Реферат

Тема: Методы защиты информации

Выполнил: студент группы

Проверил: старший преподаватель

Содержание

ВВЕДЕНИЕ

1 УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

1.1 Основные объекты защиты информации

1.2 Виды угроз

1.2.1 Случайные угрозы

1.2.2 Преднамеренные угрозы

1.2.3 Технические каналы утечки информации

2 МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

2.1 Методы инженерно-технической защиты информации

2.2 Виды защиты информации от утечки по техническим каналам

2.2.1 Экранирование электромагнитных волн

2.2.2 Безопасность оптоволоконных кабельных систем

2.2.3 Особенности слаботочных линий и сетей как каналов утечки информации

2.2.4 Скрытие информации криптографическим методом

ЗАКЛЮЧЕНИЕ

Список литературы

# ВВЕДЕНИЕ

Кто владеет информацией, тот владеет миром.

Натан Ротшильд

С развитием техники и технологий окружающая нас информация стремительно возрастает и человек уже не в силах хранить ее в собственной памяти. На помощь к нему приходят современные средства хранения информации, информационные системы. Но сохраняя информацию, на каком либо носителе мы подвергаем себя опасности вероятного доступа третьих лиц. Поэтому информационная безопасность не только становится обязательной, но и выступает как одна из важнейших характеристик информационной системы. Во многих системах безопасности отведена первостепенная роль фактору безопасности (Государственные, банковские системы). Большинство современных предприятий, занимающихся бизнесом в любом направлении, не могут вести нормальную деятельность, без уверенности в обеспечении безопасности своей информацией. Нельзя забывать и про персональные компьютерные системы, связанные между собой сетью интернет, на которых и тренируются взломщики.

Человека, пытающегося нарушить работу информационной системы или получить неразрешенный доступ к информации, называют взломщиком, а иногда «компьютерным пиратом» (хакером).

В общем смысле информация содержит сведения об окружающем нас мире, являющихся объектом хранения, передачи, преобразования и использования их для определенных целей. Исходя из этого человек размещается в постоянно изменяющемся информационном поле, влияющим на его действия и образ жизни. Информация по своему характеру может быть экономической, военной, политической, научно-технической, производственной или коммерческой. По степени секретности можно разделить информацию на секретную - конфиденциальную или несекретную. К секретной - конфиденциальной информации относят сведения, содержащие коммерческую тайну, некоторые виды служебной тайны, врачебную тайну, адвокатскую и следственную тайну, тайну переписки, почтовых и телеграфных отправлений, телефонных переговоров, а также сведения о частной жизни и деятельности граждан.

Защите подлежит только та информация, которая имеет цену. А ценной информация становится, когда ее обладатель может получить какую либо выгоду: моральную, материальную или политическую.

С современным развитием информационного общества очень большое значение приобретают проблемы, связанные с защитой конфиденциальной информации. Информация как категория, имеющая стоимость, защищается ее собственником от лиц и организаций, пытающихся завладеть ее любыми способами. В связи с этим складывается тенденция, что чем выше уровень секретности информации, тем выше и уровень ее защиты, а значит, тем больше средств затрачивается на ее защиту.

Высокой эффективностью защиты информации можно определить как совокупность следующих факторов: своевременность, активность, непрерывность и комплексность. Очень важно проводить профилактические защитные мероприятия комплексно, то есть гарантировать нейтрализацию всех опасных каналов утечки информации. Нельзя забывать, что один открытый канал утечки информации может свести на нет эффективность всей системы защиты.

# УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Под угрозой безопасности информации подразумевают действия или события, которые могут привести к несанкционированному использованию, искажению или к разрушению информационных ресурсов системы, аппаратных и программных средств.

## Основные объекты защиты информации

Основными объектами информации являются:

* Информационные ресурсы, содержащие сведения, связанные с конфиденциальной информацией и государственной тайной.
* Информационные системы (сети и системы, средства вычислительной техники), программные средства (операционные системы, системы управления базами данных, прикладное программное обеспечение), технические средства приёма, автоматизированные системы управления, системы связи и передачи данных, передачи и обработки информации ограниченного доступа (звукозапись, звукоусиление, звуковоспроизведение, переговорные и телевизионные устройства, средства тиражирование и изготовления документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), т.е. все системы и средства, обрабатывающие секретную (конфиденциальную), информацию относящуюся к государственной тайне. Все эти перечисленные средства и системы называют техническими средствами приёма, обработки и хранения информации (ТСПИ).
* Технические средства и системы, не входящие в состав ТСПИ, но расположенные в помещениях обработки конфиденциальной информации. Данное оборудование называется вспомогательными техническими средствами и системами (ВТСС). Оно состоит из следующих компонентов: системы пожарной и охранной сигнализации, технические средства телефонной, громкоговорящей связи, радиотрансляции, часофикации, контрольно-измерительная аппаратура, средства и системы передачи данных в системе радиосвязи, электробытовые приборы, а также сами помещения, предназначенные для обработки данной информации имеющей ограниченное распространение.
* ТСПИ можно рассматривать как систему, включающую в себя стационарное оборудование, соединительные линии, периферийные устройства, системы электропитания, распределительные и коммуникационные устройства и системы заземления.

Все технические средства, предназначенные для обработки секретной информации, включая помещения, в которых они расположены, представляют собой объект ТСПИ.

## Виды угроз

Исследования случаев воздействия на информацию и несанкционированного доступа к ней показывают, что их можно разделить на случайные и преднамеренные. Преднамеренные угрозы часто могут быть приведены в исполнение, путем их систематического применения через долговременные, массированные атаки, несанкционированные запросы или вирусы.

Если задача по преднамеренным угрозам выполняется, то это может привести к следующим последствиям:

* разрушению информации;
* модификации - изменению информации на ложную, похожую по своему содержанию и форме, но имеющею другой смысл;
* ознакомлением с ней третьих лиц.

Итог данных событий может быть различным: от невинных недоразумений до огромных убытков или ослабления безопасности. Основной целью создания систем безопасности и является предупреждение данных последствий.

### Случайные угрозы

Многочисленные исследования проектирования, испытаний и эксплуатации автоматизированных систем показывают, что любая информация в процессе ввода, обработки, хранения, вывода и передачи подвергается разнообразным случайным воздействиям. В результате данных воздействий на аппаратном уровне в цифровых кодах происходят физические изменения уровней сигналов, несущих информацию.

А именно в одном, двух, трех или других разрядах изменения 0 на 1 или 1 на 0, или то и другое вместе, но в разных разрядах, следствием чего в итоге является незначительное изменение значения кода. Если средства функционального контроля, применяемые для этой цели способны обнаружить данные изменения (например, контроль по модулю 2 легко обнаруживает однократную ошибку), производится браковка данного кода, а устройство, модуль, микросхема или блок, участвующие в обработке, объявляются неисправными. Если данный функциональный контроль отсутствует, либо не способен обнаружить неисправность на данном этапе обработки, процесс обработки происходит по ложному пути, т. е. происходит случайная модификация информации. В результате данной ошибки, при дальнейшей обработке информации возможна передача ложной информации адресату, пересылка информации по ложному адресу, либо стирание или запись другой информации в ОЗУ или ДЗУ, а именно возникновение нежелательных событий: разрушение (утрата), модификация и утечка информации.

Основными причинами случайных воздействий на автоматизированные системы при их эксплуатации могут быть:

* сбои и отказы аппаратуры;
* помехи на линиях связи от воздействия внешней среды;
* ошибки человека как звена системы;
* системотехнические и схемные ошибки разработчиков;
* алгоритмические, структурные и программные ошибки;
* аварийные ситуации.

Как показала практика при выборе и проектировании системы, слабой в отношении надежности функционирования аппаратуры, частота отказов и сбоев аппаратуры увеличивается.

### Преднамеренные угрозы

Преднамеренные угрозы обычно связаны с действиями, какого либо человека, причинами которых могут выступать определенное недовольство своей жизненной ситуацией, а именно материальный интерес или простое развлечение с самоутверждением своих способностей, как у хакеров.

Преднамеренные угрозы можно разделить на пассивные и активные.

Пассивные угрозы – предназначены в основном на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на нормальную работу самой системы. К пассивным угрозам можно отнести несанкционированный доступ к базам данных, прослушивание каналов связи.

Активные угрозы – имеют цель нарушения нормальной работы системы, путем целенаправленного воздействия на ее компоненты. К активным угрозам можно отнести, например, вывод из строя операционной системы компьютера, разрушение ПО компьютеров, нарушение работы линий связи и т.д.

Преднамеренные угрозы так же могут быть:

* внутренние угрозы - возникающие внутри самой управляемой организации;
* внешние угрозы – возникающие из вне, как правило, обусловленные действиями конкурентов.

К основным угрозам безопасности информации от разрушения, модификации и ознакомления с ней третьих лиц относятся:

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

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

При применении к какой либо организации или структуре любого вида шпионажа возможен бесконтрольный уход конфиденциальной информации по техническим каналам связи. Рассмотрим их более подробно.

### Технические каналы утечки информации

Наибольшую возможность образования каналов утечки информации представляют ТСПИ и ВТСС, имеющие непосредственный выход за пределы контролируемой зоны (КЗ).

Контролируемая зона - это территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа. Контролируемая зона может ограничиваться периметром охраняемой территории, либо большим размером, чем охраняемая территория, но при этом она должна обеспечивать постоянный контроль за неохраняемой частью территории.

Кроме соединительных линий ТСПИ и ВТСС за пределы данной зоны могут выходить проходящие через помещения посторонние проводники, непредназначенные для ТСПИ и ВТСС (рис. 1.1).

Зона с возможностью захвата разведывательным оборудованием побочных электромагнитных излучений, содержащих секретную информацию, называется опасной зоной. Окружающие пространство вокруг ТСПИ, в котором на случайных антеннах наводится информационный сигнал выше допустимого уровня, называется опасной зоной.

Случайными антеннами являются цепи ВТСС или посторонние проводники, воспринимающие побочные электромагнитные излучения от средств ТСПИ. Случайные антенны бывают:

* сосредоточенными (технические средства с сосредоточенными параметрами, такие как телефонный аппарат, радиотрансляционной громкоговоритель сети);
* распределёнными (их образуют проводники с распределёнными параметрами, такие как соединительные провода, кабели, металлические трубы).



Рисунок 1.1 Источники образования возможных каналов утечки информации

Информационные сигналы могут быть электрическими, акустическими электромагнитными и т.д. Они по своей природе в большинстве случаев имеют колебательный характер, а информационными параметрами являются амплитуда, длительность, фаза и частота.

Технический канал утечки информации (ТКУИ) можно рассмотреть как составляющую объекта разведки, технического средства разведки (TCP) и физической среды, непосредственно в которой распространяется данный информационный сигнал. В сути, под ТКУИ подразумевают способ получения с помощью TCP любой разведывательной информации об объекте.

В зависимости от природы возникновения сигналы распространяются в некоторых физических средах. Так средой распространения могут являться твердые, газовые (воздушные) и жидкостные (водные) среды. К данным средам относят воздушное пространство, соединительные линии и токопроводящие элементы, конструкции зданий, грунт и другие.

Противодействие экономическому и промышленному шпионажу является постоянным и адекватным процессом развития методов, средств и способов защиты информации от новых типов угроз.

Классификация каналов утечки информации.

Технические каналы утечки информации обрабатываемой ТСПИ

1. Электромагнитные:

* электромагнитные излучения элементов ТСПИ;
* электромагнитные излучения на частотах роты ВЧ-генераторов ТСПИ;
* излучения на частотах самовозбуждения усилителей низкой частоты.

1. Электрические:

* наводки электромагнитных излучений элементов ТСПИ на посторонние проводники;
* просачивание информационных сигналов в линии электропитания;
* просачивание информационных сигналов в цепи заземления;
* съем информации с использованием закладных устройств.

1. Параметрические:

* перехват информации путем «высокочастотного облучения» ТСПИ;

1. Вибрационные:

* соответствие между распечатываемым символом и его акустическим образом.

Технические каналы утечки информации при передаче ее по каналам связи

1. Электромагнитные:

* электромагнитные излучения передатчиков связи, модулированные информационным сигналом (прослушивание радиотелефонов, сотовых телефонов, радиорелейных линий связи).

1. Электрические:

* подключение к линиям связи.

1. Индукционный канал:

* эффект возникновения вокруг высокочастотного кабеля электромагнитного поля при прохождении информационных сигналов.

1. Паразитные связи:

* паразитные емкостные, индуктивные и резистивные связи и наводки близко расположенных друг от друга линий передачи информации.

Технические каналы утечки речевой информации

1. Акустические каналы:

* среда распространения - воздух.

1. Виброакустические каналы:

* среда распространения – ограждающие строительные конструкции.

1. Параметрические каналы:

* результат воздействия акустического поля на элементы схем, что приводит к модуляции высокочастотного сигнала в информационный.

1. Акустоэлектрические каналы:

* преобразование акустических сигналов в электрические.

1. Оптико-электронный канал (лазерный):

* облучение лазерным лучом вибрирующих поверхностей.

Технические каналы утечки видовой информации

1. Наблюдение за объектами:

* для наблюдения днем применяются оптические приборы и телевизионные камеры;
* для наблюдения ночью – приборы ночного видения, телевизионные камеры, тепловизоры.

1. Съемка объектов:

* для съемки объектов используются телевизионные и фотографические средства. Для съемки объектов днем с близкого расстояния применяются портативные камуфлированные фотоаппараты и телекамеры, совмещенные с устройствами видеозаписи

1. Съемка документов:

* Съемка документов осуществляется с использованием портативных фотоаппаратов.

Перечисленные пути несанкционированного доступа по техническим каналам требуют достаточно профессиональных технических знаний и соответствующих программных или аппаратных разработок со стороны взломщика.

Однако злоумышленники не пренебрегают и другими способами добычи нужной информации, такими как: инициативное сотрудничество; склонение к сотрудничеству со стороны взломщика; хищение носителей информации и документальных отходов; подслушивание; выпытывание и другие.

# МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

## 

## Методы инженерно-технической защиты информации

Теория инженерно-технической защиты информации описывает основные принципы, средства и методы обеспечения информационной безопасности объектов. Она включает в себя следующие вопросы:

* систему защиты информации;
* оценку угроз;
* принцип построения системы защиты информации.

Инженерно-техническая защита состоит из таких компонентов, как специальные органы, технические средства и мероприятия по их использованию для защиты конфиденциальной информации.

Постоянная и эффективная техническая защита информационных ресурсов является обязательной составляющей комплексной системы обеспечения информационной безопасности и способствует оптимизации денежных расходов на организацию защиты информации. Техническая защита информации предполагает целый комплекс мероприятий по защите информации от несанкционированного доступа по различным видам каналов, а также исключения специальных воздействий на нее, таких как, уничтожение, искажение или блокирование доступа.

Основными целями и задачами технической защиты являются:

* защита носителей информации от полного уничтожения в результате различных природных и техногенных воздействий;
* предотвращение проникновения злоумышленника к источникам информации с целью уничтожения, хищения или изменения;
* предотвращение утечки информации по различным техническим каналам.

При проектировании систем технической защиты необходимо выполнять следующие принципы:

* непрерывность защиты информации в пространстве и во времени, постоянная готовность и высокая степень эффективности по ликвидации угроз информационной безопасности;
* многозональность и многорубежность защиты, задающее размещение информации различной ценности во вложенных зонах с контролируемым уровнем безопасности;
* избирательность в выборе первоочередности защиты наиболее важной информации;
* интеграция (взаимодействие) различных систем защиты информации с целью повышения эффективности многокомпонентной системы безопасности;
* создание централизованной службы безопасности в интегрированных системах.

По своему функциональному назначению средства инженерно-технической защиты подразделяются на следующие группы:

* инженерные средства, представляющие собой различные сооружения и устройства, предотвращающие физическое проникновение злоумышленников на защищаемые объекты;
* аппаратные средства, представляющие собой измерительные приборы и устройства, программно-аппаратные комплексы, предназначенные для выявления каналов утечки информации, оценки их характеристик по защите информации;
* программные комплексы и средства системы защиты информации в информационных системах различного назначения и в основных средствах обработки данных;
* криптографические средства защиты компьютерной информации, передаваемой по открытым каналам передачи данных и сетям связи.

В концепции инженерно-технической защиты информации кроме целей и задач системы безопасности, определяются принципы ее организации и функционирования; правовые основы; виды угроз и ресурсы, подлежащие защите, а также основные направления разработки системы безопасности.

К основным целям защиты информации относятся: предотвращение утечки, утраты, хищения, искажения, подделки информации и применение других несанкционированных негативных воздействий.

Разработка и создание новой системы защиты, а также оценка эффективности существующей системы безопасности объекта начинается с анализа наиболее возможных угроз и оценки их реального появления. Для получения данных такого рода, необходимо произвести обследование объекта на наличие уязвимостей в защите, а так же учесть особенности расположения, инженерных конструкций, коммуникаций и тому подобного. Следующим этапом выполняется выбор соответствующих методов и средств адекватной защиты объекта.

При рассмотрении вероятных угроз объекту нельзя забывать про угрозу безопасности здоровья персонала; угрозу целости и сохранности оборудования и материальных ценностей; безопасность информации и сохранность государственной или коммерческой тайны.

При проектировании защиты в комплексную систему должно вписываться все-то разнообразие возможных информационных угроз, так как она должна обеспечивать надежное перекрытие всех опасных каналов утечки информации.

Эффективность всей системы защиты от утечки информации по техническим каналам оценивается по разнообразным критериям, которые определяются физической природой информационного сигнала, но чаще всего по соотношению «сигнал/шум».

Все способы защиты согласно руководящей документации делятся на две группы, такие как, скрытие и дезинформация.

К группе скрытие относятся:

* пассивное скрытие – заключается в исключении или значительном затруднении обнаружения объектов;
* активное скрытие – в создании техническим средствам разведки маскирующих шумовых помех различной физической природы и ложной обстановки по физическим полям;
* специальная защита – заключается в скремблирование телефонных переговоров, кодирование цифровой информации криптографическими методами, программные методы модификации информации.

К группе дезинформация относятся:

* техническая дезинформация;
* имитация;
* легендирование.

К принципам инженерно-технической защиты информации относятся:

* скрытность защиты информации;
* надежность защиты информации;
* непрерывность защиты;
* рациональность защиты;
* комплексное применение различных способов и средств защиты;
* многообразие способов защиты;
* экономичность защиты.

## Виды защиты информации от утечки по техническим каналам

Для защиты информации от утечки и снижению паразитных связей по техническим каналам используется ряд средств, представляющих собой комплекс поработанных мероприятий. Рассмотрим несколько основных:

### Экранирование электромагнитных волн

Экранирование электромагнитных волн является одним из самых действенных средств защиты объекта от утечки информации по техническим каналам и основой экологической безопасности.

Но для более эффективной защиты мало просто применить экранирование и развязывающие фильтры на каналы связи, но также в первую очередь необходимо устранять или ослаблять до допустимых значений паразитные связи путем следующих мероприятий:

* размещение вероятных источников и приемников наводок на максимально допустимом расстоянии друг от друга;
* сведение к минимуму общих сопротивлений;
* уменьшение сечения габаритов токонесущих элементов, обеспечивающих минимум паразитной связи (для получения минимальной взаимоиндуктивности катушек индуктивности их оси должны быть взаимно перпендикулярны);
* изъятие посторонних проводов, проходящих через несколько узлов или блоков, которые могут связать элементы, расположенные на удаленном растоянии друг от друга;
* при невозможности исключения посторонних проводов, создающих паразитную связь, необходимо позаботиться о том, чтобы при емкостной паразитной связи сопротивление постороннего провода относительно корпуса было минимальным, при индуктивной паразитной связи необходимо увеличивать внутреннее сопротивление посторонней линии связи.

Экранирование – это локализация электромагнитной энергии в пределах определенного пространства путем преграждения ее распространения.

Развязывающий фильтр – это устройство, ограничивающее распространение помехи по проводам, являющимся общими для источника и приемника наводки.

В настоящее время все актуальней становится проблема формирования электромагнитной обстановки, обеспечивающей нормальное функционирование электронных устройств и экологическую безопасность.

Для создания благоприятной электромагнитной обстановки и обеспечения требований по электромагнитной безопасности объекта, которая включает в себя и предотвращение несанкционированного доступа к информации с использованием специальных технических средств, производится экранирование электромагнитных волн.

Применение качественных экранов позволяет решить многие задачи, в которые входит защита информации в помещениях и технических каналах, электромагнитную совместимость оборудования и приборов при совместном использовании, защиту персонала от повышенного уровня электромагнитных полей и обеспечение безопасной экологической обстановки вокруг работающих электроустановок и СВЧ-устройств.

защита утечка информация

### Безопасность оптоволоконных кабельных систем

Важными характеристиками волоконно-оптических систем передачи информации (ВОСПИ) являются:

* слабое затухание сигнала и его маленькая зависимость от длины волны передаваемого информационного оптического сигнала, распределения мод и температуры кабеля;
* очень слабое искажение сигнала и его незначительная зависимость oт спектральной ширины, распределения мод, амплитуды и длины волны передаваемого информационного оптического сигнала, температуры окружающей среды и длины световода;
* малые потери на излучение и их незначительная зависимость от радиуса изгиба и температуры волоконного световода;
* простота укладки, сращивания и ввода излучения в световод;
* более приемлемые физические параметры – вес, размер, объем;
* высокая устойчивость к внешним воздействиям – теплостойкость, влагостойкость, стойкость к химической коррозии и к механическим нагрузкам.

Несмотря на перечисленные выше преимущества, у ВОСПИ также присутствуют недостатки, главным из которых является возможность утечки информации за счет побочного электромагнитного излучения и наводок (ПЭМИН) как в оптическом, так и в радиочастотном диапазонах.

Оптоволокно – представляет собой обычное стекло, передающее электромагнитную энергию в инфракрасном диапазоне волн. Излучение наружу практически не просачивается. Эффективный захват информации возможен только путем непосредственного физического подключения к оптоволоконной линии. Но если ВОСПИ рассматривать как систему в целом, содержащую рабочие станции, интерфейсные карты, серверы, концентраторы и другие сетевые активные устройства, которые сами непосредственно являются источником излучений, то проблема утечки информации становятся актуальной. Исходя их этого принимая решения об использовании оптоволоконных кабельных систем (ОКС), нельзя не учитывать этот фактор.

Основным элементом оптоволоконного кабеля является внутренний сердечник из стекла или пластика (рис. 2.1, позиция 1). Диаметр и прозрачность стекловолокна напрямую определяют количество передаваемого им света.

Широко распространены следующие типы оптоволоконного кабеля:

* + с сердечником 8,3 мк и оболочкой 125 мк;
  + с сердечником 62,5 мк и оболочкой 125 мк;
  + с сердечником 50 мк и оболочкой 125 мк;
  + с сердечником 100 мк и оболочкой 145 мк.

Оптоволоконные кабели толщиной в 8,3 микрона очень сложно соединить точно. В силу этого возможны монтажные ошибки, в том числе и трудно выявляемые при тестировании кабельной линии. Данные дефекты можно устранить установкой дополнительных оптоволоконных повторителей (концентраторов), но это обуславливается увеличением уровня электромагнитных излучений кабельной системы в целом. Для предотвращения данной проблемы стали изготавливать заказные кабельные комплекты, то есть кабели с уже смонтированными и проверенными в заводских условиях коннекторами, исключающими процедуры монтажа и тестирования линии в полевых условиях.

Для оптоволоконного кабеля характерны следующие особенности:

* + наличие центрального силового элемента;
  + размещение в полимерной трубке-модуле;
  + количество оптических волокон в одном модуле – от 1 до 12;
  + покрытие всех этих элементов и модулей промежуточной полимерной оболочкой;
  + заполнение пространства между модулями упрочняющими элементами (корделями из стеклонитей или нитей из кевлара и гидрофобным гелем);
  + внешняя защита оболочки из полиэтилена или металла (также возможно наличие двух защитных оболочек – металлической и полиэтиленовой).

Наряду с перечисленными общими особенностями оптоволоконные кабели различных моделей могут иметь дополнительные скрепляющие ленты, антикоррозийные и водозащитные обмотки, гофрированные металлические оболочки и т.д.

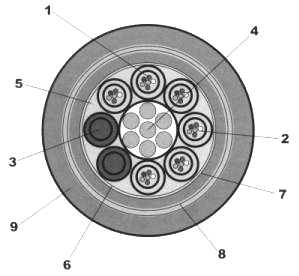


Рис. 2.1. Конфигурация оптоволоконного кабеля (на примере оптического городского кабеля производства фирмы Fujikara для прокладки в кабельной канализации, трубах, блоках, коллекторах, на мостах и в кабельных шахтах): 1 – оптическое волокно; 2 – внутримодульный гидрофобный заполнитель; 3 – кордель; 4 –центральный силовой элемент – стальной трос; 5 – гидрофобный заполнитель; 6 – скрепляющая лента; 7 –промежуточная оболочка из полиэтилена; 8 – броня из стальной гофрированной ленты; 9 – защитная оболочка из полиэтилена.

Как уже писалось, наиболее эффективным способом перехвата информации с оптоволоконных кабельных систем является непосредственное подключение к ним. Появилась информация о создании специальных дистанционно управляемых роботов, которые способны самостоятельно передвигаться по кабельным канализациям и производить подключение к оптоволоконному кабелю для последующей передачи данных, проходящих в ОКС.

Для предотвращения подключения злоумышленников, имеющим специальную технику, было предложено использовать внутренние силовые металлические конструкции оптоволоконных кабелей в качестве сигнальных проводов. Что сделало невозможным подключением к оптоволокну без нарушения целостности силовых конструкций. При нарушение целостности металлических конструкций происходит срабатывание сигнализации в центре контроля за ОКС. Дополнительного оборудования для контроля над охранной системой практически не требуется.

### Особенности слаботочных линий и сетей как каналов утечки информации

При рассмотрении задачи обеспечения безопасности помещения нельзя забывать про то что, злоумышленник может использовать телефонные и электросиловые линии, проходящие в здании.

Электросиловые линии в помещениях используются для подслушивания разговоров, через которые проходит линия. Обычно, силовая линия используется в качестве источника питания для подслушивающих устройств, передающих информацию из помещения по радиоканалу. Также линия может использоваться и в качестве проводного канала. Достоинством такого канала передачи выступает большая, чем у радиоканала, скрытность, а недостатком – что приемник информации необходимо подключать к этой же линии и не дальше первой трансформаторной подстанции.

В процессе использования электросиловой линии в качестве источника питания подслушивающее устройство может быть подключено как последовательно, так и параллельно линии. Параллельное подключение является более предпочтительным, из-за того что, устройство для питания использует напряжение линии и может работать в любое время.

Для увеличения скрытности устройства при параллельном подключении могут использоватся так называемые «сторожевые устройства», производящие отключение от сетевых проводов на заданное время при кратковременном пропадании сетевого напряжения в линии. Последовательное подключение является менее удобно для работы подслушивающего устройства, так как в данном случае для питания используется ток линии, а он появляется в линии только при подключении нагрузки.

Телефонные линии используются:

* + для прослушивания телефонных разговоров (линия используется, как источник информационного сигнала, а также может при этом выполнять функции источника питания);
  + для прослушивания разговоров в помещениях, вблизи которых проходит телефонная линия (телефонная линия используется как скрытный канал передачи информации в любое место, где есть телефон, и как источник питания);
  + в качестве бесплатного канала телефонной связи (междугородные переговоры за чужой счет) и для проникновения в банковскую компьютерную сеть для присвоения денег (в случае, когда используется телефонная линия для пересылки финансовых документов).

Для подслушивания телефонных разговоров специализированное радиоэлектронное устройство должно быть подключено в любом доступном для злоумышленников месте (в помещениях, в которых проходит линия; в телефонном аппарате; в распределительных коробках и шкафах здания; в узловых распределительных шкафах городской телефонной сети; на АТС) и подключаться параллельно линии (гальванически) или последовательно (гальванически или индуктивно).

При подслушивании разговоров в помещении специальное радиоэлектронное устройство должно быть подключено только в помещении, в котором проходят разговоры, и включаться только параллельно линии (гальванически). Работа данного устройства возможна только когда не используются телефонная линия.

В качестве канала телефонной связи, а также для проникновения в банковскую систему, радиоэлектронное устройство может быть подсоединено в любом доступном для злоумышленников месте, при помощи параллельного подключения (гальванически) и работать только в то время, когда телефонной линией не пользуются.

Для предотвращения прослушивания переговоров существует ряд устройств – анализаторов позволяющих: обнаружить блоки питания специальных радиоэлектронных передатчиков; позволяет фиксировать отклонения импеданса линии от типового значения, при подключении к линии последовательно соединенных конденсатора с емкостью 100 пФ и более и резистора с сопротивлением 1 МОм; диапазон измерения токов утечки от 0.1 до 200 мА; диапазон измерения сопротивления изоляции от 100 кОм до 20 Мом; блокировку незаконно набранного номера и другое.

### Скрытие информации криптографическим методом

Скрытие информации методом криптографического преобразования заключается в преобразовании ее составных частей (цифр, букв, слогов, слов) к неявному виду с помощью специальных алгоритмов и кодов ключей. Незащищенное конфиденциальное информационное сообщение зашифровывается и тем самым преобразуется в шифрограмму, т. е. в закрытый текст или графическое изображение документа. Для ознакомления с шифрограммой применяется обратный процесс: декодирование (дешифрование). Использование криптографии является одним из распространенных методов, значительно повышающих безопасность передачи данных хранящихся в удаленных устройствах памяти, а также при обмене информацией между удаленными пользователями и объектами.

Для шифрования обычно используется заданный алгоритм или устройство, реализующее данный алгоритм, который должен быть известен кругу лиц., для которого предназначается информация. Управление данного процесса шифрования осуществляется с помощью периодически меняющегося кода ключа, обеспечивающего каждый раз оригинальность представления информации при использовании одного и того же алгоритма. Знание секретного ключа дает возможность просто, надежно и быстро расшифровать информацию. Однако без ключа эта процедура может быть практически невыполнима даже при известном алгоритме шифрования.

Любое преобразование информации, даже самое простое, является очень эффективным средством, дающим возможность скрыть ее смысл от большинства неквалифицированных нарушителей.

Метод шифрования и кодирования использовались задолго до появления ЭВМ. Между кодированием и шифрованием нельзя провести отчетливой границы. В последнее время на практике слово "кодирование" применяют в целях цифрового представления информации при ее обработке на технических средствах, а "шифрование" — при преобразовании информации в целях защиты от НСД. В данное время некоторые методы шифрования хорошо проработаны и являются основными. Для полного обеспечения защиты информации от НСД необходимо иметь представление о некоторых традиционных методах шифрования, таких как подстановка, перестановка, комбинированных и др.

Основные требования, предъявляемые к методам защитного преобразования:

* применяемый метод должен быть достаточно устойчивым к попыткам раскрыть исходный текст, имея только зашифрованный текст;
* объем ключа должен быть оптимальным для запоминания и пересылки;
* алгоритм преобразования информации и ключ, используемые для шифрования и дешифрования, не должны быть очень сложными: затраты на защитные преобразования должны быть приемлемы при определенном уровне сохранности информации;
* ошибки в шифровании не должны вызывать потерю информации. Из-за возникновения ошибок передачи обработанного сообщения по каналам связи не должна исключаться возможность надежной расшифровки текста у получателя;
* длина зашифрованного текста не должна превышать длину исходного текста;
* необходимые временные и финансовые затраты на шифрование и дешифрование информации должны определяются требуемой степенью защиты информации.

Перечисленные требования характерны в основном для традиционных средств защитных преобразований. С развитием устройств памяти, позволяющих с большей плотностью записывать и долгое время надежно хранить большие объемы информации, ограничение на объем используемого ключа может быть снижено. Появление и развитие электронных элементов позволили разработать недорогие устройства, обеспечивающие преобразование информации.

Однако в настоящее время скорость передачи информации пока еще значительно отстает от скорости ее обработки. В условиях применения ЭВМ, при существующей надежности аппаратуры и развитых методах обнаружения и исправления ошибок требование по достоверности информации на приемке, при возникновении ошибок стало менее актуально. Кроме того, технология передачи данных, принятая в сетях ЭВМ и АСУ, предусматривает повторную передачу защищенной информации в случае обнаружения ошибок передачи сообщения.

Множество современных методов защитных преобразований можно классифицировать на четыре большие группы:

1. перестановки – заключается в том, что входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов;
2. замены (подстановки) – заключаются в том, что символы исходного текста (блока), записанные в одном алфавите, заменяются символами другого алфавита в соответствии с принятым ключом преобразования;
3. аддитивные – в данном методе в качестве ключа используется некоторая последовательность букв того же алфавита и такой же длины, что и в исходном тексте. Шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите (для примера, если используется двоичный алфавит, то производится сложение по модулю два);
4. комбинированные методы – могут содержать в себе основы нескольких методов.

Методы перестановки и подстановки характеризуются короткой длиной ключа, а надежность их защиты определяется сложностью алгоритмов преобразования.

Для аддитивных методов характерны простые алгоритмы преобразования, а их надежность основана на увеличении длины ключа.

Все перечисленные методы относятся к так называемому симметричному шифрованию: один и тот же ключ используется для шифрования и дешифрования.

В последнее время появились методы несимметричного шифрования:

один ключ для шифрования (открытый), второй — для дешифрования (закрытый).

Принципиальное значение для надежности шифрования имеет отношение длины ключа к длине закрываемого им текста. Чем больше оно приближается к единице, тем надежнее шифрование. Но также нельзя забывать и про то, что это отношение распространяется не только на данное шифруемое сообщение, но и на все остальные, закрытые этим же кодом и передаваемые постоянно и периодически в течение времени существования данного ключа до замены новым значением.

# ЗАКЛЮЧЕНИЕ

Проблема защиты информации появилась задолго до разработки компьютерной техники, а появление ЭВМ лишь перевело ее на новый уровень. И как показывает практика: лучшая защита от нападения это не допускать его. Нельзя защиту информации ограничивать только техническими методами. Основной недостаток защиты - это человеческий фактор и поэтому надежность системы безопасности зависит от отношения к ней.

Для поддержания защиты на высоком уровне необходимо постоянно совершенствоваться вместе с развитием современной техники и технологий, так сказать двигаться в ногу со временем.

# Список литературы

1. Технические средства и методы защиты информации:Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с. Источник - http://window.edu.ru/window\_catalog/pdf2txt?p\_id=33810
2. Мельников В. Защита информации в компьютерных системах. М.: Финансы и статистика, Электронинформ, 1997 – 368 с.
3. <http://kiev-security.org.ua/box/6/22.shtml>