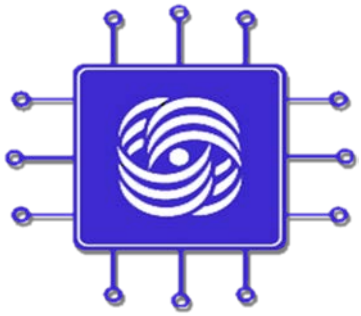


БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В СЕТЯХ ЭВМ

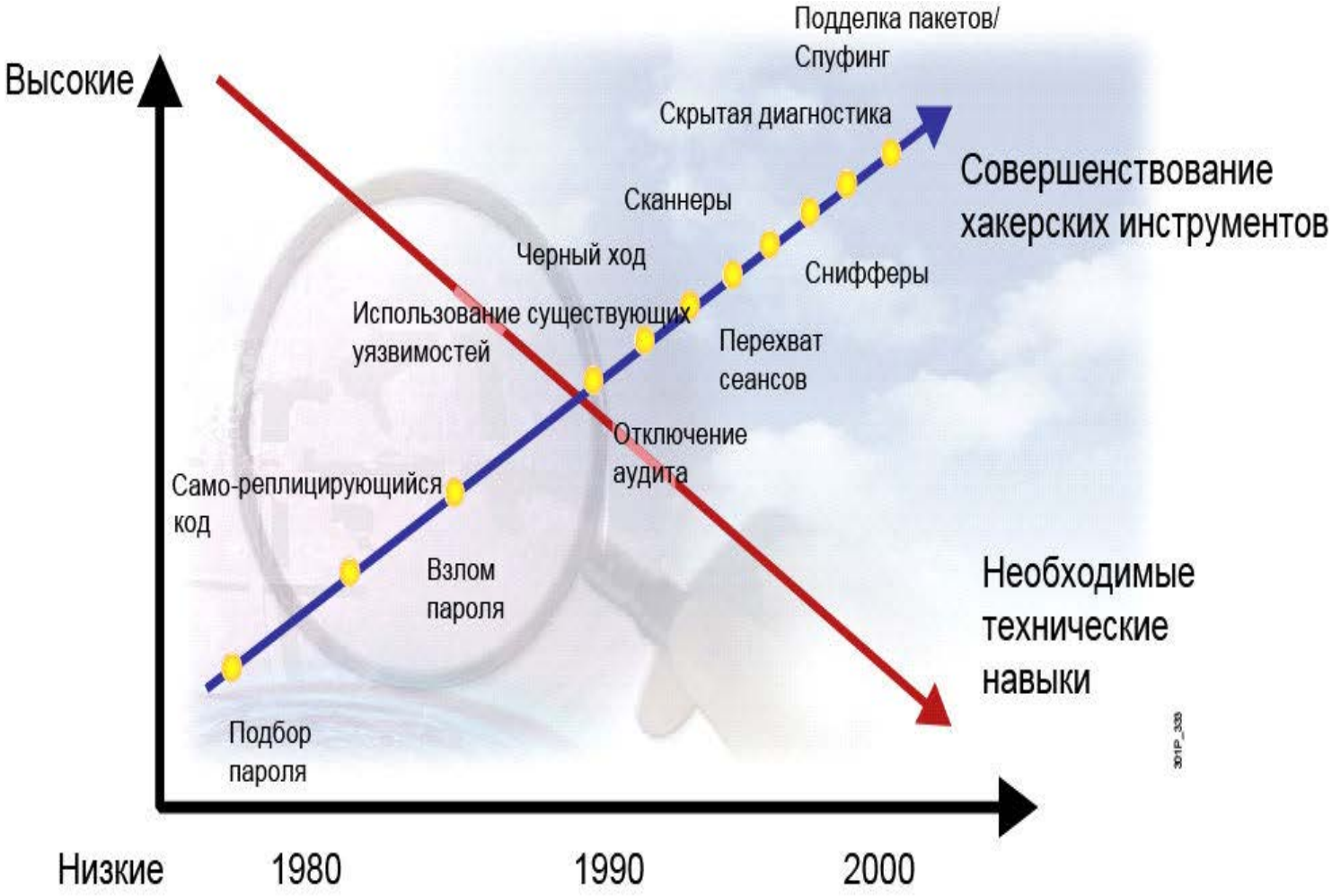
(учебник: Компьютерные сети,

Том 2, стр.147-184)

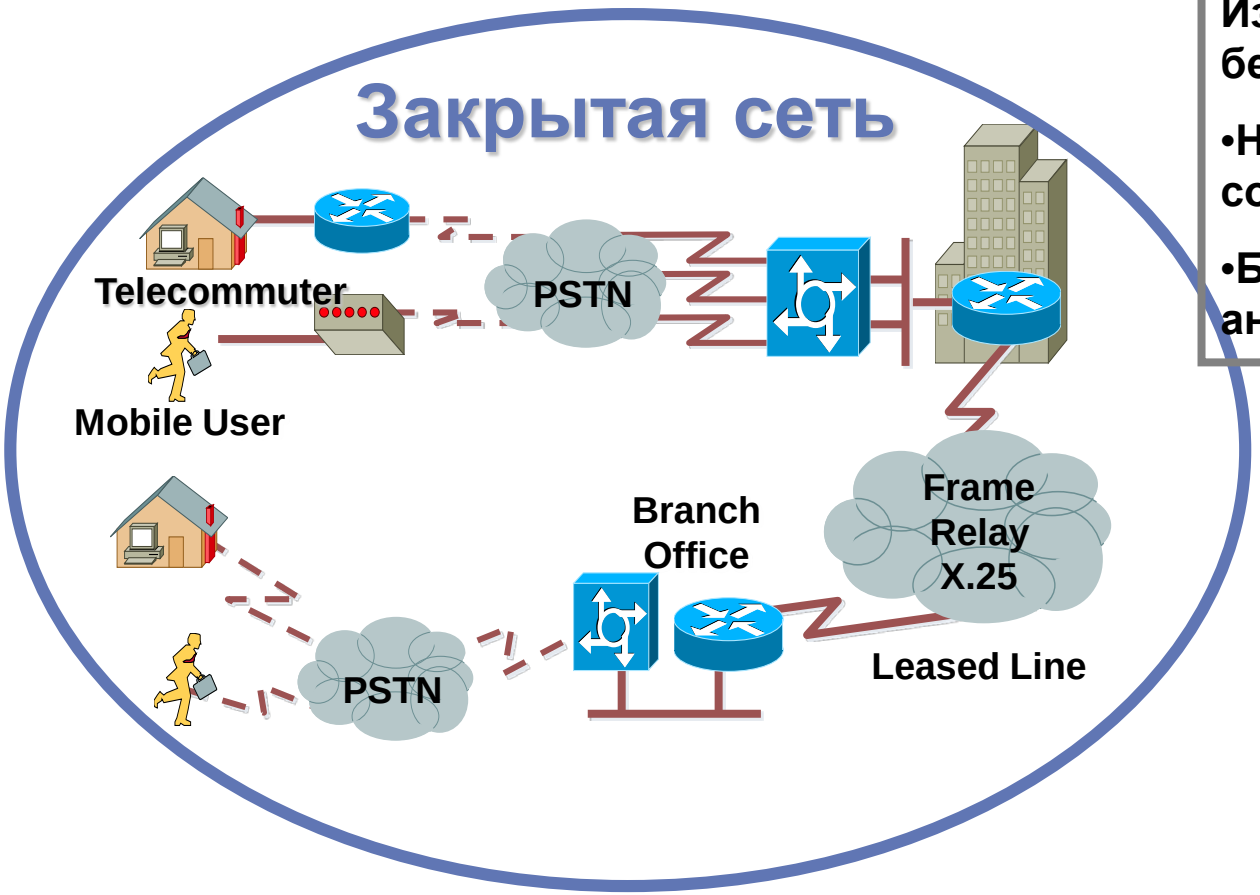
Введение в компьютерные сети
проф. Смелянский Р.Л.
Лаборатория Вычислительных комплексов
ф-т ВМК МГУ

Эволюция угроз

Угрозы в компьютерных сетях



Сети 90-х

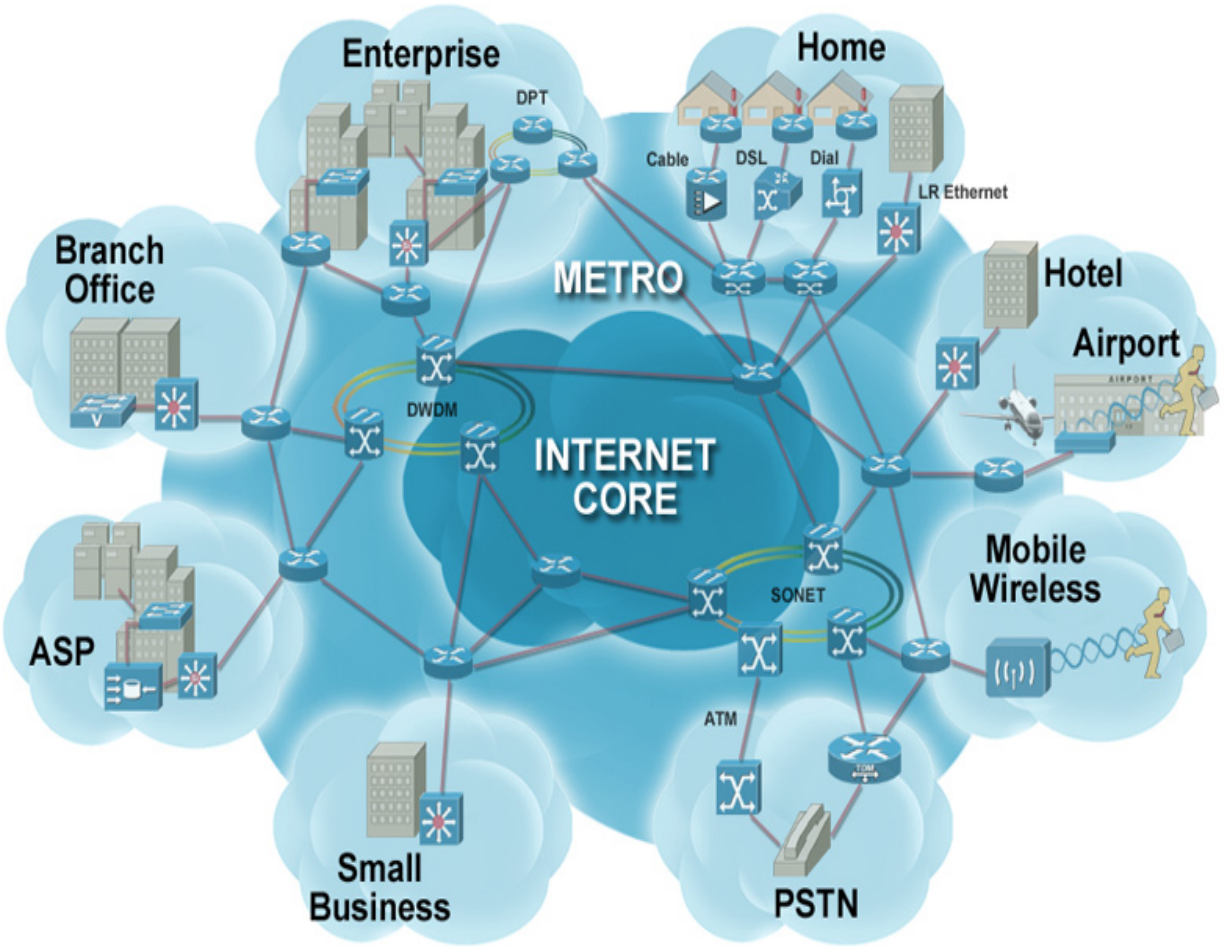


Изолированная и безопасная среда

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

Средства безопасности были рассчитаны на подобные сети

Сети 00-х



- **Распределенный доступ в Интернет, требующий безопасности**
- **Открытые Датацентры**
- **Мобильность сотрудников**
- **Появление технологий типа VLAN и IPTV, VoIP**
- **Растущий ущерб от ВПО**

Термины и определения

Информация - сведения (сообщения, данные) независимо от формы их представления (ФЗ 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»)

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. (ФЗ 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»)

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. (ФЗ 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»)

Информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (ФЗ 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»)

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (ФЗ 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»)

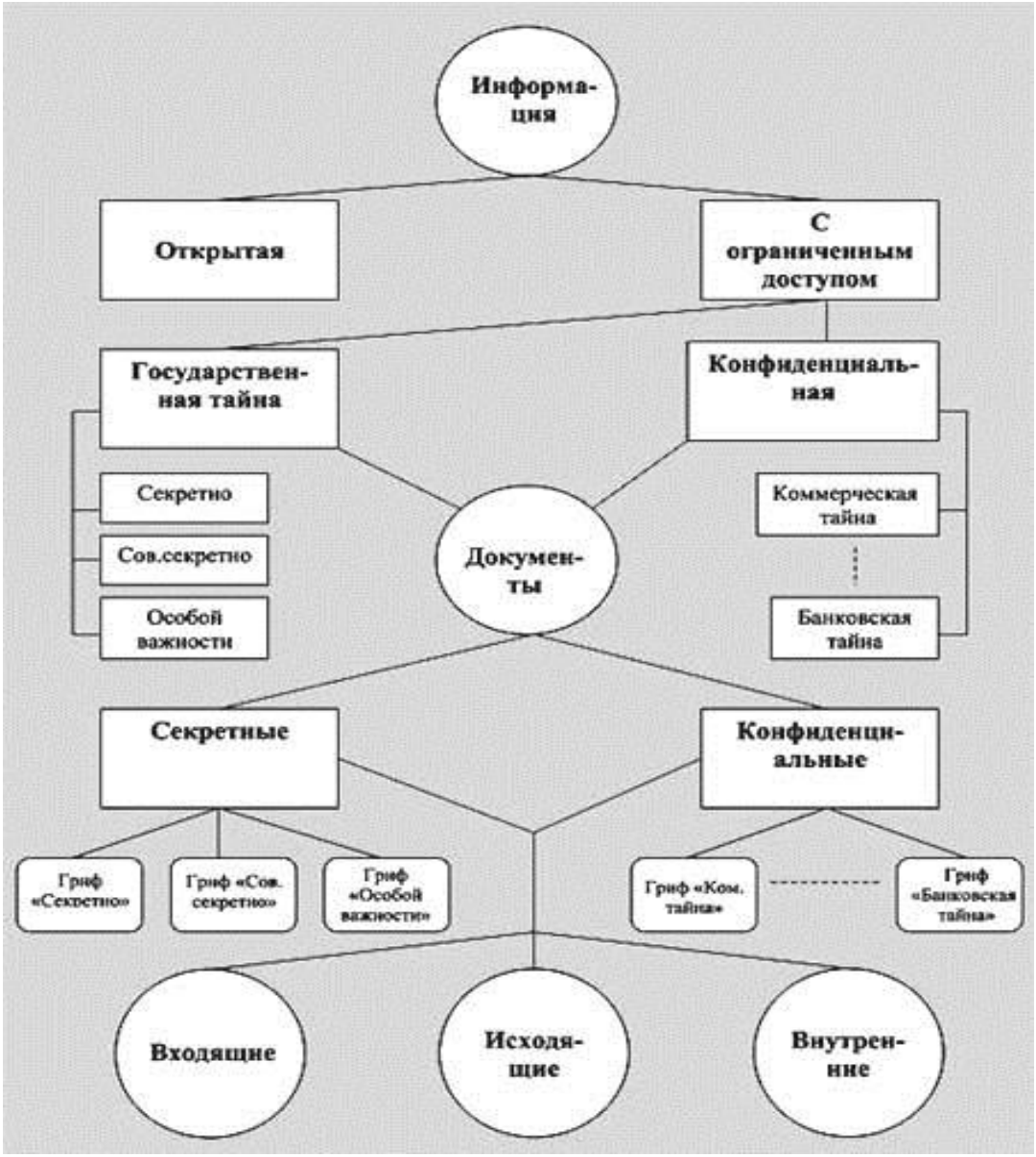
Термины и определения

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. (Носители информации - материальные объекты, в том числе физические поля, в которых сведения находят свое отображение в виде символов, образов, сигналов, технических решений и процессов)

Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах, в том числе предприятий)

Термины и определения



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

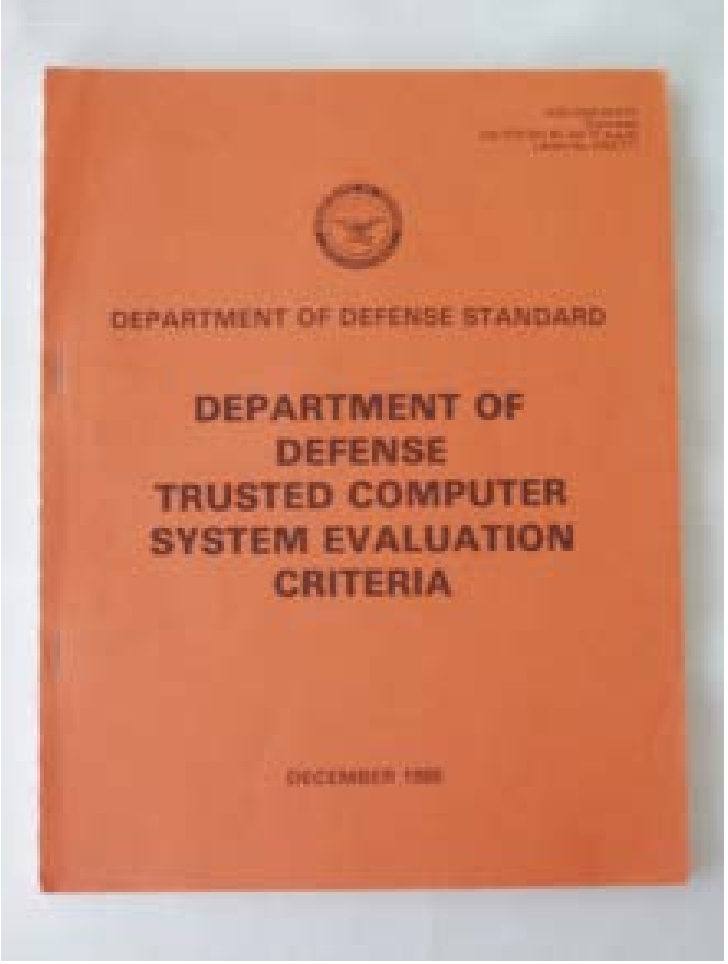
Термины и определения

Безопасность - состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. (Закон РФ «О безопасности»)

Информационная безопасность Российской Федерации - это состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства (Доктрина информационной безопасности РФ)

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



Критерии определения безопасности компьютерных систем

(*Trusted Computer System Evaluation Criteria*)

Термины и определения

Информационная безопасность

Information security

Безопасность информации

Термины и определения

Информационная безопасность* — *состояние (качество)* определенного объекта (в качестве объекта может выступать информация, данные, ресурсы автоматизированной системы, автоматизированная система, информационная система предприятия, общества, государства и т. п.)

Информационная безопасность **— защита конфиденциальности, целостности и доступности информации.

Информационная безопасность** — *деятельность*, направленная на обеспечение защищенного состояния объекта (в этом значении чаще используется термин «защита информации»)

.....

*Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006).;

**Национальный стандарт РФ «Информационная технология. Практические правила управления информационной безопасностью» (ГОСТ Р ИСО/МЭК 17799—2005).;

Понятия информационной безопасности

- ***Информационная безопасность*** – **состояние защищённости информации**, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз: нарушения ***конфиденциальности***, ***целостности*** либо ***доступности информации либо ресурсов***, а так же незаконного тиражирования информации, которые приводят к материальному или моральному ущербу владельца или пользователя информации.

Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006).;

- ***Угроза безопасности компьютерной системы*** – это **потенциально возможное происшествие**, преднамеренное или нет, которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней.

Термины и определения

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия её обладателя»... «информация — сведения (сообщения, данные) независимо от формы их представления»
- способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней

Целостность информации - состояние защищенности информации характеризуемое способностью КС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения

Доступность информации - состояние информации, характеризуемое способностью КС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия

Доступ к информации (доступ) - ознакомление с информацией, её обработка, в частности копирование, модификация или уничтожение информации.

Термины и определения

Защита информации - деятельность, направленная на предотвращение утечки, разглашения, несанкционированного доступа (НСД) защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Собственником информации могут быть: государство, юридическое лицо, группа физических лиц, отельное физическое лицо.

Термины и определения

Несанкционированный доступ к информации (НСД) - доступ к информации, нарушающий правила разграничения доступа *с использованием штатных средств*, предоставляемых средствами вычислительной техники или автоматизированными системами.

Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.

В подходе Гостехкомиссии НСД является ключевым понятием и трактуется как доступ к защищаемой информации с нарушением установленных прав или правил доступа, приводящий к получению субъектом возможности ознакомления с информацией и/или воздействия на нее

Термины и определения

- **Защита информации** характеризуется - целью защиты, объектом защиты, время защиты, эффективностью защиты.

- **Цель защиты** - это желаемый результат защиты, т.е. защиты от угроз и устранение уязвимостей.

Угроза безопасности КС - потенциально возможное воздействие на информацию или другие компоненты КС, которое может прямо или косвенно привести к нанесению ущерба интересам субъектов информационных отношений.

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.

Уязвимость информационной системы – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности информации.

Термины и определения

- ***Уязвимость компьютерной системы*** – особенность реализации системы, которая делает возможным реализацию угрозы.
- ***Атака на компьютерную систему*** – это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании уязвимости.
  - Нарушения конфиденциальности информации – случай получения доступа к информации посторонним субъектом.
  - Нарушения целостности информации – случай умышленного искажения (модификация или удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую.
  - Нарушение доступности: отказ от обслуживания, несанкционированное использование ресурсов сети.

Термины и определения

Ключевые понятия (IBM 1972)

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

Ключевые понятия (IBM 1972)

- Контроль неизменности
- Изоляция

Методы реализации

Средства защиты

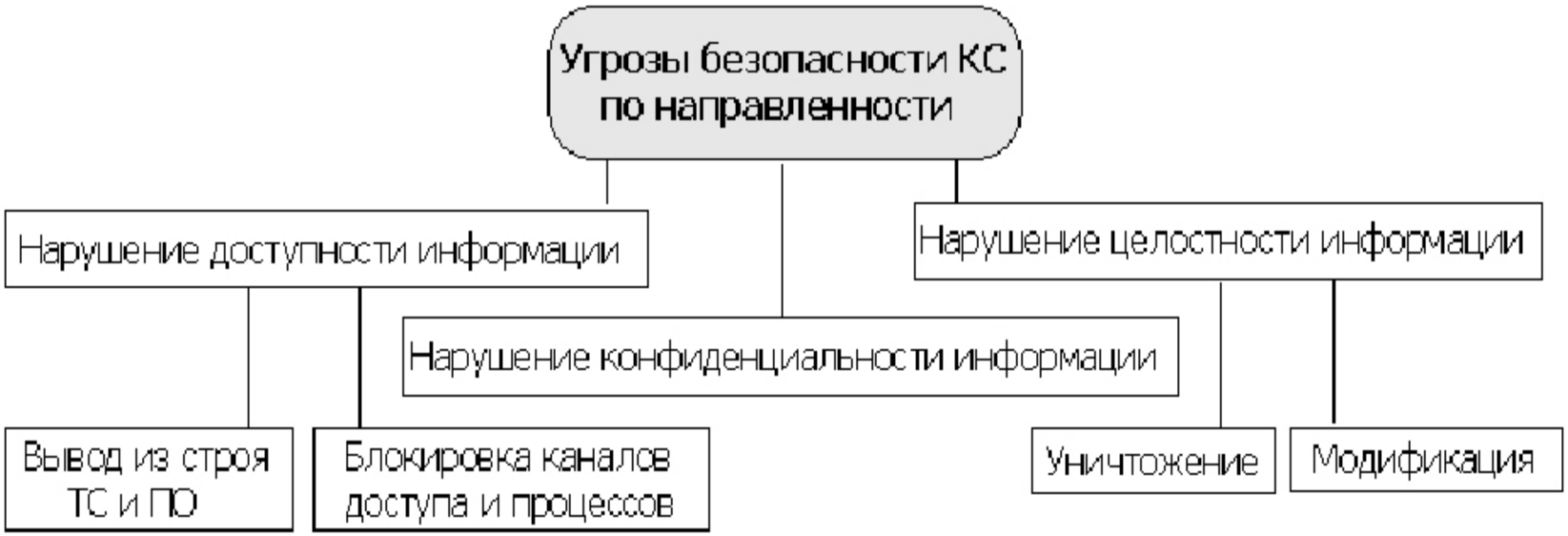
- Физические
- Технические
- Аппаратные
- Программные
- Организационные (режимные)
- Правовые
- Криптографические

Проблемы информационной безопасности

- На каком уровне решают проблемы сетевой безопасности?
- Методы обеспечения сетевой безопасности
  - санкционированный доступ в систему (аутентификация входящего)
  - защита и контроль доступа к ресурсам (авторизация доступа)
  - сокрытие информации в системе
- ***Политика безопасности*** – документ, отражающий набор норм, правил и практических приемов, которые регулируют размещение, доступ и защиту информации.

Признаки классификации угроз безопасности

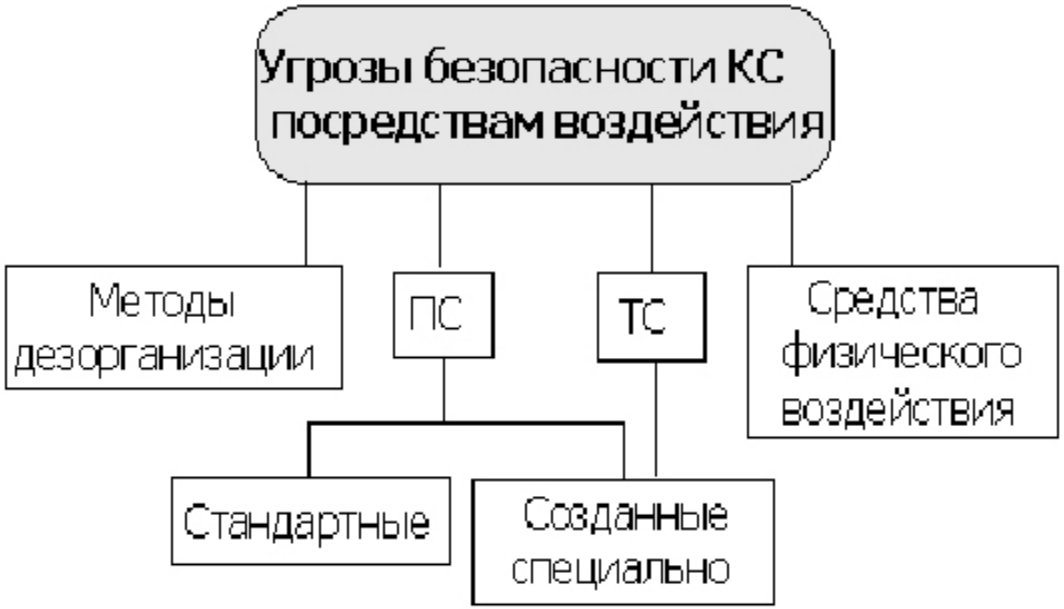
Классификация угроз по направленности реализации



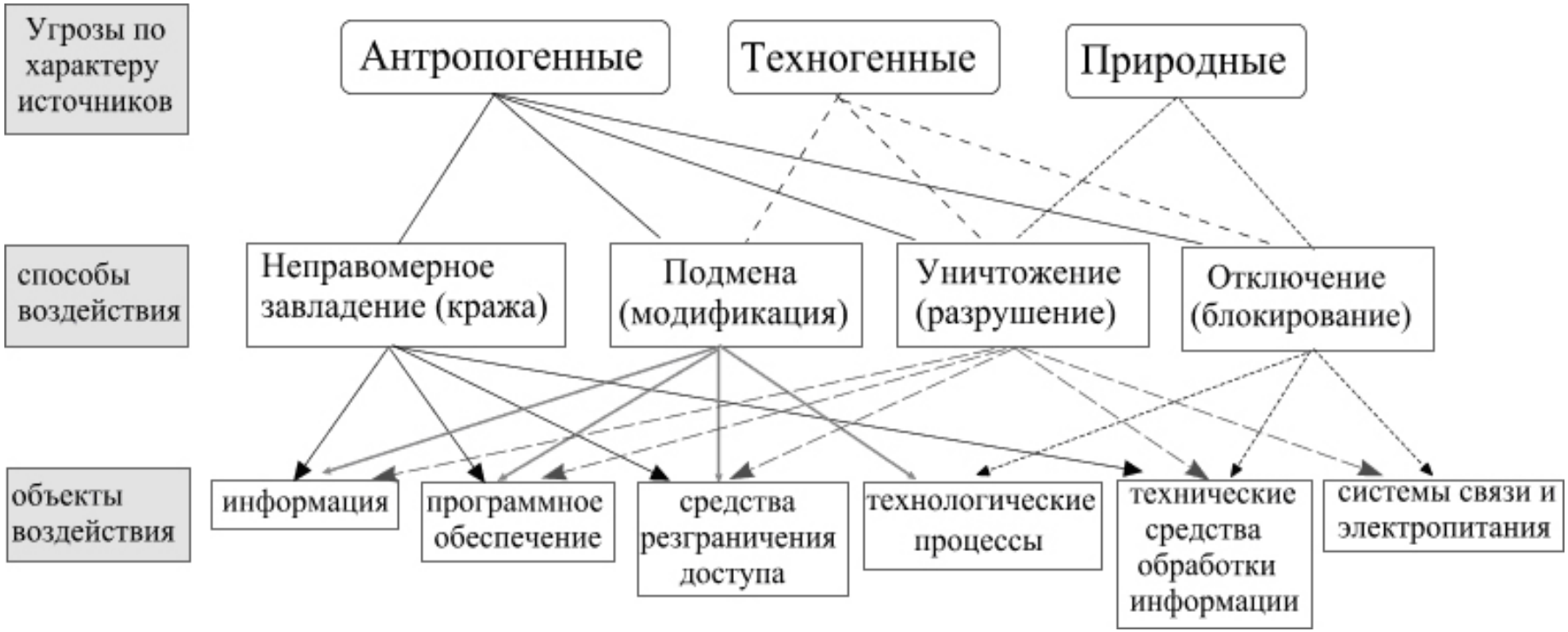
Классификация угроз по временным характеристикам воздействия

Классификация угроз по объекту воздействия

Классификация угроз по используемым средствам воздействия (нападения)



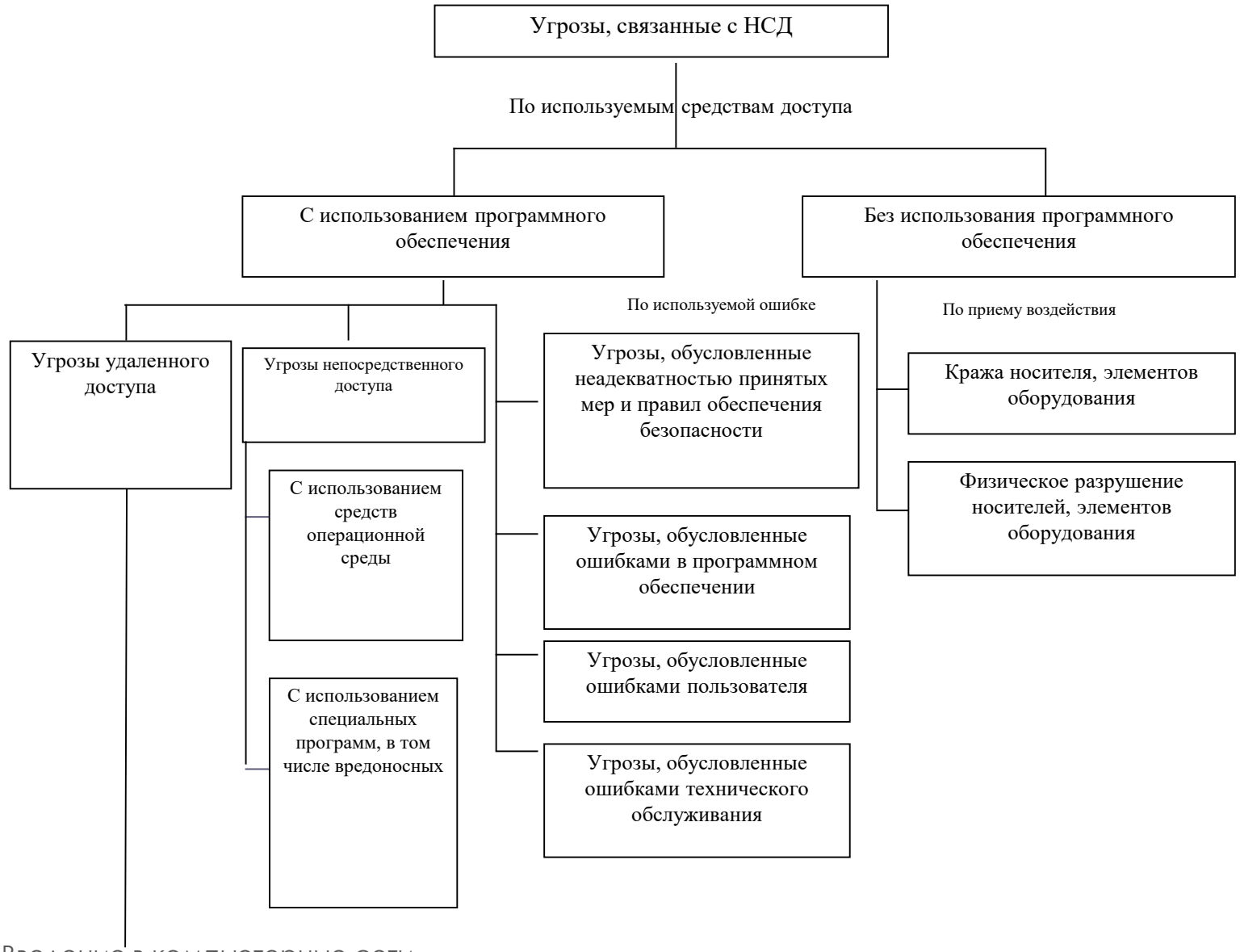
Классификация угроз по причинам (источникам) возникновения



Классификация угроз по характеру и масштабам негативных последствий

Классификация угроз по каналам доступа

Угрозы, связанные с НСД



Угрозы, связанные с НСД (продолжение)

Инцидент – сочетание угрозы и уязвимости

Инцидент – сочетание угрозы и уязвимости (примеры)

Безопасность кадровых ресурсов (ISO/IEC 27002:2005, раздел 8)

Уязвимость	Угроза, использующая уязвимость
Недостаточное обучение безопасности	Ошибка персонала технической поддержки
Неосведомленность в вопросах безопасности	Ошибки пользователей
Отсутствие механизмов мониторинга	Несанкционированное использование программного обеспечения
Отсутствие политик в области корректного использования средств телекоммуникаций и передачи сообщений	Несанкционированное использование сетевого оборудования
Не отменяются права доступа при увольнении	Несанкционированный доступ
Не существует процедуры, гарантирующей возврат ресурсов при увольнении	Кража
Немотивированный или недовольный персонал	Злоупотребление средствами обработки информации
Безнадзорная работа внешнего персонала или персонала, работающего в нерабочее время	Кража

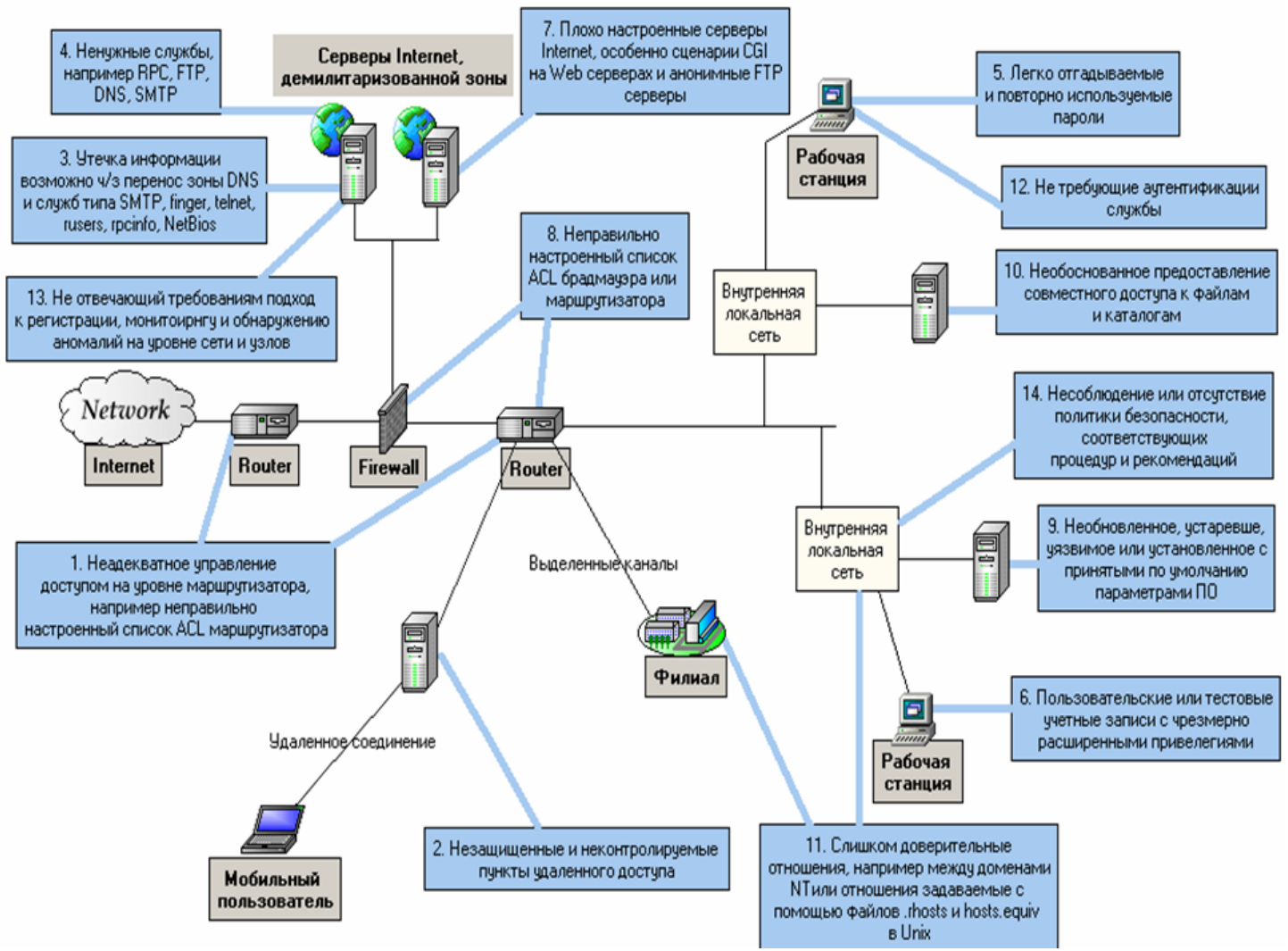
http://анализ-риска.рф/node/231

Инцидент – сочетание угрозы и уязвимости (примеры)

Управление коммуникациями и операциями (ISO/IEC 27002:2005, раздел 10)

Уязвимость	Угроза, использующая уязвимость
Сложный пользовательский интерфейс	Ошибка персонала
Передача или повторное использование средств хранения информации без надлежащей очистки	Несанкционированный доступ к информации
Неадекватный контроль изменений	Сбой системы безопасности
Неадекватное управление сетью	Перегрузка трафика
Отсутствие процедур резервного копирования	Потеря информации
Отсутствие доказательств отправки или получения сообщения	Уход от ответственности
Отсутствие обновления программного обеспечения, используемого для защиты от вредоносного кода	Вирусная инфекция
Нет разделения обязанностей	Злоупотребление системой (случайное или преднамеренное)
Нет разделения тестового и рабочего оборудования	Несанкционированная модификация действующих систем
Неконтролируемое копирование	Кража
Незащищенные соединения с сетями общего пользования	Использование программного обеспечения неавторизованными пользователями

Угрозы и уязвимости в компьютерных сетях



Потенциальные носители угроз

Злоумышленник	Ц е л ь
Студент	Поразвлечься, читая чужую почту
Хакер	Проверить чью-либо систему безопасности; украсть данные
Торговый представитель	Втереться в доверие: представляет всю Европу, а не только Албанию
Бизнесмен	Узнать о маркетинговых планах конкурента
Бывший сотрудник	Отомстить за недавнее увольнение
Бухгалтер	Присвоить себе деньги компании
Брокер	Отказаться от обещания, сделанного по электронной почте
Мошенник	Украсть номера кредитных карточек для их продажи
Шпион	Изучить военный потенциал противника
Террорист	Узнать секрет бактериологического оружия

Угрозы - источники

Злоумышленники, их мотивы и классификация атак

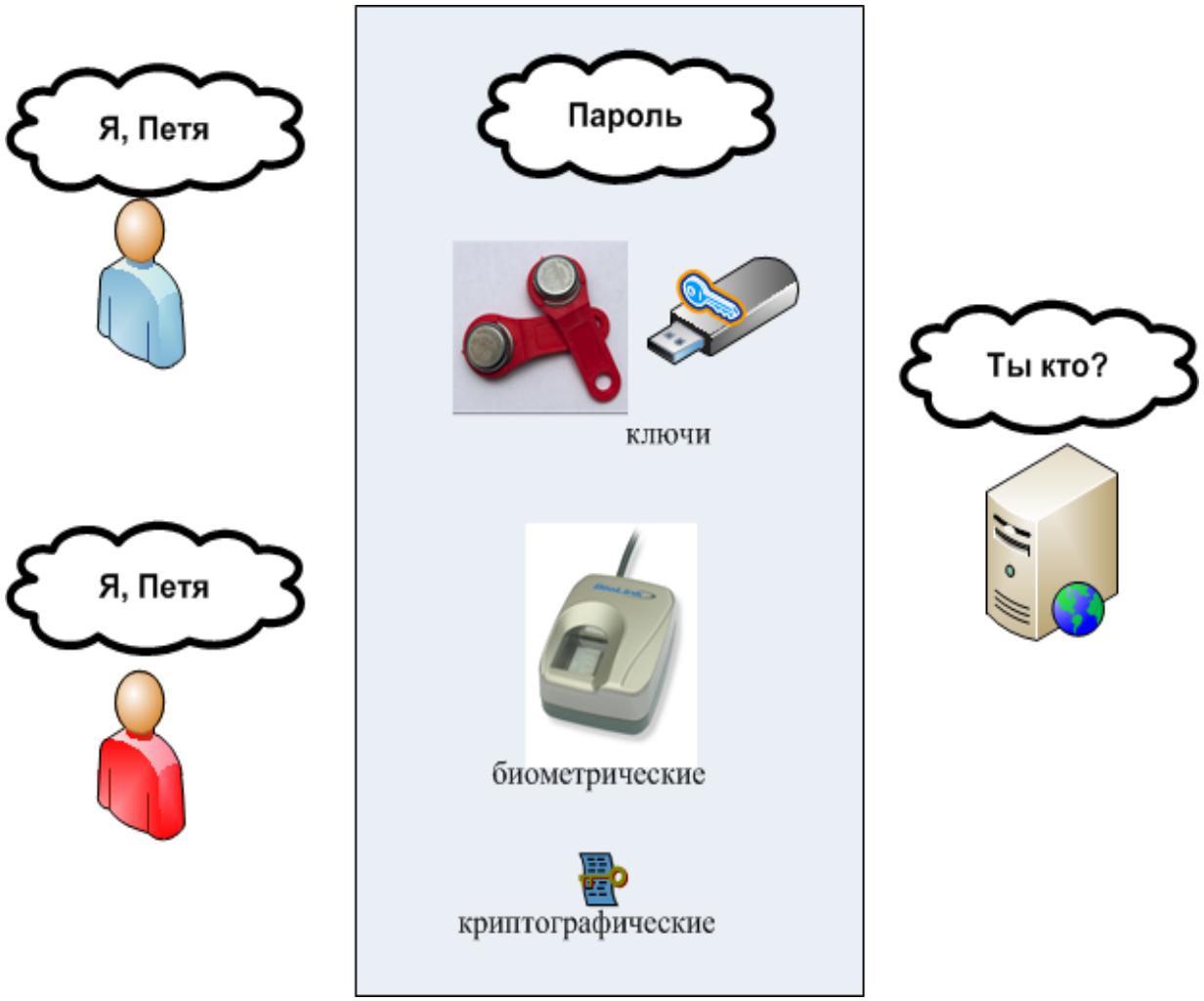
Злоумышленники	Мотивы	Классы атак
▪ Националисты ▪ Террористы ▪ Преступники ▪ Хакеры ▪ Взломщики ▪ Конкуренты ▪ «Хакеры-дилетанты» ▪ Недовольные сотрудники ▪ Правительство	▪ Разведка ▪ Кража ▪ Отказ в обслуживании ▪ Затруднение работы ▪ Соревновательные интересы	▪ Пассивные ▪ Активные ▪ С близкого расстояния ▪ Внутренние ▪ Распределенные

Общая схема оценки угроз

Опознавание - определения

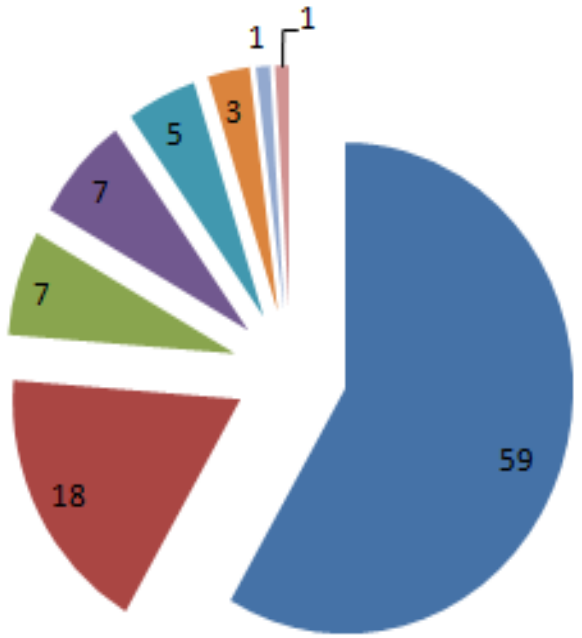
- **Идентификация** — это процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации - каждый субъект или объект системы должен быть однозначно идентифицируем.
- **Идентификация в информационных системах** — присвоение субъектам и объектам идентификатора и / или сравнение идентификатора с перечнем присвоенных идентификаторов.
- **Аутентификация** - это проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).
- **Авторизация** - процедура предоставления субъекту определенных прав доступа к ресурсам системы после успешного прохождения им процедуры аутентификации. Для каждого субъекта в системе определяется набор прав, которые он может использовать при обращении к её ресурсам.
- **Администрирование** - процесс управления доступом субъектов к ресурсам системы. Данный процесс включает в себя:
- - 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, включающий протоколирование действий субъектов при их работе с ресурсами системы в целях обеспечения возможности обнаружения несанкционированных действий.

Подтверждение подлинности

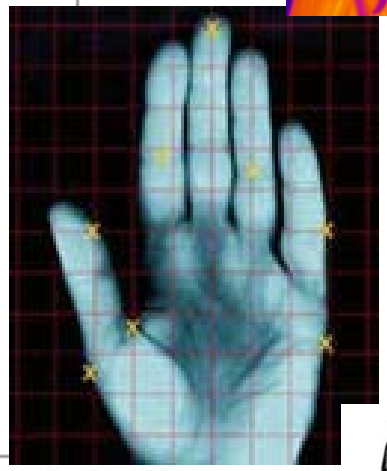


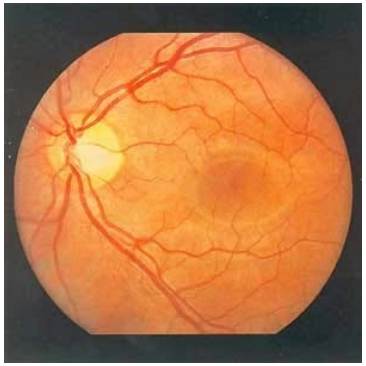
Подтверждение подлинности

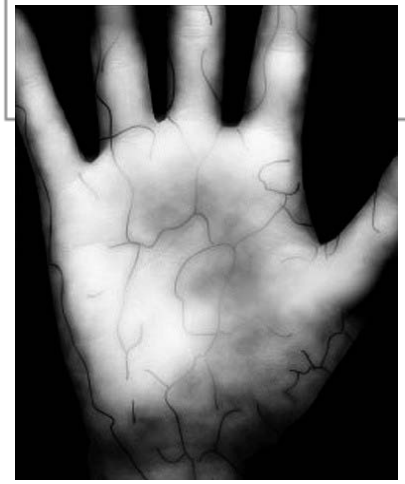
Биометрические методы аутентификации

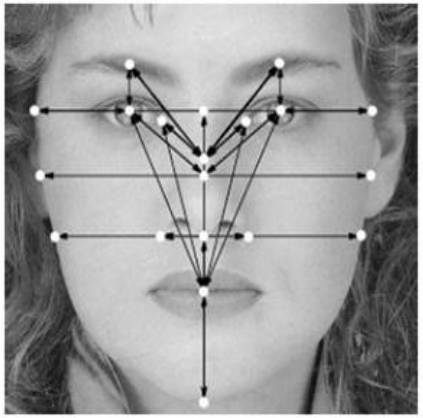


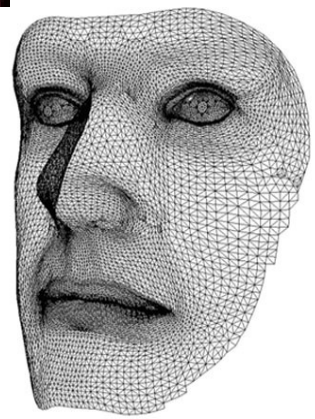
- Отпечаток пальца
- Геометрия лица (2d+3d)
- Геометрия руки
- Радужная оболочка глаза
- Голос
- Рисунок вен
- Почерк
- Прочее



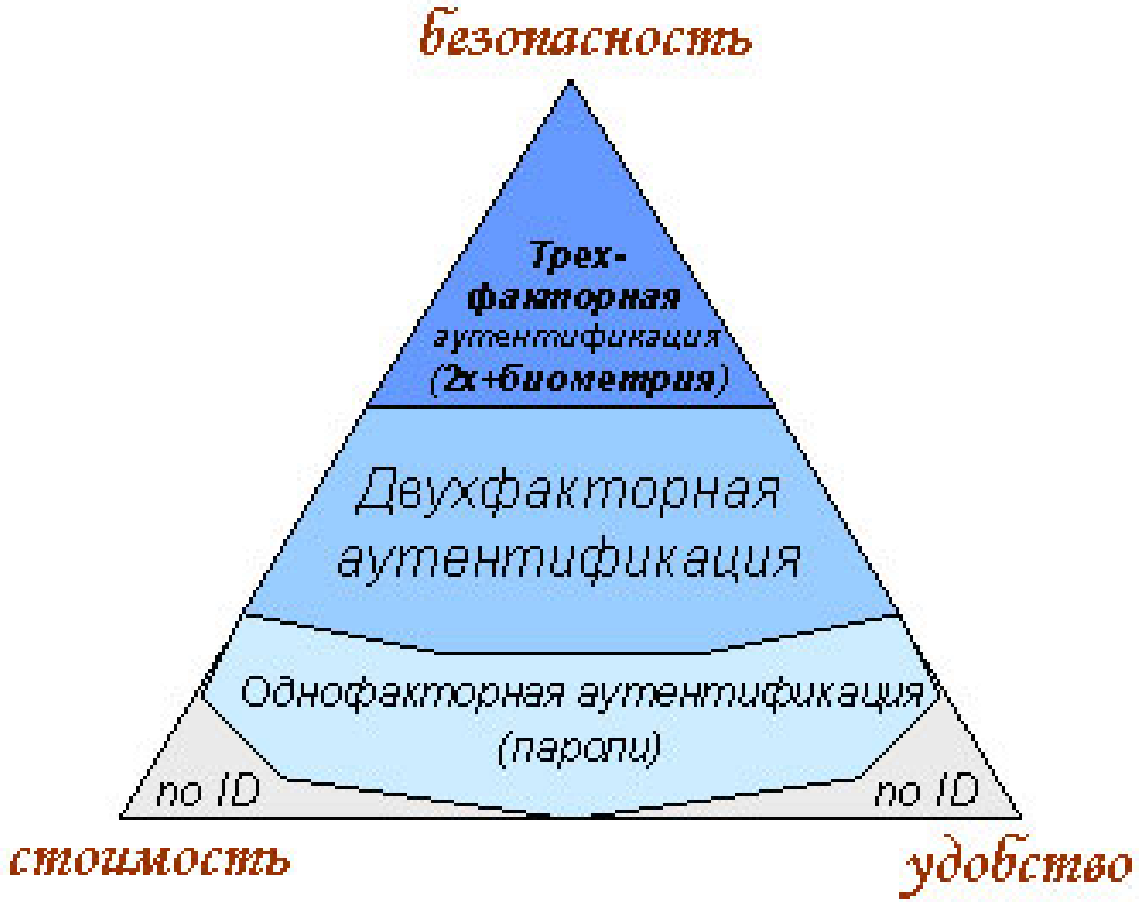








Выбор технологии аутентификации



Протоколы аутентификации в сети

PAP (Password Authentication Protocol) - двусторонний протокол обмена подтверждениями, предназначенный для использования с протоколом PPP. PAP является обычным текстовым паролем, используемым в более ранних системах SLIP.

CHAP (Challenge Handshake Authentication Protocol) -это трехсторонний протокол обмена подтверждениями, предполагающий лучшую защиту, чем протокол аутентификации PAP (Password Authentication Protocol).

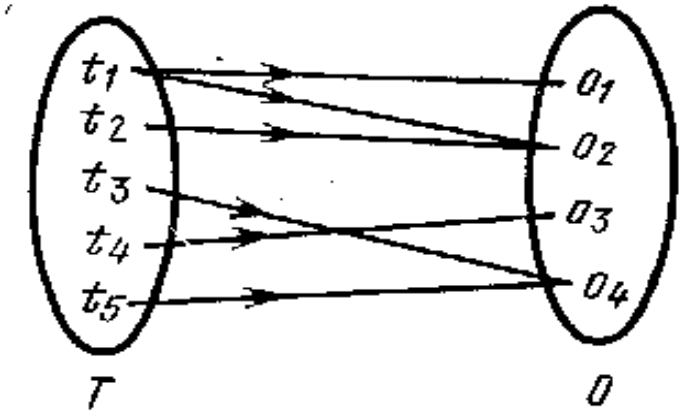
MS-CHAP (MD4) Использует версию Microsoft протокола.

MS-CHAP-V2 Предоставляет дополнительную возможность для изменения пароля, недоступную с MS-CHAP-V1 или стандартной аутентификацией CHAP.

EAP (Extensible Authentication Protocol) представляет собой расширяемый механизм аутентификации, позволяющий унифицировать процесс проверки подлинности пользователей, предоставляя при этом участникам соединения возможность использования самых разнообразных схем аутентификации.

Управление доступом и информационными потоками.

Субъектно-объектная модель компьютерной системы



Субъектно-объектная модель компьютерной системы

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

Субъектно-объектная модель компьютерной системы

- *Под **субъектом** доступа понимается активная сущность КС, которая может изменять состояние системы через порождение процессов над объектами, в том числе, порождать новые объекты и инициализировать порождение новых субъектов.*

- *Под **объектом** доступа понимается пассивная сущность КС, процессы над которой могут в определенных случаях быть источником порождения новых субъектов.*

В модели предполагается наличие априорно безошибочного механизма различения активных и пассивных сущностей (т. е. субъектов и объектов) по свойству активности (например различия между файлом с кодом программы и исполняемой (запущенной) программой).
Предполагается также, что в любой момент времени t_k , в том числе и в начальный, множество субъектов доступа не пусто.

Субъектно-объектная модель компьютерной системы

- *Под **пользователем** КС понимается лицо, внешний фактор, аутентифицируемый некоторой информацией, и управляющий одним или несколькими субъектами, воспринимающий объекты и получающий информацию о состоянии КС через субъекты, которыми он управляет.*

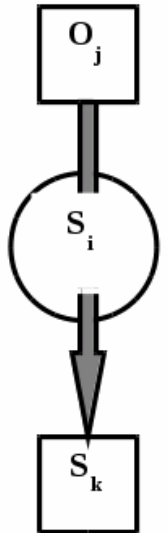
Понятия субъектов доступа и пользователей не тождественны.

Субъектно-объектная модель компьютерной системы

Субъекты порождаются субъектами (воздействием в момент времени t_k, а новый субъект порождается уже в момент времени $t_k + 1$).

- *Объект **O**$_f$ называется **источником** для субъекта **S**$_m$ если существует субъект **S**$_j$, в результате воздействия которого на объект **O**$_f$ возникает субъект **S**$_m$.*

- *Соответственно, субъект **S**$_j$, называется активизирующим для субъекта **S**$_m$, а объект **O**$_f$ – ассоциированным с **S**$_m$.*



Create (**S**$_j$, **O**$_f$) — **S**$_m$
(Если это невозможно, то *Create* (**S**$_j$, **O**$_f$) — 0)

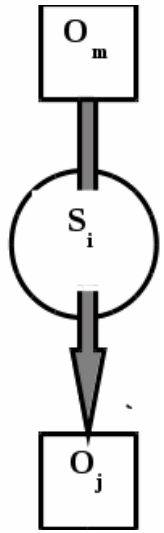
Create называют операцией порождения субъектов

Субъектно-объектная модель компьютерной системы

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

Потоком информации *между объектом* ***O****m и объектом* ***O****j называется произвольная операция над объектом* ***O****j, реализуемая в субъекте* ***S****i и зависящая от* ***O****m.*

Stream(***S****i* ***O****m*) → ***O****j*



- *Как Oj, так и Om могут быть ассоциированными или неассоциированными объектами, а также «пустыми» объектами (NULL).*
- *Объект-источник в момент порождения потока субъектом является ассоциированным с ним, а в последующие моменты времени может перестать быть или остаться ассоциированным с ним.*

Субъектно-объектная модель компьютерной системы

Поток всегда инициируется (порождается) субъектом.

- ***Доступом субъекта S**i; к объекту **O**j будем называть порождение потока информации между некоторым объектом (например, ассоциированным с субъектом объектами **S**i(**O**m)) и объектом **O**j.*

Пусть

***P** множество потоков для 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.*

Субъектно-объектная модель компьютерной системы

Аксиома 1: В защищенной сети в любой момент времени все объекты и все субъекты должны быть персонифицированы.

Аксиома 2: *В защищенной КС должна присутствовать активная компонента (субъект, процесс и т. д.) с соответствующим объектом(ами)-источником, которая осуществляет управление доступом и контроль доступа субъектов к объектам.*

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 обращений** (МО) - субъект, активизирующийся при возникновении потока от любого субъекта к любому объекту.*

***Монитор безопасности объектов** (МБО) - монитор обращений, который разрешает поток, только из множества легального доступа L.*

МБО является механизмом 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 выполнения своих функций.*
- **Непрерывность:** *Монитор безопасности должен функционировать любых штатных и нештатных, в том числе и аварийных ситуациях*

Монитор Безопасности

- ***Аксиома 3.*** *Для реализации принятой политики безопасности, управления и контроля доступа субъектов к объектам необходима (должна существовать) информация и объект(ы), ее содержащий(ие) (помимо информации для идентификации и аутентификации пользователей).*

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 для управления политикой разграничения доступа.*

Политики безопасности

Выделяется две основных (базовых) политики безопасности - дискреционная и мандатная. В терминологии сферы защиты компьютерной информации, первую называют политикой избирательного доступа или матричной моделью доступа, а вторую - политикой полномочного доступа или потоковой моделью доступа.

Политика дискреционного (избирательного) доступа.

Множество безопасных (разрешенных) доступов L задается для именованных пользователей (субъектов) и объектов явным образом в виде дискретного набора троек "Пользователь(субъект)-поток(операция)-объект".

Политики безопасности

Политика мандатного (полномочного) доступа.

Множество безопасных (разрешенных) доступов $\mathbf{P_L}$ задается неявным образом через введение для пользователей-субъектов некоторой дискретной характеристики доверия (уровня допуска), а для объектов некоторой дискретной характеристики конфиденциальности (грифа секретности), и наделение на этой основе пользователей-субъектов некими полномочиями порождать определенные потоки в зависимости от соотношения "уровень допуска – поток (операция) - уровень конфиденциальности ".

Политики безопасности

Политика тематического доступа.

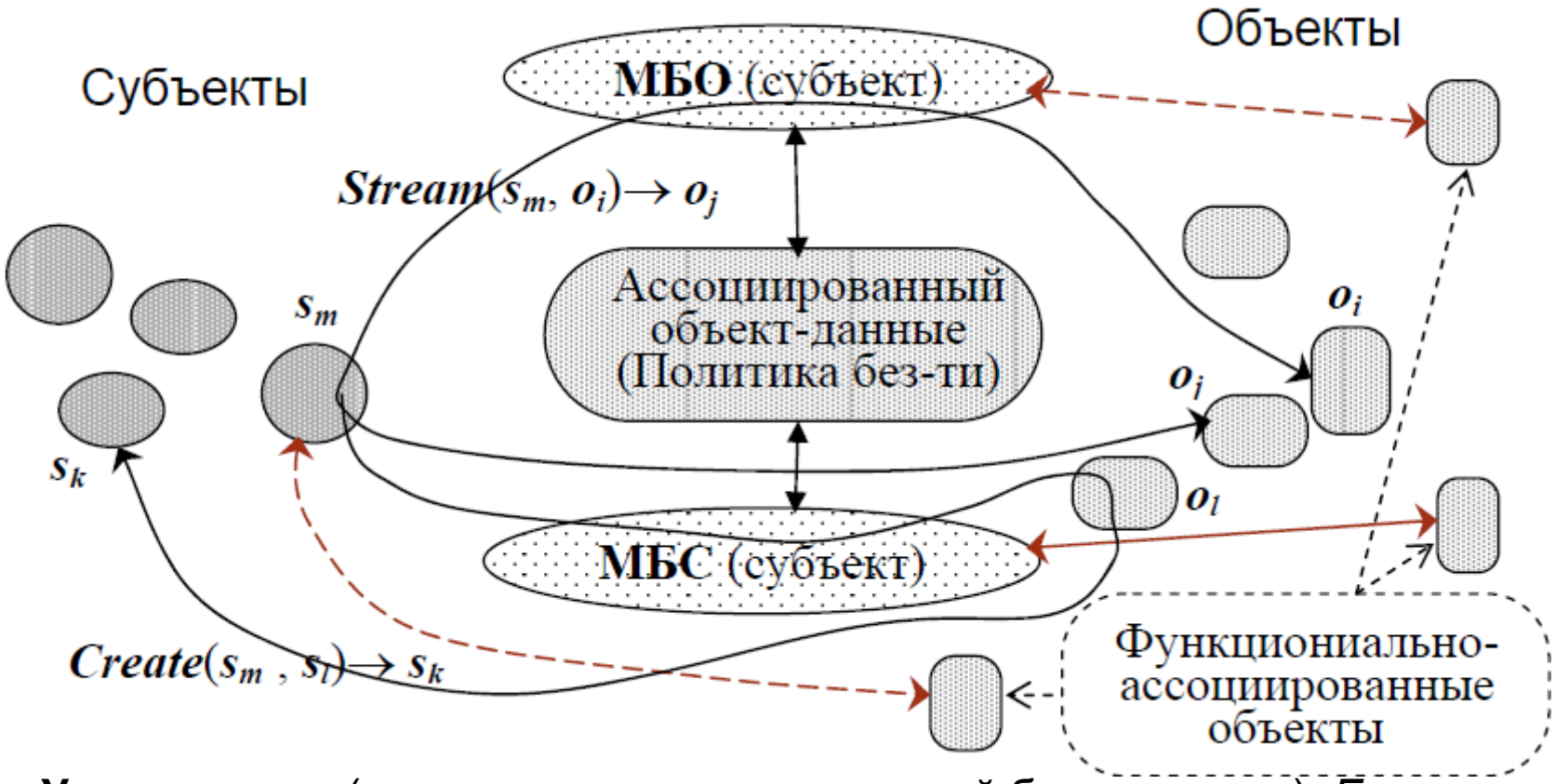
Множество безопасных (разрешенных) доступов ***L*** задается неявным образом через введение для пользователей-субъектов некоторой тематической характеристики - разрешенных тематических информационных рубрик, а для объектов аналогичной характеристики в виде набора тематических рубрик, информация по которым 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 историческом порядке:
  - Опакетные фильтры
  - Ошлюзы уровня приложений
  - Ошлюзы 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

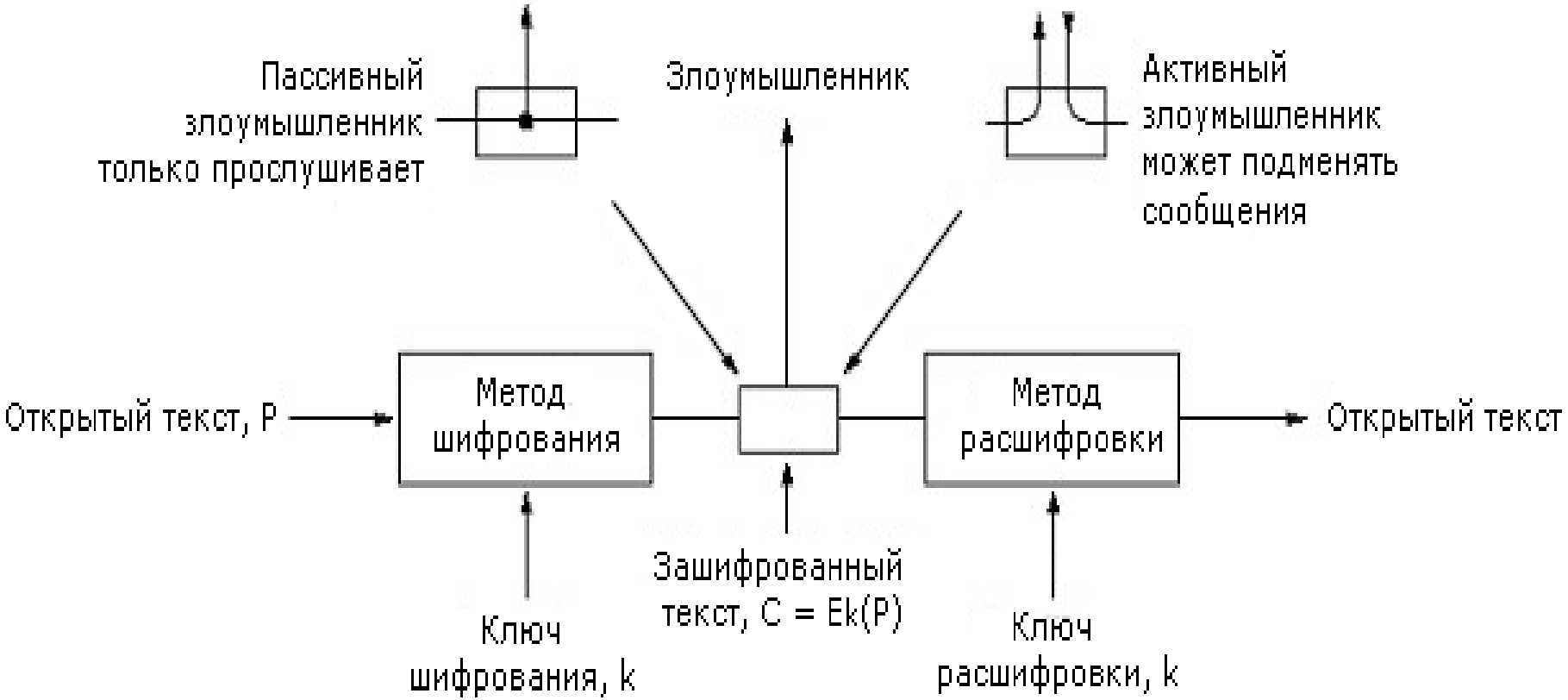
Шлюзы уровня приложений

- 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

Шифрование: модель



Шифрование

- Основная секретность – ключ. Его длина – один из основных вопросов разработки.
- 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	_	_	_	_	_	_

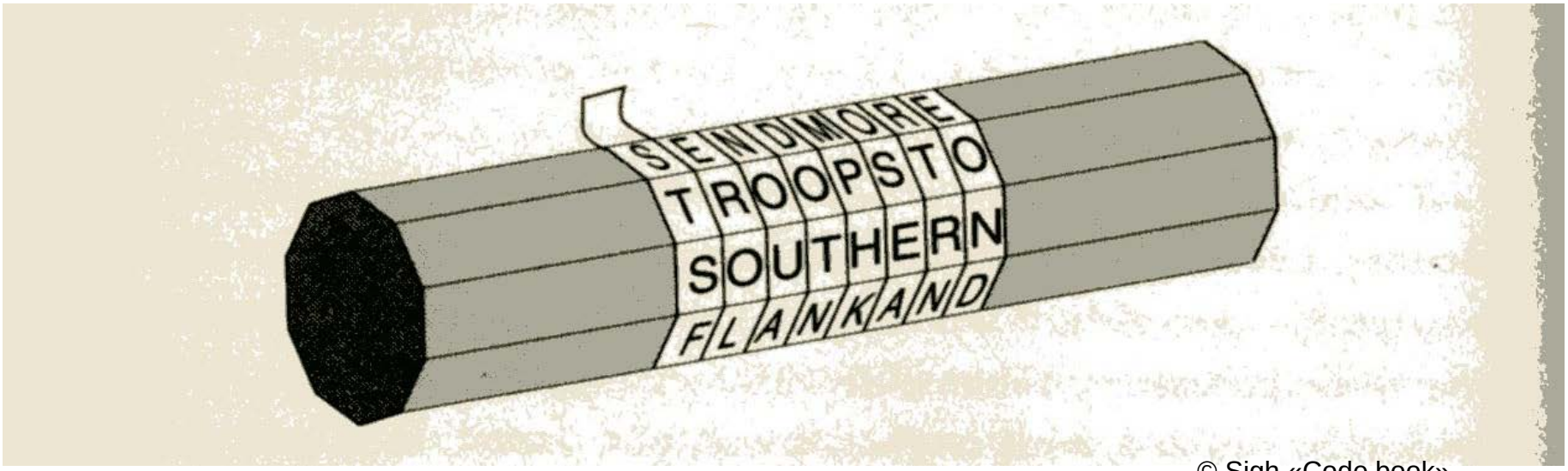
Открытый текст:

высылайтеденьгибочками

Зашифрованный текст:

йгм_аьа_лнк_ыеч_сдо_ыеб_втии

Шифр перестановкой

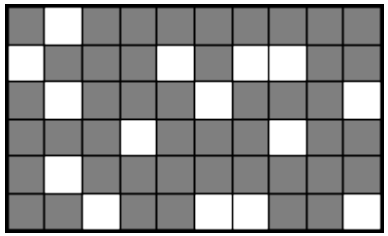


© Sigh «Code book»

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 перестановкой

- 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.

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

Квадрат Виженера, или tabula recta

Великий шифр Россиньоля

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																					

Два основных принципа шифрования

- *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.*

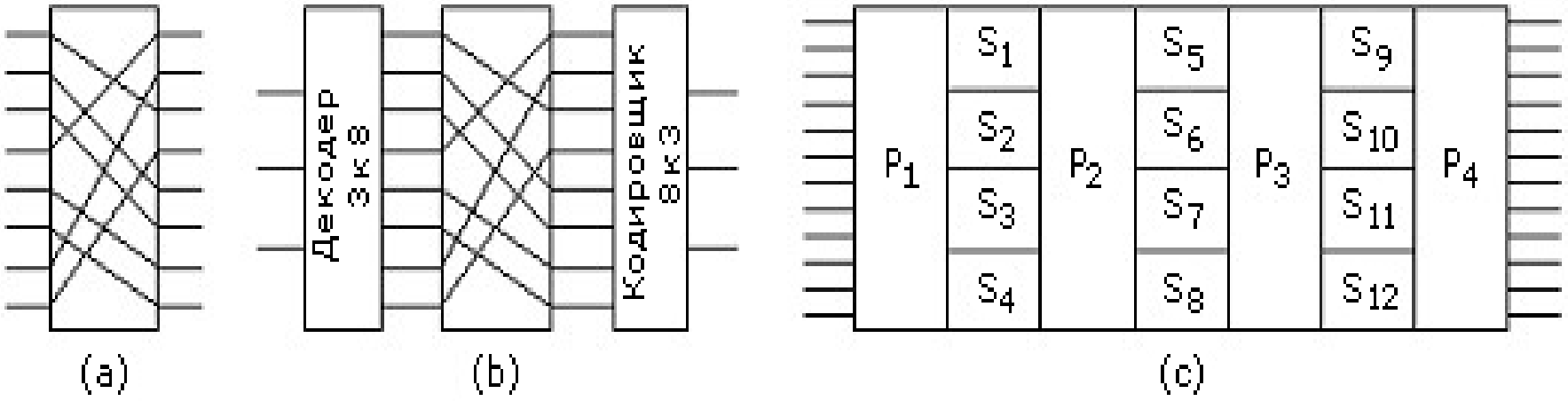
Алгоритмы с секретными ключами

(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.

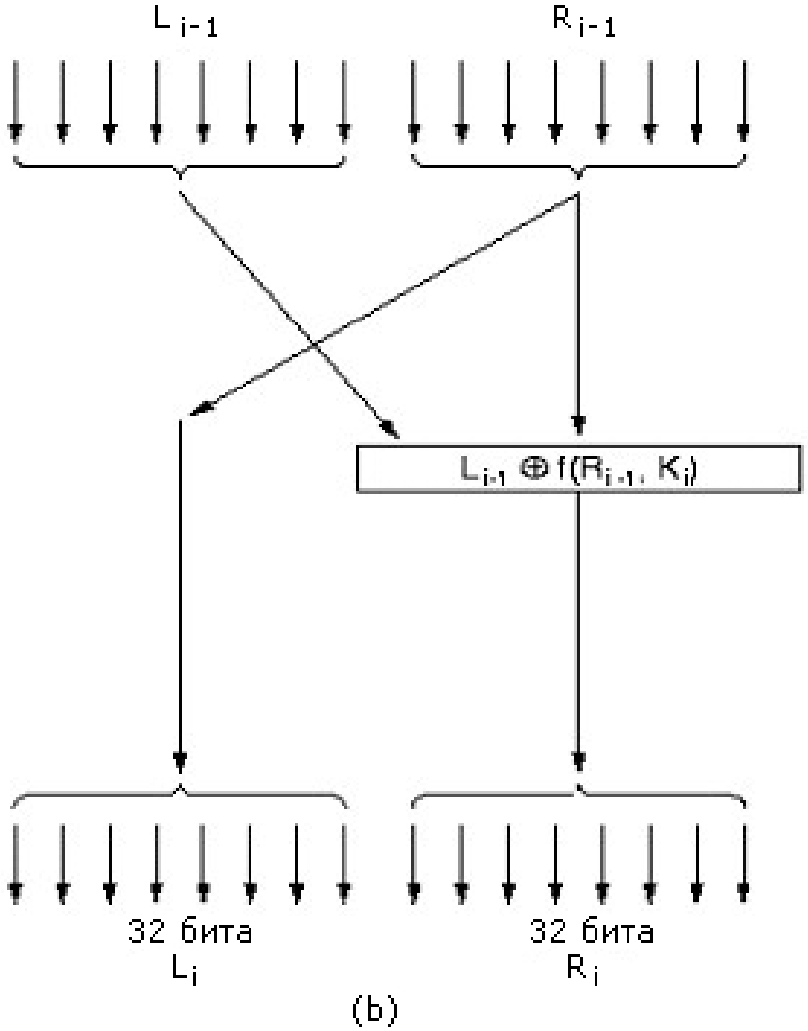
Базовые схемы шифрования



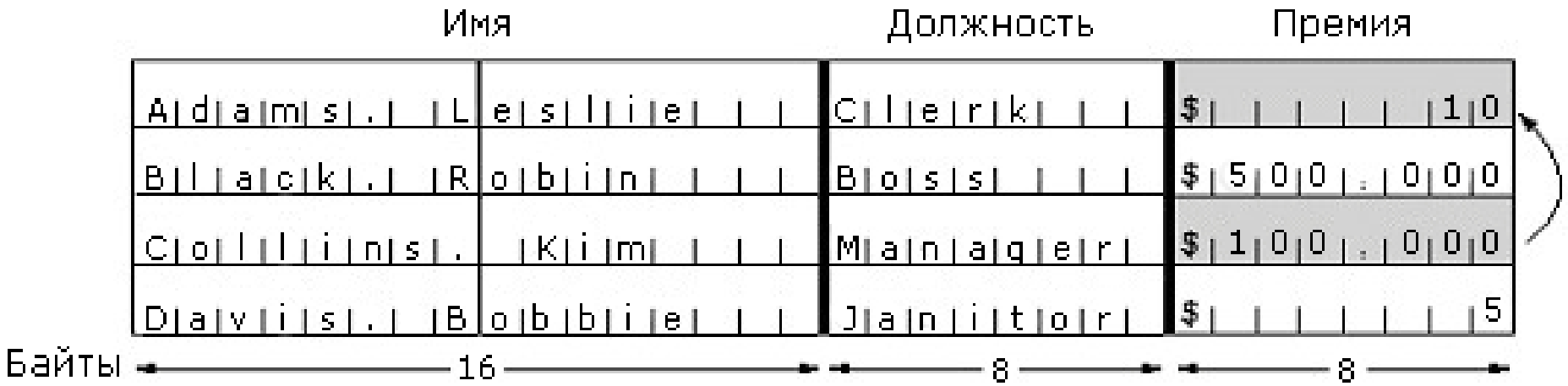
Алгоритм DES

- 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.

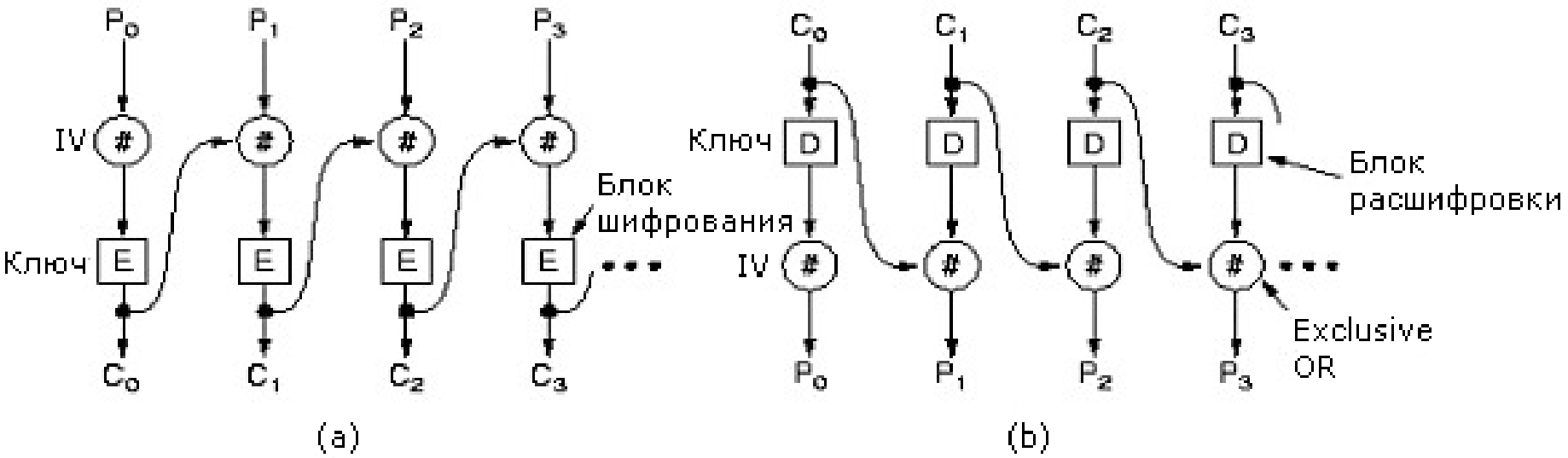
Алгоритм DES



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	$P^3 (mod 33)$	C^7	$C^7 (mod 33)$	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 $e=3$.

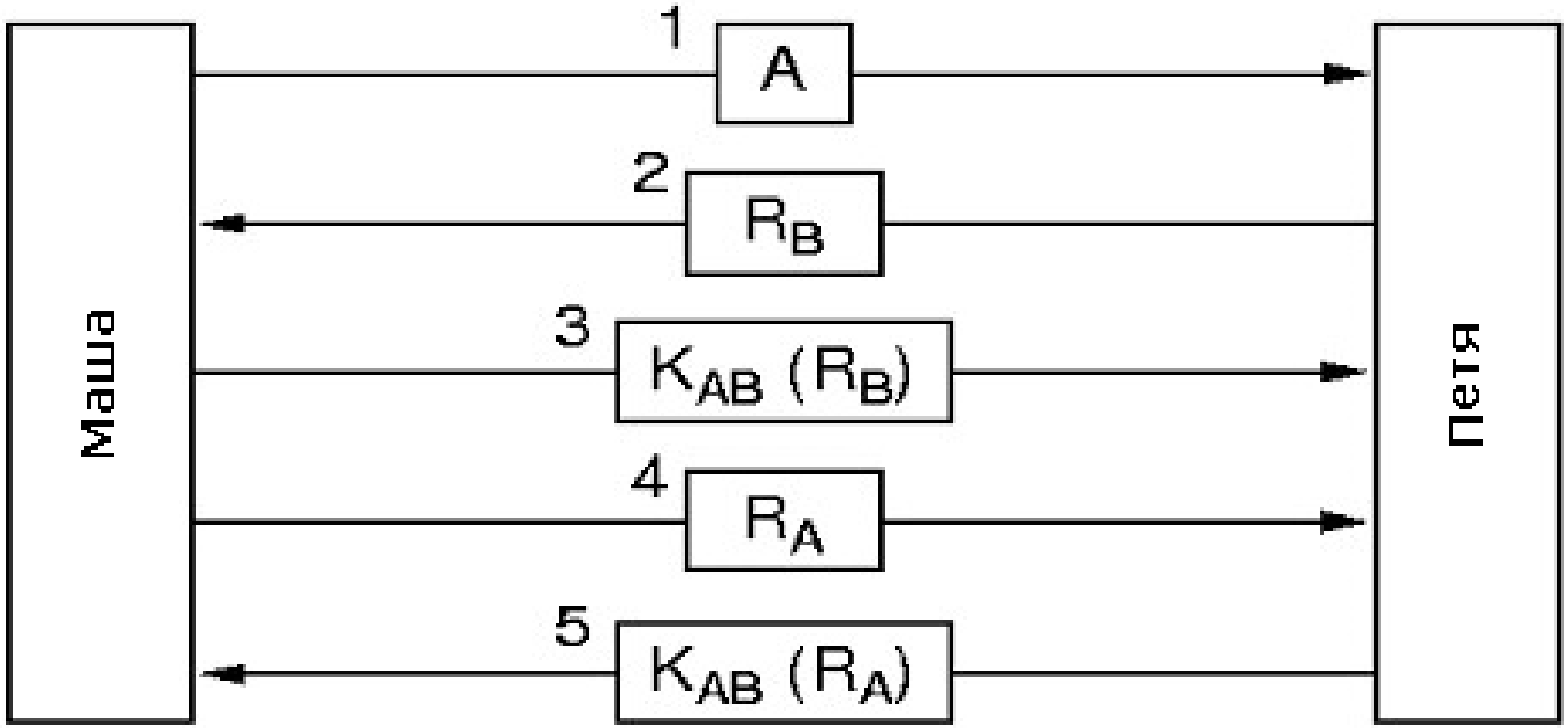
Протоколы установления подлинности

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.

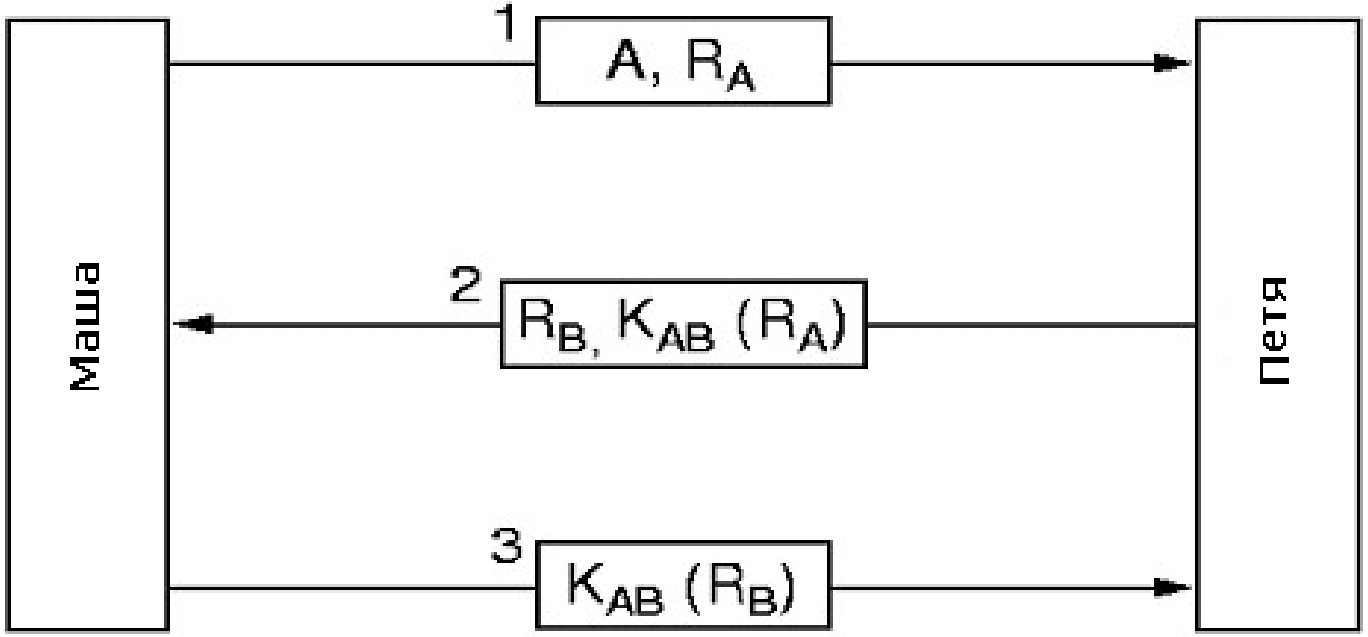
- Общая схема всех протоколов аутентификации такова: A и B начинают обмениваться сообщениями между собой или с Центром раздачи ключей (ЦРК). ЦРК всегда надежный партнер.
- Протокол аутентификации должен быть устроен так, что даже если злоумышленник перехватит сообщения между A и B, то ни A ни B не спутают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

Аутентификация на основе секретного ключа

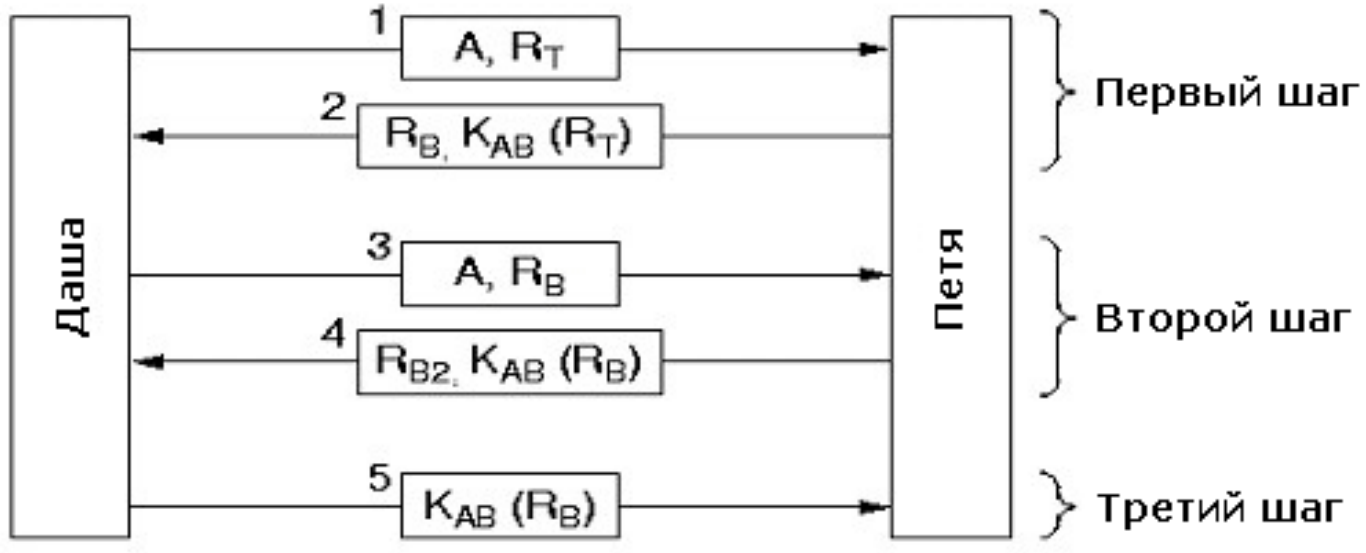


K_{AB} – общий ключ, R_A, R_B - вызовы

Сокращенная двусторонняя аутентификация



Атака отражением

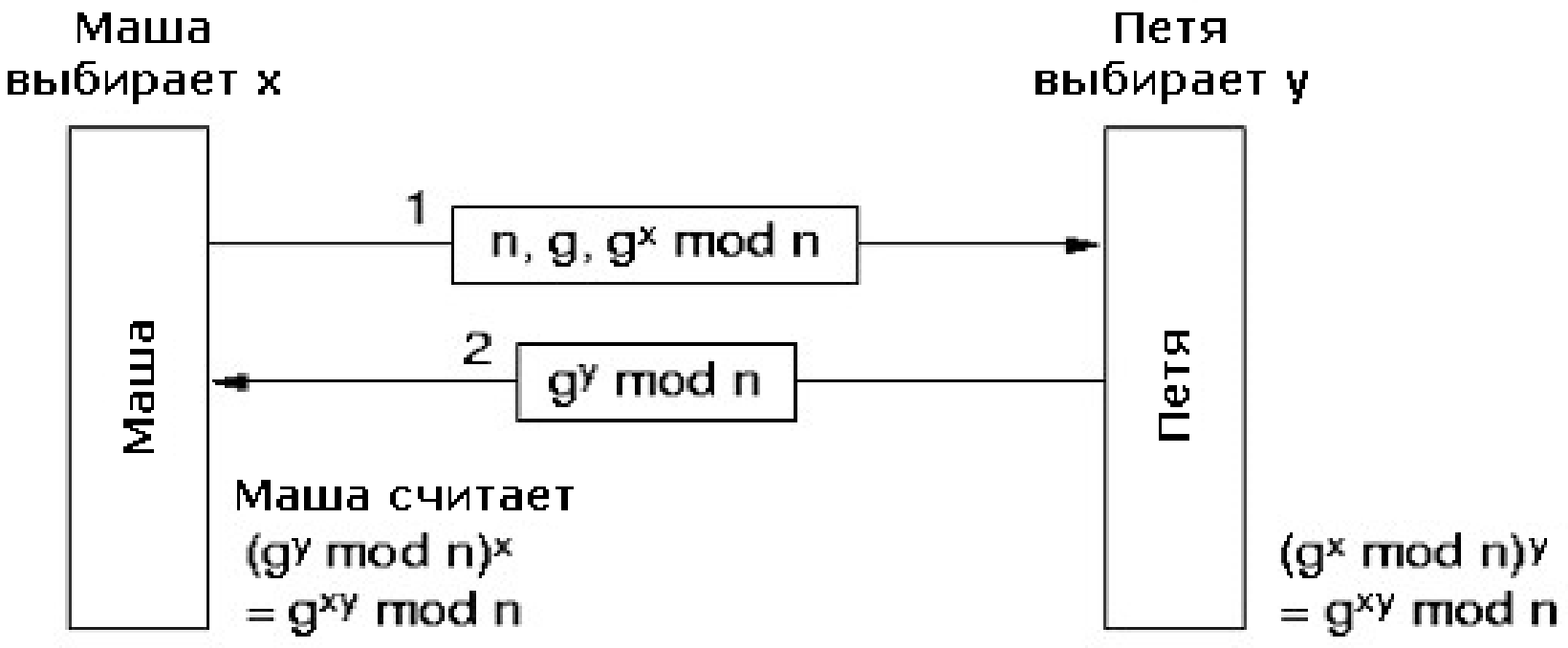


Даша - злоумышленник

На основе секретного общего ключа

- Аутентификация на основе закрытого общего ключа - протокол ответ по вызову.
- Общие правила построения протоколов аутентификации (протокол проверки подлинности или просто подлинности):
  - Инициатор должен доказать кто он есть прежде, чем вы пошлете ему какую-то важную информацию.
  - Инициатор и отвечающий должны использовать разные ключи.
  - Инициатор и отвечающий должны использовать начальные вызовы из разных непересекающихся множеств.
- Атака отражением.

Протокол Диффи-Хеллмана установления общего секретного ключа

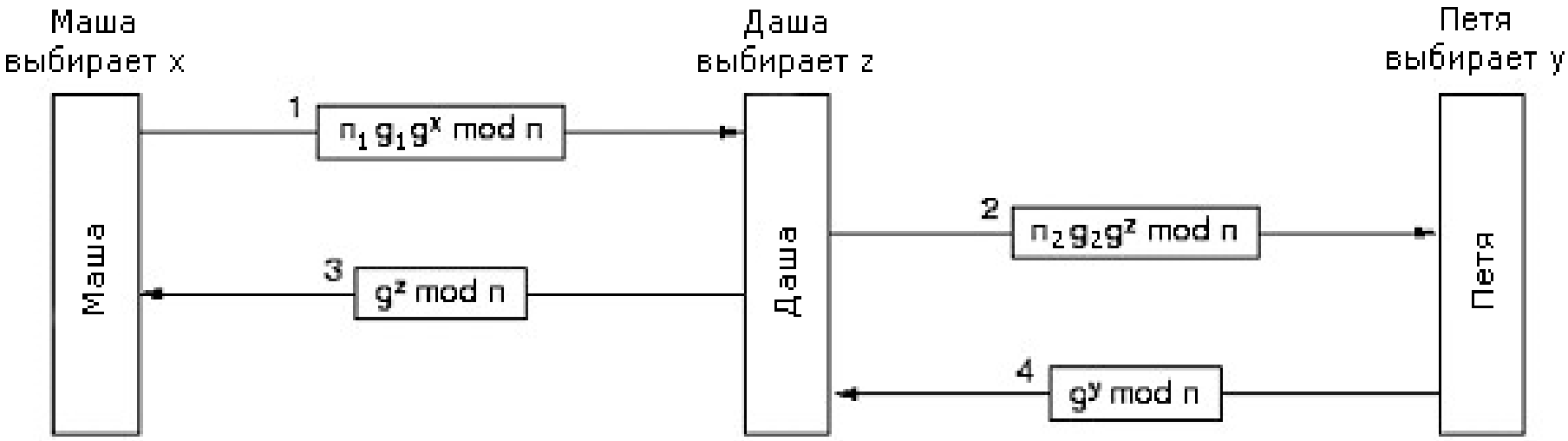


n,g – простые числа

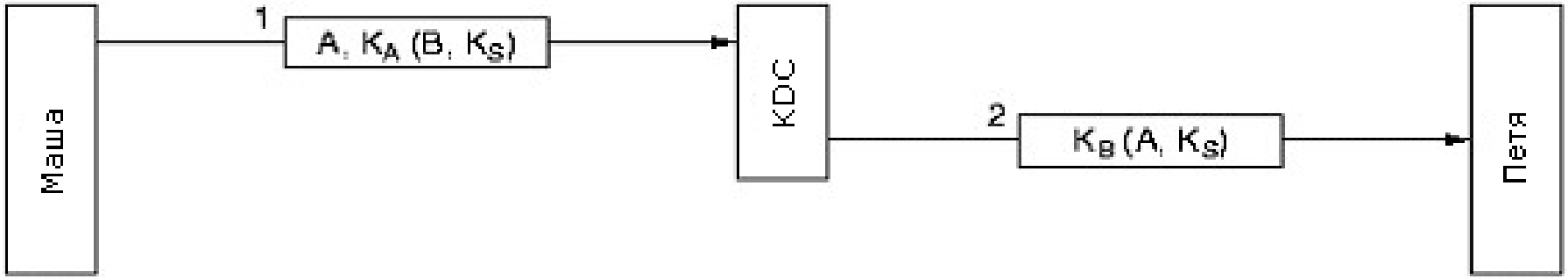
Установка общего ключа

- Как A и B могут установить общий секретный ключ?
  - Протокол обмена ключом Диффи-Хеллмана
  - 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



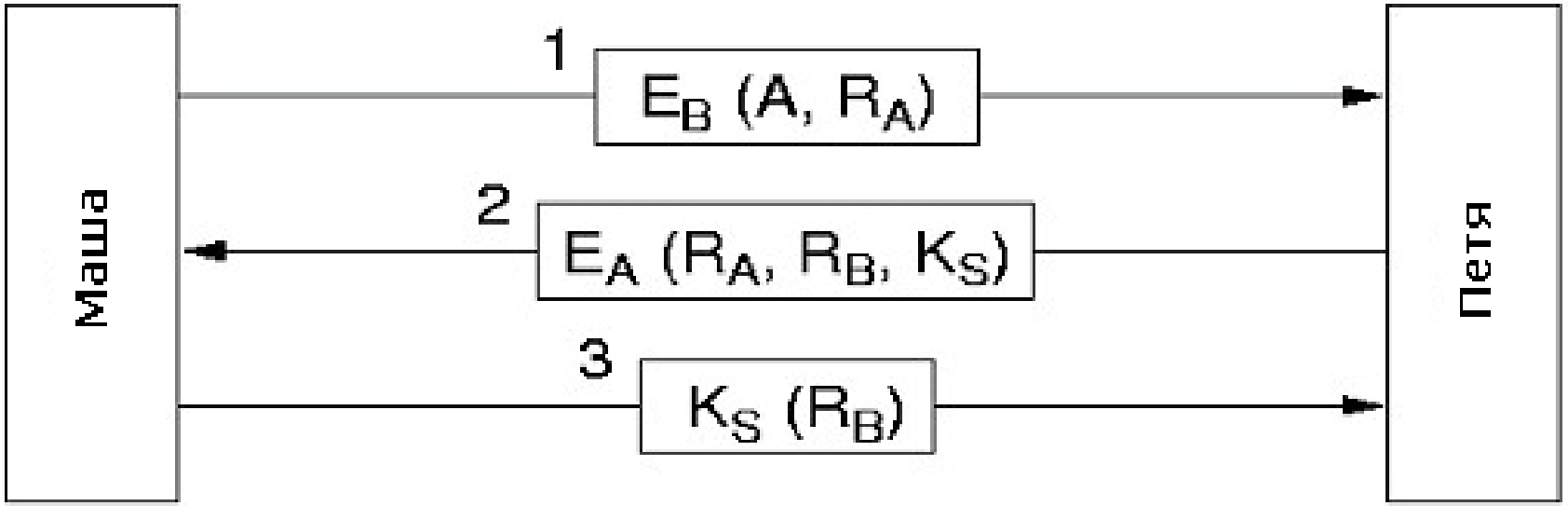
Проверка подлинности через центр раздачи ключей



Через центр раздачи ключей

- ***Атака подменой***
  - Против такой атаки есть несколько решений:
    - ***временные метки***.
    - ***разовые метки***.
- Протокол Нидхема-Шредера.
  - Опасность если злоумышленник раздобудет все-таки старый ключ сессии, то он сможет подменить сообщение 3 старым и убедить B, что это A!
- Протокол Отвей и Риис.

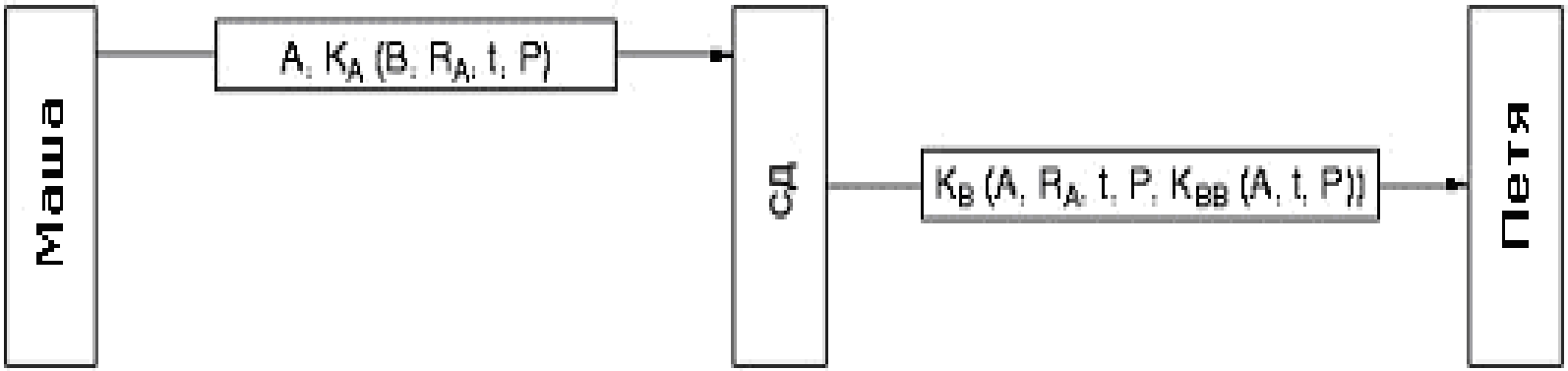
Взаимная аутентификация на основе открытых ключей



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.

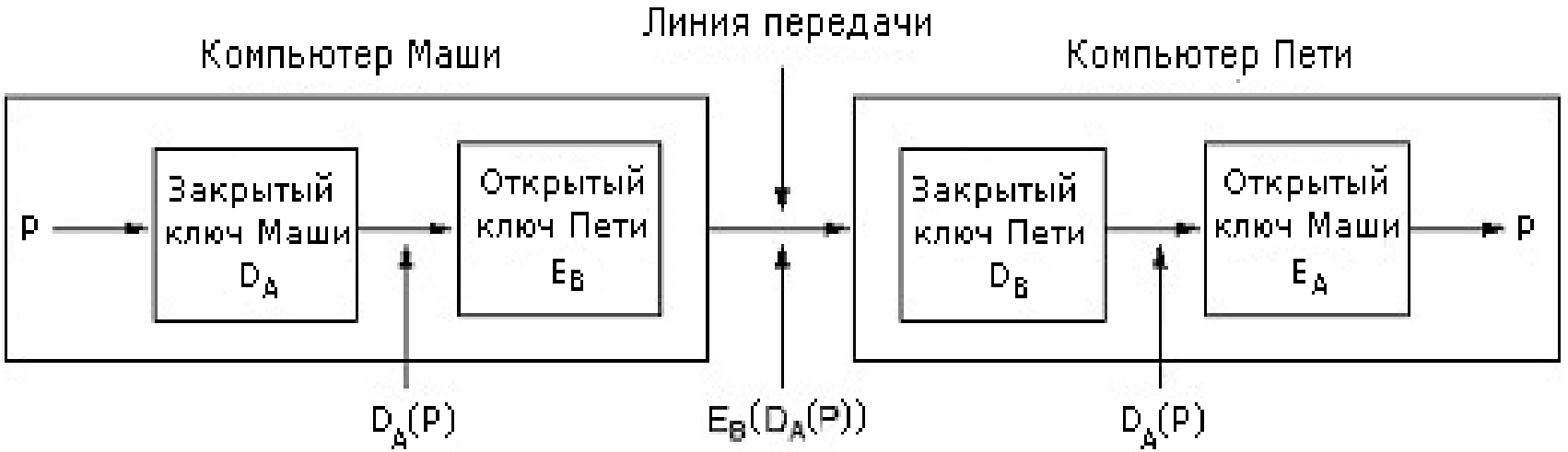
Электронная подпись посредством СД



Подпись на основе открытого ключа

- Все должны доверять СД, который может читать сообщения.
- Схема электронной подписи на основе открытых ключей.
  - D_X - закрытый ключ, E_X – открытый ключ;
  - *Предполагаем*
    - *E(D(P))=P дополнительно к D(E(P))=P (Этим свойством обладает RSA);*
  - Схема работает до тех пор, пока сторона А либо умышленно не рассекретила свой ключ, либо не изменила его в одностороннем порядке.
  - Судебный случаи.

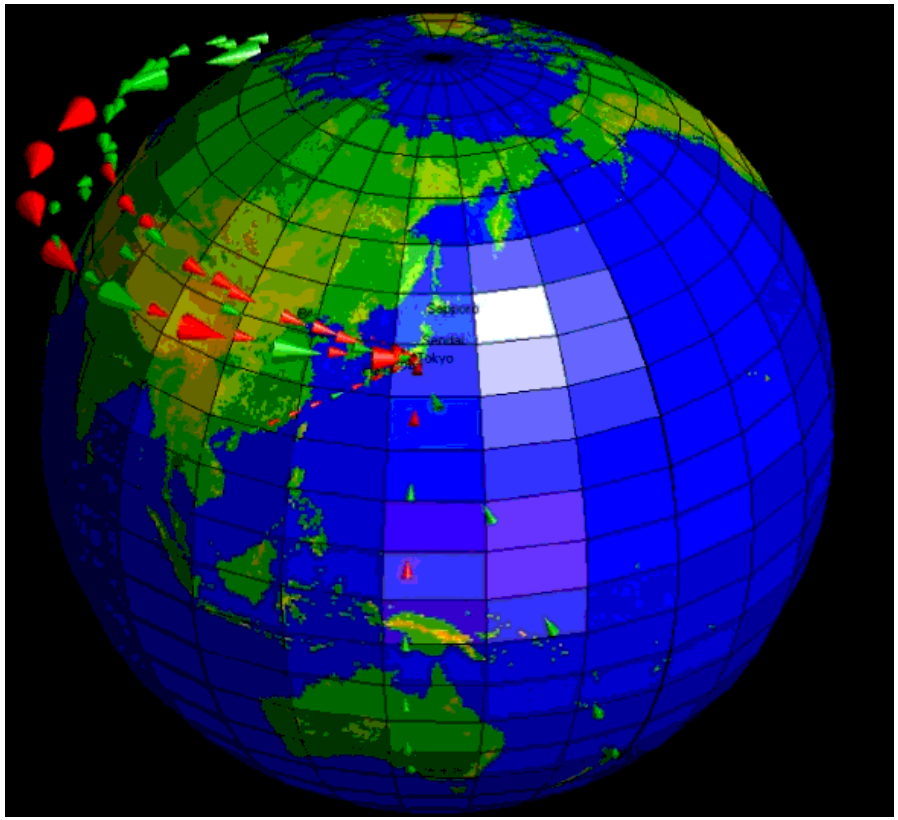
Электронная подпись на основе открытого ключа



Обнаружение и предотвращение компьютерных атак

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

Обнаружение атак



- Обнаружение сетевых атак и защита от них
- Три основных класса атак
  - Сканирование (разведка)
  - Несанкционированный доступ
  - Отказ в обслуживании

Системы обнаружения атак

Система обнаружения атак – это системы идентификации. Которая является комбинацией аппаратуры и программного обеспечения, которая идетифицирует вредоносную активность в сети

Примеры систем обнаружения атак в реальной жизни:

- Автомобильная сигнализация
- Датчики возгорания
- Домашняя сигнализация
- Системы видеонаблюдения

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
  - Пример: плагин Spade для COA Snort, Bro IDS
  - 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
  - Примеры: Snort, Suricata
  - Менее склонны к ложным срабатываниям
  - **Не могут обнаруживать даже варианты реализации известных атак, которых нет в базе описаний**

Сигнатурное обнаружение атак

- **Сигнатуры**
  - **Набор шаблонов, описывающих типичные для известных реализаций атак особенности действий и их атрибутов**
- **Типы сигнатур**
  - ***Атомарные*** — срабатывают на содержимое одного пакета

    Пример: поиск строки "/etc/passwd " в трафике
  - ***Составные*** — срабатывают на последовательности из нескольких пакетов

Примеры сигнатур Snort

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:”ICMP
   PING NMAP”; dsize: 0; itype: 8;)
```

- Алерт для пакета ICMP с пустым телом, ICMP type 8, адрес источника – во внешней сети.
- Такие пакеты используется в NMAP ping.

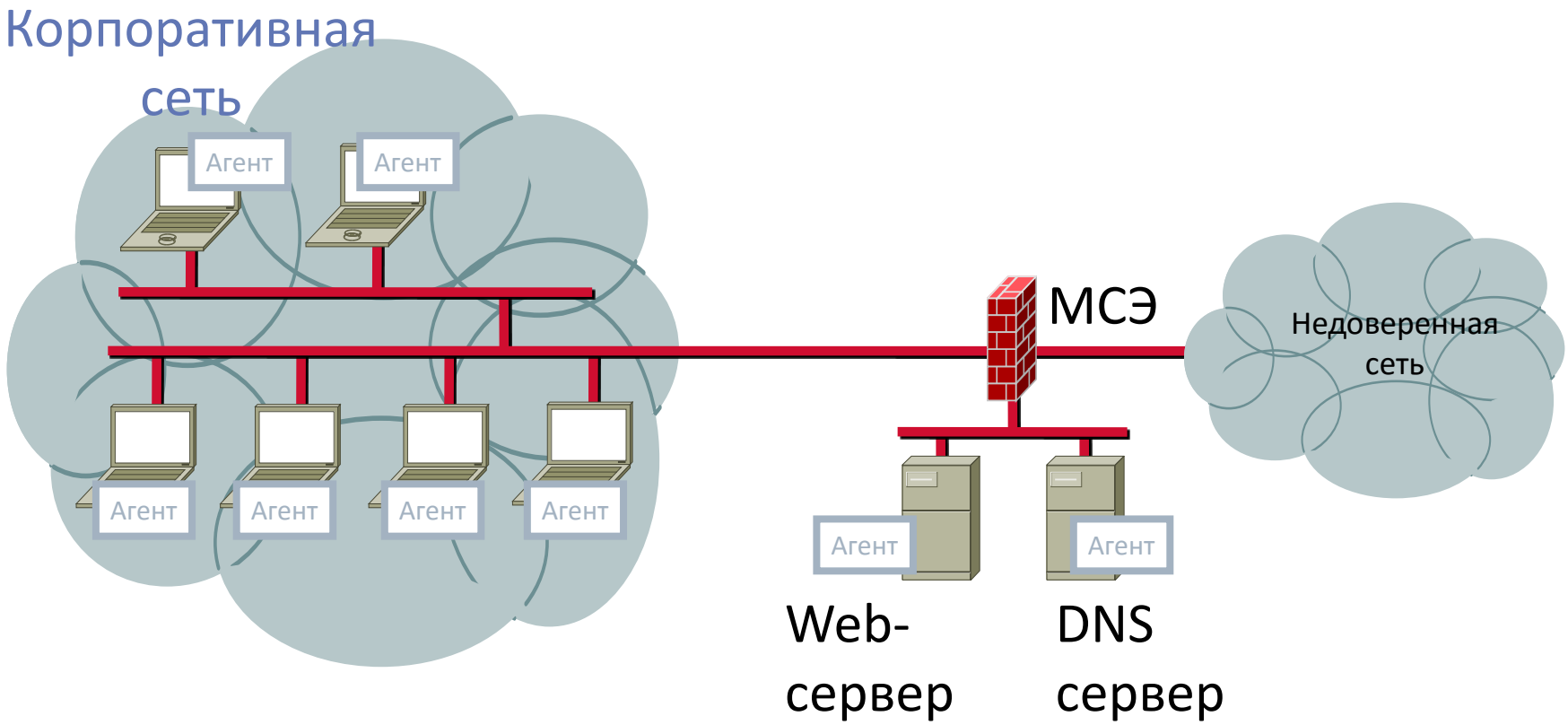
```
alert tcp $EXTERNAL_NET any -> $HOME_NET 139(msg: “DOS
   SMBdie attack”:; flags: A+;
   content:”|57724c6568004577a|”;)
```

- Алерт если TCP сегмент содержит |57724c6568004577a| и направлен на порт 139 (netbios) некоторого внутреннего узла.
- Это часть атаки переполнения на Server Message Block Service.

Типы систем обнаружения атак

- **Узловые СОА**
  - Программные наблюдатели (Агенты) установлены на узлах
  - Выполняют анализ журналов приложений, контроль целостности файлов, контроль политик безопасности, обнаружение руткитов
  - **Примеры:**
    - Cisco Security Agent (CSA) , OSSEC, Tripwire

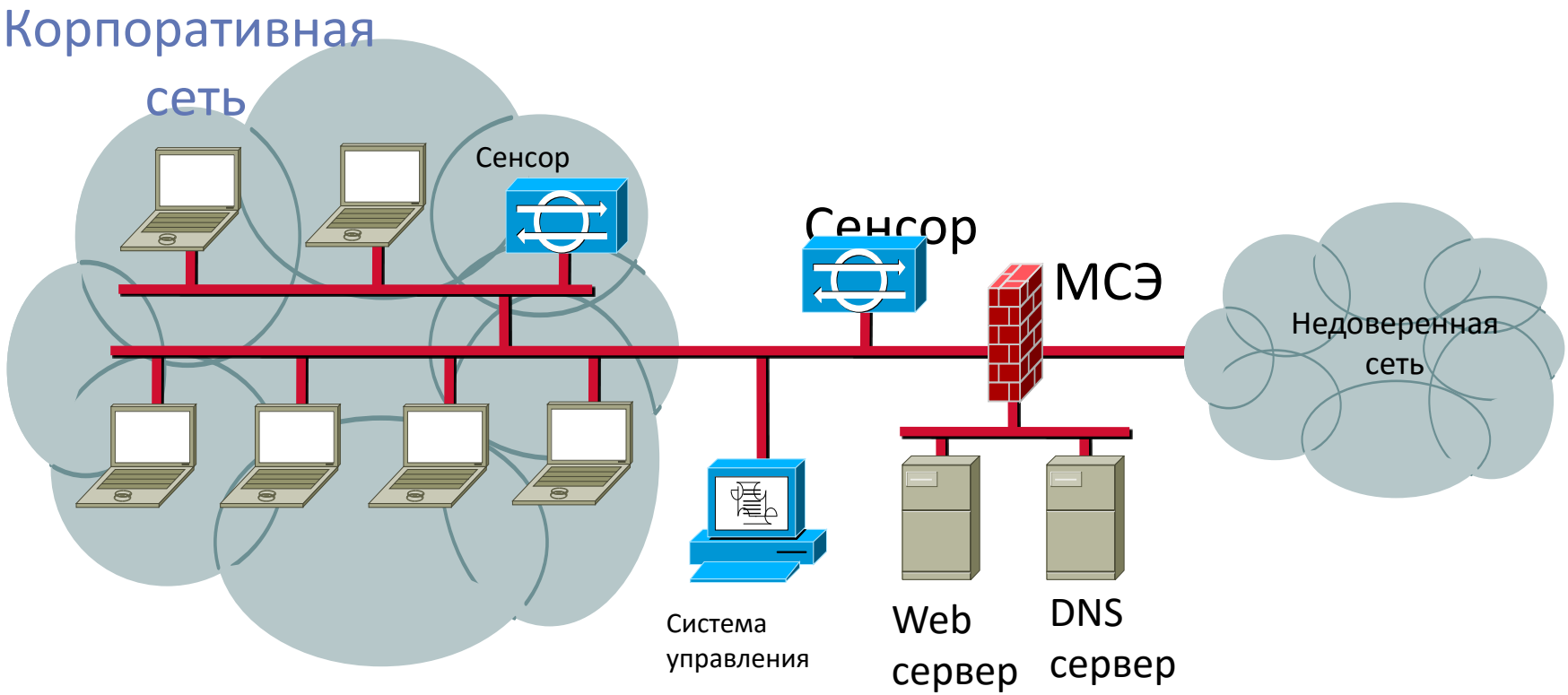
Узловые системы обнаружения атак



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



Ложные срабатывания и необнаружение

Ошибки СОА:

- False positive: нормальный трафик вызывает срабатывание СОА
  - Пример: алерт при неправильном вводе пароля; легитимные пользователи тоже ошибаются
- False negative: атака не обнаруживается

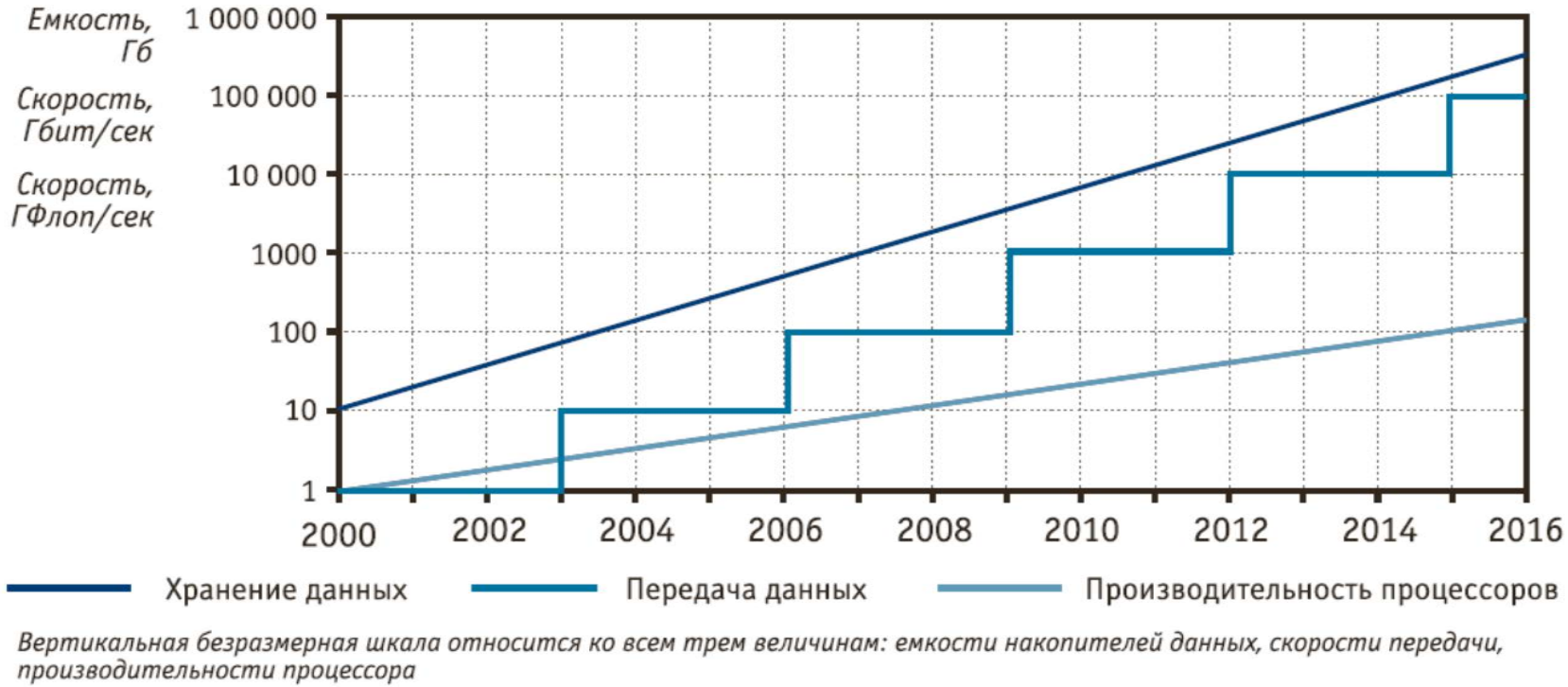
Вопрос эффективности COA

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

Виртуальные частные сети

- Объединение выделенных (и возможно географически удалённых) каналов связи в логически единую сеть
- Весь трафик шифруется, при этом подключение прозрачно для всех протоколов
- Подключаемые узлы проходят аутентификацию
- Типы VPN
  - Пользовательские – подключение удалённых пользователей
  - Узловые – подключение удалённых подсетей (филиалов)
- Компоненты VPN:
  - Сервер
  - Алгоритмы шифрования и аутентификации
  - Протокол VPN (IPSec, OpenVPN и т.д.)

Анализ трафика – задача реального времени



Вертикальная безразмерная шкала относится ко всем трем величинам: емкости накопителей данных, скорости передачи, производительности процессора

1GigE: минимальный пакет 64 байта, 672 нс на обработку (худший случай)

Проблемы информационной безопасности

(заключение)

- 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.
- Контроль доступа

Проблемы информационной безопасности

(заключение)

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