Основы кибербезопасности

Лекция 5.1
Криптографическая защита информации

- 1. История развития криптографии.
- 2. Основные понятия криптографии.
- 3. Симметричные и асимметричные криптосистемы
- 4. Требования к криптосистемам.

Криптографическая защита информации

- ФЗ «О полиции» п.1 статьи 11 в своей деятельности полицейский должен использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру.
- В обязанности современного полицейского входит обеспечение **защиты информации,** содержащейся в банках данных, от **неправомерного и случайного доступа**, уничтожения, копирования, распространения и иных неправомерных действий (ст.17 п.4 ФЗ).

1 вопрос.
История развития криптографии

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.

1 вопрос.
История развития криптографии

Тайна сопровождает всю историю человечества.

Она **была**, **есть** и **будет**.

Криптография по возрасту — ровесник египетских пирамид

- Один из самых старых шифрованных текстов из ***Месопотамии*** представляет собой глиняную табличку, написанную клинописью и содержащую рецепт для изготовления глазури в гончарном производстве (XX в. до н. э..)

Древние египтяне использовали символический язык.

- Так, в 1998 г. был дешифрован текст, записанный на каменных плитах. Этому тексту более 6 000 лет, он получил название ***Великие Арканы Таро***. В нем в символической форме трактуются принципы мироздания, говорится об абсолютной и относительной истине и своеобразно обсуждаются законы диалектики, с которой, как выяснилось, древние египтяне были знакомы.

Начиная с ***личной*** тайны, она переходит в тайны ***семьи***, ***клана, рода*** и так далее.

С образованием государств высшей формой тайны становится тайна ***государственная***.

- Появляются различные виды **тайны**: политическая, военная, дипломатическая, экономическая, ремесленническая, коммерческая, медицинская, криминальная, религиозно-мистическая и так далее.

Если есть тайна, то необходимы и способы ее защиты.

И они, естественно, сразу же появились и стали активно развиваться.

С возникновением специальных разведывательных служб государств деятельность в области обеспечения информационной безопасности государственных структур стала активно опираться на разведывательные органы.

Подкуп, шантаж, кража, внедрение агента и так далее прочно вошли в арсенал средств «информационной войны» государств.

Исторический процесс развития средств и методов защиты тайных посланий выработал ***три основных способа такой защиты.***

Первый способ защиты информации — это ***физическая защита*** от противника материального носителя информации (пергамент, бумага, магнитная лента, физические каналы передачи: проводная линия связи, радиоканал, вибро-акустический канал и так далее).

Одновременно появляются приемы и способы, затрудняющие перехват сообщений.

Главную роль здесь играет выбор канала связи, труднодоступного для перехвата (***ласточки, голуби, специальный курьер, кабельные линии связи, специальные виды радиопередач, волоконно-оптические линии связи и так далее***).

Второй способ защиты информации — Используется для определения метода защиты, основанного на попытке сокрытия от противника самого факта наличия интересующей его информации.

Такую защиту можно было бы осуществить **несколькими** принципиально различными способами.

Во-первых, можно было бы попытаться сделать «невидимым» для противника сам физический носитель информации.

В современных условиях к таким способам относится, например, использование так называемой «микроточки — микрофотографии» (размером в «точку» письменного текста), подклеиваемой под клапан конверта, почтовую марку и так далее. Сюда же относятся исторически древние приемы: ***«запрятывание»*** носителя информации в корешках книг, в каблуках, в пломбе зуба, в медицинских препаратах и так далее.

Во-вторых, можно было бы попытаться поступить таким образом, чтобы противник, даже имея в руках носитель секретной информации, ***саму эту информацию не увидел.***

В этом направлении наибольшее распространение получили так называемые ***симпатические (химические) чернила***. Текст, написанный этими чернилами между строк «невинного» послания, невидим; он проявляется только в результате применения определенной технологии проявления.

В-третьих, на носителе информации, попадающим в руки противника, ***нет ничего, кроме того текста, рисунка, графика и так далее, который он видит.***

Однако истинное секретное сообщение скрывается в буквах, точках рисунка, графика и так далее, стоящих на заранее оговоренных местах «невинного» сообщения.

Третий способ защиты информации — наиболее надежный и распространенный в наши дни — ***криптография***, (в переводе с греческого это слово также означает «тайнопись»). В этом случае в перехваченном сообщении противник ***видит хаотический набор знаков, так что смысл сообщения ему остается неясным.***

Криптографию отождествляли с черной магией.

Так, например, рекомендовалось использовать **«магический квадрат»**

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

16**(У)**	3**(И)**	2**(Р)**	13**(Д)**
5**(З)**	10**(Е)**	11**(Г)**	8**(Ю)**
9**(С)**	6**(Ж)**	7**(А)**	12**(О)**
4**(Е)**	15**(Я)**	14**(Н)**	1**(П)**

После этого шифрованный текст записывается в строку:
УИРДЗЕПОСЖАОЕЯНП

Эволюция криптографической деятельности

- Криптография (в современном понимании этого слова) появилась практически сразу же после появления письменности.
- Мощный импульс ее развитию дало изобретение алфавитной письменности.

Эволюция криптографической деятельности

- Внимание, уделяемое развитию криптографии, зависело от активности деятельности государства в различных сферах: политической, дипломатической, военной, экономической и так далее.
- Криптография выполняла заказы государства и развивалась при его соответствующей поддержке.
- Огромное влияние на развитие криптографии во всей истории ее существования оказывали достижения научно-технического прогресса.

Вопрос о том, что и как защищается (и какой ценой), что и как достается (и какой ценой) — это очень серьезный вопрос.

Один древний мудрец сказал:

«Нельзя ловить рыбу на золотой крючок».

Потеря крючка не окупается стоимостью выловленной рыбы.

Одно из требований, предъявляемое к методам и средствам защиты, — это требование оперативности связи.

- Использование средств защиты не должно существенным образом задерживать передачу сообщения.
- Информация «стареет», и ее получение с большим запозданием может свести все усилия по ее добыванию «на нет».

К проблемам в настоящее время относятся такие, как

- защита от имитации («дезинформации под шифром»),
- идентификация абонентов («электронная подпись»),
- проблема создания различных криптографических протоколов обмена информацией и так далее .

Вопрос 2. Основные понятия криптографии

- Проблемой защиты информации путем ее преобразования занимается **криптология** (kryptos - тайный, logos - 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.

Криптографические функции:

- симметричным шифрованием,
- асимметричным шифрованием
- и односторонними хэш-функциями.

Все существующие технологии аутентификации, целостности и конфиденциальности созданы на основе именно этих трех функций.

Современная криптография включает в себя четыре крупных раздела:

- Симметричные криптосистемы.
- Криптосистемы с открытым ключом.
- Системы электронной подписи.
- 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.

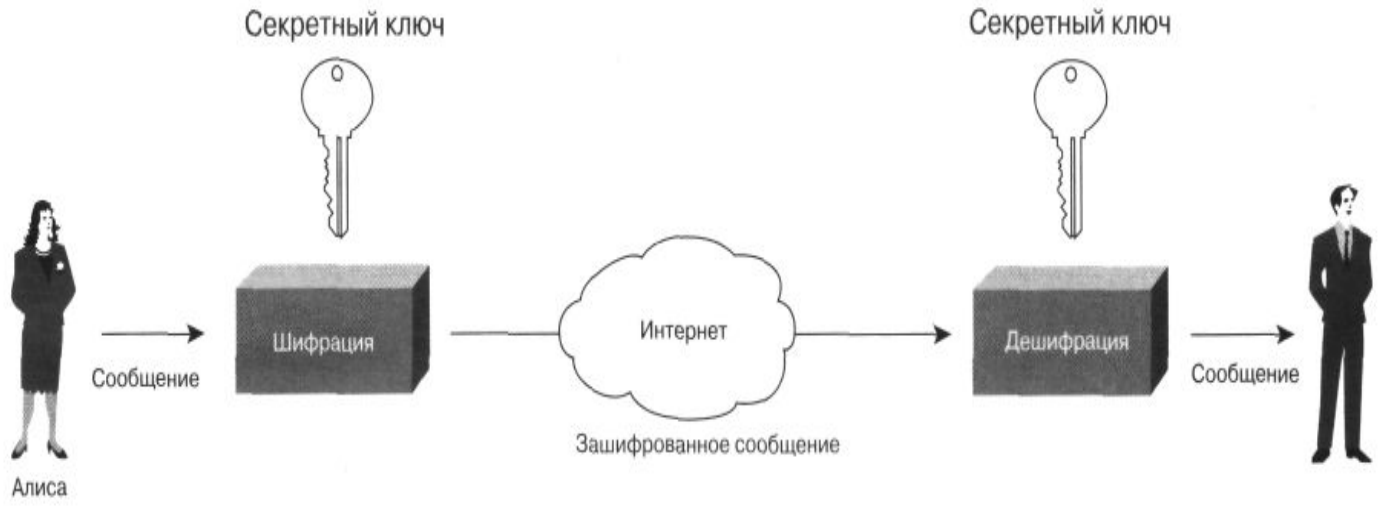
Основные понятия криптографии

- **Алфавит** - конечное множество используемых для кодирования информации знаков.
- **Текст** - упорядоченный набор из элементов алфавита.
- **Шифрование** - преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом.
- **Дешифрование** - обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.
- **Шифр** — это совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты; эти исходные сообщения обычно называются «открытыми текстами».
- **Ключ** - информация, необходимая для беспрепятственного шифрования и дешифрования текстов

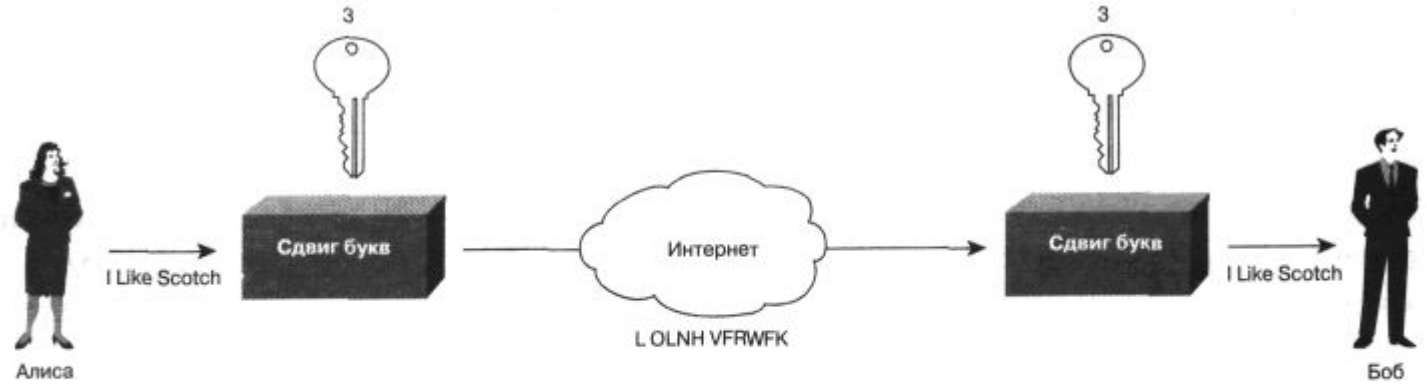
Вопрос 3. Симметричные и асимметричные криптосистемы

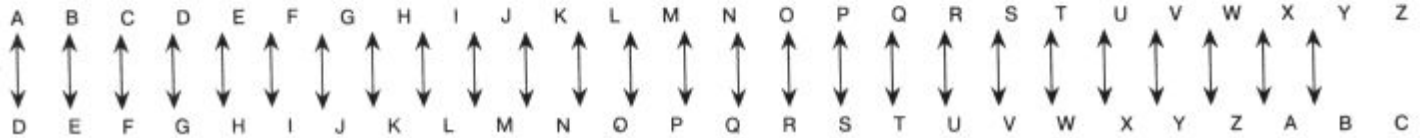
- Симметричное шифрование, которое часто называют шифрованием с помощью секретных ключей, в основном используется для обеспечения конфиденциальности данных.
- Суть их состоит в том, что каждым адресатом информационной системы генерируются два ключа, связанные между собой по определенному правилу.

Симметричные криптосистемы



Шифр Цезаря


3
3
Сдвиг букв
Интернет
Сдвиг букв
I Like Scotch
I Like Scotch
L OLNH VFRWFK
Алиса
Боб


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Сегодня широко используются такие алгоритмы секретных ключей, как Data Encryption Standard (DES), 3DES (или «тройной DES») и International Data Encryption Algorithm (IDEA).

- Эти алгоритмы шифруют сообщения блоками по 64 бита.
- Если объем сообщения превышает 64 бита (как это обычно и бывает), необходимо разбить его на блоки по 64 бита в каждом, а затем каким-то образом свести их воедино.
- Такое объединение, как правило, происходит одним из следующих четырех методов:

1. электронной кодовой книги (ECB),
2. цепочки зашифрованных блоков (CBC),
3. x-битовой зашифрованной обратной связи (CFB-x)
4. или выходной обратной связи (OFB).

С методом секретных ключей связаны следующие *проблемы*:

- Необходимо часто менять секретные ключи, поскольку всегда существует риск их случайного раскрытия.
- Трудно обеспечить безопасное генерирование и распространение секретных ключей.

Более эффективным является отечественный стандарт шифрования данных ГОСТ 28147-06

- 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.

Асимметричные криптосистемы

- Как бы ни были сложны и надежны криптографические системы - их слабое место при практической реализации - ***проблема распределения ключей.***

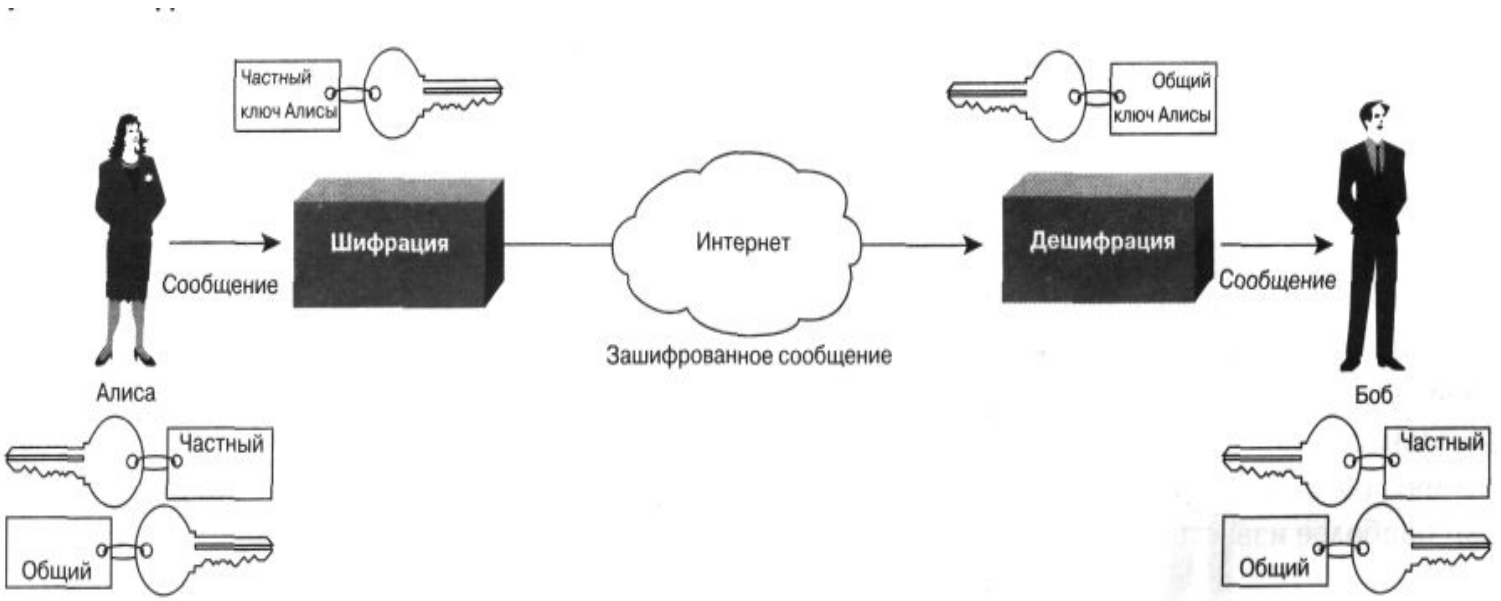
Асимметричные криптосистемы

- 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.

Асимметричные криптосистемы

- Суть их состоит в том, что каждым адресатом ИС генерируются два ключа, связанные между собой по определенному правилу.
- Один ключ объявляется открытым (общим), а другой закрытым (частным, секретным).
- 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 сообщение возможно только с использованием закрытого ключа, который известен только самому адресату.

Асимметричные криптосистемы



Асимметричные криптосистемы

Асимметричные системы для преобразования ключей используют так называемые необратимые или односторонние функции (безопасные хэш-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

Чтобы гарантировать надежную защиту информации, *к асимметричным системам* с открытым ключом предъявляются *два важных и очевидных требования*:

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

Вопрос 4. Требования к криптосистемам.

- 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;

Вопрос 4. Требования к криптосистемам.

- структурные элементы алгоритма шифрования должны быть неизменными;
- дополнительные биты, вводимые в сообщение в процессе шифрования, должен быть полностью и надежно скрыты в шифрованном тексте;
- длина шифрованного текста должна быть равной длине исходного текста;
- не должно быть простых и легко устанавливаемых зависимостей 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.

Литература

Основная:

Аполлонский А.В., Домбровская Л.А., Примакин А.И., Смирнова О.Г., Основы информационной безопасности в ОВД: Учебник для вузов. – СПб.: Университет МВД РФ, 2010

Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А., Основы информационной безопасности: Учебник для вузов. – М.; Изд-во Горячая линия – Телеком, 2011

Малюк А. А. Теория защиты информации. М.; Изд-во Горячая линия – Телеком, 2012.

Адаменко М. Основы классической криптологии. Секреты шифров и кодов. – ДМК Пресс, 2012.

Дополнительная:

Васильев А.И., Сальников В.П., Степашин С.В. Национальная безопасность России: конституционное обеспечение. Фонд «Университет». СПб 1999.

Исмагилов Р.Ф., Сальников В.П., Степашин С.В. Экономическая безопасность России: концепция – правовые основы – политика. Фонд «Университет». СПб 2001.

Доценко С.М., Примакин А.И. Информационная безопасность и применение информационных технологий в борьбе с преступностью: Учебник для вузов. – СПб.: Университет МВД РФ, 2004.