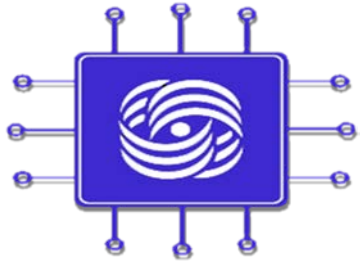


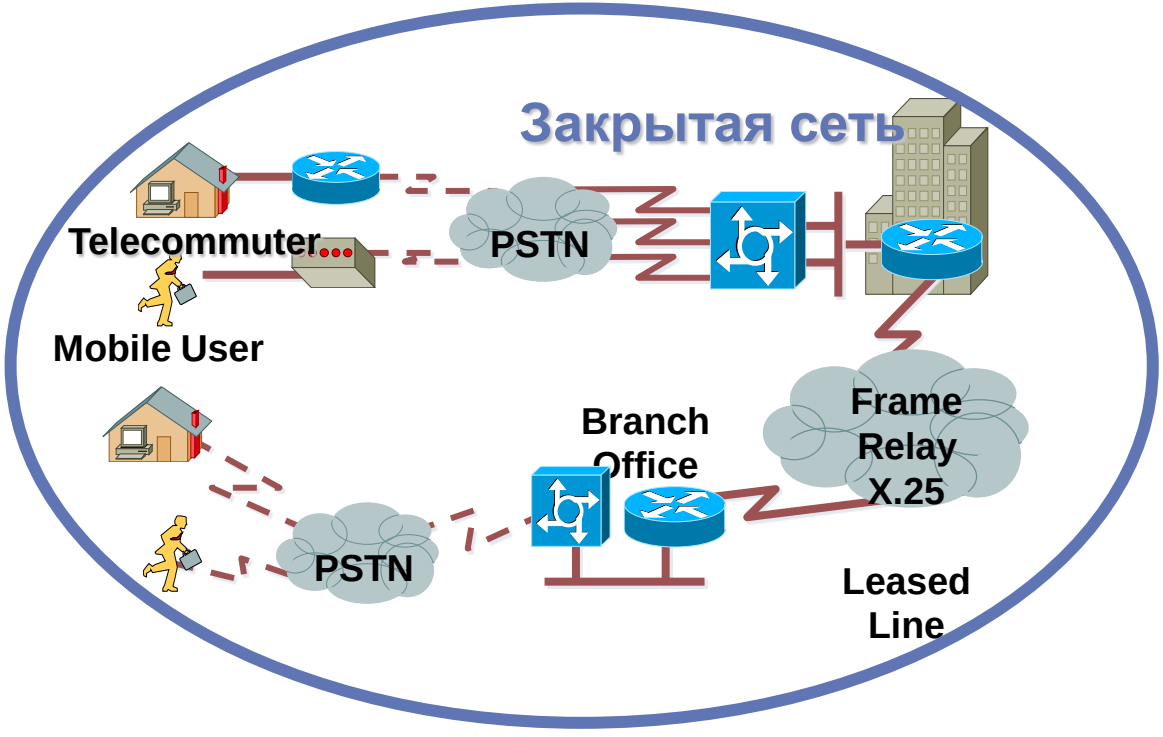
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В СЕТЯХ Передачи Данных

(учебник: Компьютерные сети, Том 2, стр.147-184)

Введение в компьютерные сети

чл.-корр. РАН Смелянский Р.Л.
Кафедра АСВК
ф-т ВМК МГУ

Сети 90-х

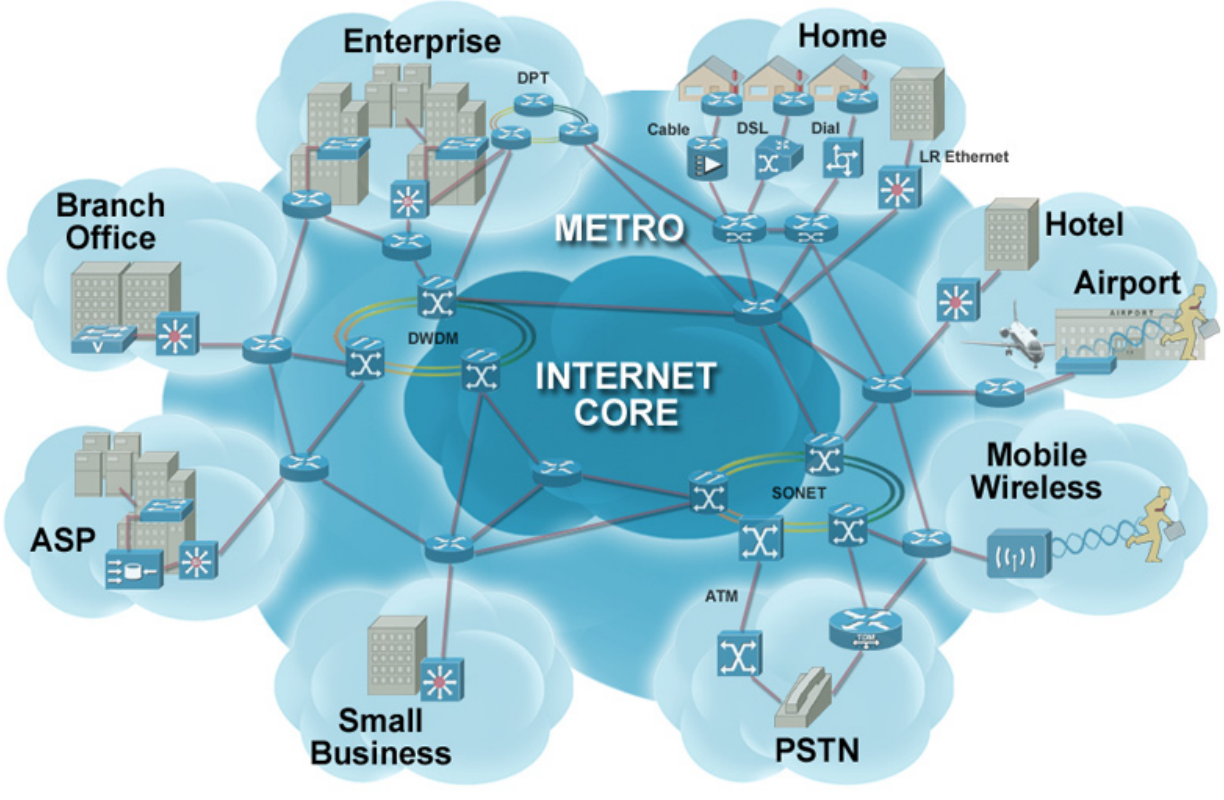


Изолированная и безопасная среда

- **Несколько безопасных соединений с WAN сетью**
- **Безопасные хосты с антивирусной защитой**

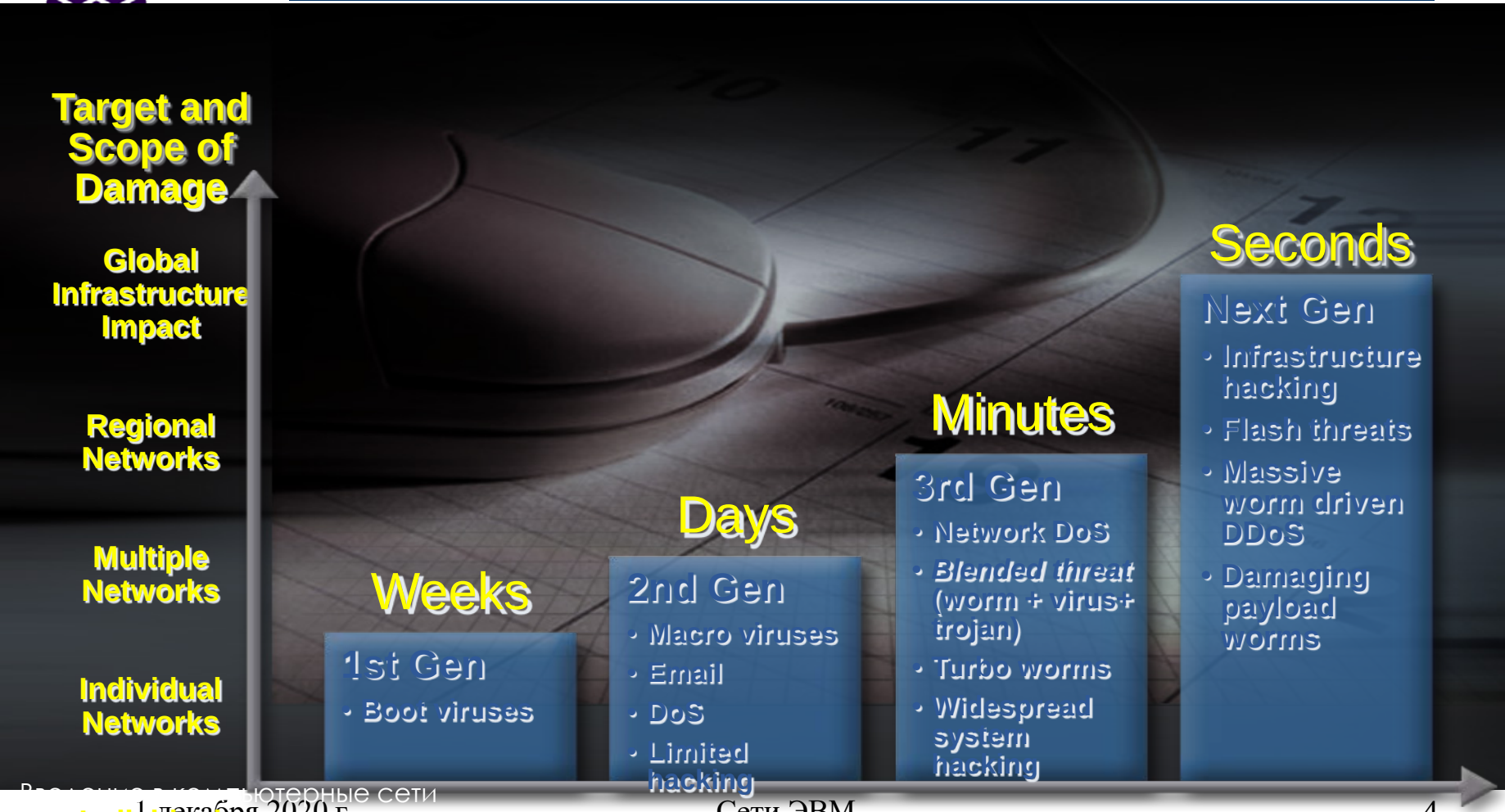
Средства безопасности были рассчитаны на подобные сети

Сети 00-х



- Доступ в сеть возможен из многих точек
- ЦОД где «смешиваются» потоки данных и ПО
- Мобильность сотрудников
- Появление технологий типа VLAN и IPTV, VoIP
- Растущий ущерб от ВПО

Эволюция угроз



Атака на физическую инфраструктуру

27 сентября 2010 в 01:48 Иранская АЭС подверглась атаке компьютерного вируса.

Первая иранская атомная электростанция в Бушере стала жертвой компьютерного вируса. Власти Ирана возложили ответственность за кибератаку на компьютерные сети Израиля.

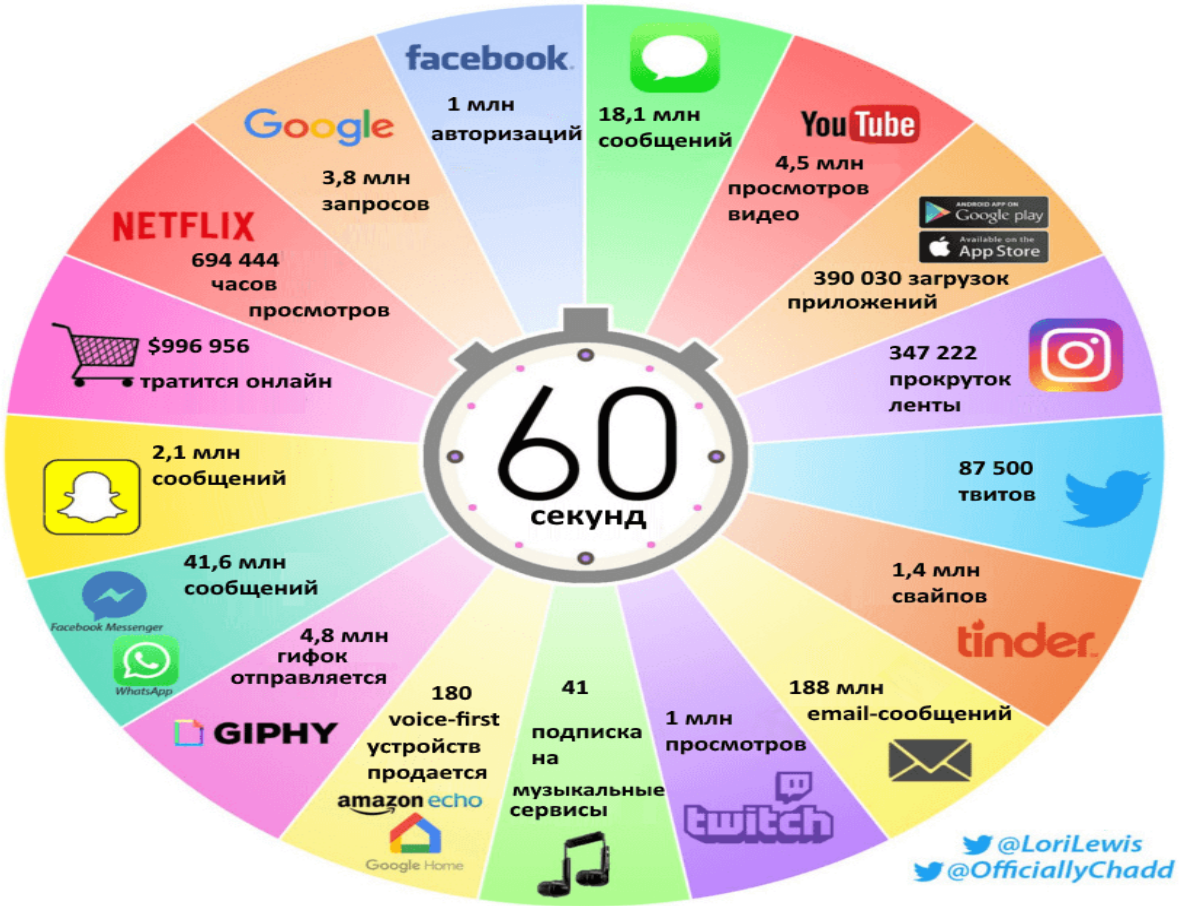
Компьютерный вирус, атаковавший более 30 тысяч компьютеров, на длительное время вывел из строя первую иранскую АЭС.

2017 Год: Казино взломали через аквариум

Завод заразили через кофеварки

Одна минута в Интернете

2019



Немного фактов

- **Сбербанк оценил ущерб экономике России от кибератак в 2019 году в 2,5 трлн рублей**
- Согласно данным Windows Defender Security Intelligence, самой часто встречающейся категорией нежелательного ПО стали трояны (10%).
- Самый серьезный вид угроз в почтовых ящиках пользователей – фишинг (53%). 180-200 миллионов фишинговых писем обнаруживались ежемесячно. В России было обнаружено 7,01 (в мире – 5,85) фишинговых сайтов на каждую 1000 хостов.
- В 2018 года клиника Hancock Health в США подверглась хакерской атаке вируса-шифровальщика SamSam, который парализовал её работу в самый разгар эпидемии гриппа в штате. Руководство больницы заплатило выкуп в размере 4 биткоинов, что на момент выплаты составила порядка $55 тыс.

Ботнеты (zombie army)

Некоторое количество хостов с запущенными на них ботами – автономным ПО, предназначенным для передачи ВПО на другие узлы сети.

Наиболее часто используются для:

- Кражи финансовой информации пользователей;
- Являются объектом купли-продажи
- Организации DDOS-атак;
- Рассылки спама;
- Хостинга ВПО;

Недавние крупные ботнеты: Torpig, Zeus botnet, Conficker

Проблемы информационной безопасности

- Конфиденциальность
  - несанкционированный доступ к информации/ресурсам;
  - несанкционированное изменение информации/состояния ресурсов;
- Идентификация подлинности
  - пользователя - имея с кем-то дело через сеть, вы должны быть уверены, что это тот, за кого он себя выдает.
  - документа
- Надежность управления
  - несанкционированное использование ресурсов;
  - отказ от обслуживания.

Угрозы безопасности данных при работе в сети

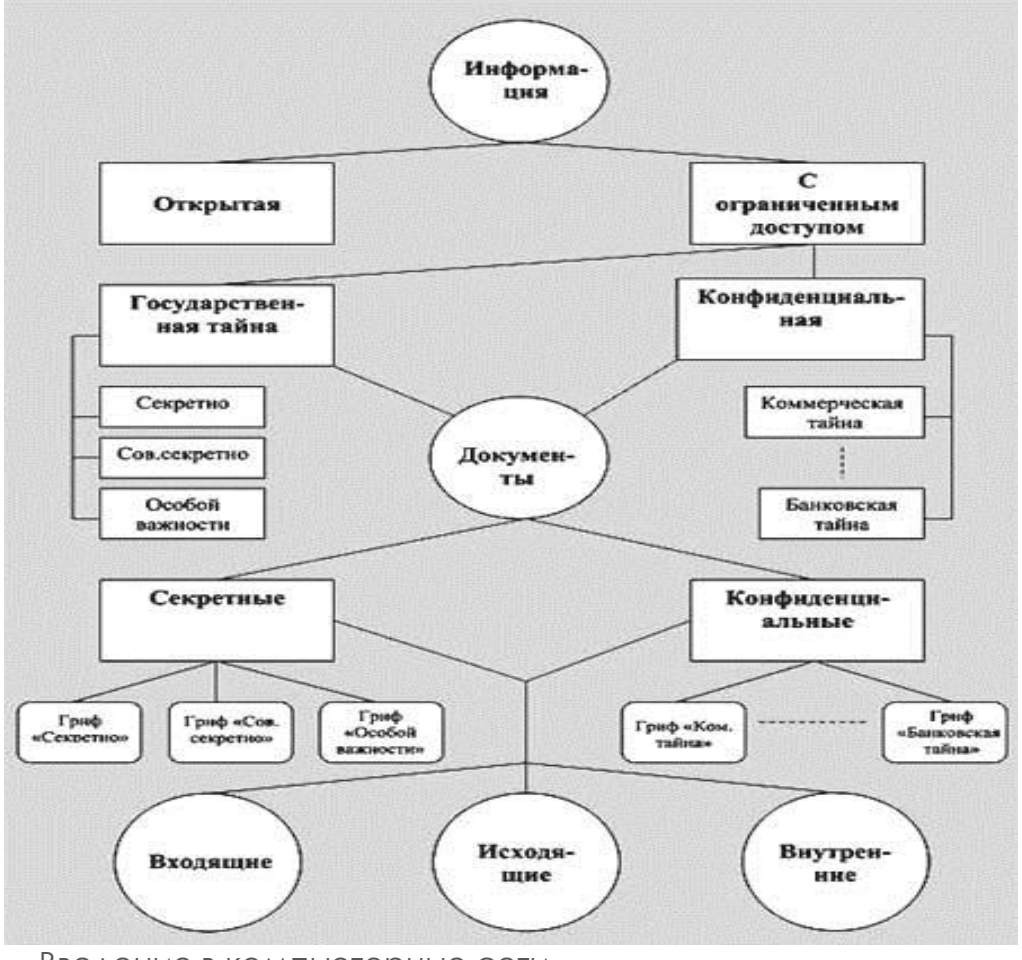
- **При передаче**
- **При хранении**
- **При обработке**
- **При вводе-выводе**.

Термины и определения

(ФЗ 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»)

- **Информация**
- **Документированная информация (документ)**
- **Информационные ресурсы**
- **Конфиденциальность информации**
- **Целостность информации**
- **Доступность информации**
- **Доступ к информации (доступ)**

Термины и определения



Конфиденциальная информация - ***документированная информация***, доступ к которой ограничен в соответствии с законодательством Российской Федерации

Термины и определения

Безопасность информации - состояние информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации, копирования и блокирования

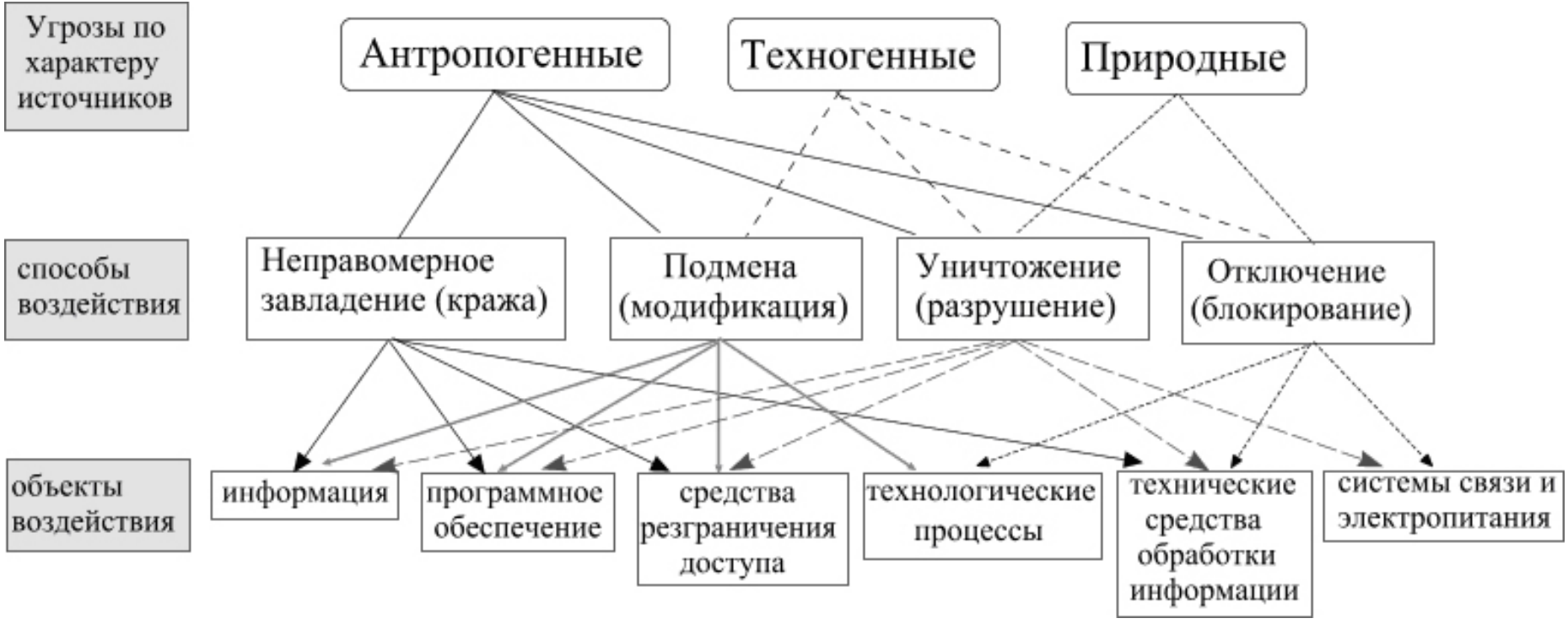
(Руководящий документ "Автоматизированные системы. Защита от несанкционированного доступа к информации. Термины и определения" Гостехкомиссия России 1998г.)

Термины и определения

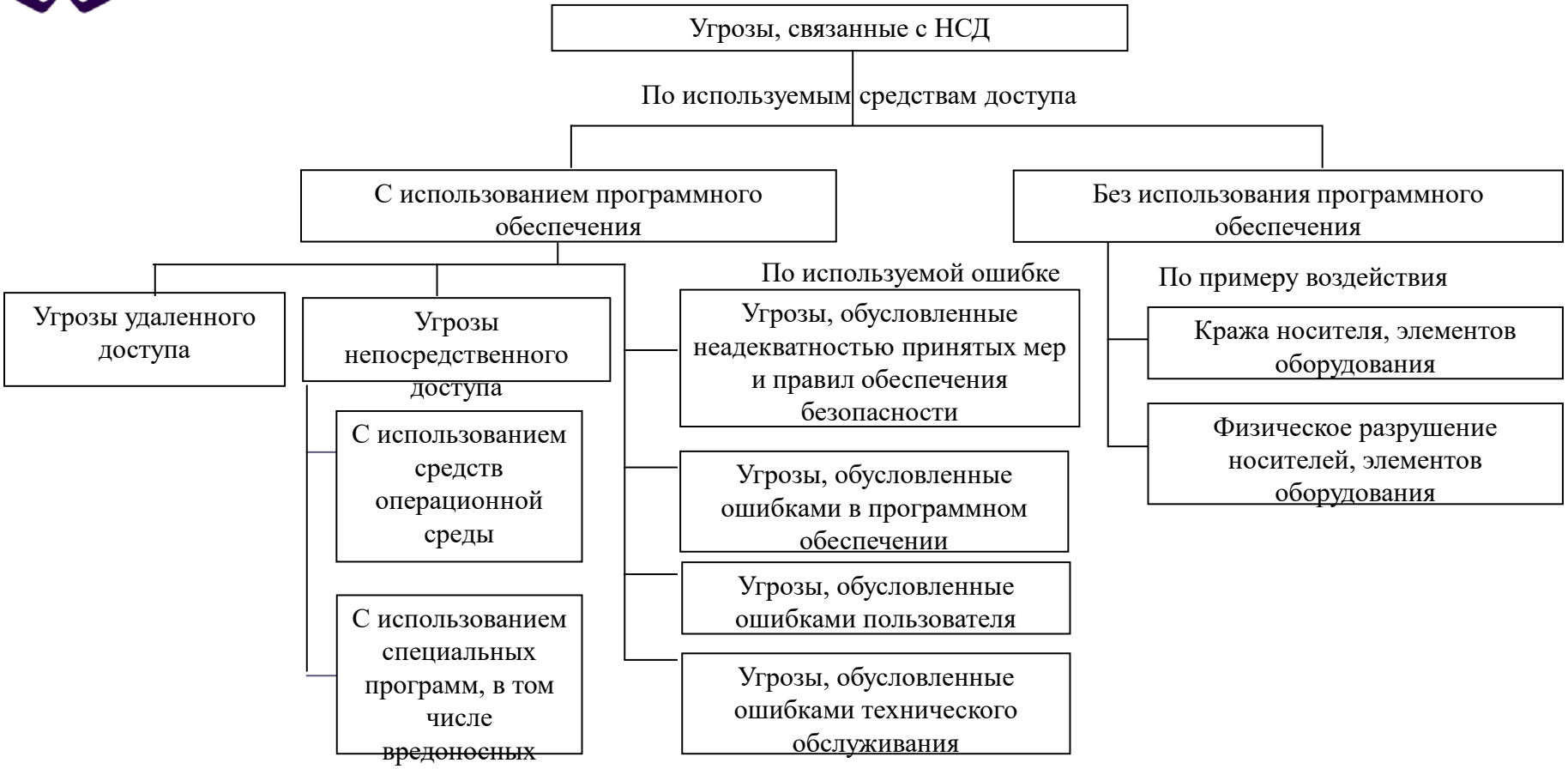
- Защита информации
- Защищаемая информация
- Несанкционированный доступ к информации (НСД)
- Угроза безопасности КС
- Угроза безопасности информации
- Уязвимость информационной системы

- ***Атака на компьютерную систему*** – это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании уязвимости.

Классификация угроз по причинам (источникам) возникновения



Угрозы, связанные с НСД



Ключевые функции системы безопасности СПД (защита от НСД)

- Опознавание *(идентиф икация и аутентиф икация)*
- Регистрация
- Управление доступом
- Изоляция
- Контроль неизменности

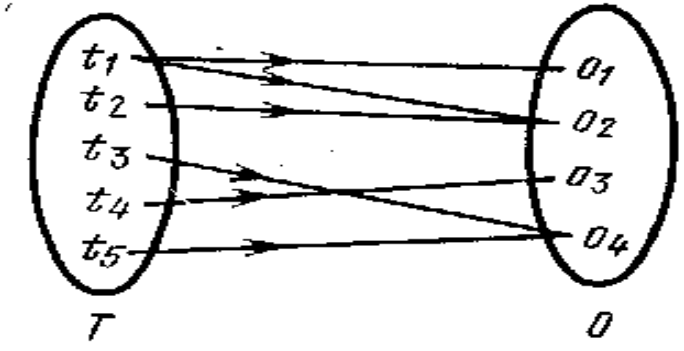
Опознавание и Регистрация:
Термины и определения

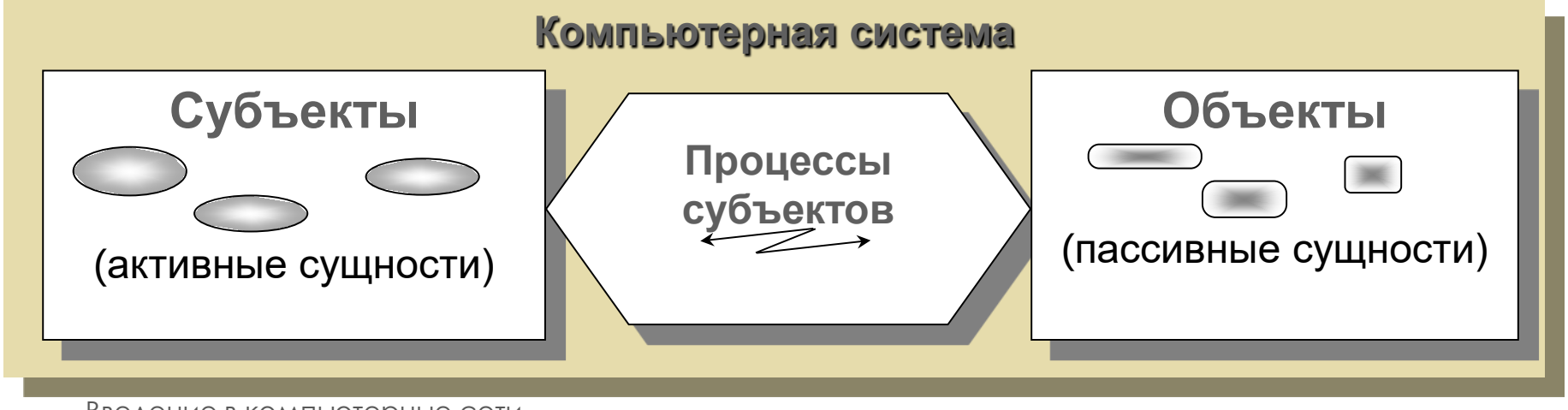
- **Идентификация** — это процесс распознавания элемента объекта/субъекта
- **Аутентификация** - это проверка подлинности объекта/субъекта
- **Авторизация** - процедура предоставления субъекту определенных прав доступа к ресурсам системы
- **Администрирование** - процесс управления доступом субъектов к ресурсам системы.
- - создание идентификатора субъекта (создание учётной записи пользователя) в системе;
- - управление данными субъекта, используемыми для его аутентификации (смена пароля, издание сертификата и т. п.);
- - управление правами доступа субъекта к ресурсам системы.
- **Аудит** - процесс контроля (мониторинга) доступа субъектов к ресурсам системы,

Подтверждение подлинности

Управление доступом.

Субъектно-объектная модель компьютерной системы





Субъектно-объектная модель КС (предположения)

1. В КС действует дискретное время.
2. В каждый фиксированный момент времени tk КС представляет собой конечное множество элементов, разделяемых на два подмножества:
   - подмножество субъектов доступа S;
   - подмножество объектов доступа O.
3. Пользователи КС представлены одним или некоторой совокупностью субъектов доступа, действующих от имени конкретного пользователя.
4. Субъекты КС могут быть порождены из объектов только активной сущностью (другим субъектом).
5. Все процессы в КС могут быть описаны через доступ субъектов к объектам, вызывающими потоки информации.

Субъектно-объектная модель КС (предположения)

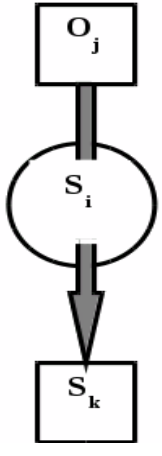
6. В защищенной сети в любой момент времени все объекты и все субъекты должны быть идентифицированы и аутентифицированы.
7. В защищенной КС есть **активный субъект (монитор безопасности)** с ассоциированным **объектом-источником (политика безопасности)**, который осуществляет управление доступом и контроль доступа субъектов к объектам.

8. Для реализации принятой политики безопасности, управления и контроля доступа субъектов к объектам должна существовать информация и объект(ы), ее содержащий(ие) (помимо информации для идентификации и аутентификации пользователей).

Субъектно-объектная модель КС

- Субъекты порождаются субъектами (воздействием в момент времени tk, а новый субъект порождается уже в момент времени tk + 1).
- Объект Of называется источником для субъекта Sm если существует субъект Sj, в результате воздействия кото[illegible]на объект Of возникает субъект Sm.
- Соответственно, субъект Sj , называется активизирую[illegible]для субъекта Sm, а объект Of – ассоциированным с Sm.
- Create (Sj, Of) — Sm

(Если это невозможно, то Create (Sj, Of) — 0)
Create называют операцией порождения субъектов

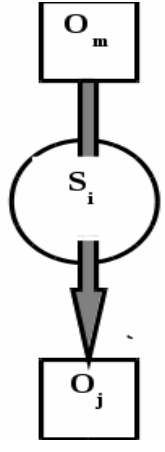


Субъектно-объектная модель КС

Все вопросы безопасности в КС описываются доступами субъектов к объектам, вызывающими потоки информации

Потоком информации между объектом Om и объектом Oj называется произвольная операция над объектом Oj, реализуемая в субъекте Si и зависящая от Om.

Stream(Si Om) → Oj



Поток всегда инициируется (порождается) субъектом.

- **Доступом субъекта Si к объекту Oj** будем называть порождение потока информации между некоторым объектом (например, ассоциированным с субъектом Si объектом Om и объектом Oj.

Субъектно-объектная модель КС

Пусть

P множество потоков при фиксированной декомпозиции КС на субъекты и объекты во все моменты времени (все множество потоков является объединением потоков по всем моментам дискретного времени);
N - подмножество потоков, характеризующее **несанкционированный доступ**;
L - подмножество потоков, характеризующих **легальный доступ**.

Монитор безопасности

- Для разделения всего множества потоков в КС на подмножества L и N необходимо существование активной компоненты (субъекта), который:
- - активизировался бы при возникновении любого потока;
- - производил бы фильтрацию потоков в соответствии с принадлежностью множествам L или N.
- **Монитор безопасности (МБ)** - субъект, активизирующийся при возникновении потока от любого субъекта к любому объекту и который разрешает поток, только из L - множества легального доступа.
- **Политика безопасности** - общий принцип (методология, правило, схема) безопасной работы (доступа) коллектива пользователей с общими информационными ресурсами
- **МБ средство реализации политики безопасности в КС.**

Требования к МБ

- **Полнота:** *Монитор безопасности должен вызываться (активизироваться) при каждом обращении за доступом любого субъекта к любому объекту, и не должно быть никаких способов его обхода.*
- **Изолированность:** *Монитор безопасности должен быть защищен от отслеживания и перехвата своей работы.*
- **Верифицируемость:** *Монитор безопасности должен быть проверяемым (само- или внешне тестируемым) на предмет работоспособности и корректного выполнения своих функций.*
- **Непрерывность:** *Монитор безопасности должен функционировать в любых штатных и нештатных, в том числе и аварийных ситуациях*

Монитор Безопасности

- **Следствие 1.** *В защищенной КС существуют особая категория субъектов (активных сущностей), которые не инициализируют и которыми не управляют пользователи системы – т. н. системные процессы (субъекты), присутствующие (функционирующие) в системе изначально.*
- **Следствие 2** *Ассоциированный с монитором безопасности объект, содержащий информацию по системе разграничения доступа, является наиболее критическим с точки зрения безопасности информационным ресурсом в защищенной КС.*
- **Следствие 3** *В защищенной системе может существовать доверенный пользователь (администратор системы), субъекты которого имеют доступ к ассоциированному с монитором безопасности объекту-данным (политика безопасности) для управления политикой разграничения доступа.*

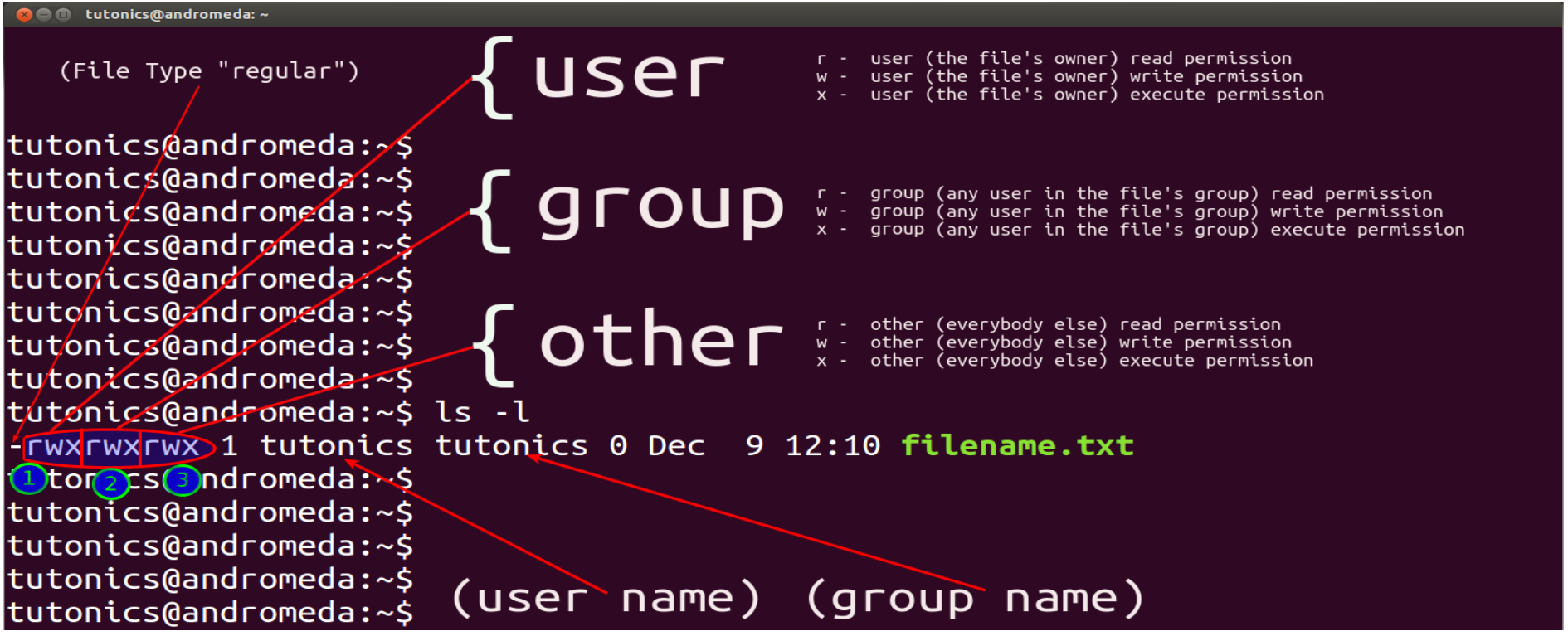
Политики безопасности

- *Базовые политики безопасности – **дискреционная (матричная) и мандатная (полномочий).***

- ***Дискреционная политика** – L задается для именованных пользователей (субъектов) и объектов явным образом в виде дискретного набора троек **"Пользователь(субъект)-поток(операция)-объект« (матрица доступа).***

- ***Политика мандатного** - L задается неявным образом через введение для пользователей-субъектов дискретной характеристики доверия (уровня допуска), а для объектов некоторой дискретной характеристики конфиденциальности (грифа секретности), и наделение на этой основе пользователей-субъектов полномочиями порождать определенные потоки в зависимости от соотношения **"уровень допуска – поток (операция) - уровень конфиденциальности ".***

Политики безопасности



Политики безопасности

Политика тематического доступа.

Множество безопасных (разрешенных) доступов L задается неявным образом через введение для пользователей-субъектов некоторой тематической характеристики - разрешенных тематических информационных рубрик, а для объектов аналогичной характеристики в виде набора тематических рубрик, информация по которым содержится в объекте, и наделение на этой основе субъектов-пользователей полномочиями порождать определенные потоки в зависимости от соотношения

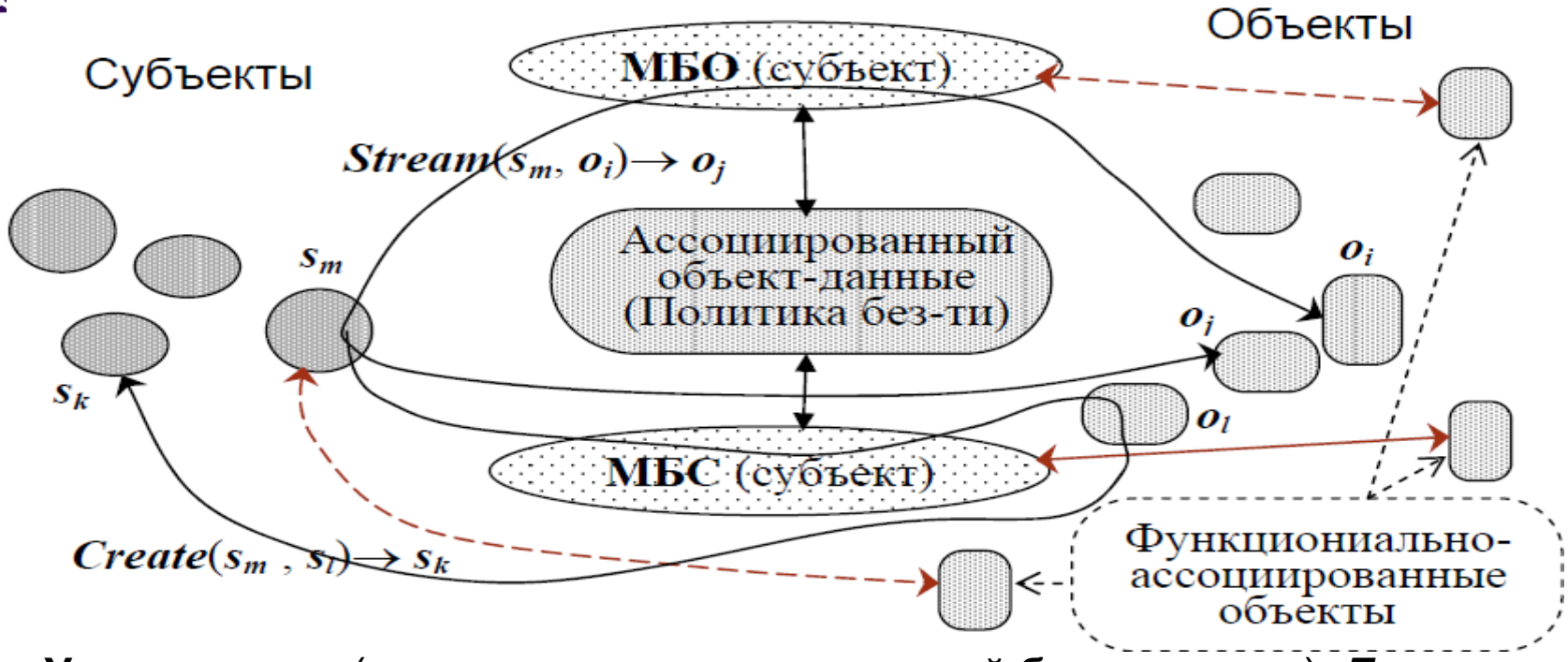
"набор тематических рубрик субъекта - набор тематических рубрик объекта".

Политики безопасности

Политика ролевого доступа.

Множество безопасных (разрешенных) доступов L задается через введение в системе дополнительных абстрактных сущностей - ролей, выступающих некими "типовыми" ролевыми субъектами доступа, с которыми ассоциируются конкретные пользователи (в роли которых осуществляют доступ), и наделение ролевых субъектов доступа на основе дискреционного или мандатного принципа правами доступа к объектам системы.

Схема защищенной системы



Утверждение (достаточное условие гарантий безопасности). *Если в абсолютно изолированной КС существует **МБО** и порождаемые субъекты абсолютно корректны относительно **МБО**, а также существует **МБС**, который абсолютно корректен относительно **МБО**, то в КС реализуется только доступ, описанный политикой разграничения доступа.*

Контроль доступа: Межсетевые экраны

Два абонента взаимодействуют через сеть: как обеспечить контроль доступа на этом уровне?
Концепция межсетевых экранов появилась в конце 80 годов XX века
Типы межсетевых экранов (в порядкеих появления):

- *пакетные фильтры*
- *шлюзы уровня приложений*
- *шлюзы уровня соединения*

Пакетные фильтры

- *Фильтрация на основе полей заголовка IP и некоторых полей транспортного уровня:*
  - *IP адреса отправителя и получателя*
  - *тип протокола*
  - *номера портов отправителя и получателя*
  - *(очень редко) содержимое пакета*
- *Каждый пакет фильтруется независимо от предыдущих*

Шлюзы уровня соединения

- *Умеют отслеживать состояние соединения транспортного уровня (состояние TCP)*
- *Каждый пакет фильтруется в зависимости от состояния соединения – можно описывать правила фильтрации вида:*

```
allow out tcp from 158.250.10.0/24 to any port 80
allow in tcp from any port 80 to 158.250.10.0/24 established
```

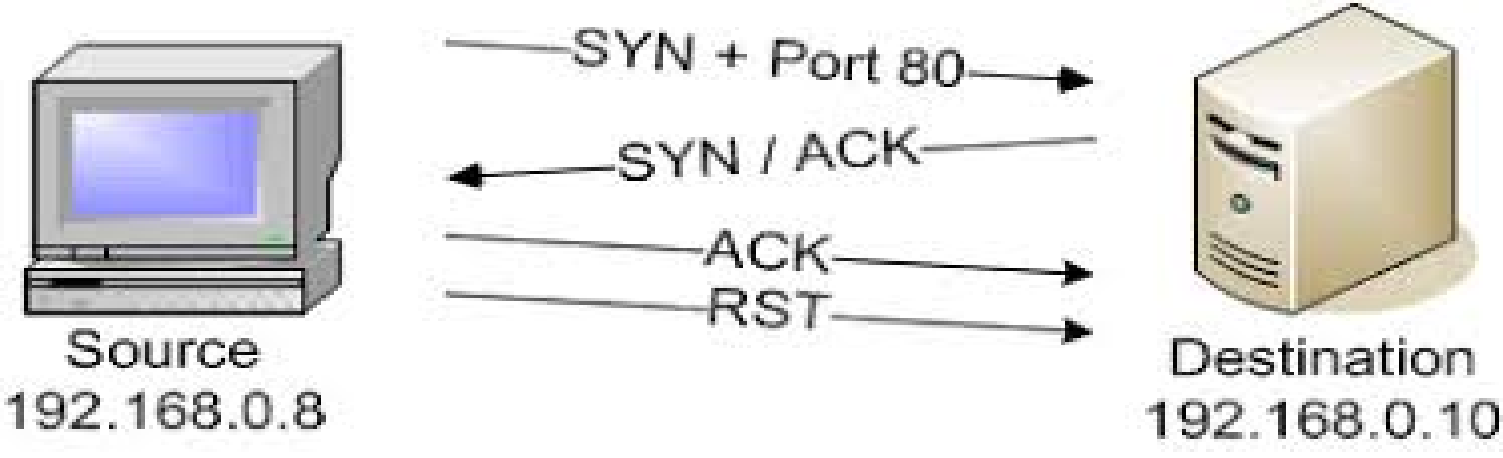
Шлюзы уровня приложений

- Анализ сессий протоколов уровня приложений
  - HTTP прокси
  - FTP прокси
  - и т.д.
- Существует два соединения – от клиента к шлюзу, и от шлюза к серверу
- Для каждого прикладного протокола требуется добавлять поддержку в программное обеспечение шлюза

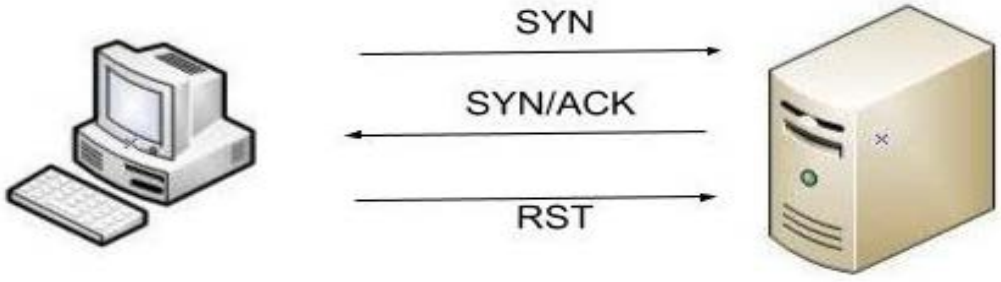
Недостатки межсетевых экранов

- *Пакетные фильтры:*
  - *ограниченные возможности контроля доступа*
  - *уязвимость к атакам подмены значений полей заголовка*
- *Шлюзы уровня приложений:*
  - *высокая вычислительная сложность, нагрузка на аппаратуру*
  - *сравнительно низкая пропускная способность*
- *Общие:*
  - *сложность защиты новых протоколов*
  - *возможность обхода*
  - *незащищенность от вредоносного программного обеспечения и компьютерных атак*

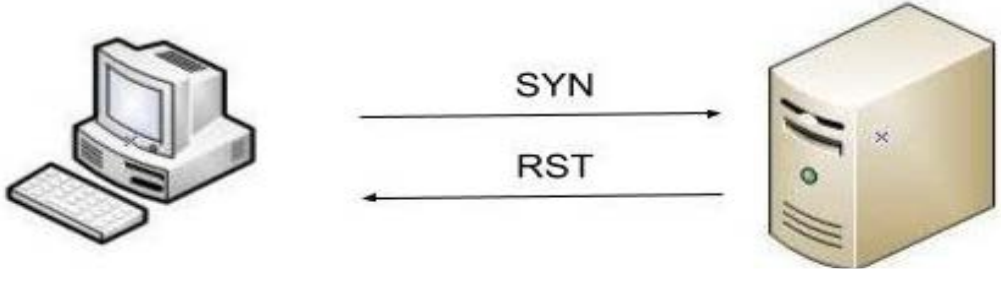
Сканирование портов



Сканирование портов



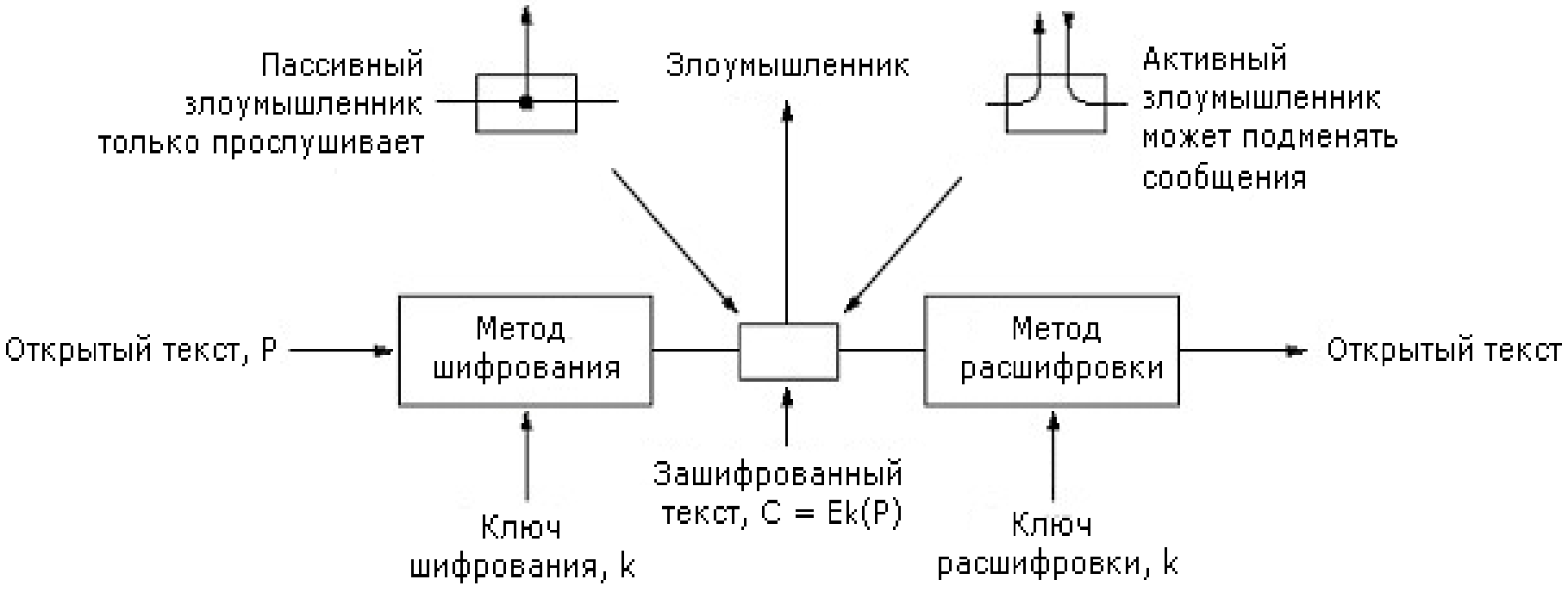
Порт открыт



Порт закрыт

ШИФРОВАНИЕ - КОНТРОЛЬ ДОСТУПА ЧЕРЕЗ ИЗОЛЯЦИЮ ПОТОКОВ ДАННЫХ

Шифрование: модель



Шифрование

- Основная секретность – ключ. Его длина – один из основных гарантов стойкости шифра.
- Публикуя алгоритм шифрования, его автор получает даром консультации многих исследователей в этой области.
- Проблема дешифровки возникает в трех вариантах:
  - есть только шифрограмма;
  - есть шифрограмма и само сообщение;
  - есть фрагменты исходного сообщения и их шифрограммы.
- Шифрование перестановкой vs Шифрование замещением

Шифрование перестановкой

- Шифрование перестановкой состоит в изменении порядка букв **без их изменения**.
- подстановка (123456 – 523146), то слово МОСКВА станет КОСВМА
- Пример, шифрование по столбцам.

Шифрование перестановкой

Ш	У	Т	О	Ч	К	А
7	5	4	3	6	2	1
В	Ы	С	Ы	Л	А	Й
Т	Е	Д	Е	Н	Ь	Г
И	Б	О	Ч	К	А	М
И	_	_	_	_	_	_

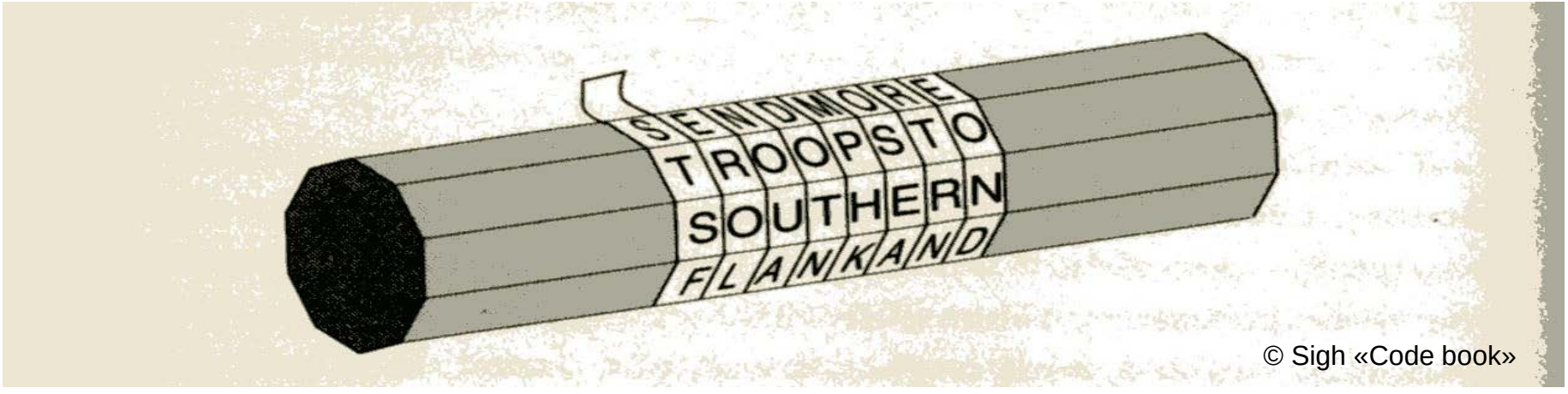
Открытый текст:

высылайтеденьгибочками

Зашифрованный текст:

йгм_аьа_лнк_ыеч_сдо_ыеб_втии

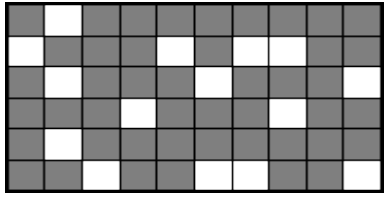
Шифр перестановкой



Шифр Сцитала

Например, используя палочку: по длине окружности - 4 символа , а длина палочки - 6 символов, то текст: «это шифр древней Спарты» превратится в: «эфвптрнао ер дйтшр ыиеС».
Длина блока n = 23, а вектор t, указывающий правило перестановки, для этого шифра может быть записан следующим образом:
t = {1, 7, 13, 19, 2, 8, 14, 20, 3, 9, 15, 21, 4, 10, 16, 22, 5, 11, 17, 23, 6, 12, 18}.

Шифр «Поворотная решетка»



1

	Ш								
И				Ф		Р	Р		
	Е				Ш				Е
			Т				К		
	А								
		Я			В	Л			Я

2

Е	Ш		Т	С			Я		
И				Ф		Р	Р	Ч	
	Е	А			Ш	С			Е
Т			Т	Н			К	Ы	
	А	М	С		Л				У
		Я			В	Л		Ч	Я

3

Е	Ш	А	Т	С	Е	М	Я		Ш
И	И			Ф		Р	Р	Ч	
	Е	А	Ф		Ш	С	Р		Е
Т	А		Т	Н	М		К	Ы	А
Р	А	М	С	Ш	Л	Р	У		У
	Т	Я			В	Л		Ч	Я

4

Е	Ш	А	Т	С	Е	М	Я	Н	Ш
И	И	О	Й	Ф	П	Р	Р	Ч	Е
Р	Е	А	Ф	Е	Ш	С	Р	С	Е
Т	А	Т	Т	Н	М	А	К	Ы	А
Р	А	М	С	Ш	Л	Р	У	Н	У
О	Т	Я	В	К	В	Л	И	Ч	Я

5

ШИФРРЕШЕТКАЯВЛЯЕТСЯЧАСТНЫМСЛУЧАЕМШИФРАМАРШРУТНОЙПЕРЕСТАНОВКИ

Шифрование замещением

- Шифрование замещением – буква или группа букв замещается другой буквой или группой букв из того же самого или другого алфавита.
- Пример, шифр Юлия Цезаря

а б в г д е ё ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я

г д е ё ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я а б в

о пришёл увидел победил

о тулыио целжзо тсдзжло

Полиалфавитный шифр замещением

Блез Виженер

Полиалфавитный шифр замещением

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

ATTACKATDOWN

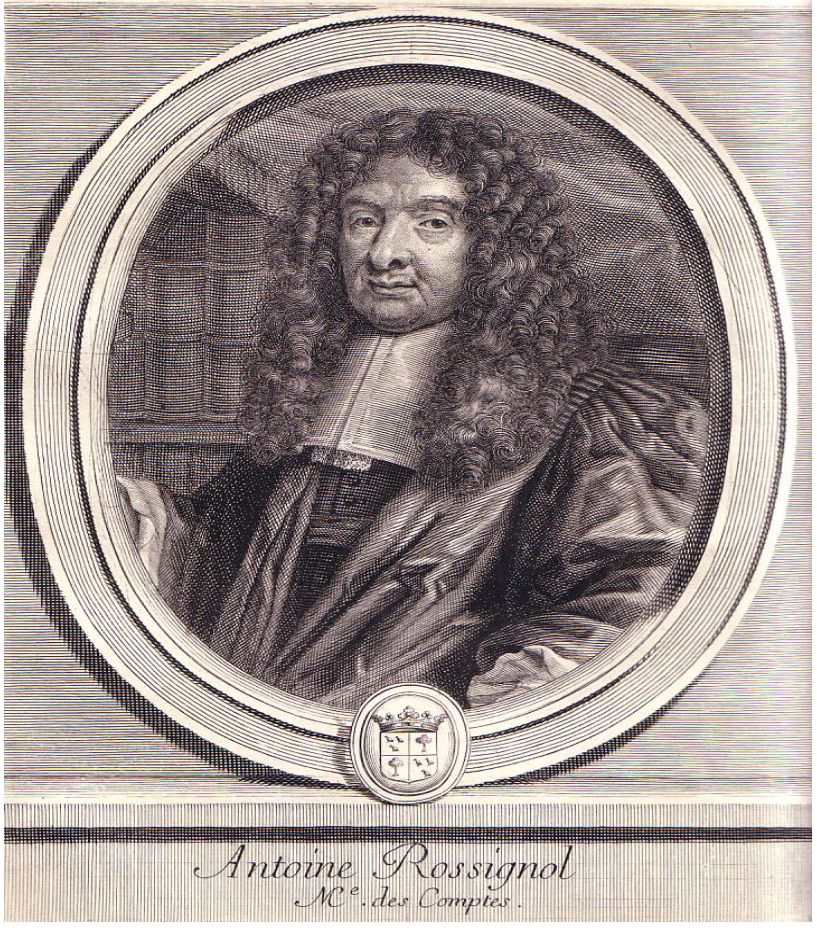
LEMONLEMONLE

LXFOPVEFRNHR

Квадрат Виженера, или tabula recta

Великий шифр Россиньоля

(омофоническая замена)



Омофоническая замена

Table 5 An example of a homophonic substitution cipher. The top row represents the plain alphabet, while the numbers below represent the cipher alphabet, with several options for frequently occurring letters.

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
09	48	13	01	14	10	06	23	32	15	04	26	22	18	00	38	94	29	11	17	08	34	60	28	21	02
12	81	41	03	16	31	25	39	70			37	27	58	05	95		35	19	20	61		89		52	
33		62	45	24			50	73			51		59	07			40	36	30	63					
47			79	44			56	83			84		66	54			42	76	43						
53				46			65	88					71	72			77	86	49						
67				55			68	93					91	90			80	96	69						
78				57										99					75						
92				64															85						
				74															97						
				82																					
				87																					
				98																					

Важные правила шифрования

- Не раскрываемый шифр - одноразовые подложки.
- Рассеивание и перемешивание
  - Цель рассеивания состоит в перераспределении избыточности исходно языка на весь исходный текст.
  - Цель перемешивания состоит в том, чтобы сделать зависимость между ключом и шифртекстом настолько сложной, на сколько это возможно. Криптоаналитик на основе анализа шифртекста не должен получать сколь-нибудь полезной информации о ключе.
- Все шифруемые сообщения должны иметь избыточность, т.е. информацию, которая не нужна для понимания сообщения.
- Надо позаботиться о специальных мерах от активного злоумышленника, который может копировать, а потом пересылать модифицированные копии.

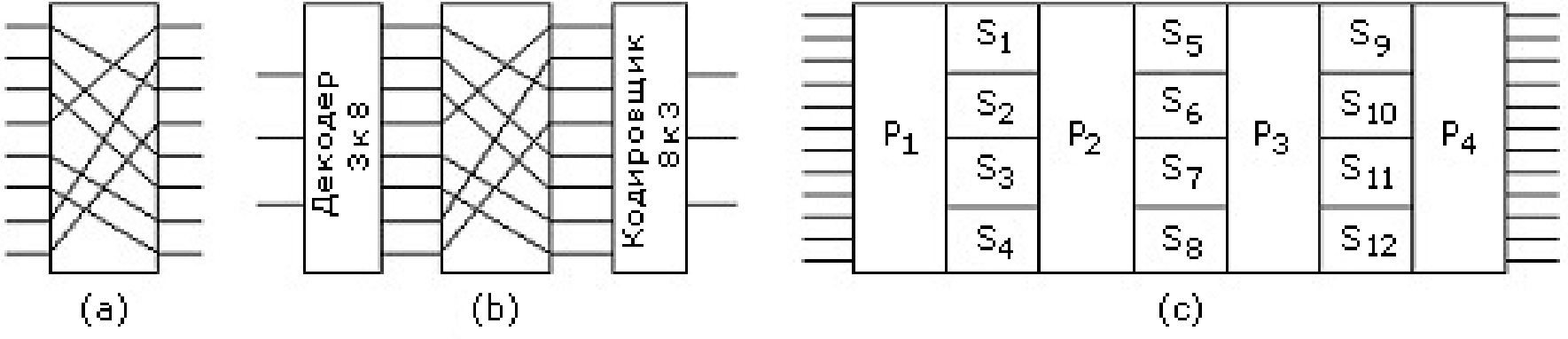
Алгоритмы с секретными ключами

(симметричное шифрование)

- Если раньше алгоритм шифрования был прост, а вся сложность заключалась в ключе, то теперь наоборот стараются алгоритм делать как можно изощреннее.

- Перестановка и замещение реализуются простыми схемами.

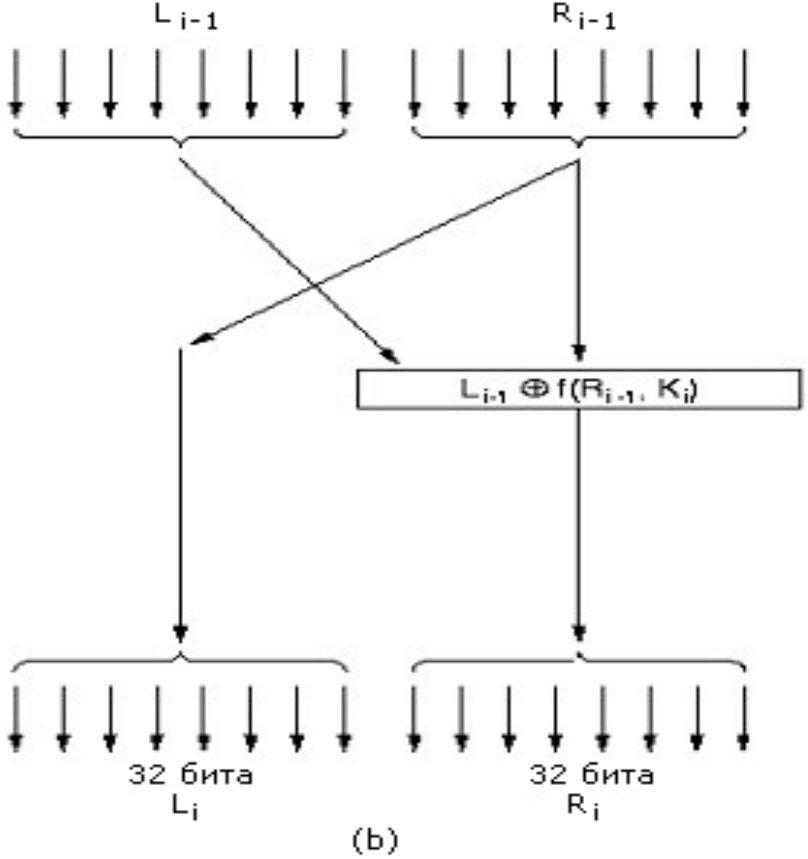
Базовые схемы шифрования



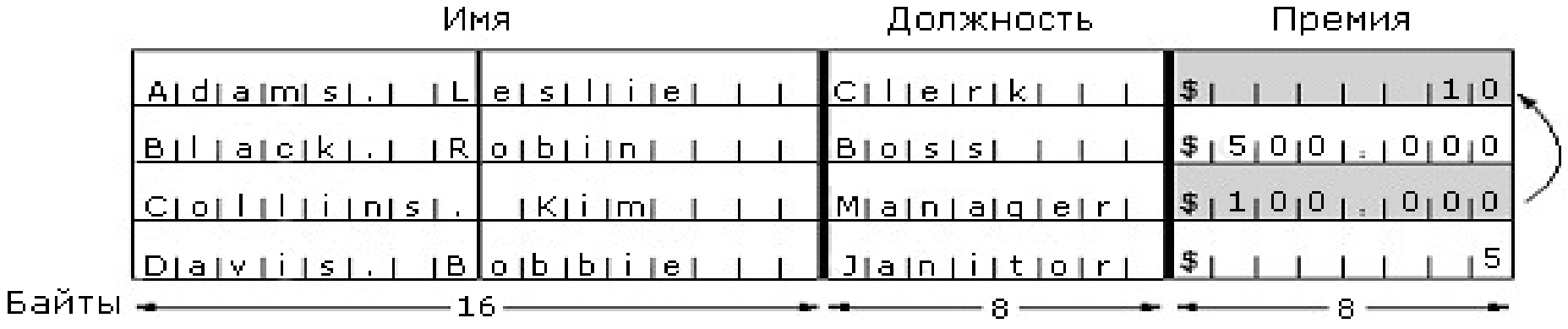
Алгоритм DES

- В январе 1977 правительство США приняло стандарт в области шифрования (Data Encryption Standard), созданный на базе разработки фирмы IBM.
- Предложенный алгоритм – это моноалфавитное замещение с 64 разрядным символом.
  - Шифрование цепочкой.
- Для начала шифрования надо иметь сразу весь исходный текст.
  - Обратная связь по шифру.

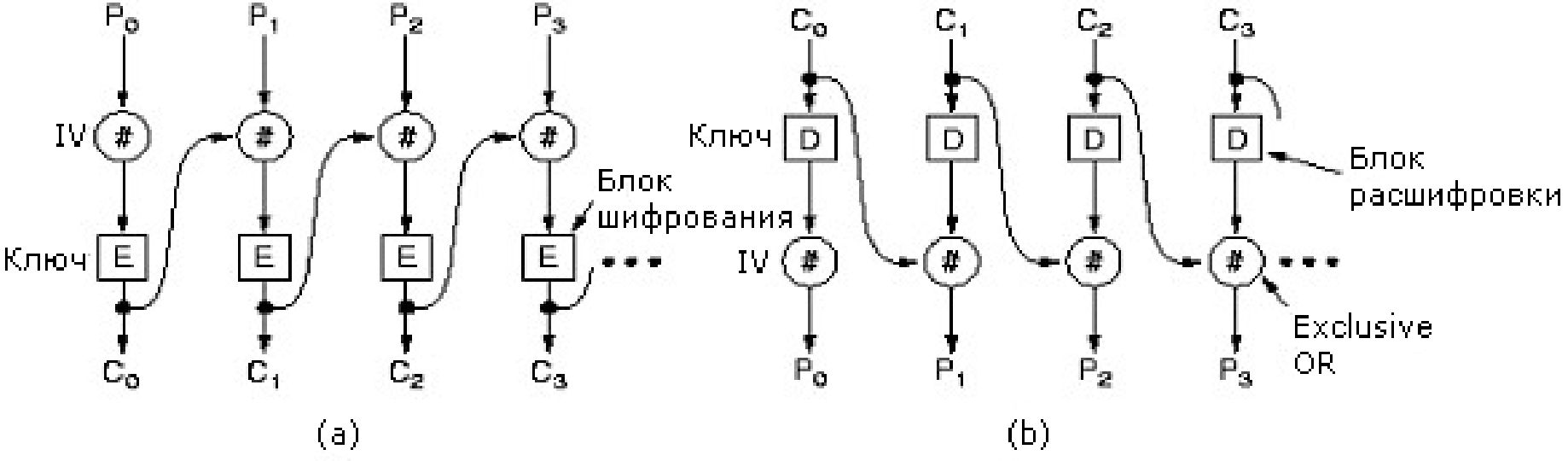
Алгоритм DES



Недостаток блочного моноалфавитного замещения



Поблочная передача зашифрованного текста



Раскрытие DES

- использование двух ключей не дает надежной схемы.

$$C_i = E_{K2}(E_{K1}(P_i)); \quad D_{K2}(C_i) = E_{K1}(P_i)$$

- Процедура взлома:
  - вычислить все возможные однократные шифрования, т.е. применения функции E к шифруемому тексту;
  - вычислить все возможные однократные дешифрации зашифрованного текста;
  - в таблице искать совпадающие строки: пара строк – пара ключей;
  - проверить эту пару на совпадение шифрования; если неудачный результат, продолжить с шага 1.
- Модификация схемы шифрования с двумя ключами в три этапа - схема EDE.

Алгоритмы с открытыми ключами

- Пусть у нас есть алгоритмы *E* и *D*, которые удовлетворяют следующим требованиям:
  - *D(E(P))=P;*
  - Чрезвычайно трудно получить *D*, зная *E;*
  - *E* нельзя вскрыть через анализ исходных текстов.
- Алгоритм шифрования *E* и его ключ публикуют или помещают так, что каждый может их получить, алгоритм *D* так же публикуют, чтобы подвергнуть его изучению, а вот ключи к последнему хранят в секрете.

Алгоритм RSA

- Ривест, Шамир и Адлеман - Алгоритм RSA 1978г. Общая схема этого алгоритма такова
  - Выберем два простых числа p и q (больше 10^{100}).
  - Вычислим $n=p\times q$ и $z=(p-1)\times(q-1)$;
  - Выберем простое d, взаимно простое к z.
  - Вычислим e такое, что $e\times d=1 \bmod z$.
- $C=P^e \pmod n$, (e,n) – это открытый ключ шифрования,
- $P=C^d \pmod n$ расшифровка, (d,n) – это закрытый ключ для расшифровки.

Пример использования алгоритма RSA

Открытый текст (P)		Шифрованный текст (C)			После расшифровки	
Символ	Число	P^3	$P^3(mod33)$	C^7	$C^7(mod33)$	Символ
S	19	6859	28	13492928512	19	S
U	21	9261	21	1601066541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	1	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	5	E
Вычисления отправителя				Вычисления получателя		

Пример для $p=3$, $q=11$, $n=33$, $z=20$, $d=7$ откуда $e=3$.

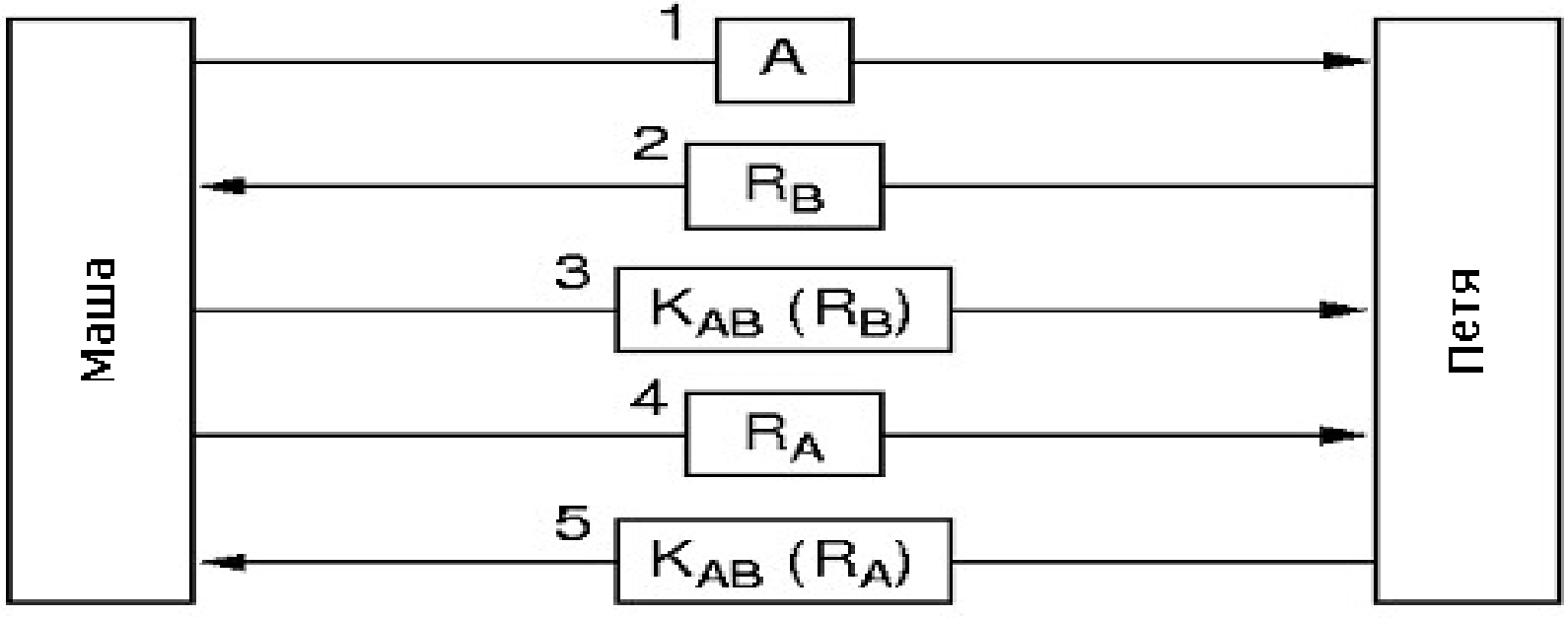
Протоколы аутентификации

Протоколы установления подлинности (аутентификации) позволяют процессу убедиться, что он взаимодействует с тем, кто должен быть, а не с тем, кто лишь представляется таковым.

- Не путать с проверкой прав и полномочий.

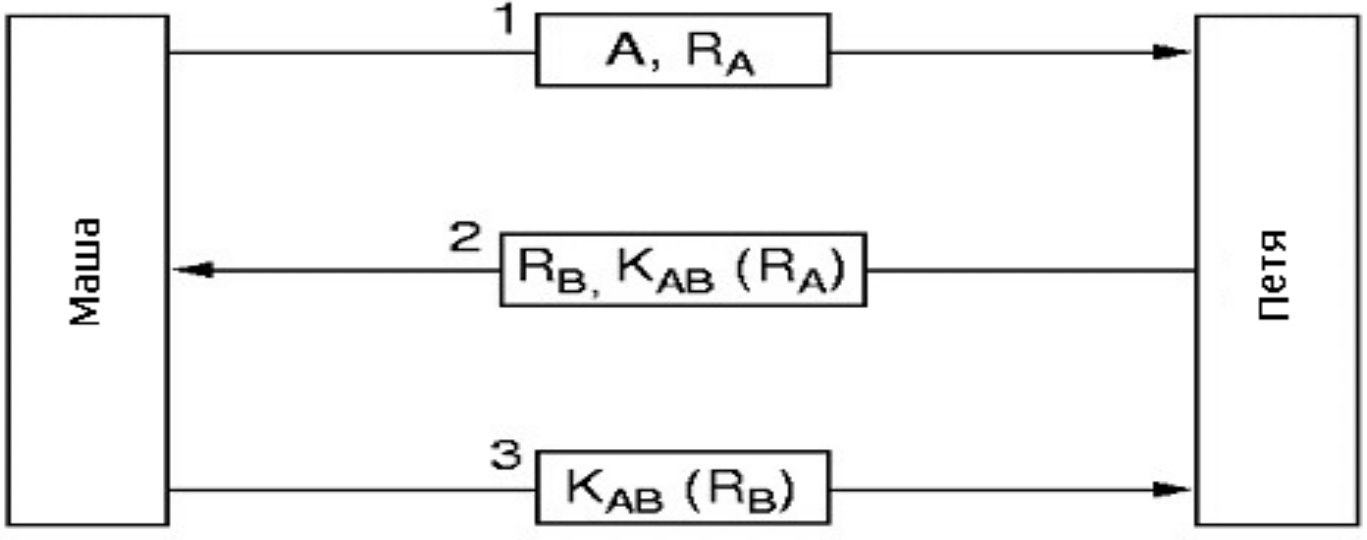
- Общая схема всех протоколов аутентификации такова: A и B начинают обмениваться сообщениями между собой или с Центром раздачи ключей (ЦРК). ЦРК всегда надежный партнер.
- Протокол аутентификации должен быть устроен так, что даже если злоумышленник перехватит сообщения между A и B, то ни A ни B не спутают друг друга с злоумышленником.

Аутентификация на основе секретного ключа

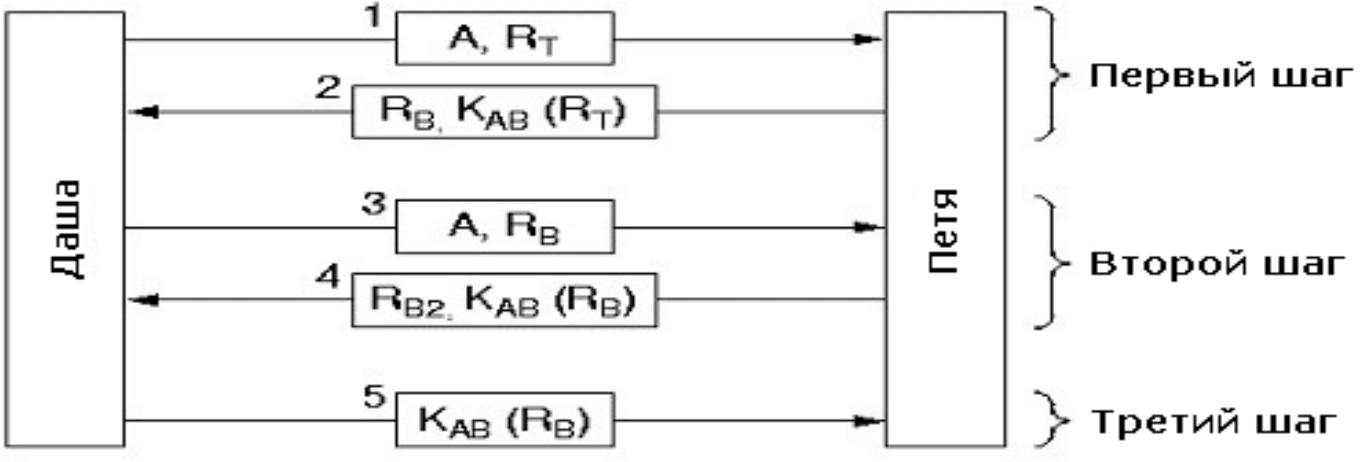


K_{AB} – общий ключ, R_A, R_B - вызовы

Сокращенная двусторонняя аутентификация

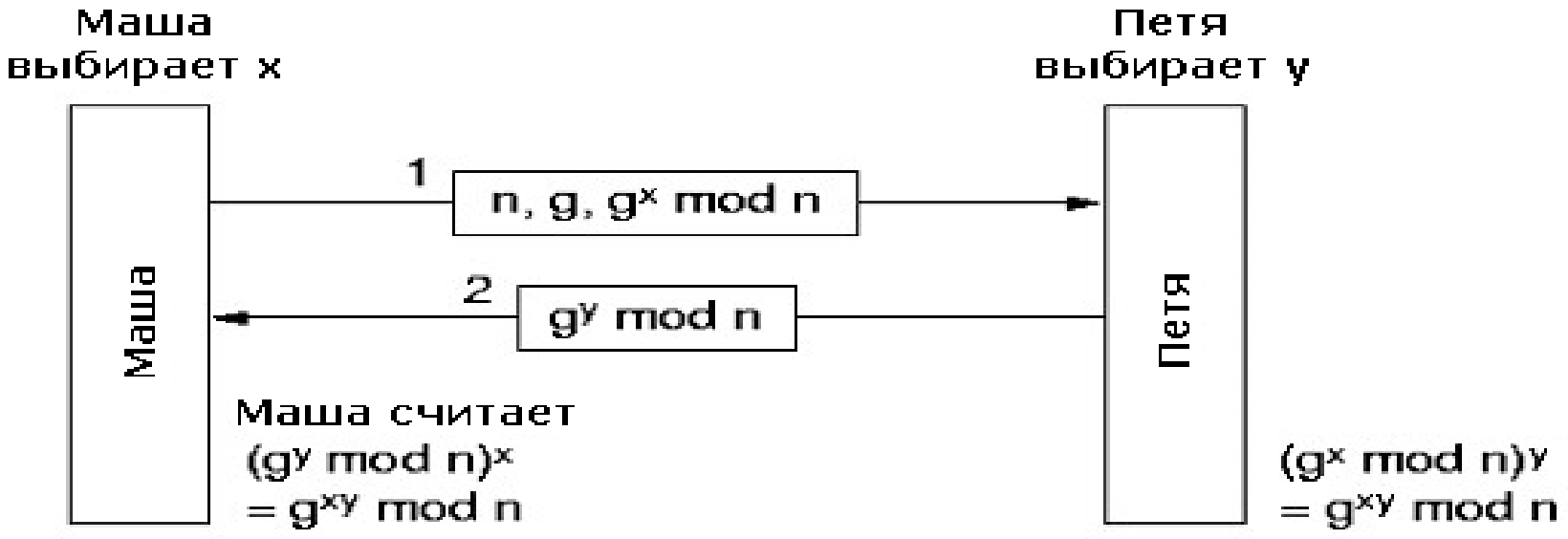


Атака отражением



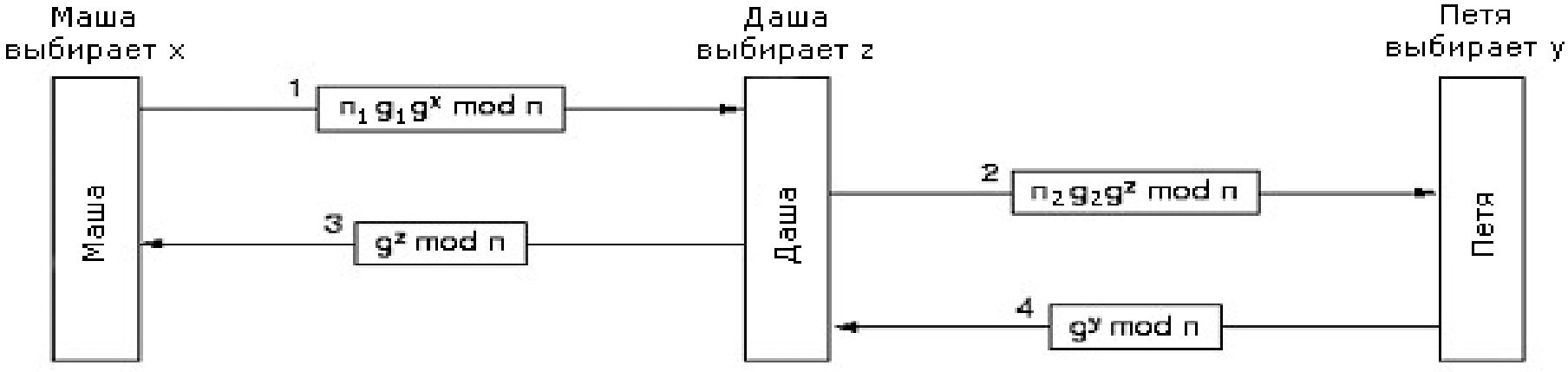
Даша - злоумышленник

Протокол Диффи-Хеллмана-Меркеле



n,g – простые числа

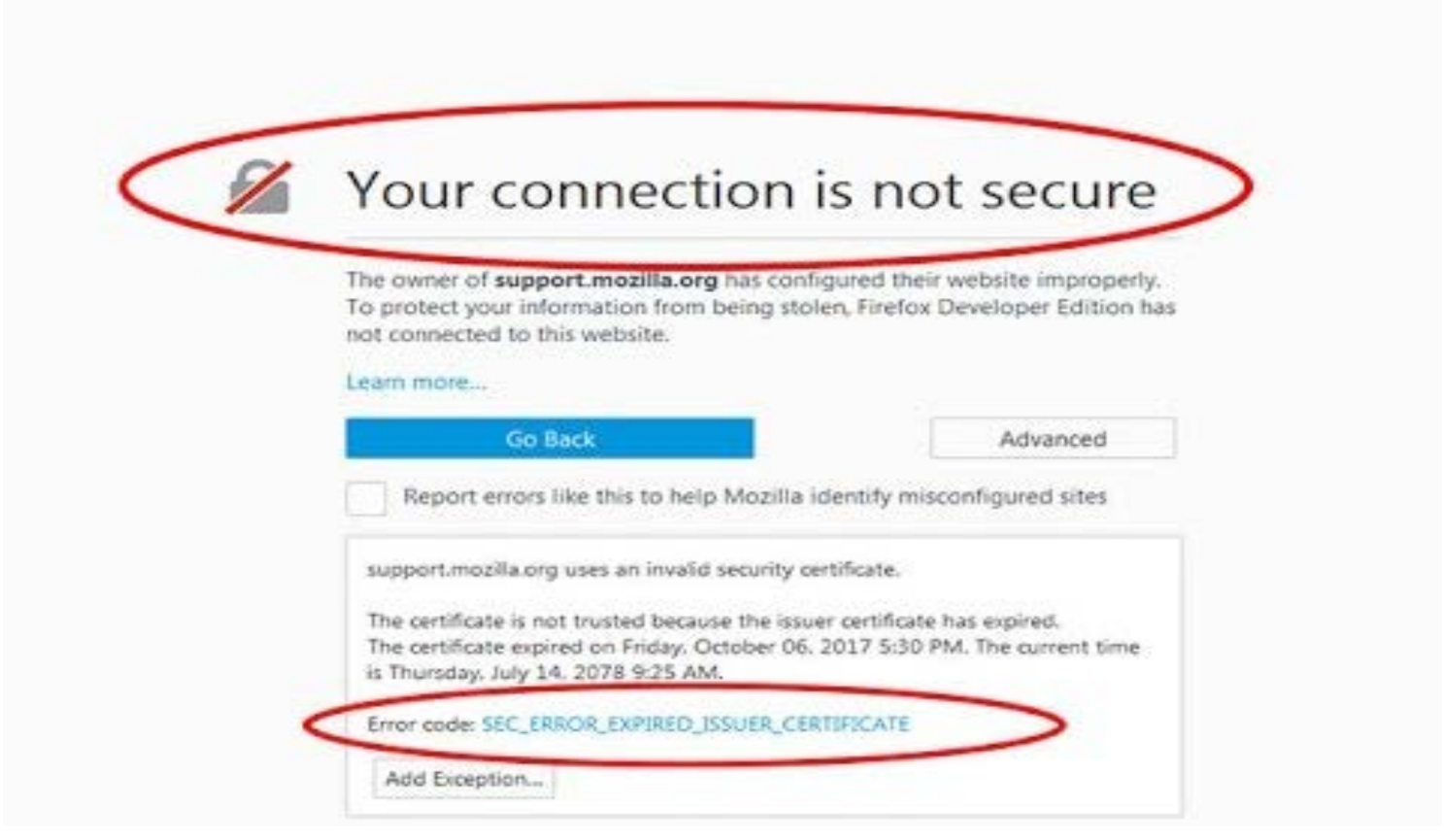
Атака чужой в середине



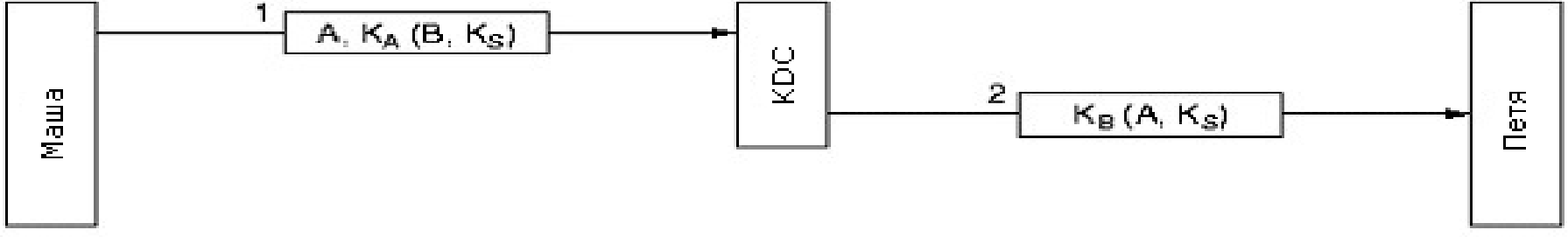
Установка общего ключа

- Как A и B могут установить общий секретный ключ?
  - Протокол обмена ключом ДХМ
  - Например, $n=47$, $g=3$, $x=8$, $y=10$, то A шлет B сообщение (47,3,28), поскольку $3^8 mod 47 = 28$. B шлет A (17). A вычисляет $17^8 mod 47 = 4$, B вычисляет $28^{10} mod 47 = 4$. Ключ установлен – 4!
  - Атака - ***чужой в середине***.

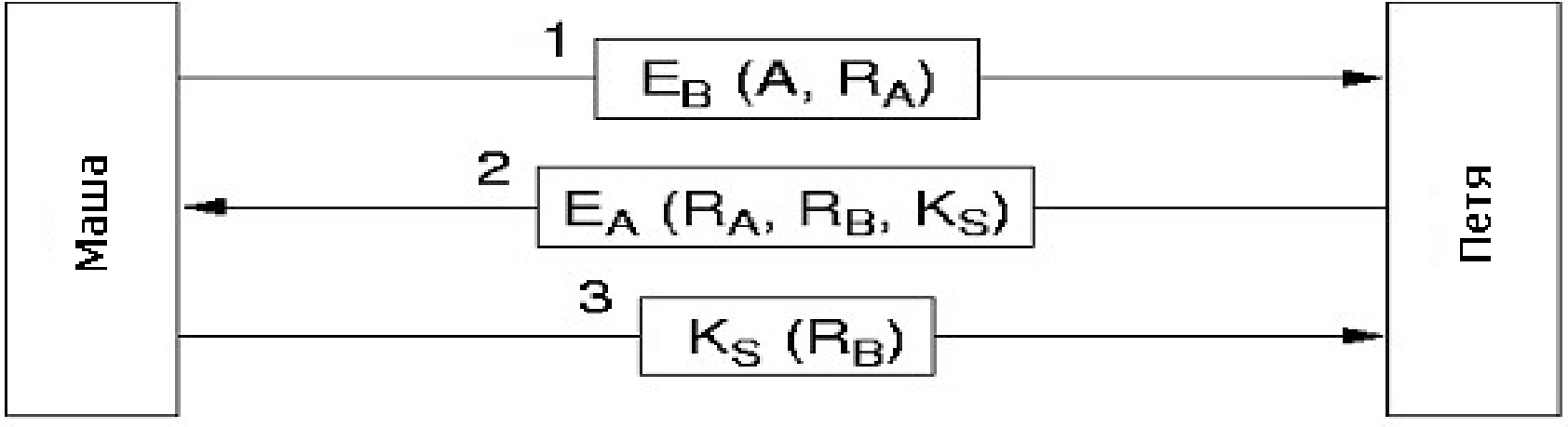
Атака чужой в середине



Проверка подлинности через центр раздачи ключей



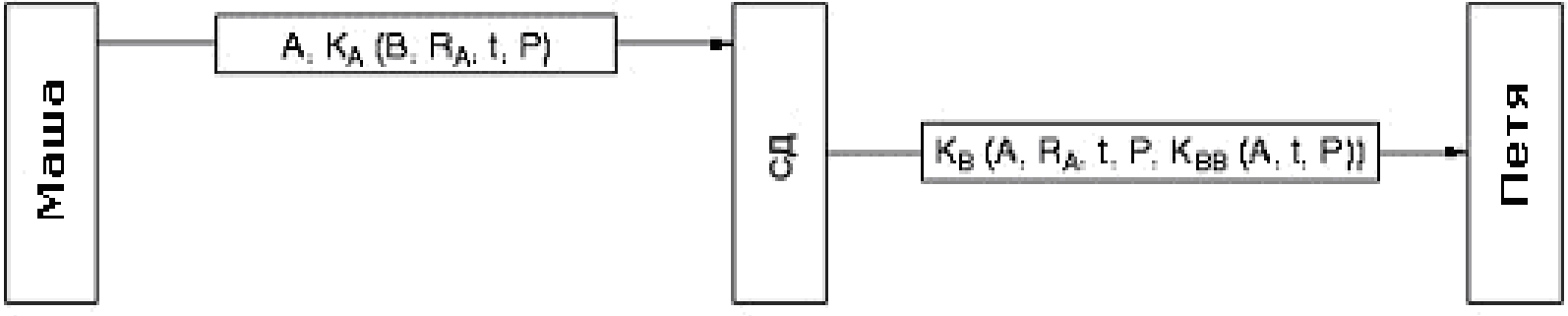
Взаимная аутентификация на основе открытых ключей



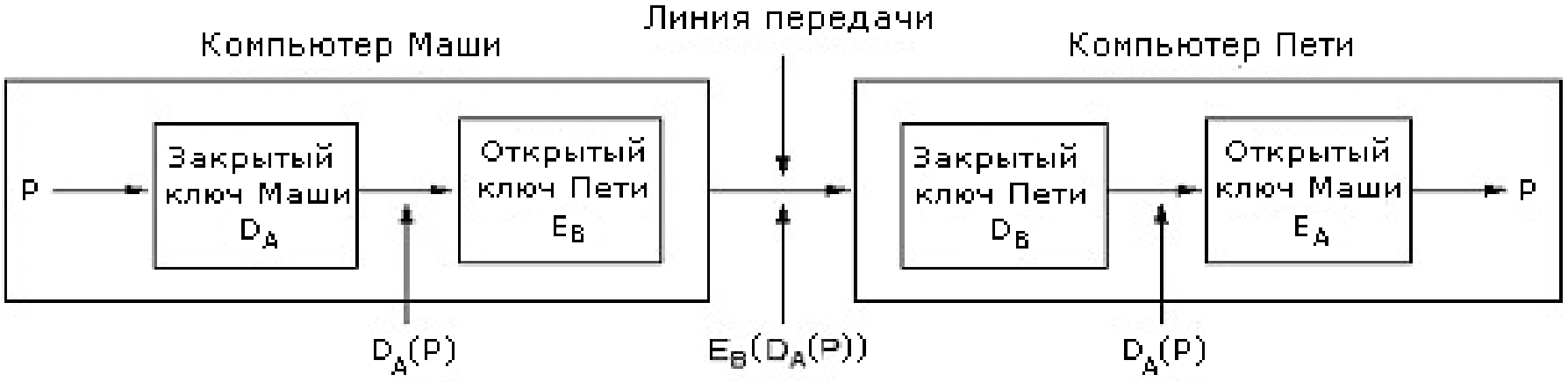
Электронная подпись

- Проблема электронного аналога для ручной подписи весьма сложна. Нужна система, которая позволяла одной стороне посылать "подписанный" документ другой стороне так, чтобы
  - Получатель мог удостовериться в подлинности отправителя;
  - Отправитель позднее не мог отречься от документа;
  - Получатель не мог подделать документ.

Электронная подпись посредством СД



Электронная подпись на основе открытого ключа

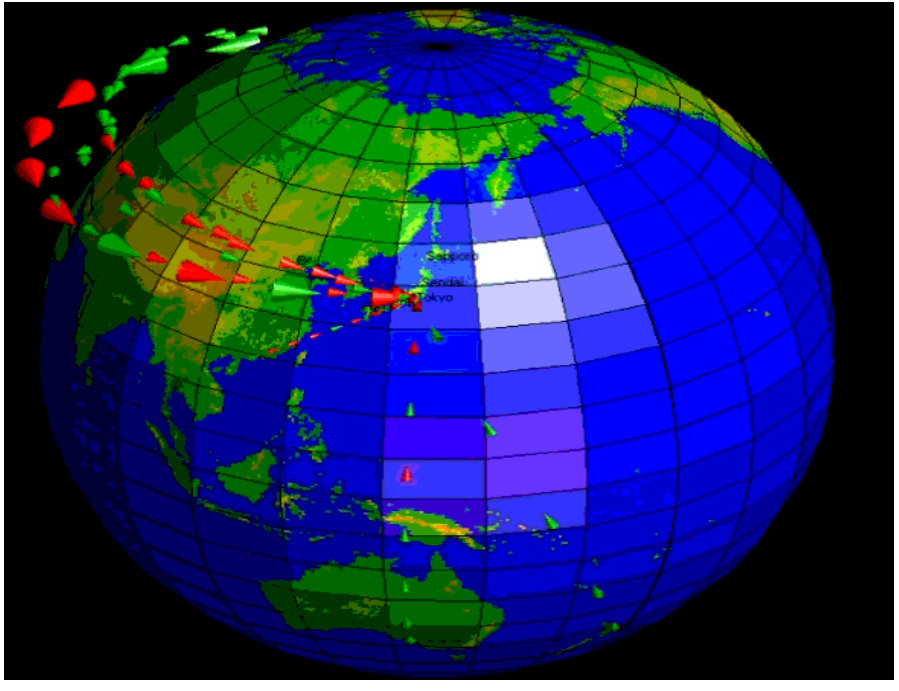


D_X- закрытый ключ, E_X – открытый ключ, где X – A или B.

Обнаружение и предотвращение компьютерных атак (идентификация субъектов)

(http://atlas.arbor.net/worldmap/index)

Обнаружение атак



- Обнаружение сетевых атак и защита от них
- Основные классы атак
  - Несанкционированный доступ
  - Отказ в обслуживании

Система обнаружения атак – это система, которая идентифицирует вредоносную активность в сети

Зачем нужны IDS?

- Безопасность – это часто дорого и неудобно:
  - Стоимость разработки и сопровождения
  - Ограничения на пользователей и функциональность
- Разработчики пытаются предложить некоторые «разумные» уровни безопасности
- Ошибки в ПО всё равно есть, и успешные атаки неизбежны
- Обнаружение позволяет:
  - Находить и исправлять наиболее критические уязвимости
  - По возможности обеспечивать наказуемость нарушителей
  - По возможности ограничивать ущерб от атаки

Методы обнаружения атак (1)

- **Обнаружение аномалий**
  - *Мониторинг сетевого трафика и сравнение с некоторым профилем нормальной работы сети*
    - *Утилизация канала, типы протоколов, номера портов, сочетания взаимодействующих узлов*
  - *Оповещение администратора, если текущий трафик существенно отличается от нормы*
  - *Ошибки первого и второго рода.*
  - *Как правило, такие методы склонны к ложным срабатываниям*

Методы обнаружения атак (2)

- ***Сигнатурные методы***
  - *Также известны как **обнаружение злоупотреблений***
    - *Мониторинг сетевого трафика, и сравнение содержимого (или атрибутов) с базой описаний ранее известных реализаций атак*
    - *Реализуется аналогично большинству антивирусных сканеров*
  - *Менее склонны к ложным срабатываниям по сравнению с подходом на основе анаомалий*
  - ***Не могут обнаруживать даже варианты реализации известных атак, которых нет в базе описаний***

Заключение
Проблемы информационной безопасности

- Конфиденциальность
  - несанкционированный доступ к информации/ресурсам;
  - несанкционированное изменение информации/состояния ресурсов;
- Идентификация подлинности
  - пользователя - имея с кем-то дело через сеть, вы должны быть уверены, что это тот, за кого он себя выдает.
  - документа
- Надежность управления
  - несанкционированное использование ресурсов;

При передаче

При хранении

При обработке

При вводе-выводе.

Заключение

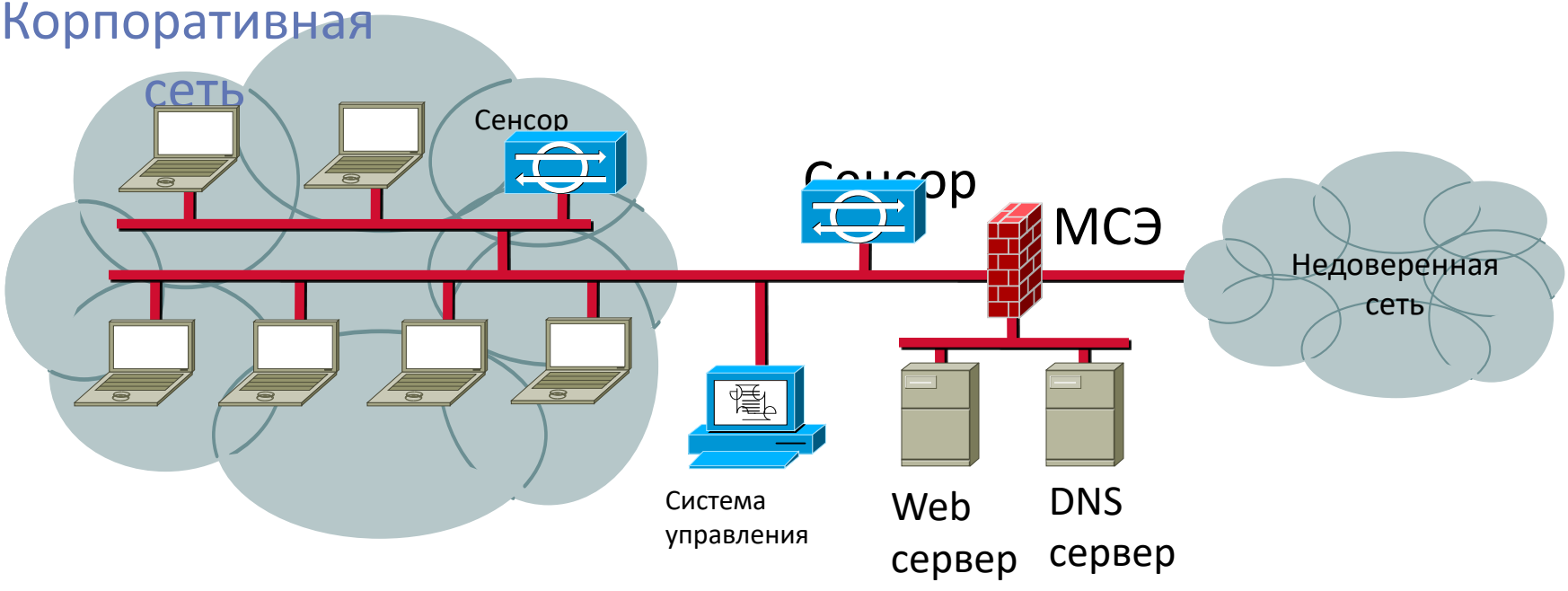
- Информационная безопасность любой СПД – важный этап ее проектирования, разработки и инсталляции
- Осознанное формирование политики ИБ
- Формирование списка угроз и модели нарушителя
- Выбор механизма контроля НСД
- Изоляция данных и кода
- Строгое разделение управления процессом и собственно процесса (вычисление, передача, хранение)

Классификация уязвимостей

Типы систем обнаружения атак

- **Сетевые СОА**
  - Функционируют на уровне сегмента сети
  - Один сенсор СОА может мониторить много узлов
  - Сетевые сенсоры обычно бывают двух видов
    - **ПАК:** состоит из специализированной аппаратуры и ПО. Аппаратура представлена специализированными сетевыми интерфейсами, сбалансированными по производительности процессорами, памятью и дисками.
      - **Примеры:** Sourcefire 3D Sensors, Cisco IPS
    - **Программа:** программное обеспечение сенсора может быть установлено на произвольную аппаратуру (COTS – Commodity Off The Shelf).
      - **Примеры:** Snort, Bro, Suricata

Сетевые системы обнаружения атак



Вопрос эффективности СОА

- Точность: низкий уровень false positive и false negative
- Производительность: скорость обработки трафика или журнальных записей
  - В некоторых случаях нельзя установить СОА на входе в сеть, т.к. канал слишком быстрый
  - Вместо этого устанавливают несколько СОА внутри
- Устойчивость: собственная устойчивость к атакам и ошибкам
  - Должна работать на выделенном узле с усиленной защитой

Проблемы информационной безопасности

(заключение)

- Модели угроз конфиденциальности, целостности, доступности
- Политики безопасности, как система ограничений снижающая или исключающая реализацию угроз безопасности
- Шифрование, мониторы безопасности доступа