**Лекция 1.  Основные цели и задачи обеспечения безопасности в телекоммуникационных системах**

Цель лекции: ознакомление студентов с целью и задачами дисциплины, с вопросами применения методов защиты информации в области телекоммуникаций.

Содержание:

а) основные цели и задачи обеспечения безопасности в телекоммуникационных системах;

б)угрозы информации;

в)средства защиты информации.

Вопрос защиты информации поднимается уже с тех пор, как только люди научились письменной грамоте. Всегда существовала информация, которую должны не все знать. Люди, обладающие такой информацией, прибегали к разным способам ее защиты. Это такие способы, как тайнопись (письмо симпатическими чернилами), шифрование ("тарабарская грамота", шифр Цезаря, более совершенные шифры замены, подстановки). В настоящее время всеобщей компьютеризации благополучие и даже жизнь многих людей зависят от обеспечения информационной безопасности множества компьютерных систем обработки информации, а также контроля и управления различными объектами. К таким объектам (их называют критическими) можно отнести системы телекоммуникаций, банковские системы, атомные станции, системы управления воздушным и наземным транспортом, а также системы обработки и хранения секретной и конфиденциальной информации. Для нормального и безопасного функционирования этих систем необходимо поддерживать их безопасность и целостность. В настоящее время для проникновения в чужие секреты используются такие возможности, как :

- подслушивание разговоров в помещении или автомашине с помощью предварительно установленных "радиожучков" или магнитофонов;

- контроль телефонов, телексных и телефаксных линий связи, радиотелефонов и  радиостанций;

- дистанционный съем информации с различных технических средств, в первую очередь, с мониторов и печатающих устройств компьютеров и другой электронной техники.

 Информационная сфера активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности РК. Национальная безопасность существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Естественно, возникает потребность защитить информацию от несанкционированного доступа, кражи, уничтожения и других преступных действий. Однако большая часть пользователей не осознает, что постоянно рискует своей безопасностью и личными тайнами. И лишь немногие, хоть каким - либо образом, защищают свои данные. Пользователи компьютеров регулярно оставляют полностью незащищенными даже такие данные, как налоговая и банковская информация, деловая переписка и электронные таблицы.

**Основные понятия в защите информации**

Угроза безопасности информации - совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации как несанкционированными, так и непреднамеренными воздействиями на нее.

Основными формами нарушения (угрозами), которые возможны  при наличии уязвимостей, применительно к основным свойствам информации,  являются:

- разглашение (конфиденциальной) информации – несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к этой информации;

- несанкционированный доступ (НСД) – получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

- изменение, искажение (модификация), копирование, уничтожение и др.  в результате непреднамеренных или несанкционированных воздействий;

- блокирование доступа к ЗИ в результате непреднамеренных или несанкционированных воздействий;

- уничтожение или сбой функционирования носителя ЗИ в результате непреднамеренных или несанкционированных воздействий.

Непреднамеренное воздействие на информацию (НПД) - ошибка пользователя информацией, сбой технических и программных средств информационных систем, природные явления или иные нецеленаправленные на изменение информации действия, приводящие к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Сбои оборудования:

- сбои кабельной системы, перебои электропитания; сбои дисковых систем; сбои систем архивации данных; сбои работы серверов, рабочих станций, сетевых карт и т.д:

-  потери информации из-за некорректной работы ПО;

- потери или изменение данных при ошибках ПО; потери при заражении системы компьютерными вирусами;

- технические средства получения информации:

- перехват электрического излучения;

- включение в электрическую цепь;

- жучки;

- акустический перехват;

- хищение информационных носителей;

- программные ловушки;

- внедрение вирусов.

Технические средства реализуются в виде электрических, электромеханических, электронных устройств. Вся совокупность технических средств принято делить на аппаратные устройства, встраиваемые непосредственно в аппаратуру, или устройства, которые сопрягаются с аппаратурой сети по стандартному интерфейсу (схемы контроля информации по четности, схемы защиты полей памяти по ключу, специальные регистры); физические - реализуются в виде автономных устройств и систем (электронно-механическое оборудование охранной сигнализации и наблюдения. Замки на дверях, решетки на окнах).

Программные средства - программы, специально предназначенные для выполнения функций, связанных с защитой информации.

**Абстрактные модели защиты информации**

Одной из первых моделей была опубликованная в 1977 модель Биба (Biba). Согласно ей все субъекты и объекты предварительно разделяются по нескольким уровням доступа, а затем на их взаимодействия накладываются следующие ограничения: 1) субъект не может вызывать на исполнение субъекты с более низким уровнем доступа; 2) субъект не может модифицировать объекты с более высоким уровнем доступа. Как видим, эта модель очень напоминает ограничения, введенные в защищенном режиме микропроцессоров Intel 80386+ относительно уровней привилегий.

Модель Гогена-Мезигера (Goguen-Meseguer), представленная ими в 1982 году, основана на теории автоматов. Согласно ей система может при каждом действии переходить из одного разрешенного состояния только в несколько других. Субъекты и объекты в данной модели защиты разбиваются на группы – домены, и переход системы из одного состояния в другое выполняется только в соответствии с так называемой таблицей разрешений, в которой указано, какие операции может выполнять субъект, скажем, из домена C над объектом из домена D. В данной модели при переходе системы из одного разрешенного состояния в другое используются транзакции, что обеспечивает общую целостность системы.

Сазерлендская (от англ. Sutherland) модель защиты, опубликованная в 1986 году, делает акцент на взаимодействии субъектов и потоков информации. Так же, как и в предыдущей модели, здесь используется машина состояний со множеством разрешенных комбинаций состояний и некоторым набором начальных позиций. В данной модели исследуется поведение множественных композиций функций перехода из одного состояния в другое.

Важную роль в теории защиты информации играет модель защиты Кларка-Вильсона (Clark-Wilson), опубликованная в 1987 году и модифицированная в 1989. Основана данная модель на повсеместном использовании транзакций и тщательном оформлении прав доступа субъектов к объектам. Но в данной модели впервые исследована защищенность третьей стороны в данной проблеме – стороны, поддерживающей всю систему безопасности. Эту роль в информационных системах обычно играет программа-супервизор. Кроме того, в модели Кларка-Вильсона транзакции впервые были построены по методу верификации, то есть идентификация субъекта производилась не только перед выполнением команды от него, но и повторно после выполнения. Это позволило снять проблему подмены автора в момент между его идентификацией и собственно командой. Модель Кларка-Вильсона считается одной из самых совершенных в отношении поддержания целостности информационных систем.

**Лекция 2. Особенности применения криптографических методов**

Цель лекции: ознакомление с основными криптографическими методами защиты информации.

Содержание:

а) криптография история развития;

б) виды шифрования.

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. История криптографии - ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. Священные книги Древнего Египта, Древней Индии тому примеры.

С широким распространением письменности криптография стала формироваться как самостоятельная наука. Первые криптосистемы встречаются уже в начале нашей эры. Так, Цезарь в своей переписке использовал уже  систематический шифр, получивший его имя.

Бурное развитие криптографические системы получили в годы первой и второй мировых войн. Начиная с послевоенного времени и по нынешний день, появление вычислительных средств ускорило разработку и совершенствование  криптографических методов.

Почему проблема использования криптографических методов в информационных системах (ИС) стала в настоящий момент особо актуальна?

С одной стороны, расширилось использование компьютерных сетей, в частности, глобальной сети Интернет, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможность доступа к ней посторонних лиц.

С другой стороны, появление новых мощных компьютеров,  технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем еще недавно считавшихся  практически не раскрываемыми.

Проблемой защиты информации путем ее преобразования занимается *криптология* (*kr*y*p*to*s* - тайный, lo*g*o*s* - наука). Криптология разделяется на два направления - *криптографию* и *криптоанализ*. Цели этих направлений прямо противоположны.

*Криптография* занимается поиском и исследованием математических методов преобразования информации.

Сфера интересов *криптоанализа* -  исследование возможности расшифровывания информации без знания ключей.

В этой книге основное внимание будет уделено криптографическим методам.

Современная криптография включает в себя четыре крупных раздела:

1)Симметричные криптосистемы.

2)Криптосистемы с открытым ключом.

3)Системы электронной подписи.

4)Управление ключами.

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

Итак, криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа.

В качестве информации, подлежащей шифрованию и дешифрованию, будут рассматриваться *тексты*, построенные на некотором *алфавите*. Под этими терминами понимается следующее.

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

*Текст* - упорядоченный набор из элементов алфавита.

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

-   алфавит Z33 - 32 буквы русского алфавита и пробел;

-   алфавит Z256 - символы, входящие в стандартные коды ASCII и КОИ8;

-   бинарный алфавит - Z2 = {0,1};

-   восьмеричный алфавит или шестнадцатеричный алфавит.

*Шифрование*- преобразовательный процесс: *исходный текст*, который носит также название *открытого текста*, заменяется *шифрованным текстом,*рисунок 2.1.

|  |
| --- |
|  |
|  |  |

Рисунок 2.1 - Шифрование

*Дешифрование* - обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный, рисунок 2.2.

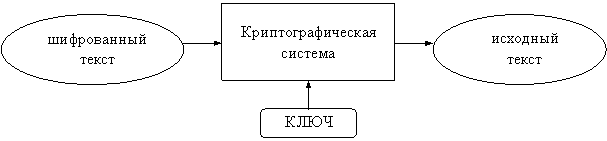


Рисунок 2.2 - Дешифрование

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

*Криптографическая система*представляет собой семейство **T**преобразований открытого текста. Члены этого семейства индексируются, или обозначаются символом *k*; параметр *k* является *ключом*. Пространство ключей *K* - это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита.

Криптосистемы разделяются на *симметричные* и *с открытым ключом*.

В *симметричных криптосистемах* и для шифрования, и для дешифрования используется *один и тот же ключ*.

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.

Термины *распределение ключей*и *управление ключами*относятся к процессам системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

*Электронной (цифровой) подписью* называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

*Криптостойкостью*называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. криптоанализу). Имеется несколько показателей криптостойкости, среди которых:

-   количество всех возможных ключей;

-   среднее время, необходимое для криптоанализа.

Преобразование T*k* определяется соответствующим алгоритмом и значением параметра *k*. Эффективность шифрования с целью защиты информации зависит от сохранения тайны ключа и криптостойкости шифра.

**Требования к криптосистемам**

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация более практична, допускает известную гибкость в использовании.

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

-  зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

-  число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;

-  число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);

-  знание алгоритма шифрования не должно влиять на надежность защиты;

-  незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения, даже при использовании одного и того же ключа;

-  структурные элементы алгоритма шифрования должны быть неизменными;

-  дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;

-  длина шифрованного текста должна быть равной длине исходного текста;

-  не должно быть простых и легко устанавливаемых зависимостью между ключами, последовательно используемыми в процессе шифрования;

-  любой ключ из множества возможных должен обеспечивать надежную защиту информации;

-        алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

**Лекция 3. Симметричные системы шифрования**

 Цель лекции:  ознакомление с основными криптографическими методами защиты информации.

Содержание:

а) общая схема симметричной криптосистемы;

б) шифры перестановки простой и сложной замены.

Все многообразие существующих криптографических методов можно свести к следующим классам преобразований, рисунок 3.1:

|  |
| --- |
|  |
|  |  |

Рисунок 3.1- Классы преобразований

*- Моно- и многоалфавитные подстановки.*

Наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие (того же алфавита) по более или менее сложному правилу. Для обеспечения высокой криптостойкости требуется использование больших ключей.

*- Перестановки.*

Также несложный метод криптографического преобразования. Используетс, как правило, в сочетании с другими методами.

*- Гаммирование.*

Этот метод заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа.

*- Блочные шифры.*

Представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста. Блочные шифры на практике встречаются чаще, чем “чистые” преобразования того или иного класса в силу их более высокой криптостойкости.

**Перестановки**

*Перестановкой* s набора целых чисел (0,1,...,N-1) называется его переупорядочение. Для того чтобы показать, что целое i перемещено из позиции i в позицию s(i), где 0 £ (i) <*n*, будем использовать запись

s=(s(0), s(1),..., s(N-1)).

Число перестановок из (0,1,...,N-1) равно*n*!=1\*2\*...\*(N-1)\*N. Введем обозначение s для взаимно-однозначного отображения (гомоморфизма) набора S={*s*0,*s*1, ...,*s*N-1}, состоящего из*n* элементов, на себя.

s: S ® S,

s: *s*i® *s*s(i), 0 £ i <*n.*

Будем говорить, что в этом смысле s является *перестановкой элементов* S. И, наоборот, автоморфизм S соответствует перестановке целых чисел (0,1,2,..,*n*-1).

*Криптографическим преобразованием* T для алфавита Zm называется последовательность автоморфизмов:

T={T(n):1£n<¥};

T(n): Zm,n®Zm,n, 1£n<¥.

Каждое T(n) является, таким образом, перестановкой*n*-грамм из Zm,n.

Поскольку T(i) и T(j)могут быть определены независимо  при i¹j, число криптографических преобразований исходного текста размерности*n* равно (mn)![[1]](https://libr.aues.kz/facultet/frts/kaf_tks/55/umm/tks_4.htm" \l "_ftn1" \o "). Оно возрастает непропорционально при увеличении*m* и*n*: так, при*m*=33 и*n*=2 число различных криптографических преобразований равно 1089!. Отсюда следует, что потенциально существует большое число отображений исходного текста в шифрованный.

Практическая реализация криптографических систем требует, чтобы преобразования {T*k*: *k*Î*K*} были определены алгоритмами, зависящими от относительно небольшого числа параметров (ключей).

**Системы подстановок**

*Определение* *Подстановкой* p на алфавите Zm называется автоморфизм Zm, при котором буквы исходного текста t замещены буквами шифрованного текста p(t):

Zm à Zm; p: t à p(t).

Набор всех подстановок называется симметрической группой Zm.

**Подстановка Цезаря**

Подстановка Цезаря является самым простым вариантом подстановки. Она относится к группе *моноалфавитных подстановок*.

Например, ВЫШЛИТЕ\_НОВЫЕ\_УКАЗАНИЯ посредством подстановки C3 преобразуется в еюыолхиврсеюивцнгкгрл.

Таблица 3.1

|  |  |  |  |
| --- | --- | --- | --- |
| Аàг | Йàм | Тàх | Ыàю |
| Бàд | Кàн | Уàц | Ьàя |
| Вàе | Лàо | Фàч | Эà\_ |
| Гàж | Мàп | Хàш | Юàа |
| Дàз | Нàр | Цàщ | Яàб |
| Еàи | Оàс | Чàъ | \_àв |
| Жàй | Пàт | Шàы |  |
| Зàк | Рàу | Щàь |  |
| Иàл | Сàф | Ъàэ |  |

При своей несложности система легко уязвима. Если злоумышленник имеет:

1) шифрованный и соответствующий исходный текст;

2) шифрованный текст выбранного злоумышленником исходного текста, то определение ключа и дешифрование исходного текста тривиальны.

Более эффективны обобщения подстановки Цезаря - *шифр Хилла* и *шифр Плэйфера*. Они основаны на подстановке не отдельных символов, а 2-грамм (шифр Плэйфера) или*n*-грамм[[2]](https://libr.aues.kz/facultet/frts/kaf_tks/55/umm/tks_4.htm" \l "_ftn2" \o ") (шифр Хилла). При более высокой криптостойкости они значительно сложнее для реализации и требуют достаточно большого количества ключевой информации.

**Многоалфавитные системы. Системы одноразового использования**

Слабая криптостойкость моноалфавитных подстановок преодолевается с применением подстановок многоалфавитных.

*Многоалфавитная подстановка* определяется ключом p=(p1,  
p2, ...), содержащим не менее двух различных подстановок. В начале рассмотрим многоалфавитные системы подстановок с нулевым начальным смещением.

Для такой системы подстановки используют также термин “одноразовая лента” и “одноразовый блокнот”. Пространство ключей К системы одноразовой подстановки является вектором рангов (*K*0, *K*1, ..., *K*n-1) и содержит*m*n точек.

Рассмотрим небольшой пример шифрования с бесконечным ключом. В качестве ключа примем текст

 “БЕСКОНЕЧНЫЙ\_КЛЮЧ....”.

Зашифруем с его помощью текст “ШИФР\_НЕРАСКРЫВАЕМ”. Шифрование оформим в таблицу 3.2:

Таблица 3.2

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ШИФРУЕМЫЙ\_ТЕКСТ | 24 | 8 | 20 | 16 | 19 | 5 | 12 | 27 | 9 | 32 | 18 | 5 | 10 | 17 | 18 |
| БЕСКОНЕЧНЫЙ\_КЛЮЧ | 1 | 5 | 17 | 10 | 14 | 13 | 5 | 23 | 13 | 27 | 9 | 32 | 10 | 11 | 30 |
| ЩРДЪАТТССЦЪЫДФЬП | 25 | 13 | 4 | 26 | 0 | 18 | 17 | 17 | 22 | 26 | 27 | 4 | 20 | 28 | 15 |

Исходный текст невозможно восстановить без ключа.

Наложение белого шума в виде бесконечного ключа на исходный текст меняет статистические характеристики языка источника. Системы одноразового использования*теоретически не расшифруемы*, так как не содержат достаточной информации для восстановления текста.

Почему же эти системы неприменимы для обеспечения секретности при обработке информации? Ответ простой - они непрактичны, так как требуют независимого выбора значения ключа для каждой буквы исходного текста. Хотя такое требование может быть и не слишком трудным при передаче по прямому кабелю Москва - Нью-Йорк, но для информационных оно непосильно, поскольку там придется шифровать многие миллионы знаков.

Посмотрим, что получится, если ослабить требование шифровать каждую букву исходного текста отдельным значением ключа.

**Системы шифрования Вижинера**

Начнем с конечной последовательности ключа

*k* = (*k*0 ,*k*1 ,...,*k*n),

 которая называется *ключом пользователя*, и продлим ее до бесконечной последовательности, повторяя цепочку. Таким образом, получим *рабочий ключ*

*k* = (*k*0 ,*k*1 ,...,*k*n), *k*j = *k*(jmod*r*, 0 £ j < ¥ .

Например, при *r* = ¥ и ключе пользователя 15 8 2 10 11 4 18 рабочий ключ будет периодической последовательностью:

15 8 2 10 11 4 18 15 8 2 10 11 4 18 15 8 2 10 11 4 18 ...

*Определение. Подстановка Вижинера* VI*Gk* определяется как

 VI*Gk* : (x0,*x*1, ...,*x*n-1) ® (y0,*y*1, ...,*y*n-1) = (x0+*k*,*x*1+*k*,. ..,*x*n-1+*k*).

Таким образом:

1) исходный текст*x* делится на *r* *фрагментов*

*x*i = (xi ,*x*i+*r* , ...,*x*i+*r*(n-1)), 0 £ i < *r*;

2) i-й фрагмент исходного текста*x*i шифруется при помощи подстановки Цезаря C*k* :

(xi ,*x*i+*r* , ...,*x*i+*r*(n-1)) ® (yi ,*y*i+*r* , ...,*y*i+*r*(n-1)).

Вариант системы подстановок Вижинера при*m*=2 называется *системой Вернама (1917 г)*.

В то время ключ *k*=(*k*0 ,*k*1 ,...,*k*к-1) записывался на бумажной ленте. Каждая буква исходного текста в алфавите, расширенном некоторыми дополнительными знаками, сначала переводилась с использованием *кода Бодо* в пятибитовый символ. К исходному тексту Бодо добавлялся ключ (по модулю 2). Старинный телетайп фирмы AT&T со считывающим устройством Вернама и оборудованием для шифрования, использовался корпусом связи армии США.

Очень распространена плохая, с точки зрения секретности, *практика использовать слово или фразу в качестве ключа* для того, чтобы                 *k*=(*k*0 ,*k*1 ,...,*k*к-1) было легко запомнить. В ИС для обеспечения безопасности информации это недопустимо. Для получения ключей должны использоваться программные или аппаратные средства случайной генерации ключей.

*Пример. Преобразование текста с помощью подстановки Вижинера (r=4).*

Исходный текст (ИТ1):

НЕ\_СЛЕДУЕТ\_ВЫБИРАТЬ\_НЕСЛУЧАЙНЫЙ\_КЛЮЧ

Ключ: КЛЮЧ

Разобьем исходный текст на блоки по 4 символа:

НЕ\_С ЛЕДУ ЕТ\_В ЫБИР АТЬ\_ НЕСЛ УЧАЙ НЫЙ\_ КЛЮЧ

и наложим на них ключ (используя таблицу Вижинера):

H+К=Ч, Е+Л=Р и т.д.

Получаем зашифрованный (ЗТ1) текст:

ЧРЭЗ ХРБЙ ПЭЭЩ ДМЕЖ КЭЩЦ ЧРОБ ЭБЮ\_ ЧЕЖЦ ФЦЫН

Следует признать, что и многоалфавитные подстановки в принципе доступны криптоаналитическому исследованию. Криптостойкость многоалфавитных систем резко убывает с уменьшением длины ключа.

Тем не менее такая система как шифр Вижинера допускает несложную аппаратную или программную реализацию и при достаточно большой длине ключа может быть использован в современных ИС.

**Лекция 4. Шифрование методом гаммирования. Стандарты DES и ГОСТ 28147-89**

 Цель лекции: ознакомление с основными симметричными методами защиты информации.

Содержание:

а) шифрование методом гаммирования;

б) датчики ПСЧ.

Гаммирование является также широко применяемым криптографическим преобразованием. На самом деле граница между гаммированием и использованием бесконечных ключей и шифров Вижинера, о которых речь шла выше, весьма условная.

Принцип *шифрования*гаммированием заключается в генерации гаммы шифра с помощью датчика псевдослучайных чисел и наложении полученной гаммы на открытые данные обратимым образом (например, используя сложение по модулю 2).

Процесс *дешифрования*данных сводится к повторной генерации гаммы шифра при известном ключе и наложении такой гаммы на зашифрованные данные.

Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей. По сути дела, гамма шифра должна изменяться случайным образом для каждого шифруемого слова. Фактически же, если период гаммы превышает длину всего зашифрованного текста и неизвестна никакая часть исходного текста, то шифр можно раскрыть только прямым перебором (пробой на ключ). Криптостойкость в этом случае определяется размером ключа.

Метод гаммирования становится бессильным, если злоумышленнику становится известен фрагмент исходного текста и соответствующая ему шифрограмма. Простым вычитанием по модулю получается отрезок ПСП и по нему восстанавливается вся последовательность.  Злоумышленники может сделать это на основе догадок о содержании исходного текста. Так, если большинство посылаемых сообщений начинается со слов “СОВ.СЕКРЕТНО”, то криптоанализ всего текста значительно облегчается. Это следует учитывать при создании реальных систем информационной безопасности.

Ниже рассматриваются наиболее распространенные методы генерации гамм, которые могут быть использованы на практике.

**атчики ПСЧ**

Чтобы получить линейные последовательности элементов гаммы, длина которых превышает размер шифруемых данных, используются *датчики ПСЧ*. На основе теории групп было разработано несколько типов таких датчиков.

**Конгруэнтные датчики**

В настоящее время наиболее доступными и эффективными являются *конгруэнтные*генераторы ПСП. Для этого класса генераторов можно сделать математически строгое заключение о том, какими свойствами обладают выходные сигналы этих генераторов с точки зрения периодичности и случайности.

Одним из хороших конгруэнтных генераторов является линейный конгруэнтный датчик ПСЧ. Он вырабатывает последовательности псевдослучайных чисел T(i), описываемые соотношением

T(i+1) = (A×T(i)+C)mod*m*,

где А и С - константы;

Т(0) - исходная величина, выбранная в качестве порождающего числа.

Очевидно, что эти три величины и образуют ключ.

Такой датчик ПСЧ генерирует псевдослучайные числа с определенным периодом повторения, зависящим от выбранных значений А и С. Значение *m* обычно устанавливается равным 2n , где*n* - длина машинного слова в битах. Датчик имеет максимальный период М до того, как генерируемая последовательность начнет повторяться. По причине, отмеченной ранее, необходимо выбирать числа А и С такие, чтобы период М был максимальным. Как показано Д. Кнутом, линейный конгруэнтный датчик ПСЧ имеет максимальную длину М тогда и только тогда, когда С - нечетное, и Аmod 4 = 1.

Для шифрования данных с помощью датчика ПСЧ может быть выбран ключ любого размера. Например, пусть ключ состоит из набора чисел*x*(j) размерностью b, где j=1, 2, ...,*n*. Тогда создаваемую гамму шифра *G* можно представить как объединение непересекающихся множеств H(j).

**Стандарт шифрования данных ГОСТ 28147-89****[[3]](https://libr.aues.kz/facultet/frts/kaf_tks/55/umm/tks_4.htm" \l "_ftn3" \o ")**

Важной задачей в обеспечении гарантированной безопасности информации в ИС является разработка и использование стандартных алгоритмов шифрования данных. Первым среди  подобных стандартов стал американский DES, представляющий собой последовательное использование замен и перестановок. В настоящее время все чаще говорят о неоправданной сложности и невысокой криптостойкости. На практике приходится использовать его модификации.

Более эффективным является отечественный стандарт шифрования данных.

Он рекомендован к использованию для защиты любых данных, представленных в виде двоичного кода, хотя не исключаются и другие методы шифрования. Данный стандарт формировался с учетом мирового опыта, и, в частности, были приняты во внимание недостатки и нереализованные возможности алгоритма DES, поэтому использование стандарта ГОСТ предпочтительнее. Алгоритм достаточно сложен, и ниже будет описана в основном его концепция.

Введем ассоциативную операцию конкатенации, используя для нее мультипликативную запись. Кроме того, будем использовать следующие операции сложения:

-  AÅB - побитовое сложение по модулю 2;

-  A[+]B - сложение по модулю 232;

-  A{+}B - сложение по модулю 232-1.

Алгоритм криптографического преобразования предусматривает несколько режимов работы. Во всех режимах используется ключ W длиной 256 бит, представляемый в виде восьми 32-разрядных чисел*x*(i).

W=X(7)X(6)X(5)X(4)X(3)X(2)X(1)X(0).

Для дешифрования используется тот же ключ, но процесс дешифрования является инверсным по отношению к исходному.

Самый простой из возможных режимов - *замена.*

Пусть открытые блоки разбиты на блоки по 64 бит в каждом, которые обозначим как T(j).

Очередная последовательность бит T(j) разделяется на две последовательности B(0) и A(0) по 32 бита (правый и левый блоки). Далее выполняется итеративный процесс шифрования описываемый следующими формулами, вид который зависит от i:

-       для i=1, 2, ..., 24, j=(i-1)mod 8;

A(i) = *f*(A(i-1) [+]*x*(j)) Å B(i-1);

B(i) = A(i-1);

-       для i=25, 26, ..., 31, j=32-i;

A(i) = *f*(A(i-1) [+]*x*(j)) Å B(i-1);

B(i) = A(i-1);

-       для i=32;

A(32) = A(31);

*B(32) = f(A(31) [+] x(0)) Å B(31).*

Здесь i обозначает номер итерации. Функция *f* – функция шифрования.

Функция шифрования включает две операции над 32-разрядным аргументом.

Первая операция является подстановкой *K*. Блок подстановки К состоит из 8 узлов замены К(1)...К(8) с памятью 64 бита каждый. Поступающий на блок подстановки 32-разрядный вектор разбивается на 8 последовательно идущих 4-разрядных вектора, каждый из который преобразуется в 4-разрядный вектор соответствующим узлом замены, представляющим из себя таблицу из 16 целых чисел в диапазоне 0...15. Входной вектор определяет адрес строки в таблице, число из которой является выходным вектором. Затем 4-разрядные векторы последовательно объединяются в 32-разрядный выходной.

Вторая операция - циклический сдвиг влево 32-разрядного вектора, полученного в результате подстановки К. 64-разрядный блок зашифрованных данных Т представляется в виде

Т=А(32)В(32).

Остальные блоки открытых данных в режиме простой замены зашифровываются аналогично.

Следует учитывать, что данный режим шифрования обладает ограниченной криптостойкостью.

В ГОСТ 28147-89 определяется процесс выработки имитовставки, который единообразен для всех режимов шифрования. Имитовставка - это блок из *р* бит (имитовставка Ир), который вырабатывается либо перед шифрованием всего сообщения, либо параллельно с шифрованием по блокам. Параметр *р* выбирается в соответствии с необходимым уровнем имитозащищенности.

Для получения имитовставки открытые данные представляются также в виде блоков по 64 бит. Первый блок открытых данных Т(1) подвергается преобразованию, соответствующему первым 16 циклам алгоритма режима простой замены. Причем в качестве ключа используется тот же ключ, что и для шифрования данных. Полученное 64-разрядное число суммируется с открытым блоком Т(2) и сумма вновь подвергается 16 циклам шифрования для режима простой замены. Данная процедура повторятся для всех*m* блоков сообщения. Из полученного 64-разрядного числа выбирается отрезок Ир длиной *р* бит.

Имитовставка передается по каналу связи после зашифрованных данных. На приемной стороне аналогичным образом из принятого сообщения выделяется  имитовставка и сравнивается с полученной. В случае несовпадения имитовставок сообщение считается ложным.

**Лекция 5.  Система шифрования с открытым ключом**. **Стандарты хэширования и цифровой подписи. Управление криптографическими ключами**

Цель лекции: ознакомить студентов с основными алгоритмами шифрования с открытым ключем.

Содержание:

а) система шифрования с открытым ключом (RSA);

б) шифр DES;

в) цифровые подписи и цифровые сертификаты.

Как бы ни были сложны и надежны криптографические системы - их слабое мест при практической реализации - проблема *распределения ключей*. Для того чтобы был возможен обмен конфиденциальной информацией между двумя субъектами ИС, ключ должен быть сгенерирован одним из них, а затем каким-то образом опять же в конфиденциальном порядке передан другому, т.е. в общем случае для передачи ключа опять же требуется использование какой-то криптосистемы.

Для решения этой проблемы на основе результатов, полученных классической и современной алгеброй, были предложены *системы с открытым ключом.*

Суть их состоит в том, что каждым адресатом ИС генерируются два ключа, связанных между собой по определенному правилу. Один ключ объявляется *открытым*, а другой - *закрытым*. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне.

Исходный текст шифруется открытым ключом адресата и передается ему. Зашифрованный текст в принципе не может быть расшифрован тем же открытым ключом. Дешифрование сообщения возможно только с использованием закрытого ключа, который известен только самому адресату, рисунок 4.1.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | | | | | |  | Скругленный прямоугольник: Адресат | |
|  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | | | | | | | | |  |
|  |  | | |  |  | |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

Рисунок 4.1

Криптографические системы с открытым ключом используют так называемые *необратимые  или односторонние функции*, которые обладают следующим свойством: при заданном значении*x* относительно просто вычислить значение *f(x),* однако, если*y*=*f(x*), то нет простого пути для вычисления значения*x.*

Множество классов необратимых функций и порождает все разнообразие систем с открытым ключом. Однако не всякая необратимая функция годится для использования в реальных ИС.

В самом определении необратимости присутствует неопределенность. Под *необратимостью* понимается не теоретическая необратимость, а практическая невозможность вычислить обратное значение, используя современные вычислительные средства за обозримый интервал времени.

Поэтому, чтобы гарантировать надежную защиту информации, к системам с открытым ключом (СОК) предъявляются два важных и очевидных требования:

1)     Преобразование исходного текста должно быть необратимым и исключать его восстановление на основе открытого ключа.

2)     Определение закрытого ключа на основе открытого также должно быть невозможным на современном технологическом уровне. При этом желательна точная нижняя оценка сложности (количества операций) раскрытия шифра.

Алгоритмы шифрования с открытым ключом получили широкое распространение в современных информационных системах. Так, алгоритм RSA стал мировым стандартом де-факто для открытых систем и рекомендован МККТТ.

Вообще же все предлагаемые сегодня криптосистемы с открытым ключом опираются на один из следующих типов необратимых преобразований:

1)     Разложение больших чисел на простые множители.

2)     Вычисление логарифма в конечном поле.

3)     Вычисление корней алгебраических уравнений.

Здесь же  следует отметить, что алгоритмы криптосистемы с открытым ключом (СОК) можно использовать в трех назначениях:

1) Как *самостоятельные средства защиты*передаваемых и хранимых данных.

2) Как *средства для распределения ключей*. Алгоритмы СОК более трудоемки, чем традиционные криптосистемы. Поэтому часто на практике рационально с помощью СОК распределять ключи, объем которых как информации незначителен. А потом с помощью обычных алгоритмов осуществлять обмен большими информационными потоками.

3)*Средства аутентификации пользователей*. Об этом будет рассказано в главе «Электронная подпись».

Ниже рассматриваются наиболее распространенные системы с открытым ключом.

Алгоритмы с открытым ключом, или *асимметричные алгоритмы*, базируются на использовании отдельных шифровального (открытого – public) и дешифровального (закрытого – private) ключей. В алгоритмах с открытым ключом требуется, чтобы закрытый ключ было невозможно вычислить по открытому ключу. Исходя из этого требования, шифровальный ключ может быть доступным кому угодно без какого-либо ущерба безопасности алгоритма шифрования.

Алгоритм Ривеста-Шамира-Эдлемана (RSA). Этот алгоритм носит инициалы его изобретателей. Он имеет важное значение, поскольку может быть использован как для шифрования, так и для цифровых подписей.

Стойкость алгоритма RSA определяется сложностью разложения больших чисел на множители. (Наверное, криптоанализ шифра RSA возможен и без использования операции разложения на множители, но никто до сих пор не доказал этого).

Ниже кратко описан принцип действия алгоритма RSA:

1)     Генерируется два простых числа *p*и *q* (100 цифр и более), причем *n=pq*.

2)     В качестве открытого ключа выбирается целое число *e*, взаимно простое с числом *(p-1)(q-1)*.

3)     Закрытый ключ d вычисляется из условия *ed mod (p-1)(q-1) = 1*.

4)     Шифрование открытого числа *m* (где *m < n*) осуществляется путем вычисления *mc mod n*.

5)     Расшифровка зашифрованного числа *c* осуществляется путем вычисления *cd mod m*.

Основным недостатком шифра RSA и других алгоритмов с открытым ключом является их низкая производительность, по сравнению с алгоритмами с секретным ключом. Алгоритм RSA уступает по скорости  сопоставимым реализациям алгоритма DES в 100, а то и в 1000 раз.

Хотя шифр RSA еще никому не удалось раскрыть, прогресс в математике может сделать этот шифр устаревшим. При наличии эффективного способа разложения больших чисел на множители шифр RSA можно легко раскрыть. К тому же алгоритм RSA и другие алгоритмы с открытым ключом не защищены от множества атак, которые определяются способами использования этих алгоритмов.

Алгоритм AlGamal. Хотя RSA и является одним из самых популярных алгоритмов шифрования с открытым ключом, имеется также множество других алгоритмов. Один из них – алгоритм AlGamal, разработанный в 1984 г. Тэгером Эль-Гамалом. Он не запатентован и может использоваться свободно.

Защищенность алгоритма AlGamal базируется на сложности вычисления дискретного логарифма в конечном поле. А заключается алгоритм в следующем:

1)     Выбирается простое число *p* и два случайных числа, *g* и *x*, меньших чем *p*.

2)     Открытый ключ состоит из чисел *g*, *p*, и *y*, где *y=gx mod p*. Закрытым ключом является число *x*.

3)     Для шифрования блока сообщения *m* выбирается случайное число *k*, такое, что *k* и *(p-1)* взаимно простые числа, и вычисляется *a=gk mod p*. Зашифрованным блоком являются оба числа – *a* и *b*.

4)     Для расшифровки *a* и *b* вычисляется *m=(b/ax) mod p*.

Шифрование с секретным ключом В некоторых алгоритмах шифрования для шифрования и расшифровки используется один и тот же ключ, или дешифровальный ключ может быть вычислен по шифровальному ключу за небольшое время. Такие алгоритмы называются алгоритмами с секретным ключом, алгоритмами с закрытым ключом или симметричными алгоритмами. Ключ, используемый в таких алгоритмах, должен храниться в тайне. Примером алгоритма с секретным ключом является алгоритм Data Encryption Stantart (DES).

В 1997 г. в США Национальным Институтом Стандартов и Технологий (NIST) в качестве стандартного алгоритма шифрования для защиты несекретной информации был принят алгоритм DES. Этот алгоритм вполне уверенно противостоял открытым попыткам взлома вплоть до середины 90-х годов, когда были отмечены попытки взлома с использованием методов дифференциального и линейного криптоанализа. К январю 1999 г. фонду Electronic Frontier Foundation уже удавалось взламывать сообщения, зашифрованные с помощью алгоритма DES, не более чем за сутки.

Несмотря на свою уязвимость, этот алгоритм все еще используется в некоторых приложениях и обеспечивает достаточно высокий уровень защиты в тех случаях, когда затраты на расшифровку информации превышают ее ценность. К тому же, DES уже используется в нескольких более сложных алгоритмов шифрования таких, например, как TripleDES.

Алгоритм DES может быть использован в различных методах шифрования, в зависимости от назначения. Вот несколько примеров методов шифрования:

Метод ECB (Electronic Codebook – Электронная шифровальная книга) – шифрование осуществляется 8-и-байтовыми блоками, причем последующий блок зашифрованного текста не зависит от предыдущих блоков как зашифрованного, так и открытого текста.

Метод CBC (Cipher Block Changing – Сцепление зашифрованных блоков) – n-ный блок шифруемого текста получается в результате выполнения операции XOR (исключающего или) над (n-1)-м блоком защифрованного текста и n-ным блоком открытого текста.

Метод CFB (Cipher Feedback – Обратная связь по шифру) – предыдущая порция зашифрованного текста объединяется со следующей порцией открытого текста.

Метод OFB (Output Feedback – Обратная связь по выходу) – алгоритм DES используется для создания псевдослучайного потока битов, который объединяется с открытым текстом, в результате чего создается поток зашифрованного текста.

Метод PCBC (Propagating Cipher Block Changing – Сцепление зашифрованных блоков с множественной связью) – Отличается от метода CBC тем, что с n-ным блоком зашифрованного текста объединяется как (n-1)-й блок зашифрованного текста, так и (n-1)-й блок открытого текста.

Алгоритм DESede.В связи с популярностью алгоритма DES и его недостатками, выявленными во второй половине 90-х годов, криптографы искали способы повышения его стойкости, при одновременном сохранении его в качестве базового алгоритма шифрования. В алгоритмах DESede выполняется троекратное шифрование по алгоритму DES, что приводит к эффективной длине ключа в 168 разрядов. В одном из вариантов DESede третий ключ равен первому, эффективная длина ключа в таком случае составляет 112 разрядов.

**Цифровые подписи и цифровые сертификаты**

Цифровые подписи обеспечивают замечательную возможность узнавать то, было ли сообщение (или иной объект) случайно или преднамеренно изменено. Цифровые сертификаты позволяют установить было ли сообщение действительно, создано конкретным лицом или организацией.

Цифровая подпись – это значение, которое вычисляется из последовательности байтов с использованием секретного ключа. Она свидетельствует о том, что владелец этого секретного ключа подтвердил корректность и подлинность содержимого сообщения. В методах цифровой подписи часто используются алгоритмы шифрования с открытым ключом, но несколько иначе, чем обычно, а именно: закрытый ключ применяется для шифрования, а открытый – для расшифровки. На практике это выглядит следующим образом:

1)     Создается цифровая подпись:

-        Вычисляется дайджест сообщения.

-        Дайджест сообщения зашифровывается с помощью закрытого ключа из пары “открытый/закрытый ключ”, в результате чего получается цифровая подпись.

2)     Производится верификация цифровой подписи:

-        Подпись расшифровывается с помощью открытого ключа из вышеупомянутой пары “открытый/закрытый ключ ”, в результате чего восстанавливается дайджест сообщения.

-        Значение расшифрованного дайджеста сообщения расшифровывается и сравнивается со значением дайджеста сообщения, вычисленного из исходного сообщения.

Если оба значения дайджеста сообщения совпадают, то подпись подлинная. В противном случае или подпись, или сообщение были изменены.

Описанный выше подход к созданию и проверке подписей несет в себе как характерные черты реальных подписей, так и другие особенности, которые обеспечивают следующие возможности:

1)     Подпись нельзя подделать – подписавшее лицо использует для подписи закрытый ключ, а он является секретным.

2)     Подлинность подписи всегда можно проверить – поскольку открытый ключ подписавшего лица общедоступен, любое лицо, имеющее в руках сообщение и цифровую подпись может проверить, что сообщение было подписано данным лицом и что ни оно, ни подпись не были изменены.

3)     Подпись неповторима – каждому сообщению соответствует своя, неповторимая подпись. Невозможно численными методами использовать подписи вместе с другим сообщением.

4)     Факт подписи невозможно отрицать – после того как сообщение подписано и отослано вместе с подписью, лицо, сделавшее это, не может отрицать, что оно сделало это (если только не докажет, это закрытый ключ был похищен).

Как видно, цифровые подписи – это прекрасный способ подтверждения того, что сообщение (или объект) было создано или проверено конкретным лицом или организацией. Но есть одна каверза – вам нужно каким-то образом определить, что открытый ключ, который вы получили от имени кого-то, - это действительно его открытый ключ. Вот где в дело вступают цифровые сертификаты.

Цифровые сертификаты – это сообщения, подписанные полномочным органом сертификации (Certificate Aythory – CA), который заверяет значение открытого ключа, принадлежащего кому-либо, и использование конкретного алгоритма шифрования. Чтобы получить сертификат полномочного органа сертификации, обычно нужно представить в него документы, подтверждающие личность заявителя.

**Лекция 6.  Управление криптографическими ключами**

Цель лекции: ознакомить студентов с основной задачей криптосистем – управление ключами.

Содержание:

а) управление ключами;

б) генерация, накопление, распределение  ключей;

в) обмен ключами по алгоритму Диффи - Хелмана.

**Управление ключами**

Кроме выбора подходящей для конкретной ИС криптографической системы, важная проблема - управление ключами. Как бы ни была сложна и надежна сама криптосистема, она основана на использовании ключей. Если для обеспечения конфиденциального обмена информацией между двумя пользователями процесс обмена ключами тривиален, то в ИС, где количество пользователей составляет десятки и сотни управления ключами - серьезная проблема.

Под *ключевой информацией*понимается совокупность всех действующих  в ИС ключей. Если не обеспечено достаточно надежное управление ключевой информацией, то, завладев ею, злоумышленник получает неограниченный доступ ко всей информации.

*Управление ключами*- информационный процесс, включающий в себя три элемента:

-         генерацию ключей;

-         накопление ключей;

-         распределение ключей.

Рассмотрим, как они должны быть реализованы для того, чтобы обеспечить безопасность ключевой информации в ИС.

**Генерация ключей**

В самом начале разговора о криптографических методах было сказано, что не стоит использовать неслучайные ключи с целью легкости их запоминания. В серьезных ИС используются специальные аппаратные и программные методы генерации случайных ключей. Как правило, используют датчики ПСЧ. Однако степень случайности их генерации должна быть достаточно высокой. Идеальными генераторами являются устройства на основе “натуральных” случайных процессов. Например, появились серийные образцы генерации ключей на основе *белого радиошума*. Другим случайным математическим объектом являются десятичные знаки иррациональных чисел, например, p или *е*, которые вычисляются с помощью стандартных математических методов.

 В ИС со средними требованиями защищенности вполне приемлемы программные генераторы ключей, которые вычисляют ПСЧ как сложную функцию от текущего времени и (или) числа, введенного пользователем.

**Накопление ключей**

Под *накоплением ключей*понимается организация их хранения, учета и удаления.

Поскольку ключ является самым привлекательным для злоумышленника объектом, открывающим ему путь к конфиденциальной информации, то вопросам накопления ключей следует уделять особое внимание.

*Секретные ключи никогда не должны записываться в явном виде на носителе, который может быть считан или скопирован.*

В достаточно сложной ИС один пользователь может работать с большим объемом ключевой информации, и иногда даже возникает необходимость организации мини-баз данных по ключевой информации. Такие базы данных отвечают за принятие, хранение, учет и удаление используемых ключей.

Итак, каждая информация об используемых ключах должна храниться в зашифрованном виде. Ключи, зашифровывающие ключевую информацию, называются *мастер-ключами*. Желательно, чтобы мастер-ключи каждый пользователь знал наизусть, и не хранил их вообще на каких-либо материальных носителях.

Очень важным условием безопасности информации является периодическое обновление ключевой информации в ИС. При этом переназначаться должны как обычные ключи, так и мастер-ключи. В особо ответственных ИС обновление ключевой информации желательно делать ежедневно.

Вопрос обновления ключевой информации связан и с третьим элементом управления ключами - распределением ключей.

**Распределение ключей**

Распределение ключей - самый ответственный процесс в управлении ключами. К нему предъявляются два требования:

1)  Оперативность и точность распределения.

2)  Скрытность распределяемых ключей.

В последнее время заметен сдвиг в сторону использования криптосистем с открытым ключом, в которых проблема распределения ключей отпадает. Тем не менее распределение ключевой информации в ИС требует новых эффективных решений.

Распределение ключей между пользователями реализуются двумя разными подходами:

1)  *Путем создания одного ли нескольких центров распределения ключей.*Недостаток такого подхода состоит в том, что в центре распределения известно, кому и какие ключи назначены,  и это позволяет читать все сообщения, циркулирующие в ИС. Возможные злоупотребления существенно влияют на защиту.

2)  *Прямой обмен ключами*между пользователями информационной системы. В этом случае проблема состоит в том, чтобы надежно удостоверить подлинность субъектов.

В обоих случаях должна быть гарантирована подлинность сеанса связи. Это можно обеспечить двумя способами:

1)  *Механизм запроса-ответа*, который состоит в следующем. Если пользователь А желает быть уверенным, что сообщения, которые он получает от В, не являются ложными, он включает в посылаемое для В сообщение непредсказуемый элемент (запрос). При ответе пользователь В должен выполнить некоторую операцию над этим элементом (например, добавить 1). Это невозможно осуществить заранее, так как неизвестно, какое случайное число придет в запросе. После получения ответа с результатами действий пользователь А может быть уверен, что сеанс является подлинным. Недостатком этого метода является возможность установления, хотя и сложной закономерности между запросом и ответом.

2)  *Механизм отметки времени (“временной штемпель”).*Он подразумевает фиксацию времени для каждого сообщения. В этом случае каждый пользователь ИС может знать, насколько “старым” является пришедшее сообщение.

В обоих случаях следует использовать шифрование, чтобы быть уверенным, что ответ послан незлоумышленником, и штемпель отметки времени не изменен.

Для обмена ключами можно использовать криптосистемы с открытым ключом, используя тот же алгоритм RSA.

Но весьма эффективным оказался алгоритм Диффи-Хелмана, позволяющий двум пользователям без посредников обменяться ключом, который может быть использован затем для симметричного шифрования.

**Алгоритм Диффи-Хеллмана**

Диффи и Хелман предложили для создания криптографических систем с открытым ключом *функцию дискретного возведения в степень*.

Необратимость преобразования в этом случае обеспечивается тем, что достаточно легко вычислить показательную функцию в конечном поле Галуа, состоящим из *p*элементов. (*p*- либо простое число, либо простое в любой степени). Вычисление же логарифмов в таких полях - значительно более трудоемкая операция.

Если*y*=a*x*,, 1<*x*<*p*-1, где  - фиксированный элемент поля *GF(p)*, то   *x*=lo*g*a*y* над *GF(p)*. Имея*x*, легко вычислить*y*. Для этого потребуется 2 ln(*x*+*y*) операций умножения.

Обратная задача вычисления*x* из*y* будет достаточно сложной. Если *p* выбрано достаточно правильно, то извлечение логарифма потребует вычислений, пропорциональных

*L(p)* = *exp* { (ln *p*ln ln *p*)0.5 }.

Для обмена информацией первый пользователь выбирает случайное число*x*1, равновероятное из целых 1...*p*-1. Это число он держит в секрете, а другому пользователю посылает число

*y*1 = a*x*mod *p.*

Аналогично поступает и второй пользователь, генерируя*x*2 и вычислив*y*2, отправляя его первому пользователю. В результате этого они могут вычислять *k*12 = a*x*1*x*2mod *p*.

Для того чтобы вычислить *k*12 первый пользователь возводит*y*2 в степень*x*1. То же делает и второй пользователь. Таким образом, у обоих пользователей оказывается общий ключ *k*12, который можно использовать для шифрования информации обычными алгоритмами. В отличие от алгоритма RSA, данный алгоритм не позволяет шифровать собственно информацию.

Не зная*x*1и*x*2, злоумышленник может попытаться вычислить *k*12, зная только перехваченные*y*1и*y*2. Эквивалентность этой проблемы проблеме вычисления дискретного логарифма есть главный и открытый вопрос в системах с открытым ключом. Простого решения до настоящего времени не найдено. Так, если для прямого преобразования 1000-битных простых чисел требуется 2000 операций, то для обратного преобразования (вычисления логарифма в поле Галуа) потребуется около 1030 операций.

Как видно, при всей простоте алгоритма Диффи-Хелмана вторым его недостатком по сравнению с системой RSA является отсутствие гарантированной нижней оценки трудоемкости раскрытия ключа.

Кроме того, хотя описанный алгоритм позволяет обойти проблему скрытой передачи ключа, необходимость аутентификации остается. Без дополнительных средств один из пользователей не может быть уверен, что он обменялся ключами именно с тем пользователем, который ему нужен. Опасность имитации в этом случае остается.

В качестве обобщения сказанного о распределении ключей следует сказать следующее. Задача управления ключами сводится к поиску такого протокола распределения ключей, который обеспечивал бы:

-         возможность отказа от центра распределения ключей;

-         взаимное подтверждение подлинности участников сеанса;

-         подтверждение достоверности сеанса механизмом запроса-ответа, использование для этого программных или аппаратных средств;

-         использование при обмене ключами минимального числа сообщений.

**Лекция 7. Защита сетей от удаленных атак с помощью межсетевых экранов**

Цель лекции: ознакомление студентов с функционированием межсетевых экранов  и их основных компонентов.

Содержание:

а) предназначение межсетевых экранов;

б) способы исполнения межсетевых экранов;

в)пакетная фильтрация.

Интенсивное развитие глобальных компьютерных сетей. появление  новых  технологий  поиска  информации привлекают  все  больше  внимания  к  сети  Internet  со стороны частных  лиц  и  различных  организаций.  Многие организации принимают решение об интеграции своих локальных и  корпоративных  сетей в глобальную сеть. В силу открытости  своей идеологии  Internet предоставляет для злоумышленников значительно большие   возможности по сравнению с традиционными информационными системами. Поэтому вопрос о проблеме защиты сетей и её  компонентов становится достаточно важным и актуальным.

Ряд задач по отражению наиболее вероятных угроз для внутренних сетей способны решать межсетевые экраны, В отечественной литературе до последнего времени использовались вместо этого термина другие термины иностранного происхождения: брандмауэр и firewall. Вне компьютерной сферы брандмауэром (или firewall) называют стену, сделанную из негорючих материалов и препятствующую распространению пожара. В сфере компьютерных сетей межсетевой экран представляет собой барьер, защищающий от фигурального пожара - попыток злоумышленников вторгнуться во внутреннюю сеть для того, чтобы скопировать, изменить или стереть информацию, либо воспользоваться памятью или вычислительной  мощностью работающих в этой сети компьютеров. Межсетевой экран призван обеспечить безопасный доступ к  внешней сети и ограничить доступ  внешних  пользователей  к  внутренней сети.

Межсетевой экран (МЭ) - это система межсетевой защиты, позволяющая разделить общую сеть  на  две  части или  более и  реализовать  набор  правил,  определяющих условия прохождения пакетов с данными через  границу  из одной части общей сети в  другую. Как  правило,  эта граница проводится между корпоративной (локальной) сетью предприятия и глобальной сетью Internet, хотя  ее  можно провести и внутри  корпоративной  сети  предприятия. МЭ пропускает через себя весь трафик, принимая для  каждого проходящего  пакета  решение - пропускать его или отбросить. Для того чтобы МЭ мог осуществить это, ему необходимо определить набор правил фильтрации.

Главный довод в  пользу  применения  межсетевого  экрана состоит в том, что  без  него  системы  внутренней  сети подвергаются опасности со стороны слабо защищенных служб сети Internet, а также зондированию и  атакам  с  каких- либо других хост-компьютеров внешней сети.

Большинство компонентов межсетевых  экранов  можно отнести к одной из трех категорий:

1)  фильтрующие маршрутизаторы;

2)  шлюзы сетевого уровня;

3)  шлюзы прикладного уровня.

Эти  категории  можно  рассматривать  как  базовые компоненты реальных межсетевых  экранов.  Лишь  немногие межсетевые экраны включают только одну из  перечисленных категорий. Тем не менее, эти категории отражают ключевые возможности, отличающие межсетевые экраны друг от друга.

Для защиты корпоративной или локальной сети применяются следующие основные схемы организации межсетевых экранов:

1)  межсетевой экран -  фильтрующий маршрутизатор;

2)  межсетевой экран на основе двупортового шлюза;

3)  межсетевой экран на основе экранированного шлюза;

4)  межсетевой экран – экранированная подсеть.

Межсетевой  экран, основанный на фильтрации  пакетов, является самым распространенным и  наиболее простым в реализации. Он  состоит  из  фильтрующего маршрутизатора, расположенного между защищаемой сетью  и сетью Internet. Фильтрующий маршрутизатор сконфигурирован для  блокирования  или фильтрации входящих и исходящих  пакетов  на  основе анализа их адресов и портов. Компьютеры, находящиеся в  защищаемой  сети,  имеют  прямой  доступ  в  сеть Internet, в то время как большая часть доступа к ним из Internet  блокируется.  Часто  блокируются  такие опасные службы, как Х Windows, NIS и NFS. В принципе фильтрующий маршрутизатор может реализовать любую из политик безопасности.

Межсетевой экран на базе двупортового прикладного шлюза  включает  двудомный  хост-компьютер  с  двумя сетевыми интерфейсами. При передаче информации между этими интерфейсами и осуществляется основная фильтрация. Для обеспечения дополнительной защиты между прикладным шлюзом и сетью Internet обычно размещают фильтрующий маршрутизатор. В результате между прикладным шлюзом и маршрутизатором образуется внутренняя экранированная подсеть. Эту подсеть можно использовать для размещения доступных извне информационных серверов.

В отличие от схемы межсетевого экрана с фильтрующим маршрутизатором прикладной шлюз полностью блокирует трафик IР между сетью internet и защищаемой сетью. Только полномочные сервера - посредники, располагаемые на прикладном шлюзе, могут предоставлять услуги и доступ пользователям.

Данный  вариант межсетевого экрана реализует политику  безопасности,   основанную на принципе "запрещено все, что не разрешено в явной форме", при этом пользователю недоступны все службы, кроме  тех, для которых определены  соответствующие  полномочия. Такой подход обеспечивает    высокий уровень безопасности, только маршруты к  защищенной  подсети известны только межсетевому экрану и скрыты от внешних систем.   Рассматриваемая  схема  организации межсетевого экрана  является  довольно  простой и достаточно эффективной. Следует отметить, что безопасность  двудомного хост-компьютера, используемого в качестве прикладного шлюза, должна поддерживаться на высоком уровне. Любая брешь в его защите  может серьезно ослабить безопасность защищаемой сети. Если шлюз окажется   скомпрометированным, у злоумышленника появится возможность проникнуть в защищаемую сеть. Этот межсетевой экран может требовать от пользователей применение средств усиленной аутентификации, а также регистрации доступа, попыток зондирования и атак системы нарушителем.

Межсетевой экран на основе экранированного шлюза объединяет фильтрующий маршрутизатор и прикладной шлюз, разрешаемый  со  стороны внутренней сети. Прикладной шлюз реализуется на хост – компьютере  и имеет только один сетевой интерфейс В этой схеме первичная безопасность обеспечивается фильтрующим маршрутизатором.

Межсетевой экран, состоящий из экранированной подсети,   представляет собой развитие схемы межсетевого экрана на основе экранированного шлюза. Для создания экранированной подсети используются два экранирующих маршрутизатора. Внешний маршрутизатор располагается между сетью  internet и экранируемой подсетью, а внутренний - между экранируемой подсетью и защищаемой внутренней сетью. Экранируемая подсеть содержит прикладной шлюз, а также может включать информационные серверы и другие системы, требующие  контролируемого  доступа. Эта схема межсетевого экрана обеспечивает хорошую безопасность  благодаря организации экранированной подсети, которая еще лучше  изолирует  внутреннюю защищаемую сеть от Internet.

Некоторые межсетевые экраны позволяют организовать виртуальные корпоративные сети. Несколько локальных сетей, подключенных к глобальной сети, объединяются в одну виртуальную  корпоративную сеть. Передача данных между этими локальными сетями производится прозрачным образом для пользователей локальных сетей. Конфиденциальность и целостность передаваемой информации должны обеспечиваться при помощи средств шифрования, использование цифровых подписей. При передаче данных может шифроваться не только содержимое пакета, но и некоторые поля заголовка.

**Пакетная фильтрация. Использование маршрутизаторов в качестве firewall**

Фильтрация осуществляется на транспортном уровне: все проходящие через межсетевой экран пакеты или кадры данных анализируются, и те из них, которые имеют в определенных полях заданные ("неразрешенные") значения, отбрасываются.

Пропуск во внутреннюю сеть пакетов сетевого уровня или кадров канального уровня по адресам (MAC-адреса, IP-адреса, IPX-адреса) или номерам портов TCP, соответствующих приложениям. Например, для того, чтобы трафик telnet не пересекал границу внутренней сети, межсетевой экран должен отфильтровывать все пакеты, в заголовке TCP которых указан адрес порта процесса-получателя, равный 23 (этот номер зарезервирован за сервисом telnet). Сложнее отслеживать трафик FTP, который работает с большим диапазоном возможных номеров портов, что требует задания более сложных правил фильтрации.

Конечно, для фильтрации пакетов может быть использован и обычный маршрутизатор, и действительно, в Internet 80% пакетных фильтров работают на базе маршрутизаторов. Однако маршрутизаторы не могут обеспечить ту степень защиты данных, которую гарантируют межсетевые экраны.

Главные преимущества фильтрации межсетевым экраном по сравнению с фильтрацией маршрутизатором состоят в следующем:

1)     Межсетевой экран обладает гораздо более развитыми логическими способностями, поэтому он в отличие от маршрутизатора легко может, например, обнаружить обман по IP-адресу.

2)     Межсетевой экран имеет большие возможности аудита всех событий, связанных с безопасностью.

**Лекция 8.  Технология виртуальных корпоративных сетей**

Цель лекции: технология VPN как один из способов защиты информации.

Содержание:

а) степень значимости VPN;

б) процесс  туннелирования;

в) основные протоколы, применяемые в технологии VPN.

Осознавая данную проблему, корпоративные пользователи Интернета в наиболее развитых странах мира уже начинают предъявлять все большие требования не только к скорости доступа, но и к качеству передачи данных, которое наряду с традиционными параметрами QoS включает в себя и обеспечение конфиденциальности, целостности и подлинности информации, передаваемой через Интернет. Особенно важным это требование становится в тех случаях, когда корпоративные пользователи по причине чрезвычайной дороговизны выделенных каналов и недостаточной их защищенности вынуждены строить собственные системы информационной безопасности (СИБ) как в рамках intranet, так и extranet сетей.

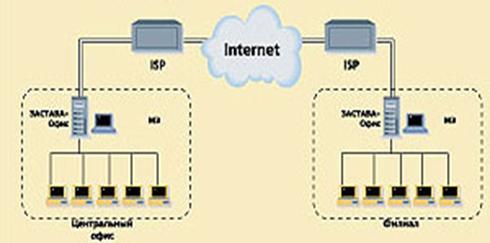
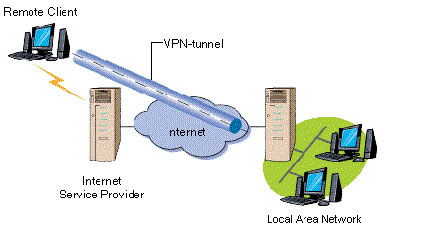


Рисунок 8.1 – Предоставление VPN-услуг

По мнению большинства экспертов, сегодня одним из самых грамотных и экономически выгодных решений для создания СИБ становится построение так называемых Virtual Private Network (VPN) - защищенных виртуальных частных сетей, основанных на современных технологиях криптографической защиты, передаваемых по открытым сетям данных. Стратегические преимущества применения VPN-технологий, видимо, уже осознали большинство распределенных компаний, поскольку отказ от выделенных линий связи и переход на VPN уже приобрел массовый характер не только на Западе, где рынок VPN-услуг в последнее время очень активно развивается, но и в России. Причем, что интересно, доминирующее положение на рынке VPN-услуг на Западе начинают занимать не специализированные фирмы - системные интеграторы, а Интернет-провайдеры, которые постепенно расширяют спектр предлагаемых своим клиентам услуг, в том числе и за счет VPN, превращаясь из традиционных Интернет-провайдеров (ISP) в сервис-провайдеров (xSP).

VPN отличается рядом экономических преимуществ по сравнению с другими методами удаленного доступа. Во-первых, пользователи могут обращаться к корпоративной сети, не устанавливая c ней коммутируемое соединение, таким образом, отпадает надобность в использовании модемов. Во-вторых, можно обойтись без выделенных линий.

  
Рисунок 8.2 – VPN для удаленных пользователей

Имея доступ в Интернет, любой пользователь может без проблем подключиться к сети офиса своей фирмы. Следует заметить, что общедоступность данных совсем не означает их незащищенность. Система безопасности VPN - это броня, которая защищает всю корпоративную информацию от несанкционированного доступа. Прежде всего, информация передается в зашифрованном виде. Прочитать полученные данные может лишь обладатель ключа к шифру. Наиболее часто используемым алгоритмом кодирования является Triple DES, который обеспечивает тройное шифрование (168 разрядов) с использованием трех разных ключей. Подтверждение подлинности включает в себя проверку целостности данных и идентификацию пользователей, задействованных в VPN. Первая гарантирует, что данные дошли до адресата именно в том виде, в каком были посланы. Самые популярные алгоритмы проверки целостности данных - MD5 и SHA1. Далее система проверяет, не были ли изменены данные во время движения по сетям, по ошибке или злонамеренно. Таким образом, построение VPN предполагает создание защищенных от постороннего доступа туннелей между несколькими локальными сетями или удаленными пользователями. Для построения VPN необходимо иметь на обоих концах линии связи программы шифрования исходящего и дешифрования входящего трафиков. Они могут работать как на специализированных аппаратных устройствах, так и на ПК с такими операционными системами, как Windows, Linux или NetWare.

Управление доступом, аутентификация и шифрование - важнейшие элементы защищенного соединения.

Туннелирование (tunneling), или инкапсуляция (encapsulation), - это способ передачи полезной информации через промежуточную сеть. Такой информацией могут быть кадры (или пакеты) другого протокола. При инкапсуляции кадр не передается в сгенерированном узлом-отправителем виде, а снабжается дополнительным заголовком, содержащим информацию о маршруте, позволяющую инкапсулированным пакетам проходить через промежуточную сеть (Internet). На конце туннеля кадры деинкапсулируются и передаются получателю. Этот процесс (включающий инкапсуляцию и передачу пакетов) и есть туннелирование. Логический путь передвижения инкапсулированных пакетов в транзитной сети называется туннелем.

VPN работает на основе протокола PPP(Point-to-Point Protocol). Протокол PPP разработан для передачи данных по телефонным линиям и выделенным соединениям "точка-точка". PPP инкапсулирует пакеты IP, IPX и NetBIOS в кадры PPP и передает их по каналу "точка-точка". Протокол PPP может использоваться маршрутизаторами, соединенными выделенным каналом, или клиентом и сервером RAS, соединенными удаленным подключением:

- Инкапсуляция обеспечивает мультиплексирование нескольких транспортных протоколов по одному каналу.

- Протокол LCP - PPP задает гибкий LCP для установки, настройки и проверки канала связи. LCP обеспечивает согласование формата инкапсуляции, размера пакета, параметры установки и разрыва соединения, а также параметры аутентификации. В качестве протоколов аутентификации могут использоваться PAP, CHAP и др.

- Протоколы управления сетью предоставляют специфические конфигурационные параметры для соответствующих транспортных протоколов. Например, IPCP протокол управления IP.

Для формирования туннелей VPN используются протоколы PPTP, L2TP, IPsec, IP-IP:

- Протокол PPTP позволяет инкапсулировать IP-, IPX- и NetBEUI-трафик в заголовки IP для передачи по IP-сети, например, Internet.

- Протокол L2TP позволяет шифровать и передавать IP-трафик с использованием любых протоколов, поддерживающих режим "точка-точка" доставки дейтаграмм. Например, к ним относятся протокол IP, ретрансляция кадров и асинхронный режим передачи (АТМ).

- Протокол IPsec позволяет шифровать и инкапсулировать полезную информацию протокола IP в заголовки IP для передачи по IP-сетям.

- Протокол IP-IP - IP-дейтаграмма инкапсулируется с помощью дополнительного заголовка IP. Главное назначение IP-IP - туннелирование многоадресного трафика в частях сети, не поддерживающих многоадресную маршрутизацию. Для технической реализации VPN, кроме стандартного сетевого оборудования, понадобится шлюз VPN, выполняющий все функции по формированию туннелей, защите информации, контролю трафика, а нередко и функции централизованного управления. На сегодняшний день VPN - это экономичное, надежное и общедоступное решение организации удаленного доступа. Каким бы ни было расстояние, VPN обеспечит соединение с любой точкой мира и сохранность передачи самых важных данных.

**Плюсы VPN**

Плюсы VPN убедительны, что многие компании начинают строить свою стратегию с учетом использования Интернета в качестве главного средства передачи информации, даже уязвимой.

При правильном выборе VPN:

1)     вы получаете защищенные каналы связи по цене доступа в Интернет, что в несколько раз дешевле выделенных линий;

2)     при установке VPN не требуется изменять топологию сетей, переписывать приложения, обучать пользователей - все это обеспечивает значительную экономию;

3)     обеспечивается масштабирование, поскольку VPN не создает проблем роста и сохраняет сделанные инвестиции;

4)     вы независимы от криптографии и можете использовать модули криптографии любых производителей в соответствии с национальными стандартами той или иной страны;

5)     открытые интерфейсы позволяют интегрировать вашу сеть с другими программными продуктами и бизнес-приложениями.

**Минусы VPN**

К ним можно отнести сравнительно низкую надежность. В сравнении с выделенными линиями и сетями на основе Frame relay виртуальные частные сети менее надежны, однако, в 5-10, а иногда и в 20 раз дешевле. По мнению западных аналитиков, это не остановит продажу VPN, поскольку лишь 5% пользователей, торгующих, например, на рынке ценных бумаг, требуются такие высокие стандарты. Остальные 95% не столь серьезно относятся к проблемам со связью, а затраты большего количества времени на получение информации не приводят к колоссальным убыткам.

В силу того, что услуга VPN предоставляется и поддерживается внешним оператором, могут возникать проблемы со скоростью внесения изменений в базы доступа, в настройки firewall, а также с восстановлением вышедшего из строя оборудования. В настоящее время проблема решается указанием в договорах максимального времени на устранение неполадок и внесение изменений. Обычно оно составляет несколько часов, но встречаются провайдеры, гарантирующие устранение неполадок в течение суток.

Еще один существенный недостаток - у потребителей нет удобных средств управления VPN, хотя в последнее время разрабатывается оборудование, позволяющее автоматизировать управление VPN. Среди лидеров этого процесса - компания Indus River Networks Inc., дочерняя компания MCI WorldCom и Novell. Как говорят аналитики Forester Research, VPN должны контролироваться пользователями, управляться компаниями-операторами, а задача разработчиков программного обеспечения - решить эту проблему.

**Лекция 9.  Методы защиты программ от разрушающих программных воздействий**

Цель лекции: изучение основных разновидностей и характеристик компьютерных вирусов.

 Содержание:

а) вирусы, характеристика, классификация;

б) разновидности компьютерных вирусов.

Можно привести массу фактов, свидетельствующих о том, что угроза информационному ресурсу возрастает с каждым днем, подвергая в панику ответственных лиц в банках, на предприятиях и в компаниях во всем мире. И угроза эта исходит от компьютерных вирусов, которые искажают или уничтожают жизненно важную, ценную информацию, что может привести не только к финансовым потерям, но и к человеческим жертвам.

Вирус - это специально написанная небольшая по размерам программа, которая может "приписывать" себя  к другим  программам (т.е. "заражать" их), а  также  выполнять различные  нежелательные действия  на компьютере. Программа, внутри  которой находится  вирус, называется "зараженной". Когда такая программа начинает работу, то сначала управление  получает вирус. Вирус находит и "заражает" другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы  или  таблицу  размещения  файлов на диске, "засоряет"  оперативную память и т.д.). Для маскировки  вируса действия  по заражению  других программ и нанесению вреда могут выполняться не  всегда, а, скажем, при выполнении  определенных условий. После того как вирус  выполнит нужные  ему действия, он  передает управление той программе, в которой он находится, и она работает так же, как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной. Разновидности вирусов  устроены так, что при запуске зараженной  программы вирус остается резидентно, т.е. до перезагрузки DOS, компьютера, и время от времени заражает программы и выполняет вредные действия на компьютере.

Компьютерный вирус может испортить, т.е. изменить ненадлежащим образом, любой файл на имеющих в компьютере дисках. Но некоторые виды файлов вирус может "заразить". Это означает, что вирус  может "внедриться" в эти файлы, т.е. изменить их так, что они будут содержать  вирус, который при некоторых обстоятельствах может начать свою работу.

Следует заметить, что тексты программ и документов, информационные файлы без данных, таблицы табличных  процессоров и другие аналогичные файлы  не могут быть заражены вирусом, он может их только испортить.

В настоящее время известно более 5000 вирусов, число которых непрерывно растет. Известны случаи, когда создавались учебные пособия, помогающие в написании вирусов.

Основные виды вирусов: загрузочные, файловые, файлово-загрузочные. Наиболее опасный вид вирусов - полиморфные. Из истории компьютерной вирусологии ясно, что любая оригинальная компьютерная разработка заставляет создателей антивирусов приспосабливаться к новым технологиям, постоянно усовершенствовать антивирусные программы.

Причины появления и распространения вирусов скрыты с одной стороны в психологии человека, с другой стороны - с отсутствием средств защиты у операционной системы.

Основные пути проникновения вирусов - съемные диски и  компьютерные сети. Чтобы этого не случилось, соблюдайте меры по защите. Также для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов следствием не вполне ясного понимания предмета.

Вирус - программа, обладающая способностью к самовоспроизведению. Такая способность является единственным средством, присущим всем типам вирусов. Но не только вирусы способны к самовоспроизведению. Любая операционная система и еще множество программ способны создавать собственные копии. Копии же вируса не только не обязаны полностью совпадать с оригиналом, но и могут вообще с ним не совпадать!

Вирус не может существовать в «полной изоляции»: сегодня нельзя представить себе вирус, который не использует код других программ, информацию о файловой структуре или даже просто имена других программ. Причина понятна: вирус должен каким-нибудь способом обеспечить передачу себе управления.

В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные. Сетевые вирусы распространяются по различным компьютерным сетям. Файловые вирусы внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения  COM  и  EXE. В файл вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению. Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-с) или в сектор, содержащий программу загрузки системного диска (Master Boot Re-cord). Файлово-загрузочные вирусы заражают как файлы, так и загрузочные сектора дисков.

По способу заражения вирусы делятся на резидентные и нерезидентные. Резидентный вирус при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными, вплоть до выключения или перезагрузки компьютера. Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

По степени воздействия вирусы можно разделить на следующие виды:

-       неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических  или звуковых эффектах;

-       опасные вирусы, которые могут привести к различным нарушениям в работе компьютера;

-       очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия. Простейшие вирусы паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены. Можно отметить вирусы-репликаторы, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии. Известны вирусы-невидимки, называемые стелс-вирусами, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска. Наиболее трудно обнаружить вирусы-мутанты, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов. Имеются и так называемые квазивирусные или «троянские» программы, которые  хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

Каждая конкретная разновидность вируса может заражать только один или два типа файлов. Чаще всего встречаются вирусы, заражающие исполнимые файлы. Некоторые вирусы заражают и файлы, и загрузочные области дисков. Вирусы, заражающие  драйверы устройств, встречаются крайне редко, обычно такие вирусы  умеют заражать  и исполнимые файлы.

В последнее время получили распространение вирусы нового типа - вирусы, имеющие файловую  систему на диске. Эти вирусы обычно называются  DIR. Т,  вирусы прячут свое тело в некоторый  участок диска (обычно - в последний кластер диска) и помечают его в таблице размещения файлов (FAT) как конец файла.

Чтобы скрыть обнаружение, некоторые вирусы применяют довольно хитрые приемы маскировки.

"Невидимые" вирусы.  Многие  резидентные  вирусы  (и файловые, и загрузочные) предотвращают свое обнаружение тем, что  перехватывают обращения  DOS (и тем самым прикладных программ) к зараженным файлам и областям диска и выдают их в исходном (незараженном) виде. Разумеется, этот  эффект наблюдается  только на  зараженном компьютере - на "чистом" компьютере  изменения  в файлах и  загрузочных областях диска можно легко обнаружить.

Самомодифицирующиеся вирусы. Другой способ, применяемый  вирусами  для  того, чтобы укрыться от  обнаружения, - модификация своего тела. Многие  вирусы хранят большую часть своего тела в закодированном виде, чтобы с помощью  дизассемблеров нельзя было разобраться в механизме их работы. Самомодифицирующиеся вирусы используют этот прием и часто меняют параметры этой кодировки, а кроме того, изменяют и свою стартовую часть, которая служит для раскодировки остальных команд  вируса. Таким образом, в теле подобного вируса не имеется ни одной  постоянной цепочки байтов, по которой можно было бы идентифицировать  вирус. Это, естественно, затрудняет нахождение таких вирусов программами-детекторами.

**Лекция 10. Методы защиты программ от разрушающих программных воздействий и сетевая безопасность**

Цель лекции: изучение основных характеристик антивирусных защит.

Содержание:

а) методы защиты от компьютерных вирусов;

б) защита информации в Интернете;

в) защита от несанкционированного доступа.

Каким бы ни был вирус, пользователю необходимо знать  основные  методы защиты от компьютерных вирусов.

Для защиты от вирусов можно использовать:

1)     общие средства защиты информации, которые полезны так же и как страховка от порчи носителей, неправильно работающих программ или ошибочных действий пользователя;

2)     профилактические меры, позволяющие уменьшить вероятность  заражения вирусов;

3)     специальные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих средств:

1)     копирование информации - создание копий  файлов  и  системных  областей диска;

2)     средства разграничения доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных  вирусами, неправильно работающими программами и ошибочными действиями пользователя.

Общие средства защиты информации  очень важны  для защиты от вирусов, все же их недостаточно.

Необходимо и применение  специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

Детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее  сообщение.

Следует подчеркнуть, что программы-детекторы могут обнаруживать только те вирусы, которые ей "известны". Программа Scan McAfee Associates и Aidstest позволяют обнаруживать всего несколько тысяч вирусов, но всего их более 80 тысяч! Некоторые программы-детекторы, например, Norton AntiVirus или AVSP, могут настраивать на новые типы вирусов, им необходимо лишь  указать комбинации байтов, присущие этим вирусам. Тем не менее, невозможно разработать такую программу, которая могла бы обнаруживать любой заранее неизвестный вирус.

Многие программы-детекторы (в том числе и Aidstest) не умеют обнаруживать заражение "невидимыми" вирусами, если такой вирус активен в памяти компьютера. Дело в том, что для чтения диска они используют функции DOS, перехватываются вирусом, который говорит, что все хорошо. Правда, Aidstest  и др. программы могут выявить вирус путем просмотра оперативной памяти, но  против  некоторых "хитрых" вирусов это не помогает.

Большинство программ-детекторов имеют функцию "доктора",  т.е. пытаются вернуть зараженные файлы или области диска в их исходное состояние. Те файлы, которые не удалось восстановить, как правило, делаются неработоспособными или удаляются.

Большинство программ-докторов умеют "лечить" только от некоторого  фиксированного набора вирусов, поэтому они быстро устаревают. Но некоторые программы могут обучаться не только способам обнаружения, но и способам лечения  новых  вирусов.

Программы-ревизоры имеют две стадии работы. Сначала они запоминают сведения о состоянии программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения жесткого диска).  Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей  дисков  с исходным. О выявленных несоответствиях сообщается пользователю.

Многие программы-ревизоры являются довольно "интеллектуальными" -  они  могут отличать изменения в файлах, вызванные, например, переходом к новой версии  программы, от изменений, вносимых вирусом, и не  поднимают ложной  тревоги.

Для проверки того, не изменился ли  файл, некоторые  программы-ревизоры  проверяют длину файла. Но эта проверка недостаточна - некоторые вирусы не  изменяют длину зараженных файлов. Более надежная проверка - прочесть  весь  файл и вычислить его контрольную сумму. Изменить файл так, чтобы его контрольная сумма осталась прежней, практически невозможно.

**Защита информации в Интернете**

Для предотвращения несанкционированного доступа к своим компьютерам все корпоративные и ведомственные сети, а также предприятия, использующие технологию intranet, ставят фильтры (fire-wall) между внутренней сетью и Internet, что фактически означает выход из единого адресного пространства. Еще большую безопасность даст отход от протокола TCP/IP и доступ в Internet через шлюзы.

Этот переход можно осуществлять одновременно с процессом построения всемирной информационной сети общего пользования, на базе использования сетевых компьютеров, которые с помощью сетевой карты и кабельного модема обеспечивают высокоскоростной доступ к локальному Web-серверу через сеть кабельного телевидения.

Для решения этих и других вопросов при переходе к новой архитектуре Internet нужно предусмотреть следующее:

1)     Ликвидировать физическую связь между будущей Internet  и корпоративными и ведомственными сетями, сохранив между ними лишь информационную связь через систему World Wide Web.

2)     Заменить маршрутизаторы на коммутаторы, исключив обработку в узлах IP-протокола и заменив его на режим трансляции кадров Ethernet, при котором процесс коммутации сводится к простой операции сравнения MAC-адресов.

3)     Перейти в новое единое адресное пространство на базе физических адресов доступа к среде передачи (MAC-уровень), привязанное к географическому расположению сети и позволяющее в рамках 48-бит создать адреса для более чем 64 триллионов независимых узлов.

Одним из наиболее распространенных механизмов защиты от интернетовских бандитов - “хакеров” является применение межсетевых экранов - брандмауэров**(**firewalls**).**

Несмотря на кажущийся правовой хаос в рассматриваемой области, любая деятельность по разработке, продаже и использованию средств защиты информации регулируется множеством законодательных и нормативных документов, а все используемые системы подлежат обязательной сертификации Государственной Технической Комиссией при президенте Казахстана.

Известно, что алгоритмы защиты информации (прежде всего шифрования) можно реализовать как программным, так и аппаратным методом.

**Лекция 11. Методы защиты информации в канале связи**

Цель лекции: произвести анализ вариантов угроз информации в канале связи.

Содержание:

а) сигнализация на абонентском участке сети;

б) защита от несанкционированного доступа.

Среди всего многообразия способов несанкционированного перехвата информации особое место занимает анализ трафика в сети доступа, поскольку сеть доступа - самый первый и самый удобный источник связи между абонентами в реальном масштабе времени, и при этом самый незащищенный.

Сеть доступа имеет еще один недостаток с точки зрения безопасности - возможность перехвата речевой информации из помещений, по которым проходит телефонная линия и где подключен телефонный аппарат (далее оконечное оборудование (ОО)), даже тогда, когда не ведутся телефонные переговоры. Для такого перехвата существует специальное оборудование, которое подключается к телефонной линии внутри контролируемого помещения или даже за его пределами. Требования к оборудованию противодействия данных угрозам описывают НД ТЗІ 2.3-002-2001, НД ТЗІ 2.3-003-2001, НД ТЗІ 4.7-001-2001 и некоторые другие нормативные документы.

В общем случае от ОО к АТС и обратно передаются:

-       сигналы управления и сигнализации стандартного оборудования (ТА, модем и т.д.);

-       сигналы передачи данных, речь;

-       сигналы сигнализации и управления нестандартного оборудования (охранная, пожарная сигнализация и др.).

**Методы защиты информации в канале связи**

Методы защиты информации в канале связи можно разделить на две группы:

-       основанные на ограничении физического доступа к линии и аппаратуре связи;

-       основанные на преобразовании сигналов в линии к форме, исключающей (затрудняющей) для злоумышленника восприятие или искажение содержания передачи.

Методы первой группы в основном находят применение в системах правительственной связи, где осуществляется контроль доступа к среде передачи данных.

Методы второй группы направлены на обратимое изменение формы представления передаваемой информации. Преобразование должно придавать информации вид, исключающий ее восприятие при использовании аппаратуры, стандартной для данного канала связи. При использовании же специальной аппаратуры восстановление исходного вида информации должно требовать затрат времени и средств, которые, по оценке владельца защищаемой информации, делают бессмысленным для злоумышленника вмешательство в информационный процесс.

При защите обмена данными решающее значение имеет форма представления сигнала в канале связи.

Следует учесть, что деление на "аналоговый" или "цифровой" сигнал условно. Для некоторых вариантов механизмов защиты информации требуется взаимная синхронизация и обмен служебными посылками между взаимодействующей аппаратурой защиты, т.е. присутствует цифровой режим, однако, поскольку этот режим не связан непосредственно с речевым обменом, требования к его скоростным характеристикам достаточно свободны.

С другой стороны, символьный (цифровой) обмен в протяженных каналах всегда осуществляется через модемное преобразование в виде аналогового сигнала.

Попробуем провести краткий анализ вариантов угроз информации в канале связи. Для удобства анализа проведем классификацию канала связи по степени защищенности (защиты) передаваемой информации.

Полученные результаты сведем в таблицу 11.1. На рисунках изображены структурные схемы передачи данных для соответствующих каналов на примере взаимодействия ОО (КСЗИ) с АТС и удаленным ОО (КСЗИ).

Таблица 11.1 - Анализ вариантов угроз информации в канале связи

|  |  |
| --- | --- |
| Класс защиты канала связи | Варианты угроз информации |
| Открытый канал | Защита информации основана на ограничении доступа к линии. Возможно несанкционированное подключение к линии. Возможен перехват: при использовании услуги "Междугородная связь по паролю" возможно перехватить этот пароль, так как он передается с помощью DTMF; управляющей информации для/от АТС; всех данных, передаваемых по каналу связи, вне зависимости от используемой технологии передачи; управляющей информации ОО (удаленное управление ОО, сигнализацией и т.д. Особенно небезопасен перехват команд отключения для некоторых видов охранной сигнализации). Возможен перехват/модификация трафика и его полный анализ. |

*Окончание таблицы 11.1*

|  |  |
| --- | --- |
| Полузакрытый канал (закрывается только информация, управляющая информация передается в открытом виде). | Защита информации основана как на ограничении доступа к линии, так и на КЗИ. Данные закрываются с использованием КСЗИ (по ГОСТ 28147-89 в любом режиме). Возможно несанкционированное подключение к линии. Возможен перехват: при использовании услуги "Междугородная связь по паролю" также возможно перехватить этот пароль (если он набирался в открытом режиме); управляющей информации для/от АТС; момента установления защищенного соединения (возможен перехват ключей); открытых данных/разговора. Возможен перехват трафика но анализ только управляющей информации и открытых данных (опять проблема перехвата команд отключения систем охранной сигнализации). |

Структурная схема передачи данных в открытом канале показана на рисунке 11.1.

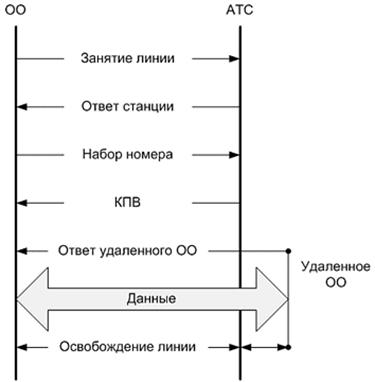


Рисунок 11.1 - Передача данных в открытом канале данных



А2 - алгоритм 2; К2 - ключ алгоритма А2.

Рисунок 11.2 - Передача данных в полузакрытом канале данных

Основная проблема, с которой сталкиваются пользователи сетей, где применяется сквозное шифрование, связана с тем, что служебная информация, используемая для установления соединения, передается по сети в незашифрованном виде.

По сравнению с канальным, сквозное шифрование характеризуется более сложной работой с ключами, поскольку каждая пара пользователей должна быть снабжена одинаковыми ключами, прежде чем они смогут связаться друг с другом. А поскольку криптографический алгоритм реализуется на верхних уровнях модели OSI, приходится также сталкиваться со многими существенными различиями в коммуникационных протоколах и интерфейсах сети доступа (для примера: отправитель - канал ТЧ, получатель - 2B+D). Все это затрудняет практическое применение сквозного шифрования.

Приведенные выше методы защиты информации уже не удовлетворяют современным требованиям. При использовании этих методов злоумышленник может перехватывать адресную информацию, вести мониторинг передаваемых данных, несанкционированно подключаться к линии, искажать передаваемую информацию.

Единственным возможным методом, удовлетворяющим всем современным требованиям, является использование комбинации канального и сквозного шифрования. При этом может закрываться вся передаваемая по каналу связи информация.

Комбинация канального и сквозного шифрования данных в сети доступа обходится значительно дороже, чем каждое из них по отдельности. Однако именно такой подход позволяет наилучшим образом защитить данные, передаваемые по сети. Шифрование в каждом канале связи не позволяет злоумышленнику анализировать служебную информацию, используемую для маршрутизации. А сквозное шифрование уменьшает вероятность доступа к незашифрованным данным в узлах сети.

Структурная схема передачи данных в закрытом канале показана на рисунке 11.3.

Кратко опишем механизм взаимодействия КСЗИ и АТС (удаленной КСЗИ) в предложенном методе.

При занятии линии (получении сигнала вызова от АТС) происходит автоматический переход в закрытый режим связи (А1, К1). После перехода в закрытый режим абонентский комплект (АК) или криптографический модуль перед АК АТС аутентифицирует КСЗИ. Данный шаг необходим для устранения возможности несанкционированного использования линии. После проведения аутентификации возможен выход из закрытого режима.

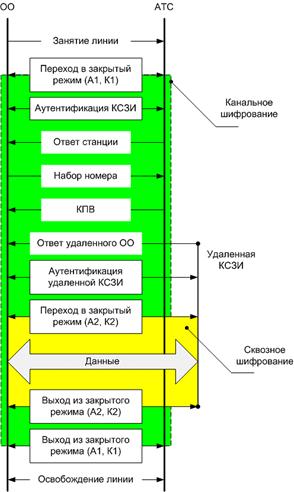
При вызове со стороны вызывающего абонента АТС принимает адресную информацию, устанавливает соединение.

При ответе удаленной КСЗИ возможны два варианта: аутентификации удаленной КСЗИ и переход в закрытый режим (А2, К2) либо переход в закрытый режим (А2, К2) и аутентификация удаленной КСЗИ.

Аутентификация удаленной КСЗИ необходима для противодействия атаке, при которой удаленная КСЗИ злоумышленника при помощи перекоммутации выдает себя за КСЗИ легального пользователя.

После удачной аутентификации удаленной КСЗИ также возможен выход из защищенного режима (отказ от вхождение в защищенный режим).

Также при передаче данных необходимо проводить т.н. проверку обратного кода. Проверка обратного кода представляет собой процедуру защиты, осуществляемую в процессе передачи данных. Заключается в том, что у удаленной КСЗИ периодически запрашивается идентифицирующая информация, которая и называется обратным кодом. Эта информация сравнивается с эталонной, сохраненной при аутентификации в начале сеанса связи. При несовпадении кодов передача блокируется. Проверкой обратного кода можно обнаружить факт изменения (перекоммутации) направлений выдачи данных или злоумышленного использования приемного устройства зарегистрированного (законного) корреспондента.



А1 - алгоритм 1, К1 - ключ алгоритма А1;

А2 - алгоритм 2, К2 - ключ алгоритма А2.

Рисунок 11.3 - Передача данных в закрытом канале данных

(закрываются все данные)

**Лекция 12. Организация защиты речевой информации, обрабатываемой техническими средствами**

Цель лекции: ознакомить с защитой информации, обрабатываемой техническими средствами.

Содержание:

а) физическая сущность «микрофонного эффекта»;

б) воздушные и вибрационные технические каналы утечки информации.

При работе некоторых технических средств, наряду с электромагнитными полями «рассеяния», возникают информативные акустические, виброакустические, гидроакустические и акустоэлектрические поля (сигналы); при телефонном разговоре - электросигнал в линии и различные наводки и влияния; при радиотелефонном разговоре появляется электромагнитный сигнал.

Акустическая энергия, возникающая при разговоре, может вызвать акустические (механические) колебания элементов электронной аппаратуры, что приводит к появлению электромагнитного излучения или к его изменению при определенных обстоятельствах. Наиболее чувствительными элементами радиоэлектронной аппаратуры к акустическим воздействиям являются катушки индуктивности и конденсаторы переменной емкости.

К электромагнитным преобразователям относятся такие устройства, как громкоговорители, электрические звонки (в т.ч. и вызывные электрические звонки телефонных аппаратов), электрорадиоизмерительные приборы.

Примером непосредственного использования этого эффекта для целей акустического преобразования является электродинамический микрофон (см. рисунок 12.1). ЭДС на выходе катушки определяется по формуле:



где *L* = 4kpm0w2S/*l*- индуктивность;

k - коэффициент, зависящий от соотношения параметров;

*l* -длина намотки катушки;

m0 - магнитная проницаемость;

S - площадь поперечного сечения катушки;

w- число витков катушки.

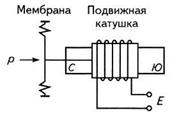


Рисунок 12.1- Электродинамический микрофон

Возникновение ЭДС на выходе такого преобразователя принято называть «микрофонным эффектом». Таким образом, микрофонный эффект - появление в цепях радиоэлектронной аппаратуры посторонних (паразитных) электрических сигналов, обусловленных механическим воздействием, в том числе давлением звуковой волны. Микрофонный эффект может проявляться как в электродинамической, так и в электромагнитной, конденсаторной и других конструкциях, широко используется в микрофонах различного назначения и исполнения (в т.ч. специальных). Каналы утечки информации, формируемые на основе «микрофонного эффекта», называются каналами за счет электроакустических преобразований, так как для их образования необходимо преобразование механических колебаний в электрические сигналы. Элементы, в которых осуществляется указанное преобразование, называются электроакустическими преобразователями.

**Воздушные и вибрационные технические каналы утечки информации**

Воздушные и вибрационные технические каналы утечки информации разведываются с помощью специальных и узконаправленных микрофонов. В воздушных ТКУИ средой распространения информационных сигналов является воздушная среда. Для их перехвата используются как скрытые проводные линии связи, оборудованные миниатюрными высокочувствительными микрофонами, так и специальные узконаправленные микрофоны. С помощью таких микрофонов можно прослушать разговор на расстоянии до 1 км в пределах прямой видимости.

Простой направленный микрофон представляет собой набор из семи алюминиевых трубок диаметром до 10 мм. Длина трубок определяет резонансную частоту звукового сигнала. Микрофон располагается в параболическом улавливателе. Усиление перехваченного сигнала осуществляется микрофонным усилителем. Этот направленный микрофон перекрывает весь спектр звуковых (речевых) колебаний (300...3300 Гц). Расширение диапазона принимаемых частот в целях обеспечения высокого качества принимаемых речевых сигналов осуществляется за счет увеличения числа резонансных трубок и изменения их длины, для чего производятся специальные инженерные расчеты (система из 37 трубок, например, обеспечивает перекрытие диапазона от 180 до 8200 Гц).

В вибрационных ТКУИ средой распространения акустических сигналов являются конструкции зданий, сооружений, трубы водоснабжения, системы отопления, канализации и другие твердые тела и поверхности. Для перехвата акустических колебаний в этом случае используются контактные микрофоны (стетоскопы). Контактные микрофоны, соединенные с электронным усилителем, называют электронными стетоскопами.

**Технические закладные устройства**

Технические закладные устройства (ТЗУ) представляют собой малогабаритные приборы (до размеров булавочной головки), предназначенные для сбора и передачи на достаточно большие расстояния (от нескольких сотен до нескольких тысяч метров) как информации, обрабатываемой, передаваемой и т.п. с помощью технических средств (аппаратурные закладки), так и речевой информации (радиомикрофоны).

По диапазону работы ТЗУ делятся на:

- радиозакладки, работающие в радиодиапазоне;

- ИК- закладки, работающие в инфракрасной части спектра.

По среде, служащей для передачи собранной информации (либо передаваемой в режиме реального времени), радиозакладки делятся на две группы:

- работающие по радиоэфиру;

- работающие по линиям связи, сетям электроснабжения и другим токопроводящим металлическим протяженным конструкциям.

Наиболее часто используемый диапазон радиозакладок первой группы 20...25; 130...174; 350...512 Мгц. Вторая группа закладок работает в диапазоне 500...300 кГц.

По конструктивному исполнению и тактическому использованию радиозакладки подразделяются на:

- телефонные (устанавливаются непосредственно в телефонах);

-микрофонные (акустическое прослушивание разговоров в помещениях).

*Радиомикрофон* - это микрофон, объединенный с радиоканалом передачи звуковой (акустической, речевой) информации. Иногда их называют как радиозакладками, радиокапсулами, иногда - «жучками» (самое точное - радиомикрофон). Популярность их обусловливается простотой и удобством оперативного применения.

В самом простом случае радиомикрофон состоит из собственно микрофона, определяющего зону акустической чувствительности ТЗУ (20...30 м) радиопередатчика, определяющего дальность его действия, скрытность работы и излучающего в пространство несущую частоту, промодулированную электрическими сигналами с микрофона. Существенное влияние на длину радиоканала оказывает тип радиоприемного устройства. В состав ТЗУ может входить устройство записи и управляющее устройство (для включения по началу разговора, голосу, режиму передачи - либо в реальном масштабе времени, либо импульсной, регулировке несущей частоты и др.).

Некоторые аппаратурные ТЗУ предназначены не для создания ТКУИ, а для уничтожения, искажения обрабатываемой, передаваемой, принимаемой, отображаемой и т.п. информации и программного обеспечения ЭВМ, а также для уничтожения отдельных узлов и плат этих устройств.

*Лазерные подслушивающие устройства*. Лазерный (один из оптико-электронных каналов) канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол, окон, картин, зеркал). Разведывательный луч лазера, попадая на вибрирующий объект разведки, модулируется по амплитуде и фазе (по закону вибрации разведываемой поверхности), отражается и в видоизмененной форме (диффузной или зеркальной) принимается приемником лазерного излучения, при демодуляции возвращенного луча выделяется речевая информация.

Лазерные подслушивающие устройства («лазерные микрофоны») являются сложными техническими системами, работающими по принципу локации, как правило, в ближнем ИК-диапазоне волн. Дальность действия таких систем составляет сотни метров.

**Лекция 13. Средства обнаружения каналов утечки информации**

Цель лекции: представление возможных вариантов прямого подключения  к телефонным и телеграфным линиям.

Содержание:

а) контактное подключение телефонного аппарата;

б) индуктивный съем информации с телефонной линии.

**Прямое подключение к телефонным и телеграфным линиям**

Самый простой способ - параллельное подключение телефонного аппарата (контактное). Контактное подключение в техническом плане легко обнаруживается, вследствие падения напряжения в линии (отбора мощности сигнала) и ухудшения слышимости в основном аппарате.

Более совершенными способами являются варианты контактного подключения к линиям связи с помощью согласующего устройства или с компенсацией падающего питающего напряжения.

Подслушивающая аппаратура и согласующее устройство (компенсирующий источник напряжения) при этих способах подключаются параллельно (см. рисунки 13.1 и 13.2).

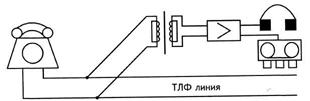


Рисунок 13.1- Подключение к телефонной линии с помощью согласующего устройства

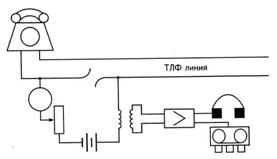


Рисунок 13.2- Подключение к телефонной линии с компенсацией напряжения

Бесконтактное подключение к линии связи осуществляется двумя основными способами за счет реализации электромагнитной индукции:

- за счет электромагнитных наводок в рамке, параллельно приложенной к проводам;

- с помощью сосредоточенной индуктивности, охватывающей контролируемую линию.

На рисунке 13.3 представлена двухпроводная телефонная линия с разнесенными проводами, в параллельных проводах которой индуцируется ЭДС, где*I*1, *I*2 - токи в двухпроводной телефонной линии, *d1, d2, d3, d4* - расстояния между рамкой и проводами подслушиваемой линии.

Токи *I*1 и *I*2 индуктируют в рамке токи противоположного направления. В рамке циркулирует ток *I*, равный разности токов, и который, попадая в усилитель поста подслушивания, усиливается и поступает на головные телефоны и магнитофон. ЭДС, наведенная в рамке, будет тем больше, чем больше активная длина рамки *l*, чем больше разнос проводов двухпроводной линии и чем ближе к линии находится рамка.

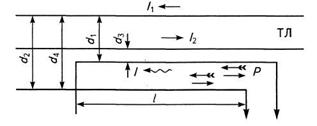


Рисунок 13.3- Подслушивание двухпроводной линии на рамку

**Индуктивный съем информации с телефонной линии**

В арсенале способов прослушивания телефонных линий имеется классический способ индуктивного съема информации с телефонной линии, который обнаружить техническими средствами практически невозможно (см. рисунок 14.4).

Два провода телефонного кабеля отделяются один от другого, и на один из них надевается магнитопровод датчика. В целях сохранения целостности линии магнитопровод исполняется из двух разделяющихся частей, которые соединяются при установке. Во время разговора по телефонным проводам течет переменный электрический ток *I*, пропорциональный звуковому давлению (звуку), который создает разговор абонентов. Этот ток одинаков для каждой жилы телефонного провода, но направлен в противоположные стороны. Вокруг каждой из жил телефонной линии возникает переменное магнитное поле, пропорциональное изменениям переменного тока.

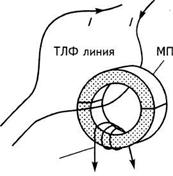


Рисунок 13.4- Принцип работы индуктивного датчика

Магнитное поле от жилы, охваченной магнитопроводом МП, создает в нем переменный магнитный поток, наводящий ЭДС в катушке *К*, намотанной на одну из половинок магнитопровода. Таким образом, на концах катушки возникает напряжение, изменяющееся вместе со звуковыми колебаниями. Далее оно усиливается и подается на вход радиопередатчика, диктофона или другого оконечного устройства.

Существуют способы подавления телефонных закладок, но если индуктивный датчик установлен по типу (см. рисунок 13.5), то он аппаратно не обнаруживаем и не подавляем (если не скремблерами).

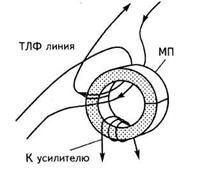


Рисунок 13.5- Способ установки индуктивного датчика, исключающий подавление синфазной помехой

Контактное и бесконтактное подключение возможно и к ВОЛС. Для контактного подключения удаляют защитные слои кабеля, стравливают в светоотражающую оболочку и изгибают кабель на необходимый угол (см. рисунок 13.6, а). В данном случае обнаружить подключение за счет утечки (ослабления мощности сигнала) очень сложно, так как достаточно отобрать 0,001% передаваемой мощности, чтобы подслушать переговоры.

Принципиальная схема бесконтактного подключения к ВОЛС реализуется, как правило, либо в период монтажа ВОЛС, либо демонтажа и ремонта аппаратуры, так как в качестве элемента съема светового информационного сигнала используется стеклянная трубка жестко фиксированная на предварительно зачищенном кабеле, запаянная с двух сторон и имеющая изогнутый отвод, на конце которого устанавливается объектив, фокусирующий световой поток на светодиод, электрический сигнал с которого подается на усилитель и оконечное устройство приема (см. рисунок 9.6, б)



а – контактное подключение, б – бесконтактное подключение.

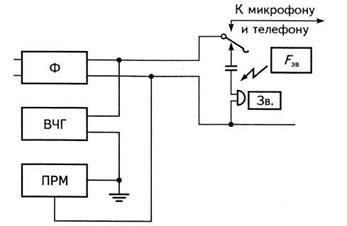
Рисунок 13.6- Варианты подключения к ВОЛС

**Высокочастотное навязывание**

Эффект «навязывания» заключается в подаче в телефонную линию в сторону приемного аппарата (специального подслушивающего устройства) разведывательного сигнала ВЧ, НЧ генератора (передатчика) с частотой 150 кГц и выше на один провод телефонной линии, ко второму проводу подключается вход приемника. Земля передатчика и приемника соединены между собой или с общей землей, например, водопроводной сетью.

Эти колебания за счет нелинейности элементов телефонного аппарата модулируются речевыми сигналами при разговоре при поднятой телефонной трубке или ЭДС микрофонного эффекта звонка (при положенной телефонной трубке). Суммарный (звуковой и ВЧ- разведывательный) сигнал является сложным сигналом, изменяющимся по закону речевых колебаний. В результате получим квазителефонную  радиозакладку, в которой и передатчик и приемник вынесены за пределы контролируемой зоны, а нелинейность телефонного аппарата выполняет роль модулятора. Суммарный сигнал детектором приемника преобразуется в речевой информативный.

Наиболее часто такой канал утечки информации используется для перехвата разговоров в закрытых служебных помещениях, где имеются телефонные аппараты с выходами за пределы контролируемой зоны



ВЧГ - ВЧ-генератор (передатчик); ПРМ - приемник; Ф - фильтр; Зв. – звонок.

Рисунок 13.7- Схема прослушивания на эффекте «навязывания»

**Лекция 14. Методы защиты информации от утечки по техническим каналам**

Цель лекции: представление возможных вариантов прямого подключения  к телефонным и телеграфным линиям.

Содержание:

а) основные стандарты защиты информации по техническим каналам;

б) классификация методов защиты;

в) методы выявления устройств перехвата информации.

В Республике Казахстан методы защиты информации от утечки по техническим каналам  стандартизованы. Отдельно выделяют защиту информации в служебных помещениях и средств вычислительной техники. В первом случае используют требования СТ РК 1700-2007 «Техническая защита информации в служебных помещениях. Общие технические требования», а во втором - СТ РК 1698-2007 «Защита информации от технических разведок и от ее утечки по техническим каналам на объекте средств вычислительной техники. Методы защиты».

**Классификация методов защиты**

Защита секретной информации, обрабатываемой на объекте с использованием средств вычислительной техники (СВТ), от утечки по техническим каналам должна обеспечиваться применением:

- организационных мероприятий;

- технических мероприятий.

Организационные мероприятия – это методы защиты, которые не требуют применения технических средств защиты информации.

К организационным мероприятиям по защите информации от утечки по техническим каналам относятся:

- категорирование объекта СВТ;

- установление контролируемой зоны объекта СВТ;

- разработка технического задания на объект СВТ с учетом требований по защите информации;

- организация и проведение проектных работ по созданию (модернизации) объекта СВТ с учетом требований по защите информации;

- организация режима секретности на объекте СВТ;

- организация подразделения по защите информации;

- обучение лиц, эксплуатирующих технические средства обработки информации, и пользователей правилам применения и эксплуатации средств защиты информации, обеспечения безопасности защищаемой информации;

- контроль реализации мероприятий по защите информации, разработанных на этапах проектирования и принятых для внедрения на объекте СВТ;

- аттестация объектов СВТ по требованиям безопасности информации.

Технические мероприятия по защите объекта СВТ – это методы, предусматривающие применение технических средств защиты информации, а также реализацию технических решений.

Технические методы подразделяются на:

- активные;

- пассивные;

- методы криптозащиты (СТ РК 1073);

- методы выявления устройств перехвата информации.

Активные методы защиты информации подразделяются на:

- энергетические методы;

- неэнергетические методы (статистические или имитации).

В свою очередь энергетические методы включают:

- методы зашумления;

- методы изменения параметров среды распространения сигналов.

Пассивные методы защиты информации подразделяются на:

- экранирование;

- фильтрацию;

- развязку.

Методы выявления устройств перехвата информации подразделяются на:

- методы радиоконтроля помещений;

- методы поиска неизлучающих ТЗУ;

- методы подавления ТЗУ.

К активным методам относятся энергетические методы

Методы зашумления и изменения параметров среды распространения относятся к энергетическим методам.

*Метод зашумления.* Сущность метода заключается в излучении (вводе в линию) широкополосного сигнала с уровнем энергетического спектра, превышающим максимальный уровень ПЭМИ технических средств обработки информации объекта СВТ.

*Метод изменения параметров среды распространения.* Сущность метода заключается в изменении параметров среды распространения (рассеивания) сигналов ПЭМИН (емкость линии, волновое сопротивление линии, характеристики пассивных отражателей в помещении). Это приводит к изменению уровня ПЭМИН, ухудшению соотношения сигнал/шум на входе приемных устройств средств технической разведки.

**Неэнергетические методы**

К неэнергетическим методам относят методы, реализуемые за счет применения имитаторов сигналов. Имитаторы сигналов предназначены для создания маскирующих помех в пространстве или в линиях с целью защиты информации, обрабатываемой на технических средствах обработки информации. Метод имитации может применяться для защиты информации от утечки за счет излучений и в оптическом диапазоне.

**Пассивные методы**

*Экранирование.*Метод предназначен для обеспечения требуемого ослабления ПЭМИН за пределами контролируемой зоны.

Различают экранирование по уровню:

- экранирование зданий;

- экранирование помещений или размещение в экранированной камере;

- экранирование технических средств обработки информации объекта СВТ или рабочих мест;

- экранирование отдельных блоков или отдельных излучающих элементов (узлов) технических средств обработки информации объекта СВТ;

- экранирование кабельных линий.

Выбор числа уровней экранирования осуществляется с учетом:

- характеристик ПЭМИ (тип, частота, мощность);

- наличия или отсутствия других методов экранирования ПЭМИН;

- минимизации затрат на экранирование.

Показателем эффективности экранирования является значение коэффициента экранирования (подавления) ПЭМИН технических средств обработки информации  объекта СВТ в заданном диапазоне частот за счет применения экранирующих конструкций.

При создании экранированных помещений необходимо решать вопросы обеспечения их вентиляцией, вводом в эти помещения цепей электропитания и информационных линий.

*Метод фильтрации.*Метод предназначен для ослабления наводок ПЭМИ технических средств обработки информации объекта СВТ в цепях электропитания и иных проводных линиях, выходящих за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средствами технической разведки на фоне шумов. Метод фильтрации реализуется применением помехоподавляющих фильтров.

Назначение фильтров помехоподавляющих (ФП): подавлять (ослаблять) сигналы (наводки) с частотами, лежащими за пределами рабочей полосы частот и пропускать без значительного ослабления сигналы с частотами, лежащими в пределах этой полосы. Для исключения попадания информационных сигналов – наводок ПЭМИ в цепи электропитания технических средств обработки информации применяются фильтры нижних частот.

*Метод развязывания электрических сигналов.*Метод предназначен для исключения (ослабления) проникновения сигналов наводок в цепях электропитания, выходящих за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средствами технической разведки.

Метод развязывания реализуется путем применения:

- разделительных трансформаторов;

- двигателей - генераторов;

- агрегатов (источников) бесперебойного питания;

- диэлектрических вставок в инженерные коммуникации и экраны кабелей;

- выполнением требований по разносу технических средств обработки информации и вспомогательных технических средств (ВТС), а также норм по разносу и параллельному пробегу информационных кабелей относительно посторонних проводников (кабелей).

**Методы выявления устройств перехвата информации**

Методы борьбы с устройствами перехвата информации (ТЗУ) включают:

 - методы радиоконтроля помещений;

 - методы поиска неизлучающих устройств;

 - методы подавления ТЗУ.

*Методы радиоконтроля помещений.*Методы радиоконтроля помещений основаны на регистрации излучений радиоэлектронных излучающих ТЗУ с использованием различных средств: индикаторов электромагнитного поля; бытовых приемников; специальных радиоприемников; автоматизированных комплексов. Автоматизированные комплексы позволяют контролировать как пространство, так и линии связи, электропитания, охранной и пожарной сигнализации. Контроль состоит в обнаружении сигналов, излучаемых ТЗУ, определении его координат, измерении характеристик сигналов. Контроль может проводиться одновременно в нескольких помещениях.

*Методы поиска неизлучающих ТЗУ.* Методы поиска неизлучающих ТЗУ включают:

- методы, основанные на анализе и выявлении нештатных сигналов в линиях;

- методы, основанные на выявлении изменений одного или нескольких параметров линии за счет подключения ТЗУ (напряжения, тока, сопротивления, емкости, индуктивности);

- методы, основанные на применении нелинейных локаторов, металлодетекторов, рентгеновских установок;

- методы, основанные на обнаружении пустот в конструкциях зданий с использованием звуковых или ультразвуковых средств, тепловизоров.

*Методы подавления ТЗУ.*Методы подавления ТЗУ основаны на применении средств активного подавления или разрушения ТЗУ:

- метод энергетического подавления основан на применении генераторов помех для подавления ТЗУ в линиях, для пространственного подавления (зашумления) радиозакладок. Средства, реализующие метод зашумления, должны излучать в пространство (вводить в линию) широкополосный сигнал с уровнем энергетического спектра, превышающим максимальный уровень сигнала ТЗУ или с уровнем, достаточным для подавления каналов управления ТЗУ. Ширина полосы частот излучаемой помехи должна быть больше ширины полосы частот ТЗУ или каналов управления ТЗУ;

- метод разрушения ТЗУ путем подачи в линии импульса большой амплитуды. При применении данного метода необходимо предварительно отключить от линии оконечные радиоэлектронные устройства.

**Методы и средства обеспечения безопасности информации**

Препятствие*—*метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

Управление доступом*—*методы защиты информации регулированием использования всех ресурсов ИС и ИТ. Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации. Управление доступом включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);

- опознание (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 протоколирования обращений к защищаемым ресурсам;

- реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т.п.) при попытках несанкционированных действий.

Механизмы шифрования*—*криптографическое закрытие информации. Эти методы защиты все шире применяются как при обработке, так и при хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

**Лекция 15. Перспективы и направления развития средств и методов информационной защиты в телекоммуникационных системах**

Цель лекции: представить студентам перспективное развитие средств и методов информационной защиты в ТКС.

Содержание:

а) изменение требований к безопасности;

б) основные типы угроз вычислительным системам.

**Изменение требований к безопасности**

В современных условиях чрезвычайно важным является обоснование требований, создание нормативной базы для установления и контроля   необходимой степени безопасности. Существует ряд международных стандартов в этой области, среди которых можно назвать ISO-7498-2, Оранжевую  книгу и тд. Согласно этим документам безопасность ВС должна поддерживаться средствами, обеспечивающими: управление доступом, идентификацию и  аутентификацию объектов и субъектов, контроль целостности и другие функции защиты. Однако развитие аппаратных и программных  средств ВС, распространение локальных  и глобальных  сетей, а также появление  и эволюция РПС  привели к возрастанию количества видов и способов   осуществления  нарушения  безопасности  и целостности ВС, что создало предпосылки для изменения требований к средствам защиты.

Рассмотрим изменение функций перечисленных средств защиты.

1)   Идентификация и аутентификация. Возникает необходимость  добавления  идентификации и аутентификации удаленных  пользователей и процессов. Причем, поскольку проблема стоит в глобальном масштабе, эти средства должны обеспечивать идентификацию и аутентификацию  объектов и  субъектов, находящихся в разных частях планеты и функционирующих на различных аппаратных платформах и в разных ОС. В настоящий момент такие средства бурно развиваются. В качестве примера можно указать широко известную систему Kerberos и специальные интерфейсы, обеспечивающие  идентификацию и аутентификацию участников взаимодействия типа  GSS-API (Generic Security Service Application Program Interface).

2)   Управление доступом. Поскольку  большинство компьютеров является персональными, разграничение прав локальных пользователей в значительной степени потеряло свою  актуальность. Задача разграничения доступа теперь сводится к ограничению доступа из сети к ресурсам, имеющимся в ВС, и к защите ресурсов, принадлежащих пользователю, но расположенных на удаленных машинах.

3)   Контроль целостности. Понятие контроля целостности теперь должно включать в себя защиту от проникновения в систему злоумышленника или РПС, в том числе через сеть. В защите каналов связи на первое место выступает не шифрование информации с целью защиты от перехвата, а защита сетевого соединения от атаки  со стороны злоумышленника  или РПС. В  качестве примера можно  привести распространенные в  последнее время системы  Firewall, защищающие локальные сети от проникновения в них со стороны Internet.

4)   РПС потребовали от защиты совершенно новой функции, а именно: механизмов, обеспечивающих безопасность и целостность системы в условиях возможного появления в ней программ, содержащих РПС.

**Основные типы угроз вычислительным системам**

Существуют три различных типа угроз, относящиеся к раскрытию, целостности или отказу служб  вычислительной системы.

Угроза раскрытия заключается в том, что информация становится известной тому, кому не следовало бы ее знать. В терминах компьютерной безопасности угроза раскрытия имеет место всякий раз, когда получен доступ к некоторой  секретной информации, хранящейся в вычислительной  системе или передаваемая от одной  системы к другой. Иногда в связи с угрозой раскрытия используется термин “утечка”.

Угроза целостности включает в себя любое умышленное изменение  информации, хранящейся в вычислительной системе или передаваемой из одной  системы в другую. Когда взломщики преднамеренно изменяют  информацию, говорят, что целостность этой информации нарушена. Целостность   также будет нарушена,  если  к несанкционированному изменению  приводит случайная ошибка. Санкционированными  изменениями являются те, которые сделаны определенными  лицами с  обоснованной целью (таким изменением является периодическая запланированная коррекция некоторой базы данных).

Угроза отказа служб возникает всякий раз, когда в результате  преднамеренных действий, предпринятых другим пользователем, умышленно  блокируется доступ к некоторому ресурсу вычислительной системы, то есть, если один пользователь запрашивает доступ к службе, а другой предпринимает что-либо для недопущения этого доступа, мы  говорим, что имеет  место  отказ службы. Реально блокирование  может   быть   постоянным,  так  чтобы запрашиваемый  ресурс никогда не был получен, или оно может вызвать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В таких случаях говорят, что ресурс исчерпан.

Политика безопасности подразумевает множество условий, при которых пользователи системы могут получить доступ к информации и ресурсам. Таким  образом, политика безопасности определяет множество  требований, которые должны быть выполнены в конкретной  реализации системы.

Очевидно, для  проведения желаемой политики безопасности в системе должны присутствовать соответствующие  механизмы. В большинстве случаев механизмы безопасности содержат некоторые автоматизированные компоненты, зачастую являющиеся частью базового вычислительного окружения (операционной системы), с соответствующим множеством   процедур  пользователя и администратора.

Одним из важнейших аспектов проблемы информационной   безопасности компьютерных систем является противодействие РПС. Существуют несколько подходов к решению этой задачи:

- создание специальных программных средств, предназначенных исключительно для поиска и ликвидации конкретных видов РПС (типа антивирусных программ);

- проектирование ВС, архитектура и модель безопасности которых либо в принципе не допускает существование РПС, либо ограничивает область их активности и возможный ущерб;

- создание и применение методов и средств анализа программного обеспечения на предмет наличия в них угроз информационной безопасности ВС и элементов РПС.

Первый подход не может привести к удовлетворительным результатам, т. к. борется только с частными проявлениями сложной проблемы. Второй подход имеет определенные перспективы, но требует серьезной переработки концепции ОС и их безопасности, что связано с огромными затратами. Наиболее эффективным представляется третий подход, позволяющий путем введения обязательной процедуры анализа безопасности программ, достаточно надежно защитить наиболее важные системы от РПС. Процедуру анализа программного обеспечения на предмет наличия в них угроз информационной безопасности ВС называются анализом безопасности  программного обеспечения. Данный подход требует разработки соответствующих теоретических моделей программ, ВС и РПС, создания методов анализа безопасности и методик их применения.

В ближайшее время прогресс в области развития средств вычислительной техники, программного обеспечения и сетевых технологий даст толчок к развитию средств обеспечения безопасности, что потребует во многом пересмотреть существующую научную парадигму информационной безопасности. Основными положениями нового взгляда на безопасность должны являться:

- исследование и анализ причин нарушения безопасности компьютерных систем;

- разработка эффективных моделей безопасности, адекватных современной степени развития программных и аппаратных средств, а также возможностям злоумышленников и РПС;

- создание методов и средств корректного внедрения моделей безопасности в существующие ВС, с возможностью гибкого управления, безопасностью в зависимости от выдвигаемых требований, допустимого риска и расхода ресурсов;

- необходимость разработки средств анализа безопасности компьютерных систем с помощью осуществления тестовых воздействий (атак).

В условиях  современной суверенизации государств и субъектов страны,  продолжающихся военных конфликтов, попыток территориальных, экономических и др. притязаний государств друг к другу, растущей угрозы терроризма в отношении отдельных граждан и государственных  структур особенно остро встали проблемы надежной защиты информации в особые периоды управления  важными  государственными объектами,  включая ВС. Это требует дальнейшего развития теории и практики обеспечения информационной безопасности в  системе МВД РК,  повышения надежности применения современных систем обработки конфиденциальной  информации  в  условиях обострения  информационной  войны  (борьбы).

Широкая информатизация обществ,  внедрение компьютерной технологии в сферу управления объектами  государственного  значения, стремительный  рост темпов научно-технического прогресса наряду с положительными достижениями в информационных технологиях, создают реальные предпосылки для утечки конфиденциальной информации.

В дипломной работе,  основной целью  которой  являлось разработка общих рекомендаций по защите информации в системах обработки данных образовательных учреждений МВД РК и разработка пакета руководящих документов по обеспечению безопасности информации,  получены следующие результаты:

- рассмотрены основные пути защиты от несанкционированного доступа к информации циркулирующей  в системах обработки данных;

- произведена классификация способов и средств защиты информации;

- детально осуществлен анализ методов ЗИ в системах обработки данных;

- рассмотрены основные направления защиты информации в СОД;

- разработаны концепция безопасности локальных вычислительных сетей образовательного учреждения МВД РК и вопросы обеспечения безопасности при групповой обработке данных в службах и подразделениях института;

- осуществлена выработка политики безопасности конкретного образовательного учреждения и дана методика реализации этой политики.

**Заключение**

Проблемы защиты информации в системах электронной обработки данных (СОД) постоянно находятся в центре внимания не только специалистов по разработке и использованию этих систем, но и широкого круга пользователей. Под системами электронной обработки данных понимаются системы любой архитектуры и любого функционального назначения, в которых для обработки информации используются средства электронно-вычислительной техники, а под защитой информации - использование специальных средств, методов и мероприятий с целью предотвращения утери информации, находящейся в СОД. Широкое распространение и повсеместное применение вычислительной техники очень резко повысили уязвимость накапливаемой, хранимой и обрабатываемой с СОД информации.

**Список литературы**

1.      Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. –М.: Гелиос АРВ, 2002. – 480 с.

2.      Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам. –М.: Горячая линия – Телеком, 2005. – 416 с.

3.      Добыкин В.Д., Куприянов А.И., Пономарев В.Г., Шустов Л.Н. радиоэлектронная борьба. Силовое поражение радиоэлектронных систем. –М.: Вузовская книга, 2007. – 468 с.

4.      Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г. Защита информации  в телекоммуникационных системах. – К.:  МК-Пресс, 2005.  – 288 с.

5.      Куприянов А.И., Сахаров А.В. Технические основы радиоэлектронной борьбы. –М.: Вузовская книга, 2007. – 356 с.

6.      Куприянов А.И., Сахаров А.В., Шевцов В.А. основы защиты информации. –М.: Издательский центр «Академия», 2006, -256 с.

7.      Максименко Г. А., Хорошко В. А. Методы выявления, обработки и идентификации сигналов радиозакладных устройств. — К.: Полиграф консалтинг, 2004. - 317 с.

8.      Модели технических разведок и угроз безопасности информации / под ред. Е. М. Сухарева. - М.: Радиотехника, 2003. - 144 с.

9.      Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009. – 576 с.

10. Петраков А. В., Лагутин В. С. Защита абонентского телетрафика. - М.: Радио и связь, 2002. - 504 с.

11. Ратманов Ю. Н. Теоретические основы защиты информации от утечки за счет побочных электромагнитных излучений и наводок. - М.: МПСС, 1985. - 84 с.

12. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. –М.: Горячая линия-Телеком, 2005.- 229 с.

13. Торокин А.А. Инженерно-техническая защита информации. –М.: Гелиос АРБ, 2005. – 960 с.

14. Хорев А. А., Железняк В. К., Макаров Ю. К. Оценка эффективности методов защиты речевой информации. Общесистемные вопросы защиты информации / под ред. Е. М. Сухарева. - М.: Радиотехника, 2003. – 296 с.

15. Чекалин А.А., Стрельцов А.А., Никитин М.М. и др. Комплексный технический контроль эффективности мер безопасности систем управления в органах внутренних дел. Часть 1. Теоретические основы технической разведки и комплексного технического контроля. –М.: Горячая линия-Телеком, 2006.- 296 с.

16. Ярочкин В.И. Информационная безопасность. – М.: Академический Проект; Гаудеамус, 2004. – 544 с.