

Безопасность в Internet и intranet

1. Основы безопасности
2. Шифрование
3. Протоколы и продукты
4. Виртуальные частные сети

- Internet по своей природе – незащищенная технология
- Глобальные связи являются менее защищенными, чем локальные
- Общедоступные территориальные сети менее защищены, чем сети для корпоративных клиентов

Подавляющее большинство атак не только не блокируется но и не обнаруживается

- Было атаковано 8932 системы DoD (100%)
- Успешно прошло 7860 атак (88%)
- В 390 случаях атаки были обнаружены (5%)
- Сообщили об атаках 19 администраторов (0.24%)

Величина ущерба от атак

(в миллионах долларов США)

Тип атаки	1998	1999	2000
Вирусы (85%)	7,9	5,3	29,2
Злоупотребления собственными сотрудниками (79%)	54,3	11,2	28,0
Отказ в обслуживании (27%)	2,8	3,3	8,2
Кража информации внешн.(20%)	33,6	42,5	66,7
Телекоммуникационные мошенничества (11%)	17,3	0,8	4,0
Финансовые мошенничества (11%)	11,2	42,5	56,0
Всего:		124	266

Основы безопасности

Общие принципы защиты

- Использование комплексного подхода к обеспечению безопасности
 - ◆ Законодательные средства
- Принцип многоуровневой защиты.
 - ◆ Морально-этические средства
 - ◆ Соблюдение баланса надежности защиты всех уровней
 - ◆ Организационные (или процедурные) меры
- Принцип единого входа
 - ◆ Административные меры
- Принцип сохранения безопасности при отказе состояния
 - ◆ Максимальной защиты
 - ◆ Физические средства защиты
- Компромисс между возможными рисками (системы контроля доступа, аудита, шифрования, цифровой подписи, антивирусной защиты, фильтрующие маршрутизаторы, межсетевые экраны)
- Предоставление каждому сотруднику минимально достаточного уровня привилегий по доступу к данным

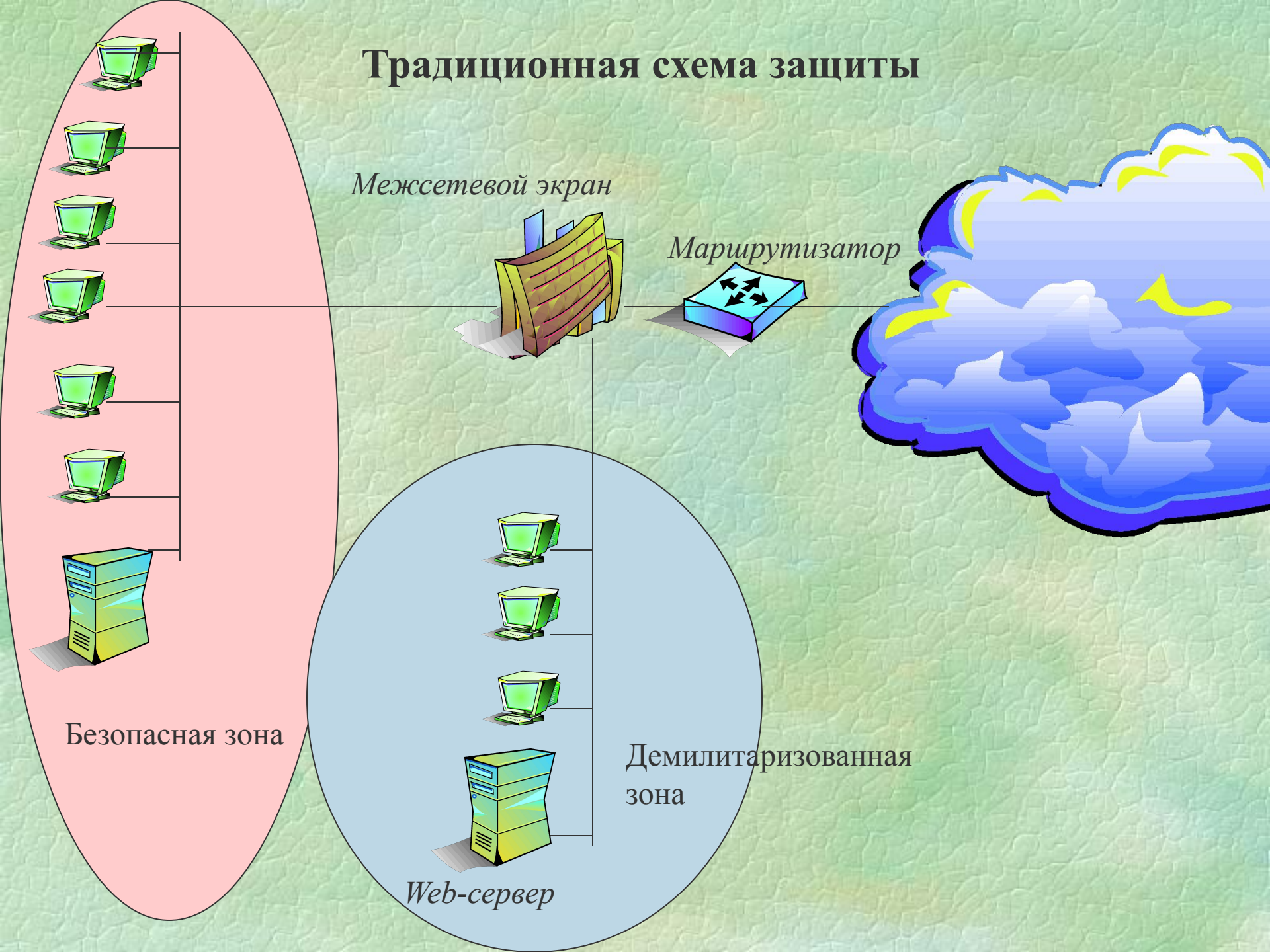
Выработка политики безопасности

- ◆ какую информацию и от кого следует защищать
- ◆ кому и какая информация требуется для выполнения служебных обязанностей
- ◆ какая степень защиты требуется для каждого вида информации
- ◆ чем грозит потеря того или иного вида информации
- ◆ как организовать работу по защите информации

Традиционная политика безопасности

- ♦ Защита межсетевым экраном
- ♦ определение сервисов внутренней сети, доступных для внешних пользователей
- ♦ определение списка сервисов Internet, пользователи внутренней сети должны иметь ограниченный доступ

Традиционная схема защиты



Свойства безопасной системы

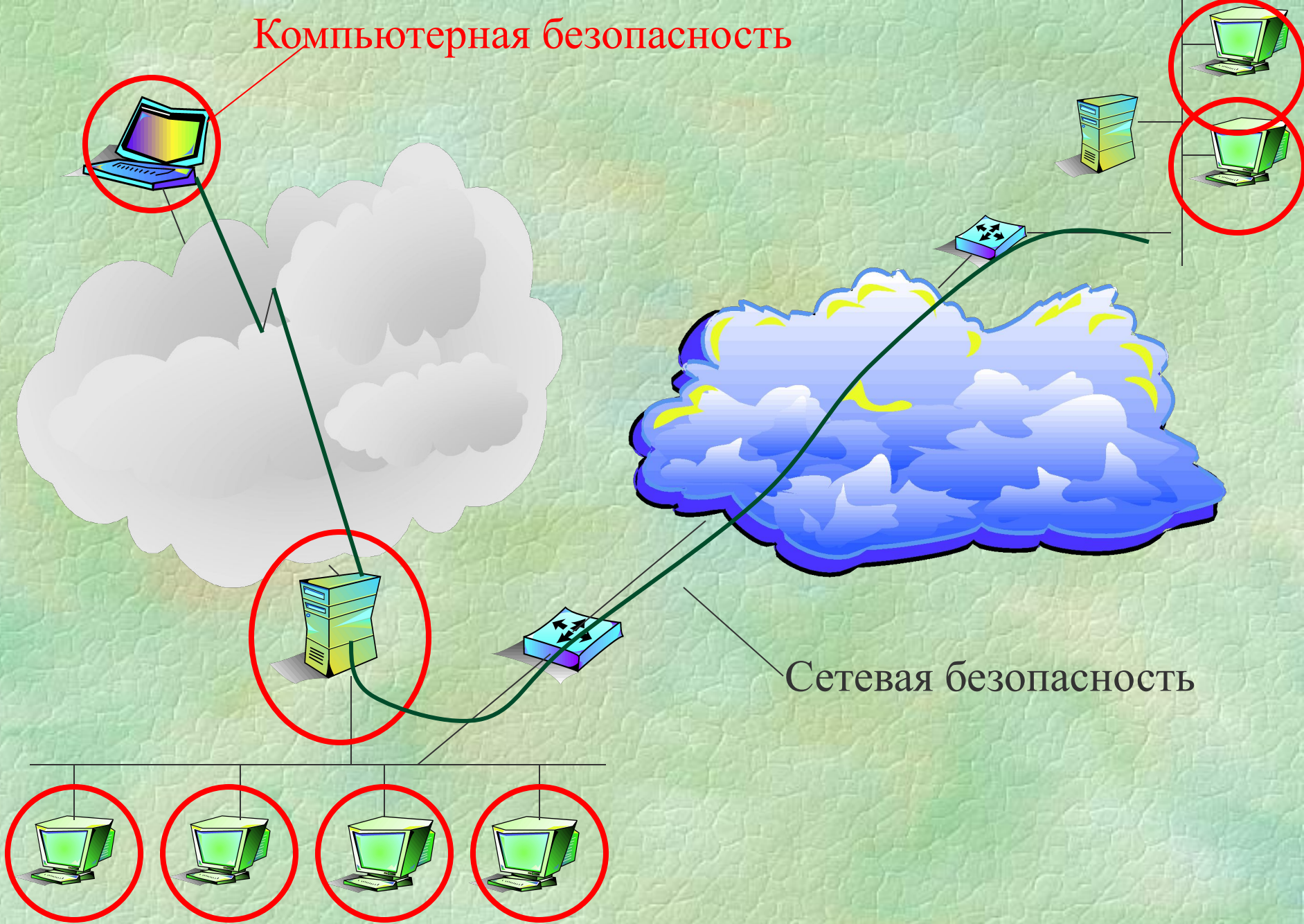
- ♦ **Конфиденциальность** (*confidentiality, privacy*) – гарантия того, что секретные данные будут доступны тем и только тем пользователям, которым этот доступ разрешен
- ♦ **Доступность** (*availability*) – гарантия того, что авторизованные пользователи всегда получают доступ к данным
- ♦ **Целостность** (*integrity*) – гарантия сохранности данными правильных значений

- Требования конфиденциальности, доступности и целостности могут быть предъявлены к устройствам
- Незаконное потребление ресурсов - нарушение безопасности системы

Безопасность информационных систем:

- ▣ **безопасность компьютера** - защита данных, хранящихся и обрабатываемых внутри компьютера; решаются ОС и приложениями, а также встроенными аппаратными средствами компьютера
- ▣ **сетевая безопасность** –
 - (1) защита данных в момент их передачи по линиям связи – **защита трафика**
 - (2) защита от несанкционированного удаленного доступа в сеть – **контроль доступа**

Компьютерная безопасность



Сетевая безопасность

Контроль доступа – программные и аппаратные средства аутентификации и авторизации, анализ входящего и выходящего трафика:

Модули ОС и приложений, межсетевые экраны (firewall), централизованные программные системы (Kerberos, Taccacs)

Защита трафика – шифрование, взаимная аутентификация сторон

Протоколы защищенных каналов (PPTP, IPSec, SSL), VPN, Firewall

Автоматизированный контроль безопасности

Системы обнаружения вторжений (SATAN, SAFESuite ISS)

Угроза –

любое действие, которое может быть направлено на нарушение конфиденциальности, целостности и/или доступности системы

Атака -

реализованная угроза

Риск —

вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса, в результате успешно проведенной атаки

Типы угроз

Неумышленные угрозы

- ошибки персонала
- отказы программ и оборудования

Умышленные угрозы

- пассивное чтение данных или мониторинг системы
- активные действия, например, нарушение целостности и доступности информации, приведение в нерабочее состояние приложений и устройств

Примеры угроз

- незаконное проникновение в один из компьютеров сети под видом легального пользователя
- разрушение системы с помощью программ-вирусов
- нелегальные действия легального пользователя
- «
внутрисетевого трафика.
подслушивание»

Базовые функции защиты

- ◆ Шифрование

- ◆ Аутентификация - определение легальных пользователей

- ◆ Авторизация - определение прав доступа для легальных пользователей

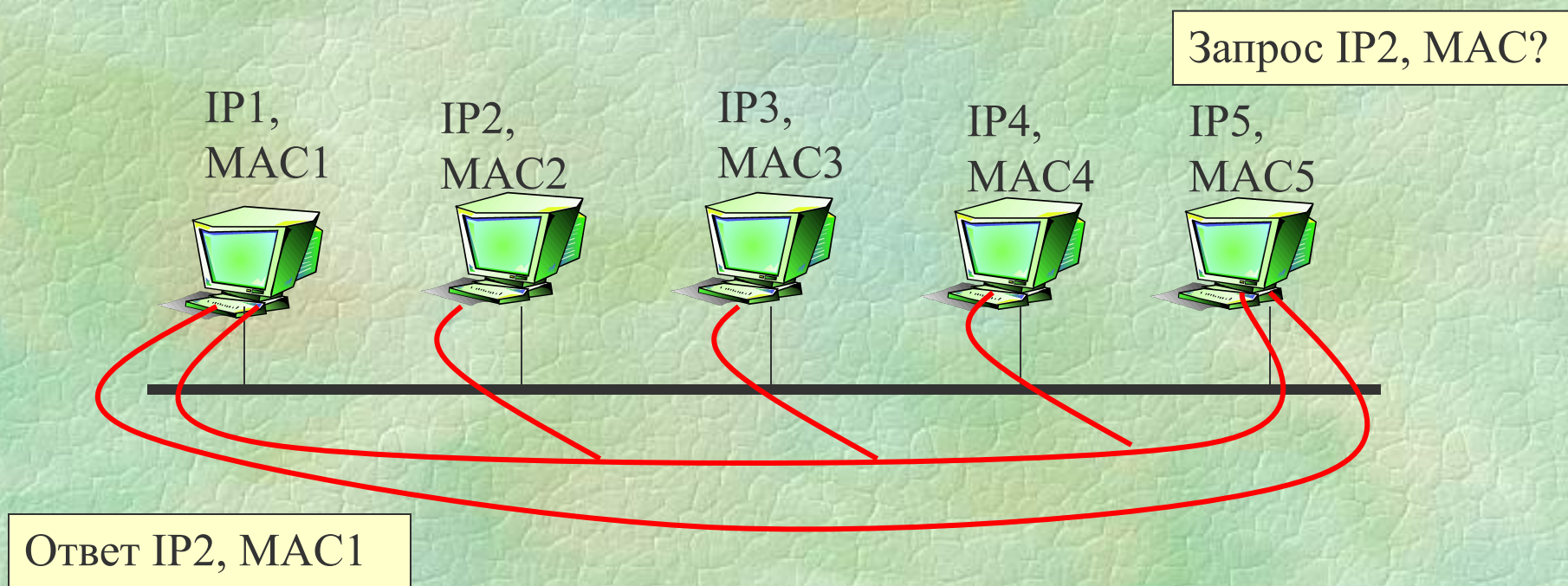
- ◆ Аудит - фиксация событий в системном журнале

- ◆ Технология защищенного канала

Специфика безопасности IP-сетей



Ложный ARP-ответ

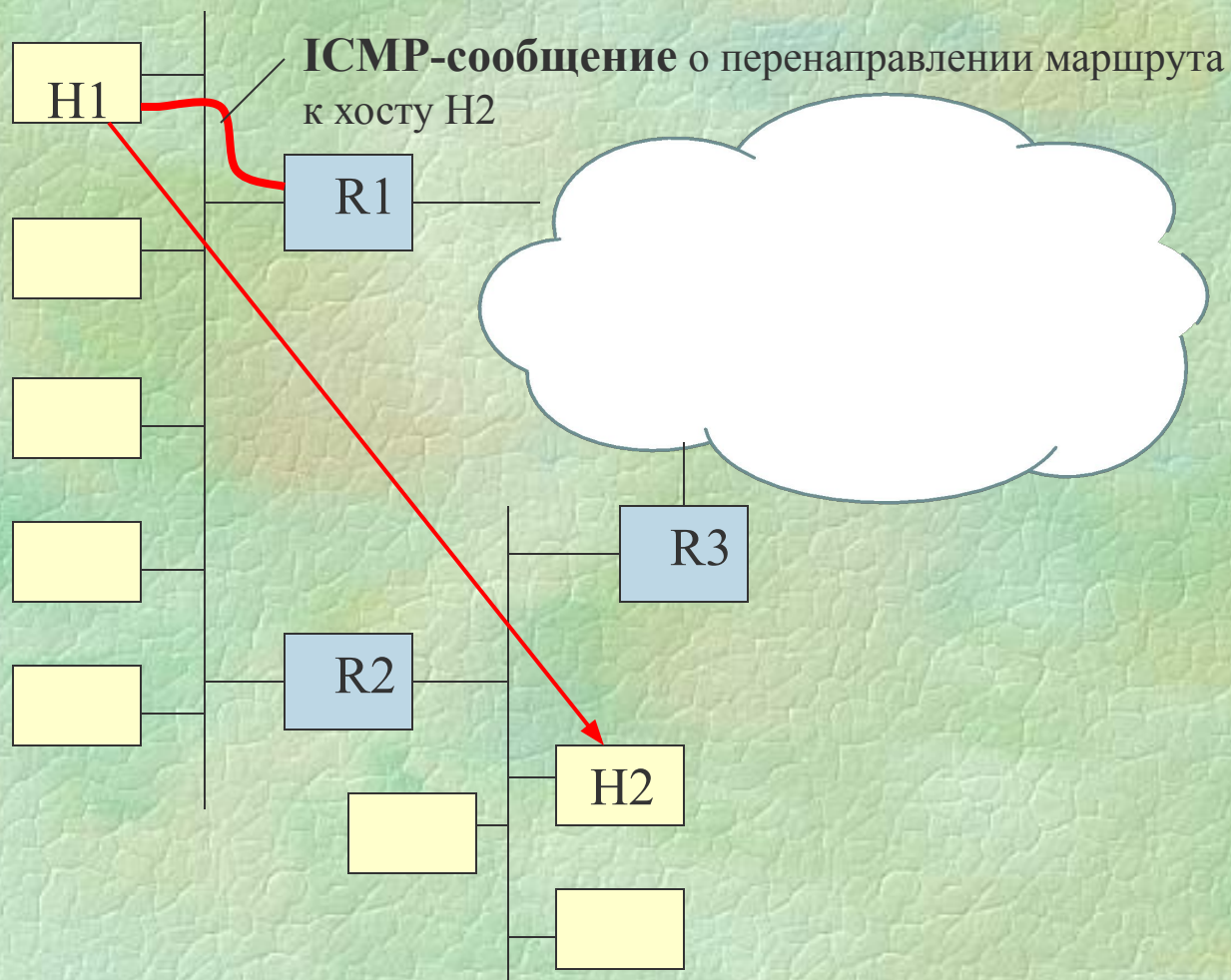


Перенаправление маршрута

средствами ICMP

Таблица маршрутизации
хоста H1

Default R1

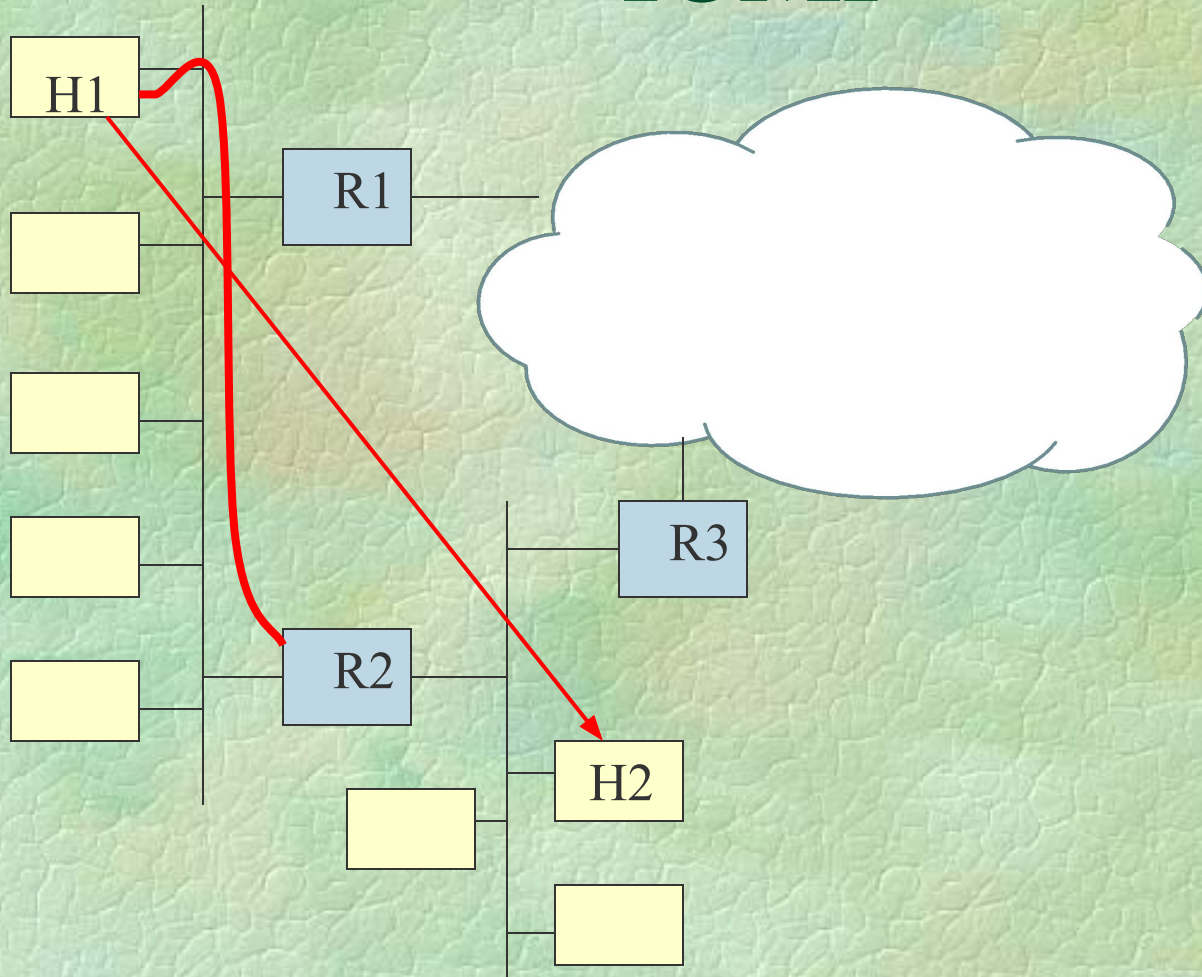


Type	Code	ChSum
Адрес марш-ра R2		
Заголовок пакета, отброшенного на маршрутизаторе R1		

Таблица маршрутизации хоста H1

Default	R1
H2	R2

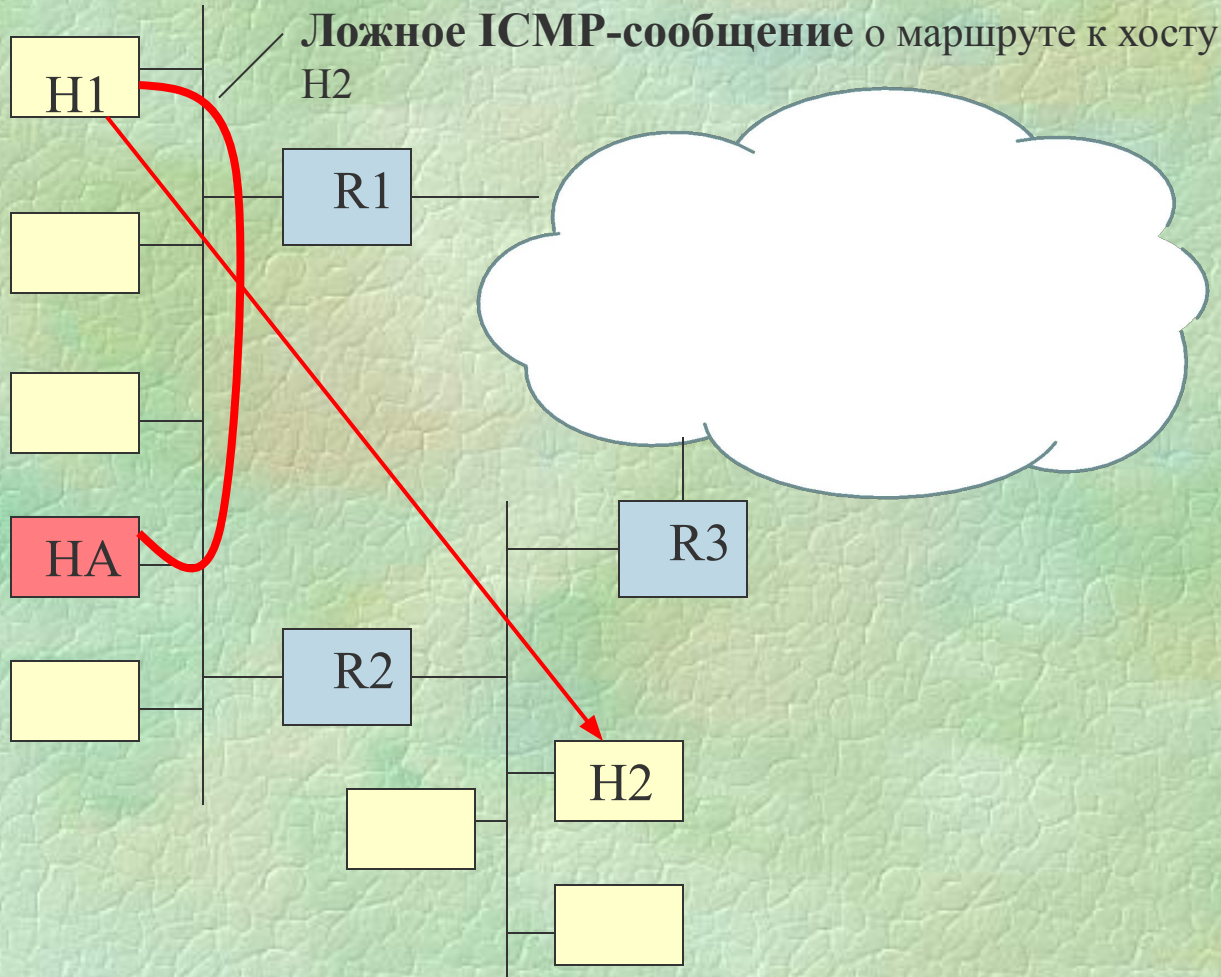
Перенаправление маршрута средствами ICMP



Навязывание ложного маршрута

Таблица маршрутизации хоста H1

Default R1

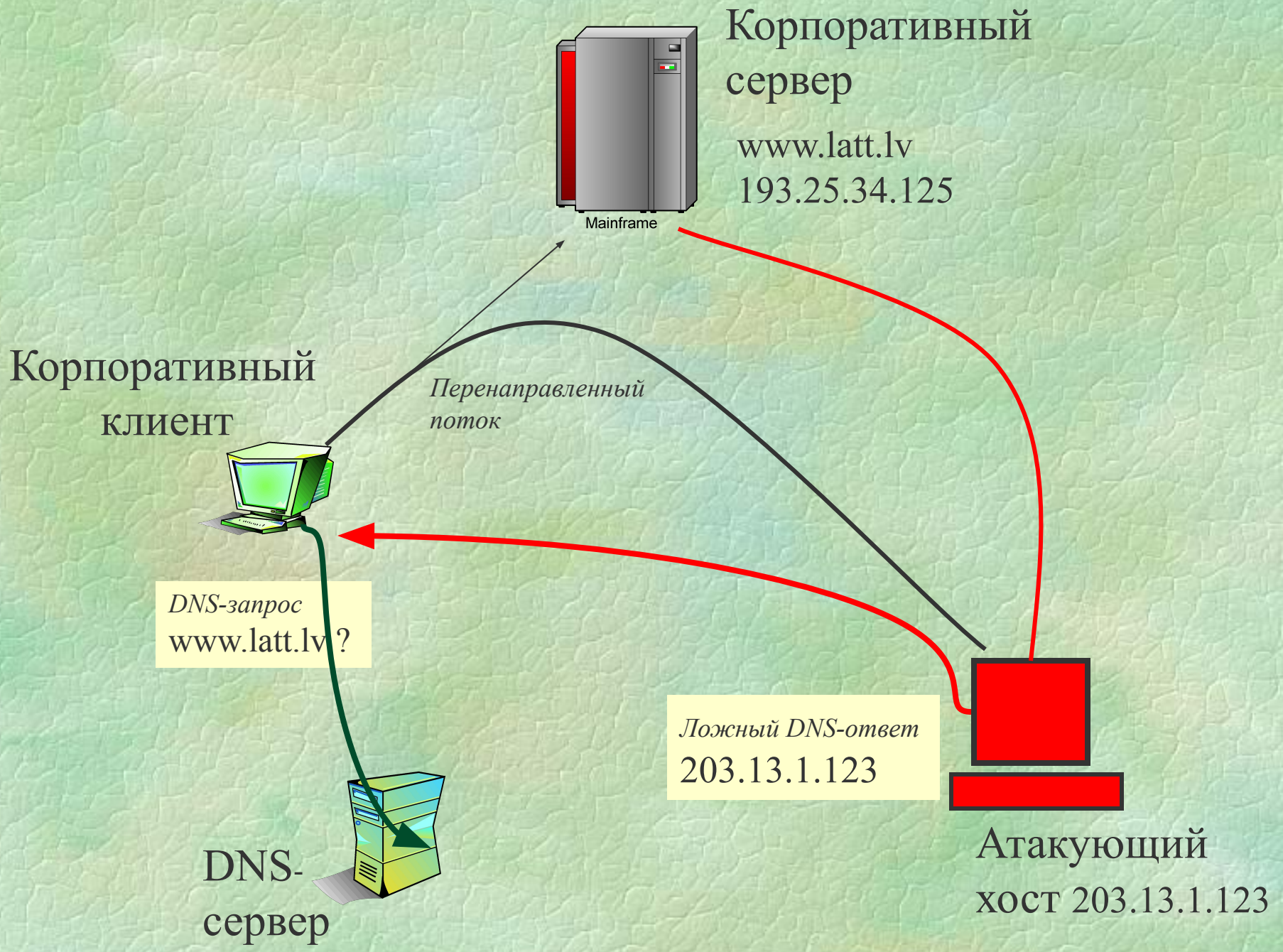


Type	Code	ChSum
Адрес хоста HA		
Заголовок пакета, отброшенного на маршрутизаторе R1		

Потенциальные источники опасности ТСП/IP

Система доменных имен DNS

- ♦ база данных не имеет хороших средств защиты
- ♦ чтение, подмена, разрушение информации
- ♦ изменение содержимого различных кэшей DNS



Сервисы FTP и Telnet

- ♦ передача пароля в открытом виде
- ♦ хакер может сконфигурировать Telnet-сервер так, чтобы он записывал имена и пароли других пользователей

В коммуникационных протоколах стека TCP/IP

- ♦ Подмена содержимого тех или иных полей заголовков пакетов –IP- spoofing
- ♦ Срочная передача в протоколе TCP (URG, urgent pointer)
- ♦ SYN-flooding
- ♦ В протоколе IP атаки типа denial-of-service (отказ в обслуживании) по схеме Ping o"Death



ACK, SYN



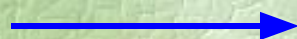
Time out

ACK, SYN



Time out

ACK, SYN



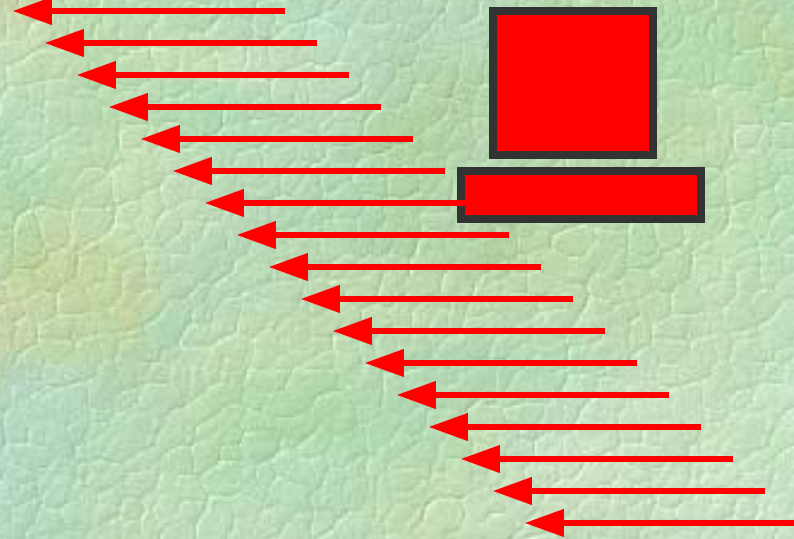
Time out

ACK, SYN



Time out

SYN



Установление TCP-сессии

← SYN

→ ACK, SYN

← ACK

Выработка политики безопасности для сетей TCP/IP

- ◆ какую информацию и от кого следует защищать
- ◆ кому и какая информация требуется для выполнения служебных обязанностей
- ◆ какая степень защиты требуется для каждого вида информации
- ◆ чем грозит потеря того или иного вида информации
- ◆ как организовать работу по защите информации