ЛЕКЦИЯ №4

ОСНОВНЫЕ ПОНЯТИЯ УГРОЗЫ *БЕЗОПАСНОСТИ.*

- *Введем ряд определений, используемых при описании средств и методов защиты информации в системах автоматизированной обработки, построенных на основе средств вычислительной техники.* ***Компьютерная система (КС)*** *- организационно-техническая система, представляющую совокупность следующих взаимосвязанных компонентов:*
- *· технические средства обработки и передачи данных;*
- *· методы и алгоритмы обработки в виде соответствующего программного обеспечения;*
- *· данные - информация на различных носителях и находящаяся в процессе обработки;*
- *· конечные пользователи - персонал и пользователи, использующие КС с целью удовлетворения информационных потребностей;*
- *· объект доступа, или объект, - любой элемент КС, доступ к которому может быть произвольно ограничен (файлы, устройства, каналы);*
- *· субъект доступа, или субъект, - любая сущность, способная инициировать выполнение операций над объектом (пользователи, процессы).*

- ***Информационная безопасность*** - состояние КС, при котором она способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз и при этом не создавать таких угроз для элементов самой КС и внешней среды.
- **Угроза информационной безопасности КС** - возможность воздействия на информацию, обрабатываемую КС, с целью ее искажения, уничтожения, копирования или блокирования, а также возможность воздействия на компоненты КС, приводящие к сбою их функционирования.
- **Уязвимость КС** - любая характеристика, которая может привести к реализации угрозы.
- **Атака КС** - действия злоумышленника, предпринимаемые с целью обнаружения уязвимости КС и получения несанкционированного доступа к информации.
- **Безопасная, или защищенная, КС** - КС, снабженная средствами защиты для противодействия угрозам безопасности.
- **Комплекс средств защиты** - совокупность аппаратных и программных средств, обеспечивающих информационную безопасность.

- **Криптография как одна из базовых технологий безопасности ОС.**
- Криптографические методы являются наиболее эффективными средствами защиты информации в КС, при передаче же по протяжённым линиям связи они являются единственным реальным средством предотвращения несанкционированного доступа к ней.
- **Метод шифрования характеризуется показателями надёжности и трудоёмкости.**
  Важнейшим показателем надёжности криптографического закрытия информации является его ***стойкость*** - тот минимальный объем зашифрованного текста, который можно вскрыть статистическим анализом.
- Таким образом, стойкость шифра определяет допустимый объем информации, зашифровываемый при использовании одного ключа. ***Трудоёмкость метода шифрования*** определяется числом элементарных операций, необходимых для шифрования одного символа исходного текста.

- ***Основные требования к криптографическому закрытию информации:***
- *1. Сложность и стойкость криптографического закрытия данных должны выбираться в зависимости от объёма и степени секретности данных.*
- *2. Надёжность закрытия должна быть такой, чтобы секретность не нарушалась даже в том случае, когда злоумышленнику становится известен метод шифрования.*
- *3. Метод закрытия, набор используемых ключей и механизм их распределения не должны быть слишком сложными.*
- *4. Выполнение процедур прямого и обратного преобразований должно быть формальным. Эти процедуры не должны зависеть от длины сообщений.*
- *5. Ошибки, возникающие в процессе преобразования, не должны распространяться по всему тексту.*
- *6. Вносимая процедурами защиты избыточность должна быть минимальной.*
- *Некоторые из этих методов рассмотрены ниже.*

- ***Шифрование заменой (подстановка)***
- Наиболее простой метод шифрования. Символы шифруемого текста заменяются другими символами, взятыми из одного (моноалфавитная подстановка) или нескольких (полиалфавитная подстановка) алфавитов.
- Наиболее простой метод - прямая замена символов шифруемого сообщения другими буквами того же самого или другого алфавита. Однако такой шифр имеет низкую стойкость. Зашифрованный текст имеет те же самые статистические характеристики, что и исходный, поэтому, используя частотный словарь появления символов в том языке, на котором написано сообщение, и подбирая по частотам появления символы в зашифрованном сообщении, можно восстановить таблицу замены. Для этого требуется лишь достаточно длинный зашифрованный текст, для того, чтобы получить достоверные оценки частот появления символов. Поэтому простую замену используют лишь в том случае, когда шифруемое сообщение достаточно коротко.

- Использование ***полиалфавитных подстановок*** повышает стойкость шифра. Для замены символов используются несколько алфавитов, причем смена алфавитов проводится последовательно и циклически: первый символ заменяется соответствующим символом первого алфавита, второй - из второго алфавита и т.д., пока не будут исчерпаны все алфавиты. После этого использование алфавитов повторяется.

ШИФРОВАНИЕ МЕТОДОМ ПЕРЕСТАНОВКИ

- Этот метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. Этот алгоритм можно представить так:
- 1. Выбирается размер блока шифрования: m строк и n столбцов.
- 2. Выбирается ключ шифра - последовательность, которая формируется из натурального ряда 1, 2, ..., n случайной перестановкой.
- 3. Шифруемый текст записывается последовательными строками под числами ключевой последовательности, образуя блок шифрования размером n m.
- 4. Зашифрованный текст выписывается колонками в последовательности возрастания номеров колонок, задаваемых номерами ключевой последовательности.
- 5. Заполняется новый блок и т.д.

- **Дешифрование** выполняется в следующем порядке.
- 1. Выделяем блок символов размером n m.
- 2. Разбиваем его на n групп по m символов и записываем их в те столбцы таблицы перестановки, номера которых совпадают с номерами групп в блоке.
- 3. Расшифрованный текст читается по строкам таблицы перестановки.
- 4. Выделяем новый блок символов и т.д.
- Например, необходимо зашифровать текст "Абсолютно надежной защиты нет". Выберем блок размером 4 8 и ключ 5-8-1-3-7-4-6-2.
- Эти методы предполагают знание ключа при шифровании и дешифровании. При этом важной задачей является безопасная передача ключа, который при этом обычно тоже шифруется. Учитывая короткую длину фразы, содержащей ключ, стойкость шифра ключа значительно выше, чем у основного текста.

СИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ.

- Наиболее перспективными системами криптографической защиты данных в настоящее время являются системы с открытым ключом. В таких системах для шифрования данных используется один ключ, а для дешифрования - другой. Первый ключ не является секретным и может быть опубликован для использования всеми пользователями системы, которые шифруют данные.
- Для дешифрования данных получатель использует второй ключ, который является секретным. Ключ дешифрования не может быть определен из ключа шифрования. В настоящее время наиболее развитым методом криптографической защиты информации с открытым ключом является ***алгоритм RSA***.
- Методы, которые используют для шифрования и дешифрования один и тот же ключ, называются ***симметричными***. В отличие от них методы с открытым ключом называются ***асимметричными*** методами криптозащиты.

ИСПОЛЬЗОВАНИЕ ХЭШ-ФУНКЦИЙ

- Функции ***хэширования*** широко используются для шифрования паролей пользователей КС и при создании электронной подписи. Они отображают сообщение любой длины в строку фиксированного размера. Особенностью ее применения является тот факт, что не существует функции, которая могла бы по сжатому отображению восстановить исходное сообщение, - это односторонняя хэш-функция.

- Получив в свое распоряжение файл, хранящий пароли пользователей, преобразованные хэш-функцией, злоумышленник не имеет возможности получить по ним сами пароли, а должен перебирать парольные комбинации символов, применять к ним хэш-функцию и проверять на соответствие полученной строки и строки из файла хэшированных паролей. Эта работа затрудняется тем, что ему неизвестна и длина пароля, по которому хэш-функцией получено отображение.

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

- При обмене электронными документами очень важным является установление авторства, подлинности и целостности информации в полученном документе. Решение этих задач возлагается на цифровую подпись, сопровождающую электронный документ.
- Функционально она аналогична обычной рукописной подписи и обладает ее основными достоинствами:
- · удостоверяет, что подписанный текст исходит от лица, поставившего подпись;
- · не дает лицу, подписавшему текст, отказаться от обязательств, связанных с подписанным текстом;
- · гарантирует целостность подписанного текста.

- Электронная цифровая подпись представляет собой относительно небольшое количество дополнительной информации, передаваемой вместе с документом. Обычно цифровая подпись шифруется с применением методов открытого ключа и связывает содержимое документа, самой подписи и пары ключей. Изменение хотя бы одного из этих элементов делает невозможным подтверждение подлинности цифровой подписи.
- На этапе формирования цифровой подписи генерируются два ключа: секретный и открытый. Открытый ключ рассылается всем абонентам, которым будет направлен электронный документ. Подпись, добавляемая к документу, содержит такие параметры отправителя, как дату подписи, информацию об отправителе письма и имя открытого ключа.

- С помощью хэш-функции, применённой ко всему документу, вычисляется небольшое число, характеризующее весь текст в целом. Это число, которое затем шифруется закрытым ключом, и является электронной цифровой подписью. Получателю пересылается сам документ в открытом виде и электронная подпись. При проверке цифровая подпись расшифровывается открытым ключом, известным получателю.
- К полученному открытому документу применяется преобразование хэш-функцией. Результат ее работы сравнивается с присланной электронной подписью. Если оба числа совпадают, то полученный документ - подлинный. Очевидно, что любое несанкционированное действие по внесению изменений в документ приведёт к изменению значения, вычисляемого хэш-функцией по открытому документу, но подменить зашифрованную секретным ключом электронную подпись злоумышленнику будет очень трудно.