# Учебный курс

# Информационная безопасность в инфокоммуникационных системах

**Раздел 2. Основы сетевой безопасности. Стратегии безопасности сервера. Реализация защищенных компьютерных сетей.**

# Сетевые уязвимости

## Раскрытие информации о сети:

- Сканирование портов TCP и UDP
- Сканирование ICMP пакетов на периметре сети
- Захват и анализ пакетов

## Недостаточный контроль над инфраструктурой:

- Неучтенные точки беспроводного доступа, модемы
- Неучтенные вэб-серверы
- Забытые Интернет соединения
- Неуправляемые VPN-клиенты
- Неконтролируемое использование приложений
- Одноранговые сети

# Сетевые уязвимости

продолжение

## Доступность компьютеров для атак:

- Атаки типа «отказ в обслуживании»
- Раскрытие информации об учетных записях
- Вирусы, трояны, шпионы, реклама
- Неуполномоченный доступ к данным
- Уничтожение или порча данных

# Международные соединения

Глобальные каналы связи могут пересекать государственные границы

При этом надо учитывать:

- Возможность взаимодействия сетей
- Стоимость
- Отказоустойчивость
- Возможность применения VPN
- Государственные регламенты

# Сетевые сервисы

Необходимо обеспечивать защиту базовых сетевых сервисов:

DHCP

DNS

Time

WINS

ICMP (PING)

…

# Уровень компьютера

Аппаратная надежность

Отказоустойчивость:

- дублирование компонентов
- кластеризация

Ремонтопригодность

Запасные части

Аппаратные средства защиты:

- Замок Кенсингтона
- TPM
- Сканер отпечатков пальцев
- Видеокамера
- И прочее

# Уровень сетевой операционной системы

В некоторых случаях – сертификация ОС

Безопасность регистрации

Безопасность файловой системы

Безопасность системы печати

Аудит

Обновления и исправления

# Модель администрирования

Централизованная

Децентрализованная (распределенная)

Комбинированная

С разделением функций

Аутсорсинговая

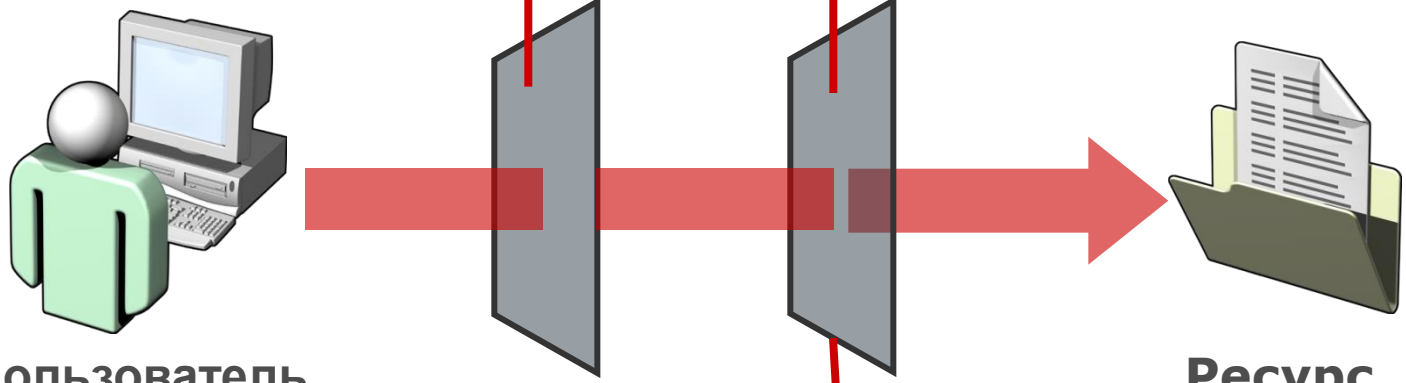
# Что такое аутентификация, авторизация и доступ

**Аутентификация: процесс идентификации и проверки того что вы тот, за кого себя выдаете**

**Кто вы?**

**Авторизация: процесс проверки того, что у вас есть право на доступ к ресурсу**

**Вы есть в списке?**



**Пользователь**

**Ресурс**

Доступ: Что вы можете делать?

# Безопасность регистрации

Службы каталога

Стандарт именования объектов

Политика паролей

Политики доступа

Группы и контейнеры

# Безопасность администрирования

Ограничить число администраторов

Ограничить использование административных учетных записей

Использовать функции повышения полномочий (run as, su)

Сложные пароли

Дополнительные методы регистрации (биометрия, токены)

Шифрование административного трафика (IPSec)

Делегирование полномочий

# Аудит

Аудит отвечает на вопросы:

Что?

Где?

Когда?

И

Кто?

# Аудит

Аудит требует значительных ресурсов

Если никто не проводит аудит и не проверяет файлы журналов, то это расход средств

Регулирующие органы могут обязать хранить данные аудита и журналы много лет

# Безопасность приложений

Выбирайте приложения исходя из своих задач

Устанавливайте обновления и исправления

Интеграция со службами каталогов

Для АСУ ТП особенность в том, что бороться приходится не с утечками, а за целостность и доступность информации.

# Безопасность данных

Разграничение доступа

Резервное копирование

Архивирование

Шифрование

Отказо- и катастрофоустойчивость

# Типы шифрования

**Шифрование преобразует данные в формат, который трудно прочесть непосредственно**

**Типы шифрования:**

- Симметричный
- Асимметричный
- Хэш

**Зашифрованное сообщение называется шифротекст**