Кафедра СИБ

Лекции по курсу

«Методы и средства защиты компьютерной информации»

Содержание

Лекция 1

Основные понятия и определения

Безопасность АСОИ

- защищенность АСОИ от случайного или преднамеренного вмешательства в нормальный процесс их функционирования, а также от попыток хищения, изменения или разрушения их компонентов.

Доступ к информации

- ознакомление с ней, ее обработка, в частности копирование, модификация и уничтожение

Субъект доступа

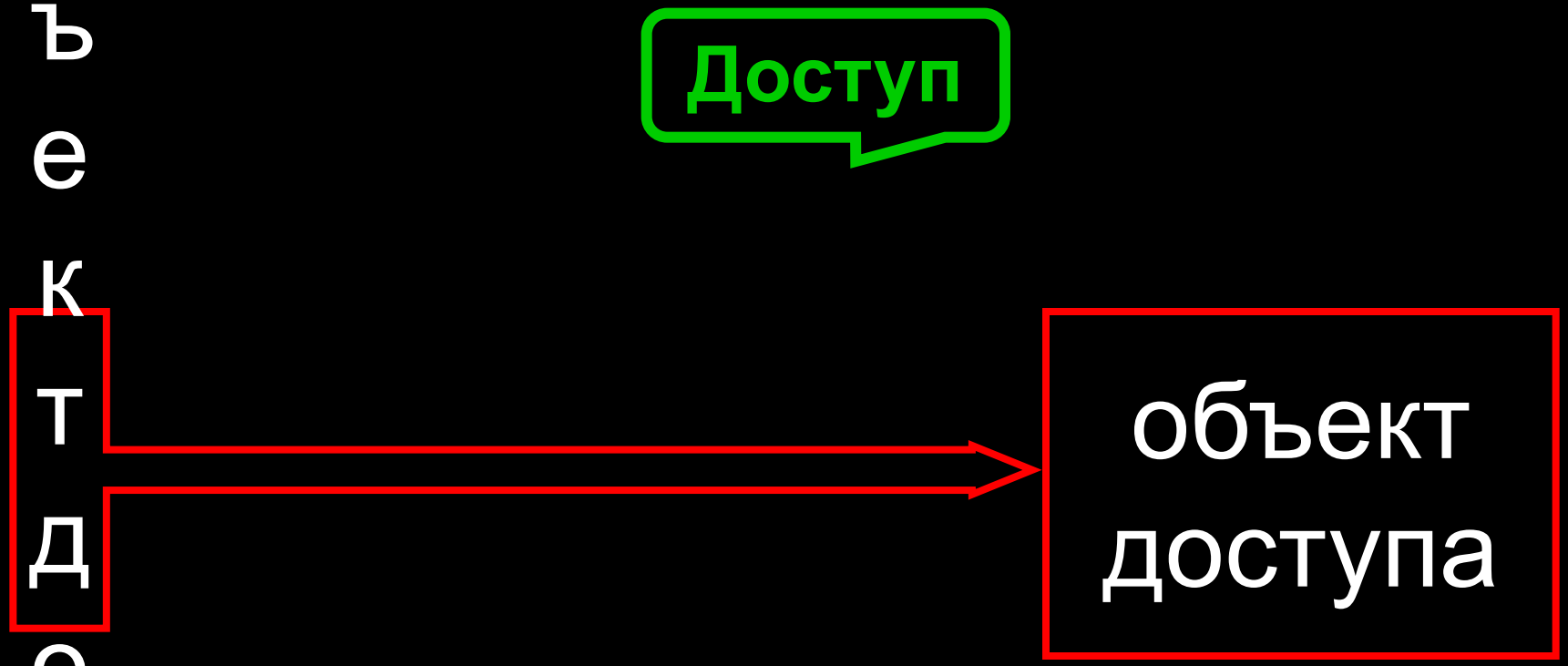
- активный компонент системы, который может стать причиной потока информации от объекта к субъекту или изменения состояния системы (пользователь, процесс, прикладная программа и т.п.)

Объект доступа

- пассивный компонент системы, хранящий, принимающий или передающий информацию

(файл, каталог и т.п.)

Субъект и объект доступа



Санкционированный доступ к информации

- доступ, не нарушающий установленные *правила разграничения доступа*, служащие для регламентации прав доступа субъектов к объектам доступа

Несанкционированный доступ (НСД) к информации

- доступ, нарушающий установленные правила разграничения доступа

Свойства информации

доступность

целостность

конфиденциальность

Ценность информации

- свойство, характеризующее потери собственника данной информации при реализации определенной угрозы, выраженные в стоимостном, временном либо ином эквиваленте.

Модель решетки ценностей

- обобщение порядковой шкалы.

Для большинства встречающихся в теории защиты информации решеток существует представление решетки в виде графа.

В основе государственных стандартов оценки ценности информации обычно используют MLS решетку (Multilevel Security).

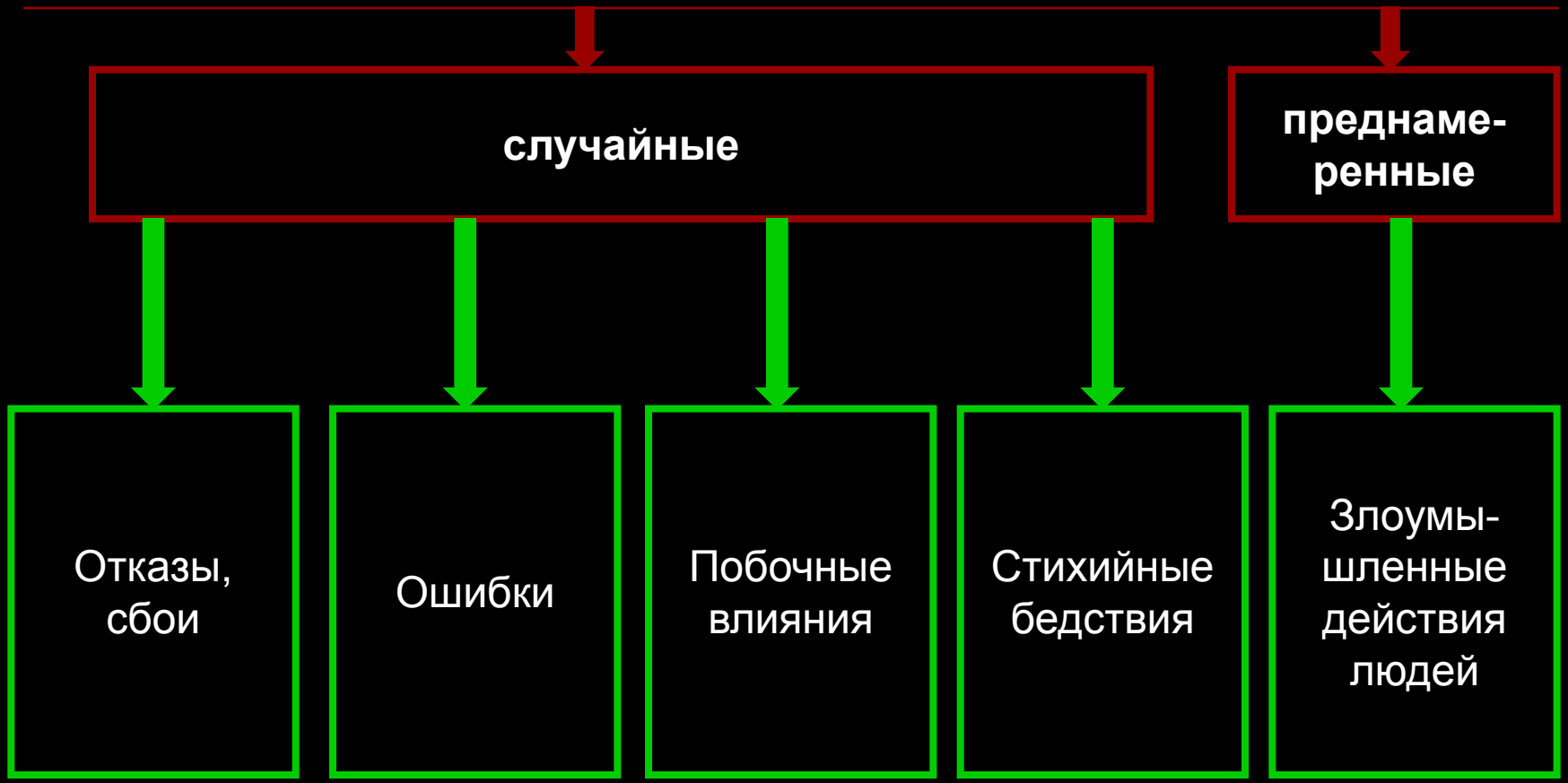
Лекция 2

Угрозы безопасности КС

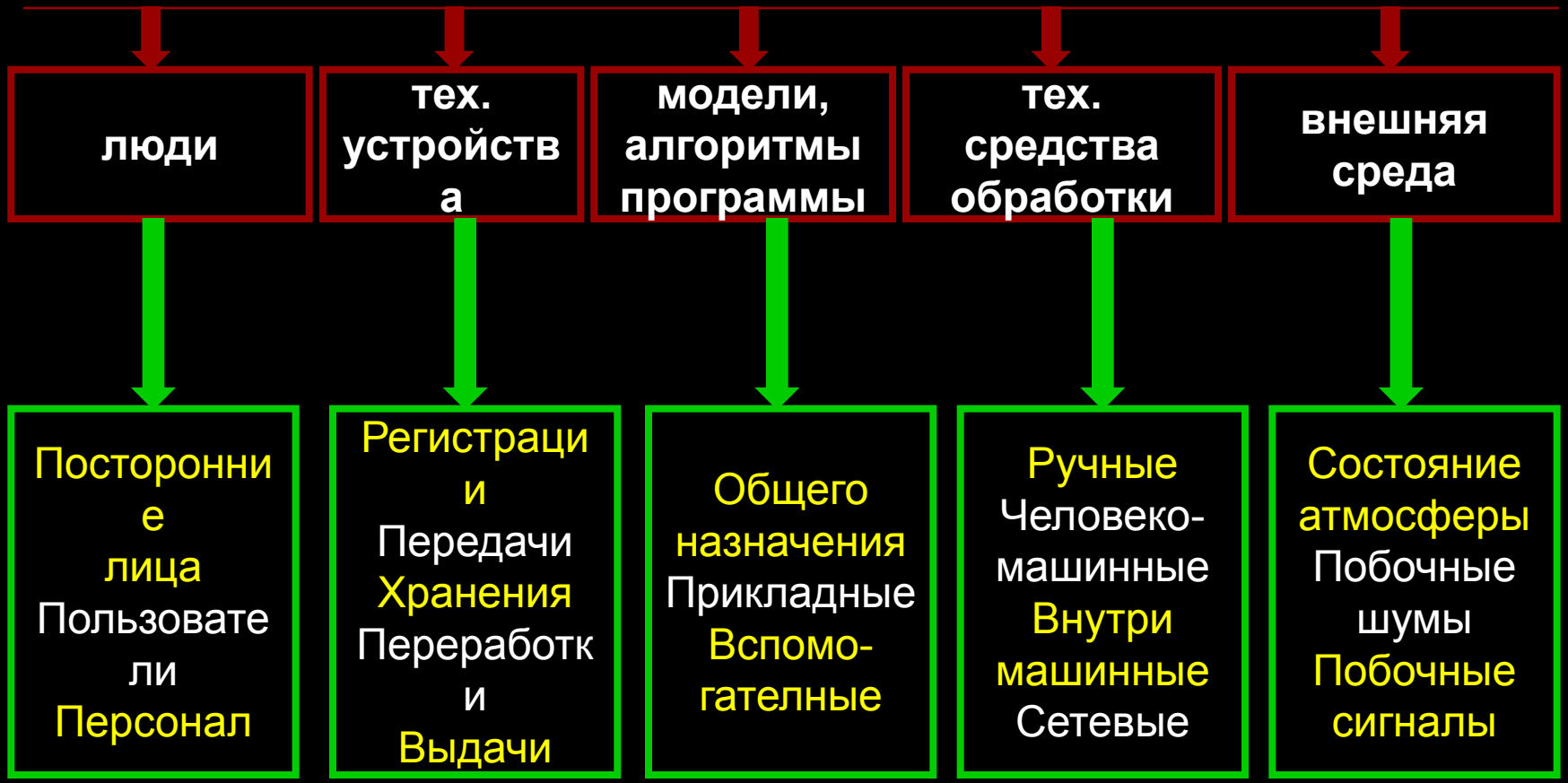
Угроза информацией в системах обработки данных (СОД)

Угроза безопасности АСОИ – потенциальная возможность определенным образом нарушить информационную безопасность (разрушение системы, кража паролей, денег).

Классификация угроз по происхождению угроз



Классификация угроз по источникам угроз



Канал утечки информации

- совокупность источника информации, материального носителя или среды распространения, несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя.

Каналы утечки информации

электромагнитный

виброакустический

визуальный

информационный

Принципы обеспечения ИБ

- Системности.
- Комплексности.
- Непрерывности защиты.
- Разумной достаточности.
- Гибкости управления и применения.
- Открытости алгоритмов и механизмов защиты.
- Простоты применения защитных мер и средств.

Меры обеспечения безопасности компьютерных систем

- правовые (законодательные);
- морально-этические;
- организационно-административные;
- физические;
- аппаратно-программные.

Лекция 3

- Основные понятия разграничения доступа
- Дискреционная модель политики безопасности

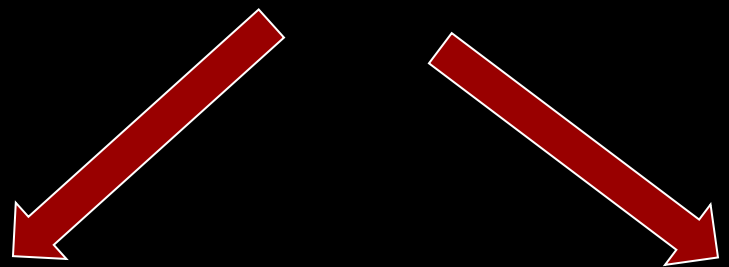
Разграничение доступа к информации

разделение информации, циркулирующей в КС, на части, элементы, компоненты, объекты и т. д., и организация такой системы работы с информацией, при которой пользователи имеют доступ только и только к той части (к тем компонентам) информации, которая им необходима для выполнения своих функциональных обязанностей или необходима исходя из иных соображений.

Политика безопасности

- это набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации.

Политики безопасности



неформальные

формальные

Формальные политики безопасности

Преимущество –

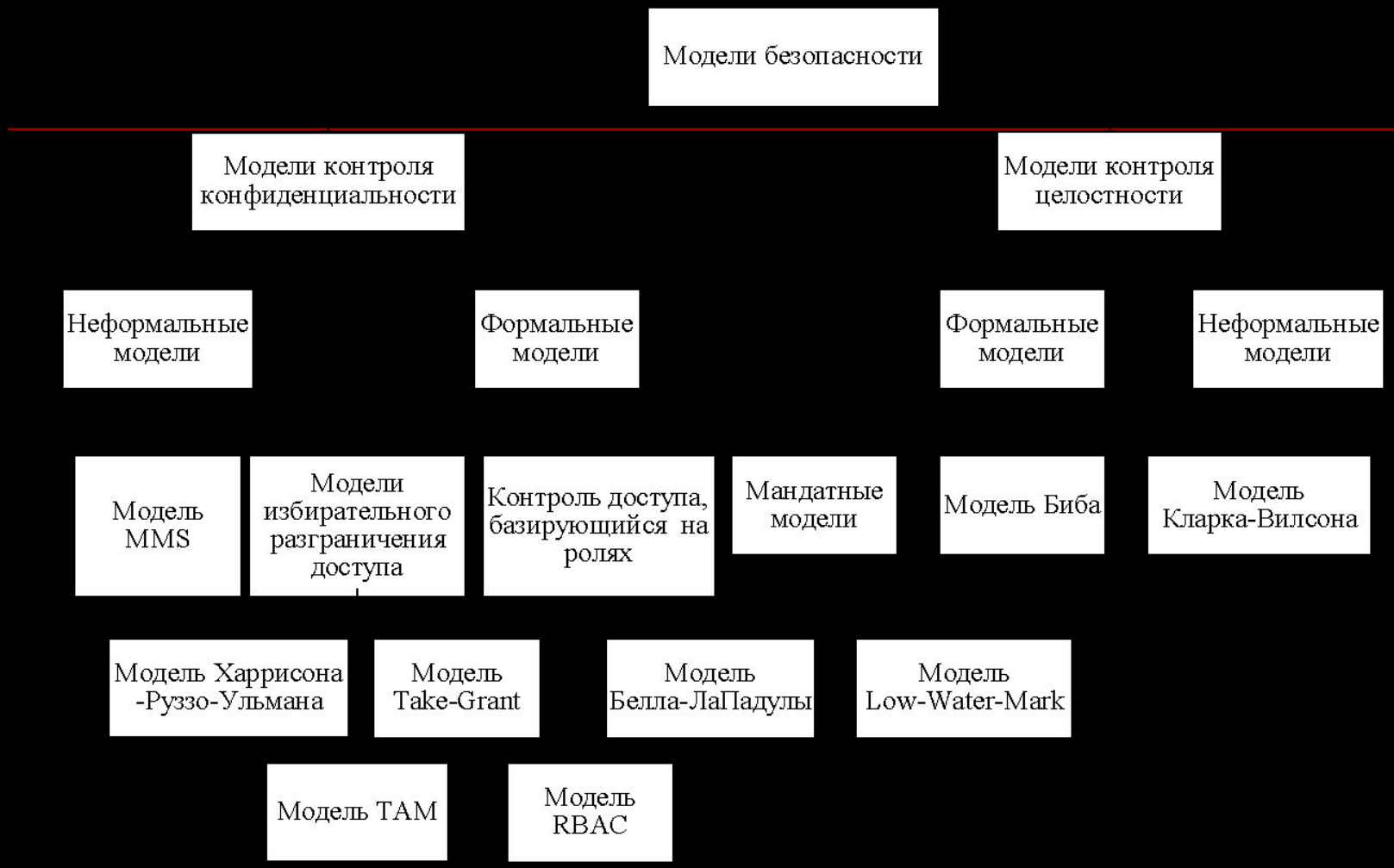
отсутствие противоречий

в политике безопасности

и возможность теоретического доказательства безопасности системы при соблюдении всех условий политики безопасности.

Недостаток формальных методов

- они имеют дело не с самой системой, а с ее моделью.


Модели безопасности
Модели контроля конфиденциальности
Модели контроля целостности
Неформальные модели
Формальные модели
Формальные модели
Неформальные модели
Модель MMS
Модели избирательного разграничения доступа
Контроль доступа, базирующийся на ролях
Мандатные модели
Модель Биба
Модель Кларка-Вилсона
Модель Харрисона -Руззо-Ульмана
Модель Take-Grant
Модель Белла-ЛаПадулы
Модель Low-Water-Mark
Модель TAM
Модель RBAC

Политики безопасности

Одной из самых простых и распространенных моделей политик безопасности является

дискреционная политика

Дискреционная политика безопасности

Пусть

O – множество объектов компьютерной системы, над которыми могут производиться различные операции,

U – множество пользователей (субъектов) компьютерной системы, которые могут производить операции над объектами,

S – множество всевозможных операций (действий) субъектов над объектами.

Дискреционная политика безопасности

определяет отображение

O -> U

(объектов на пользователей-субъектов).

Дискреционная политика безопасности

Каждый объект объявляется собственностью соответствующего пользователя, который может выполнять над ними определенную совокупность действий.

Дискреционная политика безопасности

Пользователь, являющийся собственником объекта, иногда имеет право передавать часть или все права другим пользователям

(обладание администраторскими правами).

Дискреционная политика безопасности

МАТРИЦА ДОСТУПОВ

Объект / Субъект	Файл_1	Файл_2	CD-RW
Администратор	Полные права	Полные права	Полные права
Гость	Запрет	Чтение	Чтение
Пользователь_1	Чтение, передача прав	Чтение, запись	Полные права

Модель Харрисона-Руззо-Ульмана

- *Теорема 1. Существует алгоритм для определения, является или нет моно-операционная система безопасной для данного права а.*
- *Теорема 2. Проблема определения безопасности для данного права а в системе с запросами общего вида является неразрешимой.*

Лекция 4

Мандатные модели политики безопасности

Политика безопасности

- это набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации.

Политики безопасности

Одной из базовых политик безопасности является

мандатная политика.

Исходная мандатная политика безопасности

Пусть в компьютерной системе (КС) определено

n субъектов доступа и

m объектов доступа.

1. Вводится множество атрибутов безопасности *A*, элементы которого упорядочены с помощью установленного отношения доминирования.

Исходная мандатная политика безопасности

2. Каждому объекту КС ставится в соответствие атрибут безопасности, который соответствует ценности объекта и называется его

   уровнем (грифом) конфиденциальности.
3. Каждому субъекту КС ставится в соответствие атрибут безопасности, который называется *уровнем допуска субъекта* и равен максимальному из уровней конфиденциальности объектов, к которому субъект будет иметь допуск

Исходная мандатная политика безопасности

Уровень допуска субъекта = *Максимальный из уровней конфиденциальности объектов,* к которому субъект будет иметь допуск

Исходная мандатная политика безопасности

- Субъект имеет допуск к объекту

тогда и только тогда, когда

уровень допуска субъекта

больше или равен

уровню конфиденциальности объекта.

Мандатная модель политики безопасности Белла-ЛаПадула (БЛМ)

Свойство NRU

(not read up)

«нет чтения вверх»

Свойство (NWD)

(not write down)

«нет записи вниз»

Определение безопасного состояния

Состояние безопасно
тогда и только тогда, когда
оно безопасно по чтению и записи.

Основная теорема безопасности

- *Система (v_0, R, T) безопасна тогда и только тогда, когда состояние v_0 безопасно и T таково, что для любого состояния v, достижимого из v_0 после исполнения конечной последовательности запросов из R, $T(v, c) = v^*$, где $v = (F, M)$ и $v^* = (F^*, M^*)$, переходы системы (T) из состояния в состояние подчиняются следующим ограничениям для любого s из S и для любого o из O:*

  - *если чтение принадлежит $M^*[s, o]$ и чтение $\notin M[s, o]$, то $F^*(s) \geq F^*(o)$;*
  - *если чтение принадлежит $M[s, o]$ и $F^*(s) < F^*(o)$, то чтение $\notin M^*[s, o]$;*
  - *если запись принадлежит $M^*[s, o]$ и запись $\notin M[s, o]$, то $F^*(o) \geq F^*(s)$;*
  - *если запись принадлежит $M[s, o]$ и $F(o) < F(s)$, то запись $\notin M^*[s, o]$.*

Лекция 5

Идентификация и аутентификация субъектов

Идентификация

- это присвоение пользователю некоторого несекретного идентификатора, который он должен предъявить СЗИ при осуществлении доступа к объекту.

Аутентификация

- это подтверждение пользователем своего идентификатора,

проверка его подлинности.

Стойкость подсистемы идентификации и аутентификации

определяется гарантией того, что злоумышленник не сможет пройти аутентификацию, присвоив чужой идентификатор или украв его.

Требования паролю:

- Минимальная длина пароля должна быть не менее 6 символов.
- Пароль должен состоять из различных групп символов (малые и большие латинские буквы, цифры, специальные символы ‘(’, ‘)’, ‘#’ и т.д.).
- В качестве пароля не должны использоваться реальные слова, имена, фамилии и т.д.

Требования к подсистеме парольной аутентификации.

- максимальный срок действия пароля;
- ограничение числа попыток ввода пароля;
- временная задержка при вводе неправильного пароля;

$$P=(V*T)/S=(V*T)/A^L$$

P – вероятность подбора пароля злоумышленником

A – мощность алфавита паролей *L* – длина пароля.

$S=A^L$ – число всевозможных паролей длины *L*, которые можно составить из символов алфавита A.

V – скорость перебора паролей злоумышленником.

T – максимальный срок действия пароля.

Биометрическая аутентификация

- это аутентификация, основанная на использовании индивидуальных физиологических характеристик человека.

Динамика работы пользователя на клавиатуре

- наиболее дешевый среди признаков, используемых при проведении биометрической аутентификации пользователя

Биометрическая аутентификация

характеризуется

коэффициентом ошибочных отказов
(*False rejection rate* ***FRR***)

и

коэффициентом ошибочных подтверждений

(*false acceptance rate* ***FAR***).

Лекция 6

- Введение в криптографию
- Основные термины

Элементы теории чисел

Элементы теории чисел

Числовые функции

Криптография

- совокупность методов преобразования данных (*шифрования*), направленных на то, чтобы сделать эти данные бесполезными для противника.

Ключ шифрования K

- конкретное состояние некоторого параметра (параметров), обеспечивающее выбор одного преобразования из совокупности возможных для используемого метода шифрования.

Открытый текст M

- исходное сообщение, которое шифруют для его сокрытия от посторонних лиц.

Закрытый текст (шифротекст) C

- сообщение, формируемое в результате шифрования открытого текста

Криптоанализ

- решает задачу, характерную для злоумышленника – раскрыть шифр, получив открытый текст, не имея подлинного ключа шифрования.

Типы криптоаналитических атак

- атака при наличии только известного закрытого текста *C*.
- атака по открытому тексту.
- атака методом полного перебора всех возможных ключей.
- атака методом анализа частотности закрытого текста.

Криптостойкость

- определяет стойкость шифра к раскрытию с помощью методов криптоанализа.
- определяется интервалом времени, необходимым для раскрытия шифра.

Лекция 7

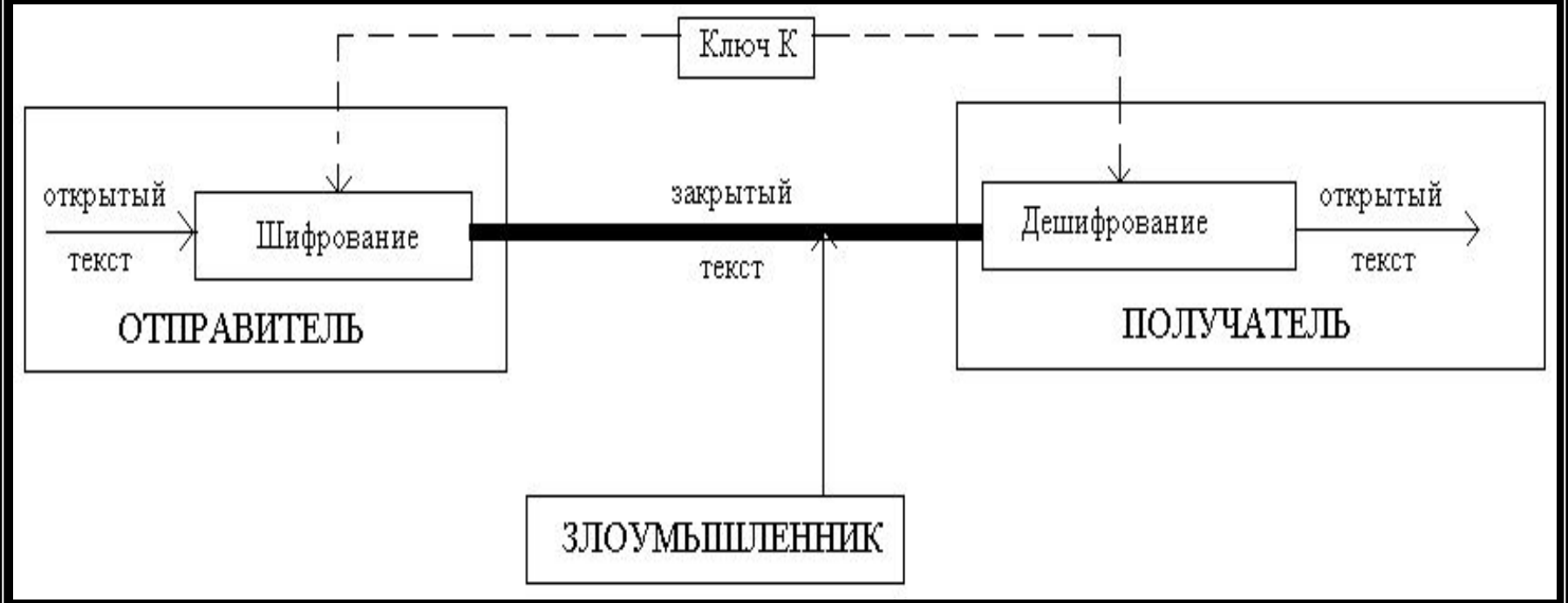
- Симметричные криптосистемы
- Шифрование заменой

Симметричные криптосистемы

Здесь шифрование и дешифрование информации осуществляется на одном ключе *K*, являющемся секретным.

Рассекречивание ключа шифрования ведет к рассекречиванию всего защищенного обмена.

Схема симметричной криптосистемы



Традиционные симметричные криптосистемы

Шифры замены

Шифры перестановки

Шифры гаммирования

Шифрование заменой (подстановкой)

символы шифруемого текста заменяются символами того же или другого алфавита в соответствие с заранее оговоренной схемой замены.

Например, шифр Цезаря.

Шифр Цезаря

- А→Г
- Б→Д
- В→Е
- Г→Ж
- Д→З

и т.д.

каждая буква заменяется на другую букву того же алфавита путем ее смещения в используемом алфавите на число позиций, равное *K*.

K=3

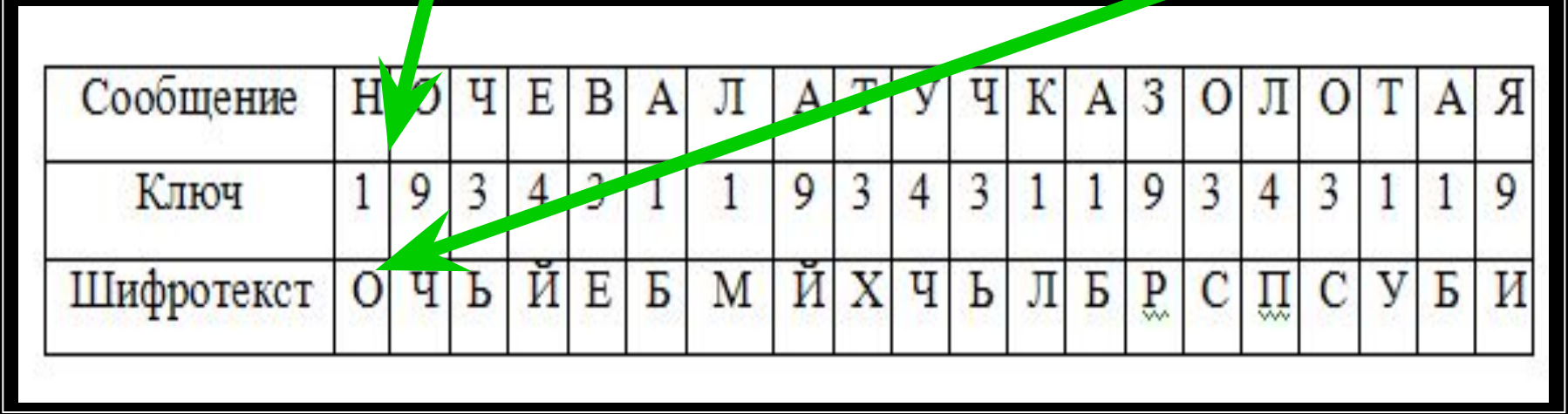
Многоалфавитная замена

Каждой букве алфавита открытого текста в различных ситуациях ставятся в соответствие различные буквы шифротекста в зависимости от соответствующего ей элемента ключа.

Шифр Гронсфельда

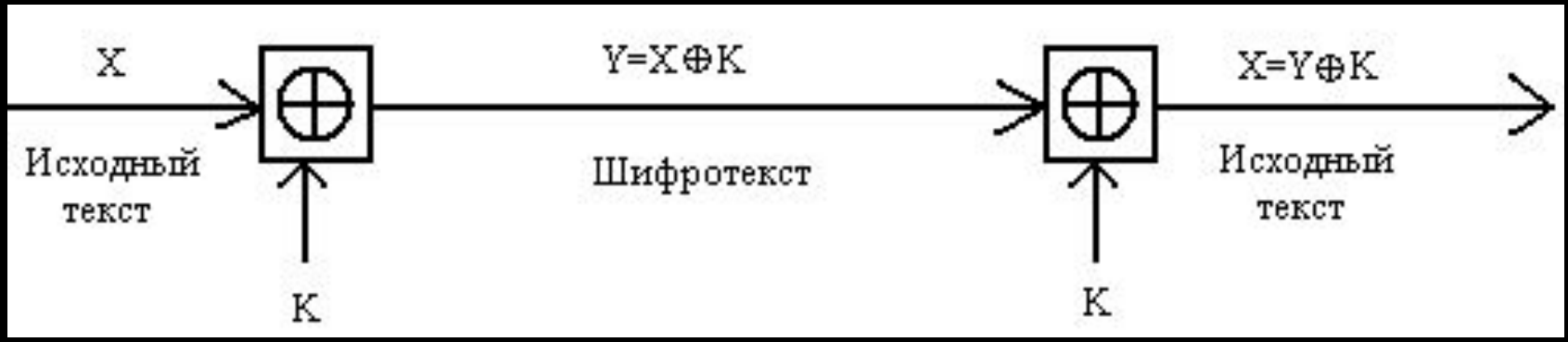
Ключ ***К*=193431**

Чтобы зашифровать первую букву сообщения **Н**, необходимо сдвинуть ее в алфавите русских букв на число позиций **1,** в результате чего получим букву **О**



Сообщение	Н	Б	Ч	Е	В	А	Л	А	Т	У	Ч	К	А	З	О	Л	О	Т	А	Я
Ключ	1	9	3	4	3	1	1	9	3	4	3	1	1	9	3	4	3	1	1	9
Шифротекст	О	Ч	Ь	Й	Е	Б	М	Й	Х	Ч	Ь	Л	Б	Р	С	П	С	У	Б	И

Шифр Вернама



Лекция 8

- Симметричные криптосистемы
- Методы перестановки
- Криптоанализ

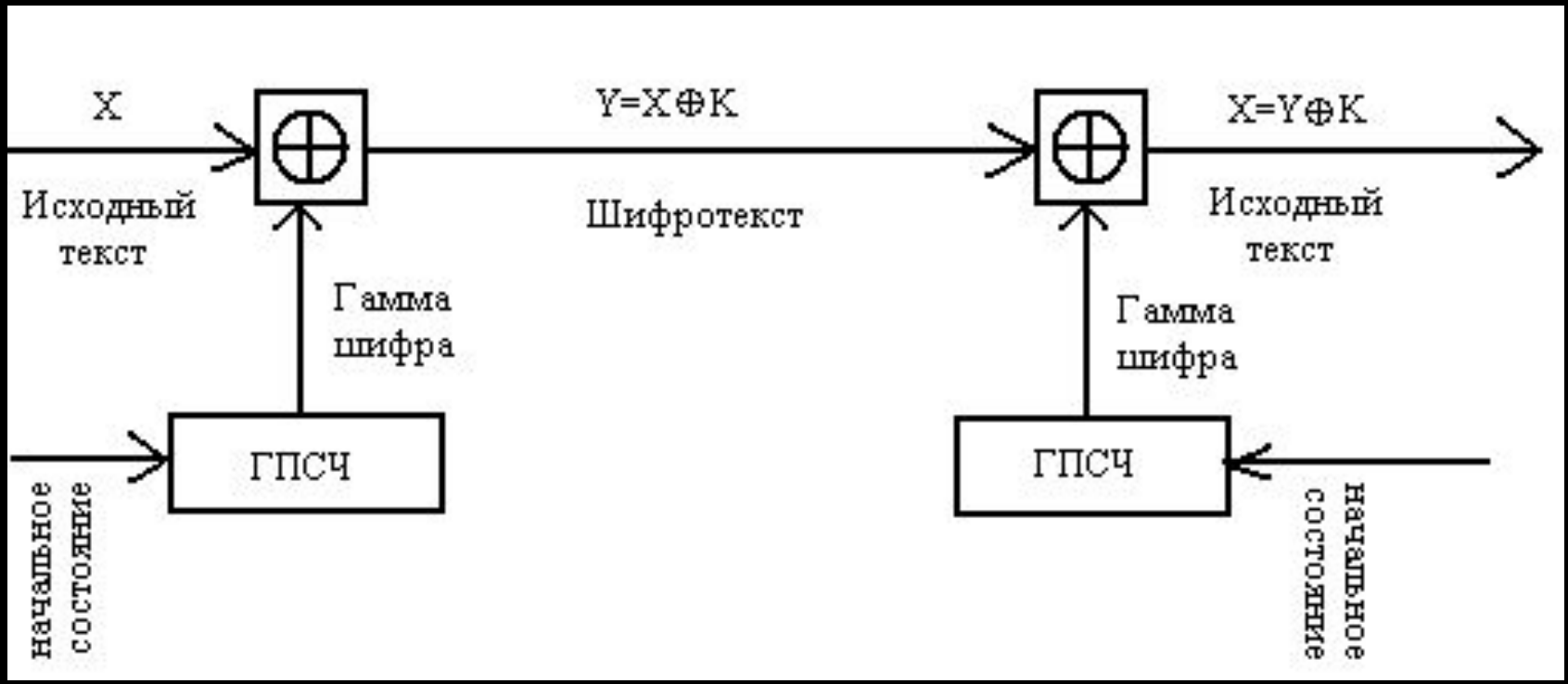
Методы перестановки

- символы открытого текста переставляются по определенному правилу в пределах некоторого блока этого текста. Данные преобразования приводят к изменению только порядка следования символов исходного сообщения

Методы перестановки

- Метод простой перестановки
- Перестановки по маршрутам типа гамильтоновских

Метод гаммирования



Метод фон-Неймана

Линейный конгруэнтный метод

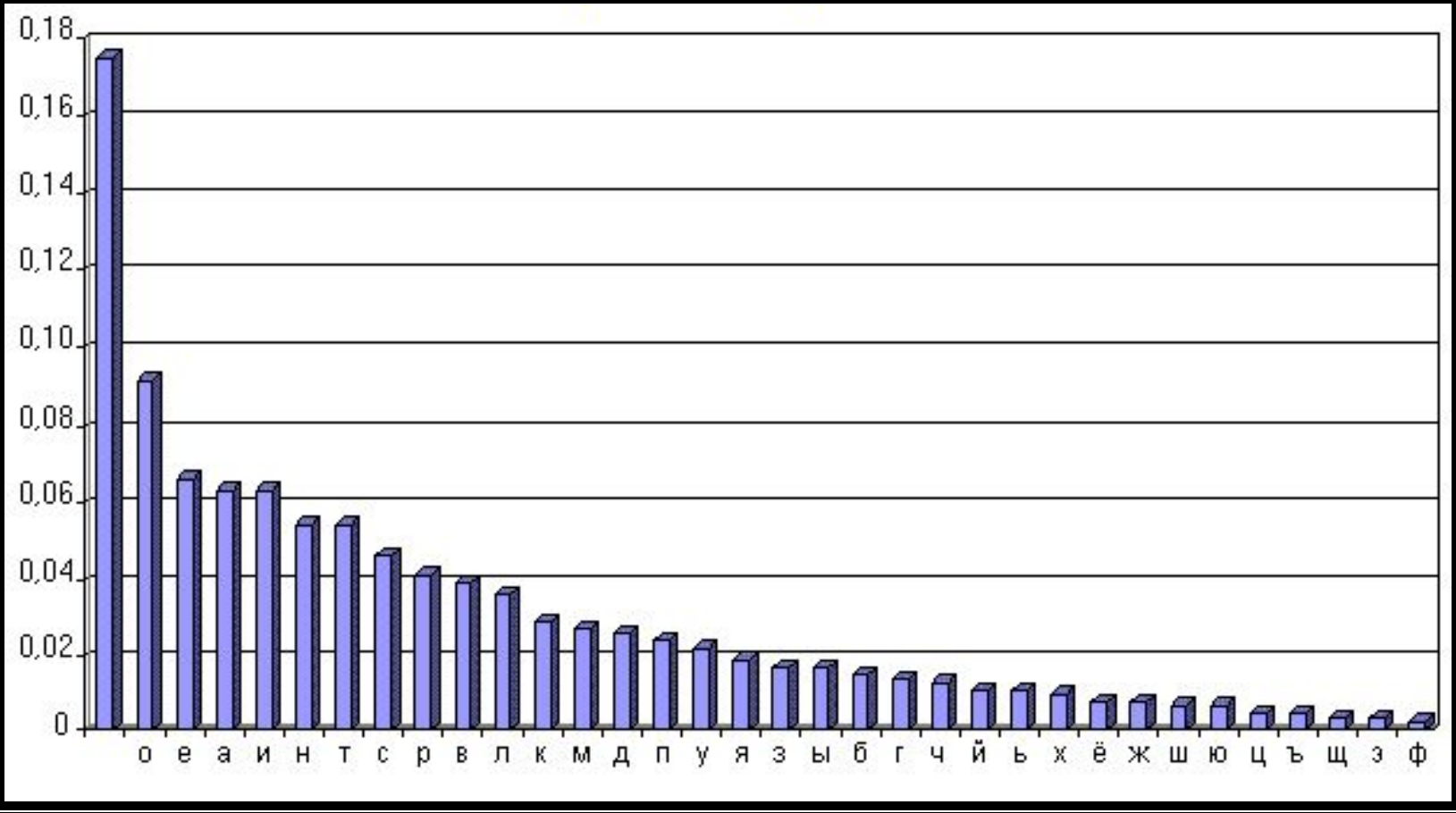
Криптоанализ

– наука о раскрытии исходного текста зашифрованного сообщения без доступа к ключу.

Особенность большинства языков

- они имеют характерное частотное распределение букв и других знаков.

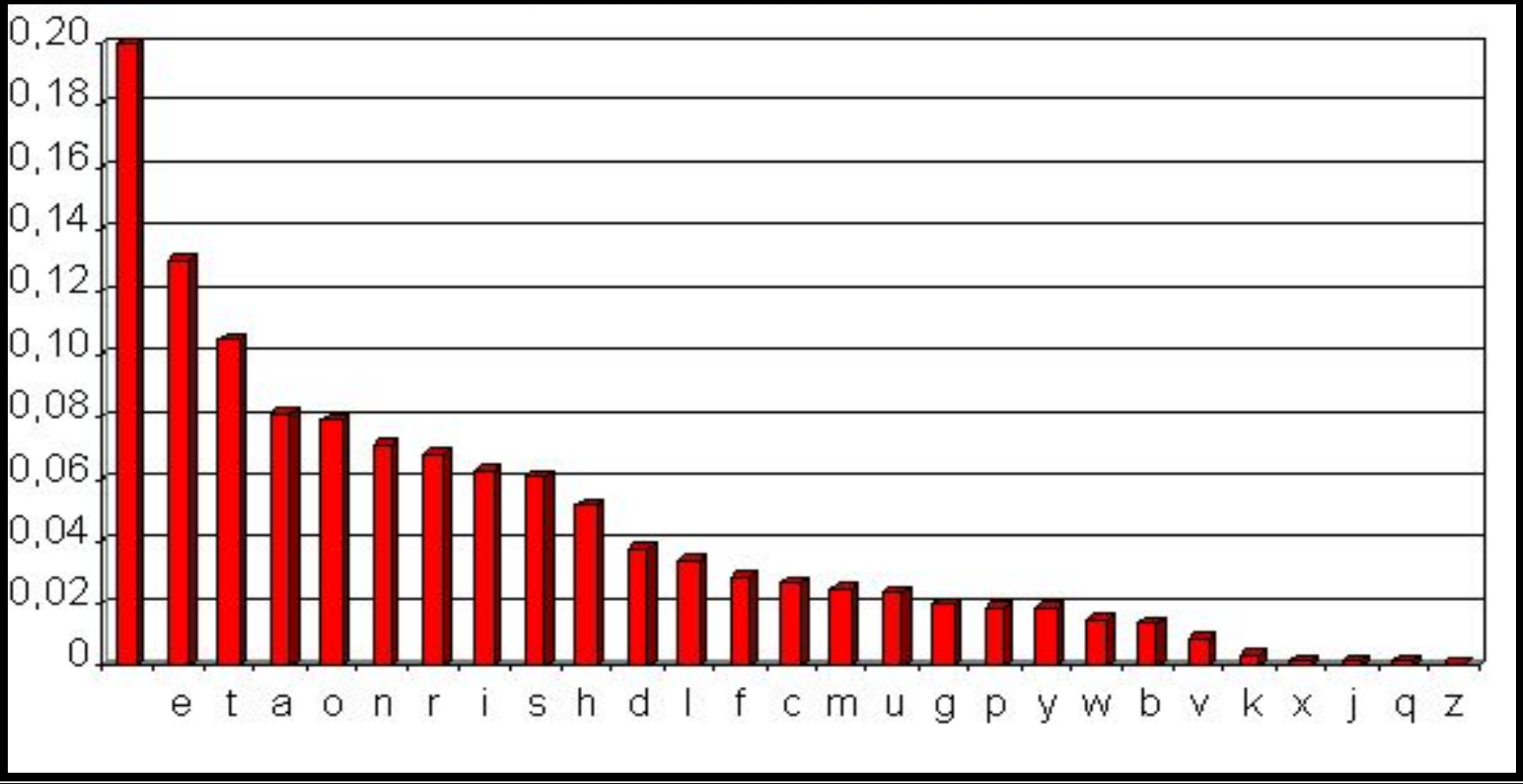
Частотное распределение букв русского алфавита



Криптоанализ, основанный на исследовании частотности символов в тексте

Если наиболее часто встречаемый в тексте символ – это «Б»,
а второй по встречаемости - «К»,
то криптоаналитик может сделать вывод, что
символ «Б» это «Пробел»,
а «К» это буква «О».

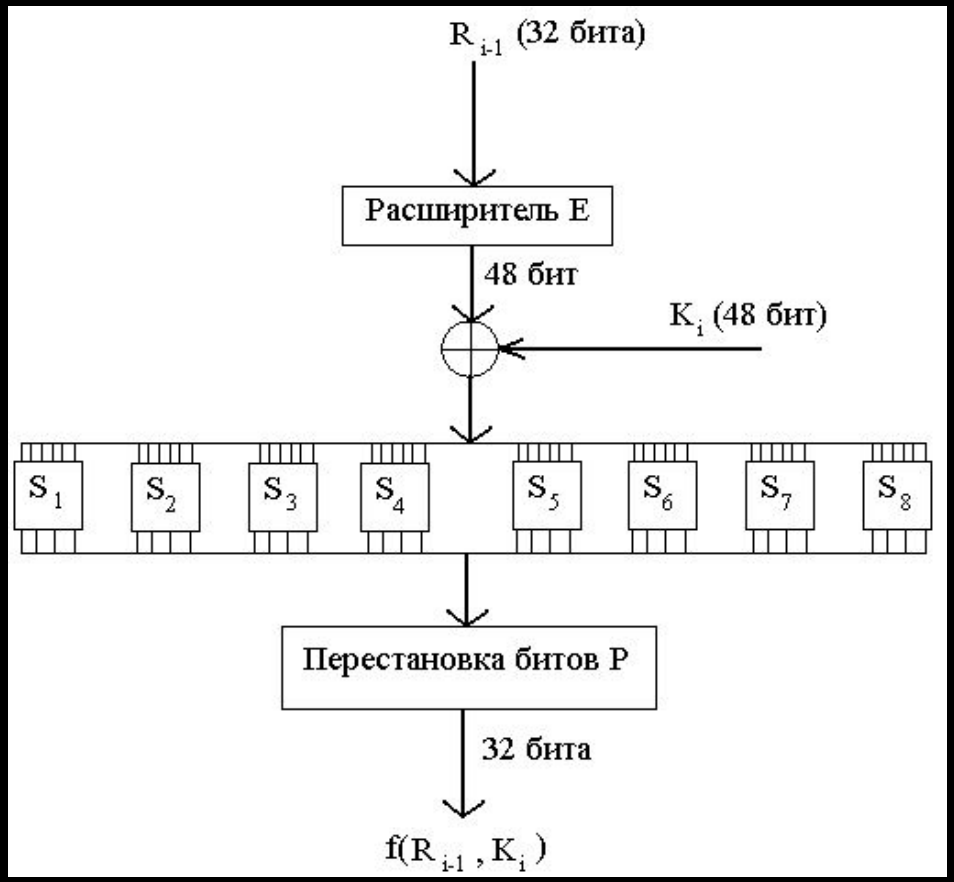
Частотное распределение букв английского алфавита



Общая схема шифрования алгоритма DES

DES

DES. Функция шифрования



ГОСТ 28147-89

ГОСТ 28147-89

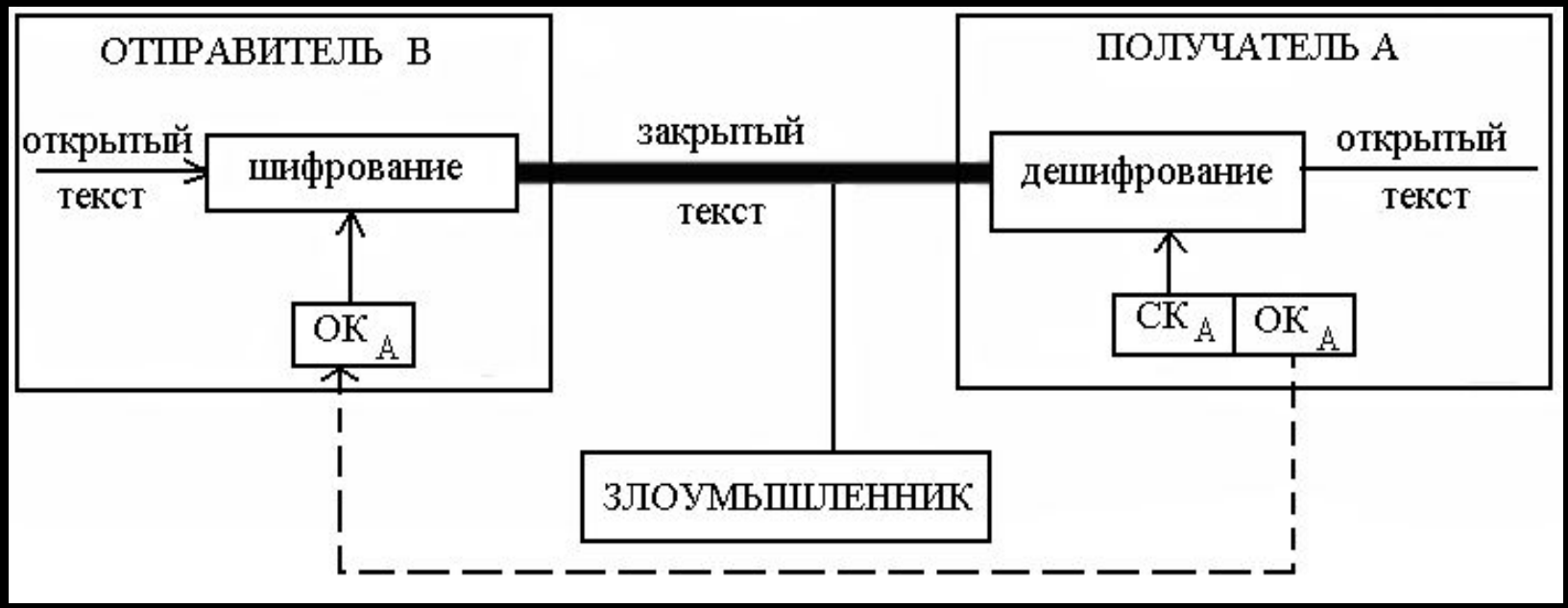
Лекция 9

- Односторонние функции
- Открытое распространение ключей
- Шифры с открытыми ключами
- Криптосистема RSA
- ЭЦП
- Стойкость ассиметричных криптосистем

Асимметричные криптосистемы

здесь используются два ключа
один для шифрования,
другой для дешифрования.

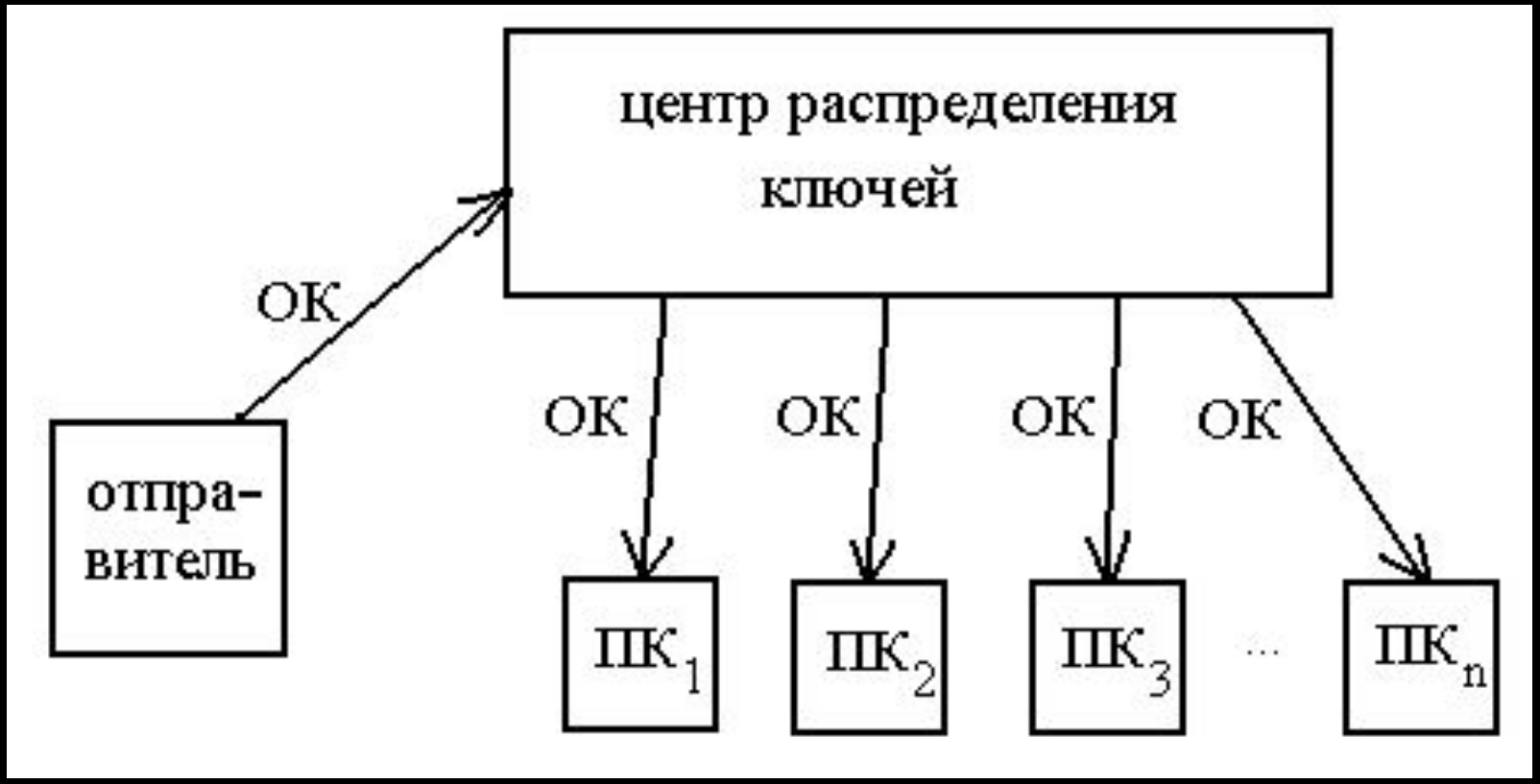
Функциональная схема ассимметричной криптосистемы



ОК – открытый ключ,

СК – секретный ключ.

Схема распределения ОК



Однонаправленные функции

$$f : X \to Y$$

$$x \in X \longrightarrow y = f(x)$$

$$y \in Y \quad \text{⊘} \quad x = f^{-1}(y)$$

Однонаправленные функции

Алгоритм шифрования RSA

стал первым алгоритмом шифрования с открытым ключом.

Надежность данного алгоритма основывается на трудности факторизации больших чисел и вычисления дискретных логарифмов

Алгоритм шифрования RSA

Электронно-цифровая подпись (ЭЦП)

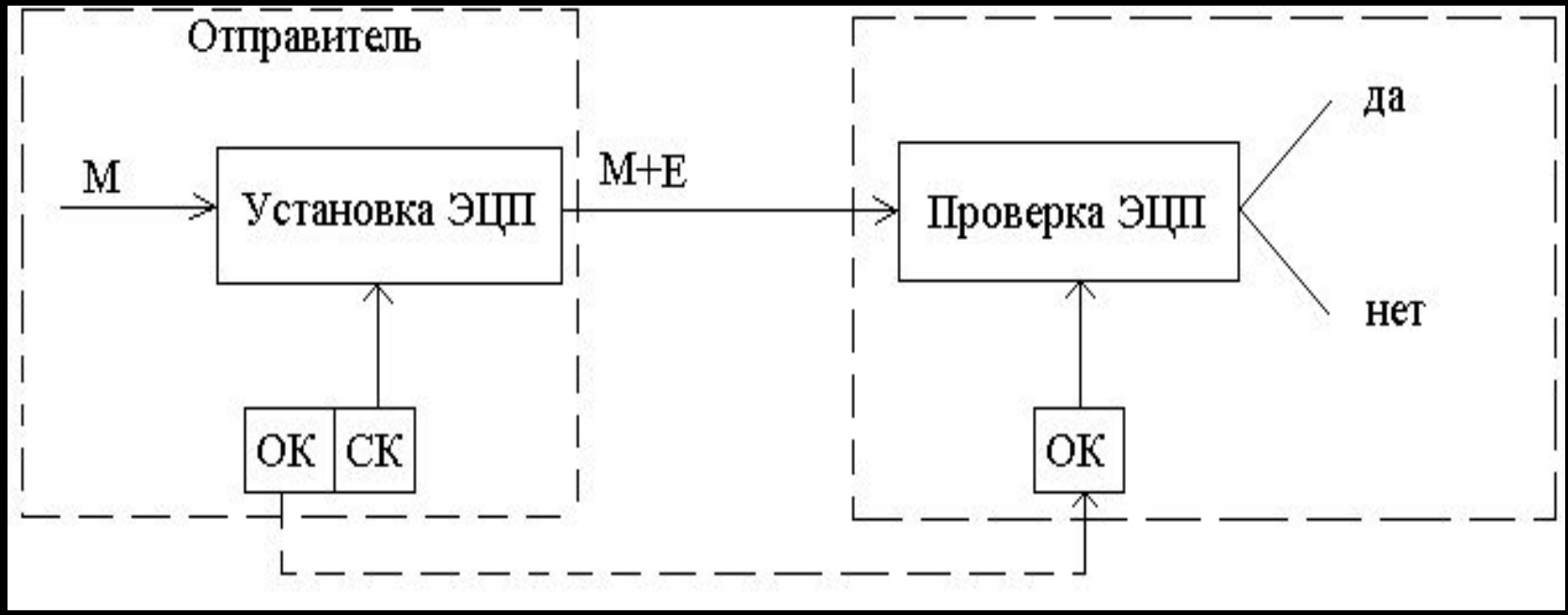
Шпе

1. удостоверяет, что подписанный текст исходит от лица, поставившего подпись.
2. не дает отказаться лицу, поставившего подпись, от своих обязательств.
3. гарантирует целостность документа.

Угрозы

- Активный перехват.
- Маскарад.
- Ренегатство.
- Подмена.
- Повтор.

Функциональная схема использования ЭЦП



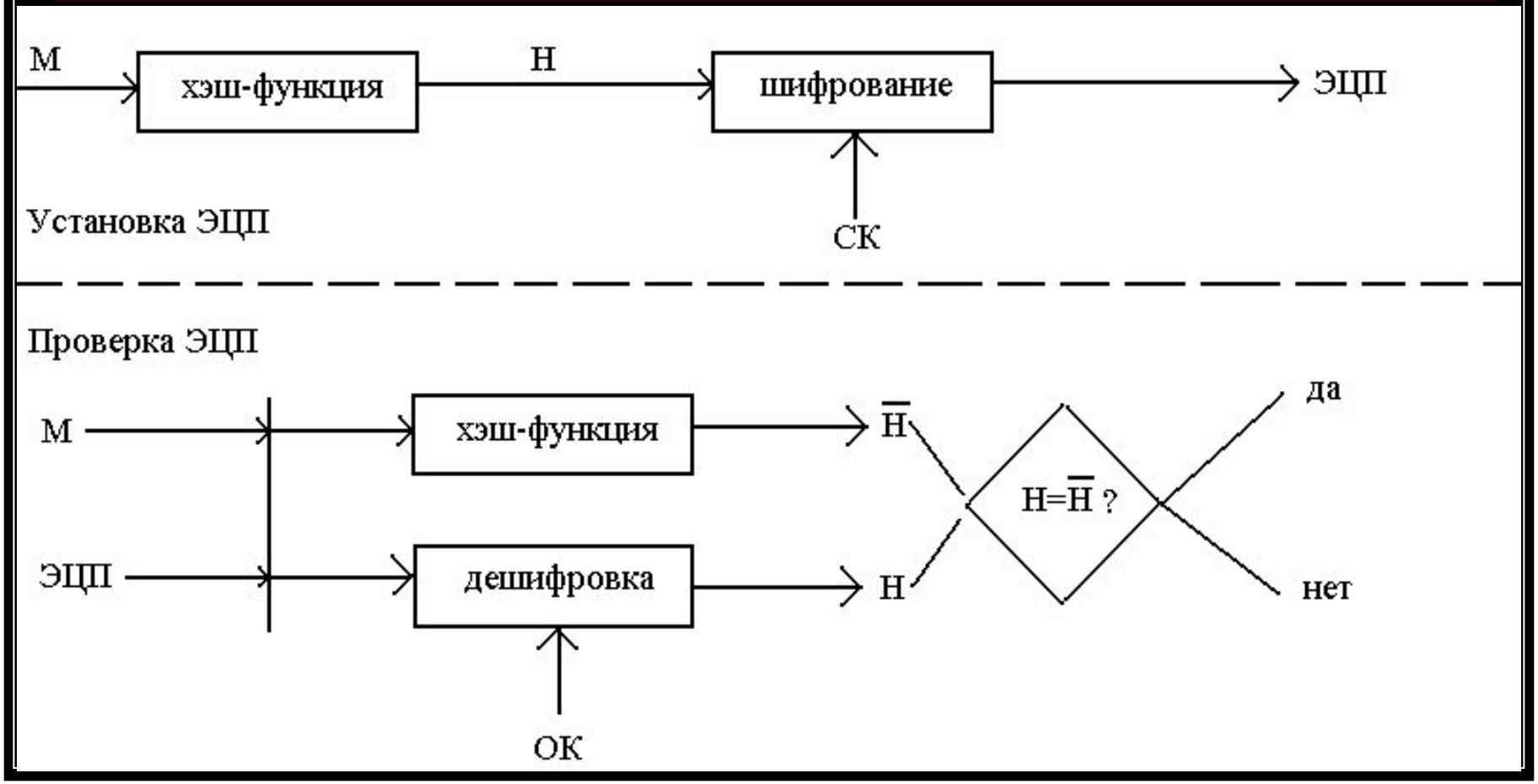
ОК – открытый ключ,

СК – секретный ключ.

Функциия хэширования H

функция, сжимающая сообщение произвольной длины *M*, в значение фиксированной длины *H(M)*, и обладающая свойствами необратимости, рассеивания и чувствительности к изменениям.

Схема процедур установки и проверки ЭЦП



Лекция 10

Хранение и распределение ключевой информации

Базу данных аутентификации в КС необходимо защищать от двух основных видов угроз

- Угрозы прямого доступа к базе данных аутентификации с целью ее копирования, исследования, модификации
- Угрозы исследования содержимого базы данных аутентификации

Первая типовая схема хранения ключевой информации

Номер пользователя	Информация для иден-тификации	Информация для аутен-тификации
1	ID_1	E_1
2	ID_2	E_2
…	…	…
N	ID_N	E_N

Вторая типовая схема хранения ключевой информации

Номер пользователя	Информация для идентификации	Информация для аутентификации
1	ID_1, S_1	E_1
2	ID_2, S_2	E_2
…	…	…
N	ID_N, S_N	E_N

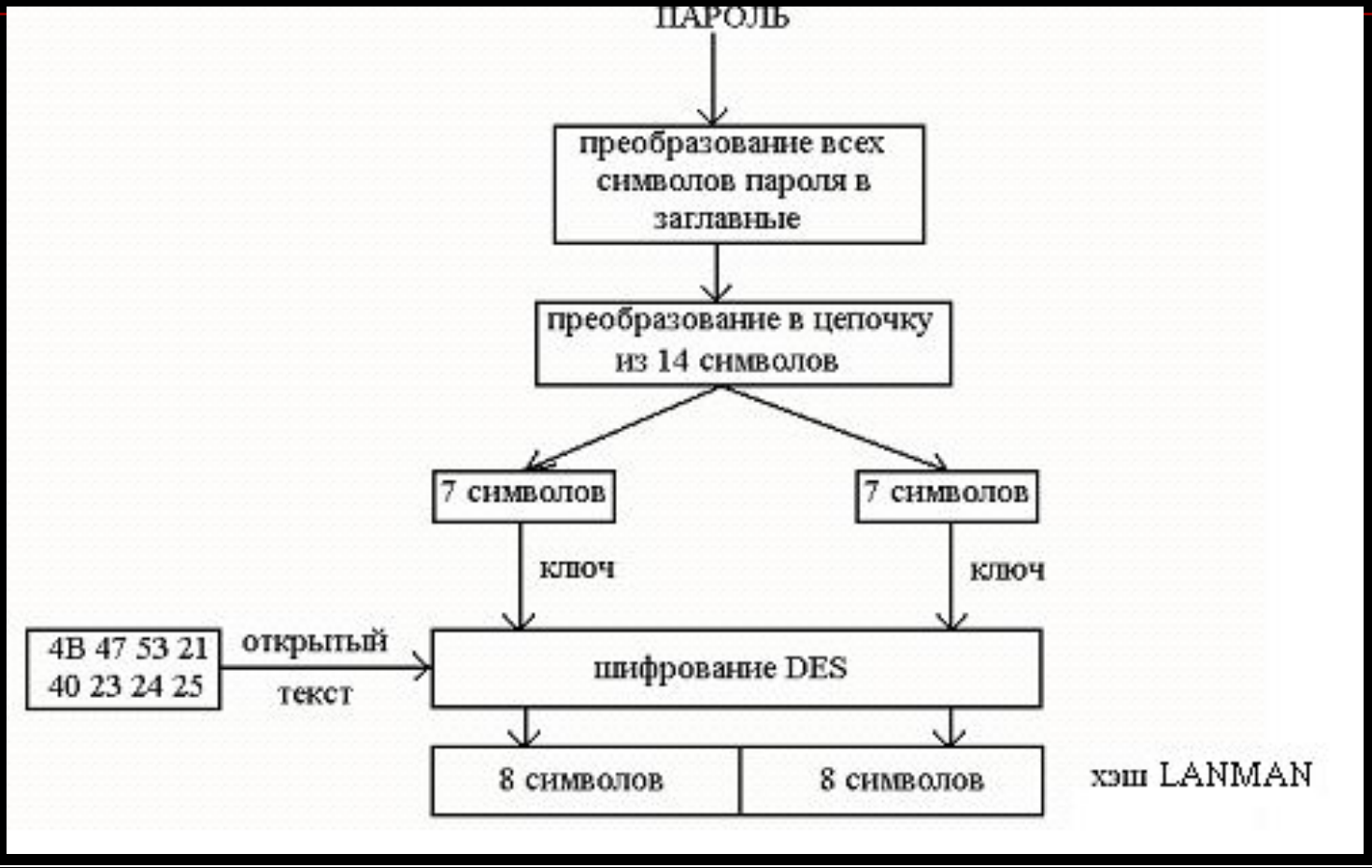
Утверждение (о подмене эталона)

- Если пользователь имеет возможность записи объекта хранения эталона, то он может быть идентифицирован и аутентифицирован (в рамках рассмотренных схем), как любой пользователь.

Защита баз данных аутентификации в ОС, построенных на технологии Windows NT

- Алгоритм хэширования LANMAN
- Алгоритм хэширования NTLM

LANMAN


ПАРОЛЬ
преобразование всех символов пароля в заглавные
преобразование в цепочку из 14 символов
7 символов
7 символов
ключ
ключ
4B 47 53 21 40 23 24 25
открытый текст
шифрование DES
8 символов
8 символов
хэш LANMAN

Иерархия ключевой информации

- мастер-ключ
- ключи шифрования ключей
- сеансовые ключи

Распределение ключей

- Распределение ключевой информацией с использованием одного либо нескольких центров распределения ключей.
- Прямой обмен сеансовыми ключами между пользователями.

Протокол Диффи-Хеллмана

Лекция 11

Протоколы безопасной аутентификации пользователей

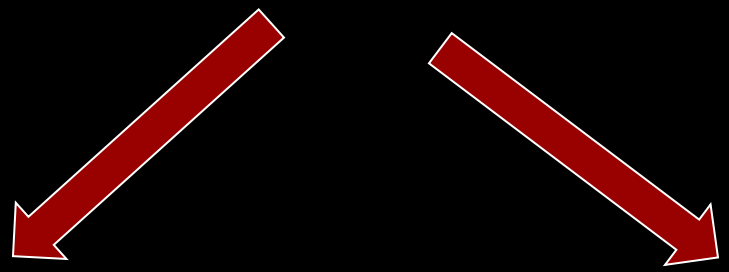
Обеспечение подлинности канала связи

- Механизм запрос-ответ
- Механизм отметки времени

Стойкость подсистемы идентификации и аутентификации

определяется гарантией того, что злоумышленник не сможет пройти аутентификацию, присвоив чужой идентификатор или украв его.

Протоколы безопасной аутентификации пользователей



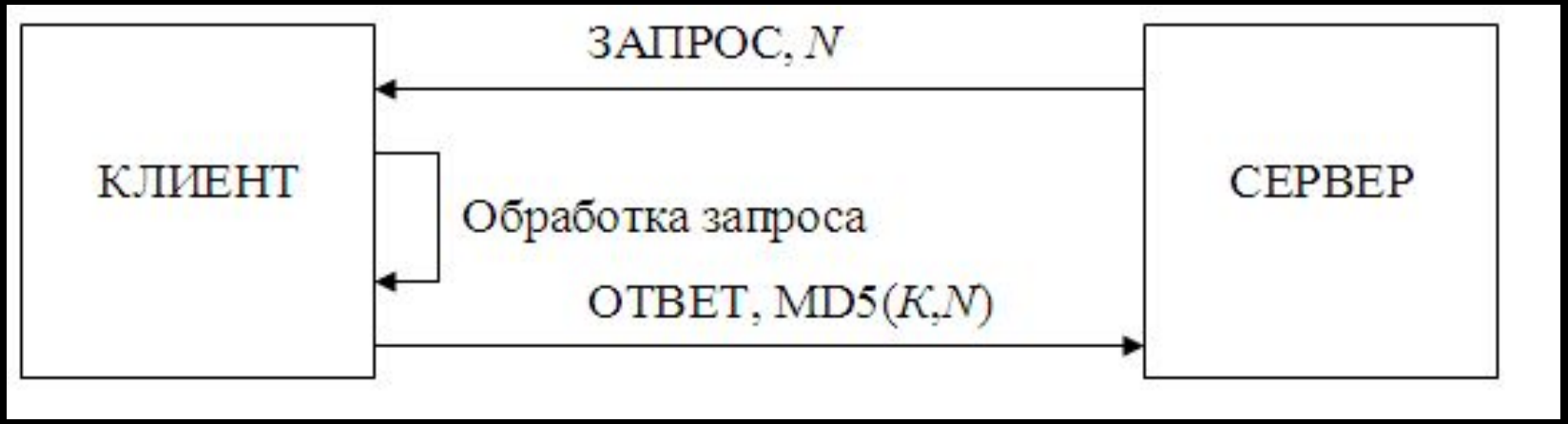
Аутентификация на основе сертификатов

Процедура «рукопожатия»

Протоколы безопасной удаленной аутентификации пользователей

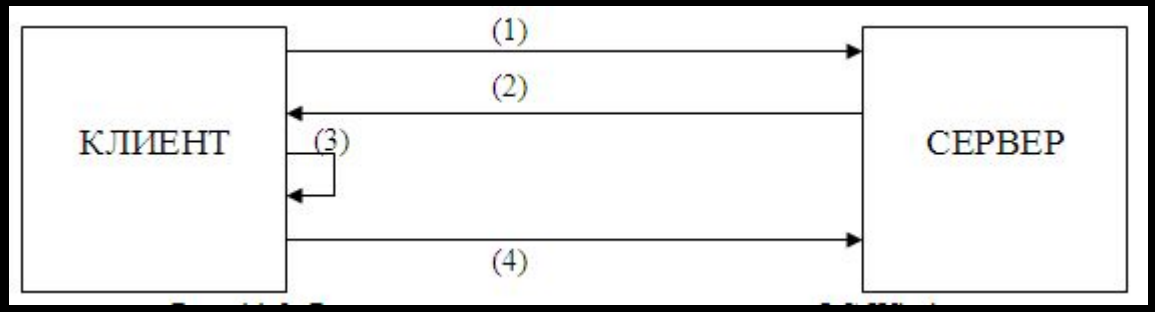
- Протокол CHAP (Challenge Handshaking Authentication Protocol)
- Протокол одноразовых ключей S/KEY

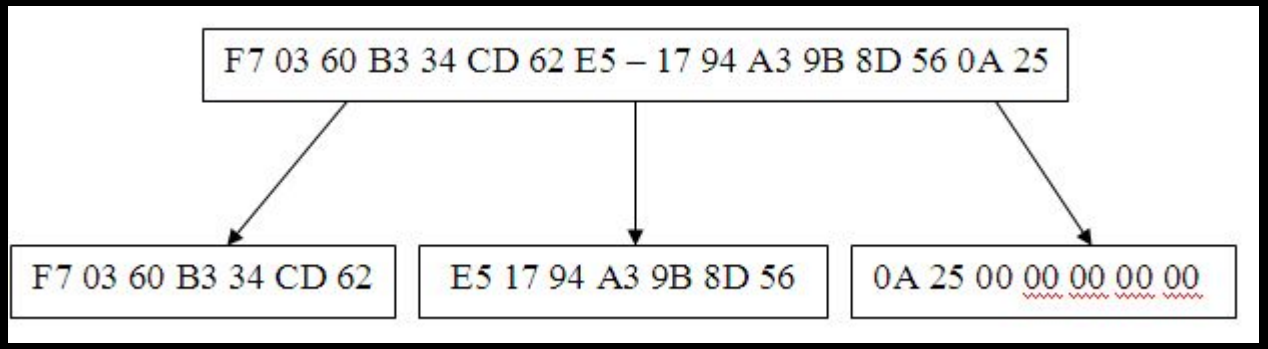
CHAP



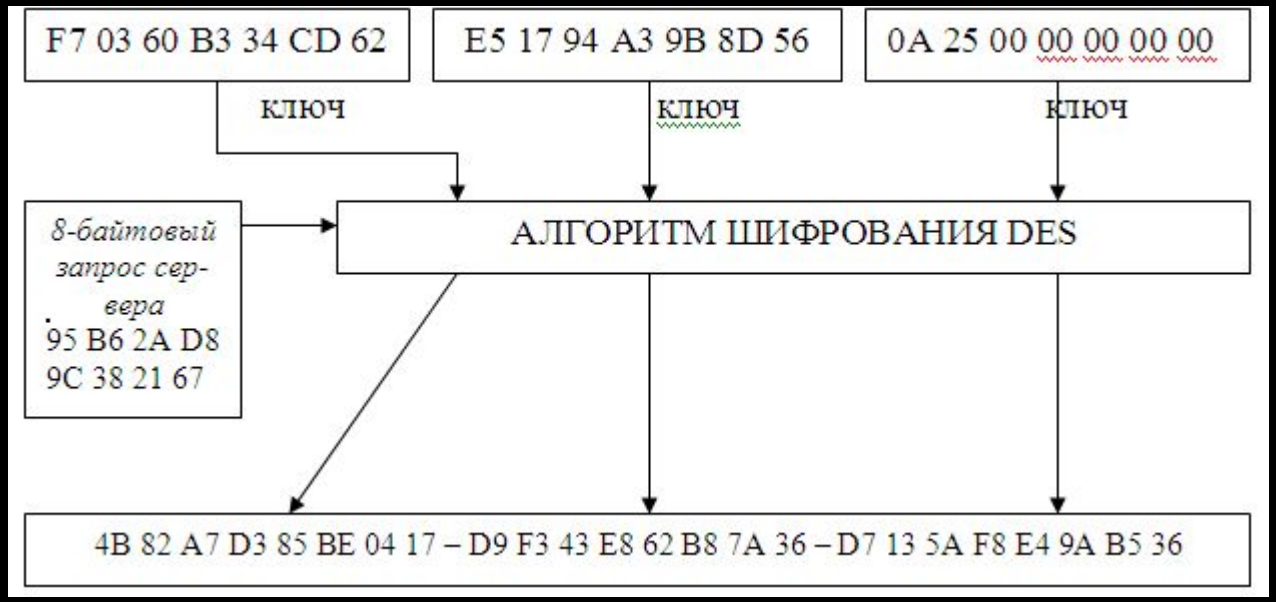
S/KEY

Удаленная аутентификация с помощью хэша LANMAN





Удаленная аутентификация с помощью хэша LANMAN



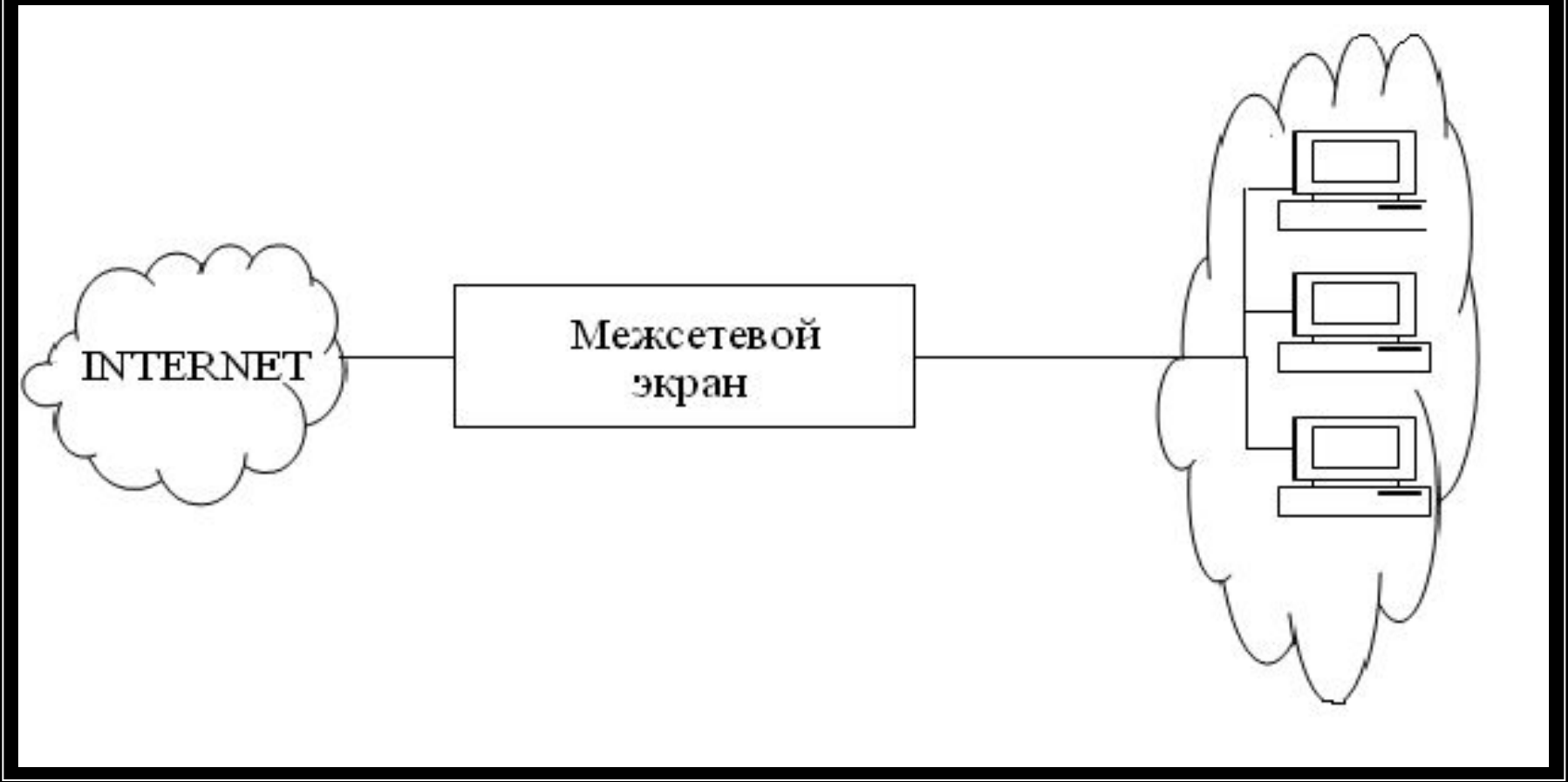
Лекция 12

Защита информации в компьютерных сетях

Классы типовых удаленных атак

- Анализ сетевого трафика
- Подмена доверенного субъекта
- Введение ложного объекта компьютерной сети
- Отказ в обслуживании (DoS)
- Сканирование компьютерных сетей

Защита внутренней сети организации от НСД из сети INTERNET



виды МЭ

- фильтрующие маршрутизаторы (пакетные фильтры);
- шлюзы сетевого уровня;
- шлюзы прикладного уровня.

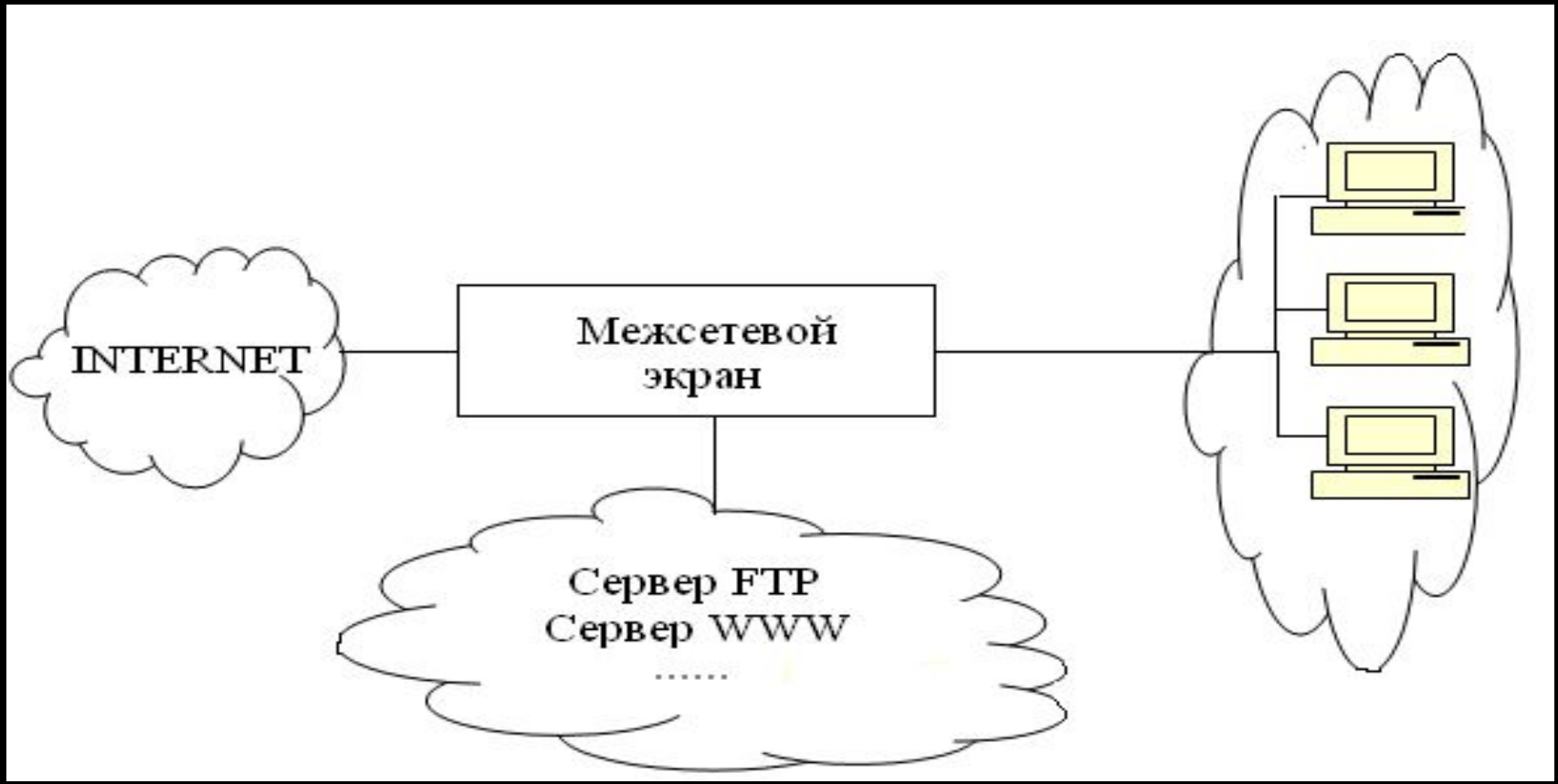
Формирование правил

- запрещать все, что не разрешено в явной форме;
- разрешать все, что не запрещено в явной форме.

Фильтрующие МЭ

Тип	Адрес отправителя	Адрес получателя	Порт отправителя	Порт получателя	Действие
TCP	*	129.1.2.3	>1023	21	Разрешить
TCP	123.6.49.234	123.1.2.9	>1023	119	Разрешить

DMZ



Лекция 13

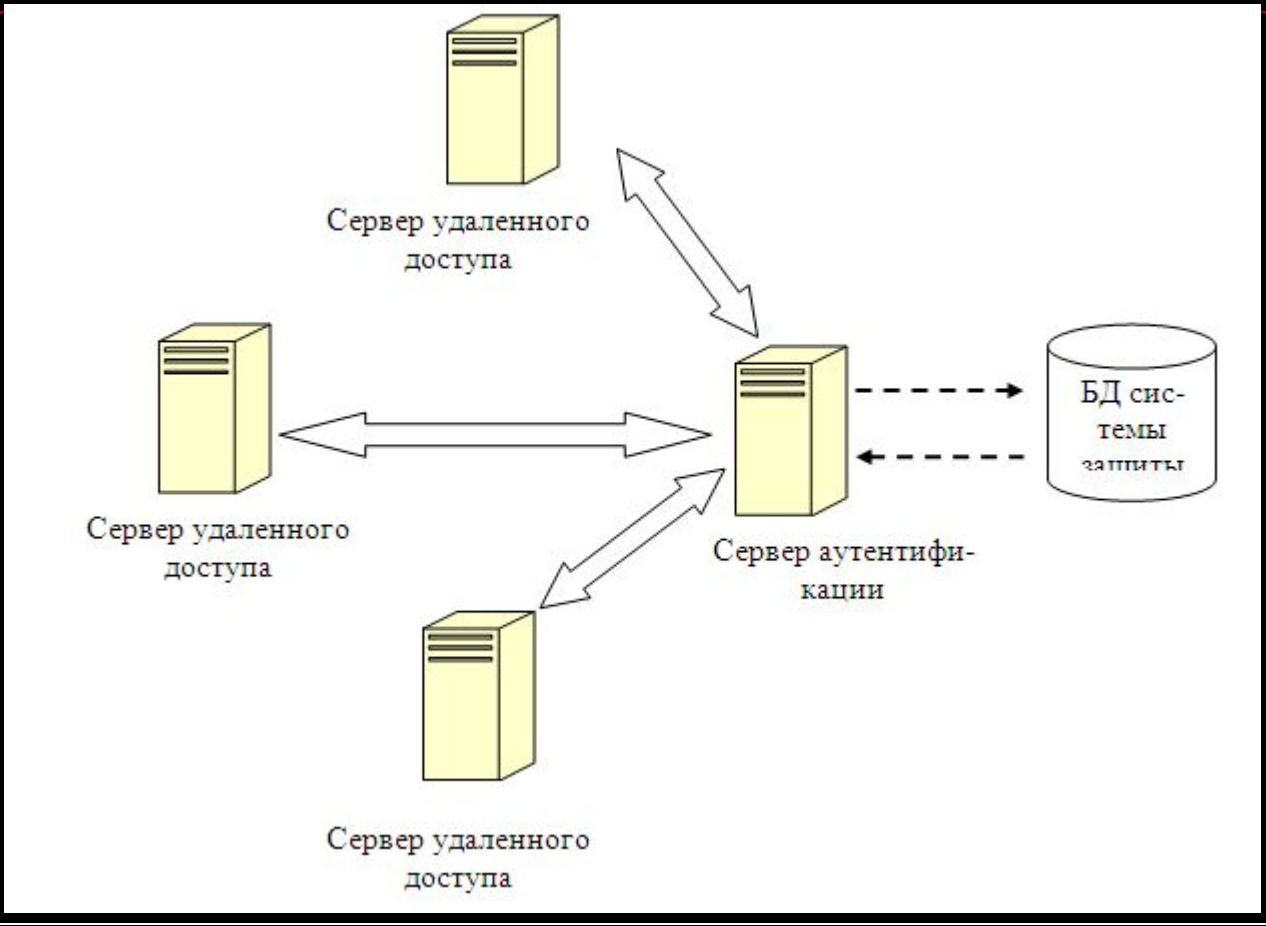
Active Directory

Защита программного обеспечения с помощью электронных ключей HASP

Электронные ключи серии
HASP 4

Доменная архитектура в Windows NT. Служба Active Directory

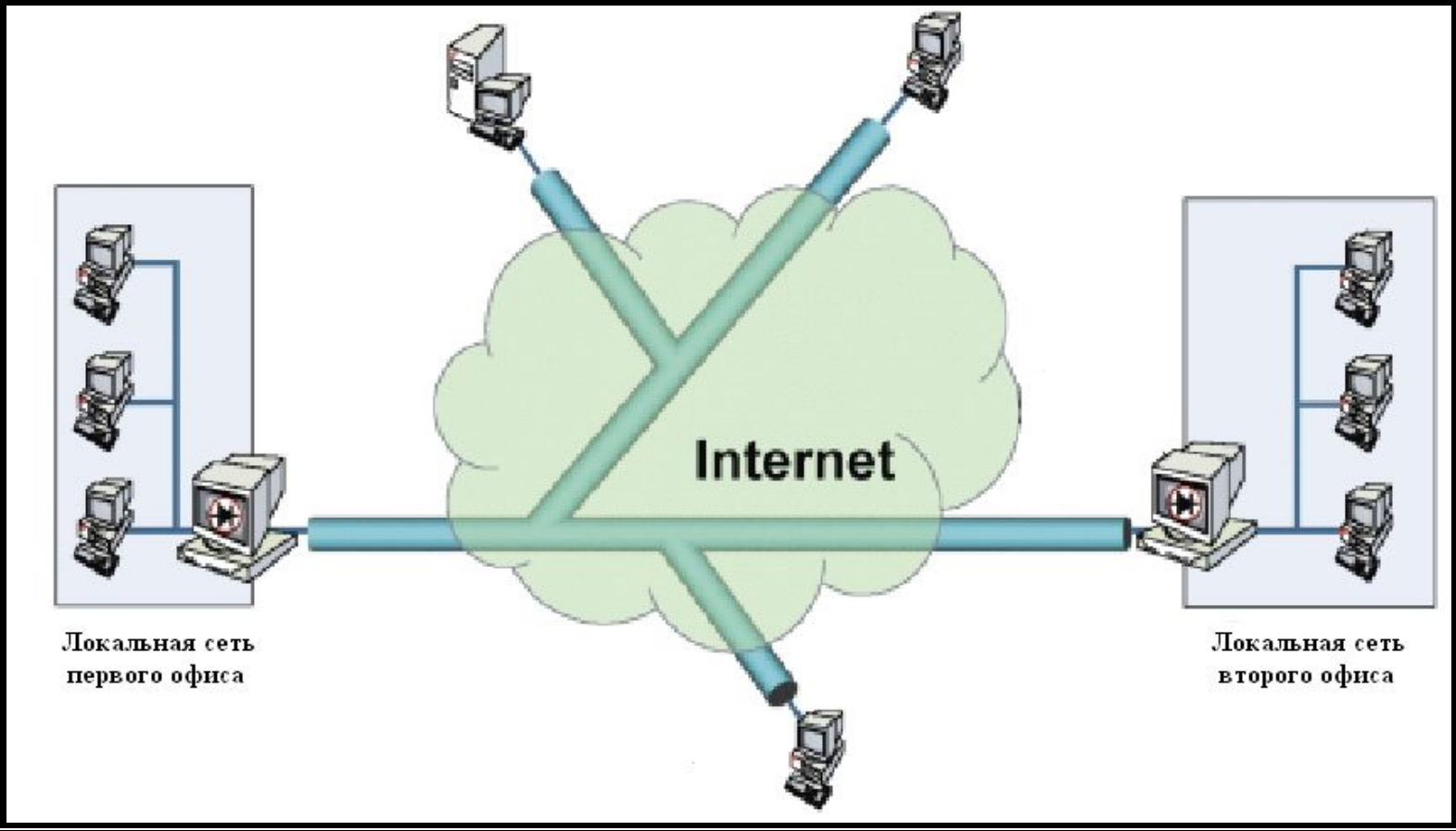
Централизованный контроль удаленного доступа



Основные задачи при взаимодействии через открытые каналы

VPN

VPN


Internet
Локальная сеть
первого офиса
Локальная сеть
второго офиса

Протокол SKIP

Лекция 14

Защита программного обеспечения с помощью электронных ключей HASP

Электронные ключи

Разработка фирмы Aladdin представляют собой современное аппаратное средство защиты ПО от несанкционированного использования.

Базовой основой ключей HASP является специализированная заказная микросхема (ASIC – Application Specific Integrated Circuit), имеющая уникальный для каждого ключа алгоритм работы и функцию шифрования и связанную с ней функцию отклика *f*(*x*), принимающую на вход 32-битный аргумент и формирующая на выходе четыре 32-битных значения.

Модели семейства ключей HASP

- HASP4 Standard;
- MemoHASP;
- TimeHASP;
- NetHASP.

Система защиты HASP Standard позволяет осуществлять

- проверку наличия HASP Standard;
- проверку соответствия выходов, формируемых функцией отклика *f(x)* для различных значений *x*, эталонным значениям;
- использовать функцию шифрования электронного ключа для шифрования и дешифрования своего исполняемого кода, используемых данных и т.д.

MemoHASP

Добавлена встроеная в них энергонезависимой памяти (EEPROM), доступной для чтения и записи во время выполнения защищенной программы.

Модификации данных ключей

- HASP4 M1 – 112 байт EEPROM, возможность одновременной защиты до 16 программ.
- HASP4 M4 – 496 байт EEPROM, возможность одновременной защиты до 112 программ.

С помощью MemoHASP могут быть реализованы

- Хранение в энергонезависимой памяти MemoHASP конфиденциальной информации – ключей шифрования, части исполняемого кода и т.д.
- Хранение в энергонезависимой памяти информации о модулях защищённого программного обеспечения, к которым пользователь имеет доступ и о тех, к которым не имеет (в зависимости от заплаченной суммы за приобретение программы).
- Хранение в энергонезависимой памяти информации о количестве запусков программы, либо об оставшемся количестве запусков. Данный подход актуален при создании демонстрационных версий программ, работа с которыми ограничена количеством запусков.

TimeHASP

- Кроме функций MemoHASP, данные ключи обладают встроенными часами реального времени с автономным питанием от литиевой батарейки (отражающие время и дату).

- Используя часы реального времени, производитель может защищать свое программное обеспечение по времени использования и на основании этого строить гибкую маркетинговую политику – сдачу программ в аренду, лизинг ПО и периодический сбор платы за его использование и т.д.

NetHASP

- Данные ключи имеют в своем составе все компоненты MemoHASP и предназначены для защиты ПО в сетевых средах.
- Один ключ, установленный на любом компьютере сети, способен защитить ПО от тиражирования, а также ограничить количество рабочих мест (лицензий), на которых ПО используется одновременно.
- Ключ может работать на выделенном либо невыделенном сервере, либо любой станции. Он поддерживает различные протоколы – IPX/SPX, NetBIOS, NetBEUI, TCP/IP.

Способы внедрения защитных механизмов в ПО с помощью электронных ключей HASP

1. HASP API (с помощью API функций).
2. Пакетный режим (HASP Envelope).

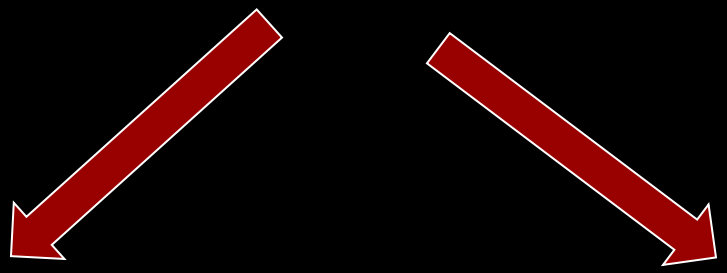
Лекция 15

- Нормативная база РФ
- Показатели защищенности СВТ
- Классы защищенности АС

Руководящие документы Гостехкомиссии России

- "Концепция защиты средств вычислительной техники от несанкционированного доступа к информации"
- "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации"
- "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации"

Критерии безопасности



показатели защищенности средств вычислительной техники (СВТ) от НСД

критерии защищенности автоматизированных систем (АС) обработки данных

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
Дискреционный принцип контроля доступа		+	+	=	+	=
Мандатный принцип контроля доступа		-	+	=	=	=
Очистка памяти		+	+	+	=	=
Изоляция модулей		-	+	=	+	=
Маркировка документов		-	+	=	=	=
Защита ввода и вывода на отчужденный физический носитель информации		-	+	=	=	=
Сопоставление пользователя с устройством		-	+	=	=	=
Идентификация и аутентификация		=	+	=	=	=
Гарантии проектирования		+	+	+	+	+
Регистрация		+	+	+	=	=
Взаимодействие пользователя с КСЗ		-	-	+	=	=
Надежное восстановление		-	-	+	=	=
Целостность КСЗ		+	+	+	=	=
Контроль модификации		-	-	-	+	=
Контроль дистрибуции		-	-	-	+	=
Гарантии архитектуры		-	-	-	-	+
Тестирование		+	+	+	+	=
Руководство пользователя		=	=	=	=	=
Руководство по КСЗ		+	=	+	+	=
Текстовая документация		+	+	+	+	=
Конструкторская (проектная) документация		+	+	+	+	+

Лекция 16

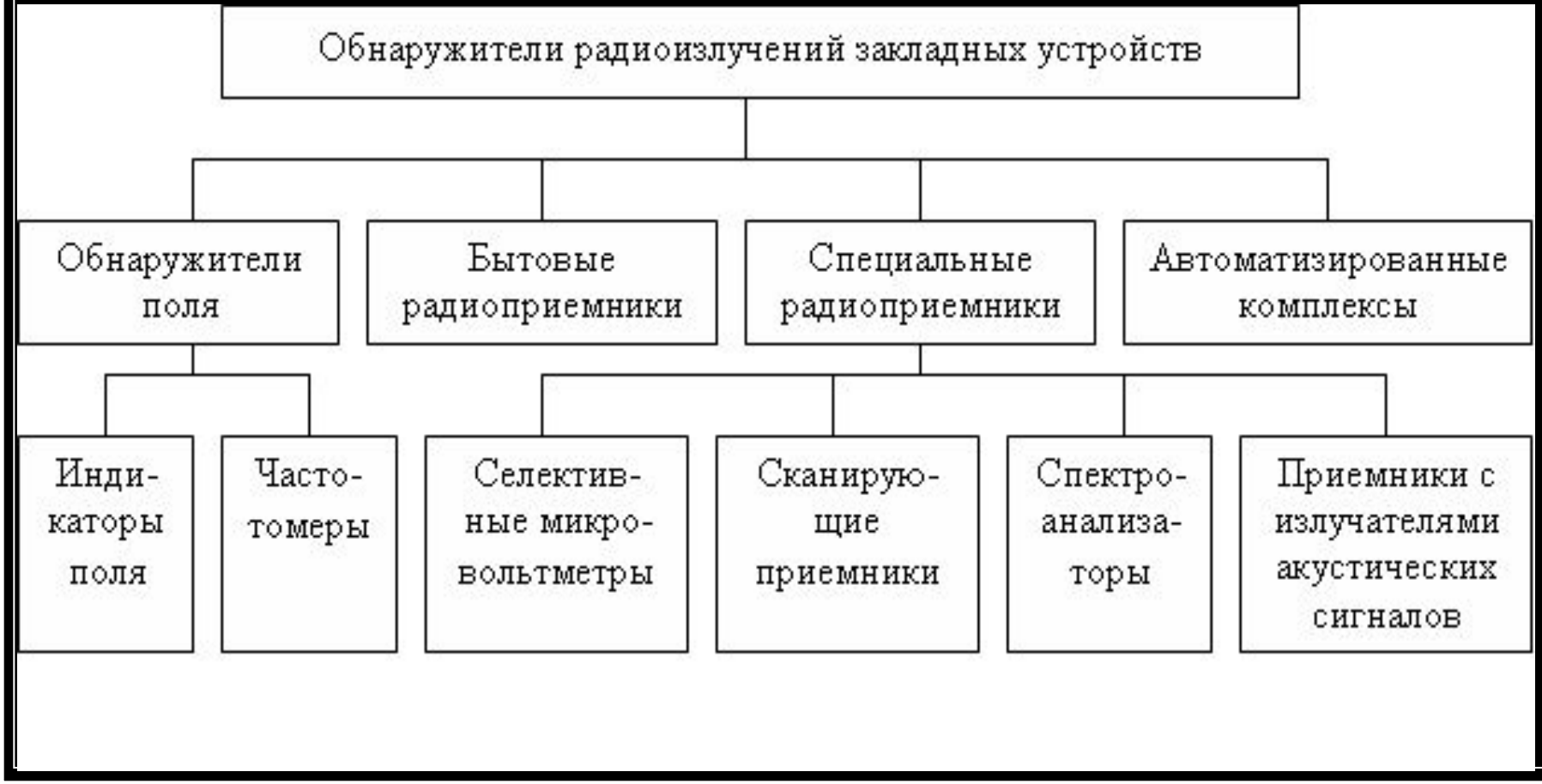
Инженерно-техническая защита информации

Классификация технических каналов

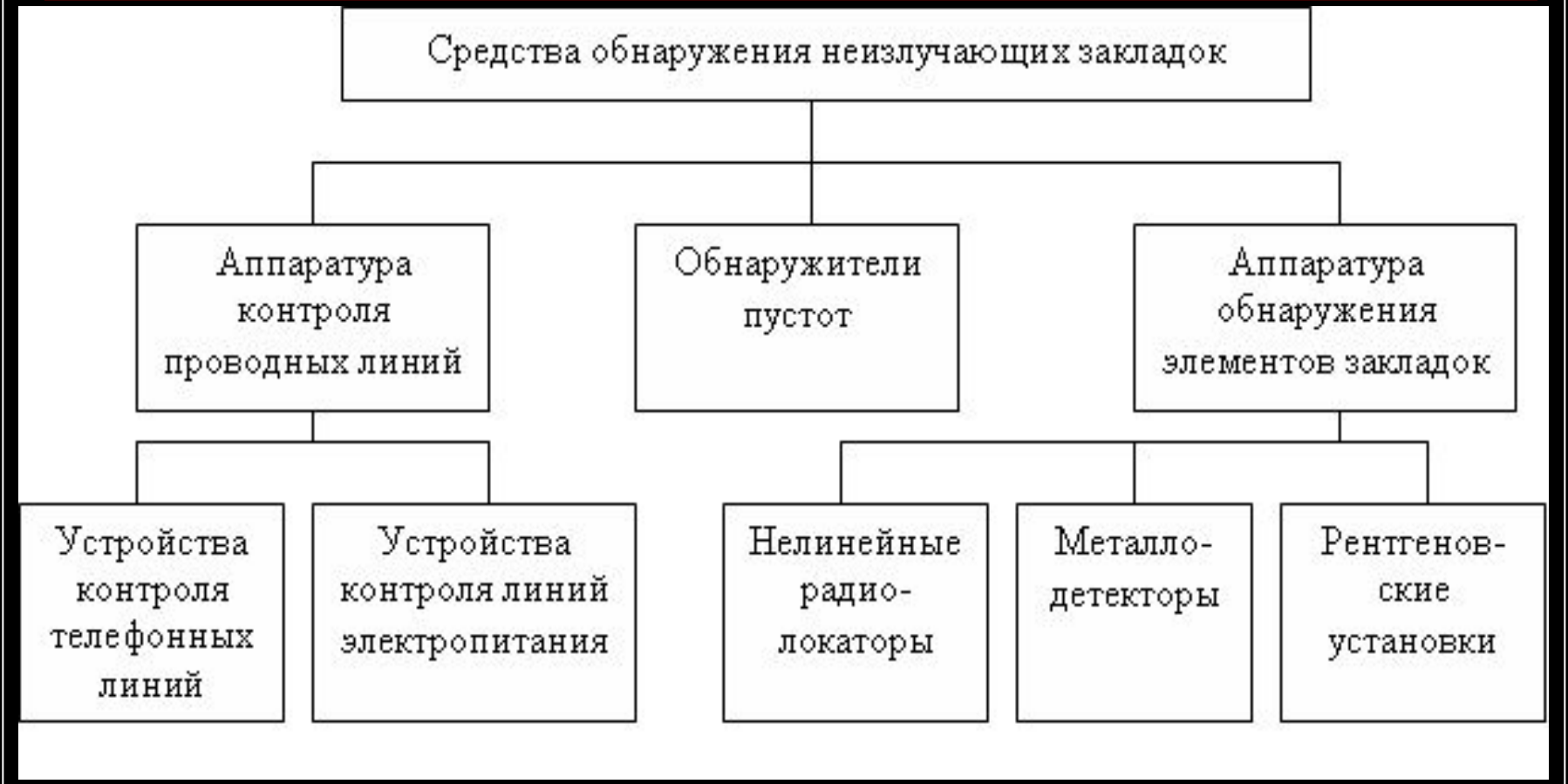
Основные группы технических средств перехвата информации

- Радиопередатчики с микрофоном
- Электронные "уши"
- Устройства перехвата телефонных сообщений
- Устройства приема, записи, управления
- Видеосистемы записи и наблюдения
- Системы определения местоположения контролируемого объекта
- Системы контроля компьютеров и компьютерных сетей

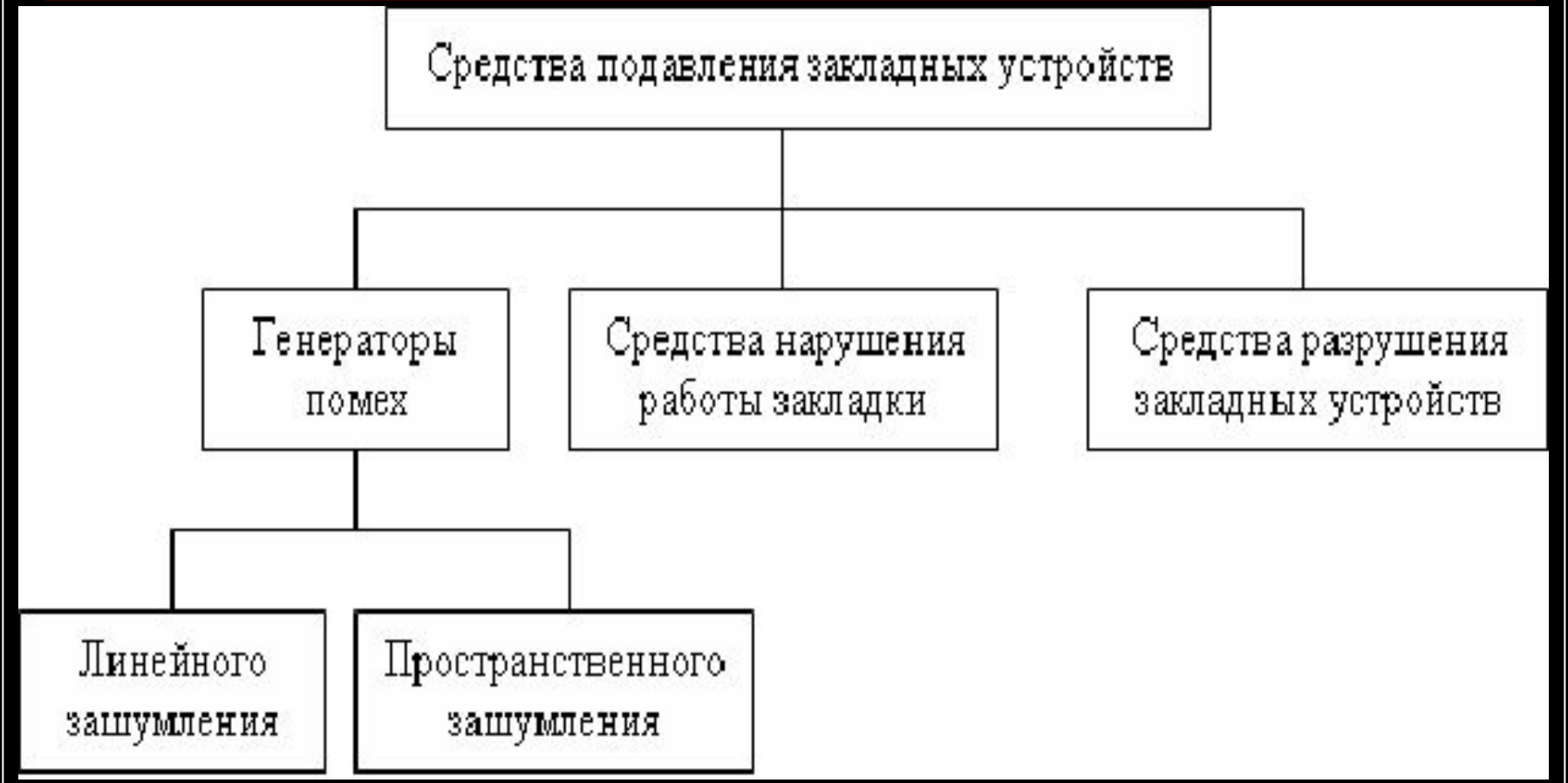
Классификация обнаружителей радиоизлучений закладных устройств



Классификация средств обнаружения неизлучающих закладок



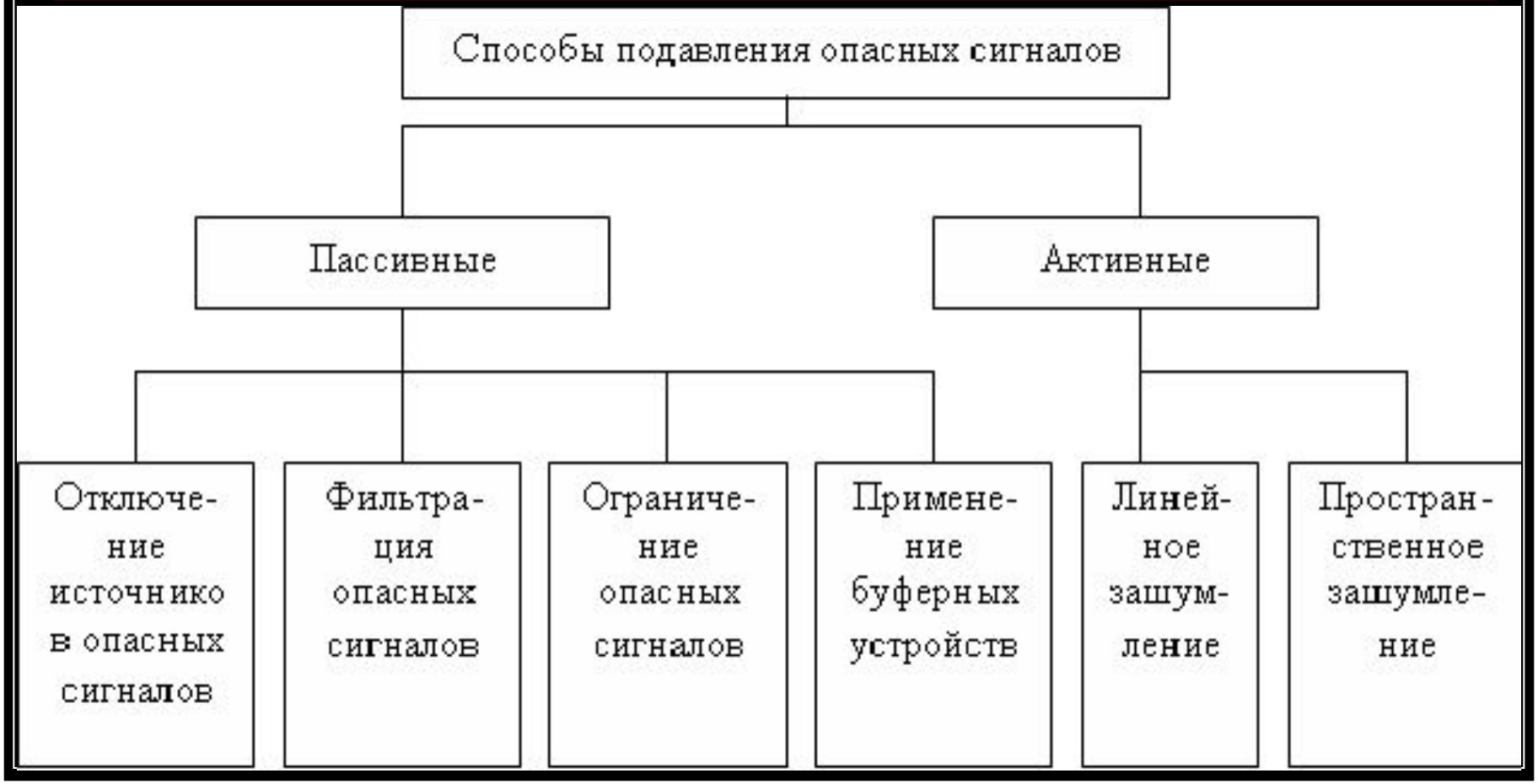
Классификация средств подавления закладных устройств



Противодействие перехвату речевой информации

- Информационное скрытие
- Энергетическое скрытие
- Обнаружение, локализация и изъятие закладных устройств

Способы подавления опасных электрических сигналов



Лекция 17

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Особенность современного развития цивилизации

- информационные ресурсы
- инфокоммуникационные системы

Первый закон

Федеральный закон Российской Федерации «Об информации, информатизации и защите информации»

№ 24-ФЗ от 20.02.95.

Информация

- сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления

Информатизация

- организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов

Документированная информация (документ)

- зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать

«Информационная война»

- особый вид отношений между государствами, при котором для разрешения существующих межгосударственных противоречий используются методы, средства и технологии силового воздействия на информационную сферу этих государств

Особенность информационной войны

- скрытность
- латентность

Информационное оружие

- стратегическое
- оперативное
- тактическое

«Хакерская» война

- организация атак на вычислительные системы и сети специально обученными лицами

Элементы негативных действий

- уничтожение
- блокирование
- модификация и копирование информации
- нарушение работы средства

Законодательная база информационного права

- «Доктрина информационной безопасности
- «Об информации»
- «О государственной тайне»
- «О связи»
- «Об оружии»
- «О безопасности»
- кодексы
  - «Уголовный»
  - «Уголовно - процессуальный»
  - «Гражданский» и др

Основные информационно-правовые статьи «Уголовного кодекса»

- Ст. 272 УК РФ – «Неправомерный доступ к компьютерной информации»
- Ст. 273 УК РФ – «Создание, использование и распространение вредоносных программ для ЭВМ»
- Ст. 274 УК РФ – «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»