

# ЗАЩИТНЫЕ МЕХАНИЗМЫ И СРЕДСТВА

Раздел 1 – Тема 3



# Средства и механизмы защиты

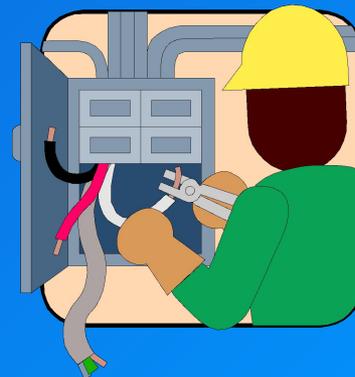
## Средства защиты



## Механизмы защиты

Аутентификация  
Разграничение доступа  
Шифрование  
Аудит  
Контроль целостности

...



# ОСНОВНЫЕ ЗАЩИТНЫЕ МЕХАНИЗМЫ

- идентификация и аутентификация
- разграничение доступа (и авторизация)
- регистрация событий (аудит)
- контроль целостности
- криптографические механизмы
- механизмы защиты периметра сетей
- обнаружение атак
- сканирование (поиск) уязвимостей

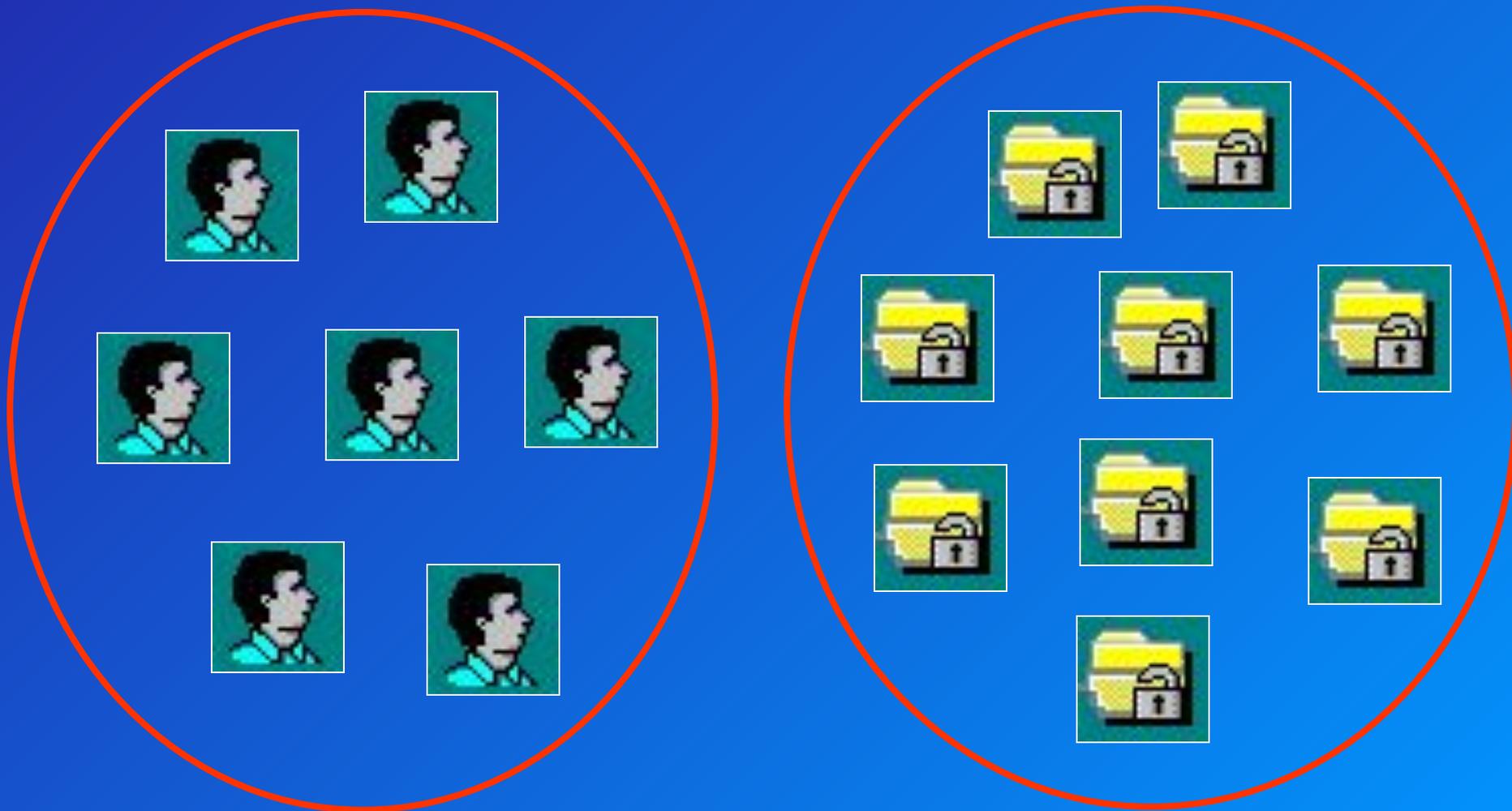
## Идентификация (субъекта или объекта):

- 1) **именование** (присвоение имен-идентификаторов);
- 2) **опознавание** (выделение конкретного из множества).

**Аутентификация (субъекта или объекта) - подтверждение подлинности** (доказательство того, что он именно тот, кем представился).



# Разграничение доступа



Субъекты и объекты

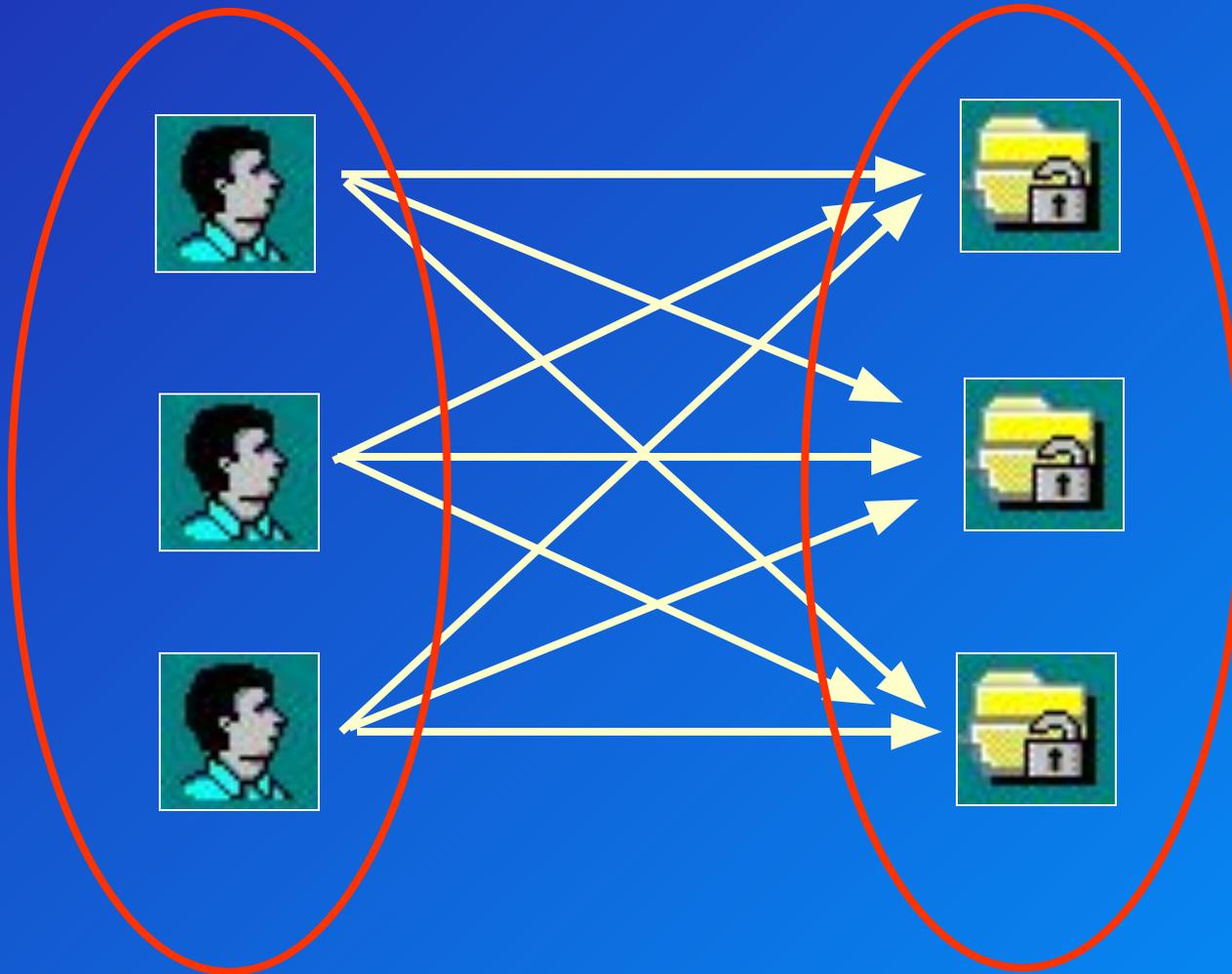
# Субъекты и объекты

**Объект доступа** - пассивная сущность системы  
(файл, каталог, блок памяти)



**Субъект доступа** -  
активная сущность системы  
(процесс, программа)

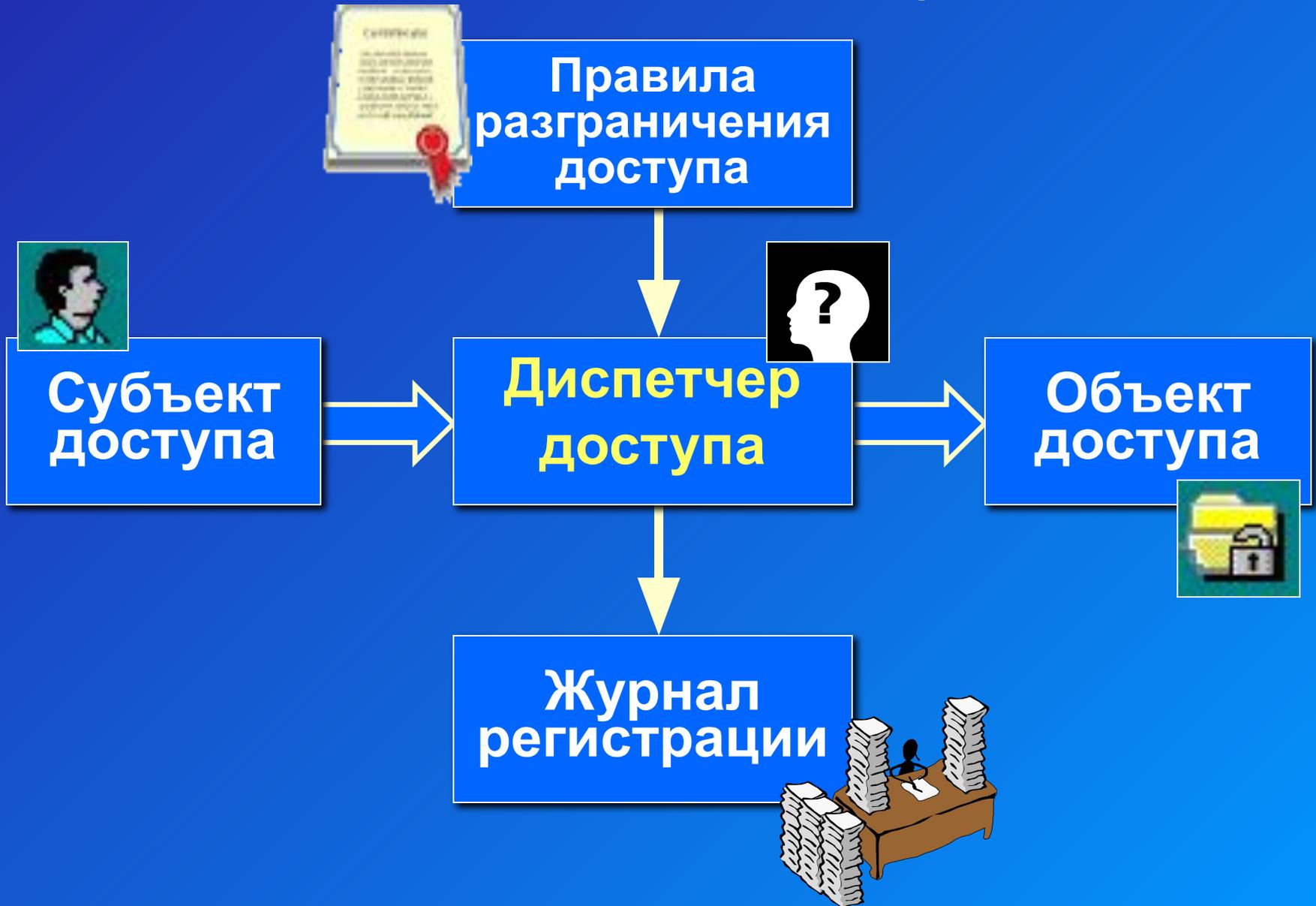
# Разграничение доступа



# Разграничение доступа

**избирательное управление доступом**  
**полномочное управление доступом**

# Разграничение доступа



# Механизм регистрации и аудита событий



# Контроль целостности



## **Механизм контроля целостности**

предназначен для своевременного обнаружения фактов модификации (искажения, подмены) ресурсов системы (данных, программ, секторов дисков и т.п).

Сравнение с эталоном, подсчет и проверка контрольных сумм и сигнатур (ЭЦП) и т.п.



## Криптографические методы защиты позволяют решать следующие задачи:

- **заккрытие данных**, хранимых в АС или передаваемых по каналам связи
- **контроль целостности и аутентичности** данных, хранимых в АС или передаваемых по каналам связи
- **усиленная аутентификация** абонентов



# Заккрытие передаваемых (хранимых) данных



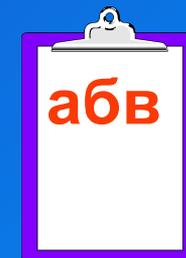
# Заккрытие передаваемых (хранимых) данных



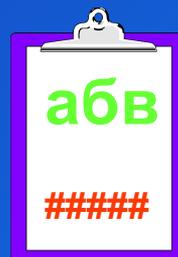
# Подтверждение подлинности (авторства и целостности) документов

Документ

Документ



Документ с ЭЦП

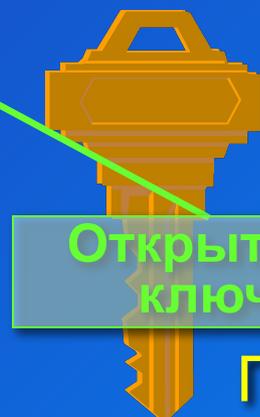


Передача  
(хранение)



Получатель

Отправитель

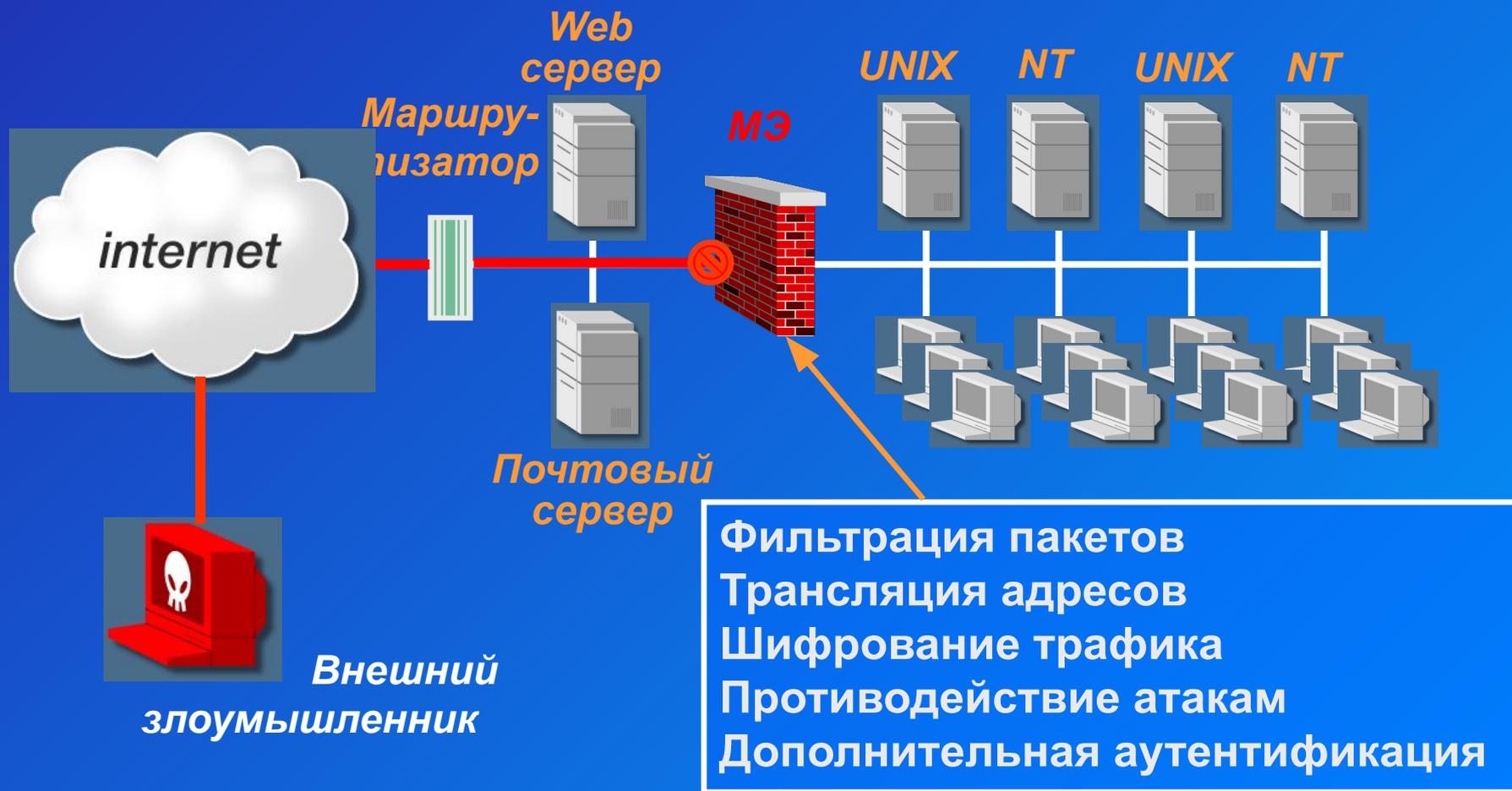


Открытый  
ключ

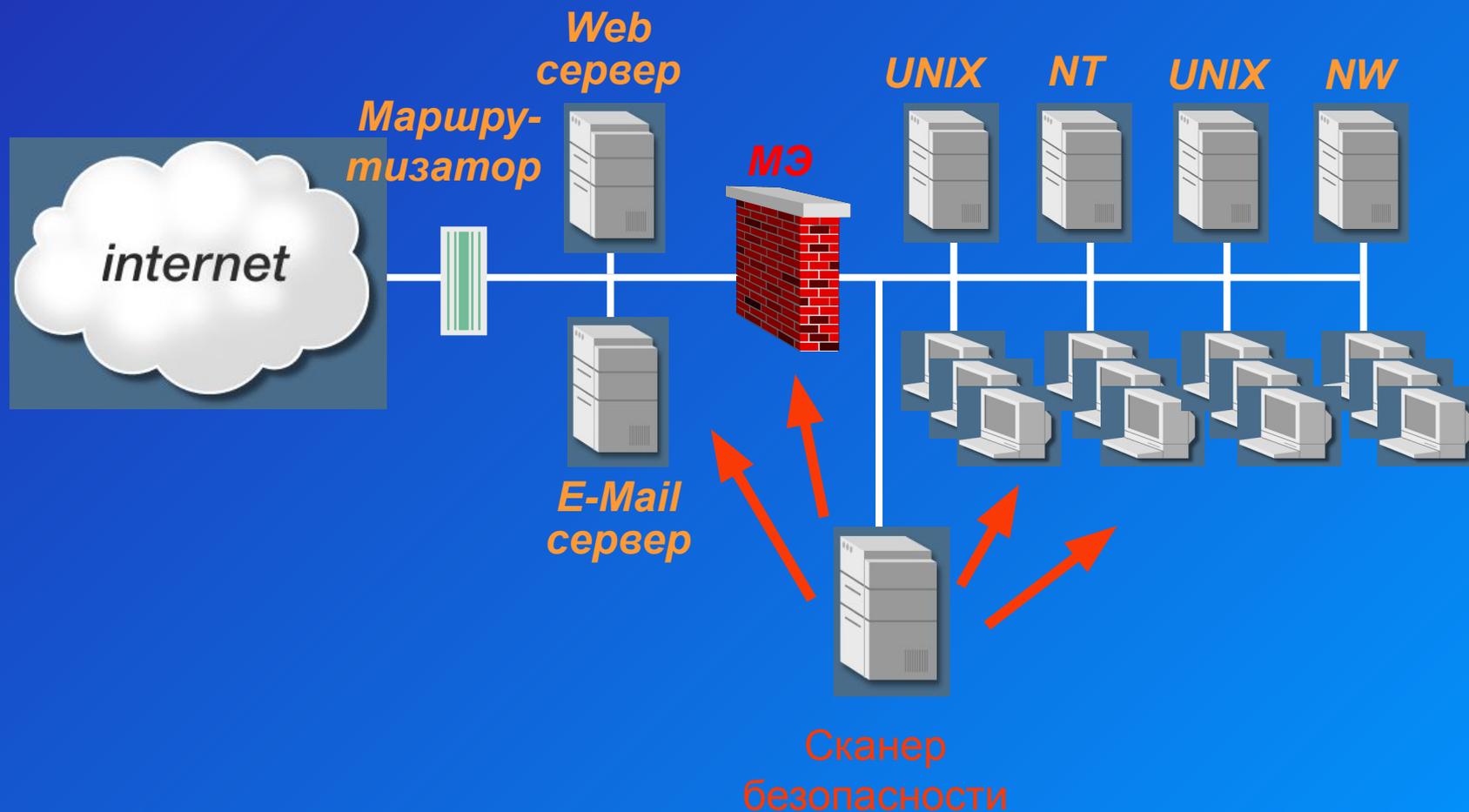
Секретный  
ключ

Применение ЭЦП

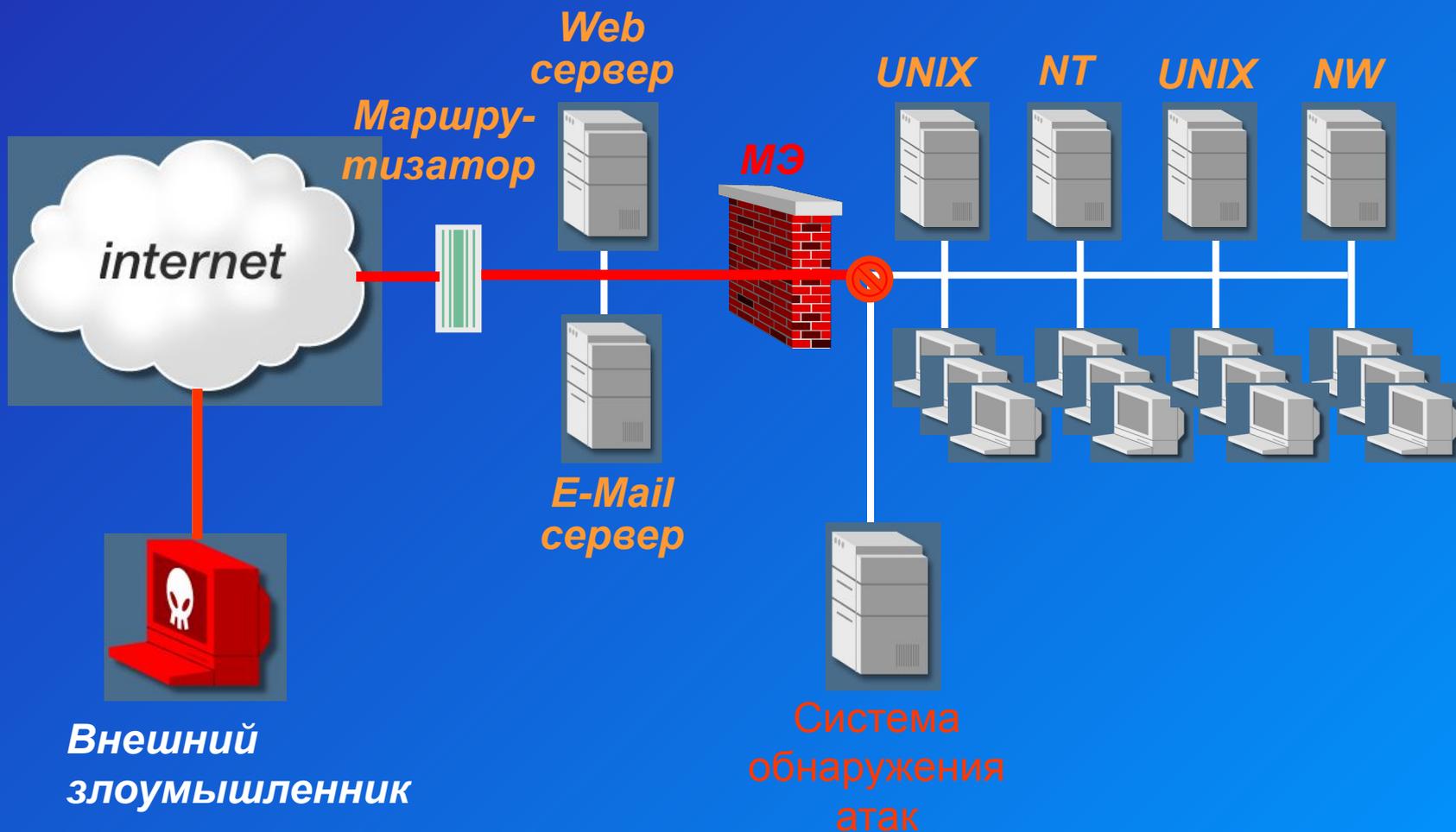
# Защита периметра сетей



# Поиск и устранение уязвимостей



# Обнаружение атак



# Средства обеспечения безопасности сетей

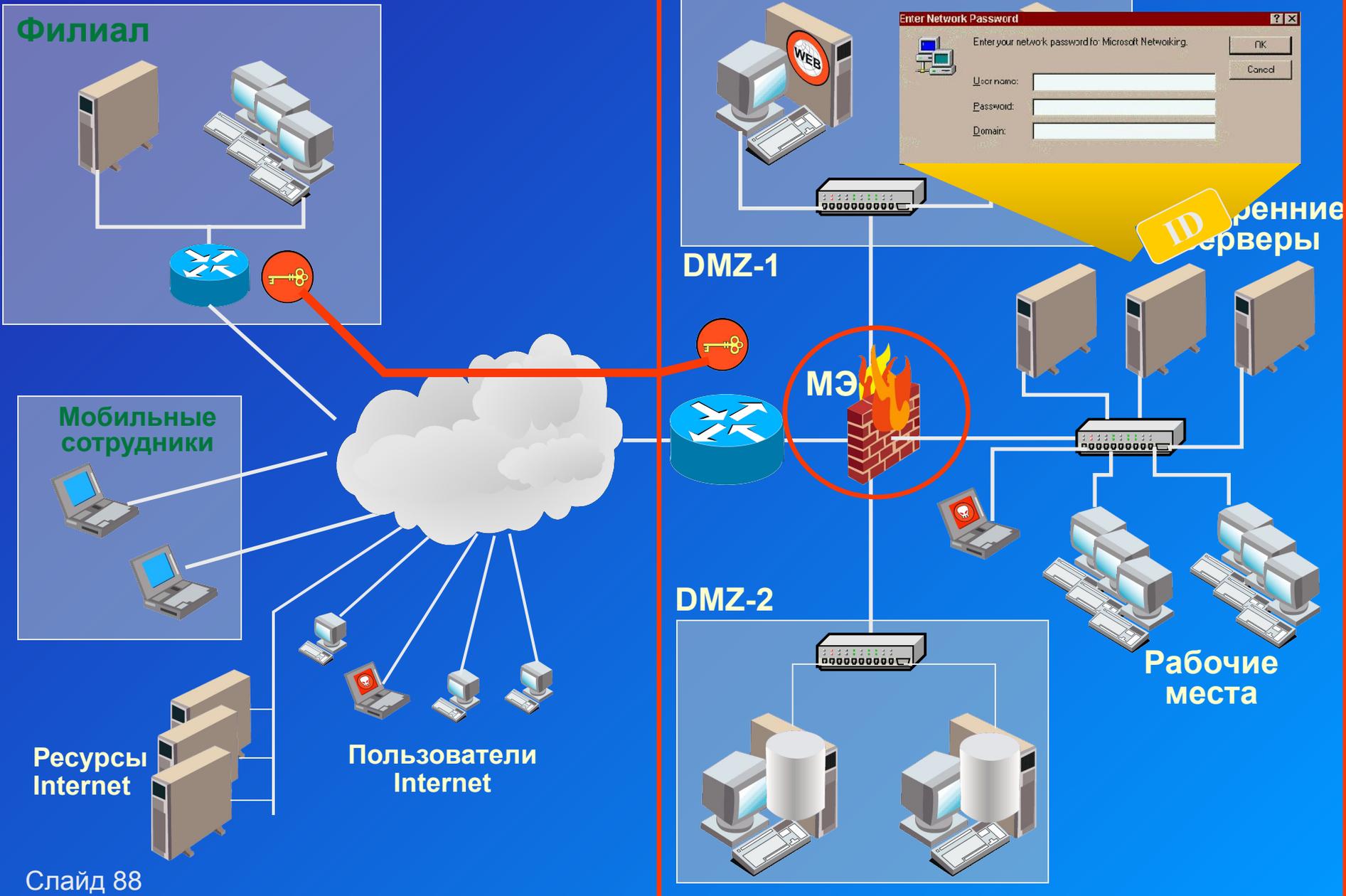
*Для защиты сети необходимо использовать комплекс средств защиты, включающий в себя:*

- Средства защиты узлов и ЛВС, обеспечивающие аутентификацию, разграничение доступа, шифрование и т.д.*
- Средства анализа защищённости и устранения уязвимостей*
- Средства обнаружения атак*

# Механизмы защиты сетей

- идентификация и аутентификация
- разграничение доступа (и авторизация)
- регистрация событий (аудит)
- контроль целостности
- криптографические механизмы
- механизмы защиты периметра сетей
- обнаружение атак
- анализ защищённости

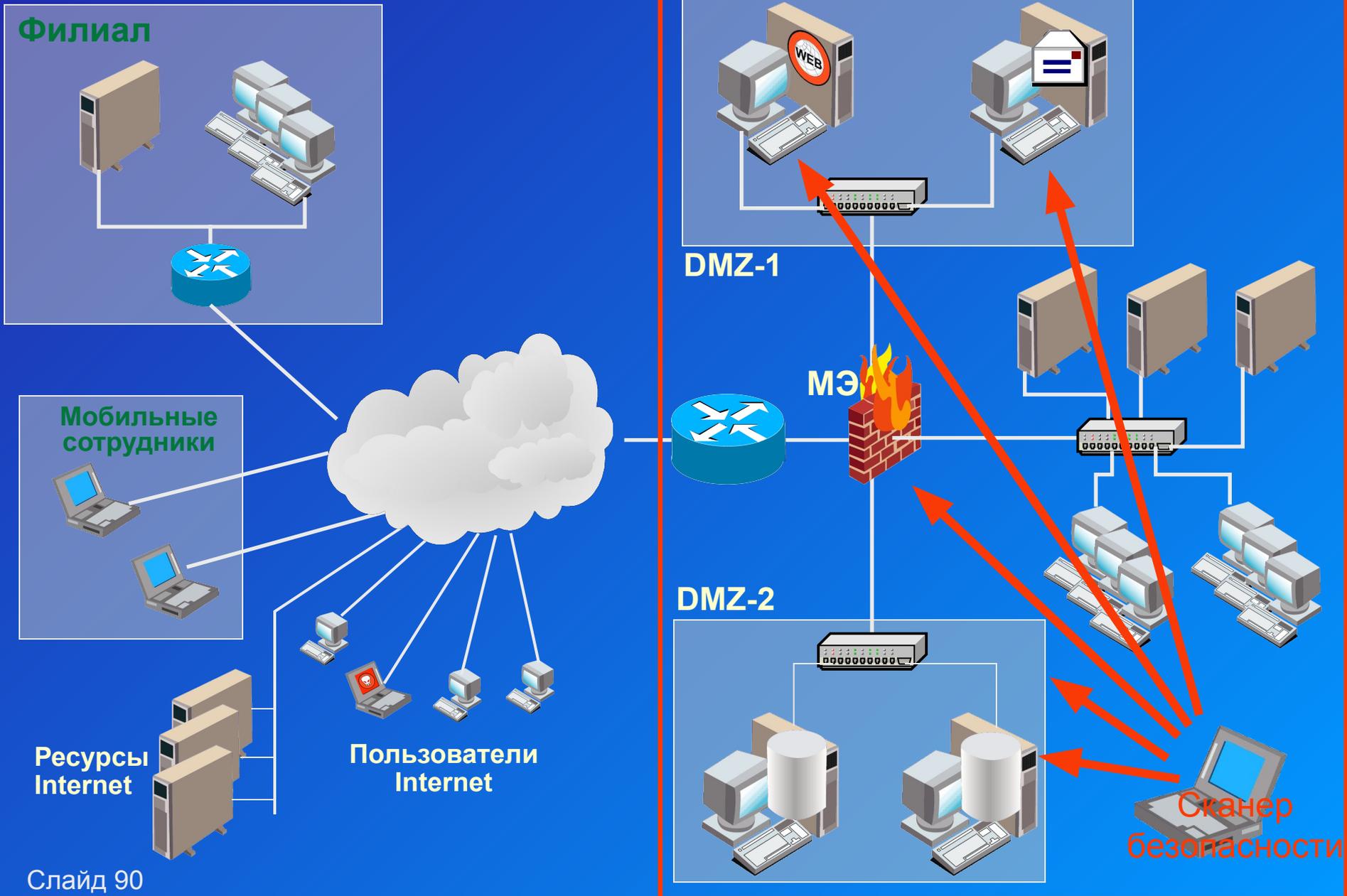
# Средства обеспечения безопасности



# Механизмы защиты сетей

- идентификация и аутентификация
- разграничение доступа (и авторизация)
- регистрация событий (аудит)
- контроль целостности
- криптографические механизмы
- механизмы защиты периметра сетей
- обнаружение атак
- анализ защищённости

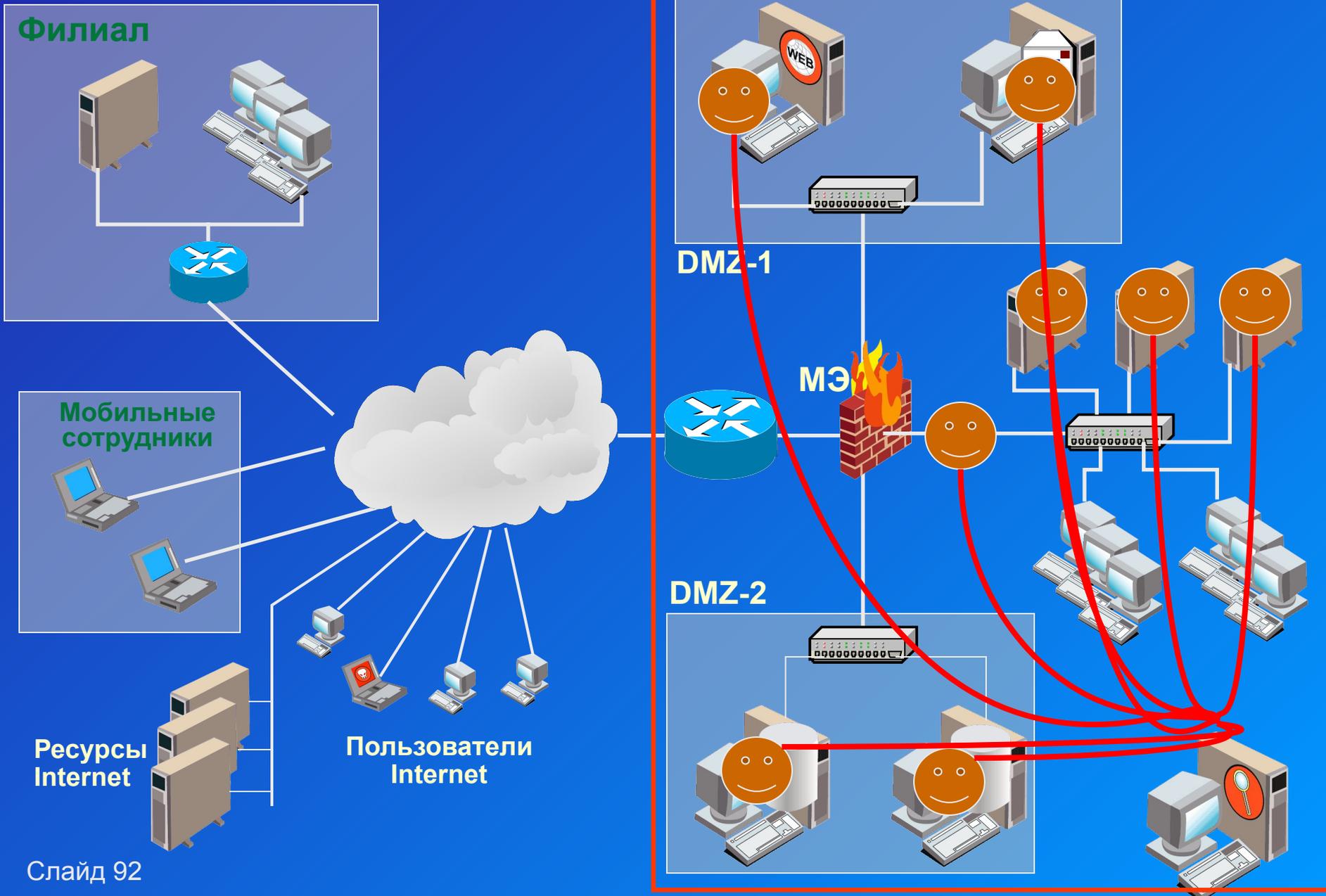
# Средства анализа защищённости



# Механизмы защиты сетей

- идентификация и аутентификация
- разграничение доступа (и авторизация)
- регистрация событий (аудит)
- контроль целостности
- криптографические механизмы
- механизмы защиты периметра сетей
- обнаружение атак
- анализ защищённости

# Средства обнаружения атак



# Раздел 1 - итоги

Основные понятия информационной безопасности

- **Конфиденциальность, Целостность, Доступность**
- **Угроза, Уязвимость, Атака**

Типовая корпоративная сеть

Классификация уязвимостей и атак

- **Уязвимости - по уровням информационной инфраструктуры**
- **Атаки - по механизмам реализации**

Защитные механизмы и средства обеспечения безопасности

