## **СОДЕРЖАНИЕ**

Введение 3

1. Основные положения теории защиты информации 5

1.1. Сущность проблемы и задачи защиты информации в информационных и телекоммуникационных сетях 5

1.2. Угрозы информации. Способы их воздействия на объекты защиты информации 8

2. Методы и средства защиты информации 14

2.1. Традиционные меры и методы защиты информации 14

2.2. Криптографические методы и средства защиты информа-ции 19

2.3. Нетрадиционные методы защиты информации 23

3. Информационная безопасность предприятия 26

3.1. Концепция информационной безопасности предприятия 26

3.2. Методы защита информации в телекоммуникационных сетях предприятия 31

Заключение 36

Библиографический список литературы 38

**Введение**

Актуальность темы курсовой работы. Применение вычислительных средств в системе управления государственных и коммерческих структур требует наличия мощных систем обработки и передачи данных. Решение этой задачи привело к созданию единой инфраструктуры. Ее использование позволило людям, имеющим компьютер и модем, получить доступ к информации крупнейших библиотек и баз, данных мира, оперативно выполнять сложнейшие расчеты, быстро обмениваться информацией с другими респондентами сети независимо от расстояния и страны проживания.

Но такие системы повлекли ряд проблем, одна из которых - безопасность обработки и передачи данных. Особенно "беззащитными" оказались данные, передаваемые в глобальных телекоммуникационных сетях. В настоящее время над проблемой защищенности передаваемой по сетям информации работает большое количество специалистов практически во всех экономически развитых странах мира. Можно сказать, что информационная безопасность сформировалась в отдельную быстро развивающуюся дисциплину. Однако, несмотря на усилия многочисленных организаций, занимающихся защитой информации, обеспечение информационной безопасности продолжает оставаться чрезвычайно острой проблемой.

Определенные трудности связаны с изменениями в технологиях обработки и передачи информации. С одной стороны, использование информационных технологий дает ряд очевидных преимуществ: повышение эффективности процессов управления, обработки и передачи данных и т.п. В наше время уже невозможно представить крупную организацию без применения новейших информационных технологий, начиная от автоматизации отдельных рабочих мест и заканчивая построением корпоративных распределенных информационных систем.

С другой стороны, развитие сетей, их усложнение, взаимная интеграция, открытость приводят к появлению качественно новых угроз, увеличению числа злоумышленников, имеющих потенциальную возможность воздействовать на систему.

В настоящее время для обеспечения защиты информации требуется не просто разработка частных механизмов защиты, а реализация системного подхода, включающего комплекс взаимосвязанных мер (использование специальных технических и программных средств, организационных мероприятий, нормативно-правовых актов, морально- этических мер противодействия и т.д.). Комплексный характер защиты проистекает из комплексных действий злоумышленников, стремящихся любыми средствами добыть важную для них информацию.

Сегодня можно утверждать, что рождается новая современная технология — технология защиты информации в телекоммуникационных сетях.

Объектом исследования является информация, передаваемая по телекоммуникационным сетям.

Предметом исследования является информационная безопасность телекоммуникационных сетей.

Основной целью курсовой работы является изучение методов защиты информации в телекоммуникационных сетях.

Поставленная цель достигается путем решения следующих задач:

1. Обозначить сущность проблемы и рассмотреть задачи защиты информации в информационных и телекоммуникационных сетях.

2. Установить угрозы информации и способы их воздействия на объекты защиты информации.

3. Рассмотреть методы и средства защиты информации.

4. Раскрыть концепцию информационной безопасности предприятия.

5. Охарактеризовать методы защита информации в телекоммуникационных сетях предприятия.

Структура курсовой работы. В соответствии с целью, задачами и логикой исследования работа состоит из введения, 3 глав, заключения, библиографического списка литературы.

## **1. Основные положения теории защиты информации**

#### 1.1. Сущность проблемы и задачи защиты информации в информационных и телекоммуникационных сетях

Широкое применение компьютерных технологий в автоматизированных системах обработки информации и управления привело к обострению проблемы защиты информации, циркулирующей в компьютерных системах, от несанкционированного доступа. Защита информации в компьютерных системах обладает рядом специфических особенностей, связанных с тем, что информация не является жёстко связанной с носителем, может легко и быстро копироваться и передаваться по каналам связи. Известно очень большое число угроз информации, которые могут быть реализованы как со стороны внешних нарушителей, так и со стороны внутренних нарушителей.

В области защиты информации и компьютерной безопасности в целом наиболее актуальными являются три группы проблем[[1]](#footnote-1):

1. нарушение конфиденциальности информации;
2. нарушение целостности информации;
3. нарушение работоспособности информационно-вычислительных систем.

Защита информации превращается в важнейшую проблему государственной безопасности, когда речь идет о государственной, дипломатической, военной, промышленной, медицинской, финансовой и другой доверительной, секретной информации. Огромные массивы такой информации хранятся в электронных архивах, обрабатываются в информационных системах и передаются по телекоммуникационным сетям. Основные свойства этой информации - конфиденциальность и целостность, должны поддерживаться законодательно, юридически, а также организационными, техническими и программными методами.

Конфиденциальность информации (от лат. confidentia - доверие) предполагает введение определенных ограничений на круг лиц, имеющих доступ к данной информации. Степень конфиденциальности выражается некоторой установленной характеристикой (особая важность, совершенно секретно, секретно, для служебного пользования, не для печати и т.п.), которая субъективно определяется владельцем информации в зависимости от содержания сведений, которые не подлежат огласке, предназначены ограниченному кругу лиц, являются секретом. Естественно, установленная степень конфиденциальности информации должна сохраняться при ее обработке в информационных системах и при передаче по телекоммуникационным сетям.

Другим важным свойством информации является ее целостность (integrty). Информация целостна, если она в любой момент времени правильно (адекватно) отражает свою предметную область. Целостность информации в информационных системах обеспечивается своевременным вводом в нее достоверной (верной) информации, подтверждением истинности информации, защитой от искажений и разрушения (стирания).

Несанкционированный доступ к информации лиц, не допущенных к ней, умышленные или неумышленные ошибки операторов, пользователей или программ, неверные изменения информации вследствие сбоев оборудования приводят к нарушению этих важнейших свойств информации и делают ее непригодной и даже опасной. Ее использование может привести к материальному и/или моральному ущербу, поэтому создание системы защиты информации, становится актуальной задачей. Под безопасностью информации (information security) понимают защищенность информации от нежелательного ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Безопасность информации в информационной системе или телекоммуникационной сети обеспечивается способностью этой системы сохранять конфиденциальность информации при ее вводе, выводе, передаче, обработке и хранении, а также противостоять ее разрушению, хищению или искажению. Безопасность информации обеспечивается путем организации допуска к ней, защиты ее от перехвата, искажения и введения ложной информации. С этой целью применяются физические, технические, аппаратные, программно-аппаратные и программные средства защиты. Последние занимают центральное место в системе обеспечения безопасности информации в информационных системах и телекоммуникационных сетях.

Задачи обеспечения безопасности[[2]](#footnote-2):

- защита информации в каналах связи и базах данных криптографическими методами;

- подтверждение подлинности объектов данных и пользователей (аутентификация сторон, устанавливающих связь);

- обнаружение нарушений целостности объектов данных;

- обеспечение защиты технических средств и помещений, в которых ведется обработка конфиденциальной информации, от утечки по побочным каналам и от возможно внедренных в них электронных устройств съема информации;

- обеспечение защиты программных продуктов и средств вычислительной техники от внедрения в них программных вирусов и закладок;

- защита от несанкционированных действий по каналу связи от лиц, не допущенных к средствам шифрования, но преследующих цели компрометации секретной информации и дезорганизации работы абонентских пунктов;

- организационно-технические мероприятия, направленные на обеспечение сохранности конфиденциальных данных.

**1.2. Угрозы информации. Способы их воздействия на объекты защиты информации**

Угрозу отождествляют обычно либо с характером (видом, способом) дестабилизирующего воздействия на информацию, либо с последствиями (результатами) такого воздействия. Однако такого рода термины могут иметь много трактовок. Возможен и иной подход к определению угрозы безопасности информации, базирующийся на понятии «угроза».

В соответствии со «Словарем русского языка» Ожегова, «угроза» - это намерение нанести физический, материальный или иной вред общественным или личным интересам, возможная опасность.

Иначе говоря, понятие угроза жестко связано с юридической категорией «ущерб», которую Гражданский Кодекс определяет как «фактические расходы, понесенные субъектом в результате нарушения его прав (например, разглашения или использования нарушителем конфиденциальной информации), утраты или повреждения имущества, а также расходы, которые он должен будет произвести для восстановления нарушенного права и стоимости поврежденного или утраченного имущества»[[3]](#footnote-3).

Анализ негативных последствий реализации угроз предполагает обязательную идентификацию возможных источников угроз, уязвимостей, способствующих их проявлению и методов реализации. И тогда цепочка вырастает в схему, представленную на рис. 1.1.

Угрозы классифицируются по возможности нанесения ущерба субъекту отношений при нарушении целей безопасности. Ущерб может быть причинен каким-либо субъектом (преступление, вина или небрежность), а также стать следствием, не зависящим от субъекта проявлений. Угроз не так уж и много. При обеспечении конфиденциальности информации это может быть хищение (копирование) информации и средств ее обработки, а также ее утрата (неумышленная потеря, утечка).



Рис. 1.1. Модель реализации угроз информационной безопасности

Источник: Вихорев С., Кобцев Р. Как определить источники угроз.//Открытые системы. – 2002. - №07-08.С.43.

При обеспечении целостности информации список угроз таков: модификация (искажение) информации; отрицание подлинности информации; навязывание ложной информации. При обеспечении доступности информации возможно ее блокирование, либо уничтожение самой информации и средств ее обработки.

Все источники угроз можно разделить на классы, обусловленные типом носителя, а классы на группы по местоположению (рис. 1.2а).

Уязвимости также можно разделить на классы по принадлежности к источнику уязвимостей, а классы на группы и подгруппы по проявлениям (рис.1.2б). Методы реализации можно разделить на группы по способам реализации (рис.1.2в). При этом необходимо учитывать, что само понятие «метод», применимо только при рассмотрении реализации угроз антропогенными источниками.

Для техногенных и стихийных источников это понятие трансформируется в понятие «предпосылка».



Рис. 1.2. Структура классификаций:

а) «Источники угроз»;

б) «Уязвимости»;

в) «Методы реализации»

Источник: Вихорев С., Кобцев Р. Как определить источники угроз.//Открытые системы. – 2002. - №07-08.С.56.

Классификация возможностей реализации угроз (атак), представляет собой совокупность возможных вариантов действий источника угроз определенными методами реализации с использованием уязвимостей, которые приводят к реализации целей атаки. Цель атаки может не совпадать с целью реализации угроз и может быть направлена на получение промежуточного результата, необходимого для достижения в дальнейшем реализации угрозы. В случае такого несовпадения атака рассматривается как этап подготовки к совершению действий, направленных на реализацию угрозы, т.е. как «подготовка к совершению» противоправного действия. Результатом атаки являются последствия, которые являются реализацией угрозы и/или способствуют такой реализации.

Сам подход к анализу и оценке состояния безопасности информации основывается на вычислении весовых коэффициентов опасности для источников угроз и уязвимостей, сравнения этих коэффициентов с заранее заданным критерием и последовательном сокращении (исключении) полного перечня возможных источников угроз и уязвимостей до минимально актуального для конкретного объекта.

Исходными данными для проведения оценки и анализа служат результаты анкетирования субъектов отношений, направленные на уяснение направленности их деятельности, предполагаемых приоритетов целей безопасности, задач, решаемых автоматизированной системой и условий расположения и эксплуатации объекта. Благодаря такому подходу возможно:

• установить приоритеты целей безопасности для субъекта отношений;

• определить перечень актуальных источников угроз;

•определить перечень актуальных уязвимостей;

• оценить взаимосвязь угроз, источников угроз и уязвимостей;

• определить перечень возможных атак на объект;

• описать возможные последствия реализации угроз.

Источники угроз безопасности информации подразделяются на внешние и внутренние.

К внешним источникам относятся:

- недружественная политика иностранных государств в области информационного мониторинга, распространения информации и новых информационных технологий;

- деятельность иностранных разведывательных и специальных, направленная против интересов Российской Федерации;

- деятельность иностранных экономических структур, направленная против интересов Российской Федерации;

- преступные действия международных групп, формирований и отдельных лиц;

- стихийные бедствия и катастрофы.

Внутренними источниками являются:

- противозаконная деятельность политических, экономических и криминальных структур и отдельных лиц в области формирования, распространения и использования информации, направленная в т.ч. и на нанесение экономического ущерба государству;

- неправомерные действия различных структур и ведомств, приводящие к нарушению законных прав работников в информационной сфере;

- нарушения установленных регламентов сбора, обработки и передачи информации;

- преднамеренные действия и непреднамеренные ошибки персонала автоматизированных систем, приводящие к утечке, уничтожению, искажению, подделке, блокированию, задержке, несанкционированному копированию информации;

- отказы технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

- каналы побочных электромагнитных излучений и наводок технических средств обработки информации.

Способы воздействия угроз на объекты защиты информации подразделяются на информационные, аппаратно-программные, физические, радиоэлектронные и организационно-правовые.

К информационным способам относятся:

- нарушение адресности и своевременности информационного обмена;

- несанкционированный доступ к информационным ресурсам;

- незаконное копирование данных в информационных системах;

- хищение информации из банков и баз данных;

- нарушение технологии обработки информации.

Аппаратно-программные способы включают:

- внедрение компьютерных вирусов;

- установку программных и аппаратных закладных устройств;

- уничтожение или модификацию данных в информационных системах.

Физические способы включают:

- уничтожение или разрушение средств обработки информации и связи;

- уничтожение, разрушение или хищение машинных или других оригиналов носителей информации;

- хищение аппаратных или программных ключей и средств криптографической защиты информации;

- воздействие на персонал;

- поставку "зараженных" компонентов информационных систем.

Радиоэлектронными способами являются:

- перехват информации в технических каналах ее утечки;

- внедрение электронных устройств перехвата информации в технические средства передачи информации и помещения;

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

- воздействие на парольно-ключевые системы;

- радиоэлектронное подавление линий связи и систем управления.

Организационно-правовые способы включают:

- закупки несовершенных или устаревших информационных технологий и компьютерных средств;

- невыполнение требований законодательства Российской Федерации в информационной сфере;

- неправомерное ограничение доступа к документам, содержащим важную для граждан и органов информацию.

Таким образом, надежная защита телекоммуникационных сетей от различного вида угроз возможна только на основе построения комплексной системы безопасности информации на всех этапах разработки, ввода в действие, модернизации аппаратно-программных средств телекоммуникаций, а также при обработке, хранении и передаче по каналам связи информации с широким применением современных средств криптографической защиты, которая бы включала в себя взаимоувязанные меры различных уровней: нормативно-правового; организационного (административного); программно-аппаратного; технического.

## **2. Методы и средства защиты информации**

#### 2.1. Традиционные меры и методы защиты информации

Для обеспечения безопасности информации в офисных сетях проводятся различные мероприятия, объединяемые понятием «система защиты информации». Система защиты информации – это совокупность мер, программно-технических средств, правовых и морально-этических норм, направленных на противодействие угрозам нарушителей с целью сведения до минимума возможного ущерба пользователям и владельцам системы.

Традиционные меры для противо­дей­ствия утечкам информации подразделяются на технические и организационные[[4]](#footnote-4).

К техническим мерам можно отнести защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

К организационным мерам можно отнести охрану серверов, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности сервера после выхода его из строя, универсальность средств защиты от всех пользователей (включая высшее руководство).

Несанкционированный доступ к информации может происходить во время профилактики или ремонта компьютеров за счет прочтения остаточной информации на носителях, несмотря на ее удаление пользователем обычными методами. Другой способ – прочтение информации с носителя во время его транспортировки без охраны внутри объекта или региона.

Современные компьютерные средства построены на интегральных схемах. При работе таких схем происходят высокочастотные изменения уровней напряжения и токов, что приводит к возникновению в цепях питания, в эфире, в близрасположенной аппаратуре и т.п. электромагнитных полей и наводок, которые с помощью специальных средств (условно назовем их "шпионскими") можно трансформировать в обрабатываемую информацию. С уменьшением расстояния между приемником нарушителя и аппаратными средствами вероятность такого рода съема и расшифровки информации увеличивается.

Несанкционированное ознакомление с информацией возможно также путем непосредственного подключения нарушителем «шпионских» средств к каналам связи и сетевым аппаратным средствам.

Традиционными методами защиты информации от несанкционированного доступа являются идентификация и аутентификация, защита паролями.[[5]](#footnote-5)

Идентификация и аутентификация. В компьютерных системах сосредоточивается информация, право на пользование которой принадлежит определенным лицам или группам лиц, действующим в порядке личной инициативы или в соответствии с должностными обязанностями. Чтобы обеспечить безопасность информационных ресурсов, устранить возможность несанкционированного доступа, усилить контроль санкционированного доступа к конфиденциальной либо к подлежащей засекречиванию информации, внедряются различные системы опознавания, установления подлинности объекта (субъекта) и разграничения доступа. В основе построения таких систем находится принцип допуска и выполнения только таких обращений к информации, в которых присутствуют соответствующие признаки разрешенных полномочий.

Ключевыми понятиями в этой системе являются идентификация и аутентификация. Идентификация – это присвоение какому-либо объекту или субъекту уникального имени или образа. Аутентификация – это установление подлинности, т.е. проверка, является ли объект (субъект) действительно тем, за кого он себя выдает.

Конечная цель процедур идентификации и аутентификации объекта (субъекта) – допуск его к информации ограниченного пользования в случае положительной проверки либо отказ в допуске в случае отрицательного исхода проверки.

Объектами идентификации и аутентификации могут быть: люди (пользователи, операторы и др.); технические средства (мониторы, рабочие станции, абонентские пункты); документы (ручные, распечатки и др.); магнитные носители информации; информация на экране монитора и др.

Установление подлинности объекта может производиться аппаратным устройством, программой, человеком и т.д.

Защита паролями. Пароль – это совокупность символов, определяющая объект (субъекта). При выборе пароля возникают вопросы о его размере, стойкости к несанкционированному подбору, способам его применения. Естественно, чем больше длина пароля, тем большую безопасность будет обеспечивать система, ибо потребуются большие усилия для его отгадывания. При этом выбор длины пароля в значительной степени определяется развитием технических средств, их элементной базой и быстродействием.

В случае применения пароля необходимо периодически заменять его на новый, чтобы снизить вероятность его перехвата путем прямого хищения носителя, снятия его копии и даже физического принуждения человека. Пароль вводится пользователем в начале взаимодействия с компьютерной системой, иногда и в конце сеанса (в особо ответственных случаях пароль нормального выхода может отличаться от входного). Для правомочности пользователя может предусматриваться ввод пароля через определенные промежутки времени.

Пароль может использоваться для идентификации и установления подлинности терминала, с которого входит в систему пользователь, а также для обратного установления подлинности компьютера по отношению к пользователю.

Для идентификации пользователей могут применяться сложные в плане технической реализации системы, обеспечивающие установление подлинности пользователя на основе анализа его индивидуальных параметров: отпечатков пальцев, рисунка линий руки, радужной оболочки глаз, тембра голоса и др.

Широкое распространение нашли физические методы идентификации с использованием носителей кодов паролей. Такими носителями являются пропуска в контрольно-пропускных системах; пластиковые карты с именем владельца, его кодом, подписью; пластиковые карточки с магнитной полосой; пластиковые карты с встроенной микросхемой (smart-card); карты оптической памяти и др.

Средства защиты информации по методам реализации можно разделить на три группы:

* программные;
* программно-аппаратные;
* аппаратные.

Программными средствами защиты информации называются специально разработанные программы, которые реализуют функции безопасности вычислительной системы, осуществляют функцию ограничения доступа пользователей по паролям, ключам, многоуровневому доступу и т.д. Эти программы могут быть реализованы практически в любой операционной системе, удобной для пользователя. Как правило, эти программные средства обеспечивают достаточно высокую степень защиты системы и имеют умеренные цены. При подключении такой системы в глобальную сеть вероятность взлома защиты увеличивается. Следовательно, этот способ защиты приемлем для локальных замкнутых сетей, не имеющих внешний выход.

Программно-аппаратными средствами называются устройства, реализованные на универсальных или специализированных микропроцессорах, не требующие модификаций в схемотехнике при изменении алгоритма функционирования. Эти устройства также адаптируются в любой операционной системе, имеют большую степень защиты. Они обойдутся несколько дороже (их цена зависит от типа операционной системы). При этом данный тип устройств является самым гибким инструментом, позволяющим вносить изменения в конфигурацию по требованию заказчика. Программно-аппаратные средства обеспечивают высокую степень защиты локальной сети, подключенной к глобальной.

Аппаратными средствами называются устройства, в которых функциональные узлы реализуются на сверхбольших интегральных системах (СБИС) с неизменяемым алгоритмом функционирования. Этот тип устройств адаптируется в любой операционной системе, является самым дорогим в разработке, предъявляет высокие технологические требования при производстве. В то же время эти устройства обладают самой высокой степенью защиты, в них невозможно внедриться и внести конструктивные или программные изменения. Применение аппаратных средств затруднено из-за их высокой стоимости и статичности алгоритма.

Программно-аппаратные средства, уступая аппаратным по скорости, позволяют в то же время легко модифицировать алгоритм функционирования и не обладают недостатками программных методов.

К отдельной группе мер по обеспечению сохранности информации и выявлению несанкционированных запросов относятся программы обнаружения нарушений в режиме реального времени.

#### 

#### 2.2. Криптографические методы и средства защиты информации

Наибольший интерес сегодня вызывают следующие направления теоретических и прикладных исследований: создание и анализ надежности криптографических алгоритмов и протоколов; адаптация алгоритмов к различным аппаратным и программным платформам; использование существующих технологий криптографии в новых прикладных системах; возможность использования технологий криптографии для защиты интеллектуальной собственности. [[6]](#footnote-6)

Интерес к исследованиям по адаптации алгоритмов к различным аппаратным и программным платформам вызван созданием кроссплатформных телекоммуникационных систем на базе единых стандартов на алгоритмы. Один и тот же алгоритм должен эффективно выполняться на самых различных аппаратных и программных платформах от мобильного телефона до маршрутизатора, от смарт-карты до настольного компьютера.

Существующие средства защиты данных в телекоммуникационных сетях можно разделить на две группы по принципу построения ключевой системы и системы аутентификации. К первой группе отнесем средства, использующие для построения ключевой системы и системы аутентификации симметричные криптоалгоритмы, ко второй - асимметричные.

Проведем сравнительный анализ этих систем. Готовое к передаче информационное сообщение, первоначально открытое и незащищенное, зашифровывается и тем самым преобразуется в шифрограмму, т. е. в закрытые текст или графическое изображение документа. В таком виде сообщение передается по каналу связи, даже и не защищенному. Санкционированный пользователь после получения сообщения дешифрует его (т. е. раскрывает) посредством обратного преобразования криптограммы, вследствие чего получается исходный, открытый вид сообщения, доступный для восприятия санкционированным пользователям.

Методу преобразования в криптографической системе соответствует использование специального алгоритма. Действие такого алгоритма запускается уникальным числом (последовательностью бит), обычно называемым шифрующим ключом. Для большинства систем схема генератора ключа может представлять собой набор инструкций и команд либо узел аппаратуры, либо компьютерную программу, либо все это вместе, но в любом случае процесс шифрования (дешифрования) реализуется только этим специальным ключом. Чтобы обмен зашифрованными данными проходил успешно, как отправителю, так и получателю, необходимо знать правильную ключевую установку и хранить ее в тайне.

Стойкость любой системы закрытой связи определяется степенью секретности используемого в ней ключа. Тем не менее, этот ключ должен быть известен другим пользователям сети, чтобы они могли свободно обмениваться зашифрованными сообщениями. В этом смысле криптографические системы также помогают решить проблему аутентификации (установления подлинности) принятой информации. Взломщик в случае перехвата сообщения будет иметь дело только с зашифрованным текстом, а истинный получатель, принимая сообщения, закрытые известным ему и отправителю ключом, будет надежно защищен от возможной дезинформации.

Кроме того, существует возможность шифрования информации и более простым способом — с использованием генератора псевдослучайных чисел. Использование генератора псевдослучайных чисел заключается в генерации гаммы шифра с помощью генератора псевдослучайных чисел при определенном ключе и наложении полученной гаммы на открытые данные обратимым способом. Этот метод криптографической защиты реализуется достаточно легко и обеспечивает довольно высокую скорость шифрования, однако недостаточно стоек к дешифрованию.

Для классической криптографии характерно использование одной секретной единицы — ключа, который позволяет отправителю зашифровать сообщение, а получателю расшифровать его. В случае шифрования данных, хранимых на магнитных или иных носителях информации, ключ позволяет зашифровать информацию при записи на носитель и расшифровать при чтении с него.

Из изложенного следует, что надежная криптографическая система должна удовлетворять ряду определенных требований[[7]](#footnote-7).

• Процедуры зашифровывания и расшифровывания должны быть «прозрачны» для пользователя.

• Дешифрование закрытой информации должно быть максимально затруднено.

• Содержание передаваемой информации не должно сказываться на эффективности криптографического алгоритма.

Наиболее перспективными системами криптографической защиты данных сегодня считаются асимметричные криптосистемы, называемые также системами с открытым ключом. Их суть состоит в том, что ключ, используемый для зашифровывания, отличен от ключа расшифровывания. При этом ключ зашифровывания не секретен и может быть известен всем пользователям системы. Однако расшифровывание с помощью известного ключа зашифровывания невозможно. Для расшифровывания используется специальный, секретный ключ. Знание открытого ключа не позволяет определить ключ секретный. Таким образом, расшифровать сообщение может только его получатель, владеющий этим секретным ключом.

Специалисты считают, что системы с открытым ключом больше подходят для шифрования передаваемых данных, чем для защиты данных, хранимых на носителях информации.

Одной из важных социально-этических проблем, порождённых всё более расширяющимся применением методов криптографической защиты информации, является противоречие между желанием пользователей защитить свою информацию и передачу сообщений и желанием специальных государственных служб иметь возможность доступа к информации некоторых других организаций и отдельных лиц с целью пресечения незаконной деятельности.

В развитых странах наблюдается широкий спектр мнений о подходах к вопросу о регламентации использования алгоритмов шифрования. Высказываются предложения от полного запрета широкого применения криптографических методов до полной свободы их использования. Некоторые предложения относятся к разрешению использования только ослабленных алгоритмов или к установлению порядка обязательной регистрации ключей шифрования. Чрезвычайно трудно найти оптимальное решение этой проблемы.

Как оценить соотношение потерь законопослушных граждан и организаций от незаконного использования их информации и убытков государства от невозможности получения доступа к зашифрованной информации отдельных групп, скрывающих свою незаконную деятельность? Как можно гарантированно не допустить незаконное использование криптоалгоритмов лицами, которые нарушают и другие законы?

Кроме того, всегда существуют способы скрытого хранения и передачи информации. Эти вопросы ещё предстоит решать социологам, психологам, юристам и политикам.

Криптография предоставляет возможность обеспечить безопасность информации в INTERNET и сейчас активно ведутся работы по внедрению необходимых криптографических механизмов в эту сеть. Не отказ от прогресса в информатизации, а использование современных достижений криптографии – вот стратегически правильное решение. Возможность широкого использования глобальных информационных сетей и криптографии является достижением и признаком демократического общества.

#### 

#### 2.3. Нетрадиционные методы защиты информации

Потребности современной практической информатики привели к возникновению нетрадиционных задач защиты электронной информации, одной из которых является аутентификация электронной информации в условиях, когда обменивающиеся информацией стороны не доверяют друг другу. Эта проблема связана с созданием систем электронной цифровой подписи.

В отечественной литературе прижились три термина для определения одного понятия: электронная подпись; электронно-цифровая подпись (ЭЦП); цифровая подпись. Последний вариант является прямым переводом английского словосочетания digital signature. Термин «цифровая подпись» более удобен и точен.

Федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, а также организации, участвующие в документообороте с указанными органами, используют для подписания своих электронных документов электронные цифровые подписи уполномоченных лиц указанных органов, организаций.

Содержание документа на бумажном носителе, заверенного печатью и преобразованного в электронный документ, в соответствии с нормативными правовыми актами или соглашением сторон может заверяться электронной цифровой подписью уполномоченного лица.

В случаях, установленных законами и иными нормативными правовыми актами Российской Федерации или соглашением сторон, электронная цифровая подпись в электронном документе, сертификат которой содержит необходимые при осуществлении данных отношений сведения о правомочиях его владельца, признается равнозначной собственноручной подписи лица в документе на бумажном носителе, заверенном печатью.

Электронная цифровая подпись - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.[[8]](#footnote-8)

Электронная цифровая подпись представляет собой последовательность символов, полученная в результате криптографического преобразования электронных данных. ЭЦП добавляется к блоку данных и позволяет получателю блока проверить источник и целостность данных и защититься от подделки. ЭЦП используется в качестве аналога собственноручной подписи[[9]](#footnote-9).

Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания. Сертификат ключа подписи - это документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;

- подтверждена подлинность электронной цифровой подписи в электронном документе. Подтверждение подлинности электронной цифровой подписи в электронном документе - положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе;

- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

ЭЦП, как и другие реквизиты документа, выполняющие удостоверительную функцию (собственноручная подпись, печать и др.), является средством, обеспечивающим конфиденциальность информации.

Механизм выполнения собственноручной (физической) подписи непосредственно обусловлен психофизиологическими характеристиками организма человека, в силу чего эта подпись неразрывно связана с биологической личностью подписывающего. Собственноручная подпись позволяет установить (идентифицировать) конкретного человека по признакам почерка.

ЭЦП, являясь криптографическим средством, не может рассматриваться в качестве свойства, присущего непосредственно владельцу ЭЦП как биологической личности. Между ЭЦП и человеком, ее поставившим существует взаимосвязь не биологического, а социального характера. Возникновение, существование и прекращение данной связи обусловлено совокупностью различных правовых, организационных и технических факторов.

Отождествление человека по собственноручной подписи и подтверждение на этой основе подлинности документа, которой он заверен, достигается путем проведения судебно-почерковедческой экспертизы, решающей данную идентификационную задачу.

Определение подлинности ЭЦП свидетельствует только о знании лицом, ее поставившим, закрытого ключа ЭЦП. Для того чтобы установить, действительно ли владелец сертификата ключа заверил документ ЭЦП, надо выяснить помимо подлинности ЭЦП и указанные выше факторы.

Задача установления факта удостоверения электронного документа ЭЦП владельцем сертификата ключа подписи решается в результате процессуальной деятельности по доказыванию в ходе судебного разбирательства.

## **3. Информационная БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ**

#### 3.1. Концепция информационной безопасности предприятия

Отличительным признаком коммерческой деятельности является соизмерение затрат и результатов работы, стремление к получению максимальной прибыли. Кроме того, одной из отличительных особенностей коммерческой деятельности является то, что она осуществляется в условиях жесткой конкуренции, соперничества, борьбы предприятий за получение выгод и преимуществ по сравнению с предприятиями аналогичного профиля.

Конкурентная борьба это спутник и движитель коммерческой деятельности, а также условие выживания коммерческих предприятий. Отсюда их стремление сохранить в секрете от конкурента приемы и особенности своей деятельности, которые обеспечивают им преимущество над конкурентом. Отсюда и стремление конкурентов выявить эти секреты, чтобы использовать их в своих интересах для получения превосходства в конкурентной борьбе. Несанкционированное получение, использование (разглашение) таких секретов без согласия их владельцев отнесены к одной из форм недобросовестной конкуренции, называемой промышленным шпионажем.

Защищаемые секреты коммерческой деятельности получили название коммерческой тайны. Под коммерческой тайной предприятия понимаются не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия, разглашение (передача, утечка), которых может нанести ущерб его интересам.

В Гражданском кодексе РФ изложены основания отнесения информации к коммерческой тайне: информация составляет коммерческую тайну в случае, когда она имеет действительную или потенциальную ценность в силу неизвестности ее третьим лицам, к ней нет доступа на законном основании и обладатель (носитель) информации принимает меры к охране ее конфиденциальности.

Нарушение статуса любой информации заключается в нарушении ее логической структуры и содержания, физической сохранности ее носителя, доступности для правомочных пользователей. Нарушение статуса конфиденциальной информации дополнительно включает нарушение ее конфиденциальности или закрытости для посторонних лиц.

Уязвимость информации следует понимать, как неспособность информации самостоятельно противостоять дестабилизирующим воздействиям, т. е. таким воздействиям, которые нарушают ее установленный статус. [[10]](#footnote-10)

Уязвимость информации проявляется в различных формах. К таким формам, выражающим результаты дестабилизирующего воздействия на информацию, относятся:

- хищение носителя информации или отображенной в нем информации (кража);

- потеря носителя информации (утеря);

- несанкционированное уничтожение носителя информации или отображенной в нем информации (разрушение);

- искажение информации (несанкционированное изменение, подделка, фальсификация);

- блокирование информации;

- разглашение информации (распространение, раскрытие ее содержания).

Та или иная форма уязвимости информации может реализоваться в результате преднамеренного или случайного дестабилизирующего воздействия различными способами на носитель информации или на саму информацию со стороны источников воздействия. Такими источниками могут быть: люди, технические средства обработки и передачи информации, средства связи, стихийные бедствия и др.

Способами дестабилизирующего воздействия на информацию являются ее копирование (фотографирование), записывание, передача, съем, заражение программ обработки информации вирусом, нарушение технологии обработки и хранения информации, вывод (или выход) из строя и нарушение режима работы технических средств обработки и передачи информации, физическое воздействие на информацию и др.

Реализация форм проявления уязвимости информации приводит или может привести к двум видам уязвимости - утрате или утечке информации.

Утечка информации в компьютерных системах может быть допущена как случайно, так и преднамеренно, с использованием технических средств съема информации.

Средства противодействию случайной утечки информации, причиной которой может быть программно-аппаратный сбой или человеческий фактор, могут быть разделены на следующие основные функциональные группы: дублирование информации, повышение надёжности компьютерных систем, создание отказоустойчивых компьютерных систем, оптимизация взаимодействия человека и компьютерной системы, минимизация ущерба от аварий и стихийных бедствий (в том числе, за счет создания распределённых компьютерных систем), блокировка ошибочных операций пользователей.

К утрате информации приводят хищение и потеря носителей информации, несанкционированное уничтожение носителей информации или только отображенной в них информации, искажение и блокирование информации. Утрата может быть полной или частичной, безвозвратной или временной, но в любом случае она наносит ущерб собственнику информации.

Несанкционированный доступ — это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям.

Наиболее распространенными путями несанкционированного доступа к информации являются:

• перехват электронных излучений;

• принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей;

• применение подслушивающих устройств (закладок);

• дистанционное фотографирование;

• перехват акустических излучений и восстановление текста принтера;

• копирование носителей информации с преодолением мер защиты

• маскировка под зарегистрированного пользователя;

• маскировка под запросы системы;

• использование программных ловушек;

• использование недостатков языков программирования и операционных систем;

• незаконное подключение к аппаратуре и линиям связи специально разработанных аппаратных средств, обеспечивающих доступ информации;

• злоумышленный вывод из строя механизмов защиты;

• расшифровка специальными программами зашифрованной: информации;

• информационные инфекции.

Перечисленные пути несанкционированного доступа требуют достаточно больших технических знаний и соответствующих аппаратных или программных разработок со стороны взломщика. Например, используются технические каналы утечки — это физические пути от источника конфиденциальной информации к злоумышленнику, посредством которых возможно получение охраняемых сведений. Причиной возникновения каналов утечки являются конструктивные и технологические несовершенства схемных решений либо эксплуатационный износ элементов. Все это позволяет взломщикам создавать действующие на определенных физических принципах преобразователи, образующие присущий этим принципам канал передачи информации — канал утечки.

Однако есть и достаточно примитивные пути несанкционированного доступа:

хищение носителей информации и документальных отходов;

инициативное сотрудничество;

склонение к сотрудничеству со стороны взломщика;

выпытывание;

подслушивание;

наблюдение и другие пути.

Для обеспечения эффективного применения системы защиты информации в телекоммуникационной сети предприятия при ее построении необходимо учитывать следующие требования:[[11]](#footnote-11)

- эшелонированность. Система защиты должна состоять из нескольких уровней. Нарушение защиты на каком-либо уровне не должно повлечь за собой ослабления других уровней или недееспособности системы защиты в целом; согласованность. Средства защиты, в том числе входящие в региональные составляющие телекоммуникационной сети предприятия, должны обеспечивать возможность их эксплуатации в рамках единой системы;

- интегрируемость. Средства защиты информации должны оптимальным образом встраиваться в инфраструктуру телекоммуникационной сети;

- контролируемость. События, связанные с функционированием системы защиты, должны контролироваться средствами мониторинга безопасности;

- сертифицируемость. Применяемые при построении системы защиты средства должны удовлетворять установленным стандартам и требованиям;

- масштабируемость. При построении системы защиты должна быть обеспечена возможность ее развития с учетом развития телекоммуникационных сетей предприятия.

#### 

#### 3.2. Методы защита информации в телекоммуникационных сетях предприятия

Отраслевой стандарт по информационной безопасности определяет защиту информации как деятельность, направленную на предотвращение утечки информации, несанкционированных и непреднамеренных воздействий на информацию. И если первое направление (предотвращение утечки) должно предупреждать разглашение конфиденциальных сведений, несанкционированный доступ к ним и/или их получение разведками (например, коммерческой разведкой фирм-конкурентов), то два других направления защищают от одинаковых угроз (искажение конфиденциальной информации, ее уничтожение, блокирование доступа и аналогичные действия с носителем информации). Вся разница заключается в наличии или отсутствии умысла в действиях с информацией (рис. 3.1.).



Рис.3.1. Защита информации на предприятии

Источник: Дъяченко С.И. Правовые аспекты работы в ЛВС. –СПб.: «АСТ», 2002.С.34.

Больше всего угроз по-прежнему создают компьютерные вирусы (в число которых помимо традиционных файловых, загрузочных, макровирусов и т. п. вредоносных программ входят также «трояны», «вандалы», перехватчики паролей и т. д.) и атаки распространителей спама.

Многие сети годами остаются открытыми для пришельцев из Интернета, и неизвестно, что в этом случае опаснее — сознательный взлом злоумышленником корпоративной сети для съема конфиденциальной информации или же осуществляемая дезорганизация работы сети с помощью атак типа «отказ в обслуживании». Поскольку для малых и средних коммерческих структур создание специально защищенных линий связи невозможно, приходится использовать открытые каналы для обмена кроме прочего и конфиденциальной информацией, а это чревато как перехватом этой информации, так и нарушением ее целостности или подменой.

Внутри локальной сети актуальна задача надежной аутентификации пользователей: хрестоматийный пример прикрепления к монитору бумажки с записанным логином и паролем.

Зачастую не придается значения разграничению доступа между легальными пользователями. Здесь можно привести такую аналогию: иерархию кабинетов все сотрудники соблюдают свято, никому не приходит в голову оккупировать стол или комнату начальства, а вот по отношению к конфиденциальной информации действует, так сказать, принцип «каждому — по интересам», и сведения, предназначенные двум-трем топ-менеджерам, становятся известны чуть ли не половине фирмы.

В качестве еще одного канала вероятной утечки можно назвать, к примеру, сервис-центры, в которые поступают диски с не уничтоженной должным образом информацией. Наконец, не стоит забывать, что в значительном числе случаев пользователи оперируют информацией не только в электронном, но и в бумажном виде, и регулярное обследование содержимого мусорных ведер, куда отправляются черновики и наброски, может дать вашим конкурентам больше, чем хитроумные атаки и попытки взлома.

Таким образом, можно сделать вывод: защита информации — одно из ключевых направлений деятельности любой успешной фирмы. Перед специально отобранным для этого сотрудником (или подразделением) стоят следующие задачи:

• анализ угроз конфиденциальной информации, а также уязвимых мест автоматизированной системы и их устранение;

•формирование системы защиты информации - закупка и установка необходимых средств, их профилактика и обслуживание;

• обучение пользователей работе со средствами защиты, контроль за соблюдением регламента их применения;

• разработка алгоритма действий в экстремальных ситуациях и проведение регулярных "учений";

• разработка и реализация программы непрерывной деятельности автоматизированной системы и плана восстановительных мероприятий (в случае вирусной атаки, сбоя/ошибки/отказа технических средств и т. д.).

Итак, можно констатировать, что деятельность по защите информации протекает в рамках четырехугольника «руководство компании — служба защиты информации — пользователи», и от доброй воли всех этих сторон зависит, будет ли их сотрудничество эффективным.

С какими же проблемами приходится сталкиваться при построении системы защиты информации[[12]](#footnote-12)?

Метод заплаток. «Кусочное» обеспечение информационной безопасности лишь на отдельных направлениях. Следствие — невозможность отразить атаки на незащищенных участках и дискредитация идеи информационной безопасности в целом.

Синдром амебы. Фрагментарное реагирование на каждый новый раздражитель; часто сочетается с применением «метода заплаток». Следствие — запаздывание с отражением новых угроз, усталость от бесконечной гонки по кругу.

Лекарство от всего. Попытки возложить на одно средство защиты информации все функции обеспечения информационной безопасности (например, стремление отождествить аутентификацию и полный комплекс задач защиты от несанкционированного доступа).

Следствие — непрерывный переход, миграция от одного средства защиты к другому, «более комплексному», последующее разочарование и паралич дальнейших действий.

Волшебная палочка. Вторая ипостась поисков «универсального лекарства», искреннее непонимание необходимости дополнения технических мер защиты организационными. Следствие — предъявление завышенных требований к системе или средству защиты.

Стремление к экономии. Желание построить систему защиты на беззатратной основе. Следствие — применение непроверенных и/или нелицензионных средств защиты, отсутствие поддержки со стороны производителей, постоянные попытки разобраться во всем самостоятельно, неэффективные и разорительные, как и любая самодеятельность.

Таким образом, на предприятии должен быть создан следующий набор средств и методов для защиты информации в сети (табл.3.1)

Таблица 3.1

Средства и методы защиты информации в сети предприятия

|  |  |
| --- | --- |
| Минимальный пакет | Оптимальный пакет (в дополнение к минимуму) |
| Средства антивирусной защиты рабочих станций, файловых и почтовых серверов | Антивирусные средства в программно-аппаратном исполнении; средства контроля содержимого (Content Inspector) и борьбы со спамом |
| Программный межсетевой экран (МЭ) | Программно-аппаратный МЭ, система обнаружения атак (Intrusion Detection System) |
| Программные средства формирования защищенных корпоративных сетей (VPN - Virtual Private Network) | То же в программно-аппаратном исполнении и интеграции с межсетевым экраном |
| Аппаратные средства аутентификации пользователей (токены, смарт-карты, биометрия и т. п.) | То же в интеграции со средствами защиты от несанкционированного доступа (НСД) и криптографическими средствами |
| Разграничение доступа пользователей к конфиденциальной информации штатными механизмами защиты информации и разграничение доступа операционных систем, прикладных программ, маршрутизаторов и т. п. | Программно-аппаратные средства защиты от НСД и разграничения доступа |
| Программные средства шифрования и электронной цифровой подписи (ЭЦП) для обмена конфиденциальной информацией по открытым каналам связи | Аппаратные шифраторы для выработки качественных ключей шифрования и ЭЦП; интеграция со средствами защиты от НСД и аутентификации |
| Средства "прозрачного" шифрования логических дисков пользователей, используемых для хранения конфиденциальной информации | Средства "прозрачного" шифрования конфиденциальной информации, хранимой и обрабатываемой на серверах |
| Средства уничтожения неиспользуемой конфиденциальной информации (например, с помощью соответствующих функций шифраторов) | Аппаратные уничтожители носителей информации |
| Средства резервного копирования, источники бесперебойного питания, уничтожители бумажных документов | |

## **Заключение**

Цель курсового исследования достигнута путём реализации поставленных задач. В результате проведённого исследования по теме "Методы защиты информации в телекоммуникационных сетях" можно сделать ряд выводов:

Проблемы, связанные с повышением безопасности информационной сферы, являются сложными, многоплановыми и взаимосвязанными. Они требуют постоянного, неослабевающего внимания со стороны государства и общества. Развитие информационных технологий побуждает к постоянному приложению совместных усилий по совершенствованию методов и средств, позволяющих достоверно оценивать угрозы безопасности информационной сферы и адекватно реагировать на них.

Предотвращение несанкционированного доступа к конфиденциальной информации, циркулирующей в телекоммуникационных сетях государственного и военного управления, к информации национальных и международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью и международным терроризмом, а также в банковских сетях является важной задачей обеспечения безопасности глобальной информации. Защите информации в последнее время уделяется все большее внимание на самых различных уровнях - и государственном, и коммерческом.

Под защитой информации принято понимать использование различных средств и методов, принятие мер и осуществление мероприятий с целью системного обеспечения надежности передаваемой, хранимой и обрабатываемой информации.

Можно выделить несколько основных задач, решение которых в информационных системах и телекоммуникационных сетях обеспечивает защиту информации.

Это:

- организация доступа к информации только допущенных к ней лиц;

- подтверждение истинности информации;

- защита от перехвата информации при передаче ее по каналам связи;

- защита от искажений и ввода ложной информации.

Защитить информацию – это значит:

* обеспечить физическую целостность информации, т.е. не допустить искажений или уничтожения элементов информации;
* не допустить подмены (модификации) элементов информации при сохранении ее целостности;
* не допустить несанкционированного получения информации лицами или процессами, не имеющими на это соответствующих полномочий;
* быть уверенным в том, что передаваемые (продаваемые) владельцем информации ресурсы будут использоваться только в соответствии с обговоренными сторонами условиями.

Радикальное решение проблем защиты электронной информации может быть получено только на базе использования криптографических методов, которые позволяют решать важнейшие проблемы защищённой автоматизированной обработки и передачи данных. При этом современные скоростные методы криптографического преобразования позволяют сохранить исходную производительность автоматизированных систем.

Криптографические преобразования данных являются наиболее эффективным средством обеспечения конфиденциальности данных, их целостности и подлинности. Только их использование в совокупности с необходимыми техническими и организационными мероприятиями могут обеспечить защиту от широкого спектра потенциальных угроз.

Электронная цифровая подпись (ЭЦП) - вид аналога собственноручной подписи, являющийся средством защиты информации, обеспечивающим возможность контроля целостности и подтверждения подлинности электронных документов.

**Библиографический список литературы**

**I. Источники**

1. Гражданский кодекс Российской Федерации. Часть вторая: Федеральный закон от 26.01.1996 № 14-ФЗ (в ред. от 02.02.2006.).
2. Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации от 27 июля 2006 г. № 149-ФЗ».
3. Федеральный закон Российской Федерации «Об электронной цифровой подписи» от 10 января 2002 года № 1-ФЗ.

**II. Литература**

1. Биячуев, Т.А. Безопасность корпоративных сетей / Т.А. Биячуев. – СПб: СПб ГУ ИТМО, 2004.- 161 с.
2. Вихорев, С. Как определить источники угроз / С. Вихорев, Р.Кобцев //Открытые системы. – 2002. - №07-08.-С.43.
3. Волчков, А. Современная криптография / А.Волчков // Открытые системы.- 2002. - №07-08. –С.48.
4. Гмурман, А.И. Информационная безопасность/ А.И. Гмурман - М.: «БИТ-М», 2004.-387с.
5. Дъяченко, С.И. Правовые аспекты работы в ЛВС/ С.И. Дъяченко–СПб.: «АСТ», 2002.- 234с.
6. Зима, В. Безопасность глобальных сетевых технологий / В.Зима, А. Молдовян, Н. Молдовян – СПб.: BHV, 2000. – 320 с.
7. Информатика: Базовый курс / С.В. Симонович [и др]. – СПб.: Питер, 2002. – 640с.:ил.
8. Конахович, Г. Защита информации в телекоммуникационных системах/ Г.Конахович.-М.:МК-Пресс,2005.- 356с.
9. Коржов, В. Стратегия и тактика защиты / В.Коржов //Computerworld Россия.- 2004.-№14.-С.26.
10. Мельников, В. Защита информации в компьютерных системах / В.Мельников - М.: Финансы и статистика, Электронинформ, 1997. – 400с.
11. Молдовян, А.А. Криптография / А.А.Молдовян, Н.А. Молдовян, Советов Б.Я. – СПб.: Издательство “Лань”, 2001. – 224с.,ил.
12. Осмоловский,  С. А. Стохастические методы защиты информации/ С. А. Осмоловский – М., Радио и связь, 2002. – 187с.
13. Острейковский, В.А. Информатика: Учеб. пособие для студ. сред. проф. учеб. Заведений/ В.А. Острейковский– М.: Высш. шк., 2001. – 319с.:ил.
14. Семенов, Г. Цифровая подпись. Эллиптические кривые / Г.Семенов // Открытые системы.- 2002. - №07-08. – С.67-68.
15. Титоренко, Г.А. Информационные технологии управления/ Г.А. Титоренко - М.: Юнити, 2002.-376с.
16. Устинов, Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий/ Г.Н. Устинов– М.: Радио и связь, 2003.-342с.
17. Шахраманьян, М.А. Новые информационные технологии в задачах обеспечения национальной безопасности России/ Шахраманьян, М.А. – М.: ФЦ ВНИИ ГОЧС, 2003.- 222с.
18. Экономическая информатика / под ред. П.В. Конюховского и Д.Н. Колесова. – СПб.: Питер, 2000. – 560с.:ил.
19. Ярочкин, В.И. Информационная безопасность. Учебник для вузов/ В.И. Ярочкин– М.: Академический Проект, Мир, 2004. – 544 с.

1. Гмурман А.И. Информационная безопасность.- М.: «БИТ-М», 2004.С.23-35. [↑](#footnote-ref-1)
2. Зима В., Молдовян А., Молдовян Н. Безопасность глобальных сетевых технологий. – СПб.: BHV, 2000. С.56. [↑](#footnote-ref-2)
3. Гражданский Кодекс РФ, часть I, ст. 15. [↑](#footnote-ref-3)
4. Конахович Г. Защита информации в телекоммуникационных системах. – М.: МК-Пресс,2005.С.123. [↑](#footnote-ref-4)
5. Коржов В. Стратегия и тактика защиты.//Computerworld Россия.- 2004.-№14.С.26. [↑](#footnote-ref-5)
6. Волчков А. Современная криптография. // Открытые системы.- 2002. №07-08. С.48. [↑](#footnote-ref-6)
7. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. – СПб.: Издательство “Лань”, 2001.С.56-76. [↑](#footnote-ref-7)
8. Федеральный закон "Об электронной цифровой подписи" от 10 января 2002 года № 1-ФЗ, ст.3. [↑](#footnote-ref-8)
9. Семенов Г. Цифровая подпись. // Открытые системы.- 2002. №07-08. С.67-78. [↑](#footnote-ref-9)
10. Устинов Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий. – М.: Радио и связь, 2003.С.128. [↑](#footnote-ref-10)
11. Биячуев Т.А. Безопасность корпоративных сетей / под ред. Л.Г.Осовецкого. – СПб: СПб ГУ ИТМО, 2004.С.187. [↑](#footnote-ref-11)
12. Мельников В. Защита информации в компьютерных системах. - М.: Финансы и статистика, Электронинформ, 1997.С.79-81. [↑](#footnote-ref-12)