**Тема №3 Системы с обратной связью.**

*Занятие №2.* **Теоретико-информационная концепция криптозащиты сообщений в телекоммуникационных системах**

*Цель*: Ознакомиться с основными положениями и принципами криптозащиты в ТКС

*План лекции*

|  |  |
| --- | --- |
| № п/п | Учебные вопросы |
| 1 | ВВОДНАЯ ЧАСТЬ |
| 2 | ОСНОВНАЯ ЧАСТЬ   1. Основы криптозащиты информации 2. Методы криптозащиты информации |
| 3 | ЗАКЛЮЧИТЕЛЬНАЯ ЧАСТЬ |

Желание конфиденциально общаться уходит корнями в далекое прошлое. Одним из примеров классического древнего шифра был шифр Цезаря, который использовал Ю.Цезарь во времена его Гальских походов. Он использовал циклический сдвиг алфавита для шифрования важной информации. Другим примером древнего использования шифрования является квадрат Полибиуса, при котором буквы сводились в таблицу 5х5, и каждая шифровалась номером строки и столбца. Так зародилась криптология – наука о защите информации от прочтения ее посторонними. Защита достигается шифрованием, то есть преобразованием сообщения в шифрованную последовательность, из которой невозможно извлечь информацию без знания специального ключа.

Вопросам методам защиты информации и посвящена данная лекция.

**1. Основы криптозащиты информации**

Криптология – наука о защите информации от прочтения ее посторонними лицами.

Криптография - раздел криптологии, который изучает методы защиты информации и проверки ее подлинности.

Криптоанализ – раздел криптологии занимается способами вскрытия алгоритмов шифрования и имитацией сигналов, чтобы они были приняты как подлинные.

Для построения систем связи интерес представляет криптография. В рамках данной лекции будем знакомиться с основами криптографии.

При передаче информации по незащищенной системе связи существуют угрозы для ее безопасности:

1. Перехват данных – несанкционированное подключение к линии связи и счёт информации, или получение информации на дистанции за счёт побочного электромагнитного излучения.
2. Анализ трафика – обзор информации, касающийся связи между пользователями (н-и, наличие или отсутствие, частота, скорость и т. д.), то есть приёмник может получить некоторый объём информации, исходя их характера потока трафика.
3. Отказ пользователя от сообщения – отрицание передающего пользователя своего авторства в предъявленном получателем сообщении или отрицания факта получения сообщения.
4. Изменение потока сообщения – внесение в него искажений, удаление сообщений и т. д.
5. Маскарад – стремление пользователя выдать себя за некоторого другого пользователя с целью получения доступа к каким-либо ресурсам или с другими вредительскими целями.

Для обеспечения зашиты информации создаются системы обеспечения информации (СОБН).

СОБН – это совокупность различных мероприятий (правовых, организационных, технических), позволяет предотвратить или существенно затруднить нанесение ущерба интересам поставщиков и потребителей информации.

Задачи СОБН

1. обеспечение целостности информации
2. сохранение конфиденциальности информации
3. обеспечение доступности пользователям, которые имеют соответствующие полномочия.

Эти задачи решаются с помощью организационно-правовых (инструкции, приказы) и технические методы защиты.

Технические методы защиты стандартизированы МОС и МСЭ-Т и предусматривают основные механизмы защиты:

1. шифрование данных – конфиденциальность
2. обеспечение аутентификации – контроль доступа
3. обеспечение целостности данных – запрет модификации сообщений
4. цифровая подпись – решение вопроса отрицания пользователя от сообщения.

Для реализации технических методов защиты информации создаются криптографическая система.

Криптографическая система – это совокупность технических средств для преобразования открытого сообщения в зашифрованное с помощью ключа (К)

Правило преобразования называется криптоалгоритмом.

Результат шифрования называется криптограммой.

Для управления процессом шифрования используется секретный ключ. стойкость шифра определяется только секретностью ключа.

На приемной стороне реализуется расшифровка – обратное преобразование, при которой восстанавливается исходный текст.

Рассмотрим методы построения криптосистем.

**2. Методы криптозащиты информации**

Различают два класса криптосистем:

- симметричные (одноключевые) – основанные на использовании секретного ключа

- несимметричные (двухключевые) – используют два типа ключа – секретного и открытого.

Шифрование с секретным ключом

Такая криптосистема предполагает только одной единицей секретной информации – ключа, задание которого позволяет отправителю зашифровать информацию, а получателю – расшифровать.



Рис 2.1. Схема шифрования секретным ключом

М – открытое сообщение

Ек – алгоритм обратного преобразования

С=Ек(М) – зашифрованное сообщение

Dк=Ек-1 – обратное преобразование

Математическая модель

Dк= Ек-1[Eк(М)] =М



Схемы шифрования разбиваются на две категории:

- блочное- нешифрованный текст делится на блоки, каждый блок шифруется независимо

- поточное – каждый бит открытого текста шифруется с помощью одного элемента ключа.

Примером алгоритма с секретным ключом является алгоритм DES (Data Encryption Standard). Создан в 1997 году в США Национальным институтом Стандартов и Технологий. В РФ аналогом DES является алгоритм ГОС 28147-89. DES использует блочную систему шифрования.

Объём алфавита системы равен 264 символа.

В алгоритме DES используют 64-х разрядный ключ. Из них 8 бит применяются для исправления ошибок (код с проверкой на четкость). В результате эффективная длина ключа составляет 56 бит.

Алгоритм DES

1. На входе шифрования поступает блок txt=64 бита, происходит начальная перестановка txt
2. Блок txt делится на 2 субблока по 32 бита каждый R1 и R2
3. Первый субблок R1 шифруется ключом К1 и складывается по модулю 2 со вторым субблоком R2

R3(K1)R2= R3



1. Субблок R3 шифруется ключом К2 и складывается с субблоком R1

R3(K2)R1= R4



К2 получается путём циклической перестановки К1.

1. Затем R4 шифруется К3 и складывается по модулю 2 с R2

R4(K3)R2= R5 и т.д.



Таких перестановок всего осуществляется 16.



Рис 2.2. Схема сложения субблоков с ключом К1

Недостатком этого метода шифрования является наличие секретного ключа, что создаёт трудности с хранением, передачей и распределением секретных ключей. Если ключ станет известен криптоаналитику, информация будет дешифрована

В настоящее время используются усовершенствованные алгоритмы на основе стандарта DES. Например, DESede – это «тройной» DES, использующий ключ длиной 168 бит (56 бит3), алгоритм CAST и IPEA.



Однако, и эти алгоритмы не решают вопросы сохранности ключа, от которых зависит защищенность системы, так как один и тот же ключ применяется как для шифрования, так и для дешифрования.

Этот вопрос решается с помощью систем, использующих открытый ключ.

Криптосистемы с открытыми ключами

Используют два разных ключа: один – для шифрования (ОК), другой – для дешифрования (ЗК). При этом требуется, чтобы закрытый ключ (ЗК) было невозможно вычислить по открытому ключу. Поэтому общедоступными являются не только алгоритм шифрования, но и ключ, применяемый для шифрования.

В секрете держатся только ключ дешифрования. Все ключи шифрования содержатся в общедоступном каталоге всех абонентов



Рис 2.3. Схема шифрования с секретным ключом

Особенности криптосистемы с ОК

1. Алгоритмы шифрования Ек и дешифрования Dк являются взаимообратным и определяются ключом К
2. Для каждого ключа алгоритмы Ек и Dк легковычисляемые
3. Для любого К определение Dк из Ек трудноосуществляемо

Криптосистемы с открытыми ключами строятся на основе алгоритмов Ривеста-Шалмера-Адельмана (RSA), ALGamal.

В этих алгоритмах используют одностороннюю функцию – она легко вычисляется, но для неё невозможно вычислить обратную функцию.

Например: y=xab, если известны a и b легко вычислить у. Однако, если a известно, а b – нет, то y – трудновычисляемо.

RSA

Сообщение в схеме RSA представляется как целое из интервала (0, n-1). Каждый пользователь выбирает значение n и пару положительных целых чисел e и d. e и d выбираются по определенному алгоритму.

Пользователь получает свой ключ шифрования, числовую пару (n, e), в общедоступный каталог. Ключ дешифрования держится в секрете – он состоит из числовой пары (n, d). d – секрет.

Выбор e и d связан с произведением: n=pq



Получается, если e и d известны, произведение n=pq легко вычислить, то есть зная e и d становятся известны p и q и наоборот. Однако, если известно только n получить множители p и q затруднительно, а из них ключ дешифрования соответственно тоже трудно вычислить. Если длина каждого множителя p и q 100 разрядов умножение n=pq – доли секунды, а разложение на множители n – миллиарды лет.

