Содержание

Введение………………………………………………………………………………….2-4

Структурное скрытие речевой информации……………………………………………5-7

Паразитные связи и наводки……………………………………………………………8-13

Алгоритмы шифрования………………………………………………………………13-14

Методы противодействия прослушиванию………………………………………….14-15

Заключение…………………………………………………………………………………

Список используемое литературы………………………………………………………..

**Введение**

То, что информация имеет ценность, люди осознали очень давно – недаром переписка сильных мира сего издавна была объектом пристального внимания их недругов и друзей. Тогда-то и возникла задача защиты этой переписки от чрезмерно любопытных глаз. Древние пытались использовать для решения этой задачи самые разнообразные методы, и одним из них была тайнопись – умение составлять сообщения таким образом, чтобы его смысл был недоступен никому, кроме посвященных в тайну. Есть свидетельства тому, что искусство тайнописи зародилось еще в до античные времена. На протяжении всей своей многовековой истории, вплоть до совсем недавнего времени, это искусство служило немногим, в основном верхушке общества, не выходя за пределы резиденций глав государств, посольств и – конечно же – разведывательных миссий. И лишь несколько десятилетий назад все изменилось коренным образом – информация приобрела самостоятельную коммерческую ценность и стала широко распространенным, почти обычным товаром. Ее производят, хранят, транспортируют, продают и покупают, а значит – воруют и подделывают – и, следовательно, ее необходимо защищать. Современное общество все в большей степени становится информационно–обусловленным, успех любого вида деятельности все сильней зависит от обладания определенными сведениями и от отсутствия их у конкурентов. И чем сильней проявляется указанный эффект, тем больше потенциальные убытки от злоупотреблений в информационной сфере, и тем больше потребность в защите информации. Одним словом, возникновение индустрии обработки информации с железной необходимостью привело к возникновению индустрии средств защиты информации. Изменился сам подход к понятию «информация». Этот термин сейчас больше используется для обозначения специального товара, который можно купить, продать, обменять на что-то другое и т.д. При этом стоимость подобного товара зачастую превосходит в десятки, а то и в сотни раз стоимость самой вычислительной техники, в рамках которой он функционирует. Даже более того, информация, в данное время, является одним из основных товаров. Естественно, возникает потребность защитить информацию от несанкционированного доступа, кражи, уничтожения, изменения и других преступных действий

Существуют в российском законодательстве законы, в котором информация, безусловно, признается объектом собственности человека. И человек, как владелец своей информации имеет право определять правила ее обработки и зашиты. Базовым в этом отношении является Закон Российской Федерации «Об информации, информатизации и защите информации», принятый 25 января 1995 г. В соответствии с ним любой российский гражданин может предпринимать необходимые меры для предотвращения утечки, хищения, утраты, искажения и подделки информации. Вопрос состоит в том, какие действия являются на самом деле необходимыми для адекватной защиты вашей информации.

Как и дверной замок, любая система защиты информации не является полностью безопасной. Всегда найдется кто-нибудь, способный взломать защитные механизмы. Таким образом, задача обеспечения информационной безопасности противоречива по самой своей сути. С одной стороны, средств обеспечения безопасности никогда не бывает слишком много в том смысле, что защиту всегда можно тем или иным способом преодолеть (просто каждый раз, когда повышается уровень защиты, приходится придумывать более изощренный способ ее обхода). С другой стороны, чем сильнее кого-то или что-то защищают, тем больше возникает неудобств и ограничений, и в результате вместо чувства спокойствия информационная защита вызывает лишь раздражение и стремление от нее отмахнуться. Установка строгих ограничений на доступ к информации создает дополнительные трудности при совместной работе с этой информацией. Поэтому идеальной и универсальной системы защиты информации не существует: здесь все слишком индивидуально, и вариант защиты, наиболее близкий к оптимальному, все время приходится подбирать заново.

**Структурное скрытие речевой информации**

Так как передача речевой информации составляет основу телекоммуникации в человеческом обществе, то ее защита— важнейшая задача инженернотехнической защиты информации. Речевая информация, передаваемая по каналу связи, содержится в информационных параметрах электрических и радиосигналов. Сигналы распространяются по линиям связи в аналоговом и цифровом виде. В результате несанкционированного перехвата этих сигналов и их модуляции речевая информация может быть добыта злоумышленником.

Для структурного скрытия речевой информации в каналах связи применяют шифрование и техническое закрытие.

При шифровании аналоговый речевой сигнал с выхода микрофона преобразуется с помощью аналоговоцифрового преобразователя в цифровой сигнал. При аналогоцифровом преобразовании амплитуда сигнала измеряется через равные промежутки времени, называемые шагом дискретизации. Для того чтобы цифровой речевой сигнал имел качество не хуже переданного по телефонному каналу в аналоговой форме, шаг дискретизации в соответствии с теоремой Котельникова не должен превышать 160 мкс, а количество уровней квантования амплитуды речевого сигнала— не менее 128. В этом случае один отсчет амплитуды кодируется 7 битами. Такой вид модуляции сигнала называется импульснокодовой комбинацией (ИКМ) и требует скорости передачи 4864 кбит/с, существенно превышающей пропускную способность стандартного телефонного канала связи. С целью снижения необходимой скорости разработаны различные методы сжатия речевого сообщения. Методы сжатия используют избыточность речевого сигнала или допускают снижение качества речи за счет показателей, несущественных для семантики сообщения. Например, широко применяемый метод дельтамодуляции (ДМ), который предусматривает передачу не абсолютных значений оцифрованных амплитуд исходного речевого сигнала, а величины изменения (дельты) амплитуды при каждом шаге квантования, позволяет снизить скорость передачи до 2024 кбит/с. Еще меньшая скорость передачи (812 кбит/с), но со снижением качества речи, требуется при передаче клипированной речи, которая представляет собой ограниченный по амплитуде дискретный речевой сигнал. Шифрование речевой информации в цифровой форме производится известными методами (заменой, перестановками, аналитическими преобразованиями, гаммированием и др.).

Гарантированное засекречивание сообщений обеспечивается при использовании стандартизованных алгоритмов типа DES в США и ГОСТ 2814789 в России. Алгоритм DES, применяемый в США с 1976 года, обеспечивает суперпозицию шифров, состоящих из 16 последовательных циклов и в каждом из которых сочетаются подстановки и перестановки. Он реализуется программно, обеспечивает скорость передачи 10200 кБ/с и криптостойкость 1017 операций при длине ключа 56 бит.

Алгоритм криптографического преобразования, определяемый ГОСТ 2814789, обладает криптостойкостью, оцениваемой 10™ операций (длина ключа 256 бит), обеспечивает скорость шифрования 5070 кБ/с и реализуется в основном аппаратно. С увеличением длины ключа время раскрытия шифртекста резко возрастает. Например, при быстродействии компьютера около 1012 оп./с это время составляет около 10 ч для ключа длиной 56 бит, для ключа в 64 бита оно повышается до 3,2 месяца, при длине 70 бит — 17,5 лет, а для 75 бит превышает 560 лет.

Хотя развитие связи характеризуется постепенной заменой аналоговой техники на цифровую, менее дорогая аналоговая связь, особенно телефонная проводная, еще длительное время будет одним из основных видов связи. Но стандартный телефонный канал имеет узкую полосу пропускания в 3 кГц, недостаточную для передачи с высоким качеством шифрованного цифрового сигнала.

Скрытие речевого сигнала в узкополосном телефонном канале осуществляется методами технического или аналогового закрытия. По названию технических средств, обеспечивающих техническое закрытие, эти методы называются также скремблированием (перемешиванием). Техническое закрытие (скремблирование) отличается от криптографического тем, что при шифровании происходит скрытие речевого сообщения в символьной форме, а при техническом закрытии — скрытие речевого сигнала без преобразования его в цифровую форму. При техническом закрытии изменяются признаки (характеристики) исходного речевого сигнала таким образом, что он становится похож на шум, но занимает ту же частотную полосу. Это позволяет передавать скремблированные сигналы по обычным стандартным телефонным каналам связи. Классификация методов технического закрытия приведена на рис. 11.1.

По виду преобразования сигнала различают частотные и временные методы технического закрытия, а по режиму закрытия — статическое и динамическое. Частотные методы скремблирования, реализуемые на элементах аналоговой техники, появились раньше временных методов, которые выполняются существенно проще на элементах дискретной техники. В настоящее время в связи с прогрессом в микроминиатюризации дискретной техники оба метода используют дискретную элементную базу.

**Паразитные связи и наводки**

В любом радиоэлектронном средстве или электрическом приборе наряду с токопроводами (проводами, проводниками печатных плат), предусмотренными их схемами, возникают многочисленные побочные пути, по которым распространяются электрические сигналы, в том числе опасные сигналы акустоэлектрических преобразователей. Эти пути создаются в результате паразитных связей и наводок. Первопричиной их являются поля, создаваемые электрическими зарядами и токами в цепях радиоэлектронных средств и приборов.

Постоянные электрические заряды и электрический ток в элементах и цепях радиосредств и электрических приборов создают соответствующие электрические и магнитные поля, а заряды и ток переменной частоты — электромагнитные поля. Поля распространяются в пространстве и воздействуют на элементы и цепи других технических средств и систем. Кроме того, для функционирования средств и систем необходимо обеспечить гальваническое соединение их элементов. Изза гальванических соединений возникают дополнительные пути для распространения сигналов одних узлов и блоков по цепям других. В результате воздействия побочных полей и влияния через проводники и резисторы сигналов одних узлов и блоков на сигналы других блоков и узлов возникают паразитные связи и наводки как внутри радиоэлектронных средств, так и между рядом расположенными средствами. Эти связи и наводки ухудшают работу узлов, блоков и средств в целом. Поэтому при проектировании радиоэлектронных средств уровни этих паразитных связей и наводок снижают до допустимых значений. Чем выше требования к характеристикам средств, тем требуются большие усилия, а следовательно, и затраты для нейтрализации паразитных связей и наводок. Основная часть высокой цены (десятки тысяч долларов) высокоточных контрольноизмерительных приборов фирм Hewlett Packard, Ronde & Scwarz и др. приходится на меры по уменьшению паразитных связей и наводок.

Однако несмотря на принимаемые меры по снижению уровня паразитных связей и наводок для обеспечения требуемых характеристик радиоэлектронного средства, остаточный их уровень создает угрозы для информации, содержащейся в информационных параметрах сигналов, циркулирующих в радиоэлектронном средстве. Поэтому любое радиоэлектронное средство или электрический прибор следует с точки зрения информационной безопасности рассматривать как потенциальный источник угрозы безопасности информации.

Известны три вида паразитных связей:

• емкостная;

• индуктивная;

• гальваническая.

Емкостная связь образуется в результате воздействия электрического поля, индуктивная — воздействия магнитного поля, гальваническая связь — через общее активное сопротивление.

На этом рисунке Ua — потенциал заряда точки А относительно корпуса, создающий электрическое поле. В результате воздействия этого поля в точке В возникает заряд противоположного знака. Величина потенциала заряда (наведенного напряжения) Ub точки В относительно корпуса определяется соотношением емкостного сопротивления Сп, и сопротивлений Zb:

Емкостная паразитная связь возникает между любыми элементами схемы: проводами, радиоэлементами схемы и корпусом (шасси). Величина паразитной емкости на единицу длины проводов, параллельно расположенных на удалении b друг от друга.

Так как между рядом расположенными основными и вспомогательными средствами существует паразитная емкостная связь, способствующая передаче сигналов с защищаемой информацией от ОТСС к ВТСС, то для определения величины наводки надо знать их паразитные емкости. Эти емкости называются собственными емкостями радиоэлектронного средства и электрического прибора. Вычислить собственную емкость можно только для простейших конфигураций типа штырь, шар, диск. Например, для штыря длиной L паразитная емкость составляет Сп ~ 0,1L, для диска Сп ~ 0,35D, шара — Cn ~ 0,56D, где D — диаметр шара и диска. Для реальных радиоэлектронных средств сложной конфигурации собственная емкость Сп определяется экспериментально путем размещения средства в однородном электрическом поле и измерением наведенного напряжения на его выходе UH. Предварительно измеряется наведенное эталонное напряжение U в простейшем устройстве (диске, шаре и др.) с известной (эталонной) собственной емкостью Спэ, помещенном в это поле. На основе полученных данных собственная емкость исследуемого средства определяется методом замещения, в соответствии с которым Cn = С Ц/U .

Взаимная индуктивность замкнутых цепей зависит от взаимного расположения и конфигурации проводников. Она тем больше, чем большая часть магнитного поля тока в одной цепи пронизывает проводники другой цепи.

Следует различать взаимную индуктивность между проводниками разных цепей от индуктивности проводника. Индуктивность характеризует свойство проводника препятствовать изменению проходящего через него тока, которое обусловлено явлением са' моиндукции. Она возникает, когда силовые линии переменного магнитного поля пронизывают проводники, по которым протекает ток, создающий это магнитное поле. Следовательно, переменное магнитное поле, как гоголевская унтерофицерская вдова, способно само себя высечь.

Гальваническую паразитную связь еще называют связью через общее сопротивление, входящее в состав нескольких цепей. Такими общими сопротивлениями могут быть сопротивление соединительных проводов и устройств питания и управления. Например, узлы и блоки компьютера, осуществляющего обработку информации, соединены с напряжением +5 В блока питания. Для установки «О» триггеров дискретных устройств на соответствующие их входы подается одновременно соответствующий сигнал управления. На рис. 5.7 приведена упрощенная схема, иллюстрирующая возникновение гальванической связи.

Если побочные поля и электрические токи являются носителями защищаемой информации, то паразитные наводки и связи могут приводить к утечке информации. Следовательно, паразитные связи и наводки представляют собой побочные физические процессы и явления, которые могут приводить к утечке защищаемой информации.

Возможность утечки информации через паразитные связи и наводки носит вероятностный характер и зависит от многих факторов, в том числе от конфигурации, размеров (относительно периода колебаний протекающих токов) и взаимного положения излучающих и принимающих токопроводящих элементов средств. В отличие от предусмотренных для связи функциональных антенн, конструкция и характеристики которых определяются при создании радиопередающих и радиоприемных средств, эти элементы можно назвать случайными антеннами.

Случайными антеннами могут быть монтажные провода, соединительные кабели, токопроводы печатных плат, выводы радиодеталей, металлические корпуса средств и приборов и другие элементы средств. Параметры случайных антенн существенно хуже функциональных. Но из за небольших расстояний между передающими и приемными случайными антеннами (в радиоэлектронном средстве или одном помещении) они создают угрозы утечки информации.

Случайные антенны имеют сложную и часто априори неопределенную конфигурацию, достаточно точно рассчитать значения их электрических параметров, совпадающих с измеряемыми, очень сложно. Поэтому реальную случайную антенну заменяют ее моделями в виде проволочной антенны — отрезка провода (вибратора) и рамки.

В ближней зоне вибратор создает преимущественно электрическое поле. Свойства проволочной антенны преобразовать электрический сигнал в поле (радиосигнал) и наоборот характеризуются параметром антенны, названным действующей высотой h и измеряемым в м. Действующая высота передающей антенны представляет собой параметр, связывающий напряженность электрического поля, создаваемого антенной в направлении главного излучения, с уровнем сигнала в самой антенне. Действующая высота приемной антенны равна отношению ЭДС в приемной антенне к напряженности вызывающего ее электрического поля: h = = Ua/Ea. При этом предполагается, что приемная антенна ориентирована в пространстве в соответствии с поляризацией электромагнитного поля и прием осуществляется с направления максимального уровня поля. Так как отношение напряженностей электрической и магнитной составляющих электромагнитного поля возле случайной антенны равно волновому сопротивлению среды (Za = Еа/На), то h = U /H Z .

Паразитные связи могут вызывать утечку информации по проводам и создавать условия для возникновения побочных электромагнитных излучений. За счет паразитных связей возникают опасные сигналы в проводах кабелей различных линий и цепей, в том числе в цепях заземления и электропитания, а также возникают паразитные колебания в усилителях, дискретных устройствах и др.

**Алгоритмы шифрования**

Для передачи ценной информации по незащищенным каналам связи обычно используются алгоритмы шифрования. Они делятся на два вида: Симметричные и ассиметричные. На данный момент существует множество алгоритмов шифрования, но мы в данном случае рассмотрим два алгоритма RSA и DEC, которые по моему мнению наиболее популярны и имеют хорошую криптостойкость.

1. Симметричный – секретный ключ шифрования совпадающий с секретным ключом дешифрования(DEC)
2. Ассиметричный – открытый ключ для шифрования, закрытый для дешифрования (Алгоритм RSA)

C=E(m)=M^e mod n – шифрование по RSA

M=D© = c^d mod n – дешифрование по RSA

|  |  |  |
| --- | --- | --- |
| Характеристика | DEC | RSA |
| Скорость шифрования | Высокая | Низкая |
| Использ-е функция | Перестановка и подстановка | Возведене в степень |
| Длина ключа | Мин 56 бит | >500 бит |
| Наименее затратный криптоанализ | Перебор по всему ключевому пространству | Разложение модуля |
| Время ген-ии ключа | Мс | Мин |
| Тип ключа | Симметричный | ассиметричный |

По моему методу наилучшим методом шифрования является ассиметричный алгоритм RSA, но его существенным недостатком является низкая скорость шифрования. На взлом 512 битного ключа займет порядка 10 лет и затраты превысят 100.000$ . Единственный способ, с помощью которого можно довольно быстро найти ключ:

1. Взлом непосредственной базы компьютера и хищение ключа
2. Подмена ключей на шифрующем компьютере. Следовательно на магистрали злоумышленник перехватывает информацию, имею уже ключи для дешифрования, в то время как получатель не сможет расшифровать пакет, т.к. ключи были подменены.

**Методы противодействия прослушиванию**

Методы противодействия подслушиванию направлены, прежде всего, на предотвращение утечки информации в простом акустическом (гидроакустическом, сейсмическом) каналах. Кроме того, для повышения дальности подслушивания применяются составные каналы утечки информации, которые содержат наряду с простыми акустическими также радиоэлектронные (с использованием закладных устройств и вч-навязывания) и оптические (с лазерными средствами) каналы. Поэтому защита информации от подслушивания включает способы и средства блокирования любых каналов, с помощью которых производится утечка акустической информации.

В соответствии с общими методами защиты информации для защиты от подслушивания применяются следующие способы:

1. структурное скрытие, предусматривающее:

• шифрование семантической речевой информации в функциональных каналах связи;

• техническое закрытие электрических и радиосигналов в телефонных каналах связи;

• дезинформирование;

1. энергетическое скрытие путем:

• звукоизоляции акустического сигнала;

• звукопоглощения акустической волны;

• зашумления помещения или твердой среды распространения другими звуками (шумами, помехами), обеспечивающими маскировку акустических сигналов;

Какое шифрование лучше

Основной недостаток симметричного шифрования - необходимость передачи ключей "из рук в руки". Недостаток этот весьма серьезен, поскольку делает невозможным использование симметричного шифрования в системах с неограниченным числом участников. Однако в остальном симметричное шифрование имеет одни достоинства, которые хорошо видны на фоне серьезных недостатков шифрования асимметричного.

Первый из них - низкая скорость выполнения операций зашифрования и расшифрования, обусловленная наличием ресурсоемких операций. Другой недостаток "теоретический" - математически криптостойкость алгоритмов асимметричного шифрования не доказана. Это связано прежде всего с задачей дискретного логарифма - пока не удалось доказать, что ее решение за приемлемое время невозможно. Излишние трудности создает и необходимость защиты открытых ключей от подмены - подменив открытый ключ легального пользователя, злоумышленник сможет обеспечить зашифрование важного сообщения на своем открытом ключе и впоследствии легко расшифровать его своим секретным ключом.

Тем менее эти недостатки не препятствуют широкому применению алгоритмов асимметричного шифрования. Сегодня существуют криптосистемы, поддерживающие сертификацию открытых ключей, а также сочетающие алгоритмы симметричного и асимметричного шифрования

Заключение

В ходе выполнения курсовой работы были изучены основные типы и алгоритмы шифрования. Были проанализированы их плюсы и минусы. Как выяснилось идиальных и надежных на 100% систем не существует. Данные процедуры защиты только помогаю улучшить безопасность, но лучше что бы средств обеспечения безопасности было как можно больше, при условии что сама информация имеет ценность, превышающую по стоимости саму систему безопасности.

Использованная литература

1. Алгоритмы шифрования. Специальный справочник - Панасенко С. 2009, 564с
2. Утечка и защита информации в телефонных каналах - Лагутин В.С., Петраков А.В , Год издания: 2009, 324с
3. Кодирование и передача речи - Рихтер С.Г, 2009, 304с
4. <http://ru.wikipedia.org/wiki/RSA>
5. http://base.vingrad.ru/view/1154-Algoritm-shifrovaniya-MD5