**УДК 338.516**

**ББК 65.01**

**П 16**

Одобрено редакционно-издательским советом КЮИ МВД России.

**Рецензенты:**

доктор педагогических наук, профессор С.Я. Казанцев
(Казанский юридический институт МВД России)
кандидат экономических наук Т.В. Любавина
(Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ)
кандидат экономических наук М.Н. Сафиуллин
(Управление ЭБиПК МВД по Республике Татарстан)

**П 16 Панченко В.В.**

Правовые основы информационной безопасности в органах внутренних дел: учебное пособие /В.В. Панченко, Г.А. Гудочкин. - Казань: КЮИ МВД России, 2016. – 102 с.

Учебное пособие «Правовые основы информационной безопасности» ориентировано на изучение основных понятий и положений информационной безопасности в свете совершенствования и развития современных информационных технологий, повышения требований к информационной безопасности органов внутренних дел. В рамках учебного пособия освещены правовые аспекты защиты информационных ресурсов и обеспечения безопасности ведомственной информации, средств и систем информатизации.

Учебное пособие ориентировано на курсантов и слушателей системы учебных заведений МВД России по курсу «Основы информационной безопасности».

**ISBN 078-901593-68-4** **ББК 65.01**

# ОГЛАВЛЕНИЕ

# Введение

Зависимость общества от информационных технологий породила новое отношение к информации. С одной стороны, значительно упростился доступ широких слоев населения к сведениям самого разного характера, с другой – существенно возросло влияние, оказываемое информацией на принимаемые людьми и группами людей решения. Можно сказать, что стоимость распространения информации снизилась, но одновременно с этим выросла значимость, ценность самой информации.

В связи с этим образовался новый тип ресурсов – информационные ресурсы, которые наряду с материальными, энергетическими и прочими ресурсами обеспечивают не только функционирование общественных и государственных институтов, а также оказывают существенное влияние на жизнь каждого человека в отдельности.

Любой ресурс нуждается в защите, и информационные ресурсы – не исключение. Но в случае информационных ресурсов традиционные методы защиты не всегда применимы. Особый подход к процессу защиты информации от различных угроз обусловлен качественным своеобразием информационных ресурсов, их отличием от прочих видов ресурсов. Среди основных таких отличий можно выделить простоту копирования, изменения и уничтожения информации.

Говоря о ценности информации для общества, следует отметить, что любое развитое общество обладает институтами, в той или иной мере этим обществом управляющими. Несомненно, ценность информации для таких институтов значительно выше, чем для всех остальных. Отсюда логически вытекает необходимость для этих организаций в более развитой защите информации. Одним из таких общественных институтов являются правоохранительные органы, представляющие собой один из основных элементов государства. Вследствие этого каждый сотрудник органов внутренних дел должен обладать информационной культурой, в частности, основами культуры обеспечения информационной безопасности.

Поэтому целью учебной дисциплины «Основы информационной безопасности в органах внутренних дел» является подготовка специалистов с необходимым в настоящее время профессиональным

уровнем информационной культуры, владеющих методами и средствами обеспечения информационной безопасности своей профессиональной деятельности.

Достижение данной цели возможно путем приобретения обучаемыми базовых теоретических знаний, практических навыков и умений в данной сфере.

# ГЛАВА 1.
# Основные понятия информационной безопасности

## 1.1. Модель информационной сферы

Регулирование общественных отношений, связанных с информацией, происходит в информационной сфере.

Информационная сфера – сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации.

В информационной сфере происходят информационные процессы - процессы создания, сбора, обработки, накопления, хранения, поиска, распространения и потребления информации, процессы создания и применения информационных систем, информационных технологий и средств их обеспечения.

Общественные отношения, возникающие в информационной сфере при осуществлении информационных процессов, называются информационными отношениями.

Деятельность по осуществлению информационных процессов называется информационной деятельностью.

Рассматривая информационные отношения, необходимо отметить, что несмотря на всю их разнообразность, они происходят между составными частями информационной сферы. Схематично информационную сферу можно представить в виде пяти областей (рис.1).

Справа расположены три области, в которых и происходит обращение информации. Области, расположенные слева, являются вспомогательными и обеспечивают обращение информации. Все области тесно взаимосвязаны друг с другом, поэтому разделение между ними можно считать условным.

Область поиска, получения и потребления информации определяет потребность в информации, задает пути ее формирования, обеспечивает информацией потребителей.

Поиск информации происходит в информационных ресурсах или посредством информационных продуктов и информационных услуг. Получение информации может осуществляться посредством поиска или при ее тиражировании и распространении. После осуществления получения информации происходит ее потребление, которое может быть

конечным пунктом оборота информации или источником для создания новой информации.

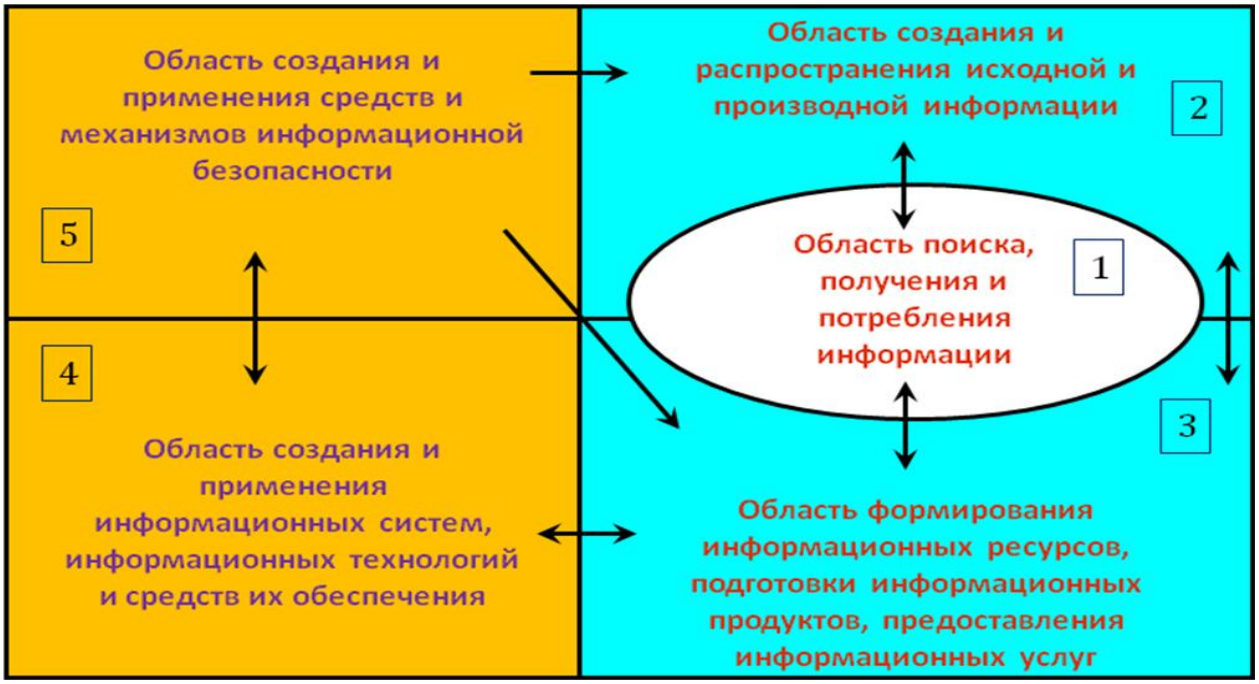


Рис. 1. Информационная сфера

В области создания и распространения исходной и производной информации создается новая информация, которая потом используется в области поиска, получения и потребления информации и в области формирования информационных ресурсов, подготовки информационных продуктов, предоставления информационных услуг.

Именно на основе вновь созданной или измененной информации создаются информационные ресурсы. Информация в этой области может создаваться как с конкретной целью, так и без таковой.

В области формирования информационных ресурсов, подготовки информационных продуктов, предоставления информационных услуг в виде информационных ресурсов концентрируется информация, созданная в области создания и распространения исходной и производной информации.

Посредством информационных ресурсов индивидуальные знания преобразуются в коллективные, что позволяет считать информационные ресурсы основой системы образования и науки, основой государства. Создаваемые на основе информационных ресурсов информационные

продукты и услуги стали одним из основных товаров на современном рынке.

Область создания и применения информационных систем, информационных технологий и средств их обеспечения является обеспечивающей для трех областей, рассмотренных выше.

Особенно тесно она взаимодействует с областью формирования информационных ресурсов, создания информационных продуктов, предоставления информационных услуг.

Область создания и применения средств и механизмов информационной безопасности обеспечивает защиту информации в других областях.

Наиболее тесно данная область взаимодействует с областью создания и применения информационных технологий и средств их обеспечения, а также с областью формирования информационных ресурсов, создания информационных продуктов, предоставления информационных услуг. В каждой области информационной сферы средства и механизмы информационной безопасности решают различные задачи.

## 1.2. Основные понятия информационной безопасности и защиты информации

### 1.2.1. Общие определения

*"Информация"* от латинского слова *"informatio"*, что означает *сведения, разъяснения и изложения*. Понятие информации является одним из самых обсуждаемых в науке и обществе. На данный момент наука старается найти обобщающие свойства и закономерности, которые присущи обширному понятию *информация*, но в настоящее время это понятие остается подсознательным и получает различные смысловые объяснения.

В литературе выделяется несколько понятий «информации». Например, в физике «информация понимается как отличительное свойство всех элементов и систем, которые существуют, а также выражает смысл существования».

С термином «информация» определились, но чтобы полностью раскрыть значение высказывания «информационная безопасность», необходимо выяснить, что в себя включает термин «безопасность».

В Толковом словаре В. Даля «безопасность – это есть отсутствие опасности, сохранность, надежность». Толковый словарь русского языка Ожегова С.И. «безопасность – это состояние, в котором не угрожает опасность, есть защита от опасности». Также «безопасность» – это состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз».[1]

Таким образом, обобщив эти два понятия: «информация» и «безопасность» можно сделать вывод, что собой представляет «информационная безопасность».

Информационная безопасность как понятие впервые было нормативно закреплено в ФЗ «О безопасности» в 1992 г. В этом источнике «информационная безопасность» толковалась, как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций и государства.

В настоящее время *информационная безопасность* – это поддержание сохранности информационных ресурсов и защита законных прав общества и личности в информационной сфере, в том числе.

Если сказать проще, то информационная безопасность – это безопасность, которая связана как с информацией, так и со сферой информации.

Целями информационной безопасности являются:

– защита национальных интересов;

– обеспечение гражданина и общества достоверной, полной и доступной информацией;

– правовая защита человека и общества при получении, распространении и использовании информации.

Информационная сфера на данном этапе имеет 2-е составляющие:

– информационно – техническую (искусственно созданный человеком мир технологий, техники и т.д.);

– информационно – психологическую (естественный мир живой природы, который включает и самого человека).

---

[1] О безопасности: Федеральный закон от 28 декабря 2010 г. № 390-ФЗ // Российская газета. 2010. №295.

Опасным явлением для информационной безопасности является возникновение «инцидента информационной безопасности» (*information security incident*) – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.[1]

То есть это те случаи, которые при своем появлении ведут к нарушению информационной безопасности. Например, системные сбои или перегрузки, ошибки пользователей, неконтролируемые изменения систем, сбои программного обеспечения и отказа технических средств, нарушение правил доступа и т.п.

Эти происшествия могут вызываться ошибкой людей или неправильным функционированием технических средств, или влиянием природного фактора (такого как пожар, наводнение и т.д.), или предумышленными действиями, которые могут привести к нарушению секретности, доступности, целостности и т.д.

В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» *информация* – это сведения (сообщения, данные), независимо от формы их представления[2].

Данное определение является достаточно общим. Необходимо отметить, что с точки зрения обеспечения информационной безопасности имеет смысл рассматривать информацию *только как сведения, имеющие материальное выражение*. Это связано с тем, что невозможно обрабатывать информацию, которая не зафиксирована каким-либо образом. Поэтому мы будем оперировать понятием «документированная информация», которое также определено в указанном законе.

*Документированная информация* – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель[3].

---

[1] Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий: ГОСТ Р ИСО/МЭК 18045-2013: утверждена приказом Федерального агентства по техническому регулированию и метрологии от 28 августа 2013 г. № 624-ст.

[2] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 №149-ФЗ // Российская газета. 2006. №165.

[3] Там же.

Обрабатываемая информация в большинстве случаев представляет собой не отдельные документы, а документы, определенным образом сгруппированные, т.е. массивы документов, или, иначе говоря, информационные ресурсы.

*Информационные ресурсы* – организованная и структурированная документированная информация, содержащаяся в библиотеках, архивах, фондах, банках данных, информационных системах[1].

Поскольку в настоящее время подавляющее большинство информации обрабатывается с использованием автоматизированных информационных систем, ограничимся их рассмотрением.

Федеральный закон «Об информации, информационных технологиях и о защите информации» дает следующее определение:

*Информационная система* – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств[2].

В то же время нельзя забывать и о том, что любая информационная система не существует «сама по себе». Деятельность информационной системы обеспечивают *обслуживающий персонал* и целый ряд *вспомогательных систем* – системы электроснабжения, кондиционирования и отопления, водоснабжения, средства коммуникаций и т.д. Такие вспомогательные системы мы будем называть поддерживающей инфраструктурой.

*Поддерживающая инфраструктура* – совокупность технических средств и технологий, обеспечивающих функционирование информационной системы.

Таким образом, можно сформулировать определение термина «информационная безопасность» применительно к информационным системам:

*Информационная безопасность* – состояние защищенности информационной системы, поддерживающей ее инфраструктуры и обслуживающего персонала от воздействий, которые могут нанести неприемлемый ущерб субъектам информационных правоотношений.

---

[1] Прокопенко А.Н. Правовое регулирование информационных ресурсов МВД России: монография / А.Н. Прокопенко. - Белгород: БелЮИ МВД России, 2010.

[2] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 №149-ФЗ // Российская газета. 2006. №165.

Обеспечение информационной безопасности осуществляется путем выполнения различного рода действий и мероприятий, носящих общее название «защита информации».

*Защита информации* – комплекс мероприятий, направленных на обеспечение информационной безопасности.

Следует четко различать эти два понятия: если «информационная безопасность» представляет собой определенное состояние информационной системы, то «защита информации» – это процесс, т.е. выполняемые действия.

Рассматривая определение информационной безопасности, необходимо отметить, что перед существительным «ущерб» стоит прилагательное «неприемлемый». Очевидно, что застраховаться от всех видов ущерба невозможно, тем более, крайне сложно сделать это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но зачастую порог неприемлемости имеет материальное (денежное) выражение, а целью защиты информации становится уменьшение размеров ущерба до допустимых значений. В органах внутренних дел недопустимым ущербом, кроме вышеперечисленного, может являться нарушение режима работы с информацией ограниченного доступа.

Выделяют следующие *виды защиты информации*:

- правовая,
- техническая,
- криптографическая,
- физическая.

*Правовая защита информации* – защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

*Техническая защита информации(ТЗИ)* – защита информации, заключающаяся в обеспечении не криптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в

соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

*Криптографическая защита информации* – защита информации с помощью ее криптографического преобразования.

Здесь используются методы шифровки информации, которые кодируют информацию таким образом, чтобы её содержание было доступно только при предъявлении некоторой специфической информации (ключа). Осуществляться шифрование может либо вручную (что представляет сложную и кропотливую процедуру), либо автоматически, с помощью специальных аппаратных средств (шифраторов) или специального программного обеспечения. Специалисты считают криптографическое закрытие информации наиболее эффективным и надежным средством защиты информации.

*Физическая защита информации* – защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.

К объектам защиты информации могут быть отнесены: охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации.

Оборотной стороной защищенности являются угрозы информационной безопасности.

*Угрозы информационной безопасности* – воздействия на информационную систему, поддерживающую инфраструктуру либо обслуживающий персонал, способные нарушить информационную безопасность.

*Спектр интересов субъектов* информационных правоотношений, связанных с использованием информационных систем, можно разделить на следующие категории:

1. Обеспечение целостности информации.
2. Обеспечение конфиденциальности информации.
3. Обеспечение доступности информации.

Раскроем содержание указанных терминов.

*Целостность* – свойство информации предотвращать несанкционированные создание, модификацию или уничтожение.

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению действий над информацией). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи денежных средств.

Целостность оказывается важнейшим аспектом ИБ в тех случаях, когда информация служит «руководством к действию». Рецептура лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным. Недопустимо и искажение официальной информации, будь то текст закона или страница Web-сервера правительственной организации.

*Конфиденциальность* – свойство информации предотвращать несанкционированное ознакомление или копирование.

Конфиденциальность – самый проработанный у нас в стране аспект информационной безопасности.

*Доступность* – свойство информации, обеспечивающее беспрепятственное обращение к ней для проведения санкционированных операций.

Информационные системы создаются или приобретаются для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений.

### 1.2.2. Угрозы безопасности информации

Существует несколько видов информационной безопасности, но среди них самую важную роль занимает компьютерная безопасность, которая в предмет своего ведения включает сохранение информации на носителях, предотвращение утечек, обеспечение сохранности программ, до-

кументов, сведений, данных и основная задача это защита компьютера от вирусов.

Имеется некая классификация угроз информационной безопасности (ИБ), чтобы разобрать эту классификацию необходимо в первую очередь выявить то, что же действительно влияет на появление угроз ИБ.

Для начала определимся с термином «угроза информационной безопасности» - это те или иные события и процессы, которые несут какое-либо отрицательное воздействие на информацию в целом, а также на её информационную систему. Тем самым они приводят к искажению, утечке, удалению, несанкционированному копированию и т.д. информации.

Угрозы информационной безопасности – понятие обширное и многогранное. Соответственно, и *классификация угроз* может осуществляться по различным критериям:

*1. По возникновению:*

а) естественная угроза, которая вызвана влиянием физических воздействий и (или) стихийных природных явлений (бедствий);

б) искусственная угроза, она вызвана человеческой деятельностью.

*2. По преднамеренности появления:*

а) случайные;

б) преднамеренные (умышленные).

*3. По источнику угрозы:*

а) природная среда (стихийные бедствия, явления);

б) сам человек (разглашение сведений содержащих секретную информацию и данные);

в) программно – аппаратные средства, при том, что они должны быть санкционированными (прекращение работы операционной системы);

г) программно – аппаратные средства, которые несанкционированны (заражение вирусами).

*4. По положению источника угроз:*

а) за пределами контролируемой зоны (перехват и утечка сведений и данных, которые передаются по каналам связи);

б) входящие в контролируемую зону (кража и хищение распечаток, носителей информации – дисков, флэшек и т.д.)

в) находящиеся в самой зоне (неправильное и некорректное использование ресурсов, которые необходимы для работы).

*5. По воздействию:*

а) пассивные (при работе они ничего не меняют в системе и содержании, при этом может произойти угроза копирования сведений, данных и информации);

б) активные (при влиянии изменяют структуру и основу, приводит к внедрению аппаратных и программных вложений).

*6. По этапам доступа пользователей к ресурсам:*

а) угроза (проявляется на этапе доступа к ресурсам и источникам);

б) угроза (проявляется после разрешения доступа).

*7. По месту расположения информации:*

а) угроза доступа к информации на внешних запоминающих устройствах (ВЗУ), копирование с жесткого диска;

б) угроза доступа к информации в оперативной памяти;

в) угроза доступа к информации, которая функционирует по линиям связи (незаконное подключение).

*8. По способу доступа к ресурсам:*

а) угроза, которая использует стандартный путь доступа к ресурсам при помощи паролей (полученные незаконно) или путем использования терминалов, которые принадлежат законным пользователям;

б) угроза, которая использует нестандартный (скрытый) путь доступа, обходя средства защиты.

*9. По степени зависимости от активности:*

а) угроза проявляется независимо от активности (хищение, кража носителей информации);

б) угроза в процессе обработки сведений и данных (распространение, размножение вирусов).

Рассмотрим основные понятия в области угроз безопасности информации.

*Угроза* – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

*Фактор* – явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

*Источник угрозы* – субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

*Уязвимость* (информационной системы) – свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

*Вредоносная программа* – программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы.

*Несанкционированное воздействие на информацию* – воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

*Преднамеренное силовое электромагнитное воздействие на информацию* – несанкционированное воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения (генерирования) в автоматизированных информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования (сбой в работе) технических и программных средств этих систем.

*Модель угроз(безопасности информации)* – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации. Видом описательного представления свойств или характеристик угроз безопасности информации может быть специальный нормативный документ.

### 1.2.3. Основные направления защиты информации

К основным направлениям защиты информации относят защиту:

- от утечки,
- от несанкционированного воздействия,
- от непреднамеренного воздействия,
- от разглашения,
- от несанкционированного доступа.

Каждому из направлений соответствует способ защиты информации.

*Способ защиты информации* – порядок и правила применения определенных принципов и средств защиты информации.

*Защита информации от утечки* – предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также исключение (затруднение) получения защищаемой информации иностранными разведками и другими заинтересованными субъектами.

Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

*Защита информации от несанкционированного воздействия (НСВ)*– предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

*Защита информации от непреднамеренного воздействия* – предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных не целенаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

*Защита информации от разглашения* – предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

*Защита информации от несанкционированного доступа (НСД)* – предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

*Защита информации от преднамеренного воздействия (ПДВ)* – предотвращение преднамеренного воздействия, в том числе

электромагнитного и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях.

*Защита информации от иностранной разведки* – предотвращение получения защищаемой информации иностранной разведкой.

*Цель защиты информации* – предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

*Объект защиты информации* – информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

*Защищаемая информация* – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Собственниками информации могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

*Система защиты информации* – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

*Политика безопасности информации* – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

*Безопасность информации* – состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

*Носитель защищаемой информации* – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

*Защищаемый объект информатизации* – объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.

*Защищаемая информационная система* – информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности.

### 1.3. Информационная безопасность Российской Федерации

Существует ряд органов и подразделений, обеспечивающие информационную безопасность. В зависимости от статуса информационной угрозы (в рамках государственных органов власти или коммерческих организаций) деятельность организуется специальными государственными органами (подразделениями) или отделами (службами) предприятия.

К государственным органам Российской Федерации, контролирующие деятельность в области защиты информации относятся:

– Комитет Государственной Думы по безопасности;

– Совет безопасности России;

– Федеральная служба по техническому и экспортному контролю (ФСТЭК России);

– Федеральная служба безопасности Российской Федерации (ФСБ России);

– Федеральная служба охраны Российской Федерации (ФСО России);

– Служба внешней разведки Российской Федерации (СВР России);

– Министерство обороны Российской Федерации (Минобороны России);

– Министерство внутренних дел Российской Федерации (МВД России);

– Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор);

– Центральный банк Российской Федерации (Банк России).

Службы, организующие защиту информации на уровне предприятия:

– Служба экономической безопасности;

– Служба безопасности персонала (Режимный отдел);

– Кадровая служба;

– Служба информационной безопасности.

Концептуальные основы обеспечения информационной безопасности нашей страны изложены в «Доктрине информационной безопасности Российской Федерации»[1]. Указанный документ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности государства.

В «Доктрине…» на основе анализа состояния информационной безопасности Российской Федерации определены цели, задачи и ключевые проблемы ее обеспечения, объекты обеспечения информационной безопасности и соответствующие угрозы, методы предотвращения и нейтрализации этих угроз, а также основные положения государственной политики, намечены первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.

*Защищаемая информация* – информация, которая является предметом собственности и подлежит защите в соответствии с требованиями правовых документов.

Защиту информации не следует понимать как информационную безопасность, это совсем разные понятия.

Под защитой информации понимается принятие правовых, организационных и технических мер, которые направлены, во – первых, на обеспечение защиты информации от неправомерного доступа, модифицирования, уничтожения, копирования, блокирования, распространения, предоставления, а также от иных неправомерных действий по отношению к информации, во – вторых, на соблюдение конфиденциальности (секретности) информации ограниченного доступа и в – третьих, на реализацию права к информационному доступу.

*Под информационной безопасностью Российской Федерации* понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

[1] Доктрина информационной безопасности Российской Федерации: утв. Президентом РФ 09.09.2000 №Пр-1895 // Российская газета. 2000. № 187.

Система национальных интересов Российской Федерации[1] определяется совокупностью следующих основных интересов:

- *личности* – реальное обеспечение конституционных прав и свобод, личной безопасности, повышение качества и уровня жизни, физическое, духовное и интеллектуальное развитие;

- *общества* – упрочение демократии, достижение и поддержание общественного согласия, повышение созидательной активности населения и духовное возрождение России;

- *государства* – защита конституционного строя, суверенитета и территориальной целостности, установление политической, экономической и социальной стабильности, безусловное исполнение законов и поддержание правопорядка, развитие международного сотрудничества на основе партнерства.

Применительно к информационной сфере эти интересы заключаются в следующем:

- *личности* – реализация конституционных прав человека и гражданина на доступ к информации, использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, защита информации, обеспечивающей личную безопасность;

- *общества* – обеспечение интересов личности, упрочение демократии, создание правового социального государства, достижение и поддержание общественного согласия, духовное возрождение России;

- *государства* – создание условий для гармоничного развития российской информационной инфраструктуры, реализация конституционных прав и свобод человека и гражданина в процессе получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, безусловное обеспечение законности и правопорядка, развитие равноправного и взаимовыгодного сотрудничества.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи

[1] О Стратегии национальной безопасности Российской Федерации до 2020 года: Указ Президента РФ от 12.05.2009 №537 // Российская газета. 2009. №88.

внутренней и внешней политики государства по обеспечению информационной безопасности.

Доктрина определила *четыре основные составляющие национальных интересов* Российской Федерации в информационной сфере:

1. Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

2. Информационное обеспечение государственной политики РФ, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

3. Развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

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

Для реализации этих составляющих в рамках государственной политики необходимо:

- повысить безопасность информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и информационных систем органов государственной власти, финансово-

кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;

- интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью;
- обеспечить защиту сведений, составляющих государственную тайну;
- расширять международное сотрудничество Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

По своей общей направленности *угрозы информационной безопасности Российской Федерации подразделяются на следующие виды*:

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- угрозы информационному обеспечению государственной политики РФ;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние.

Отдельные разделы Доктрины посвящены основам государственной политики обеспечения информационной безопасности.

## 1.4. Защита информации как обеспечение информационной безопасности и безопасности информации

Проблема надежного обеспечения сохранности информации является одной из важнейших проблем современности.

Особенностями современных информационных технологий являются:

- увеличение числа автоматизированных процессов в системах обработки данных и важность принимаемых на их основе решений;
- территориальная разнесённость компонентов компьютерных систем и передача информации между этими компонентами;
- усложнение программных и аппаратных средств компьютерных систем;
- накопление и длительное хранение больших массивов данных на электронных носителях;
- интеграция в единую базу данных информации различной направленности;
- непосредственный доступ к ресурсам компьютерной системы большого количества пользователей различной категории и с различными правами доступа в системе;
- рост стоимости ресурсов компьютерных систем.

Рост количества и качества угроз безопасности информации в компьютерных системах не всегда ведет к адекватному ответу на создание надежной системы и безопасных информационных технологий. В большинстве коммерческих и государственных организаций, не говоря о простых пользователях, в качестве средств защиты используются только антивирусные программы и разграничение прав доступа пользователей на основе паролей.

Системный подход к описанию информационной безопасности предлагает выделить следующие составляющие информационной безопасности:

- Законодательная, нормативно-правовая и научная база.
- Структура и задачи органов (подразделений), обеспечивающих безопасность ИТ.
- Организационно-технические и режимные меры и методы (политика информационной безопасности).

- Программно-технические способы и средства обеспечения информационной безопасности.

Целью реализации информационной безопасности какого-либо объекта является построение системы обеспечения информационной безопасности данного объекта (СОИБ). Для построения и эффективной эксплуатации СОИБ необходимо проведение следующих этапов:

1. Выявить требования защиты информации, специфические для данного объекта защиты.
2. Учесть требования национального и международного законодательства.
3. Использовать наработанные практики (стандарты, методологии) построения подобных СОИБ.
4. Определить подразделения, ответственные за реализацию и поддержку СОИБ.
5. Распределить между подразделениями области ответственности в осуществлении требований СОИБ.
6. На базе управления рисками информационной безопасности определить общие положения, технические и организационные требования, составляющие политику информационной безопасности объекта защиты.
7. Реализовать требования политики информационной безопасности, внедрив соответствующие программно-технические способы и средства защиты информации.
8. Реализовать систему менеджмента (управления) информационной безопасности (СМИБ).
9. Используя СМИБ, организовать регулярный контроль эффективности СОИБ и при необходимости пересмотр и корректировку СОИБ и СМИБ.

## 1.5 Обеспечение безопасности ведомственной информации, информационных ресурсов, средств и систем информатизации

Под средствами информатизации, как в обычных организациях, так и в специализированных ведомствах подразумеваются ПК (персональные, офисные, мобильные компьютеры и рабочие станции), системы автоматизированного проектирования, в том числе автоматизированные

системы и рабочие места, а также их утилиты, миниПК и носители информации. Системами информатизации чаще называются локальные вычислительные сети (ЛВС) и глобальные вычислительные сети (ГВС). Все они используются различными ведомствами РФ, в том числе МВД. Их техническая защита является одним из важных инструментов политики обеспечения безопасности ведомственной информации.

Комплексный подход к защите всех средств и систем информатизации предполагает объединение всех вышеперечисленных компонентов в единую информационную систему в пределах ведомства, ее контроль и охрану. Контроль и охрана могут осуществляться посредством аппаратно-программного комплекса (VPN) для создания частных виртуальных сетей. Использование VPN позволяет решить две основные проблемы (защиту ЛВС от несанкционированного доступа из ГВС и защиту передаваемой через ГВС информации), возникающие при применении общедоступных каналов связи или ГВС, следующим образом: вся передаваемая между удаленными ЛВС через ГВС информация зашифровывается, кроме того, обмен информацией принципиально возможен только между зарегистрированными в системе ЛВС или отдельными компьютерами. ЛВС и ее топология изолируются от ГВС.

Можно выделить *три аспекта уязвимости* информации в ОВД:

1. Подверженность физическому уничтожению.

2. Возможность несанкционированной (случайной или злоумышленной) модификации (изменения).

3. Опасность несанкционированного (случайного или преднамеренного) получения информации посторонними лицами.

В настоящее время системы защиты информации разрабатываются по *двум направлениям*:

- Обеспечение достоверности и целостности передачи информации. Используются методы помехоустойчивого кодирования (коды Грея, Шеннона и др.) и помехоустойчивого приема.
- Защита информации от несанкционированного доступа, преднамеренного искажения или разрушения.

Отечественный и зарубежный опыт защиты информации показывает, что эффективной может быть лишь комплексная система защиты, сочетающая следующие меры.

## 1.6. Меры защиты информации: виды, достоинства и недостатки

### 1.6.1. Меры защиты информации

По способам осуществления все меры защиты информации, ее носителей и систем ее обработки подразделяются на:

- правовые (законодательные);
- морально-этические;
- технологические;
- организационные (административные и процедурные);
- физические;
- технические (аппаратурные и программные).

**Правовые меры защиты информации**

Правовые меры защиты информации представляют собой разработку и применение системы правовых норм, регулирующих общественные отношения в информационной сфере.

Возникновение и развитие информационного общества обусловило возникновение новой отрасли права – информационного права, регулирующего общественные отношения в информационной сфере.

*Информационное право* – система социальных норм и отношений, охраняемых силой государства, возникающих в информационной сфере – сфере производства, преобразования и потребления информации.

Информационное право как отдельная отрасль права осуществляет регулирование общественных отношений в информационной сфере – информационных отношений.

*Информационные отношения* – обособленная однородная группа общественных отношений, возникающих при обращении информации в информационной сфере в результате осуществления информационных процессов в порядке реализации каждым информационных прав и свобод, а также в порядке исполнения органами государственной власти и местного самоуправления своих обязанностей по обеспечению гарантий информационных прав и свобод.

Их основной особенностью является то, что они возникают, развиваются и прекращаются в информационной сфере при обращении

информации. Кроме того, в ходе информационных отношений реализуется государственная политика в информационной сфере, а также применяются все методы правового регулирования, присущие российскому праву.

Как и любая отрасль права, информационное право имеет свои принципы, основывающиеся на конституционных нормах, закрепляющих информационные права и свободы и гарантирующих их осуществление, а также на особенностях и юридических свойствах информации как объекта правоотношений.

Выделяют следующие принципы информационного права:

- *Приоритетности прав личности*. Этот принцип устанавливается Конституцией РФ, где утверждается, что обязанность государства – признание, соблюдение и защита прав и свобод человека и гражданина. В соответствии с данным принципом органам государственной власти предписывается защищать права и свободы человека и гражданина в информационной сфере.

- *Свободного производства и распространения любой информации, не ограниченной федеральным законом*. Этот принцип определяет, что ограничение информационной свободы возможно только федеральным законом лишь в целях и интересах личности, общества, государства.

- *Запрещения производства и распространения информации, вредной и опасной для личности, общества, государства*. Этот принцип направлен на защиту интересов и свобод личности, общества, государства от воздействия вредной и опасной информации.

- *Гласности*. Этот принцип заключается в том, что государственные организации не имеют права вводить ограничения по доступу к информации, которой они обладают в соответствии с установленной компетенцией, если эта информация затрагивает права и свободы человека и гражданина либо представляет общественный интерес.

- *Полноты обработки и оперативности предоставления информации*. Любой государственный орган или орган местного самоуправления обязан собирать, накапливать и хранить информацию в полном объеме в соответствии с установленной компетенцией, а также предоставлять потребителям запрашиваемую информацию в установленные сроки.

- *Законности*. Субъекты информационного права обязаны строго соблюдать Конституцию РФ и законодательство РФ.

- *Ответственности*. Этот принцип означает обязательное наступление ответственности за нарушение требований и предписаний информационно-правовых норм.

- *Оборотоспособности информации*. Оборотоспособность информации позволяет осуществлять гражданский оборот информации.

- *Отчуждения информации от ее создателя*. Этот принцип основывается на обособляемости информации – ее фиксирования на материальном носителе и дальнейшем распространении независимо от создателя.

- *Информационного объекта*. Этот принцип позволяет осуществлять правовое регулирование оборота информационных продуктов и определяет необходимость защиты интеллектуальной собственности.

- *Распространяемости информации*. Одна и та же информация может копироваться в неограниченном количестве экземпляров без изменения содержания, при этом информация может принадлежать неограниченному кругу субъектов, права которых могут существенно отличаться.

- *Организационной формы*. Для осуществления оборота информации она должна иметь определенную организационную форму.

- *Экземплярности информации*. При распространении информации в виде документов или информационных продуктов возможно осуществить учет и регистрацию отдельных экземпляров. Этот принцип позволяет осуществлять оборот информации ограниченного доступа.

Все субъекты информационного права в зависимости от своей организационной формы подразделяются на три группы:

1. Государственные и муниципальные органы власти, организации, предприятия, учреждения.

2. Негосударственные (в том числе иностранные) организации.

3. Физические лица.

В зависимости от роли, выполняемой в информационной сфере, субъекты информационных правоотношений подразделяются на производителей, обладателей и потребителей информации.

Информационное право состоит из множества отдельных информационно-правовых норм, которые составляют общую и особенную части информационно права.

К общей части относятся нормы, закрепляющие общие принципы, формы и методы правового регулирования деятельности в информационной сфере.

Особенная часть информационного права охватывает нормы, регулирующие отношения в области обращения открытой информации и информации ограниченного доступа, а также информационной безопасности.

Поскольку информационные отношения затрагивают все сферы жизнедеятельности общества, информационное право является комплексной областью права и взаимодействует практически со всеми прочими отраслями права. Наиболее тесно оно взаимодействует с конституционным правом, так как основано на конституционных нормах и затрагивает деятельность представительных и исполнительных органов власти.

Кроме того, при регулировании имущественных отношений и личных неимущественных отношений по поводу информации и информационных объектов информационное право неизбежно взаимодействует с гражданским правом. Отдельно следует отметить такой аспект взаимодействия, как взаимодействие по поводу вопросов интеллектуальной собственности.

Взаимодействие с административным правом выражается в том, что информационное право использует административно-правовые нормы при установлении ответственности за правонарушения в информационной сфере, регулировании деятельности субъектов в данной сфере, а также в том, что они используют одинаковый метод правового регулирования отношений, возникающих при осуществлении органами государственной власти и местного самоуправления обязанностей в области массовой информации, библиотечного и архивного дела, формирования государственных информационных ресурсов.

Информационное право взаимодействует также с уголовным правом, которое устанавливает ответственность за преступления в информационной сфере и нарушения норм информационного законодательства.

Источниками информационного права в соответствии с уровнем принятия законодательных и нормативных актов являются:

1. Конституция РФ.

2. Федеральные законы, регламентирующие деятельность в информационной сфере. Пример: Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Указы Президента РФ, постановления Правительства РФ, нормативные акты федеральной исполнительной власти. Пример: постановление Правительства РФ от 02.06.2008 №418 «О Министерстве связи и массовых коммуникаций Российской Федерации».

4. Законодательные и нормативные акты органов государственной власти субъектов РФ. Пример: Закон Белгородской области от 17.12.2009 №317 «О порядке утверждения перечней информации о деятельности государственных органов Белгородской области, размещаемой в сети Интернет».

5. Акты органов местного самоуправления. Пример: решение Совета депутатов г. Белгорода от 29.12.2009 №307 «О порядке организации доступа к информации о деятельности Совета депутатов города Белгорода и председателя Совета депутатов города Белгорода».

В соответствии с областью правового регулирования, источники информационного права подразделяются на:

- законодательство о праве на доступ к информации. Основано на конституционных нормах. Специального законодательного акта по этим вопросам не принято. Отдельные вопросы регулируются федеральными законами в области библиотечного и архивного дела, международных отношений и т.д.;

- законодательство о документированной информации. Основано на Федеральном законе от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации». Отдельные вопросы регулируются законодательными актами о культуре, об электронной цифровой подписи, об обязательном экземпляре документов и т.д.;

- законодательство о гражданском обороте информации. Осуществляется в соответствии с Гражданским кодексом РФ. Отдельные

вопросы оборота открытой информации регламентируются административным законодательством;

- законодательство об информационных системах, информационных технологиях и средствах их обеспечения. Основано на Федеральном законе от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федеральном законе от 07.07.2003 №126-ФЗ «О связи». Отдельные вопросы регулируются нормами административного, финансового и муниципального права;

- законодательство об информационной безопасности. Основано на «Доктрине информационной безопасности», Федеральном законе от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федеральном законе от 05.03.1992 №2446-1 «О безопасности». Отдельные вопросы регулируются законодательными и нормативными актами об информации ограниченного доступа, административным и уголовным законодательством;

- законодательство об интеллектуальной собственности. Основано на Гражданском кодексе РФ и ряде федеральных законов;

- законодательство о средствах массовой информации. Основано на конституционных нормах и Федеральном законе от 27.12.1991 №2124-1 «О средствах массовой информации». Отдельные вопросы регулируются нормами административного, финансового, муниципального законодательства;

- законодательство о библиотечном деле. Основано на Федеральном законе от 29.12.1994 №78-ФЗ «О библиотечном деле», аналогичных законодательных актах субъектов РФ. Отдельные вопросы регулируются нормами административного, финансового и муниципального законодательства;

- законодательство об архивном деле. Основано на Федеральном законе от 22.10.2004 №125-ФЗ «Об архивном деле», аналогичных законодательных актах субъектов РФ. Отдельные вопросы регулируются нормами административного, финансового и муниципального законодательства;

- законодательство о государственной тайне. Основано на Федеральном законе от 28.12.2010 №390-ФЗ «О безопасности» и Федеральном законе от 21.07.1993 №5485-1 «О государственной тайне».

Отдельные вопросы регулируются нормами административного и уголовного законодательства;

- законодательство о коммерческой, профессиональной и служебной тайне. Основано на Федеральном законе от 29.07.2004 №98-ФЗ «О коммерческой тайне», Гражданском кодексе РФ. Отдельные вопросы регулируются нормами гражданского, административного, финансового и муниципального законодательства;

- законодательство о персональных данных. Основано на конституционных нормах и Федеральных законах от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» и от 27.07.2006 №152-ФЗ «О персональных данных». Отдельные вопросы регулируются нормами административного и финансового законодательства.

Опираясь на законодательство Российской Федерации в области информационной безопасности необходимо подчеркнуть, что основным законом в Российской Федерации считается Конституция РФ от 12 декабря 1993 года. В ст. 24 Конституции – органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Ст. 23 Конституции гарантирует право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, ст. 29 – право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к средствам защиты информации. Ст. 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, ст. 42 – право на знание достоверной информации о состоянии окружающей среды. [1]

В сентябре 2000 г. Президент Российской Федерации Владимир Владимирович Путин утвердил «Доктрину информационной безопасности». Доктрина закрепляет основы информационной политики государст-

[1] Конституция Российской Федерации. – М., 2015.

ва. С учетом существующих угроз для защиты национальных интересов России. [1]

В Гражданском кодексе Российской Федерации согласно ст. 139, «информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности». Это подразумевает, как минимум, компетентность в вопросах ИБ и наличие доступных (и законных) средств обеспечения конфиденциальности. [2]

В Уголовном кодексе Российской Федерации глава 28 «Преступления в сфере компьютерной информации» содержит 3 статьи: ст. 272 «Неправомерный доступ к компьютерной информации»; ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ»; ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети». Ст. 138 УК РФ, защищая конфиденциальность (секретность) персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет ст. 183 УК РФ.[3] Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Законе «О государственной тайне» (с изменениями и дополнениями от 8 марта 2015 года). В нем государственная тайна определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. А также дается определение средств защиты информации.

Согласно данному Закону, это технические, криптографические, программные и другие средства, которые предназначены для защиты све-

---

[1] Доктрина информационной безопасности Российской Федерации: утв. Президентом РФ 09.09.2000 №Пр-1895 // Российская газета. 2000. № 187.

[2] Гражданский кодекс РФ. - М., 2015.

[3] Уголовный кодекс Российской Федерации. - М., 2015.

дений и составляют государственную тайну; средства, в которых они реализованы и средства контроля эффективности защиты информации. [1]

Таким образом, информационное законодательство носит комплексный характер и затрагивает практически все области жизнедеятельности общества. Суть правового обеспечения информационной безопасности заключается в том, что посредством законодательных и нормативных правовых актов закрепляется порядок регулирования информационных отношений и ответственность за нарушения в информационной сфере.

Меры обеспечения информационной безопасности подразделяются на организационные, технические, экономические и правовые.

## Организационные меры защиты информации

Как было сказано выше, организационные меры защиты информации – это деятельность по регламентации действий сотрудников организации, направленная на обеспечение информационной безопасности.

Основное содержание организационных мер защиты информации – планирование, финансирование, контроль и анализ выполнения мероприятий. Это могут быть самые разные мероприятия, направленные на разработку регламентов создания и использования информационных систем, организацию поддерживающей инфраструктуры и обеспечение ее бесперебойного функционирования, работу с обслуживающим персоналом.

Организационные меры базируются на соответствующей правовой основе и являются ее логическим продолжением.

Основные регламентирующие документы, относящиеся к обеспечению защиты информационной системы, должны быть разработаны еще до создания самой информационной системы. В дальнейшем в процессе жизненного цикла системы, вплоть до этапа выведения системы из эксплуатации, организационные меры защиты реализуются посредством новых документов, описывающих действия обслуживающего персонала в тех или иных ситуациях.

---

[1] О государственной тайне: Федеральный закон от 21 июня 1993 г. № 5485-I // Российская газета. 1993. №182.

В соответствии с направленностью организационные меры защиты можно классифицировать следующим образом:

1. Направленные на обеспечение работы поддерживающей инфраструктуры. Это мероприятия, осуществляемые при проектировании, строительстве и эксплуатации зданий и сооружений, выделение и аттестация помещений и рабочих зон для работы с конфиденциальной информацией и т.д.

2. Направленные на обеспечение работы информационной системы. К этому классу мер можно отнести разработку технологических инструктивных документов, определение порядка резервного копирования информации, требований к используемым аппаратным и программным средствам и т.д.

3. Направленные на работу с персоналом организации. Сюда относятся мероприятия, проводимые при подборе и обучении кадров, правила поведения сотрудников, владеющих ценной информацией, формирование и организация работы подразделения по защите информации, физическая охрана особо ценных сотрудников и т.д.

Главная цель организационных мер защиты информации – формирование программы действий в области информационной безопасности и обеспечение ее выполнения посредством выделения необходимых ресурсов и контроля текущего состояния.

Особое место среди организационных мер защиты информации занимает разработка политики безопасности.

*Политика безопасности* – совокупность документов, описывающих цели защиты информации, риски информационной системы с точки зрения обеспечения информационной безопасности и общий порядок действий, направленных на ликвидацию либо минимизацию таких рисков.

На основе целей, определенных в политике безопасности, разрабатывается программа обеспечения информационной безопасности.

*Программа должна обеспечивать эффективное противодействие угрозам в соответствии с четырехуровневой моделью защиты*:

- Уровень 1. *Предотвращение*. Цель данного уровня – не допустить нарушение информационной безопасности. Примерами мероприятий этого уровня могут служить организация пропускного режима в целях предотвращения несанкционированного доступа к информации, определение требований к сложности пароля на вход в систему,

поддержание требуемого температурного режима в помещениях с вычислительной техникой для предотвращения перегрева и выхода из строя аппаратных устройств, обеспечение проверки получаемых из сторонних информационных систем данных для предотвращения несанкционированной модификации информации, обучение и периодическая проверка знаний сотрудников и т.д.

- Уровень 2. *Обнаружение*. Цель данного уровня – обеспечить своевременное обнаружение нарушений информационной безопасности и оперативное реагирование. Примеры мероприятий по организации обнаружения нарушений безопасности: установка охранно-пожарной сигнализации, контроль персонала и т.д.

- Уровень 3. *Ограничение*. Цель мероприятий по ограничению нарушений безопасности – минимизация ущерба, полученного вследствие наступления нештатной ситуации. Примеры мероприятий данного уровня: отключение компьютера, зараженного вредоносной программой, от сети организации, отключение водоснабжения в здании в случае аварии водопровода, увольнение скомпрометировавшего себя сотрудника или перевод его на другую должность и т.д.

- Уровень 4. *Восстановление*. Цель мероприятий этого уровня – восстановление нормального функционирования информационной системы после ликвидации нарушения безопасности. Примеры: восстановление базы данных из резервной копии, замена неисправных устройств аппаратной части информационной системы или поддерживающей инфраструктуры, переход на использование новых каналов связи взамен нефункционирующих или небезопасных и т.д.

Программа обеспечения информационной безопасности должна быть сформулирована предельно конкретно – кто, в каких случаях и что должен делать. Каждое действие по защите информации должно быть регламентировано. Кроме того, необходимо пересматривать содержание программы в случае модификации структуры информационной системы, внедрения новых технологий, изменения штатной структуры организации и т.п. Целесообразно также проводить учения и тренировки с целью отработки персоналом действий в случае нарушений информационной безопасности.

Организационные меры защиты являются решающим звеном формирования и реализации комплексного обеспечения информационной безопасности.

**Морально-этические**

К морально-этическим мерам защиты относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как требования нормативных актов, однако их несоблюдение ведет обычно к падению авторитета или престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав, кодекс чести и т.п.) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах пользователей и обслуживающего персонала АС.

**Технологические**

К данному виду мер защиты относятся разного рода технологические решения и приемы, основанные обычно на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий. Примером таких мер является использование процедур двойного ввода ответственной информации, инициализации ответственных операций только при наличии разрешений от нескольких должностных лиц, процедур проверки соответствия реквизитов исходящих и входящих сообщений в системах коммутации сообщений, периодическое подведение общего баланса всех банковских счетов и т.п.

## Меры физической защиты

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также средств визуального наблюдения, связи и охранной сигнализации.

Это - замки на дверях, решетки на окнах, различные механические, электромеханические и электронные устройства охраны здания и охранной сигнализации и т.д.

К данному типу относятся также меры и средства контроля физической целостности компонентов АС (пломбы, наклейки и т.п.).

Физические меры защиты, как правило, применяются в совокупности с административными мероприятиями, которые включают в себя меры по организации соответствующего режима секретности, пропускного и внутреннего режима и т.д.

## Технические

Технические меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав АС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты.

К *техническим* мерам защиты относится использование разнообразных механических, электромеханических, электронных, оптических, радиолокационных и других устройств и систем, которые способны самостоятельно либо в совокупности с другими средствами выполнять функции защиты информации. К ним относятся, например, технические средства защиты от побочных электромагнитных излучений, защитное зашумление, средства охранного освещения, обнаружения, наблюдения, сигнализации и др. Они дополняют физические и административные меры и позволяют значительно повысить её эффективность.

Взаимосвязь рассмотренных выше мер обеспечения безопасности приведена на рисунке 2.

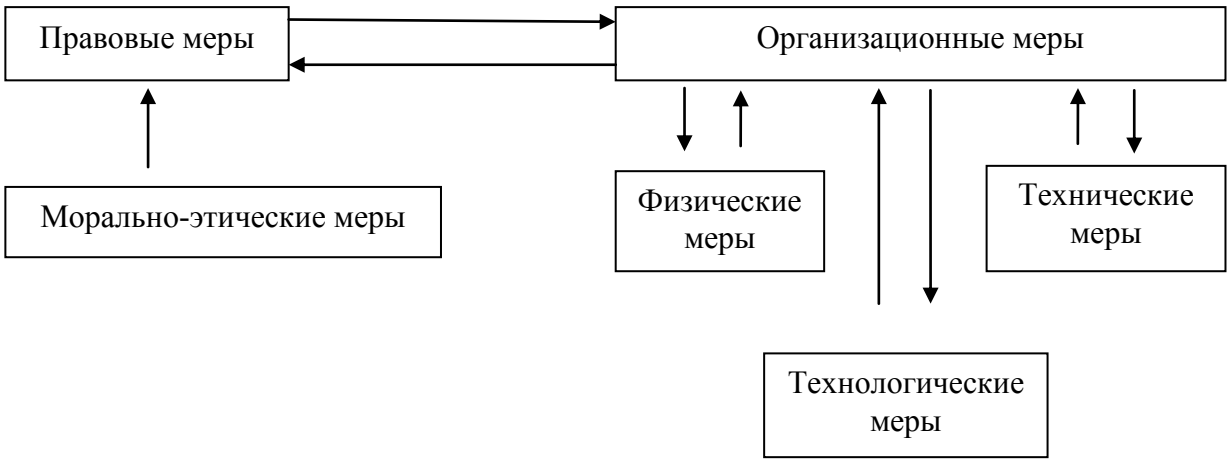


Рис. 2. Взаимосвязь мер обеспечения информационной безопасности

*Программные* меры являются средством защиты информации, находящейся в компьютере. Системы защиты компьютера должны позволять пользователю при соответствующем контроле получать доступ к вычислительной технике и хранимой в ней информации. Для защиты от чужого вторжения следует предусмотреть меры непосредственной защиты вычислительных устройств и информации от несанкционированного доступа.

Основными функциями, которые должны осуществлять средства защиты, являются:

- идентификация субъектов и объектов;
- разграничение (иногда полная изоляция) доступа к вычислительным ресурсам и информации;
- регистрация действий в системе.

Процедура идентификации и подтверждения подлинности предполагает проверку, является ли субъект, осуществляющий доступ (или объект, к которому осуществляется доступ), тем, за кого себя выдаёт. В процессе идентификации используются различные методы: простые, сложные или одноразовые пароли, обмен вопросами и ответами с администратором или через соответствующую программу, использование различных опознавательных элементов (ключ, кодовая карточка, удостоверение личности, жетон, фотоснимок лица), методы

биометрической идентификации личности (по отпечаткам пальцев, размеру и отпечатку ладони, сетчатке глаза) и т.д.

*Разграничение доступа* к вычислительным ресурсам и информации осуществляется на трех уровнях:

- аппаратуры;
- программного обеспечения;
- данных.

Защита на уровнях аппаратуры и программного обеспечения предусматривает управление доступом к таким вычислительным ресурсам, как отдельные устройства, оперативная память, операционная система, специальные служебные и личные программы пользователя.

Защита информации на уровне данных направлена на:

- защиту информации при передаче по каналам между различными ЭВМ;
- обеспечение доступа только к разрешённым данным, хранимым в ЭВМ, и выполнение только допустимых операций над ними.

Для защиты информации при передаче является целесообразным шифрование данных перед вводом в канал связи и расшифровывание на выходе из него.

Управление доступом к информации позволяет ответить на вопросы: кто может выполнять, какие операции и над какими данными. Объектом, доступ к которому контролируется, может выступать файл, запись в файле или отдельное поле записи файла, а в качестве факторов, влияющих на принятие решения о доступе, - внешнее событие, значение данных, состояние системы, полномочия пользователя и т.д.

Доступ, управляемый событием, предусматривает блокировку обращения пользователя, например, в определенные интервалы времени или при обращении с определённого терминала. Доступ, зависящий от состояния, осуществляется в зависимости от текущего состояния вычислительной системы, управляющих программ и системы защиты. Например, может быть запрещён доступ к файлу, если диск не находится в состоянии «Только чтение». Доступ, управляемый значением, открывает путь к данным в зависимости от их текущего значения.

Что касается доступа, зависящего от полномочий, то он предусматривает обращение пользователя к программам, данным, оборудованию в зависимости от предоставленного режима. Например,

субъекту может быть разрешено «Только чтение», «Только выполнение» и др.

Другой подход к построению средств защиты доступа основан на контроле информационных потоков и разделении субъектов и объектов доступа на классы секретности. Средства контроля должны разрешать поток информации для чтения, если уровень информационного объекта-источника соответствует или не превосходит категорию субъекта-получателя информации, и для записи, если категория субъекта-источника соответствует или превышает уровень секретности информационного объекта.

Средства регистрации, как и средства контроля доступа, относятся к эффективным мерам противодействия несанкционированным действиям. Однако, если средства контроля доступа предназначены для предотвращения таких действий, то задача регистрации - обнаружить уже совершенные действия или их попытки.

### 1.6.2. Достоинства и недостатки различных видов мер защиты

**Законодательные и морально-этические меры**

Эти меры определяют правила обращения с информацией и ответственность субъектов информационных отношений за их соблюдение.

Законодательные и морально-этические меры противодействия являются универсальными в том смысле, что принципиально применимы для всех каналов проникновения и НСД к АС и информации. В некоторых случаях они являются единственно применимыми, как например, при защите открытой информации от незаконного тиражирования или при защите от злоупотреблений служебным положением при работе с информацией.

**Организационные меры**

Очевидно, что в организационных структурах с низким уровнем правопорядка, дисциплины и этики ставить вопрос о защите информации просто бессмысленно. Прежде всего надо решить правовые и организационные вопросы.

Организационные меры играют значительную роль в обеспечении безопасности компьютерных систем. Организационные меры - это

единственное, что остается, когда другие методы и средства защиты отсутствуют или не могут обеспечить требуемый уровень безопасности. Однако это вовсе не означает, что систему защиты необходимо строить исключительно на их основе, как это часто пытаются сделать чиновники, далекие от технического прогресса.

Этим мерам присущи серьезные недостатки, такие, как:

• низкая надежность без соответствующей поддержки физическими, техническими и программными средствами (люди склонны к нарушению любых установленных дополнительных ограничений и правил, если только их можно нарушить);

• дополнительные неудобства, связанные с большим объемом рутинной и формальной деятельности.

Организационные меры необходимы для обеспечения эффективного применения других мер и средств защиты в части, касающейся регламентации действий людей. В то же время организационные меры необходимо поддерживать более надежными физическими и техническими средствами.

**Физические и технические средства защиты**

Физические и технические средства защиты призваны устранить недостатки организационных мер, поставить прочные барьеры на пути злоумышленников и в максимальной степени исключить возможность неумышленных (по ошибке или халатности) нарушений регламента со стороны персонала и пользователей системы.

Рассмотрим известное утверждение о том, что создание абсолютной (то есть идеально надежной) системы защиты принципиально невозможно.

Даже при допущении возможности создания абсолютно надежных физических и технических средств защиты, перекрывающих все каналы, которые необходимо перекрыть, всегда остается возможность воздействия на персонал системы, осуществляющий необходимые действия по обеспечению корректного функционирования этих средств (администратора АС, администратора безопасности и т.п.). Вместе с самими средствами защиты эти люди образуют так называемое "ядро безопасности". В этом случае стойкость системы безопасности будет определяться стойкостью персонала из ядра безопасности системы, и

повышать ее можно только за счет организационных (кадровых) мероприятий, законодательных и морально-этических мер.

Но даже имея совершенные законы и проводя оптимальную кадровую полигику, все равно проблему защиты до конца решить не удастся.

Во-первых, потому, что вряд ли удастся найти персонал, в котором можно было быть абсолютно уверенным, и в отношении которого невозможно было бы предпринять действия, вынуждающие его нарушить запреты.

Во-вторых, даже абсолютно надежный человек может допустить случайное, неумышленное нарушение.

## 1.7. Основные принципы построения системы защиты ресурсов автоматизированных систем

Построение системы обеспечения безопасности информации в автоматизированных системах (АС) и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность
- системность
- комплексность
- непрерывность
- своевременность
- преемственность и непрерывность совершенствования
- разумная достаточность
- персональная ответственность
- разделение функций
- минимизация полномочий
- взаимодействие и сотрудничество
- гибкость системы защиты
- открытость алгоритмов и механизмов защиты
- простота применения средств защиты
- научная обоснованность и техническая реализуемость
- специализация и профессионализм
- взаимодействие и координация
- обязательность контроля

**Законность.** Предполагает осуществление защитных мероприятий и разработку системы безопасности информации в АС в соответствии с действующим законодательством в области информации, информатизации и защиты информации, других нормативных актов по безопасности, утвержденных органами государственной власти в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией.

**Системность.** Системный подход к защите информации в АС предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения информационной безопасности в АС.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей, пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

**Комплексность.** Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонированно. Внешняя защита должна обеспечиваться физическими средствами, организационными, технологическими и правовыми мерами.

Одним из наиболее укрепленных рубежей призваны быть средства защиты, реализованные на уровне операционных систем (ОС) СВТ в силу того, что ОС - это та часть компьютерной системы, которая управляет использованием всех ее ресурсов. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

**Непрерывность защиты.** Защита информации - не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а *непрерывный целенаправленный процесс*, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления ее функционирования.

**Своевременность.** Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите АС и реализацию мер обеспечения безопасности информации на ранних стадиях разработки АС в целом и ее системы защиты информации в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

**Преемственность и совершенствование.** Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования АС и ее системы защиты с учетом изменений в методах и средствах перехвата информации и воздействия на компоненты АС, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

**Разделение функций.** Принцип разделения функций требует, чтобы ни один сотрудник организации не имел полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Все такие

операции должны быть разделены на части, и их выполнение должно быть поручено различным сотрудникам. Кроме того, необходимо предпринимать специальные меры по недопущению сговора и разграничению ответственности между этими сотрудниками.

**Разумная достаточность (экономическая целесообразность, сопоставимость возможного ущерба и затрат).** Предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы АС, в которой эта информация циркулирует. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока информация находится в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов компьютерной системы и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

**Персональная ответственность.** Предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

**Минимизация полномочий.** Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью. Доступ к информации должен

предоставляться только в том случае и объеме, в каком это необходимо сотруднику для выполнения его должностных обязанностей.

**Взаимодействие и сотрудничество.** Предполагает создание благоприятной атмосферы в коллективах подразделении. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений обеспечения безопасности информации.

**Гибкость системы защиты.** Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на уже работающую систему, не нарушая процесса ее нормального функционирования. Кроме того, внешние условия и требования с течением времени меняются. В таких ситуациях свойство гибкости системы защиты избавляет владельцев АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

**Открытость алгоритмов и механизмов защиты.** Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это однако не означает, что информация о конкретной системе защиты должна быть общедоступна.

**Простота применения средств защиты.** Механизмы зашиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

**Научная обоснованность и техническая реализуемость.** Информационные технологии, технические и программные средства,

средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации.

**Специализация и профессионализм.** Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственные лицензии на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными сотрудниками (специалистами подразделений обеспечения безопасности информации).

**Взаимодействие и координация.** Предполагают осуществление мер обеспечения безопасности информации на основе взаимодействия всех заинтересованных министерств и ведомств, предприятий и организаций при разработке и функционировании АС и ее системы защиты информации, подразделений и специалистов органов МВД специализированных предприятий и организаций в области защиты информации, привлеченных для разработки системы защиты информации в АС, координации их усилий для достижения поставленных целей Гостехкомиссией России (на этапе разработки и внедрения АС) и подразделениями безопасности органов МВД (на этапе функционирования системы).

**Обязательность контроля.** Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства зашиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

## 1.8. Ответственность за совершение информационных и компьютерных преступлений

В РФ законодательством предусмотрена административная и уголовная ответственность за преступления в информационной сфере.

В УК РФ вопросам ответственности за информационные и компьютерные преступления посвящены статьи 272-274.

*Статья 272. Неправомерный доступ к компьютерной информации*

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

*Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ*

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

*Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети*

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок до четырех лет.

Кодекс об административных правонарушениях РФ также содержит ряд статей, определяющих административную ответственность при совершении ряда нарушений.

Рассмотрим соответствующие статьи КоАП РФ.

*Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)*

1. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) - влечет предупреждение или наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц - от пяти до десяти минимальных размеров оплаты труда; на юридических лиц - от пятидесяти до ста минимальных размеров оплаты труда.

*Статья 13.12. Нарушение правил защиты информации*

2. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), - влечет наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц - от пяти до десяти минимальных размеров оплаты труда; на юридических лиц - от пятидесяти до ста минимальных размеров оплаты труда.

3. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты

информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), - влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от десяти до двадцати минимальных размеров оплаты труда; на юридических лиц - от ста до двухсот минимальных размеров оплаты труда с конфискацией несертифицированных средств защиты информации или без таковой.

4. Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, - влечет наложение административного штрафа на должностных лиц в размере от двадцати до тридцати минимальных размеров оплаты труда; на юридических лиц - от ста пятидесяти до двухсот минимальных размеров оплаты труда.

5. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, - влечет наложение административного штрафа на должностных лиц в размере от тридцати до сорока минимальных размеров оплаты труда; на юридических лиц - от двухсот до трехсот минимальных размеров оплаты труда с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой.

6. Грубое нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), - влечет наложение административного штрафа на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, в размере от десяти до пятнадцати минимальных размеров оплаты труда или административное приостановление деятельности на срок до девяноста суток; на должностных лиц - от десяти до пятнадцати минимальных размеров оплаты труда; на юридических лиц - от ста до ста

пятидесяти минимальных размеров оплаты труда или административное приостановление деятельности на срок до девяноста суток.

*Статья 13.13. Незаконная деятельность в области защиты информации*

1. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), - влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой; на должностных лиц - от двадцати до тридцати минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой; на юридических лиц - от ста до двухсот минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой.

2. Занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, без лицензии, - влечет наложение административного штрафа на должностных лиц в размере от сорока до пятидесяти минимальных размеров оплаты труда; на юридических лиц - от трехсот до четырехсот минимальных размеров оплаты труда с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой.

*Статья 13.14. Разглашение информации с ограниченным доступом*

Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, - влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда; на должностных лиц - от сорока до пятидесяти минимальных размеров оплаты труда.

# ГЛАВА 2.
# Защита информации и информационных процессов

## 2.1. Защита информации от утечки на объектах информатизации органов внутренних дел

Утечка информации является нарушением принципа конфиденциальности информации.

В основе утечки лежит неконтролируемый перенос информации посредством физических полей и материальных объектов.

Информация, содержащаяся в базах и банках данных автоматизированных систем органов внутренних дел, представляет немалый интерес для преступных элементов. Поэтому обеспечение конфиденциальности информации, обрабатываемой средствами информатизации правоохранительных органов, является одной из ключевых задач обеспечения информационной безопасности в ОВД.

### 2.1.1. Понятие и виды каналов утечки информации

Информация сама по себе нематериальна. К информации, которую один человек просто знает, и никак это знание не проявляет, никто другой доступа получить никаким образом не может. Для того, чтобы с одной стороны, передать, а с другой – получить информацию, она должна обрести материальную форму, то есть информация должна быть зафиксирована с помощью какого-либо вещества либо физического явления. Иными словами, доступ к информации может быть получен только тогда, когда информация зафиксирована на некоем носителе информации.

С точки зрения физических явлений, в качестве таких носителей могут выступать:

- материалы и вещества;
- световые лучи;
- звуковые волны;
- электромагнитные волны.

Иной возможности для переноса информации в природе не существует.

Используя в своих интересах те или иные физические поля, человек создает определенную систему передачи информации. Такие системы принято называть системами связи.

Однако при определенных условиях возможно образование системы передачи информации из одной точки в другую независимо от желания источника информации. По аналогии с каналом передачи информации такой канал называют каналом утечки информации.

*Утечка информации* – неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к ней, а также ее получение разведками и другими заинтересованными субъектами.

*Канал утечки информации* – физический путь от источника конфиденциальной информации, по которому возможна утечка или несанкционированное получение информации.

Основными направлениями защиты информации от утечки по техническим каналам являются:

- предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами, а также за счет электроакустических преобразований;
- выявление внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);
- предотвращение перехвата с помощью технических средств речевой информации из помещений и объектов.

Применительно к практике с учетом физической природы образования *каналы утечки информации можно разделить на следующие группы*:

- визуально-оптические;
- акустические;
- электромагнитные;
- материально-вещественные.

В визуально-оптических каналах переносчиком информации выступает свет, испускаемый источником информации или отраженный от него в видимом, инфракрасном или ультрафиолетовом диапазонах. Получение информации с помощью визуально-оптического канала осуществляется путём непосредственного или удаленного наблюдения.

К примеру, оптический канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол окон, зеркал и т.д.). Отраженное лазерное излучение (диффузное или зеркальное) модулируется вибрирующей поверхностью по амплитуде и фазе и принимается приемником оптического излучения, при демодуляции которого выделяется акустическая информация. Для перехвата речевой информации по данному каналу используются сложные лазерные акустические локационные системы, называемые “лазерными микрофонами”. Работают они, как правило, в ближнем инфракрасном диапазоне волн.

*В акустическом канале* переносчиком информации выступает звук, лежащий в полосе слышимого, ультразвукового или инфразвукового диапазонов. Акустическая информация возникает в ходе ведения в помещениях разговоров, а также при работе систем звукоусиления и звуковоспроизведения. Речевой сигнал является сложным акустическим сигналом в диапазоне частот от 100 Гц … 7 кГц.

Получение информации посредством акустического канала осуществляется путем прослушивания либо восприятия вибраций с помощью технических средств.

*В электромагнитных каналах* переносчиком информации являются электромагнитные волны в диапазоне от сверхдлинных (длина волны 10 000 м, частота – менее 30 Гц) до субмиллиметровых (длина волны 1-0,1 мм, частота – от 300 до 3000 ГГц). Получение информации из электромагнитных каналов утечки осуществляется с помощью технических средств.

*Материально-вещественными каналами утечки информации* выступают самые различные материалы в любом агрегатном состоянии. Получение информации посредством материально-вещественного канала осуществляется путем непосредственного получения носителя информации.

Например, документальная информация содержится в графическом или буквенно-цифровом виде на бумаге, а также в электронном виде на магнитных и других носителях. Особенность документальной информации в том, что она в сжатом виде содержит сведения, подлежащие защите.

Очевидно, что каждый источник информации может в той или иной степени обладать определенной совокупностью каналов утечки информации.

Широкое использование самых различных технических средств автоматизации производственной и научной деятельности, систем автоматизированной обработки информации привело к расширению спектра каналов утечки информации. Переносчиками информации в них выступают побочные электромагнитные излучения и наводки (ПЭМИН).

Побочные электромагнитные излучения и наводки присущи любым электронным устройствам по самой природе проявления. О существовании таких излучений и наводок известно сравнительно давно. Известен следующий случай: в 1884 году при пользовании телефонными аппаратами в домах на одной из улиц Лондона были слышны звуки передаваемых телеграфных сообщений. При проверке выяснилось, что причиной этому являлись телеграфные провода, проложенные в земле параллельно телефонным на большом протяжении. Можно считать, что это был первый намек на возможность получения информации за счет побочного излучения и наводок.

Следует отметить, что технические средства и системы могут не только непосредственно излучать сигналы, содержащие обрабатываемую информацию, но и улавливать за счет своих микрофонных или антенных свойств акустические или магнитные излучения, преобразовывать их в электрические сигналы и передавать по своим линиям связи. Это еще более усиливает опасность утечки информации.

Анализ причин и условий появления источников побочного электромагнитного излучения и наводок показывает, что их можно разделить на две группы: несовершенство схемных решений технических средств и эксплуатационный износ элементов изделия. В свою очередь, в каждой из этих групп также выделяют по две группы причин и условий:

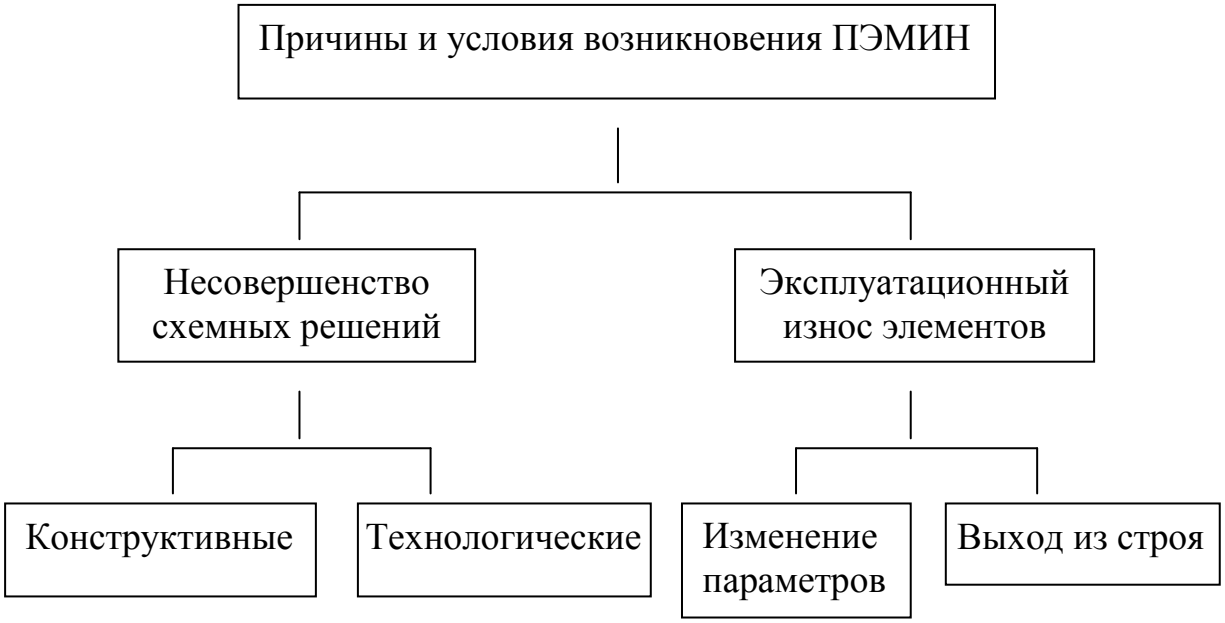


Рис.3. Причины и условия возникновения ПЭМИН

### 2.1.2. Технические средства несанкционированного доступа к информации

Рассмотрим общие характеристики технических средств несанкционированного доступа к информации и технологии их использования.

***Технические средства визуально-оптического получения информации***

Визуальное наблюдение является самым древним и очень эффективным методом сбора информации. Однако непосредственное наблюдение обладает теми недостатками, что, во-первых, получаемая информация хранится только в памяти человека и в большинстве случаев не может в дальнейшем быть воспроизведена с требуемой точностью, а во-вторых, человеческий глаз не в силах рассмотреть мелкие детали изображения на значительном расстоянии или в условиях плохой видимости. Эти недостатки могут быть устранены путем использования технических средств наблюдения.

В настоящее время для сбора информации могут использоваться специальные оптические системы (бинокли, телескопы и т.п.), а также миниатюрные скрытые и камуфлированные под обычные приборы фото-

и видеокамеры. Аппаратура для скрытой фото- и видеосъемки, как правило, оборудуется специальными объективами и насадками:

- предназначенными для съемки через отверстия небольшого размера;
- позволяющими осуществлять съемку со значительного расстояния;
- позволяющими осуществлять съемку в темное время суток и в условиях плохой видимости.

***Технические средства получения информации по акустическому каналу***

Получение информации по акустическому каналу также называют подслушиванием.

Подслушивание может быть непосредственным – когда акустические колебания достигают подслушивающего прямо или через конструкции зданий и помещений, и удаленное – осуществляемое с помощью различных технических средств.

Получение акустической информации с помощью технических средств может выполняться следующими основными способами:

- посредством микрофона;
- лазерное подслушивание.

Микрофон является базовым звеном в технической системе получения акустической информации.

Каждый микрофон обладает двумя основными параметрами:

1. Чувствительность – отношение напряжения на выходе микрофона к воздействующему на него звуковому давлению.

2. Частотная характеристика – зависимость чувствительности от частоты звукового давления (инфразвук: ниже 16 Гц, слышимый звук: 16 – 20 000 Гц, ультразвук: выше 20 000 Гц).

Передача информации с микрофона может осуществляться с помощью проводных или беспроводных линий связи. В случае использования проводного канала связи для передачи сигнала могут применяться как уже существующие проводные линии (телефонные, электрические и т.д.), так и специально проложенные. Среди беспроводных линий связи можно выделить передачу информации по радиоканалу (радиомикрофоны) и инфракрасному каналу.

Кроме того, микрофоны можно также классифицировать как устанавливаемые непосредственно в помещении, так и вне помещения. Среди последних следует отметить стетоскопные микрофоны, которые устанавливаются на поверхности твердой преграды и фиксируют вибрации, возникающие в них под воздействием акустических волн в воздухе помещения, и лазерные микрофоны, позволяющие посредством лазерного луча со значительного расстояния регистрировать колебания оконных стекол.

***Технические средства получения информации по электромагнитному каналу***

Получение сведений по электромагнитному каналу возможно посредством доступа к каналу связи либо путем получения и анализа информации из побочных электромагнитных излучений и наводок.

Получение информации из каналов связи осуществляется с помощью контактного или бесконтактного подключения к проводным системам связи либо путем банального радиоперехвата.

Бесконтактное подключение к линии связи осуществляется двумя путями:

- за счет электромагнитных наводок на параллельно проложенные провода;
- с помощью сосредоточенной индуктивности, охватывающей контролируемую линию.

Для получения информации посредством электромагнитного канала могут использоваться антенны и специальные электронные устройства.

### 2.1.3. Защита информации от утечки по техническим каналам

Защита информации от утечки по техническим каналам в общем плане сводится к следующим действиям:

1. Своевременное определение возможных каналов утечки информации.
2. Определение энергетических характеристик канала утечки информации на границе контролируемой зоны.
3. Оценка возможности контроля каналов утечки со стороны злоумышленников.

4. Исключение или ослабление энергетики каналов утечки.

С целью предотвращения утечки информации по визуально-оптическим каналам рекомендуется использовать следующие основные меры защиты:

- располагать объекты защиты так, чтобы исключить излучение или отражение света в стороны возможного расположения злоумышленника;
- использовать средства преграждения или ослабления светового потока.

Для защиты информации от утечки по акустическим каналам применяют как архитектурно-планировочные и режимные мероприятия, так и мероприятия по звукоизоляции, звукопоглощению и звукоподавлению.

Защита информации от утечки по электромагнитным каналам осуществляется, в основном, с помощью конструкторско-технологических решений, ориентированных на исключение возможности возникновения таких каналов.

К таким решениям относятся:

- экранирование элементов и узлов аппаратуры;
- ослабление электромагнитной связи между элементами аппаратуры;
- фильтрация сигналов.

Кроме того, целесообразно выбирать места установки технических средств с учетом особенностей их электромагнитных полей с таким расчетом, чтобы исключить их выход за пределы контролируемой зоны.

Большую роль в защите от утечки информации по техническим каналам играет обнаружение и нейтрализация технических средств несанкционированного получения информации.

Поиск несанкционированных технических средств может осуществляться с помощью визуального контроля либо путем использования специальной аппаратуры для обнаружения радиоэлектронных устройств.

Для поиска аппаратуры негласного получения информации могут применяться:

- досмотровые зеркала;
- металлоискатели;
- тепловизоры;

- нелинейные локаторы (позволяют обнаружить полупроводниковые приборы);

- индикаторы электромагнитных излучений – позволяют обнаруживать радиопередатчики;

- локаторы проводных линий;

- детекторы сигналов электросети;

- указатели пары (трассоискатели) – позволяют обнаружить ответвления от основной линии;

- прочие приборы и устройства.

Система защиты информации будет действенной только в том случае, если она является комплексной. Поэтому для защиты информации от утечки наряду с техническими следует использовать правовые и организационные меры защиты.

### 2.1.4. Основные направления инженерно-технической защиты информации

Защита информации от утечки по техническим каналам достигается проектно-архитектурными решениями, проведением организационных и технических мероприятий, а также выявлением портативных электронных устройств перехвата информации (закладных устройств).

*Организационное мероприятие* – это мероприятие по защите информации, проведение которого не требует применения специально разработанных технических средств.

К основным организационным и режимным мероприятиям относятся:

- привлечение к проведению работ по защите информации организаций, имеющих лицензию на деятельность в области защиты информации, выданную соответствующими органами;
- категорирование и аттестация объектов информатизации и выделенных для проведения закрытых мероприятий помещений по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности;
- использование на объекте сертифицированных технических средств обработки и хранения информации, а также вспомогательных технических средств и средств связи;

- установление контролируемой зоны вокруг объекта;
- привлечение к работам по строительству, реконструкции объектов с защищаемой информацией организаций, имеющих лицензию на деятельность в области защиты информации по соответствующим пунктам;
- организация контроля и ограничение доступа на защищаемые объекты и в выделенные помещения;
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;
- отключение от линий связи на период закрытых мероприятий технических средств, имеющих элементы со свойствами электроакустических преобразователей, и т.д.

*Техническое мероприятие* – это мероприятие по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений.

Технические мероприятия направлены на закрытие каналов утечки информации путем ослабления уровня информационных сигналов или уменьшения отношения сигнал/шум в местах возможного размещения портативных средств разведки или их датчиков до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки, и проводятся с использованием активных и пассивных средств.

К техническим мероприятиям с использованием пассивных средств относятся:

- контроль и ограничение доступа на объекты защиты и в выделенные помещения;
- установка на объектах защиты и в выделенных помещениях технических средств и систем ограничения и контроля доступа;
- локализация излучений;
- экранирование объектов защиты и их соединительных линий;
- заземление объектов защиты и экранировка их соединительных линий;
- звукоизоляция выделенных помещений;
- развязывание информационных сигналов;

- установка специальных средств защиты во вспомогательных технических средствах и системах, обладающих «микрофонным эффектом» и имеющих выход за пределы контролируемой зоны;
- установка специальных диэлектрических вставок в оплетки кабелей электропитания, труб систем отопления, водоснабжения и канализации, имеющих выход за пределы контролируемой зоны;
- установка автономных или стабилизированных источников электропитания средств обработки и хранения информаци;
- установка в цепях электропитания технических средств, а также в линиях осветительной и розеточной сетей выделенных помещений помехоподавляющих фильтров.

Выявление портативных электронных устройств перехвата информации (закладных устройств) осуществляется проведением специальных поисковых мероприятий. При этом осуществляется:

- установка в выделенных помещениях средств и систем обнаружения лазерного облучения (подсветки) оконных стекол;
- установка в выделенных помещениях стационарных обнаружителей диктофонов;
- поиск закладных устройств с использованием индикаторов поля, интерсепторов, частотомеров, сканерных приемников и программно-аппаратных комплексов контроля;
- организация радиоконтроля (постоянно или на время проведения конфиденциальных мероприятий) и контроля побочных электромагнитных излучений технических средств защищаемого помещения;
- проверка выделенных помещений с использованием нелинейных локаторов;
- специальная проверка выделенных помещений и технических средств с использованием рентгеновских комплексов.

## 2.1. Защита информационных процессов в компьютерных системах

### 2.2.1. Основные угрозы безопасности информации в компьютерных системах

Большинство современных компьютерных систем обработки информации в общем случае представляет собой территориально распределенные системы интенсивно взаимодействующих между собой по данным и управлению локальных вычислительных сетей (ЛВС) и отдельных ПК.

В общем случае компьютерная система состоит из следующих основных структурно-функциональных элементов:

- рабочих станций – отдельных ПК или удаленных терминалов сети, на которых реализуются автоматизированные рабочие места пользователей (абонентов, операторов);
- серверов или Host-машин (служб файлов, печати, баз данных ит.п.), не выделенных (или выделенных, то есть не совмещенных с рабочими станциями) высокопроизводительных ПК, предназначенных для реализации функций хранения, печати данных, обслуживания рабочих станций сети и т.п. действий;
- межсетевых мостов - элементов, обеспечивающих соединение нескольких сетей передачи данных либо нескольких сегментов одной и той же сети, имеющих различные протоколы взаимодействия(шлюзов, центров коммутации пакетов, коммуникационных ПК);
- каналов связи (локальных, телефонных, с узлами коммутации и т.д.).

*Рабочие станции* являются наиболее доступными компонентами сетей и именно с них могут быть предприняты наиболее многочисленные попытки совершения несанкционированных действий. С рабочих станций осуществляются управление процессами обработки информации, запуск программ, ввод и корректировка данных, на дисках рабочих станций могут размещаться важные данные и программы обработки. На видеомониторы и печатающие устройства рабочих станций выводится информация при работе пользователей (операторов), выполняющих

различные функции и имеющих разные полномочия по доступу к данным и другим ресурсам системы. Именно поэтому рабочие станции должны быть надежно защищены от доступа посторонних лиц и содержать средства разграничения доступа к ресурсам со стороны законных пользователей, имеющих разные полномочия. Кроме того, средства защиты должны предотвращать нарушения нормальной настройки рабочих станций и режимов их функционирования, вызванные неумышленным вмешательством неопытных (невнимательных) пользователей.

В особой защите нуждаются такие привлекательные для злоумышленников элементы сетей, как *серверы* (Host-машины) и *мосты*. Первые – как концентраторы больших объемов информации, вторые – как элементы, в которых осуществляется преобразование (возможно через открытую, нешифрованную форму представления) данных при согласовании протоколов обмена в различных участках сети.

Благоприятным для повышения безопасности серверов и мостов обстоятельством является, как правило, наличие возможностей по их надежной защите физическими средствами и организационными мерами в силу их выделенности, позволяющей сократить до минимума число лиц из персонала сети, имеющих непосредственный доступ к ним. Иными словами, непосредственные случайные воздействия персонала и преднамеренные воздействия злоумышленников на выделенные серверы и мосты можно считать маловероятными. В то же время надо ожидать массированной атаки на серверы и мосты с использованием средств удаленного доступа. Здесь злоумышленники, прежде всего, могут искать возможности повлиять на работу различных подсистем серверов и мостов, используя недостатки протоколов обмена и средств разграничения удаленного доступа к ресурсам и системным таблицам. Использоваться могут все возможности и средства, от стандартных (без модификации компонентов) до подключения специальных аппаратных средств (каналы, как правило, слабо защищены от подключения) и применения высококлассных программ для преодоления системы защиты.

Конечно, сказанное выше не означает, что не будет попыток внедрения аппаратных и программных закладок в сами мосты и серверы, открывающих дополнительные широкие возможности по

несанкционированному удаленному доступу. Закладки могут быть внедрены как с удаленных станций (посредством вирусов или иным способом), так и непосредственно в аппаратуру и программы серверов при их ремонте, обслуживании, модернизации, переходе на новые версии программного обеспечения, смене оборудования.

*Каналы и средства связи* также нуждаются в защите. В силу большой пространственной протяженности линий связи (через неконтролируемую или слабо контролируемую территорию) практически всегда существует возможность подключения к ним либо вмешательства в процесс передачи данных.

Основными видами угроз безопасности компьютерных систем являются:

- стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т.п.);
- сбои и отказы оборудования (технических средств) компьютерной системы;
- последствия ошибок проектирования и разработки компонентов компьютерной системы (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.);
- ошибки эксплуатации (пользователей, операторов и другого персонала);
- преднамеренные действия нарушителей и злоумышленников(обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т.п.).

Все множество потенциальных угроз информации по природе их возникновения разделяется на два класса: естественные (объективные) и искусственные (субъективные).

*Естественные угрозы* – это угрозы, вызванные воздействиями на компьютерную систему и ее элементы объективных физических процессов или стихийных природных явлений, не зависящих от человека.

*Искусственные угрозы* – это угрозы компьютерной системе, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить непреднамеренные и преднамеренные.

*Непреднамеренные угрозы* (неумышленные, случайные) - вызванные ошибками при проектировании информационной системы и ее элементов, разработке программного обеспечения, ошибками персонала.

*Преднамеренные (умышленные) угрозы* – угрозы, связанные с корыстными устремлениями людей (злоумышленников).

Источники угроз по отношению к компьютерным систем могут быть *внешними* или *внутренними* (компоненты самой компьютерной системы – ее аппаратура, программы, персонал).

*Основные непреднамеренные искусственные угрозы* информационной системе (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности без злого умысла):

- неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.;
- неправомерное отключение оборудования или изменение режимов работы устройств и программ;
- запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
- нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения сотрудником своих служебных обязанностей);
- заражение компьютера вирусами;
- неосторожные действия, приводящие к разглашению конфиденциальной информации или делающие ее общедоступной;
- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
- игнорирование организационных ограничений при работе в системе;
- вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);
- некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
- пересылка данных по ошибочному адресу абонента (устройства);

- ввод ошибочных данных;
- неумышленное повреждение каналов связи.

Основные возможные пути умышленной дезорганизации работы системы, проникновения в систему и несанкционированного доступа к информации:

- физическое разрушение системы;
- отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
- внедрение агентов в число персонала системы (в том числе в административную группу, отвечающую за безопасность);
- вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих необходимые полномочия;
- применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;
- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства;
- перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя;
- хищение носителей информации;
- несанкционированное копирование носителей информации;
- хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
- чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
- незаконное получение паролей и других реквизитов разграничения доступа с последующей маскировкой под зарегистрированного пользователя («маскарад»);
- несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие, как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;
- вскрытие шифров криптозащиты информации;

- внедрение аппаратных спецвложений, программных «закладок» и «вирусов» («троянский конь» и «жучки»), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяют преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;
- незаконное подключение к линиям связи с целью работы «между строк», с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;
- незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

Чаще всего для достижения поставленной цели злоумышленник использует не один, а совокупность перечисленных выше путей.

### 2.2.2. Способы защиты информации в компьютерных системах от случайных и преднамеренных угроз

**Разграничение доступа к информации**

Одним из основных видов угроз целостности, конфиденциальности и доступности информации являются преднамеренные угрозы. Эти угрозы могут осуществляться как при непосредственном участии человека (злоумышленника), так и при помощи специально разработанных компьютерных программ.

Одним из механизмов, позволяющим предотвратить реализацию преднамеренных угроз, является разграничение доступа пользователей и программ к элементам информационной системы.

Для реализации системы разграничения и контроля доступа необходимо для каждой пары «субъект-объект» определить множество допустимых операций и контролировать выполнение установленного порядка.

Описание отношений «субъекты-объекты» осуществляют с помощью составления матрицы доступа.

*Матрица доступа* – таблица, в строках которой перечислены субъекты, в столбцах – объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны разрешенные виды доступа и дополнительные условия (например, время и место действия).

Пример: фрагмент матрицы доступа.

| | АИС «Розыск» | | СПС «Гарант» | | АИС «Статистика» | | АИС «Бухгалтерия» | |
|---|---|---|---|---|---|---|---|---|
| | Запись | Чтение | Запись | Чтение | Запись | Чтение | Запись | Чтение |
| Начальник | | + | | + | | + | | + |
| Бухгалтер | | | | + | | | + | + |
| Следователь | + | + | | + | + | + | | |
| Статистик | | | | + | + | + | | |

Для того, чтобы реализовать разграничение полномочий, кроме матрицы доступа необходима подсистема, способная отличить одного пользователя (или программу) от другого. При этом используется идентификация и аутентификация субъектов доступа.

Идентификация – присвоение субъектам и объектам информационной системы уникальных идентификаторов и сравнение предъявленного идентификатора с утвержденным перечнем.

Наличие идентификатора позволяет реализовать процедуру выделения конкретного субъекта из множества однотипных субъектов.

Аутентификация – процесс проверки подлинности предъявленных при идентификации сведений.

Цель аутентификации заключается в том, чтобы убедиться, что субъект действительно является тем, за кого себя выдает.

Аутентификация может быть односторонней – когда субъект, обращающийся к информационным ресурсам, доказывает свою подлинность, и двусторонней – когда свою подлинность доказывают обе стороны информационного обмена.

Примером односторонней аутентификации может служить обычная процедура входа пользователя в системы. Двусторонняя аутентификация выполняется, например, в системах работы с финансовой информацией, когда требуется не только убедиться в праве пользователя на доступ к данным, но и подтвердить, что не выполнена мошенническая подмена данных.

Аутентификация субъектов информационных отношений может осуществляться путем проверки одной из следующих сущностей:

- нечто, что субъект знает;
- нечто, чем субъект владеет;
- нечто, что есть часть субъекта.

Аутентификация субъекта на основе его знаний является самым простым, дешевым, но вместе с тем и самым ненадежным способом. Чаще всего используется парольная аутентификация, когда для подтверждения своей подлинности субъект должен сообщить системе некий набор символов, в идеале известный только ему. Может использоваться и система «вопрос-ответ», когда пользователю задаются вопросы, ответы на которые анализируются и на основе этого анализа делается заключение о подлинности субъекта доступа.

Однако если в качестве пароля выбрано логически осмысленное слово или словосочетание, либо число, такой пароль достаточно легко подобрать. В то же время бессмысленный набор символов сложно запомнить, и у пользователя возникает стремление хранить его в записанном виде. При этом существует вероятность, что злоумышленник получит доступ к такому листу бумаги с паролем, и в дальнейшем сможет выдать себя за легального пользователя.

В качестве «золотой середины» рекомендуется использовать комбинацию описанных приемов – пароль должен быть сравнительно легко запоминающимся, но вместе с тем быть сложным для отгадывания, т.е. содержать в себе символы разных регистров, чередование букв, цифр и специальных символов.

Кроме того, при организации парольной защиты целесообразно использовать пароли большой длины, т.к. при этом увеличивается время его подбора. Пароли должны периодически меняться.

Аутентификация на основе предъявления субъектом чего-либо, чем он владеет, несколько повышает степень защищенности системы. В этом случае злоумышленник для доступа к объектам информационной системы должен либо стать обладателем ключевого предмета, либо иметь его достаточно точную копию. В качестве таких предметов могут выступать съемные носители информации, на которых записан код субъекта доступа, электронные и механические ключи, пластиковые карты.

Предметы-идентификаторы могут использоваться только для получения доступа к системе или постоянно должны быть подключены до окончания работы пользователя. Такие аппаратно-программные устройства, в отличие от парольной защиты, способны обеспечить контроль доступа на протяжении всего сеанса работы.

Наиболее высокий уровень безопасности обеспечивается аутентификацией на основе неотъемлемой части субъекта доступа – его биометрических характеристик. Используемые в них данные не могут быть похищены или скопированы.

Биометрическая идентификация – совокупность автоматизированных методов идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик.

К числу физиологических характеристик относятся особенности отпечатков пальцев, геометрии руки, запаха, ДНК, формы уха, геометрии лица, опечатка ладони, сетчатки глаза, рисунка радужной оболочки глаза, голоса, температуры кожи лица. К поведенческим характеристикам относятся динамика подписи (ручной), стиль работы с клавиатурой. На стыке физиологии и поведения находятся анализ особенностей голоса и распознавание речи.

В общем виде работа с биометрическими данными организована следующим образом. Сначала создается и поддерживается база данных характеристик потенциальных пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки (называемый биометрическим шаблоном) заносится в базу данных (исходные данные, такие как результат сканирования пальца или роговицы, обычно не хранятся).

В дальнейшем для идентификации (и одновременно аутентификации) пользователя процесс снятия и обработки повторяется, после чего производится поиск в базе данных шаблонов. В случае успешного поиска личность пользователя и ее подлинность считаются установленными. Для аутентификации достаточно произвести сравнение с одним биометрическим шаблоном, выбранным на основе предварительно введенных данных.

Биометрический способ подвержен тем же угрозам, что и другие методы аутентификации. Во-первых, биометрический шаблон сравнивается не с результатом первоначальной обработки характеристик

пользователя, а с тем, что «пришло» к месту сравнения. Во-вторых, биометрические методы не более надежны, чем база данных шаблонов. В-третьих, следует учитывать разницу между применением биометрии на контролируемой территории и в «полевых» условиях, когда, например к устройству сканирования могут поднести муляж и т.п. В-четвертых, биометрические данные человека меняются, так что база шаблонов нуждается в сопровождении, что создает определенные проблемы и для пользователей, и для администраторов систем безопасности.

**Криптографическая защита информации**

Защита информации путем преобразования, исключающего ее прочтение посторонним лицом, является одним из наиболее действенных методов обеспечения информационной безопасности, и имеет давнюю историю. Проблемой преобразования информации занимается наука криптология. Исходя из направленности практического применения, *криптология разделяется на два противоположных направления*: *криптографию и криптоанализ*.

Криптография – наука о методах защиты информации на основе ее преобразования с сохранением достоверности содержания.

*Криптоанализ*– наука о методах раскрытия и модификации данных без знания ключей.

Это научное направление преследует две цели. Первая – исследование закодированной информации с целью восстановления содержания исходного документа. Вторая – распознавание и изучение метода кодирования информации с целью фальсификации сообщения.

Современная криптография включает в себя четыре крупных раздела:

1. Симметричные криптосистемы.
2. Криптосистемы с открытым ключом.
3. Системы электронной подписи.
4. Управление ключами.

Основные направления использования криптографических методов:

- передача конфиденциальной информации по каналам связи;
- установление подлинности передаваемых сообщений;
- хранение информации в зашифрованном виде.

Перечислим основные понятия и определения криптографии.

*Шифрование* – процесс, при котором исходный (открытый) текст сообщения заменяется шифрованным текстом.

*Дешифрование* – процесс преобразования шифрованного текста в открытый с помощью ключа шифрования.

*Ключ шифрования* – информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

*Текст* – упорядоченный набор из элементов (символов) алфавита.

*Алфавит* – конечное множество используемых для кодирования информации знаков.

В качестве примеров алфавитов, используемых в современных информационных системах, можно привести следующие:

- алфавит Z33 – 32 буквы русского языка и пробел;
- алфавит Z256 – стандартные символы компьютерной кодировки знаков латинского и национального алфавитов, цифры, знаки препинания и специальные символы;
- бинарный алфавит Z2 – цифры 0 и 1, восьмеричный, шестнадцатеричный и т.п. алфавиты.

Процесс криптографического преобразования информации может осуществляться аппаратным или программным способами. Аппаратная реализация характеризуется существенно большей стоимостью, высокой защищенностью и скоростью работы, простотой в использовании. Программный способ более практичен, допускает известную гибкость в использовании, но сравнительно медленнее и хуже защищен.

Все современные алгоритмы криптографического преобразования информации используют ключ для управления шифрованием и дешифрованием.

*Алгоритмы с использованием ключа делятся на два класса*:

- *Симметричные (с секретным ключом)*. Для шифрования и дешифрования используется один и тот же ключ, или же ключ для дешифрования вычисляется на основе ключа шифрования.
- *Асимметричные (с открытым ключом)*. Шифрование информации осуществляется с использованием открытого ключа, который известен всем. Дешифрование производится с помощью закрытого ключа, известного только получателю сообщения.

Симметричные алгоритмы работают быстрее, чем асимметричные. На практике оба типа алгоритмов часто используются совместно.

*Электронная цифровая подпись* – присоединяемое к тексту его криптографическое преобразование с использованием закрытого ключа.

Электронная цифровая подпись позволяет идентифицировать владельца подписи, а также установить отсутствие искажения информации в электронном документе.

Процесс использования электронной цифровой подписи в общем виде выглядит следующим образом (Рис.4):

1. Отправитель рассчитывает хэш-функцию текста – идентификатор, полученный путем сжатия информации с помощью математического алгоритма.
2. Отправитель, используя свой секретный ключ, зашифровывает хэш-функцию. В результате получается определенная цифровая последовательность – цифровая подпись.
3. Отправитель формирует пересылаемое сообщение, включающее в себя исходный текст и его цифровую подпись.
4. Отправитель по открытому каналу связи передает пересылаемое сообщение.
5. Получатель выделяет из принятого сообщения текст и его цифровую подпись.
6. Получатель вычисляет хэш-функцию полученного текста.
7. Получатель сообщения с помощью открытого ключа расшифровывает цифровую подпись.
8. Получатель сравнивает результат расшифровки с рассчитанной им хэш-функцией.

*Отправитель* *Получатель*

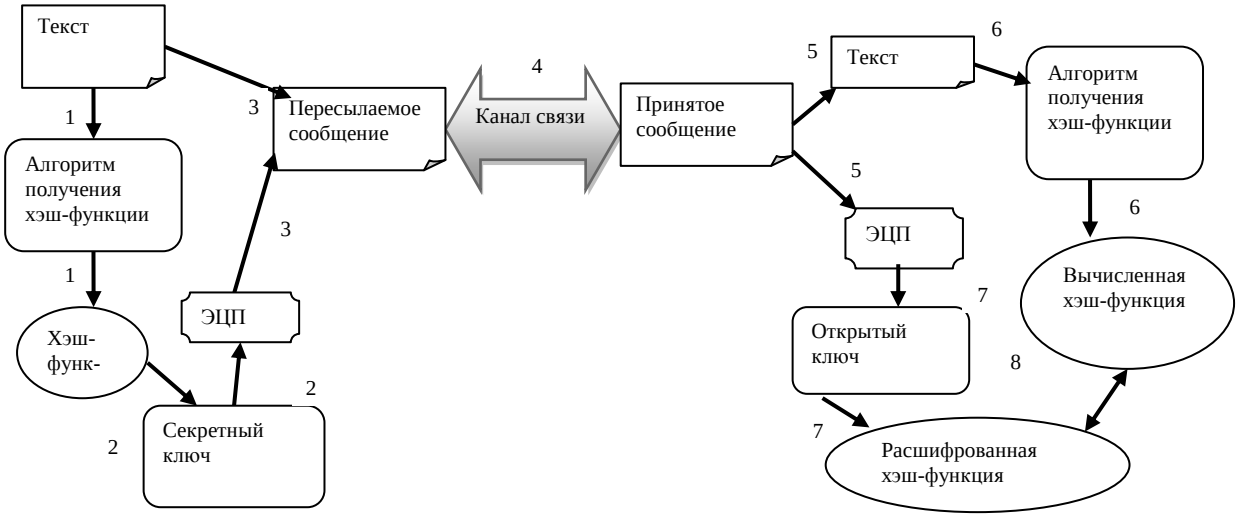


Рис. 4. Процесс использования электронной цифровой подписи

Если вычисленная и расшифрованная хэш-функции совпадают, то сообщение считается подтвержденным.

Важной проблемой всей криптографии с открытым ключом, в том числе и систем ЭЦП, является управление ключами. Необходимо обеспечить доступ любого пользователя к подлинному открытому ключу любого другого пользователя, защитить эти ключи от подмены злоумышленником, а также организовать отзыв ключа в случае его компрометации. Управлением ключами занимаются удостоверяющие центры.

Наряду с обычным шифрованием, используется и такой способ сокрытия данных, как стеганография.

*Стеганография* – совокупность методов, обеспечивающих сокрытие факта существования информации в той или иной среде, а также средства реализации таких методов.

К стеганографии можно отнести огромное множество секретных средств связи, таких, как невидимые чернила, микрофотоснимки, условное расположение знаков и т.д.

В настоящее время активно развивается компьютерная стеганография. Она рассматривает вопросы, связанные с сокрытием информации, хранящейся на цифровых носителях или передаваемой по телекоммуникационным каналам связи.

Для стеганографического преобразования необходимы:

- скрываемая информация;
- контейнер данных;
- программное обеспечение для добавления информации в файл-контейнер и ее извлечения.

В качестве контейнера для скрываемого сообщения могут выступать графические, аудио- или видеофайлы.

Основная идея стеганографического сокрытия информации заключается в том, что добавление «секретного» сообщения в файл-контейнер должно вызывать лишь незначительные изменения последнего, не улавливаемые органами чувств человека. Поэтому файл-контейнер должен быть достаточно большого размера.

Стеганографические технологии используются для решения следующих задач:

- защита информации от несанкционированного доступа;
- защита авторских прав на объекты интеллектуальной собственности;
- противодействие системам мониторинга передаваемых данных;
- создание скрытых каналов утечки информации.

Стеганография позволяет внедрить в компьютерные графические изображения, аудио- и видеопродукцию, литературные тексты, программы специальную цифровую метку, незаметную при обычном использовании файла, но распознаваемую специальным программным обеспечением. Такие специальные сведения могут рассматриваться в качестве подтверждения авторства.

### 2.2.3. Защита информации от вредоносных программ

Защита информационных систем от воздействия вредоносного программного обеспечения имеет особое значение по ряду причин:

1. Данный вид защиты актуален для всех информационных систем, независимо от характера обрабатываемой ими информации.
2. Риск заражения вредоносными программами очень велик вследствие высокого динамизма обмена информацией как по каналам связи, так и с помощью переносных носителей информации.
3. Защита от вредоносных программ требует особого профессионализма, поскольку некоторые из них носят специфический

индивидуальных характер, а их обнаружение и нейтрализация требуют глубокого знания особенностей функционирования информационных систем.

Вредоносные программы представляют собой специально разработанное программное обеспечение, оказывающее негативное воздействие на данные, обрабатываемые информационными системами, или на процесс функционирования самих информационных систем.

Воздействие вредоносного программного обеспечения представляется особо опасным в силу сравнительной простоты реализации и повышенной трудности защиты.

Основными причинами проникновения вредоносных программ в информационные системы являются:

- массовый обмен данными с помощью переносных носителей информации и компьютерных сетей;
- широкое распространение нелицензионных копий программного обеспечения;
- возможность удаленного воздействия на информационные системы, подключенные к сетям общего пользования.

Исходя из целей защиты от вредоносных программ, их целесообразно классифицировать по следующим критериям:

1. Характеру вредоносного воздействия.
2. Времени проникновения в информационные системы.
3. Способности к саморазмножению.

По характеру вредоносного воздействия вредоносные программы подразделяются на:

– искажающие или уничтожающие информацию;

– формирующие каналы несанкционированного доступа к информации;

– нарушающие работу информационной системы.

По времени проникновения в информационные системы вредоносные программы делятся на:

– вредоносные компоненты, создаваемые в процессе разработки информационной системы;

– проникающие в информационную систему в процессе ее эксплуатации;

– вносимые в информационную систему в процессе ее обслуживания.

По способности к саморазмножению вредоносные программы классифицируются как:

– саморазмножающиеся.

– неспособные к саморазмножению.

В настоящее время известно значительное количество разновидностей вредоносных программ, основными из которых являются:

1. *Троянский конь*. Несаморазмножающаяся вредоносная программа, представляющая собой компонент полезного программного обеспечения, способная выполнять нежелательные действия.

2. *Логическая бомба*. Несаморазмножающаяся вредоносная программа одноразового использования, приводящаяся в действие в определенных условиях и выполняющая разрушение информации.

3. *Ловушка*. Несаморазмножающаяся вредоносная программа, осуществляющая несанкционированный перехват информации и ее передачу по каналам связи или запись на переносные носители информации.

4. *Люк*. Несаморазмножающаяся вредоносная программа, обеспечивающая злоумышленнику возможность несанкционированного доступа к информационной системе.

5. *Вирус*. Саморазмножающаяся вредоносная программа, выполняющая нежелательные действия.

Сложность защиты информации от вредоносных программ усугубляется тем, что в настоящее время злоумышленниками используются комбинации перечисленных категорий, например, вирус-люк, вирус-ловушка и т.д.

Для защиты от вредоносных программ используются правовые, организационные и технические меры.

Правовые меры сводятся к установлению ответственности за создание и распространение вредоносных программ и причинение ущерба. Следует отметить, что доказать авторство и умышленность создания таких программ довольно трудно.


Рис.5. Классификация вредоносных программ

Организационная защита заключается в выработке и неукоснительном осуществлении мероприятий, направленных на предупреждение проникновения вредоносных программ в информационные системы, обнаружение заражения, нейтрализацию негативного воздействия и ликвидацию последствий.

Технические меры защиты сводятся преимущественно к использованию специального программного обеспечения, получившего название антивирусных программ. Кроме того, могут использоваться специальные устройства, препятствующие проникновению вредоносных программ на компьютер, устройства резервного копирования данных и т.д.

### 2.2.4. Антивирусные программы

На сегодняшний день перечень доступных антивирусных программ весьма обширен. Они различаются как по цене (от весьма дорогих до абсолютно бесплатных), так и по своим функциональным возможностям.

Наиболее мощные (и, как правило, наиболее дорогие) антивирусные программы представляют собой на самом деле пакеты специализированных утилит, способных при совместном их использовании поставить заслон практически любому виду вредоносных программ.

Типовой перечень функций, которые способны выполнять антивирусные программы:

- сканирование памяти и содержимого дисков по расписанию;
- сканирование памяти компьютера, а также записываемых и читаемых файлов в реальном режиме времени с помощью резидентного модуля;
- выборочное сканирование файлов с измененными атрибутами;
- распознавание поведения, характерного для компьютерных вирусов;
- блокировка и/или удаление выявленных вирусов;
- восстановление зараженных информационных объектов;
- принудительная проверка подключенных к корпоративной сети компьютеров;
- удаленное обновление антивирусного программного обеспечения и баз данных с информацией о вирусах, в том числе автоматическое обновление баз данных по вирусам через Интернет;
- фильтрация трафика Интернета на предмет выявления вирусов в передаваемых программах и документах;
- выявление потенциально опасных Java–апплетов и модулей ActiveX;
- ведение протоколов, содержащих информацию о событиях, касающихся антивирусной защиты.

Как показывает практика, для максимальной защиты компьютера от внешних угроз одного только антивируса недостаточно. Такое положение дел вызвано тем, что в свое время при создании сети Интернет не было

уделено достаточно внимания требованиям безопасности, а в основном интересовало удобство обмена информацией. Этим успешно пользуются различные хакеры. Поэтому для защиты от кражи и потери информации, а также иных вредоносных действий с ПК необходимо установить на него фаервол, или брандмауэр. Сам термин «фаервол» происходит от английского слова firewall, обозначающего противопожарную стену.

Программный фаервол представляет из себя программное обеспечение, фильтрующее интернет-трафик или иную сетевую активность, пресекающее несанкционированные попытки доступа к компьютеру из внешней сети, анализируя трафик по заданному набору правил. Все пакеты данных, как входящие, так и исходящие, анализируются этой программой, и в зависимости от принимаемого решения пропускаются либо отклоняются.

Надо заметить, что установленный на компьютере антивирус не является основанием для того, чтобы отказаться от установки фаервола. Эти программы работают по разному принципу: например, при обнаружении троянской активности антивирус будет пытаться найти его и обезвредить, тогда как фаервол просто запретит трояну отправлять данные, чем его и нейтрализует.

Чтобы лучше понять принцип работы фаервола, рассмотрим основные принципы функционирования компьютерных сетей.

Информация между компьютерами в сети передается отдельными порциями, именуемыми пакетами данных. Для отправки данных на компьютер необходимо знать его адрес. Его роль выполняет IP, представляющий из себя четыре группы чисел от 0 до 255, разделенных между собой точками, например. 91.122.214.4. (для локальных сетей это 10.27.*.* и 192.168.*.*). Для отправки и приема данных используются порты, имеющие свой номер от 0 до 65535, которые используют в своей работе различные программы. Так, для электронной почты обычно используются порты 25 и 110, интернет-браузеры используют 80-й порт. А фаервол контролирует пакеты, проходящие через эти порты. Порты могут иметь три состояния – открыт, закрыт и невидим. Если порты невидимы, то злоумышленник просто не увидит ваш компьютер в сети, поэтому брандмауэр тоже следит за этим, а также держит неиспользуемые порты закрытыми. Кроме этого, фаервол следит за активностью запускаемых приложений и блокирует попытки доступа, вызывающие

подозрение, так как зачастую вредоносные программы маскируются под нужное для работы ПО, либо внедряются в его исходный код и действуют как бы от его имени. Фаервол же отсекает все такие несанкционированные попытки передачи данных.

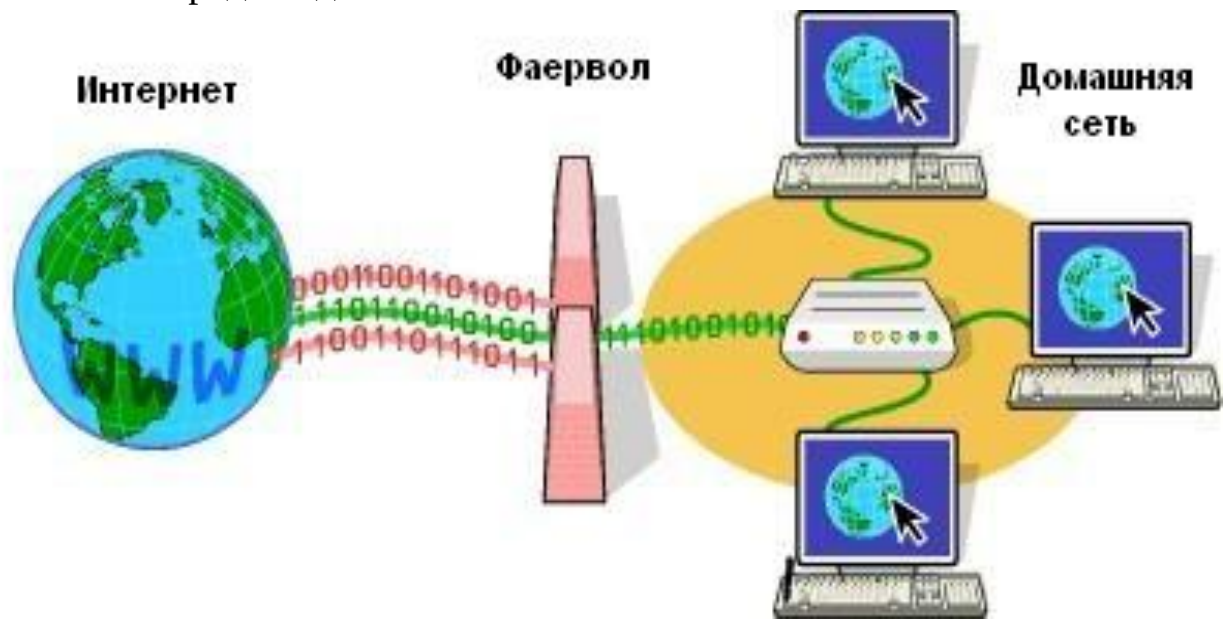


Рис.6. Фаервол

Как же определить, что именно нужно блокировать, при этом не закрывая доступ к Интернету нужным программам типа браузера или почтового клиента? Для этого существует определенный ряд правил, заложенных в него автором, которыми руководствуется брандмауэр. Пользователь также может в настройках самостоятельно указать надежные приложения-исключения, которые не будут блокироваться фаерволом, а также программы, которым следует полностью запретить сетевую активность.

Фаервол также, как и антивирус, нуждается в периодическом обновлении, но гораздо реже, примерно раз в несколько месяцев.

Как же определить, что именно нужно блокировать, при этом не закрывая доступ к Интернету нужным программам типа браузера или почтового клиента? Для этого существует определенный ряд правил, заложенных в него автором, которыми руководствуется брандмауэр. Пользователь также может в настройках самостоятельно указать надежные приложения-исключения, которые не будут блокироваться фаерволом, а также программы, которым следует полностью запретить сетевую активность.

Фаервол так же, как и антивирус, нуждается в периодическом обновлении, но гораздо реже, примерно раз в несколько месяцев.

Несмотря на все плюсы, фаервол не сможет защитить систему от проникновения вирусов в случае, если те используют, к примеру, уязвимости программного обеспечения или операционной системы, поэтому при защите ПК от всех видов вредоносных угроз необходим комплексный подход с использованием различных программ для защиты вашего компьютера. Фаервол же рассматривается лишь как одна из составляющих, обеспечивающих безопасность ПК, имеющего подключение к сети, хотя и крайне необходимых.

К наиболее мощным и популярным на сегодняшний день в России антивирусным пакетам относятся:

- DoctorWeb (DrWeb) – программа российской компании;
- Антивирус Касперского (AVP) - разработка еще одной российской фирмы;
- NortonAntiVirus - корпорации Symantec;
- McAfee VirusScan - компании Network Associates;
- PandaAntivirus.
- Nod32 Antivirus.

Популярность перечисленных выше пакетов обусловлена, прежде всего, тем, что в них реализован комплексный подход к борьбе с вредоносными программами. То есть, установив такой пакет, вы избавляетесь от необходимости использовать какие-либо дополнительные антивирусные средства.

## 2.3. Защита информации в телекоммуникационных системах (Интернет, ЕИТКС ОВД)

### 2.3.1. Угрозы информационной безопасности в телекоммуникационных системах

Хаотичный и в ряде случаев неконтролируемый рост числа абонентов сети, увеличение объемов хранимой и передаваемой информации, территориальная разнесенность сетей приводят к возрастанию потенциально возможного количества преднамеренных и непреднамеренных нарушений безопасности информации, уязвимых звеньев или возможных каналов несанкционированного проникновения в сеть.

Соотношение внешних и внутренних угроз примерно можно охарактеризовать следующим образом: 82% угроз совершается самими сотрудниками и пользователями компьютеров при их непосредственном или опосредованном участии; 17% - внешние угрозы и наконец 1% - угрозы совершаемые случайными лицами.

Под угрозой информационной безопасности понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию ресурсов сети, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства.

При построении обобщенной модели угроз информационной безопасности телекоммуникационных систем следует подробно рассмотреть следующие вопросы:

- классификацию угроз информационной безопасности телекоммуникационных систем;
- определение видов представления информации, подлежащей защите в телекоммуникационных системах, и определение возможных каналов ее утечки;
- создание модели вероятного нарушения.

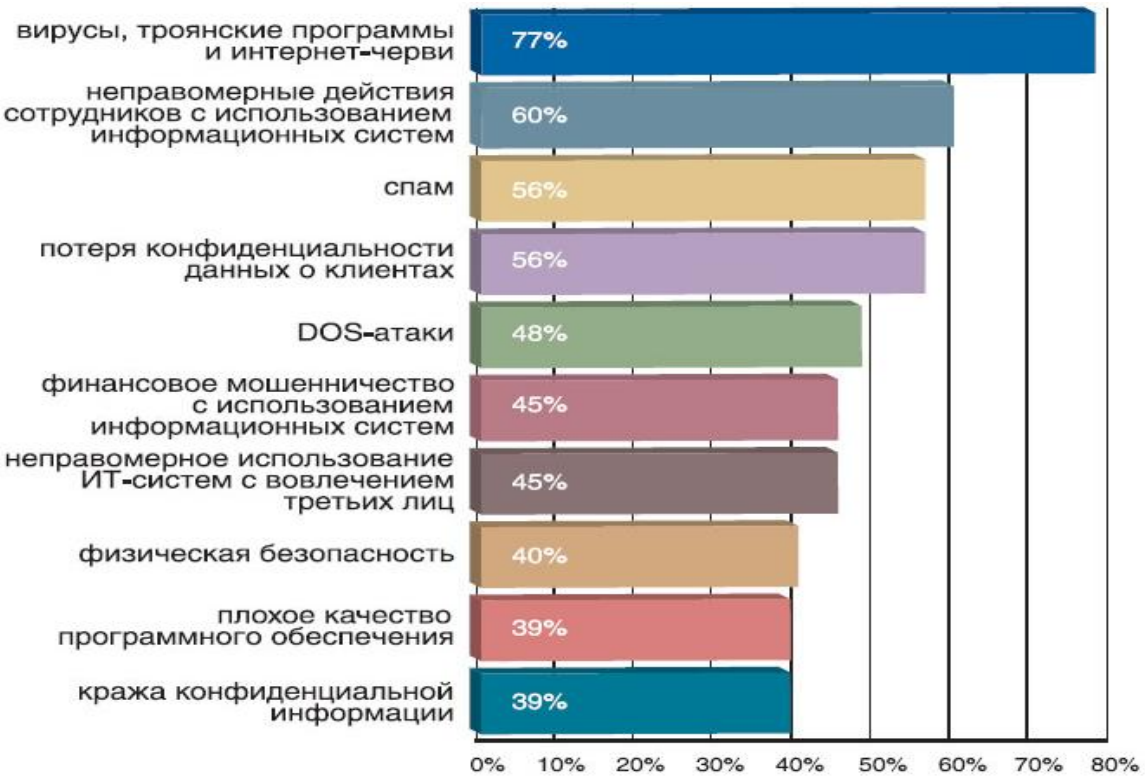


Рис. 7. 10 главных угроз информационной безопасности

Отметим основные проблемы, увеличивающие сложность организации защиты информации в телекоммуникационных системах по сравнению с обычными информационными системами:

1. *Расширение зоны контроля*. Администратор или оператор отдельной системы или подсети должен контролировать деятельность пользователей, находящихся вне пределов его досягаемости, возможно, в другой стране. При этом он должен поддерживать рабочий контакт со своими коллегами в других организациях.

2. *Комбинация различных программно-аппаратных средств*. Соединение нескольких систем, пусть даже однородных по характеристикам, в сеть увеличивает уязвимость всей системы в целом. Система настроена на выполнение своих специфических требований безопасности, которые могут оказаться несовместимыми с требованиями на других системах. В случае соединения разнородных систем риск повышается.

3. *Неизвестный периметр*. Легкая расширяемость сетей ведет к тому, что определить границы сети подчас бывает сложно; один и тот же узел может быть доступен для пользователей различных сетей. Более того, не всегда можно точно определить, сколько пользователей имеют доступ к определенному узлу и кто они.

4. *Множество точек атаки*. В сетях один и тот же набор данных или сообщение могут передаваться через несколько промежуточных узлов, каждый из которых является потенциальным источником угрозы. Это не может способствовать повышению защищенности сети. В списке уязвимых мест сети также фигурируют линии связи и различные виды коммуникационного оборудования: усилители сигнала, ретрансляторы, модемы и т.д.

5. *Сложность управления и контроля доступа к системе*. Многие атаки на сеть могут осуществляться без получения физического доступа к определенному узлу с помощью сети из удаленных точек. В этом случае идентификация нарушителя может оказаться очень сложной, если не невозможной. Кроме того, длительность атаки может оказаться слишком мала для принятия адекватных мер.

### 2.3.2. Классификация угроз информационной безопасности телекоммуникационных систем

По своей сути проблемы защиты сетей обусловлены их двойственным характером. С одной стороны, сеть есть единая система с едиными правилами обработки информации, а с другой – совокупность обособленных систем, каждая из которых имеет свои собственные правила обработки информации.

Защита сетей, как и защита отдельных систем, преследует три цели: поддержание конфиденциальности передаваемой и обрабатываемой в сети информации, целостности и доступности ресурсов (компонентов) сети.

Как и для любой автоматизированной системы, защита сети должна планироваться как единый комплекс мер, охватывающий все особенности обработки информации. В этом смысле организация защиты сети, разработка политики безопасности, ее реализация и управление защитой подчиняются общим правилам. Однако необходимо учитывать, что каждый узел сети должен иметь индивидуальную защиту в зависимости от выполняемых функций и от возможностей сети. При этом защита отдельного узла должна являться частью общей защиты.

Таким образом, защита сети как единой системы складывается из мер защиты каждого отдельного узла и защиты потоков данных сети.

Приведем классификацию угроз, специфических именно для сетей:

1. *Случайные (непреднамеренные) и умышленные (преднамеренные) угрозы*.

Источником первых могут быть ошибки в программном обеспечении, выход из строя аппаратных средств, неправильные действия пользователей или администрации сети и т.п. Умышленные угрозы, в отличие от случайных, преследуют цель нанесения ущерба пользователям (абонентам) сети.

2. *Пассивные и активные угрозы*.

Пассивные угрозы, как правило, направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на функционирование сети. Пассивной угрозой, например, является попытка получения информации, циркулирующей в каналах передачи данных, посредством прослушивания последних.

Активные угрозы имеют цель нарушения нормального процесса функционирования сети посредством целенаправленного воздействия на ее аппаратные, программные и информационные ресурсы.

К активным угрозам относят, например, разрушение или радиоэлектронное подавление линий связи сети передачи данных, вывод из строя ППК или ее операционной системы, искажение сведений в пользовательских базах данных или системной информации сети, разрушение или искажение операционной системы сети и т.п. Источниками таких угроз могут быть непосредственные действия злоумышленников, вредоносное программное обеспечение и т.п.

3. *Внешние и внутренние угрозы*.

К внешним угрозам относятся:

- деятельность иностранных разведывательных и специальных служб;

- деятельность конкурирующих экономических структур;

- деятельность политических и экономических структур, преступных групп и формирований, а также отдельных лиц внутри страны, направленная против интересов граждан, общества и государства и проявляющаяся в виде воздействий на телекоммуникационные системы;

- стихийные бедствия и катастрофы.

К внутренним угрозам относятся:

- нарушения установленных требований информационной безопасности (умышленные либо случайные) по вине пользователей и обслуживающего персонала телекоммуникационной системы;

- отказы и неисправности технических средств обработки, хранения и передачи информации, средств защиты и средств контроля эффективности принятых мер защиты, сбои программного обеспечения.

4. *По способу реализации угрозы: организационные, программно-математические, физические, радиоэлектронные*.

К организационным угрозам информационной безопасности относятся:

- нарушения установленных требований информационной безопасности, допускаемые пользователями и обслуживающим персоналом телекоммуникационной системы;

- несанкционированный доступ пользователей и обслуживающего персонала к информационным ресурсам;

- манипулирование информацией (дезинформация, скрытие или искажение информации);

- несанкционированное копирование данных;

- хищение машинных носителей информации;

- хищение ключевых документов средств криптографической защиты;

- уничтожение или модификация данных.

К программно-математическим угрозам относится внедрение вредоносного программного обеспечения.

Физические угрозы:

- уничтожение или разрушение средств сбора, обработки, передачи, защиты информации, целенаправленное внесение в них неисправностей;

- уничтожение или разрушение машинных носителей информации;

- воздействие на пользователей и обслуживающий персонал с целью реализации физических, программно-математических или организационных угроз.

К радиоэлектронным угрозам относятся:

- перехват информации в технических каналах утечки;

- внедрение электронных средств перехвата информации в аппаратные средства и помещения;

- перехват и дешифрование информации в сетях передачи данных и линиях связи;

- навязывание ложной информации в сетях передачи данных и линиях связи;

- радиоэлектронное подавление линий связи, дезорганизация систем управления телекоммуникационными системами.

Решение проблемы обеспечения безопасности информации в сетях передачи данных должно осуществляться системно на основе оценки эффективности защиты информации, передаваемой по каналам связи, и не должно рассматриваться как чисто техническая задача, которая может быть решена попутно с разработкой элементов сети.

### 2.3.3. Утечка информации в телекоммуникационных системах

Одной из основных причин, обусловливающих сложность решения проблемы защиты конфиденциальной информации в телекоммуникационных сетях, является особенность ее физического

представления. Следует отметить, что при перемещении информации внутри телекоммуникационной системы ее физическое представление может изменяться. Так, хранение информации может осуществляться в виде изменений состояния носителей информации (например, магнитные и оптические диски), представление информации потребителю производится обычно в форме текста или графических изображений на бумаге и экране монитора, звуковых сигналов, передача информации по каналам связи обычно осуществляется в виде электрических сигналов или электромагнитных волн.

Многообразие видов физического представления информации предопределяет наличие различных возможных каналов ее утечки, рассмотренных нами в ходе предыдущей лекции. Следует отметить, что выявление всех возможных каналов утечки информации из телекоммуникационной системы является необходимым условием для определения путей и способов решения проблемы ее защиты, а также конкретных мер по их реализации.

Одним из основных каналов, через которые вероятные нарушители могут получить сведения закрытого характера, является канал побочных электромагнитных излучений и наводок. Это обусловлено его стабильностью, достоверностью и неявной формой получения информации.

Существует определенная классификация методов воздействия нарушителей на безопасность компьютерных сетей, схематично представленная на рисунке 8 ниже.

Выделяют следующие *наиболее характерные приемы проникновения*:

1. Использование точек входа, установленных в системе обслуживающим персоналом, или точек, обнаруженных при проверках цепей системного контроля.

2. Подключение к сети связи специального терминала, обеспечивающего вход в систему под видом законного пользователя ЭВМ, с последующим восстановлением связи по типу ошибочного сообщения, а также в момент, когда законный пользователь не проявляет активности, но продолжает занимать канал связи.

3. Аннулирование сигнала пользователя о завершении работы с системой и последующее продолжение работы от его имени.

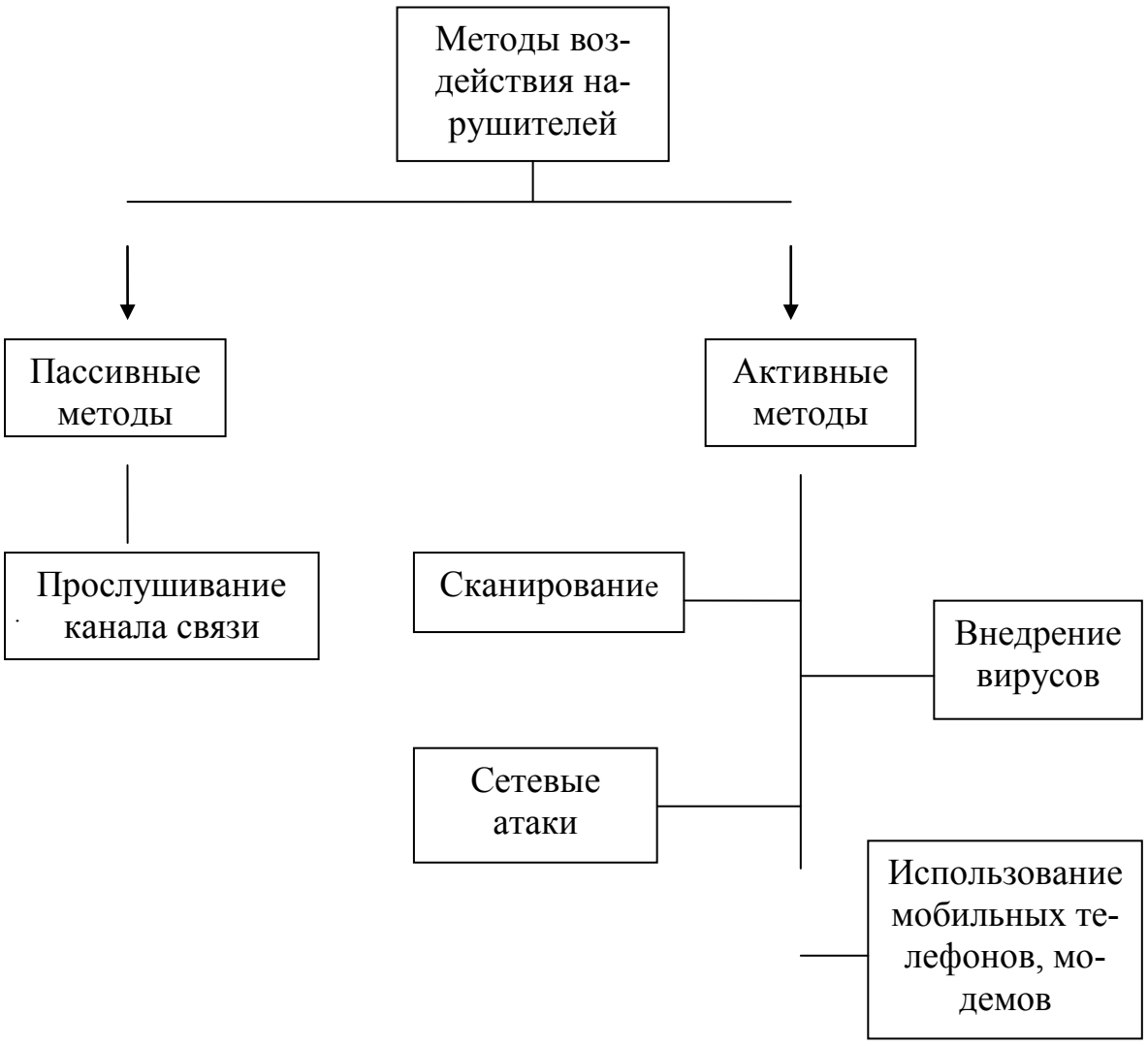


Рис. 8. Классификация методов воздействия нарушителей

### 2.3.4. Несанкционированный доступ к информации телекоммуникационных систем

Несанкционированный доступ к информации, обрабатываемой в телекоммуникационных системах, имеет целью:

- наблюдение за выполнением процессов;
- внесение изменений;
- уничтожение информации;
- ввод ложной информации;
- задержка обработки информации;
- копирование информации;
- изменение маршрута передачи информации;
- повторная передача сообщений.

Обобщенно процесс реализации угроз несанкционированного доступа характеризуется следующим:

- сбор сведений о системе в целом;
- изучение системы защиты информации и выявление ее слабых мест;
- анализ и разработка средств воздействия на средства защиты информации на основе новых информационных технологий;
- разработка средств воздействия на информацию;
- проникновение в систему, преодоление средств зашиты информации и осуществление требуемого воздействия на информацию.

Процесс несанкционированного доступа, как правило, выполняется в два этапа:

1. Сбор сведений о телекоммуникационной системе и встроенных средствах защиты;
2. Выполнение попыток вхождения в систему и осуществление вредоносных действий.

Сбор сведений может осуществляться следующими способами:

- подбором соучастников, подслушиванием разговоров, подключением к телефонным аппаратам, сбором информации по каналам утечки и т.п.;
- изучением утерянных инструкций и документов;
- анализом периодических изданий и документации;
- перехватом сообщений;
- перехватом паролей;
- организацией краж;
- вымогательством, подкупом.

После получения необходимого количества предварительной информации осуществляется непосредственное вторжение в телекоммуникационную систему. Номенклатура и количество используемых при этом средств зависит от количества информации о телекоммуникационной системе, ее достоверности, от разницы во времени между получением информации и попытками входа в систему. Чтобы осуществить несанкционированное вторжение, необходимо иметь доступ к компьютерам, линиям связи, иметь протоколы работы, описание процедур вхождения в систему, коды пользователей и пароли.

Поэтому целесообразно распространять как можно меньше информации о самой телекоммуникационной системе до момента идентификации пользователя и предоставления ему права доступа в систему.

### 2.3.5. Обеспечение информационной безопасности в телекоммуникационных системах

Каждая телекоммуникационная система использует свой комплекс мер защиты информации, направленных на сохранение ее целостности, доступности и конфиденциальности. При этом эффективность защиты информации от преднамеренных воздействий злоумышленников тем выше, чем меньше они знают о применяемых мерах защиты и чем сложнее вскрыть их номенклатуру и параметры.

Многолетнее развитие телекоммуникационных систем и существование непрерывного информационного конфликта привели к появлению и совершенствованию различных мер защиты. При этом можно выделить два основных направления защиты информации:

1. Защита от ошибок;
2. Обеспечение безопасности информации.

Меры по защите от ошибок имеют целью обеспечение доставки информации от источника сообщений к получателю в целости и без искажений в условиях воздействия на сигналы непреднамеренных и преднамеренных разрушающих воздействий различного происхождения.

К мерам защиты от ошибок относятся:

- помехоустойчивое кодирование – для обнаружения и исправления ошибок;
- перемежение символов – для преобразования групповых ошибок в одиночные, наиболее легко обнаруживаемые и исправляемые;
- обратная связь – для исправления обнаруженных ошибок;
- адаптивная перестройка параметров сигнала – для снижения вероятности ошибки и отстройки от помех;
- использование узконаправленных антенн – для повышения энергопотенциала сигнала и отстройки от помех;
- использование помехоустойчивых видов модуляции – для снижения вероятности ошибки и т.д.

Меры обеспечения безопасности информации имеют целью сокрытие содержания передаваемой информации, а по возможности и самого факта передачи, и недопущение навязывания ложной информации.

К таким мерам относятся:

- аутентификация абонентов сети и идентификация их оборудования – для обеспечения работы только с санкционированными корреспондентами;

- шифрование – для сокрытия содержания передаваемых сообщений;

- перестройка параметров сигнала – для сокрытия факта передачи сообщения и его содержания.

Для реализации указанных мер защиты в состав телекоммуникационной системы включаются специальные механизмы – сервисы безопасности. Их содержание может быть представлено следующим образом:

1. *Сервисы идентификации/аутентификации*.

Современные средства идентификации и аутентификации должны удовлетворять двум условиям:

- быть устойчивыми к сетевым угрозам (пассивному и активному прослушиванию сети);

- поддерживать концепцию единого входа в сеть.

Первое требование можно выполнить, используя криптографические методы, рассмотренные нами ранее.

Единый вход в сеть – это, в первую очередь, требование удобства для пользователей. Если в сети много сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация становится слишком обременительной.

2. *Сервисы разграничения доступа*.

Разграничение доступа является самой исследованной областью информационной безопасности. При этом следует отметить, что разграничение доступа направлено не только на защиту от злоумышленников. Современные телекоммуникационные системы характеризуются чрезвычайной сложностью, и их внутренние ошибки представляют не меньшую опасность, чем внешние воздействия.

3. *Сервисы протоколирования и аудита*.

Данные сервисы обеспечивают возможность анализа последствий нарушения информационной безопасности и выявления

злоумышленников. Такой аудит называют пассивным. В последнее время в арсенал защитных средств вошел активный аудит, направленный на выявление подозрительных действий в реальном масштабе времени. Активный аудит включает два вида действий: выявление нетипичного поведения и выявление начала злоумышленных действий.

Нетипичное поведение выявляется статистическими методами путем сопоставления с ранее полученными образцами. Начало злоумышленной активности обнаруживается по совпадению с сигнатурами известных атак.

4. *Сервисы экранирования*.

Межсетевой экран представляет собой программное или аппаратно-программное средство, реализующее контроль за информацией, поступающей в автоматизированную систему или выходящей из нее. Межсетевой экран осуществляет фильтрацию информации по совокупности критериев на основе заранее заданной базы правил, что позволяет реализовывать достаточно гибкую политику безопасности.

Экранирование как сервис безопасности выполняет следующие функции:

- разграничение межсетевого доступа путем фильтрации передаваемых данных;
- преобразование передаваемых данных.

Преобразование передаваемых данных может затрагивать как прикладные данные, так и служебную информацию. Преобразование служебной информации, как правило, осуществляется путем трансляции адресов, позволяющей скрыть топологию защищаемой системы. Преобразование данных может состоять в их шифровании и/или сжатии.

В процессе экранирования может выполняться дополнительный контроль, например, антивирусная проверка.

5. *Сервисы туннелирования*.

Их суть состоит в том, чтобы «упаковать» передаваемую порцию данных вместе со служебной информацией в новый «конверт». Данные сервисы могут применяться в целях:

- осуществления перехода между сетями с разными протоколами;
- обеспечения конфиденциальности и целостности всей передаваемой информации, включая служебную.

Комбинация туннелирования и шифрования позволяет реализовать такое важное в современных условиях защитное средство, как

виртуальные частные сети. Такие сети, наложенные поверх сетей общего пользования (например, сети Интернет), существенно дешевле и безопаснее, чем действительно собственные сети на выделенных каналах.

6. *Сервисы шифрования*.

Шифрование – важнейшая средство обеспечения конфиденциальности и одновременно самое конфликтное место информационной безопасности. У компьютерной криптографии две стороны – собственно криптографическая и интерфейсная, позволяющая сервисам шифрования взаимодействовать с другими сервисами телекоммуникационной системы. При этом важно, чтобы были обеспечены достаточное функциональное богатство интерфейсов и их стандартизация.

7. *Сервисы контроля целостности*.

Контроль целостность призван охранять потоки данных от несанкционированной модификации.

8. *Сервисы контроля защищенности*.

Идея данного сервиса в том, чтобы обнаружить слабости в защите раньше злоумышленников. Это реализуется посредством попыток «взлома» телекоммуникационной системы силами обслуживающего персонала системы.

9. *Сервисы обнаружения отказов и оперативного восстановления*.

Обнаружение отказов и оперативное восстановление обеспечивают высокую доступность телекоммуникационной системы. Работа этих сервисов опирается на существование избыточности в аппаратно-программной конфигурации системы.

10. *Сервисы управления*.

Эти сервисы отвечают за нормальную совместную работу функционально полезных компонентов телекоммуникационной системы и других сервисов безопасности. Сложность современных систем такова, что без правильно организованного управления они постепенно деградируют как в плане эффективности, так и в плане защищенности.

## Заключение

Широкое использование компьютерной техники в деятельности органов внутренних дел требует обеспечения защиты информации от её уничтожения, утечки и т.п.

В российском законодательстве имеется немало нормативных правовых актов, направленных на обеспечение информационной безопасности, но без правильной организации защиты информации техническими и программными методами, обеспечением режима секретности и пр., грамотных специалистов в области защиты информации в современном обществе невозможно обеспечить её полную безопасность.

Режим секретности представляет собой комплекс мер по защите информации на конкретном объекте (в министерстве, ведомстве, организации) или при выполнении определенной работы. Основная задача режима секретности заключается в установлении на режимном объекте уровня защиты информации, соответствующего степени секретности имеющихся там защищаемых сведений.

Направления защиты информации определяются используемыми мероприятиями по обеспечению защиты секретных и конфиденциальных сведений.

Каждый сотрудник органов внутренних дел должен прекрасно понимать, что он является источником огромной информации, при этом используя информационные технологии, не должен забывать о защите служебной информации, использовать все имеющиеся методы для её защиты от любых угроз.

Однако рост количества и качества угроз безопасности информации в компьютерных системах и телекоммуникационных сетях не всегда ведет к адекватному ответу на создание надежной системы и безопасных информационных технологий. Но к, сожалению, в настоящее время в большинстве организаций, в т.ч. в подразделениях ОВД в качестве средств защиты используются только антивирусные программы и разграничение прав доступа пользователей на основе паролей.

# ЛИТЕРАТУРА


***а) нормативные правовые акты:***

1. Конституция Российской Федерации. – М., 2015.
2. Кодекс Российской Федерации об административных правонарушениях. - М., 2015.
3. Уголовный кодекс Российской Федерации. - М., 2015.
4. Гражданский кодекс РФ. - М., 2015.
5. Трудовой кодекс Российской Федерации. - М., 2015.
6. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 №149-ФЗ //Российская газета. 2006. №165.
7. О персональных данных: Федеральный закон от 27 июля 2006 №152-ФЗ //Российская газета. 2006. №165.
8. О государственной тайне: Федеральный закон от 21 июня 1993 г. № 5485-I //Российская газета. 1993. №182.
9. О коммерческой тайне: Федеральный закон от 29 июля 2004 г. № 98-ФЗ //Российская газета. 2004. №166.
10. О безопасности: Федеральный закон от 28 декабря 2010 г. № 390-ФЗ // Российская газета. 2010. №295.
11. О ратификации Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации: Федеральный закон от 1 октября 2008 г. №164-ФЗ //Российская газета. 2008. №62.
12. О лицензировании отдельных видов деятельности: Федеральный закон от 4 мая 2011 г. № 99-ФЗ //Российская газета. 2011. №97.
13. О техническом регулировании: Федеральный закон от 27 декабря 2002 г. № 184-ФЗ //Российская газета. 2002. №245.
14. Об электронной подписи: Федеральный закон от 6 апреля 2011 г. № 63-ФЗ //Российская газета. 2011. №75.
15. О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера: Федеральный закон 21 декабря 1994 г. № 68-ФЗ //Российская газета. 1994. №250.
16. Доктрина информационной безопасности Российской Федерации: утв. Президентом РФ 09.09.2000 №Пр-1895 //Российская газета. 2000. № 187.
17. О Стратегии национальной безопасности Российской Федерации до 2020 года: Указ Президента Российской Федерации от 12 мая 2009 г. № 537 //Собрание законодательства РФ. – 2009. – № 20. – Ст. 2444.
18. Защита информации. Основные термины и определения: ГОСТ Р 50922-2006 //Утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст.
19. Защита информации. Система стандартов. Основные положения: ГОСТ Р 52069.0-2013 //Утвержден приказом Федерального агентства по техническому регулированию и метрологии от 28 февраля 2013 г. № 3-ст.

20. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий: ГОСТ Р ИСО/МЭК 18045-2013 //Утвержден приказом Федерального агентства по техническому регулированию и метрологии от 28 августа 2013 г. № 624-ст.

21. Об утверждении национального стандарта: приказ Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. №531-ст. //Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения: ГОСТ Р 53113.1-2008.

22. Об утверждении национального стандарта: приказ Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 г. №841-ст. //Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов: ГОСТ Р 53113.2-2009.

***б) основная литература:***

1. Мельников В.П. Информационная безопасность и защита информации: учебное пособие /В.П. Мельников, С.А. Клейменов, А.В. Петраков. – М., Академия, 2011.

2. Чуянов А. Г. Обеспечение информационной безопасности в компьютерных системах: учебное пособие / А.Г. Чуянов, А.А. Симаков. - М.: ФГКУ ВНИИ МВД России, 2012. - 204 с.

3. Кемпф В. А. Основы информационной безопасности органов внутренних дел: учебное пособие / В. А. Кемпф. - Барнаул: Барнаульский юридический институт МВД России, 2014. - 104 с.

***в) дополнительная литература:***

1. Прокопенко А.Н. Правовое регулирование информационных ресурсов МВД России: монография / А.Н. Прокопенко. - Белгород: БелЮИ МВД России, 2010.

2. Смирнов А. А. Система обеспечения информационной безопасности в Европейском Союзе: монография / А.А. Смирнов. - М.: ФГКУ "ВНИИ МВД России", 2012. - 164 с.

3. Гашков С.Б. Криптографические методы защиты информации: учебное пособие /С.Б. Гашков, Э.А. Применко, М.А. Черепнев. – М., Академия, 2010.

**УЧЕБНОЕ ИЗДАНИЕ**

Панченко Владислав Вячеславович
Гудочкин Григорий Анатольевич

# ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

***Учебное пособие***

Корректор Н.А. Климанова

Подписано в печать 04.04.2016 Формат 60х90 1/16
Усл. печ. л. 5,4 Тираж 30 экз.

Типография КЮИ МВД России
420108, г. Казань, ул. Магистральная, 35