**1. Свойства информации**

**1.1 Свойства информации**

Как и всякий объект, информация обладает свойствами. Характерной отличительной особенность информации от других объектов природы и общества, является дуализм: на свойства информации влияют как свойства данных, составляющих её содержательную часть, так и свойства методов, взаимодействующих с данными в ходе информационного процесса. По окончании процесса, свойства информации переносятся на свойства новых данных, т.е. свойства методов могут переходить на свойства данных.

С точки зрения информатики наиболее важными представляются следующие свойства: объективность, полнота, достоверность, адекватность, доступность и актуальность информации.

Понятие объективности информации является относительным, это понятно, если учесть, что методы являются субъективными. Более объективной принято считать ту информацию, в которую методы вносят меньший субъективные элемент.

Полнота информации во многом характеризует её качество и определяет достаточность данных для принятия решений или для создания новых данных на основе имеющихся. Чем полнее данные, тем шире диапазон методов, которые можно использовать, тем проще подобрать метод, вносящий минимум погрешностей в ход информационного процесса.

Данные возникают в момент регистрации сигналов, но не все сигналы являются «полезными» - всегда присутствует какой-то уровень посторонних сигналов, в результате чего полезные данные сопровождаются определённым уровнем «информационного шума». Если полезный сигнал зарегистрирован более чётко, чем посторонние сигналы, достоверность информации может быть более высокой. При увеличении уровня шумов достоверность информации снижается. В этом случае при передаче того же количества информации требуется использовать либо больше данных, либо более сложные методы.

Адекватность информации – степень соответствия реальному объективному состоянию дела. Неадекватная информация может образовываться при создании новой информации на основе неполных или недостоверных данных. Однако и полные, и достоверные данные могут приводить к созданию неадекватной информации в случае применения к ним неадекватных методов.

Доступность информации – мера возможности получить ту или иную информацию. На степень доступности информации влияют одновременно как доступность данных, так и доступность адекватных методов для их интерпретации. Отсутствие доступа к данным или отсутствие адекватных методов обработки приводят к одинаковому результату: информация оказывается недоступной.

Актуальность информации – степень соответствия информации текущему моменту времени. Нередко с актуальностью, как и с полнотой, связывают коммерческую ценность информации. Поскольку информационные процессы растянуты во времени, то достоверная и адекватная, но устаревшая информация может приводить к ошибочным решениям. Необходимость поиска (или разработки) адекватного метода для работы с данными может приводить к такой задержке получения информации, что она становится неактуальной и ненужной. На этом, в частности, основаны многие современные системы шифрования данных с открытым ключом. Лица, не владеющие ключом (методом) для чтения данных, могут заняться поиском ключа, поскольку алгоритм его работы доступен, но продолжительность этого поиска столь велика, что за время работы информация теряет актуальность и, естественно связанную с ней практическую ценность.

**1.2 Носители данных**

Данные – диалектическая составная часть информации. Они представляют собой зарегистрированные сигналы. При этом физический метод регистрации может быть любым: механическое перемещение физических тел, изменение их формы или параметров качества поверхности, изменение электрических, магнитных, оптических характеристик, химического состава или характера химических связей, изменение состояние электронной системы и многое другое. В соответствии с методом регистрации данные могут храниться транспортироваться на носителях различных видов.

Самым распространённым носителем данных, хотя и не самым экономичным является бумага. На бумаге данные регистрируются путём изменения оптических характеристик её поверхности. Изменение оптических свойств используется также в устройствах осуществляющих запись лазерным лучом на пластмассовых носителях с отражающим покрытием (CD-ROM). В качестве носителей, использующих изменение магнитных свойств, можно назвать магнитные ленты и диски. Регистрация данных путём изменения химического состава поверхностных веществ носителя широко используется в фотографии. На биохимическом уровне происходит накопление и передача данных в живой природе. От свойств носителя нередко зависят такие свойства информации, как полнота, доступность и достоверность.

**1.3 Операции с данными**

В ходе информационного процесса данные преобразуются из одного вида в другой с помощью методов. Обработка данных включает в себя множество различных операций. По мере развития научно-технического прогресса и общего усложнения связей в человеческом обществе трудозатраты на обработку данных неуклонно возрастают. Прежде всего, это связано с постоянным усложнением условий управления производством и обществом. Второй фактор, также вызывающий общее увеличение объёмов обрабатываемых данных, тоже связан с научно-техническим прогрессом, а именно с быстрыми темпами появления и внедрения новых носителей данных, средств их хранения и доставки.

Основные операции, которые можно производить с данными:

* сбор данных – накопление информации с целью обеспечения достаточной полноты для принятия решений;
* формализация данных – приведения данных, поступающих из разных источников, к одинаковой форме, чтобы сделать их сопоставимыми между собой, т.е. повысить их уровень доступности;
* фильтрация данных – отсеивание лишних данных, в которых нет необходимости для принятия решений; при этом должен уменьшатся уровень «шума», а достоверность и адекватность данных должны возрастать;
* сортировка данных – упорядочивание данных по заданному признаку с целью удобства использования; повышает доступность информации;
* архивация данных - организация хранения данных в удобной и легкодоступной форме; служит для снижения экономических затрат по хранению данных и повышает общую надёжность информационного процесса в целом;
* защита данных – комплекс мер, направленных на предотвращение утраты, воспроизведения и модификации данных;
* приём передача данных между удалёнными участниками информационного процесса; при этом источник данных в информатике принято называть сервером, а потребителя – клиентом;
* преобразование данных – перевод данных из одной формы в другую или из одной структуры в другую. Преобразование данных часто связано с изменением типа носителя.

**2. Виды умышленных угроз безопасности информации**

**2.1 Пассивные и активные угрозы**

Пассивные угрозы направлены в основном на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на ее функционирование. Например, несанкционированный доступ к базам данных, прослушивание каналов связи и т.д.

Активные угрозы имеют целью нарушение нормального функционирования информационной системы путем целенаправленного воздействия на ее компоненты. К активным угрозам относятся, например, вывод из строя компьютера или его операционной системы, разрушение программного обеспечения компьютеров, нарушение работы линий связи и т.д. Источником активных угроз могут быть действия взломщиков, вредоносные программы и т.п.

Умышленные угрозы подразделяются на внутренние (возникающие внутри управляемой организации) и внешние.

Внутренние угрозы чаще всего определяются социальной напряженностью и тяжелым моральным климатом.

Внешние угрозы могут определяться злонамеренными действиями конкурентов, экономическими условиями и другими причинами (например, стихийными бедствиями). Широкое распространение получил промышленный шпионаж - это наносящий ущерб владельцу коммерческой тайны незаконные сбор, присвоение и передача сведений, составляющих коммерческую тайну, лицом, не уполномоченным на это ее владельцем.

К основным угрозам безопасности информации и нормального функционирования информационных систем относятся:

* ошибочное использование информационных ресурсов;
* несанкционированный обмен информацией между абонентами;
* отказ от информации;
* нарушение информационного обслуживания;
* незаконное использование привилегий.
* утечка конфиденциальной информации;
* компрометация информации;

Ошибочное использование информационных ресурсов будучи санкционированным тем не менее может привести к разрушению, утечке или компрометации указанных ресурсов. Данная угроза чаще всего является следствием ошибок, имеющихся в программном обеспечении информационных технологий.

Несанкционированный обмен информацией между абонентами может привести к получению одним из них сведений, доступ к которым ему запрещен. Последствия — те же, что и при несанкционированном доступе.

Отказ от информации состоит в непризнании получателем или отправителем этой информации фактов ее получения или отправки. Это позволяет одной из сторон расторгать заключенные финансовые соглашения техническим путем, формально не отказываясь от них, нанося тем самым второй стороне значительный ущерб.

Нарушение информационного обслуживания - угроза, источником которой являются информационные технологии. Задержка с предоставлением информационных ресурсов абоненту может привести к тяжелым для него последствиям.

Незаконное использование привилегий. Любая защищенная система содержит средства, используемые в чрезвычайных ситуациях, или средства которые способны функционировать с нарушением существующей политики безопасности. Например, на случай внезапной проверки пользователь должен иметь возможность доступа ко всем наборам системы. Обычно эти средства используются администраторами, операторами, системными программистами и другими пользователями, выполняющими специальные функции.

Компрометация информации (один из видов информационных инфекций). Реализуется, как правило, посредством несанкционированных изменений в базе данных в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений. При использовании скомпрометированной информации потребитель подвергается опасности принятия неверных решений.

Утечка конфиденциальной информации — это бесконтрольный выход конфиденциальной информации за пределы круга лиц, которым она была доверена по службе или стала известна в процессе работы.

Эта утечка может быть следствием:

* разглашения конфиденциальной информации;
* ухода информации по различным, главным образом техническим, каналам;
* несанкционированного доступа к конфиденциальной информации различными способами.

Разглашение информации ее владельцем или обладателем есть умышленные или неосторожные действия должностных лиц и пользователей, которым соответствующие сведения в установленном порядке были доверены по службе или по работе, приведшие к ознакомлению с ним лиц, не допущенных к этим сведениям.

Возможен бесконтрольный уход конфиденциальной информации по визуально-оптическим, акустическим, электромагнитным и другим каналам.

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;
* чтение остаточной информации в памяти системы после выполнения санкционированных запросов;
* 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.

Любые способы утечки конфиденциальной информации могут привести к значительному материальному и моральному ущербу, как для организации, где функционирует информационная система, так и для ее пользователей.

Довольно большая часть причин и условий, создающих предпосылки и возможность неправомерного овладения конфиденциальной информацией, возникает из-за элементарных недоработок руководителей организаций и их сотрудников. Например, к причинам и условиям, создающим предпосылки для утечки коммерческих секретов, могут относиться:

* недостаточное знание работниками организации правил защиты конфиденциальной информации и непонимание необходимости их тщательного соблюдения;
* использование неаттестованных технических средств обработки конфиденциальной информации;
* слабый контроль за соблюдением правил защиты информации правовыми, организационными и инженерно-техническими мерами;
* текучесть кадров, в том числе владеющих сведениями, составляющими коммерческую тайну.

Также большой вред могут нанести вредоносные программы.

**2.2 Вредоносные программы**

Вредоносные программы классифицируются следующим образом:

Логические бомбы - как вытекает из названия, используются для искажения или уничтожения информации, реже с их помощью совершаются кража или мошенничество. Манипуляциями с логическими бомбами обычно занимаются чем-то недовольные служащие, собирающиеся покинуть данную организацию, но это могут быть и консультанты, служащие с определенными политическими убеждениями и т.п.

Троянский конь - программа, выполняющая в дополнение к основным, т. е. запроектированным и документированным действиям, действия дополнительные, не описанные в документации. Троянский конь представляет собой дополнительный блок команд, тем или иным образом вставленный в исходную безвредную программу, которая затем передается (дарится, продается, подменяется) пользователям. Этот блок команд может срабатывать при наступлении некоторого условия (даты, времени, по команде извне и т.д.).

Вирус - программа, которая может заражать другие программы путем включения в них модифицированной копии, обладающей способностью к дальнейшему размножению.

Считается, что вирус характеризуется двумя основными особенностями:

* способностью к саморазмножению;
* способностью к вмешательству в вычислительный процесс (т. е. к получению возможности управления).

Червь — программа, распространяющаяся через сеть и не оставляющая своей копии на магнитном носителе. Червь использует механизмы поддержки сети для определения узла, который может быть заражен. За тем с помощью тех же механизмов передает свое тело или его часть на этот узел и либо активизируется, либо ждет для этого подходящих условий.

Захватчик паролей — это программы, специально предназначенные для воровства паролей. При попытке обращения пользователя к терминалу системы на экран выводится информация, необходимая для окончания сеанса работы. Пытаясь организовать вход, пользователь вводит имя и пароль, которые пересылаются владельцу программы- захватчика, после чего выводится сообщение об ошибке, а ввод и управление возвращаются к операционной системе.

**3. Методы и средства защиты информации**

**3.1 Методы защиты информации**

**Установка препятствия** — метод физического преграждения пути злоумышленнику к защищаемой информации, в т.ч. попыток с использованием технических средств съема информации и воздействия на нее.

**Управление доступом** — метод защиты информации за счет регулирования использования всех информационных ресурсов, в т.ч. автоматизированной информационной системы предприятия. Управление доступом включает следующие функции защиты:

* идентификацию пользователей, персонала и ресурсов информационной системы (присвоение каждому объекту персонального идентификатора);
* аутентификацию (установление подлинности) объекта или субъекта по предъявленному им идентификатору;
* проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
* разрешение и создание условий работы в пределах установленного регламента;
* регистрацию (протоколирование) обращений к защищаемым ресурсам;
* реагирование (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.

**Маскировка** — метод защиты информации с использованием инженерных, технических средств, а также путем криптографического закрытия информации.

**Криптографические методы защиты информации**

Современная криптография включает в себя четыре крупных раздела:

1. Симметричные криптосистемы. В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ. (Шифрование - преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом, дешифрование - обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный);
2. Криптосистемы с открытым ключом. В системах с открытым ключом используются два ключа - открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.( Ключ - информация, необходимая для беспрепятственного шифрования и дешифрования текстов.);
3. Электронная подпись. Системой электронной подписи называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.
4. Управление ключами*.* Это процесс системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

**О**сновные направления использования криптографических методов - передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

**3.2 Средства защиты информации**

Средства защиты информации можно разделить на:

Средства, предназначенные для защиты информации. Эти средства не предназначены для непосредственной обработки, хранения, накопления и передачи защищаемой информации, но находящиеся в одном помещении с ними.

Делятся на:

пассивные – физические (инженерные) средства, технические средства обнаружения, приборы контроля радиоэфира, линий связи и т.п.;

активные – источники бесперебойного питания, шумогенераторы, скремблеры, устройства отключения линии связи, программно-аппаратные средства маскировки информации и др.

Пассивные средства защиты акустического и виброакустического каналов утечки речевой информации.

Для предотвращения утечки речевой информации по акустическому и виброакустическому каналам, осуществляются мероприятия по выявлению каналов утечки. В большинстве случаев для несанкционированного съема информации из помещения противник применяет соответствующие замыслу закладные устройства.

Всю процедуру поиска закладных устройств можно условно разбить на несколько этапов:

• физический поиск и визуальный осмотр;

• обнаружение радиозакладных устройств как электронных средств;

• проверка наличия каналов утечки информации.

**Физический поиск и визуальный осмотр.**

Осмотр осуществляется путем обследования всех предметов в зоне контроля, размеры которых достаточно велики для того, чтобы можно было разместить в них технические средства негласного съема информации (настольные приборы, рамы картин, телефоны, цветочные горшки, книги, питаемые от сети устройства: компьютеры, ксероксы, радиоприемники и т. д.).

Физический поиск и визуальный осмотр объектов проводят с применением специальных средств видеонаблюдения и металлодетекторов.

**Обнаружение радиозакладных устройств (РЗУ).**

Необнаруженных РЗУ при визуальном осмотре осуществляют по их демаскирующим признакам с применением специальных средств обнаружения. РЗУ, как правило, содержат в своей конструкции электронные схемы и, при своей работе излучают радиосигнал.

Основными признаками излучения радиозакладок являются:

* относительно высокий уровень излучения, обусловленный необходимостью передачи сигнала за пределы контролируемого помещения.
* непрерывная или непрерывная в течение некоторого времени работа (прерывистый режим работы днем и практически, полное молчание ночью; излучение возникает одновременно с поднятием трубки и исчезает, когда трубка положена).
* появление нового источника в обычно свободном частотном диапазоне.
* использование в ряде радиозакладок направленных антенн приводит к сильной локализации излучения, то есть существенной неравномерности его уровня в пределах контролируемого объекта.
* особенности поляризации излучения радиозакладок. При изменении пространственного положения или ориентации приемной антенны наблюдается изменение уровня всех источников. Однако однотипные удаленные источники одного диапазона ведут себя примерно одинаково, тогда как сигнал закладки изменяется отлично от остальных. Эффект поляризации обнаруживается при использовании анализаторов спектра.
* изменение («размывание») спектра излучений радиомикрофонов при возникновении каких-либо шумов в контролируемом помещении. Он проявляется только в том случае, если РЗУ работает без кодирования передаваемой информации.

К основным устройствам, применяемым для обнаружения РЗУ относятся:

- индикаторы поля;

- специальные радиоприемники;

- программно-аппаратные комплексы радиоконтроля;

- нелинейные радиолокаторы.

Индикаторы поля – приборы определяющие наличие ЗУ по их радиоизлучению. Индикаторы, или детекторы поля являются простейшими средствами обнаружения факта использования радиозакладок. Это приемники с низкой чувствительностью, поэтому они обнаруживают излучения радиозакладных устройств на предельно малых расстояниях (10- 40 см), чем и обеспечивается селекция «нелегальных» излучений на фоне мощных «разрешенных» сигналов. Важное достоинство детекторов - способность находить передающие устройства вне зависимости от применяемой в них модуляции. Основной принцип поиска состоит в выявлении абсолютного максимума уровня излучения в помещении.

Иногда детекторы используют и в так называемом сторожевом режиме. В этом случае после полной проверки помещения на отсутствие ЗУ фиксируется уровень поля в некоторой точке пространства (обычно это стол руководителя или место ведения переговоров), и прибор переводится в дежурный режим. В случае включения закладки (примерно на удалении до двух метров от детектора), индикатор выдает сигнал о повышении уровня электромагнитного поля. Однако необходимо учитывать тот факт, что если будет использоваться радиозакладка с очень низким уровнем излучения, то детектор скорее всего не зафиксирует ее активизацию.

Радиоприемные устройства, как устройства выявления радиозакладок, должны удовлетворять трем основным условиям:

* иметь возможность настройки на частоту работы устройств, скрытно передающихперехваченную информацию, т.е. иметь возможность контролировать большой набор частот либо одновременно во всем диапазоне либо перестраиваясь от значения к значению за предельно малый промежуток времени - панорамные приемники;
* обладать функциями выделения нужного сигнала по характерным признакам на фоне мешающих сигналов и помех (избирательность по спектру частот);
* обладать способностью к демодуляции различных видов сигналов (избавляться от сигнала несущей частоты, а полезный сигнал преобразовывать в низкочастотный сигнал и демодулировать с помощью детектора, соответствующего типу использованной модуляции).

Программно-аппаратные комплексы радиоконтроля-для расширения возможностей специальных приемников их функционально совмещают с персональными компьютерами, что существенно повышает надежность и оперативность поиска ЗУ, делает процедуру выявления более удобной (технологичной).

На компьютер при этом возлагается решение следующих задач:

* хранение априорной информации о радиоэлектронных средствах, работающих в контролируемой области пространства и выбранных диапазонах частот;
* получение программными методами временных и частотных характеристик принимаемых сигналов;
* тестирование принимаемых сигналов по совокупности признаков на принадлежность к излучению ЗУ.

Программно-аппаратные комплексы радиоконтроля обеспечивают:

* выявление излучений РЗУ;
* пеленгование РЗУ в реальном масштабе времени;
* определение дальности до источников излучения;
* аналого-цифровую обработку сигналов с целью определения их принадлежности к излучению РЗУ;
* контроль силовых, телефонных, радиотрансляционных и других сетей;
* работу в многоканальном режиме, позволяющем контролировать несколько объектов одновременно;
* постановку прицельных помех на частотах излучения РЗУ и др.

Программно-аппаратные комплексы радиоконтроля состоят из следующих элементов:

* широкодиапазонного перестраиваемого по частоте приемника (сканера);
* блока распознавания РЗУ, осуществляющего идентификацию излучений радиомикрофонов на основе сравнения принятых детектированных сигналов с естественным акустическим фоном помещения (пассивный способ) или тестовым акустическим сигналом (активный способ);
* блока акустической локации, позволяющего по запаздыванию переизлученного зондирующего звукового импульса определять расстояние до активных радиомикрофонов;
* электронно-вычислительной машины (процессора), осуществляющей как обработку полученных данных, так и управление приемником.
* По принципу построения все известные приборы данного класса делятся на две основные группы:
* специально разработанные комплексы, конструктивно выполненные в виде единого устройства;
* комплексы, сформированные на базе серийного сканера, персонального компьютера (обычно notebook) и специального программного обеспечения.

Нелинейные радиолокаторы применяются для поиска внедренных РЗУ, не использующих радиоканал для передачи информации, а также РЗУ, находящихся в пассивном (неизлучающем) состоянии.

Нелинейные радиолокаторы - приборы, излучающие электромагнитную волну с частотой f, а принимающие переизлученные сигналы на частотах f. Если такие сигналы будут обнаружены, то в зоне действия локатора есть полупроводниковые элементы, и их необходимо проверить на возможную принадлежность к ЗУ. Нелинейный радиолокатор обнаруживает только радиоэлектронную аппаратуруи, в отличие от классического линейного радиолокатора, «не видит» отражений от окружающих предметов, то есть обладает высокой избирательностью. Источниками помех для его работы могут служить контакты со слабым прижимом, для которых характерно наличие промежуточного окисного слоя.

Активные технические средства защиты акустического и виброакустического канала.

Для активной защиты речевой информации от необнаруженных закладных устройств и съема по другим каналам используется аппаратура активной защиты:

* Технические средства пространственного зашумления;
* Устройства виброакустической защиты;
* Технические средства ультразвуковой защиты.

##### Технические средства пространственного и линейного зашумления.

По принципу действия все технические средства пространственного и линейного зашумления можно разделить на три большие группы:

Средства создания акустических маскирующих помех:

* генераторы шума в акустическом диапазоне;
* устройства виброакустической защиты;
* технические средства ультразвуковой защиты помещений;

Средства создания электромагнитных маскирующих помех:

* технические средства пространственного зашумления;
* технические средства линейного зашумления, которые в свою очередь делятся на средства создания маскирующих помех в коммуникационных сетях и средства создания маскирующих помех в сетях электропитания;
* многофункциональные средства защиты.

**3.3 Защита информации в компьютерных сетях**

## Программные средства защиты информации.

Специализированные программные средства защиты информации от несанкционированного доступа обладают в целом лучшими возможностями и характеристиками, чем встроенные средства сетевых ОС. Кроме программ шифрования, существует много других доступных внешних средств защиты информации. Из наиболее часто упоминаемых следует отметить следующие две системы, позволяющие ограничить информационные потоки.

1. Firewalls - брандмауэры (дословно firewall — огненная стена). Между локальной и глобальной сетями создаются специальные промежуточные сервера, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/ транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность совсем. Более защищенная разновидность метода - это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой.
2. Proxy-servers (proxy - доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью — попросту отсутствует маршрутизация как таковая, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом методе обращения из глобальной сети в локальную становятся невозможными в принципе.
3. [VPN](http://ru.wikipedia.org/wiki/VPN) (виртуальная частная сеть) позволяет передавать секретную информацию через сети, в которых возможно прослушивание трафика посторонними людьми. Используемые технологии:

* [PPTP](http://ru.wikipedia.org/wiki/PPTP)(туннельный [протокол](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) типа [точка-точка](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D1%8C_%D1%82%D0%BE%D1%87%D0%BA%D0%B0-%D1%82%D0%BE%D1%87%D0%BA%D0%B0), позволяющий компьютеру устанавливать [защищённое соединение](http://ru.wikipedia.org/wiki/VPN) с сервером за счёт создания специального туннеля в стандартной, незащищённой сети. PPTP помещает (инкапсулирует) кадры [PPP](http://ru.wikipedia.org/wiki/PPP_%28%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%29) в [IP](http://ru.wikipedia.org/wiki/IP)-пакеты для передачи по глобальной IP-сети, например [Интернет](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82).),
* [PPPoE](http://ru.wikipedia.org/wiki/PPPoE)([сетевой протокол](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) передачи кадров [PPP](http://ru.wikipedia.org/wiki/PPP_%28%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%29) через [Ethernet](http://ru.wikipedia.org/wiki/Ethernet). В основном используется [xDSL](http://ru.wikipedia.org/wiki/XDSL)-сервисами. Предоставляет дополнительные возможности ([аутентификация](http://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F), [сжатие данных](http://ru.wikipedia.org/wiki/%D0%A1%D0%B6%D0%B0%D1%82%D0%B8%D0%B5_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85), [шифрование](http://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)),
* [IPSec](http://ru.wikipedia.org/wiki/IPSec) (набор [протоколов](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) для обеспечения защиты данных, передаваемых по межсетевому протоколу [IP](http://ru.wikipedia.org/wiki/IP), позволяет осуществлять подтверждение подлинности и/или [шифрование](http://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) IP-пакетов. IPsec также включает в себя протоколы для защищённого обмена [ключами](http://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_%28%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F%29) в сети [Интернет](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82).)

## Аппаратные средства защиты информации

К аппаратным средствам защиты относятся различные электронные, электронно-механические, электронно-оптические устройства. К настоящему времени разработано значительное число аппаратных средств различного назначения, однако наибольшее распространение получают следующие:

* специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
* устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;
* схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.
* устройства для шифрования информации (криптографические методы).

# Защита от воздействия вредоносных программ

В настоящее время одним из основных вопросов обеспечения безопасности информации является защита от вредоносных программ. Существует огромное множество разновидностей вредоносных программ: вирусы, троянские кони, сетевые черви, логические бомбы, - и с каждым днем их становится все больше и больше. Защита от вредоносных программ не ограничивается лишь традиционной установкой антивирусных средств на рабочие станции пользователей. Это сложная задача, требующая комплексного подхода к решению.

Одно из главных преимуществ данного решения - рассмотрение подсистемы защиты информации от вредоносных программ как многоуровневой системы.

Первый уровень включает в себя средства защиты от вредоносных программ, устанавливаемые на стыке с глобальными сетями (Интернет-шлюз и/или межсетевой экран; публичные серверы Web, SMTP, ftp.) и осуществляющие фильтрацию основных видов трафика (HTTP, SMTP, FTP и т. д. )

Второй уровень - средства защиты, устанавливаемые на внутренних корпоративных серверах и серверах рабочих групп (файловых хранилищах, серверах приложений и т.д.).

И, наконец, третий уровень - средства защиты от вредоносных программ, устанавливаемые на рабочих станциях пользователей, включая удаленных и мобильных пользователей.

Преимущества данного решения заключаются:

* в использовании продуктов мировых лидеров;
* в централизованном управлении всей подсистемой защиты от вредоносных программ;
* в автоматическом обновлении антивирусных баз;
* в тесном взаимодействии антивирусных средств всех уровней подсистемы и т. д.

**Защита от компьютерных вирусов.**

Основным средством борьбы с вирусами были и остаются антивирусные программы. Можно использовать антивирусные программы (антивирусы), не имея представления о том, как они устроены. Однако без понимания принципов устройства антивирусов, знания типов вирусов, а также способов их распространения, нельзя организовать надежную защиту компьютера. Как результат, компьютер может быть заражен, даже если на нем установлены антивирусы.

Сегодня используется несколько основополагающих методик обнаружения и защиты от вирусов:

* сканирование;
* эвристический анализ;
* использование антивирусных мониторов;
* обнаружение изменений;
* использование антивирусов, встроенных в BIOS компьютера.

Кроме того, практически все антивирусные программы обеспечивают автоматическое восстановление зараженных программ и загрузочных секторов. Конечно, если это возможно.

## Особенности защиты корпоративной интрасети

Корпоративня интрасеть может насчитывать сотни и тысячи компьютеров, играющих роль рабочих станций и серверов. Эта сеть обычно подключена к Интернету и в ней имеются почтовые серверы, серверы систем автоматизации документооборота, такие как Microsoft Exchange и Lotus Notes, а также нестандартные информационные системы.

Для надежной защиты корпоративной интрасети необходимо установить антивируы на все рабочие станции и серверы. При этом на файл-серверах, серверах электронной почты и серверах систем документооборота следует использовать специальное серверное антивирусное программное обеспечение. Что же касается рабочих станций, их можно защитить обычными антивирусными сканерами и мониторами.

Разработаны специальные антивирусные прокси-серверы и брандмауэры, сканирующие проходящий через них трафик и удаляющие из него вредоносные программные компоненты. Эти антивирусы часто применяются для защиты почтовых серверов и серверов систем документооборота.

### Защита почтовых серверов.

Антивирусные мониторы неэффективны для обнаружения вирусов в почтовых сообщениях. Для этого необходимы специальные антивирусы, способные фильтровать трафик SMTP, POP3 и IMAP, исключая попадание зараженных сообщений на рабочие станции пользователей.

Для защиты почтовых серверов можно приобрести антивирусы, специально предназначенные для проверки почтового трафика, или подключить к почтовому серверу обычные антивирусы, допускающие работу в режиме командной строки.

### Защита нестандартных информационных систем

Для антивирусной защиты нестандартных информационных систем, хранящих данные в собственных форматах, необходимо либо встраивать антивирусное ядру в систему, либо подключать внешний сканер, работающий в режиме командной строки.

**3.4 Защита от внутренних угроз**

При поступлении на работу работодатель должен провести проверку личности.

Методы изучения личности.

* Изучения жизненного пути личности.
* Изучение мнения коллектива(ов) в котором работает(ал) человек.
* Изучения ближнего окружения.
* Изучения высказывания личности о своей роли в коллективе и.т.д.

Эти методы помогают побольше узнать о человеке.

Качества не способствующие к доверенности тайны:

* Эмоциональное расстройство
* Неуравновешенность поведения
* Разочарование в себе
* Отчуждение от коллег по работе
* Недовольство своим служебным положением
* Ущемлённое самолюбие
* Эгоистичный характер
* Нечестность
* Употребление наркотиков и алкоголя

Мотивация – процесс побуждения себя и других к деятельности для достижения личных целей или целей организации.

В первую очередь среди мотивов следует выделить: интерес к деятельности чувство долга, стремление к профессиональному росту.

Так – же начальник должен одинаково относиться ко всем работникам, поощрять и развивать подчинённых за их творческие способности, продвигать подчинённых по карьерной лестнице и т. д.

**Заключение**

Нужно четко представлять себе, что никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных в любой организации. В то же время можно существенно уменьшить риск потерь при комплексном подходе к вопросам безопасности. Средства защиты информации нельзя проектировать, покупать или устанавливать до тех пор, пока специалистами не произведен соответствующий анализ. Анализ должен дать объективную оценку многих факторов (подверженность появлению нарушения работы, вероятность появления нарушения работы, ущерб от коммерческих потерь и др.) и предоставить информацию для определения подходящих средств защиты – административных, аппаратных, программных и прочих.

Однако обеспечение безопасности информации - дорогое дело. Большая концентрация защитных средств в информационной системе может привести не только к тому, что система окажется очень дорогостоящей и потому нерентабельной и неконкурентоспособной, но и к тому, что у нее произойдет существенное снижение коэффициента готовности. Например, если такие ресурсы системы, как время центрального процессора будут постоянно тратиться на работу антивирусных программ, шифрование, резервное архивирование, протоколирование и тому подобное, скорость работы пользователей в такой системе может упасть до нуля.

Так же стоит большое внимание уделять и внутренним угрозам. Даже самый честный и преданный сотрудник может оказаться средством утечки информации.

Главное при определении мер и принципов защиты информации это квалифицированно определить границы разумной безопасности и затрат на средства защиты с одной стороны и поддержания системы в работоспособном состоянии и приемлемого риска с другой.

1. **Список литературы**

1 Симонович С.В. Информатика.

2 Барсуков В.С. Безопасность: технологии, средства, услуги.

3 Барсуков В.С. Современные технологии безопасности.

4 www.infosecmd.narod.ru

5 www.informyx.ru

6 www.inattack.ru

7 www.osp.ru