Костанайский государственный университет имени А.Байтурсынова

Сатмаганбетовой Жанар Зарлыкановна

Тема:

Основные понятия криптографическо й защиты информации

Один из важнейших методов защиты информации - *информационное скрытие*

- когда конф-я информация находится, циркулирует, передается или существует в какой либо иной форме в неконтролируемой зоне
- когда нельзя применить методы разграничения доступа или существует реальная угроза их преодоления нарушителем

Основные цели криптографии

Криптографическая защита - защита информации на основе использования специальных систем и средств, основанных на криптографических методах преобразования информации

Криптографическое преобразование информации

- специальное преобразование информации с помощью т.н. ***кодов*** или ***шифров*** с целью скрытия ее смысла или содержания при доступе к ней лиц, не владеющих соответствующими кодами или шифрами

Сферы применения криптографической защиты в компьютерных системах и сетях:

- при обмене данными между распределенными узлами вычислительных систем и сетей
- при размещении и хранении информации на съемных и несъемных носителях компьютерных систем
- при аутентификации электронных документов и сообщений

Некоторые опред ия:

Шифрование - криптографическое преобразование совокупности данных (текста,сообщения, файла, бл ограниченного по времени процесса, при котором

--преобразованию подвергается каждый символ данных;

--результат преобразования каждого символа оп местоположением символа в исходной совокупно

Кодирование -криптографическое преобразова вной последовательности (потока) данных по специальному коду для каждого символа (единичного элемента) или определенной их совокупности (смысловой - слова, фразы, технологической - блоки, пакеты и т.п.)

Чем шифрование отличается от кодирование?

Некоторые определения (продолжение):

Шифр -совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, заданных алгоритмом криптографического преобразования

Ключ -конкретное ***секретное*** состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного варианта из совокупности всевозможных для данного алгоритма

Криптография -научная дисциплина и отрасль производственно-технологической деятельности по разработке методов криптографического преобразования информации, созданию и эксплуатации криптографических систем

Криптоанализ -совокупность методов, приемов и средств по раскрытию (взлому) по зашифрованным данным (тексту, сообщению, файлу) их открытой формы (содержания, смысла) без знания и владения соответствующими шифрами или кодами

Криптостойкость -характеристика шифра, определяющая его стойкость к взлому (обычно определяется периодом времени или объемом вычислительных затрат, необходимых для осуществления успешной криптоаналитической атаки)


Криптографическое закрытие информации
Шифрование
Кодирование
Другие виды
Замена (подстановка)
Перестановка
Аналитическое преоб раз-е
Гаммирование
Комбинированные
Смысловое
Символьное
Рассечение - разнесение
Сжатие - расширение
Простая (одноалфавитная)
Многоалфавитная одноконтурная обыкновенная
Многоалфавитная одноконтурная монофоническая
Многоалфавитная многоконт-я
Простая
Усложненная по таблице
Усложненная по маршрутам
По правилам алгебры матриц
По особым зависимостям
С конечной короткой гаммой
С конечной длинной гаммой
С бесконечной гаммой
Замена + перестановка
Замена + гаммирование
Перестановка+гаммирование
Гаммирование+гаммирование
По спец. таблицам (словарям)
По кодовому алфавиту
Смысловое
Механическое

Характеристика некоторых методов шифрования:

Шифрование замены (подстановка) -символы шифруемого текста заменяются с символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены

Шифрование перестановкой -символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста

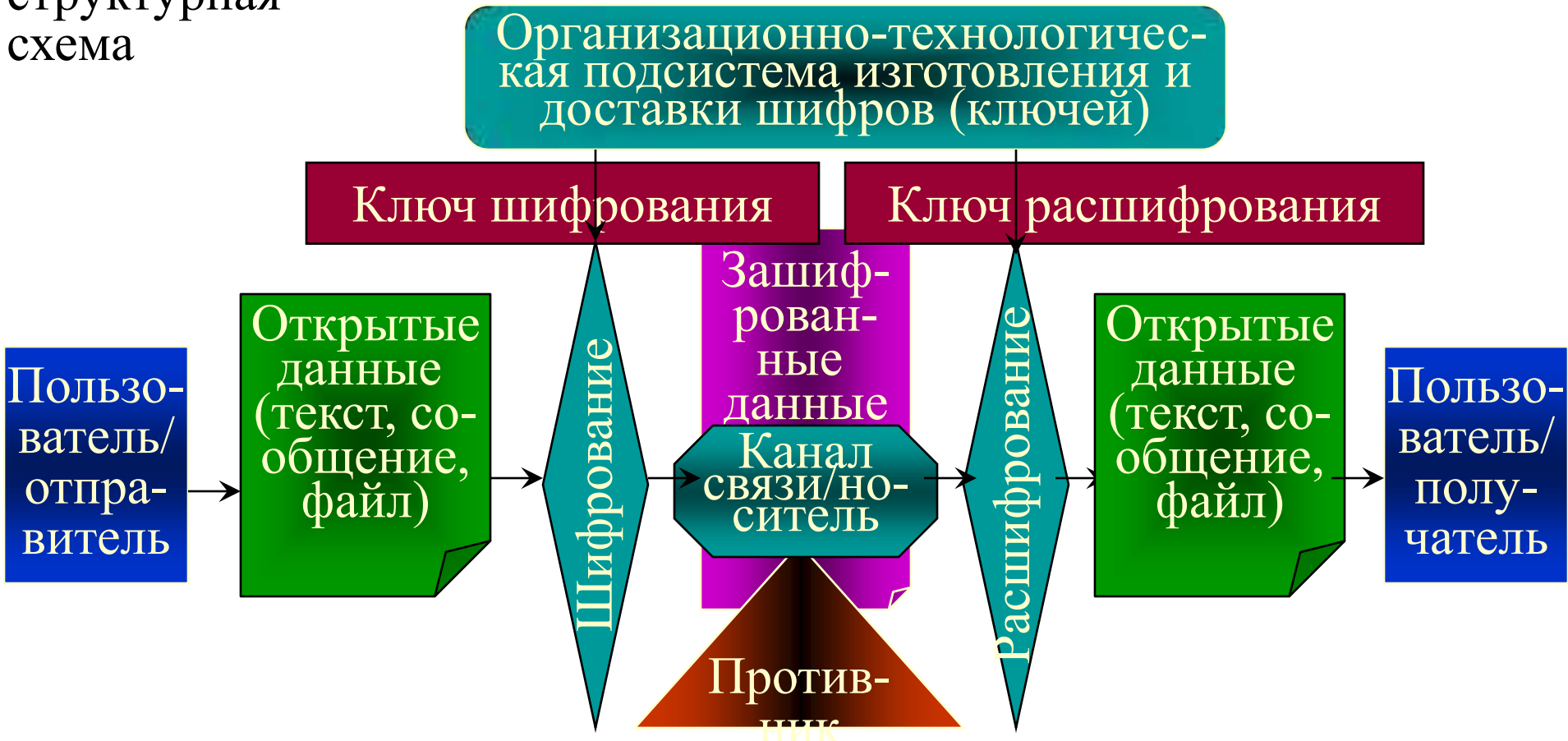
Шифрование аналитическим преобразованием -шифруемый текст преобразуется по некоторому аналитическому правилу (формуле)

Шифрование гаммированием -символы шифруемого текста складываются с символами некоторой случайной последовательности, именуемой ***гаммой шифра***

Криптографическая система

-организационно-технологическая система закрытия конфиденциальной информации при ее передаче или хранении на основе криптографических методов преобразования информации

Обобщенная структурная схема



Классификация и основные виды криптосистем

В зависимости от ***решаемых задач***

- Системы закрытия данных
- Системы защиты от навязывания ложных данных
- Системы аутентификации (ЭЦП, криптопротоколы)

В зависимости от ***типа (функции, алгоритма) криптографического преобразования***

- Симметричные (классические) криптосистемы
- Асимметричные (с открытым ключом) криптосистемы

В зависимости от ***способа криптографического преобразования единичных элементов данных***

- Поточного шифрования
- Блочного шифрования

Современная криптография включает в себя четыре крупных раздела :

- Симметричные криптосистемы
- Криптосистемы с открытым ключом
- Системы электронной подписи
- Управление ключами

Наиболее известные криптостандарты

Наименование	Год	Страна	Длина ключа	Метод	Назначение
Симметричные криптосистемы					
DES (Data Encryption Standard)	1977	США	64 (56+8)	Подстановка + перестановка	В гос.и ком. учр.США для защ. несекр. до 01.01.88
ГОСТ 28147-89	1989	СССР	256	Замена + гаммирование	Для защ. секр. инф. люб. степени
IDEA (International Data Encryption Algoritm)	1990	Международ-й	128	Комбинированный	В сист. PGP
Blowfish (Б.Шнейер)	1993	США	0-255	Сложение, сдвиг	в больших микропроцессорах
RC5 (Р.Ривест)	1994	США	0-255	Сложение, сдвиг	Быстрый как DES,но проще

Наиболее известные криптостандарты

Наименование	Год	Страна	Длина ключа	Метод	Назначение
Асимметричные криптосистемы (с открытым ключом)					
RSA	1978	США	300… 600 бит	Анал-й (возведение в степень)	в т.ч. в SWIFT
Эль-Гамаля	1985	США		=\=	
Системы электронной цифровой подписи (ЭЦП)					
RSA	1978	США		Хэш-функция MD4, MD5	
DSA	1991	США		Хэш-функция DSS (SHA-1)	
ГОСТ Р 34.10-94	1994	Россия		Хэш-функция ГОСТ Р 34.11-94	


Ахмет Байтұрсынов атындағы
Қостанай мемлекеттік университеті
ЕТ және БКе
Бағдарламалық қамтамасыз ету
кафедрасы