Содержание:

Введение

Настоящая работа посвящена теме предотвращения угрозы информационной безопасности и рассматривает наиболее важные и актуальные вопросы в этой области.

Работа состоит из трёх глав, по три раздела в каждой, введения, заключения и списка литературы из 11 учебников и учебных пособий и двух законодательных актов.

Общий объём работы составляет 29 страниц.

Проблема, затронутая в работе, весьма актуальна в настоящее время, так в связи с все возрастающими объемами пользования, создания и передачи информации встает и проблема её защиты от намеренного или непреднамеренного посягательства, искажения, хищения и уничтожения.

Каждое юридическое или физическое лицо должно быть грамотным в вопросах использования информационных ресурсов и обладать необходимым наборов средств, методов и инструментов для защиты себя от преступных действий со стороны третьих лиц.

Все данные вопросы нашли подробное отражение на страницах настоящей работы.

Целью данной работы является изучение состава угроз информационной безопасности, для достижения поставленной цели, были выделены следующие задачи:

- рассмотреть понятие информационной безопасности;

- изучить средства защиты информации;

- рассмотреть методы защиты информации.

Объект исследования – информационная безопасность.

Предмет исследования - состава угроз информационной безопасности.

Структура работы состоит из введения, основной части, заключения и списка литературы.

Теоретической и методологической базой данной работы послужили труды российских авторов в области информационной безопасности, материалы периодических изданий и сети Интернет.

ГЛАВА 1. ПОНЯТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Цели поддержки информационной безопасности

Выделяют три вида целей поддержки информационной безопасности [10, с.36]:

1. Конфиденциальность;
2. целостность;
3. готовность.

Рассмотрим их более подробно.

1. Конфиденциальность.

Под конфиденциальностью понимают наиболее обобщённый аспект информационной безопасности. Каждая организация и её руководство стремятся защитить свои данные, не допустить их утечки, предпринять предварительные меры по охране информации. Особенно ярко это проявляется на военных предприятиях, однако, не стоит забывать и о важности сохранения конфиденциальности в коммерческих фирмах.

Схожие с конфиденциальностью термины – секретность, неразглашение, коммерческая и иная тайна.

Конфиденциальность важна для производственных предприятий, банков, государственных организаций, частных фирм, различных видов юридических лиц.

Конфиденциальность актуальна не только при хранении данных, но и при их передаче другим лицам. То есть необходимо обеспечивать сохранность передаваемой информации.

2. Целостность.

Информация имеет свойство меняться, как со стороны предприятий, так и со стороны тех лиц, с которыми они взаимодействуют.

Понятие целостности означает, что любые изменения «должны быть сделаны только разрешенными объектами и с помощью разрешенных механизмов» [6, с. 27].

Нарушение целостности может произойти как в результате намеренных, так и случайных действий – форс-мажор, авария, сбои в системах и прочее.

3. Готовность.

Готовность – это доступность информации только разрешённым объектам. С другой стороны, информация становится бесполезной, если она не доступна никому. Односторонний доступ к сведениям порождает отсутствие сделок, контактов и, как следствие, нормального функционирования фирмы.

Говоря о целях информационной безопасности, необходимо упомянуть атаки, способствующие нарушению этих целей.

Существует несколько классификаций информационных атак, приведём одну из них (рис. 1).

Данная классификация основана на целях нарушения информационной безопасности и предусматривает деление всех атак на три группы с последующим делением внутри групп в зависимости от угрожающих действий.

Рассмотрим данную классификацию более подробно.

1. Атаки, угрожающие конфиденциальности делятся на две подгруппы:
    1. Вмешательство.

Под вмешательством понимается «неправомочный доступ или перехват данных» [6, с. 32]. Например, передаваемый в сети Интернет файл содержит в себе конфиденциальную информацию, при этом лицо, не имеющее полномочий на передачу и использование данного файла может вмешаться и остановить передачу, с тем чтобы впоследствии использовать данные для собственной

выгоды.

Рис. 1. Классификация информационных атак (авторская схема).

- 1. Наблюдение за трафиком и его анализ.

Здесь подразумеваются действия стороннего лица по получению данных не о самом содержании файла, а о внешних характеристиках – электронном адресе, количестве сессий и т.д.

1. Атаки, угрожающие целостности, также делятся на следующие подгруппы:
    1. Модификация.

Данный вид атаки подразумевает со стороны злоумышленника не только прерывание передачи файла, но и его изменение. Здесь могут быть:

- изменение содержания сообщения;

- изменение типа операции;

- изменение внешних данных;

- задержка сообщения;

- удаление сообщения и др.

2.2. Имитация источника.

Под данной атакой понимается то, что «атакующий имитирует кого-то, кто имеет право на производимые действия» [6, с. 34]. Например, действия при помощи полученной информации под видом настоящего фигуранта, или имитация места события (подмена сайта, адреса и пр.).

- 1. Повторная передача информации.

Это так называемая атака воспроизведения, подразумевающая использование полученных данных для своих целей при помощи простого дублирования действий (предъявления тех же документов повторно, набор того же кода и т.д.).

- 1. Отказ от сообщения.

Данный вид атаки может быть выполнен одной из сторон контакта – передающей или принимающей. Они могут отрицать факт получения или передачи данных.

1. Атаки, угрожающие готовности

В данную группу входит один вид атаки, наиболее для неё характерный - отказ в обслуживании.

3.1. Отказ в обслуживании подразумевает несколько стратегий для достижения целей атакующего:

- передача фиктивных запросов;

- прерывание или удаление ответа;

- перезагрузка системы и др.

Наряду с вышепредложенной существует и иная классификация атак (рис. 2):

Рис. 2. Классификация информационных атак (авторская схема).

Пассивные атаки – это атаки, «нацеленные только на получение информации» [7, с. 64].

Активные атаки направлены на «изменение данных или повреждение системы» [7, с. 65]. Здесь количество методов шире, а вред больше.

1.2 Понятие информационной безопасности

Итак, что же является информационной безопасностью?

Информационная безопасность – это «защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре» [4, с. 11].

Ещё одно определение безопасности в области информации – «состояние защищенности информационной среды организации, обеспечивающее ее формирование, использование и развитие» [7, с. 6].

Информационная среда состоит из двух областей:

- информационно - технической (антропологический фактор: созданные человеком технологии);

- информационно - психологической (природный фактор).

Многие авторы формируют так называемую модель информационной безопасности, включающей в себя следующие категории:

- конфиденциальность;

- целостность;

- доступность;

- неотказуемость;

- аутентичность;

- подотчетность;

- достоверность;

- апеллируемость и другие.

Однако, необходимо помнить именно о комплексном подходе.

Для обеспечения информационной безопасности используют следующие уровни (сферы) (рис. 3).

Рис. 3. Уровни обеспечения информационной безопасности (авторская схема).

1. Наиболее важным является законодательный уровень, так как он обеспечивает законность и отсутствие противоправности действий, подразумевая наказание за них.

Данный уровень включает две группы методов:

1) меры ограничительной направленности – это факторы, «направленные на создание и поддержание в обществе негативного отношения к нарушениям и нарушителям информационной безопасности» [9, с. 21];

2) направляющие и координирующие меры – это факторы, которые помогают «повысить образованность общества в области информационной безопасности» [9,

с. 21], а также способствуют разработке и внедрению средств обеспечения информационной безопасности.

Другие законы и подзаконные акты.

1. Административный уровень безопасности включает в себя «действия общего характера, находящиеся в компетенции руководства организации» [9, с. 25].

Основная цель здесь - политика безопасности организации, её действия по сохранности собственных активов.

Составляющие данной политики:

- управление персоналом;

- поддержание работоспособности;

- физическая защита;

- организация восстановительных работ;

- реагирование на нарушения режима безопасности.

Два других уровня будут рассмотрены в дальнейших разделах настоящей работы.

1.3 Виды информационных угроз

Все информационные угрозы можно условно выделить в четыре основных группы [1] (рис. 4):

Рис. 4. Виды информационных угроз (авторская схема).

Основываясь на вышеприведённой классификации, приведём внешние и внутренние источники угроз, а также формы их проявления (табл. 1).

Таблица 1

Источники и формы угроз

Источники угроз	Формы угроз

Внутренние	1.Сотрудники организации. 2. Аппаратные средства. 3. Программное обеспечение.	1. Ошибки пользователей программ и администраторов сети. 1. Нарушения работниками организации установленных нормативов сбора, передачи, обработки, уничтожения информацию. 2. Ошибки в программном обеспечении; 3. Отказы и ошибки в работе компьютеров и копировального оборудования.
Внешние	1.Компьютерные вирусы и программы. 2.Юридические и физические лица. 3.Форс-мажор.	1. 1.Заражение ПК и ЭВМ вирусами или программами, содержащими вирусы. 2. 2. Несанкционированный доступ к информации фирмы. 3. 3.Информационный мониторинг со стороны сторонних фирм и специальных организаций и служб. 4.Действия государственных и муниципальных структур. 4. 5.Аварии, техногенные катастрофы, иные факторы форс-мажора.

Предложена ещё одна классификация информационных угроз по способам воздействия [9, с. 52].

Систематизируем их следующим образом (табл. 2):

Таблица 2

Классификация информационных угроз

Виды угроз	Разновидности угроз
1. Информационные	- нелегальный доступ к базе информационных ресурсов; - несанкционированное копирование даинформации; - хищение сведений из архивов, баз данных, библиотек; - нарушение технологии и техники обработки и сбора информации; - противозаконное использование данных; - применение информационного оружия.
1. Программные	- использование ошибок в программном обеспечении; - компьютерные вирусы и программы, содержащие наборы вирусов.
1. Физические	- уничтожение или искажение данных в средствах по сбору и обработке информации; - хищение и кража носителей данных и баз данных; - хищение кодов, шифров, программных ключей, а также средств криптографической охраны сведений;
1. Радиоэлектронные	- использование электронных устройств хищения данных в помещения или компьютеры; - расшифровка, замена, уничтожение данных, передаваемых по каналам связи.

1. Организационно - правовые	- закупки бракованных или утративших актуальность информационных технологий и аппаратных средств; - нарушение законов, нормативов, предписаний в информационной сфере.

ГЛАВА 2. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

2.1 Организационные средства защиты

Организационные средства защиты информации включают в себя следующие группы (рис. 5).

Рис. 5. Организационные средства защиты информации (авторская схема).

Организационно-технические средства включают в себя:

- подготовка и надлежащее оборудование помещений, где размещаются компьютеры;

- прокладка кабеля с учетом стандартов;

- установка компьютерной техники.

Организационно-правовые средства включают в себя:

- законы и подзаконные нормативно-правовые акты;

- внутренние нормативы организации;

- решения руководства.

Организационные средства имеют свои преимущества и недостатки. К сильным сторонам относятся:

- одновременное решение различных проблем и вопросов;

- простота исполнения;

- быстрое реагирование на нарушения в сети;

- широкие возможности развития.

К слабым сторонам можно отнести:

- повышенную зависимость от субъективных факторов;

- особенности работы на предприятии.

Выделяют следующие организационные мероприятия [4, с. 101]:

К организационным мероприятиям можно отнести следующие:

- четкая структура персонала, а также разделение помещений для работы разных структурных подразделений предприятия;

- ограничение или запрет доступа посторонних лиц в специальные помещения;

- охрана или сигнализация помещений;

- четкое ограничение списка лиц, имеющих право доступа к компьютерам и иному оборудованию;

- промежуточные меры защиты информации (пароли, специальные программы).

2.2 Технические средства защиты

Технические или аппаратные средства понимаются как «устройства различного типа, решающие аппаратными средствами задачи защиты информации» [4, с. 103]. К техническим средствам можно отнести:

- механические,

- электронные,

- электромеханические и др.

К аппаратным средствам защиты можно отнести соответствующие устройства:

- электронные,

- электронно-оптические,

- электронно-механические.

Например, наиболее широко употребляются:

- регистры для реквизитов защиты (разных идентифицирующих кодов, паролей, грифов секретности и т.д.);

- устройства определения индивидуальных качеств человека для его идентификации (отпечатков пальцев, голоса и пр.);

- схемы периодической проверки адреса данных путем прерывания передачи;

- инструменты для шифрования информации (более подробно это будет рассмотрено в третьей главе настоящей работы).

Помимо этого для внешней защиты информационной системы используются такие средства как:

1. системы цифрового видеонаблюдения (камеры наружного и внутреннего наблюдения);
2. системы пожарной сигнализации;
3. системы охранной сигнализации;
4. системы управления доступом;
5. различные контрольные системы.

Утечка информации охраняется посредством использования следующих средств:

- применение экранированного кабеля и экранированных конструкций при его прокладке;

- оборудование экранированных помещений;

- применение высококачественных фильтров связи;

- создание зон контроля;

- установка и использование активных систем зашумления.

2.3 Программные средства защиты

Программные средства это различные программы, используемые в следующих целях [4, с. 107]:

- контроля доступа,

- идентификации пользователей,

- шифрования и кодирования информации,

- удаления промежуточной рабочей информации,

- контроля системы защиты в тестовом режиме и др.

Программные средства обладают преимуществами:

- универсальностью,

- надежностью,

- гибкостью,

- простотой установки и использования,

- возможностью к модификации.

Наряду с преимуществами есть и свои недостатки, а именно:

- ограниченная функциональность сети,

- высокий уровень реакции на случайные или преднамеренные изменения,

- зависимость от типов и видов компьютеров.

Авторами выделяются такие виды программных средств (рис. 6).

Рассмотрим их более подробно.

1. Встроенные средства просты в эксплуатации и удобны.
2. Специализированные средства имеют большие возможности по сравнению с встроенными.
3. Межсетевые экраны это промежуточные серверы, предназначенные для фильтрации трафика разных уровней. Сетевые экраны, носящие название фильтров, делают локальную сеть невидимой и не пропускают вредные пакеты, не соответствующие той или иной конфигурации.

Рис. 6. Виды программных средств (авторская схема).

1. Прокси-серверы – это специальные серверы-посредники, ограничивающие и полностью запрещающие несоответствующую маршрутизацию в сети. Однако, данные метод не обеспечивает защиту на более высоких уровнях.
2. VPN - виртуальная частная сеть. Её предназначение в том, чтобы передать секретную информацию через те сети, где возможна их прослушка.

ГЛАВА 3. МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

3.1 Методы защиты информационных ресурсов

Наиболее распространены два основных метода защиты информации:

1. Криптография (общий метод).
2. Стенография (специальный метод).
3. Криптография при переводе с греческого означает «тайну написанного». В настоящее время криптография понимается как «искусство преобразования сообщений, делающее их безопасными» [11, с. 119].

Криптография включает в себя три механизма (рис. 7).

Рис. 7. Механизмы криптографии (авторская схема).

Данные механизмы имеют следующее назначение:

1. Шифрование симметричными ключами подразумевает шифровку с применением секретного ключа и алгоритма его расшифровки.
2. Шифрование асимметричными ключами основано на использовании двух ключей вместо одного.
3. При хэшировании из «сообщения переменной длины может быть создан дайджест фиксированной длины, как правило, меньшего размера, чем исходное сообщение» [11, с. 121].
4. Стеганография использовалась изначально для засекречивания связи. При переводе с греческого слово переводится как «закрытая запись». Отличие стенографии от криптографии заключается в том, что она скрывает не содержание сообщения, шифруя его, а само сообщение.

Помимо вышеприведенных двух методов используются следующие:

- Скрывающие тексты. Здесь используются двоичные символы, пробелы и пр.

- Словарь слов, применяемых по их грамматическим значениямс закрепленным кодом.

- Использование изображений.

- Использование аудио- и видеоинформации.

3.2 Правовые основы защиты информации

Правовые основы защиты информации базируются на законодательстве и включают в себя четыре уровня обеспечении безопасности [1]:

1. Первый уровень правовой защиты основан на законодательных актах, применимых на территории РФ и за её пределами. Сюда можно отнести:

- международные конвенции по направлениям охраны информационной и промышленной собственности, авторском и патентном праве, защиты информации в сети Интернет;

- Конституция РФ (статья 23 Конституции провозглашает право граждан на такие действия частной жизни как ведение личной переписки, тайну сообщений и пр.);

- Гражданский кодекс РФ (статья 139 ГК РФ устанавливает ответственность за нарушение коммерческой и служебной тайны, иные незаконные действия в области информации);

- Уголовный кодекс РФ (статья 273 устанавливает ответственность за нарушение эксплуатации оборудования, за злонамеренное распространение вредоносных программ);

- Федеральный закон «Об информации, информатизации и защите информации» от 20.02.95 № 24-ФЗ (статья 10 определяет понятие государственной тайны и конфиденциальной информации, статья 21 определяет порядок защиты информации);

- Федеральный закон «О государственной тайне» от 21.07.93 № 5485-1 (статья 5 перечисляет сведения, составляющие государственную тайну, статья 8 степень

секретности информации, статья 20 перечисляет органы по защите государственной тайны, статья 28 сертификацию средств защиты информации);

- ФЗ «О лицензировании отдельных видов деятельности» от 08.08.2001 № 128-ФЗ;

- ФЗ «О связи» от 16.02.95 № 15-ФЗ и другие законные акты.

2. Второй уровень правовой защиты включает в себя подзаконные акты (указы Президента, постановления Правительства, постановления Арбитражного Суда и т.д.).

3. Третий уровень защиты информации основан на ГОСТах, стандартах, нормативах.

4. Четвертый уровень защиты связан с использованием локальных нормативных актов, положений, инструкций и т.д.

3.3 Информационная безопасность в сети Интернет

Интернет является на настоящий момент основным средством общения, работы, передачи огромного количества информации.

Всемирная сеть растёт огромными темпами, вбирает в себя обширное количество сайтов, организует функционирование множества ресурсов.

Однако, велик процент и нарушений, связанных с пользованием Интернетом. Одной из причин выступает недостаточная грамотность пользователей в области защиты своей информации.

В рамках отдельно взятой организации данную проблему можно решить, помимо всех вышеперечисленных средств и методов обеспечения безопасности, путём составления документа, прописывающего следующие положения:

1. порядок ведении работы с документами и информацией организации;
2. лица, имеющие доступ к информации;
3. порядок копирования и передачи данных;
4. режим работы на компьютерном оборудовании;
5. наличие необходимой документации;
6. надлежащее оборудованеи помещений;
7. наличие журналов и инструкции по их ведению.

Помимо этого каждая организация должна следить за изменениями в законодательстве, публикациями в СМИ, принимать участие в различных мероприятиях, посвящённых охране информации.

ЗАКЛЮЧЕНИЕ

В настоящей работе была рассмотрена проблема предотвращения информационной безопасности.

Работа состоит из трех глав, в каждой из которых рассмотрены вопросы, касающиеся защиты информации.

В первой главе рассмотрены теоретические вопросы понятия информационной безопасности, ее терминологии и классификация.

В первом разделе рассмотрены цели безопасности и угрозы (атаки), которые могут ей угрожать.

Второй раздел посвящен проблемам понятия безопасности, а также здесь приведена модель безопасности.

Третий раздел содержит две классификации информационных угроз.

Вторая глава работы посвящена рассмотрению организационных, технических и программных средств защиты информации (разделы 1, 2 и 3 соответственно).

В третьей главе рассмотрены методы защиты информации (первый раздел), отдельно изучены методы правовой защиты информации (второй раздел) и рассмотрены вопросы пользования всемирной сетью Интернет.

По итогам работы необходимо сделать вывод о необходимости предварительного принятия мер по охране информации, используемой как в коммерческой деятельности, так и в личных целях, чтобы обеспечить бесперебойное пользование данными и сохранением секретных сведений, составляющих право каждого юридического и физического лица.

СПИСОК ЛИТЕРАТУРЫ

1. Ассоциация «РусКрипто»: Информационная безопасность [Электронный ресурс]: материалы конференций. - Режим доступа: http://www.ruscrypto.ru/events/infosecurity/
2. Баймакова И.А., Новиков А.В., Рогачев А.И., Хыдыров А.Х. Обеспечение защиты персональных данных. Методическое пособие. М. Книжный мир, 2016. – 354 с.
3. Галатенко В.А. Основы информационной безопасности. Интернет-университет информационных технологий. ИНТУИТ.ру, 2016.
4. Гафнер В.В. Информационная безопасность. Ростов н/Д.: Феникс, 2015. – 324 с.
5. Информационная безопасность: Виды угроз [Электронный ресурс]: статья. - Электрон, дан. - Режим доступа: http://www.infosecurity.ru/site/threats.shtml.
6. Лейбин В.М. Глобалистика, информатизация, системные исследования. Том 2. Информатизация, системные исследования. Спб.: Ленанд, 2016. – 200 с.
7. Лопатин В.Н. Информационная безопасность России: Человек, общество, государство. Серия: Безопасность человека и общества. М.: 2015. - 428 с.
8. Справочная правовая база «Консультант плюс» [Электронный ресурс]: нормативно-правовые документы. - Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=40541.
9. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства. Москва: ДМК Пресс, 2015.- 544 с.
10. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. М.: Книжный мир, 2014. - 352 с.
11. Ярочкин В.И. Информационная безопасность. Учебник для вузов. М.: Академический проект, Мир, 2016. – 544 с.

Законодательные акты:

1. Закон “Об информации, информатизации и защите информации” Федеральный закон от 20 февраля 1995 года N 24-ФЗ.
2. Указ Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03.2008 № 351.