МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

КАЗАНСКИЙ (ПРИВОЛЖСКИЙ) ФЕДЕРАЛЬНЫЙ
УНИВЕРСИТЕТ

ИНСТИТУТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Кафедра системного анализа и информационных технологий

Долгов Дмитрий Александрович

ВВЕДЕНИЕ В КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ЧАСТЬ 1

Методическое пособие

КАЗАНЬ, 2020

УДК 004.056.55
ББК 22.1, 32.811.4

Рецензенты:
доктор физико-математических наук, профессор кафедры системного анализа и информационных технологий ИВМиИТ КФУ
Ш.Т. Ишмухаметов;
кандидат физико-математических наук, доцент кафедры алгебры и математической логики КФУ **М.М. Ямалеев**

Долгов Д.А.

Введение в комплексное обеспечение информационной безопасности. Часть 1: Методическое пособие / Д.А. Долгов. – Казань: КФУ, 2020. – 31 с.

Методическое пособие предназначено для проведения практических занятий по курсу «Комплексное обеспечение информационной безопасности» для студентов, обучающихся по направлениюю «Информационная безопасность». В данном методическом пособии подробно рассматриваются различные методы защиты информации: физические, технические и правовые. Произведен скрупулезные анализ законодательства Российский Федерации в области информационной безопасности. Также стоит отметить обзор существующих технических решений по обеспечению защиты информации. В конце пособия приводится один из основных ассиметричных шифров – RSA.

Содержание

1. Введение

Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры. В данном пособии дается обзор основных физических, правовых и технических методов защиты информации. Особое внимание уделяется текущему законодатеству в области информационной безопасности.

Невозможно представить информационную безопасность без криптографии. Криптография - это наука, которая занимается построением безопасных шифров, т.е. алгоритмов, которые преобразуют электронные документы в некоторый нечитаемый набор символов, из которого можно восстановить исходный документ только зная секретное слово. Известны примеры древних шифров римлян, греков и других народов. Современная криптография началась относительно недавно, в 70-е годы XX века с изобретения протокола Диффи-Хелмана выработки общего ключа и алгоритма ассиметричной криптографии RSA, который приведен в конце данного пособия.

Подробное изложение материала можно найти в [9, 1, 2].

2. Введение в информационную безопасность

Понятие информации дано в федеральном законе от 27 июля 2006 года № 149-ФЗ (ред. от 29.07.2017 года) «Об информации, информационных технологиях и о защите информации», статья 2: Информация – это сведения (сообщения, данные) независимо от формы их представления».

Определение 1. *Информационная безопасность – это состояние информационной системы, в котором угрозы нарушения конфиденциальности, целостности и доступности информации сведены к минимуму.*

Основная цель информационной безопасности – сведение к минимуму этих угроз, т.е. угроз конфиденциальности, целостности, доступности информации.

Конфиденциальность – обеспечение доступа к информации зарегистрированным (легальным) пользователям, которые имеют разрешение владельца на доступ к информационному ресурсу, запрет доступа несанкционированным пользователям.

Целостность – сохранность данных в том виде, в каком они были созданы.

Доступность – обеспечение неограниченного доступа к информации или к её частям всем легальным пользователям.

Под «*угрозой*» понимается потенциальная возможность тем или иным способом нарушить информационную безопасность. Попытка реализации угрозы называется «*атакой*», а тот, кто реализует данную попытку, называется «*злоумышленником*». Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем. Угрозы могут быть нацелены на данные, программы, аппаратуру и инфраструктуру.

В зависимости от типа информационного ресурса или условий его функционирования на первый план может выступать та или иная составляющая информационной безопасности.

Примеры.

1) Нарушения конфиденциальности:

   - получение злоумышленником пароля для доступа к информации на компьютере жертвы.
   - получение злоумышленником конфиденциальных данных о коммерческих разработках конкретной компании.

- появление в открытом виде информации о личной жизни, состоянии здоровья людей.

2) Нарушения целостности:

   - попытка злоумышленника изменить номер аккаунта в банковской транзакции, а также изменение суммы перевода;
   - случайное изменение информации при передаче или при неисправной работе жёсткого диска;

3) Нарушения доступности:

   - отказ сервера ввиду ddos атаки на него;
   - отказ системы ввиду ошибок при её (пере)конфигурировании.
   - отказ системы из-за отказов программного и аппаратного обеспечения;
   - отказ системы из-за вредоносного программного обеспечения.

Определение 2. *Защита информации — это деятельность по предотвращению утечки, хищения, утраты, модификации (подделки), несанкционированных и непреднамеренных воздействий на защищаемую информацию.*

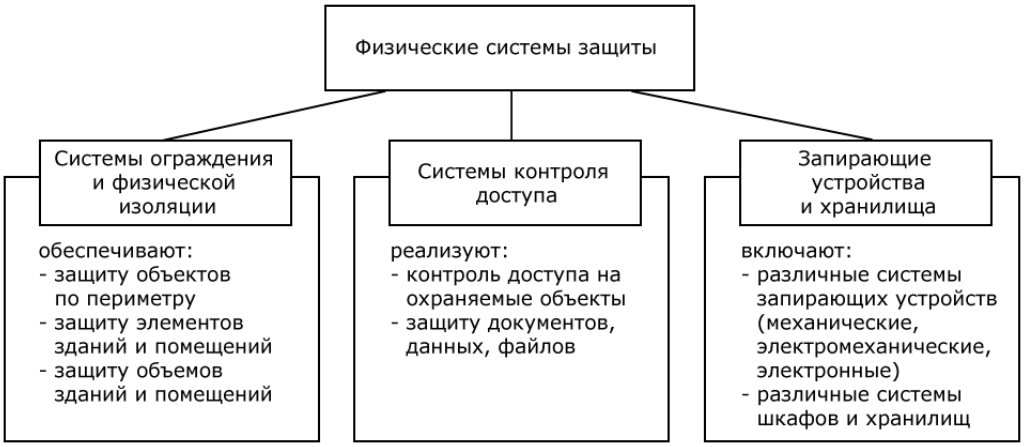
Защита информации обеспечивается различными методами и средствами. В целом, их можно разбить на три большие группы: физические, организационно-правовые и технические средства защиты. Только вместе в совокупности средств можно добиться создания защищенной инфрастуктуры и обеспечить защиту информации.

В конце представим немного фактов о ситуации в сфере информационной безопасности на начало 2020 года:

- хакерские атаки случаются каждые 39 секунд.
- DDoS-атаки в среднем увеличились в размерах более чем на 500%.
- атаки с использованием уязвимостей сайтов, в том числе с применением JavaScript-снифферов, продолжатся и в дальнейшем ввиду их высокой эффективности. Известен пример заражения JS-сниффером сайта компании British Airways.
- актуальные векторы мобильных угроз связаны с новыми способами получения root и jailbreak, техниками обхода биометрии и пиннингом.

3. Физические методы защиты информации

Физические средства защиты - это разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников. Они образуют внешний уровень защиты.



К физическим средствам относят механические, электронные, электромеханические, радио- и радиотехнические, электронно-оптические и другие устройства для воспрещения несанкционированного доступа, проноса (выноса) средств и материалов и других возможных видов преступных действий.

Данные средства применяют для решения следующих задач:

- охрана территории предприятия и наблюдение за ней;
- охрана зданий, внутренних помещений и контроль за ними;
- охрана оборудования, продукции, финансов и информации;
- осуществление контролируемого доступа в здания и помещение.

Все физические средства защиты объектов можно разделить на три категории:

- средства предупреждения,
- средства обнаружения,
- системы ликвидации угроз.

В общем плане по физической природе и функциональному назначению все средства этой категории можно разделить на следующие группы:

- охранные и охранно-пожарные системы;
- охранное телевидение;
- охранное освещение;
- средства физической защиты.

К средствам физической защиты относятся:

- ограждение и физическая изоляция,
- запирающие устройства,
- системы контроля доступа.

К системам контроля доступа относятся:

- системы, использующие различные карты и карточки, на которых помещается кодированная или открытая информация о владельце, также используются токены (компактное устройство, которое находится в собственности пользователя);
- системы опознавания по отпечаткам пальцев;
- системы опознавания по голосу;
- системы опознавания по почерку;
- система опознавания по геометрии рук.

Все устройства идентификации могут работать как отдельно, так и в комплексе.

У биометрической идентификации есть особенности, которые отличают её от привычной пары логин/пароль или «безопасной» двухфакторной:

- Биометрические данные публичны. Можно найти фотографии, видео- и аудиозаписи практически любого жителя планеты Земля и использовать их для идентификации.
- Невозможно заменить лицо, голос, отпечатки пальцев или сетчатку с той же лёгкостью, как пароль, номер телефона или токен для двухфакторной аутентификации.

- Биометрическая идентификация подтверждает личность с вероятностью, близкой, но не равной 100%. Другими словами, система допускает, что человек может в какой-то степени отличаться от своей биометрической модели, сохранённой в базе.

Существуют много способов подделки биометрии. Исследователи из X-Lab за 20 минут разблокировали смартфон с помощью отпечатка пальца его хозяина, взятого со стакана. Воссоздать отпечаток пальца позволило приложение Tencent Security, способное реконструировать отпечаток даже по его фрагментам, снятым с нескольких предметов, а также гравировальный аппарат стоимостью 140 долл. США [7].

При этом точность идентификации в системах, использующих биометрию, сильно зависит от качества биометрических данных, сохранённых в системе. Чтобы обеспечить достаточное для надёжного распознавания качество и не совершить ошибку, необходимо иметь высокоточное оборудование.

Например, если вам для идентификации нужны голос и фото, но вы используете дешёвые микрофоны для записи образца голоса, бюджетные камеры для создания фото и биометрической модели, то при таком сценарии значительно возрастает количество ложных узнаваний. Повышается вероятность того, что система примет одного человека за другого, с близким по тональности голосом или сходной внешностью. Таким образом, некачественные биометрические данные создают больше возможностей для обмана системы, которыми могут воспользоваться злоумышленники.

Также необходимо принять во внимание ситуацию с deepfakes и другими способами обмана биометрических систем. Тем не менее использование сочетания традиционных способов идентификации пользователя (пароли, двухфакторная аутентификация и usb-токены) с биометрическими могут принести пользу.

Далее покажем степень защищенности различных личных данных при наличии физического доступа к смартфону или компьютеру.

Пример 1. В октябре 2018 года студент первого курса колледжа Уэйк Текникал Натаниэль Сачи обнаружил, что мессенджер Telegram сохраняет сообщения и медиафайлы на локальном диске компьютера в открытом виде. Он получил доступ к собственной переписке, включая текст и картинки. Данные были не зашифрованы. И доступ к ним можно получить даже в том случае, если пользователь установил на приложение пароль. Можно было найти телефоны собеседников. Информация из закрытых чатов тоже хранилась в открытом виде.

Пример 2. WhatsApp тоже хранит данные на диске компьютера в незашифрованном виде. Соответственно, если у злоумышленника есть доступ к устройству пользователя, то все данные тоже открыты.

Пример 3. Данные с незашифрованного телефона можно извлечь почти в ста процентах случаев. «Почти» здесь относится скорее к случаям, когда телефон попытались физически повредить или уничтожить непосредственно перед снятием данных. Во многих устройствах Android и Windows Phone есть сервисный режим, позволяющий слить все данные из памяти аппарата через обычный USB-кабель. Это касается большинства устройств на платформе Qualcomm (режим HS-USB, работающий даже тогда, когда загрузчик заблокирован), на китайских смартфонах с процессорами MediaTek (MTK), Spreadtrum и Allwinner (если разблокирован загрузчик). Но даже если в телефоне и нет сервисного «черного хода», данные из устройства все равно можно получить, разобрав аппарат и подключившись к тестовому порту JTAG. В самых запущенных случаях из устройства извлекается чип eMMC, который вставляется в простейший и очень дешевый адаптер и работает по тому же протоколу, что и самая обычная SD-карта. Если данные не были зашифрованы, из телефона легко извлекается вообще все вплоть до маркеров аутентификации, предоставляющих доступ к твоим облачным хранилищам.

Если у кого-то есть личный доступ к смартфону с важной информацией, то при желании взломать его можно, что бы ни говорили производители.

Понятно, что всё сказанное касается не только смартфонов, но и компьютеров с ноутбуками на различных ОС. Если не прибегать к продвинутым защитным мерам, а довольствоваться обычными методами вроде пароля и логина, то данные будут оставаться в опасности. Опытный взломщик при наличии физического доступа к устройству сможет получить практически любую информацию — это лишь вопрос времени.

4. Правовые методы защиты информации

Подробную информацию можно найти в [8, 10, 11, 12].

В Российской Федерации к нормативно-правовым актам в области информационной безопасности относятся:

1) Акты федерального законодательства:
   - Международные договоры РФ;
   - Конституция РФ;
   - Законы федерального уровня (включая федеральные конституционные законы, кодексы);
   - Указы Президента РФ;
   - Постановления правительства РФ;
   - Нормативные правовые акты федеральных министерств и ведомств;
   - Нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.
2) Методические документы государственных органов России:
   - Доктрина информационной безопасности РФ;
   - Руководящие документы ФСТЭК (Гостехкомиссии России);
   - Приказы ФСБ;
3) Стандарты информационной безопасности, из которых выделяют:
   - Международные стандарты;
   - Государственные (национальные) стандарты РФ;
   - Рекомендации по стандартизации;
   - Методические указания.

Определение 3. *Государственная тайна — это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной, оперативно-розыскной деятельности, распространение которых может нанести ущерб государству.*

4.1. Базовые законы. Направления регулирования в сфере ИБ

Базовым документом по информационной безопасности в России является утвержденная Президентом "Доктрина информационной безопасности" Российской Федерации, которая представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации. Доктрина понимает под информационной безопасностью Российской Федерации состояние защищенности национальных интересов России в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. Угрозы национальным интересам Российской Федерации в данных сферах признаются Доктриной угрозами информационной безопасности. Дадим некоторые выдержки из них:

1) соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею.

2) защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Перечень сведений, которые могут составлять конфиденциальную информацию, содержится в указе президента от 6 марта 1997 г. №188 (ред. от 13 июля 2015 г.) «Об утверждении перечня сведений конфиденциального характера». Данный указ выделяет следующие типы конфиденциальных данных: личные, коммерческие, служебные, судебные, профессиональные.

Законодательство Российской федерации в сфере информационной безопасности развивается по следующим направлениям:

1) закрепление общих положений о доступе к информации, о конфиденциальности и защите информации. Базовым актом здесь является Федеральный закон «Об информации, информационных технологиях и защите информации»;

2) определение правового режима отдельных видов информации:

   - персональных данных – Федеральный закон «О персональных данных»

- семейной тайны и тайны личной жизни – Гражданский и Семейный кодексы
- государственной тайны – Закон РФ «О государственной тайне»
- коммерческой тайны – Гражданский кодекс РФ и Федеральный закон «О коммерческой тайне»
- профессиональных, процессуальных тайн – процессуальными кодексами и законами о соответствующих видах деятельности (об адвокатуре, нотариате, охране здоровья граждан и т.п.);

3) административное регулирование деятельности по защите информации, в том числе связанной с оборотом криптографических средств;

4) определение порядка осуществления оперативно-розыскных мероприятий в информационной сфере;

5) борьба с преступлениями в сфере информационной безопасности путем закрепления соответствующих составов преступлений в Уголовном кодексе РФ.

Базовый закон Российской Федерации в области информатизации – "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция). Здесь описаны понятия и определения в области технологии правового регулирования в сфере информации, информационных технологий, а также регулирование отношений при осуществлении права на поиск, получение, передачу, производство и распространение информации при применении информационных технологий. Стоит отметить статьи:

1) Статью № 8 "Право на доступ к информации", в которой описана доступность граждан и организаций к информации, а также невозможность ограничений доступа к информации в определенных сферах деятельности.

2) Статью № 9 "Ограничение доступа к информации", в которой говорится о действии федерального закона "О первональных данных о приказе Роскомнадзора от 14.12.2017 N 249, о действии государственной тайны.

3) Статью № 16 "Защита информации", в которой рассказывается об обязательствах оператора информационной системы (пункт 4) и связи с требованиями защиты информации, не составляющей государственную тайну, содержащиуюся в государственных информационных системах (Приказ ФСТЭК России от 11.02.2013 N 17

(ред. от 28.05.2019)). В частности, стоит отметить, что на основании пункта 4 обладатель информации, оператор информационной системы обязаны обеспечить нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации (п. 7 введен Федеральным законом от 21.07.2014 № 242-ФЗ).

Закон устанавливает, что информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами. На практике есть и третья категория информации: доступ к которой не ограничен федеральным законом, однако обладатель которой принимает меры по обеспечению ее конфиденциальности. В то же время, в законе установлена формальная презумпция общедоступности информации: информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

Государство также определят меру ответственности за нарушение положений законодательства в сфере информационной безопасности. Например, глава 28 «Преступления в сфере компьютерной информации» в Уголовном кодексе Российской Федерации, включает три статьи:

1) Статья 272 «Неправомерный доступ к компьютерной информации»;
2) Статья 273 «Создание, использование и распространение вредоносных компьютерных программ»;
3) Статья 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей».

4.2. Персональные данные

В 2007 году вступил в силу закон "О персональных данных". *Персональные данные* определяются законом как любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Закон не содержит никаких указаний относительно сложности способов, позволяющих сопоставить данные лицу, таким образом, определяя понятие персональных данных максимально широко.

Обработка персональных данны — это любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными.

Субъектами отношений в области обработки персональных данных являются сам субъект персональных данных (физическое лицо), а также оператор — любое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных. Законом различаются автоматизированная и неавтоматизированная обработка персональных данных. Автоматизированной признается обработка персональных данных с помощью средств вычислительной техники. Отдельно стоит обратить внимание на закрепленное законом понятие обезличивания персональных данных. Под ним понимаются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных. Роскомнадзором утверждены требования и методы по обезличиванию персональных данных.

К свойствам обезличенных данных относятся:

- полнота (сохранение всей информации о конкретных субъектах или группах субъектов, которая имелась до обезличивания);
- структурированность (сохранение структурных связей между обезличенными данными конкретного субъекта или группы субъектов, соответствующих связям, имеющимся до обезличивания);
- релевантность (возможность обработки запросов по обработке персональных данных и получения ответов в одинаковой семантической форме);
- семантическая целостность (сохранение семантики персональных данных при их обезличивании);
- применимость (возможность решения задач обработки персональных данных, стоящих перед оператором), без предварительного деобезличивания всего объема записей о субъектах).
- анонимность (невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации).

Отметим основные принципы обработки персональных данных:

- Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

- Обработке подлежат только персональные данные, которые отвечают целям их обработки.

- Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

Закон предусматривает закрытый перечень из 11 случаев, в которых могут обрабатываться персональные данные, обработку специальных категорий персональных данных, обработку биометрических персональных данных, трансграничную передачу персональных данных. В законе описаны права и обязанности оператора.

Персональные данные не относятся к информации ограниченного доступа, однако, в соответствии с законом, операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

В целях выполнения возложенных законом на оператора обязанностей, оператор разрабатывает и воплощает меры, включающие в себя, в частности:

- назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

- издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных и устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений;

- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

- осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему закону и политике оператора в отношении обработки персональных данных;

- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения закона, соотношение указанного вреда и принимаемых оператором мер;

- ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства, документами, определяющими политику оператора в отношении обработки персональных данных, и (или) обучение указанных работников.

Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются ФСБ России и ФСТЭК России.

ФСБ России и ФСТЭК России осуществляют контроль и надзор за реализацией требований к информационной безопасности персональных данных при их обработке только в отношении государственных информационных систем. Для остальных информационных систем требования по информационной безопасности де-факто являются рекомендательными. Уполномоченным органом по защите прав субъектов персональных данных является Роскомнадзор. Он наделен широкими полномочиями по контролю и надзору за операторами.

4.3. Государственная тайна

К государственной тайне относят:

1) сведения в военной области;

2) сведения в области экономики, науки и техники;

3) сведения в области внешней политики и экономики:

4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты.

В статье 7 Закона РФ «О государственной тайне» заранее установлен состав сведений, которые не могут быть засекречены, т. е. отнесены к государственной тайне. Не подлежат отнесению к государственной тайне и засекречиванию сведения:

- о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствия, а также о стихийных бедствиях и их официальных прогнозах и последствиях;
- о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
- о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- о фактах нарушения прав и свобод человека и гражданина;
- о размерах золотого запаса и государственных валютных резервах РФ;
- о состоянии здоровья высших должностных лиц РФ;
- о фактах нарушения законности органами государственной власти и их должностными лицами.

Законность отнесения сведений к государственной тайне и их засекречивание заключается в соответствии засекречиваемых сведений положениями ст. 5 и ст. 7 закона о государственной тайне.

В зависимости от степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения сведений, устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «особой важности», «совершенно секретно» и «секретно».

Срок засекречивания сведений, составляющих государственную тайну, не должен превышать 30 лет и может быть продлен по заключению межведомственной комиссии по защите государственной тайны. Перечни сведений, подлежащих засекречиванию, подлежат пересмотру не реже, чем раз в 5 лет в части обоснованности засекречивания сведений и их соответствия установленной ранее степени секретности. Носители сведений, составляющих государственную тайну, рассекречиваются не позднее сроков, установленных при их засекречивании. До истечения этих сроков носители подлежат рассекречиванию, если изменены положения действующего в данном органе государственной власти, на предприятии, в учреждении и организации перечня, на основании которых они были засекречены.

4.4. Техническая защита информации

Органом, уполномоченным в сфере технической защиты информации (кроме криптографической защиты), является Федеральная служба по техническому и экспортному контролю, ФСТЭК России. На нее возложены функции:

- обеспечения безопасности (некриптографическими методами) информации в ключевых системах информационной инфраструктуры);
- противодействия иностранным техническим разведкам на территории Российской Федерации;
- обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации (далее — техническая защита информации);
- защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств; осуществления экспортного контроля.

ФСТЭК России осуществляет издание нормативно-правовых и нормативно-технических актов по вопросам технической защиты информации. Разработка и производство средств защиты конфиденциальной информации, деятельность по технической защите конфиденциальной информации могут осуществляться только на основании лицензии ФСТЭК России. Лицензируемыми видами деятельности являются:

- контроль защищенности конфиденциальной информации от утечки по техническим каналам;
- контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
- сертификационные испытания на соответствие требованиям по безопасности информации продукции, используемой в целях защиты

конфиденциальной информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации);

- проектирование в защищенном исполнении, аттестационные испытания и аттестация на соответствие требованиям по защите информации;

- разработка и производство; установка, монтаж, испытания, ремонт средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации).

5. Технические методы защиты информации

Интегральные схемы, на которых основана работа компьютеров, создают высокочастотные изменения уровня напряжения и токов. Колебания распространяются по проводам и могут не только трансформироваться в доступную для понимания форму, но и перехватываться специальными устройствами. В компьютер или монитор могут устанавливаться устройства для перехвата информации, которая выводится на монитор или вводится с клавиатуры. Перехват возможен и при передаче информации по внешним каналам связи, например, по телефонной линии.

В состав практически любой системы ИБ входят традиционные системы (по отдельности или в комбинации):

- межсетевой экран (Firewall);
- система предотвращения вторжений (IPS);
- списки контроля доступа (ACL);
- система контроля доступа в сеть (NAC);
- антивирусные системы (Antivirus/Antimalware);
- системы управления события ИБ (SIEM).

5.1. Шифрование данных

VeraCrypt — программное обеспечение, используемое для шифрования «на лету», бесплатный и открытый проект. Для шифрования данных можно использовать VeraCrypt контейнеры с надежными паролями. Их можно использовать как файл-контейнер (его можно потом хоть по е-мейлу отправить), так и как целый раздел жесткого диска. После подключения контейнера через VeraCrypt любой софт работает с ним как с обычным логическим диском. VeraCrypt может использовать следующие алгоритмы шифрования: AES, Serpent, Twofish, Camellia, Кузнечик, а также комбинации этих алгоритмов. Использует криптографические хеш-функции: RIPEMD-160, SHA-256, SHA-512, Стрибог и Whirlpool. VeraCrypt использует режим шифрования XTS.

VeraCrypt, также как и TrueCrypt, поддерживает возможность отрицаемого шифрования, позволяя создавать внутри зашифрованного тома ещё один, «скрытый том». Кроме того, версия VeraCrypt для Windows

позволяет создавать и выполнять скрытый экземпляр операционной системы Windows, чьё наличие также можно правдоподобно отрицать.

VeraCrypt подвержена ряду потенциальных атак, к которым чувствительно и другое программное обеспечение для шифрования дисков, например BitLocker. Для смягчения этой опасности разработчики VeraCrypt предоставили пользователям ряд профилактических рекомендаций:

1) *Ключи шифрования, хранимые в оперативной памяти.* VeraCrypt сохраняет ключи в оперативной памяти в открытом виде. Теоретически, злоумышленник мог бы получить доступ к её содержимому с помощью так называемой атаки методом холодной перезагрузки, при которой атакующий получает физический доступ к содержимому модулей оперативной памяти компьютера после его выключения и посредством специального программного обеспечения или оборудования восстанавливает их старое содержимое. Подобная атака была успешно применена в отношении разделов диска, зашифрованных TrueCrypt. Для противодействия некоторым атакам данной категории, начиная с версии 1.24 в VeraCrypt добавлено шифрование ключей в оперативной памяти, а также стирание ключей из памяти при перезагрузке или завершении работы системы.

2) *Физическая безопасность.* VeraCrypt не обеспечивает безопасности данных на компьютере, к которому атакующий имеет физический доступ, в процессе работы с зашифрованными данными. Эта уязвимость относится не к случаю потерянных, конфискованных или украденных компьютеров, а когда злоумышленники имеют возможность установить на компьютер тот или иной вид шпионской аппаратуры — аппаратный кейлоггер, bus-master устройство, обладающее прямым доступом к оперативной памяти, или какое-то ещё устройство, предназначенное для решения подобных задач.

3) *Вредоносное ПО.* VeraCrypt не обеспечивает безопасности данных на компьютере с установленным вредоносным ПО. Многие вредоносные программы этого типа содержат в себе кейлоггеры и могут, в частности, считывать вводимые с клавиатуры пароли и передавать их злоумышленникам.

5.2. Умные гаджеты

Умные гаджеты плохо защищены от взлома. Многие из них содержат вшитые учетные данные, уязвимости, легко обнаруживаемые и эксплуатируемые злоумышленниками. Тем не менее умные устройства пред-

ставляют опасность для бизнеса или частного лица даже тогда, когда они уже выброшены и находятся в мусорном контейнере. В некоторых из них хранится информация о доступе к локальным беспроводным сетям и другие данные. И если раньше взломщики охотились за записями и накопителями, которые выбрасывают сотрудники разных компаний, то сейчас может начаться охота и за IoT системами, поскольку в них могут сохраняться ключи, пароли и другие данные.

Пример 1. Специалисты компании Limited Results изучили несколько популярных моделей умных ламп. Команда исследователей приобрела новую лампочку LIFX, подключила ее к беспроводной сети. Затем лампочку выключили и разобрали. После загрузки данных, хранящихся на лампочке, оказалось, что в дампе есть доступы от WiFi сети, к которой устройство подключили после покупки. Данные хранились в открытом виде. Доступны оказались даже корневой сертификат и частный RSA-ключ.

Нужно обезопасить все умные устройства, которые подключены к вашей сети.

Пример 2. Известен случай, когда злоумышленники смогли залезть в корпоративную сеть частного банка через умные камеры, к которым получили доступ [6].

В январе 2018 года специалисты по информационной безопасности из Университета Бен-Гуриона рассказали о проверке почти двух десятков случайных умных устройств — популярных гаджетов, купленных у производителя. Как оказалось, подавляющее большинство взламываются примерно за полчаса. Самый простой способ получить доступ к девайсу — подобрать дефолтный пароль. Причина проста – производители стремятся удешевить устройство, а для внедрения качественного механизма информационной защиты нужно время и деньги.

5.3. DLP и SIEM системы

К техническим методам относят и программные методы защиты информации. Примером комплексных программных решений служат DLP-системы и SIEM-системы.

DLP-системы («Data Leak Prevention» дословно «предотвращение утечки данных») – это программные продукты, которые служат для предотвращения утечки, переформатирования информации и перенаправления информационных потоков [13].

Подобного рода системы создают защищенный цифровой «периметр» вокруг организации, анализируя всю исходящую, а в ряде случаев и входящую информацию. Контролируемой информацией должен быть не

только интернет-трафик, но и ряд других информационных потоков: документы, которые выносятся за пределы защищаемого контура безопасности на внешних носителях, распечатываемые на принтере, отправляемые на мобильные носители через Bluetooth и т.д.

Поскольку DLP-система должна препятствовать утечкам конфиденциальной информации, то она в обязательном порядке имеет встроенные механизмы определения степени конфиденциальности документа, обнаруженного в перехваченном трафике. Как правило, наиболее распространены два способа: путём анализа специальных маркеров документа и путём анализа содержимого документа. В настоящее время более распространен второй вариант, поскольку он устойчив перед модификациями, вносимыми в документ перед его отправкой, а также позволяет легко расширять число конфиденциальных документов, с которыми может работать система.

Помимо своей основной задачи, связанной с предотвращением утечек информации, DLP-системы также хорошо подходят для решения ряда других задач, связанных с контролем действий персонала.

Наиболее часто DLP-системы применяются для решения следующих неосновных для себя задач:

- контроль использования рабочего времени и рабочих ресурсов сотрудниками;
- мониторинг общения сотрудников с целью выявления «подковерной» борьбы, которая может навредить организации;
- контроль правомерности действий сотрудников (предотвращение печати поддельных документов и пр.);
- выявление сотрудников, рассылающих резюме, для оперативного поиска специалистов на освободившуюся должность.

За счет того, что многие организации полагают ряд этих задач (особенно контроль использования рабочего времени) более приоритетными, чем защита от утечек информации, возник целый ряд программ, предназначенных именно для этого, однако способных в ряде случаев работать и как средство защиты организации от утечек. От полноценных DLP-систем такие программы отличает отсутствие развитых средств анализа перехваченных данных, который должен производиться специалистом по информационной безопасности вручную, что удобно только для совсем небольших организаций (до десяти контролируемых сотрудников).

SIEM-системы («Security Information and Event Management», что в переводе означает «Управление событиями и информационной безопасностью») – это программные продукты, которые обеспечивают анализ в реальном времени событий (тревог) безопасности, исходящих от сетевых устройств и приложений. SIEM представлено приложениями, приборами или услугами, и используется также для журналирования данных и генерации отчетов в целях совместимости с прочими бизнес-данными [14].

SIEM-система должна собирать, анализировать и представлять информацию из сетевых устройств и устройств безопасности. Также в эту систему должны входить приложения для управления идентификацией и доступом, инструменты управления уязвимостями и базы данных и приложений. Для наглядности мы выделим несколько функций, которые обычно поставляются SIEM-системами:

- Возможность отправки предупреждений на основе предопределенных настроек.
- Отчеты и логирование для упрощения аудита.
- Возможность просмотра данных на разных уровнях детализации.

По словам некоторых экспертов, SIEM представляет собой улучшенную систему обнаружения вредоносной активности и различных системных аномалий. Работа SIEM позволяет увидеть более полную картину активности сети и событий безопасности. Когда обычные средства обнаружения по отдельности не видят атаки, но она может быть обнаружена при тщательном анализе и корреляции информации из различных источников. Поэтому многие организации рассматривают использование SIEM-системы в качестве дополнительного и очень важного элемента защиты от целенаправленных атак.

Типовые сценарии использования SIEM-системы:

1) Отслеживание аутентификации и обнаружение компрометации аккаунтов пользователей и администраторов.
2) Отслеживание случаев заражения. Обнаружение вредоносных программ с использованием исходящих журналов брандмауэра и журналов веб-прокси, а также внутренних журналов подключения и сетевых потоков.
3) Мониторинг подозрительного исходящего трафика и передаваемых по сети данных с использованием журналов брандмауэра, журна-

лов веб-прокси и NetFlow. Обнаружение кражи данных и других подозрительных внешних соединений.

4) Отслеживание системных изменений и других административных действий во внутренних системах и их соответствия разрешенной политике.

5) Отслеживание атак на веб-приложения и их последствий с использованием журналов веб-сервера, WAF (Web Application Firewall, экран для защиты веб-приложений) и логов приложений. Обнаружение попыток компрометации веб-приложений путем анализа разных отчетов.

В конце укажем основные методы, которые снижают вероятность получения сторонними лицами ваших данных:

- В обязательном порядке использовать шифрование данных как на смартфоне, так и на ПК. Разные ОС зачастую предоставляют неплохие средства по умолчанию.
- Ставить пароли везде и всюду, включая историю переписки в Telegram и прочих мессенджерах. Естественно, пароли должны быть сложными.
- Двухфакторная аутентификация — да, это может быть неудобно, но необходимо.
- Контролировать физическую безопасность своих устройств.

6. Алгоритм RSA

Определение 4. *Односторонняя функция (англ. one-way function) — математическая функция, которая легко вычисляется для любого входного значения, но задача нахождения аргумента по заданному значению функции относится к классу NP-полных задач.*

Криптографические системы с открытым ключом используют так называемые односторонние функции. Под односторонностью понимается вычислить обратное значение, используя современные вычислительные средства, за обозримый интервал времени. В начале выполняется шифрование сообщения, потом его расшифровка. Часто расшифрование путают с дешифрованием. Разница в этих двух понятиях в том, что при расшифровании происходит процесс преобразования зашифрованного сообщения в осмысленный текст, путем использования известного алгоритма/ключа, а при дешифровании происходит "взлом" шифра, попытка вскрытия сообщения без обладания исходным ключем.

В основу криптографической системы с открытым ключом RSA положена сложность задачи факторизации произведения двух больших простых чисел [9]. Для шифрования используется операция возведения в степень по модулю большого числа. Для расшифрования используется операция возведения в степень по модулю большого числа. При дешифровании необходимо узнать за разумное время значение функции Эйлера от данного большого числа, для чего необходимо знать его разложение числа на простые множители.

Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений, включая PGP, S/MIME, TLS/SSL, IPSEC/IKE и других. Рассмотрим работу алгоритма RSA. Он состоит из двух этапов.

6.1. Генерация ключей

1) Выбираем два произвольных простых числа p и q.

2) Вычисляем их произведение $n = p \times q$ и функцию Эйлера $\phi(n) = (p-1)(q-1)$.

3) Выбираем случайное число e, $2 \leqslant e < n$, взаимно-простое с e. Последнее означает, что НОД(n, e)=1. Объявляем $\{e, n\}$ открытым ключом RSA.

4) Вычисляем число d, $1 < d < n$, обратный к e по модулю $\phi(n)$. Иначе говоря, d должен удовлетворять условию $e \times d = 1 \mod \phi(n)$. Для вычисления d необходимо использовать обобщенный алгоритм Евклида. Объявляем $\{d, n\}$ закрытым ключом RSA.

6.2. Шифрование, расшифрование

Для шифрования текстовой строки M выполним следующие действия:

1) Разобьем текст на отдельные символы.

2) Заменим последовательность символов последовательностью их кодов.

3) Зашифруем последовательность, заменяя каждый код k по формуле: $c = enc(k) = k^e \mod n$.

Для расшифрования шифростроки enc(M) выполним следующие действия:

1) Расшифруем последовательность, заменяя каждый шифрокод c на код $k = dec(c)$, вычисляемый по формуле: $k = h^d \mod n$.

2) Заменим коды k на символы текста, восстанавливая сообщение.

Пример. Пусть $p = 11$, $q = 5$.

1) Вычислим $n = pq = 55$ и функцию Эйлера $\phi(n) = 10 * 4 = 40$.

2) Возьмем открытый ключ, равным $e = 7$. Проверим условие НОД(40,7)=1.

3) Найдем $d = 23$.

4) Зашифруем число m = 15: h = enc(15) = me mod n = $15^7 \mod 55 = 5$.

5) Расшифруем шифротекст $k = 5^{23} \mod 55 = 15$.

Список литературы

[1] Физические средства защиты информации – URL : https://ru.bmstu.wiki/Физические_средства_защиты_информации (дата обращения: 19.02.2020).

[2] Организационно-правовые аспекты защиты информации – URL: https://www.intuit.ru/studies/courses/600/456/lecture/10227 (дата обращения: 19.02.2020).

[3] Android и шифрование данных. О том, как все плохо и почему вряд ли станет лучше – URL: https://xakep.ru/2016/05/02/android-encryption/ (дата обращения: 19.02.2020).

[4] Когда шифрование не поможет: рассказываем про физический доступ к устройству – URL: https://habr.com/ru/company/hidemy_name/blog/448708/ (дата обращения: 19.02.2020).

[5] VeraCrypt – URL: https://ru.wikipedia.org/wiki/VeraCrypt (дата обращения: 19.02.2020).

[6] Не выбрасывайте умные лампочки в мусор, или опасность IoT – URL: https://habr.com/ru/post/453410/ (дата обращения: 19.02.2020).

[7] Исследователи из X-Lab за 20 минут разблокировали смартфон, используя отпечаток пальца его хозяина, взятый со стакана – URL: https://habr.com/ru/news/t/473914/ (дата обращения: 19.02.2020).

[8] Обзор законодательства Российской Федерации в сфере информационной безопасности – URL: https://digital.report/zakonodatelstvo-rossii-informatsionnaya-bezopasnost/ (дата обращения: 19.02.2020).

[9] Ишмухаметов, Ш.Т., Рубцова, Р.Г. Математические основы защиты информации [Текст] / Шамиль Талгатович Ишмухаметов, Рамиля Гакилевна Рубцова. Электронное пособие, Казань, 2012. — 138 с.

[10] Обзор законодательства Российской Федерации: Персональные данные, личная и семейная тайна – URL: https://digital.report/zakonodatelstvo-rossii-personalnyie-dannyie/ (дата обращения: 19.02.2020).

[11] Обзор законодательства Российской Федерации в сфере информационной безопасности — Часть 3: Государственная тайна – URL: https://digital.report/zakonodatelstvo-rossii-gosudarstvennaya-tayna/ (дата обращения: 19.02.2020).

[12] Обзор законодательства Российской Федерации в сфере информационной безопасности — Часть 7: Техническая защита информации – URL: https://digital.report/zakonodatelstvo-rossii-zashhita-informatsii/ (дата обращения: 19.02.2020).

[13] DLP системы – URL: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/ (дата обращения: 19.02.2020).

[14] SIEM системы – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Popular-SIEM-Starter-Use-Cases (дата обращения: 19.02.2020).

Методическое пособие

Долгов Дмитрий Александрович

ВВЕДЕНИЕ В КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ЧАСТЬ 1