методы LSB являются неустойчивыми к разного рода «шуму». Например, в случае если на передаваемый контент накладываются какие-либо «мусорные» биты, это искажает как исходный контент, так и (что для нас особенно важно) скрытое сообщение. Иногда оно

даже становится нечитаемым. Аналогичная методика используется и для других форматов.

Еще один метод заключается в так называемом впаивании скрытой информации. В данном случае происходит наложение скрываемого изображения (звука, иногда текста) поверх оригинала. Простейший пример: надпись белым цветом на белом же фоне в PDF-документе. Злоумышленники обычно не используют данный метод по причине относительной простоты обнаружения автоматическими методами. Однако данный метод зачастую применяется при создании «водяных знаков» для защиты авторства контента. В этом случае данные знаки, как правило, не скрываются.

И третий метод – использование особенностей форматов файлов. К примеру, это может быть запись информации в метаданные, используемые данным форматом файла, или в различные другие, не используемые зарезервированные поля. Например, это может быть документ Microsoft Word, внутри которого будет спрятана информация, никак не отображаемая при открытии данного документа.

Стеганография на практике может определяться утилитами *steghide*, *outguess* и *steg*.

Steghide предназначена для работы с графическими и аудио файлами. Поддерживаются форматы *.jpeg*, *.bmp*, *.wav*, и *au*. Так же *steghide* поддерживает сжатие и шифрование внедряемых данных. Несмотря на то, что последний релиз *steghide* состоялся в далеком 2003 г., можно без труда найти эту утилиту почти в любом дистрибутиве Linux.

Outguess. Данный набор утилит поддерживает работу только с форматами PNM и JPEG. Последний релиз состоялся в 2004 г., но пакет *outguess* так же присутствует почти во всех современных дистрибутивах.

Steg данная утилита значительно моложе двух предыдущих и менее широко представлена в стандартных репозиториях, зато имеет графический интерфейс. *Steg* – это кроссплатформенная утилита для Linux, Windows и Mac OS. Графический интерфейс реализован на QT. Поддерживается работа с изображениями в форматах JPEG, TIFF, PNG и BMP.

Мамедова Фатима Фармановна¹,
заместитель декана факультета права
Научно-исследовательского университета
Высшей школы экономики

Мигачева Елена Дмитриевна²,
заместитель начальника кафедры оперативно-технических
мероприятий органов внутренних дел Всероссийского
института повышения квалификации МВД России

Колокольчикова Ольга Николаевна³,
старший преподаватель кафедры оперативно-технических
мероприятий органов внутренних дел Всероссийского
института повышения квалификации МВД России

Алескеров Вагиф Исмаилович⁴,
профессор кафедры оперативно-технических
мероприятий органов внутренних дел Всероссийского
института повышения квалификации МВД России

О ПРЕСТУПЛЕНИЯХ, СОВЕРШАЕМЫХ В СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

В настоящее время в мире происходят экономические преобразования динамического характера, которые влияют не только на политический сегмент, но и на быстро развивающуюся сферу информационных-телекоммуникационных и компьютерных технологий. Информационные потоки, вливающиеся во все сферы жизнедеятельности современного общества, придают возможности бурного развития социального обеспечения, финансов, экономики, медицины, образования, всевозможных научных исследований на всех направлениях. Несмотря на эту положительную сторону, как всякое новое веяние, преобразования, кроме масштабных революционных изменений, неизбежно влекут за собой и некоторые нежелательные последствия. К таким последствиям мы можем отнести преступления, совершаемые в сфере телекоммуникаций и компьютерной информации. Одним из разновидностей таких преступлений являются преступления, совершаемые в системе дистанционного банковского обслуживания, статистика которых из года в год

¹ © Мамедова Ф. Ф., 2019.

² © Мигачева Е. Д., 2019.

³ © Колокольчикова О. Н., 2019.

⁴ © Алескеров В. И., 2019.

показывает геометрическую прогрессию, а ущерб от данного вида преступлений, к нашему сожалению, велик.

За последние годы проводится целый ряд глубоких исследований преступлений данной направленности, на основе чего подготовлены доклады, отчеты, статьи и рекомендации, но во всех перечисленных документах прослеживается четкое высказывание, что преступления, совершаемые в системе дистанционного банковского обслуживания, являются преступлениями, относящимися к разновидностям киберпреступлений. А если выражаться еще точнее, то данный вид преступлений можно отнести и к компьютерно-экономическим преступлениям. Повсеместное использование технологических возможностей информационно-телекоммуникационных сетей и компьютерной информации в глобальной сети Интернет порождает благоприятные условия, способствующие осуществлению преступного замысла среди лиц, совершающих преступления в системе дистанционного банковского обслуживания. Данное обстоятельство не может не вызывать тревогу у сотрудников оперативных подразделений, призванных вести активную и целенаправленную работу по противодействию данному виду преступлений, так как в большинстве случаев лица, совершающие этот вид преступлений, остаются без соответствующего наказания.

Рост киберпреступности является следствием продолжающейся глобализации внедрения информационно-телекоммуникационных технологий и появления международных компьютерных сетей. С масштабным ростом информационных систем в различных областях деятельности возрастает и их применение в целях совершения преступлений. В этой связи можно утверждать, что электронная революция дала толчок преступности, использующей возможности информационно-телекоммуникационных сетей для извлечения прибыли. Появились новые формы и виды преступлений, представляющие угрозу для граждан, предприятий, организаций, государств.

Алексей Лунин, автор статьи «Как не стать жертвой мошенников?», не зря упоминает о том, что воры-психологи все чаще крадут деньги с банковских карт пенсионеров. Так, по оценкам аналитиков, в 2017 г. мошенники с помощью социальной инженерии похитили с банковских карт жителей нашей страны почти 750 млн руб., причем большая часть пострадавших – пенсионеры. Он же в своей статье «Реально ли победить киберпреступность?» приводит следующую информацию: «Сумму ущерба мировой экономике от действий киберпреступников в 2017 г. аналитики экономического форума в Давосе оценили в 1 трлн

долл. США»¹. В России потери тоже ощутимы. «Статистика говорит о 150–200 млн руб. в 2017 г. но, видимо, это только официально зафиксированные и как-то расследованные инциденты. Оценка аналитиков, касающаяся всей страны приравнивается к 550–600 млрд руб. Что касается прогноза возможных потерь на 2018 г., то они могут составить 1 трлн руб.», – приводит красноречивые цифры заместитель председателя правления Сбербанка России С. Кузнецов.

В начале июля Сбербанк провел в Москве Международный конгресс по кибербезопасности. Это один из первых шагов России к созданию всемирной системы обмена информацией о киберрисках и борьбы с киберпреступностью. Разработчики антивирусных программ, руководители банков, представители Интерпола и правоохранительных органов обменивались опытом и обсуждали общие правила противодействия киберугрозам. Как организатор конгресса Сбербанк решил открыто показать свои методы работы. Защищая своих клиентов, он действует по четырем направлениям:

- безопасность центральных банковских систем, где хранятся все сведения о счетах;
- разработка новых финансовых продуктов, в программный код которых уже на старте проекта зашиваются базовые принципы безопасности;
- анализ нестандартных действий и ошибок клиентов. Для этого используется специальная система антифрода с искусственным интеллектом, которая способна выявить и не допустить до 97 % мошеннических операций;
- тщательное расследование каждой кибератаки, нацеленное на выявление мошенников².

В целях консолидации усилий в противодействии электронной преступности Советом Европы была разработана Конвенция о киберпреступности, ставшая первым международно-правовым документом в этой области. На заседании в Будапеште 23 ноября 2001 г. министрами иностранных дел Европейского Сообщества принята Европейская Конвенция по борьбе с компьютерной преступностью, а сегодня к этой конвенции присоединилось более 40 стран³.

Мошенничество является одним из самых распространенных криминальных проявлений на территории Российской Федерации. Прежде

¹ Аргументы и факты. – 2018. – № 26. URL : <https://www/aif.ru>).

² Там же.

³ Тарасов А. М. Электронное правительство и информационная безопасность : учебное пособие. СПб. : ГАЛАРТ, 2011. – 648 с.

всего, это связано с тем, что российское законодательство придает особое значение проблемам усиления ответственности за различные виды мошеннических действий. В период с 2003 г. по 2011 г. в ст. 159 УК РФ внесены значительные изменения и дополнения, усиливающие уголовную ответственность за данный вид хищения. На основании Федерального закона от 29 ноября 2012 г. № 207-ФЗ в Уголовный кодекс введены шесть новых видов мошеннических действий, в том числе:

- ст. 159.1 – мошенничество в сфере кредитования;
- ст. 159.2 – мошенничество при получении выплат;
- ст. 159.3 – мошенничество с использованием платежных карт;
- ст. 159.4 – мошенничество в сфере предпринимательской деятельности;
- ст. 159.5 – мошенничество в сфере страхования;
- ст. 159.6 – мошенничество в сфере компьютерной информации.

В соответствии со ст. 159 УК РФ, мошенничеством признается хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

При мошенничестве обман, или злоупотребление доверием, является способом завладения чужим имуществом. Особенностью такого вида хищения, как мошенничество, является то, что в результате обмана потерпевший сам передает преступнику имущество, при этом добровольность передачи имущества является мнимой, поскольку обусловлена совершенным в отношении потерпевшего обманом, введением его в заблуждение. Любая форма обмана и злоупотребления доверием, в целом, сводится к тому, что виновный при осуществлении своих действий создает у потерпевшего уверенность в правомерности или выгоды для него передачи имущества или права на него. С развитием современного общества, появлением прогрессивных технических возможностей, научными открытиями и изобретениями, к сожалению, все чаще выявляются новые виды мошеннических действий, которые в последнее время активно совершенствуются.

Мошенничество – это общественно опасное деяние, которое причиняет не только имущественный вред гражданам, но и подрывает доверие между людьми, разрушает нравственные устои общества в целом. Как показывает практика, за последнее время нашел активное распространение такой вид преступления, как мошенничество с использованием средств сотовой телефонной связи и дистанционного банковского обслуживания. С 2008 г. данные виды мошенничества начали активно совершенствоваться и получили достаточно широкое распространение на территории Российской Федерации. Среди большого многообразия

видов мошенничества данные виды получили название «телефонное» мошенничество и мошенничество в сфере дистанционного банковского обслуживания, поразив практически все регионы России.

«Телефонное» мошенничество можно охарактеризовать как мошенничество, при котором деньги похищаются у потерпевшего под различными предложениями: путем обмана или введения в заблуждение последнего, с помощью средств сотовой телефонной связи. По данным ФКУ «ГИАЦ МВД России», в структуре преступности за период 2008–2017 гг. мошенничество занимает примерно 6–7 %, что составляет шестую часть от всего объема хищений. Особо следует отметить, что в 2017 г., несмотря на предпринимаемые меры противодействия, произошел рост рассматриваемых видов преступлений на 9,8 %. В настоящее время количество рассматриваемых видов преступлений продолжает расти.

Список литературы

1. Захаров, Д. Н., Щерба, В. В. Особенности расследования киберпреступлений // Научно-практический журнал «Вопросы кибербезопасности». – 2017. – № 2. – Т. 2.

2. Алескеров, В. И., Новокшанов, О. Н. Понятие и уголовно-правовая характеристика некоторых видов киберпреступности // Вестник Всероссийского института повышения квалификации сотрудников МВД России. – 2012. – № 1. – С. 52–59

3. Тарасов, А. М. Электронное правительство и информационная безопасность: учебное пособие. – СПб. : ГАЛАРТ. – 2011. – 648 с.

*Денисов Николай Леонидович¹,
доцент кафедры уголовного права
Московского университета
МВД России имени В.Я. Кикотя*

ВОПРОСЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, СОПРЯЖЕННЫХ С ТЕРРОРИЗМОМ И ЭКСТРЕМИЗМОМ

В рамках противодействия современному терроризму и экстремизму уголовно-правовыми следует рассматривать различные формы и особенно сферы проявления преступлений соответствующей направленности. В частности, в силу различных причин такое преступное поведение проникает и в сферу компьютерной информации. Среди таких причин особо можно выделить более широкую аудиторию, в отношении которой можно осуществлять распространение соответствующей информации. Также достаточно активное использование данной сферы для реализации различных государственных функций государственными органами, различными организациями и гражданами, в том числе в рамках обеспечения безопасности. Все это повышает общественную опасность преступлений, террористической и экстремистской направленности, совершенных в вышеуказанной сфере.

При этом бывают некоторые коллизии применения уголовно-правовых норм в отношении некоторых преступлений, совершенных в сфере компьютерной информации, но при этом сопряженных с терроризмом и экстремизмом. В качестве такого примера можно рассмотреть ч. 2 ст. 272 УК РФ, которая предполагает, что лицо осуществило неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, совершенное из корыстной заинтересованности и ч. 2 ст. 273 УК РФ, предусматривающую в качестве преступления создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, совершенные из корыстной заинтересованности.

Уже давно не секрет, что террористические и экстремистские организации помимо денежных средств своих спонсоров, пожертвований

¹ © Денисов Н. Л., 2019.

своих единомышленников и других финансовых поступлений активно осуществляют противоправную деятельность по сбору средств через интернет, в том числе и путем совершения действий, которые указаны в указанных нормах УК РФ. Если не рассматривать деятельность лица, совершающих данные деяния как часть функционирования преступной организованной группы или преступного сообщества, то возникает вопрос о разграничении применения этих норм и, например, ч. 3 ст. 205.1 УК РФ, предусматривающей в качестве преступления пособничество в совершении хотя бы одного из преступлений, предусмотренных ст. 205, ч. 3 ст. 206, ч. 1 ст. 208 УК РФ путем предоставления средств, а также ч. 2 ст. 282.1 УК РФ, предполагающей преступным участие в экстремистском сообществе, в том числе путем финансирования.

По указанным преступлениям существуют документы судебного толкования в виде постановления Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» и постановления Пленума Верховного Суда Российской Федерации от 9 февраля 2012 г. № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности». Однако даже в их последних редакциях ничего не указывается в качестве решения указанной коллизии. В то же время таких пояснений в отношении ст.ст. 272 и 273 УК РФ до сих пор отсутствуют.

В уголовном праве бывают схожие случаи в рамках конкуренции уголовно-правовых норм. В частности, когда речь идет о конкуренции более общей и более специальной статье. При такой конкуренции квалификация осуществляется по специальной норме, если лицо совершившее деяние является субъектом ответственности по данной норме.

В рассматриваемой нами ситуации нельзя говорить об указанной конкуренции в силу того, что ч. 2 ст.ст. 272 и 273 УК РФ соотносятся с ч. 3 ст. 205.1 УК РФ и ч. 2 ст. 282.1 УК РФ как специфический способ совершения и само преступление в целом.

Если взять существующую практику в аналогичных случаях, то можно увидеть, что, например, в рамках квалификации мошенничества, совершенного путем использования подделанного этим лицом официального документа, предоставляющего права или освобождающего от обязанностей, помимо самой ст. 159 УК РФ требует дополнительной квалификации по ч. 1 ст. 327 УК РФ.

*Ромашкина Наталья Юрьевна¹,
курсант факультет подготовки сотрудников
для подразделений экономической безопасности
и противодействия коррупции
Московского университета
МВД России имени В.Я. Кикотя*

*Денисов Николай Леонидович²,
доцент кафедры уголовного права
Московского университета
МВД России имени В.Я. Кикотя*

ПРОТИВОДЕЙСТВИЕ УГОЛОВНО-ПРАВОВЫМИ СРЕДСТВАМИ ПРОПАГАНДЕ ТЕРРОРИЗМА И ЭКСТРЕМИЗМА В ЭЛЕКТРОННЫХ СМИ

Уже на протяжении длительного времени в России проводится последовательная и целенаправленная политика по противодействию терроризму и экстремизму, которые уже многие годы являются одними из основных глобальных угроз современного мира. В ходе осуществления данного политического направления Российская Федерация стала участницей Конвенции Совета Европы «О предупреждении терроризма» 2005 г. Согласно ч. 2 ст. 5 данной Конвенции на Россию возлагаются обязательства по принятию мер, в которых может возникнуть необходимость при признании «публичного подстрекательства к совершению террористического преступления» в качестве уголовно-наказуемого деяния на основе национального законодательства³.

В рамках осуществления требований данной нормы международного права в действующем Уголовном кодексе Российской Федерации законодатель предусмотрел ответственность за публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганду терроризма (ст. 205.2), а также за публичные призывы к осуществлению экстремистской деятельности (ст. 280)⁴.

¹ © Ромашкина Н. Ю., 2019.

² © Денисов Н. Л., 2019.

³ Конвенции Совета Европы «О предупреждении терроризма» от 16 мая 2005 г. (CETS N 196) // Собрание законодательства Российской Федерации. – 2009 – № 20, ст. 2393.

⁴ Уголовный кодекс Российской Федерации (принят Государственной Думой Федерального Собрания Российской Федерации 13 июня 1996 г.). М. : Проспект, 2002. 160 с.

Данные нормы Уголовного кодекса предусматривают также и квалифицированные составы, содержащие такой признак объективной стороны как особый способ совершения преступления – использование СМИ, информационно-телекоммуникационных либо электронных сетей, включая сеть «Интернет». Эти квалифицированные составы появились не случайно.

Это связано с тем, что сегодня происходит постоянный рост числа интернет-пользователей и быстрое развитие социальных сетей и различных порталов, что принесло некоторое изменение в деятельность правоохранительных органов по борьбе с терроризмом и экстремизмом и в законодательство соответственно. Теперь в рамках этой деятельности все больше внимания органами ФСБ России, МВД России и иных правоохранительных служб уделяется мониторингу глобальной сети Интернет и ее сайтов.

При выявлении фактов размещения запрещенных к обороту материалов, призывов к национальной, религиозной вражде, осуществлению террористической деятельности принимаются меры к блокированию запрещенного контента, а виновные лица привлекаются к уголовной ответственности по ч. 2 упомянутых статей.

О необходимости усиления работы в этом направлении свидетельствует огромное количество совершенных подобным способом деяний: около 80 % выявленных преступлений экстремистской и террористической направленности сегодня совершаются с использованием сети интернет¹.

Большое внимание на протяжении нескольких последних месяцев обращено на случаи привлечения к уголовной ответственности за, так называемые, репосты и лайки публикаций, пропагандирующих терроризм и экстремизм.

На начало 2016 г. более 54 человек были привлечены к уголовной ответственности за «разжигание ненависти» в России, большинство из них – за публикацию запрещенного контекста, но есть и те, кто получил судимость за то, что поделились или оценили эту информацию. Эта цифра почти в пять раз превышает аналогичный показатель пять лет тому назад, согласно данным правозащитной группы СОБА. Количество приговоров за разжигание ненависти выросло с 92 в 2010 г. до 233 в 2015 г.²

¹ URL : <http://genprok-urfo.ru/rasprostranenie-i-propagandu-ekstremizma-v>.

² URL : <https://inosmi.ru/social/20160603/236751298.html>.

Почему же сегодня такое большое внимание направлено на, казалось бы, безобидные «лайки и репосты» в популярных социальных сетях?

По сообщению первого заместителя руководителя аппарата Национального антитеррористического комитета генерал-лейтенанта Ильина более 7000 сайтов, содержащих информацию террористической и экстремистской направленности, 500 из которых – русскоязычные, действуют сегодня в сети «Интернет», в сегменте, в котором не распространяется юрисдикция Российской Федерации¹.

Если еще недавно в списках средств массовой информации, содержащих пропаганду экстремизма и терроризма, были в основном печатные издания, то сегодня это, главным образом, материалы, которые размещены в «Интернете» и на его социальных сетях. Главная проблема этой тенденции заключается в том, что авторы подобных материалов анонимны и, как правило, не просто оперируют экстремистской риторикой националистической или религиозной направленности, а напрямую пропагандируют идеи запрещенных организаций. Важно, что экстремисты и террористы не ограничивают себя обычными текстовыми публикациями. Благодаря развитой системе информационно-телекоммуникационных технологий пропагандисты все чаще прибегают к использованию документальных видеоматериалов, аудиосообщений и, что самое страшное, личного общения через визуальные средства общения сети Интернет – Skype, Viber, WhatsApp, LINE.

Что же касается антитеррористической деятельности нашего государства, то на сегодняшний день в России существует чуть более 50 официальных интернет-ресурсов антитеррористической направленности². Их оказывается слишком мало для эффективного противодействия пропагандистским действиям сторонников запрещенных организаций.

Это приводит к необходимости бороться с пропагандой иными способами, в том числе уголовно-правовыми, что включает ужесточение наказания за пропаганду терроризма и экстремизма в электронных ресурсах. Сегодня это является одним из необходимых направлений деятельности уголовно-правовой политики, поскольку влияние электронных средств массовой информации на пользователей возрастает с каждым днем.

¹ Более 500 экстремистских сайтов на русском языке действуют вне рунета // РИА Новости. URL : <http://news.mail.ru/incident/10633770>.

² Официальный сайт ФГБОУВО МГТУ «Станкин» // URL : <http://www.stan-kin.ru/countering-the-ideology-of-terrorism/official-internet-resources-on-counter-terrorism.php>.2017.

Сборник научных трудов Всероссийской конференции
28 февраля 2019 г.

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Научное электронное издание

В авторской редакции
Компьютерная верстка *Абилова Ф. А.*
14,82 усл. печ. л

Систем. требования: CPU 1,5 Гц ; RAM 90,4 МБ ; Windows XP SP3;
1 Гб свободного места на жестком диске.

Подписано к изданию 2019 г.

ISBN 978-5-9694-0811-1



Московский университет МВД России имени В.Я. Кикотя
117437, г. Москва, ул. Академика Волгина, д. 12