

# Служба каталога Active Directory (AD)

Горячев Александр Вадимович  
Доцент кафедры  
Информационной безопасности  
[avgoriachev@etu.ru](mailto:avgoriachev@etu.ru)

# Модель эшелонированной обороны

Физический  
доступ

Политики, процедуры,  
осведомленность

Хранение

ACL EFS Bitlocker

Backup Mirror RAID SC

Обработка

APPs

Antivirus Updates

OS/.NET

Antispyware **Authentication** HIDS-HIPS

PKI

AD

Передача

Intranet

Routing

IPSec

RMS

NIDS-NIPS

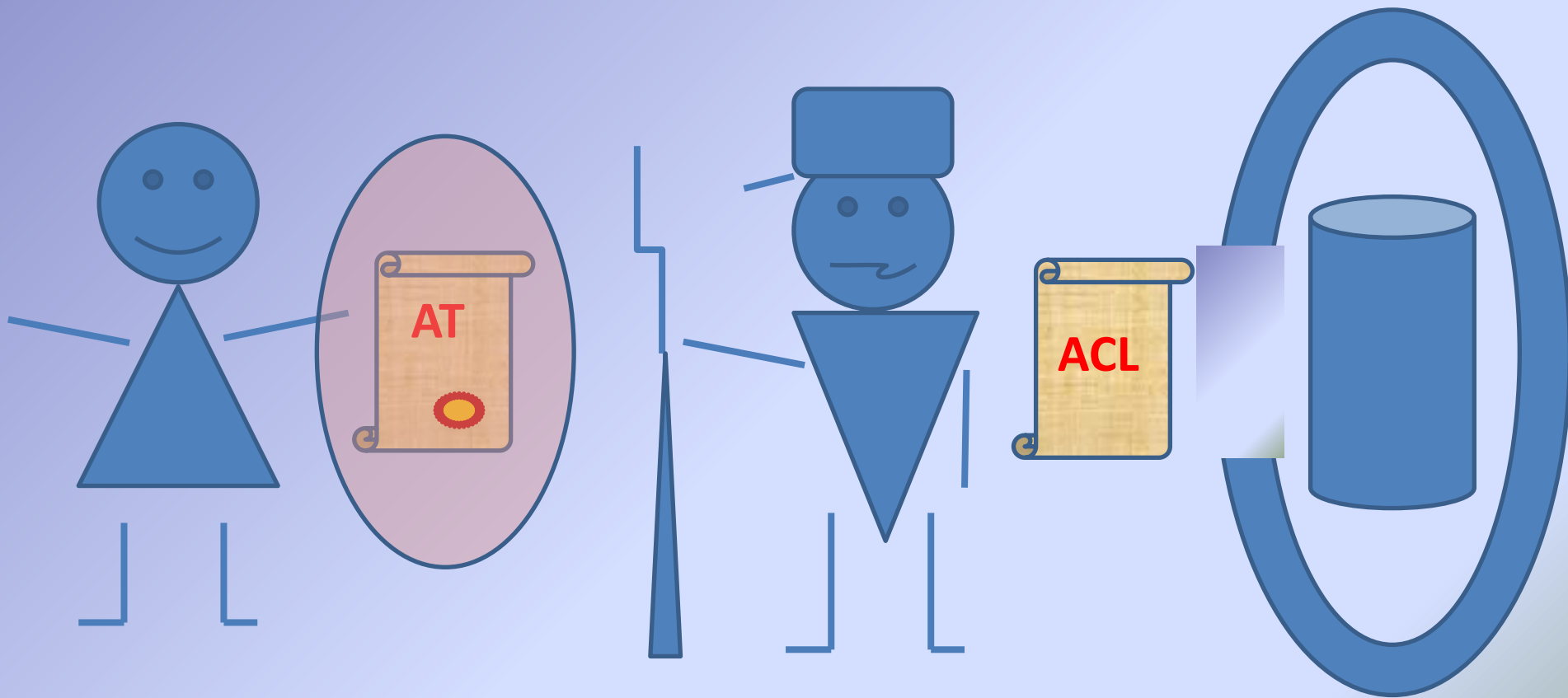
Internet

Firewall

VPN

NAP

# Список контроля доступа



# Получение доступа

- Идентификация
- Аутентификация
- Авторизация



# Три кита аутентификации

- «Что ты знаешь» - пароль
- «Что ты имеешь» - единственный ключ
- «Что ты есть» - биометрия

*Но всю эту информацию надо где-то хранить и как-то проверять...*

# Хранилище учётных данных

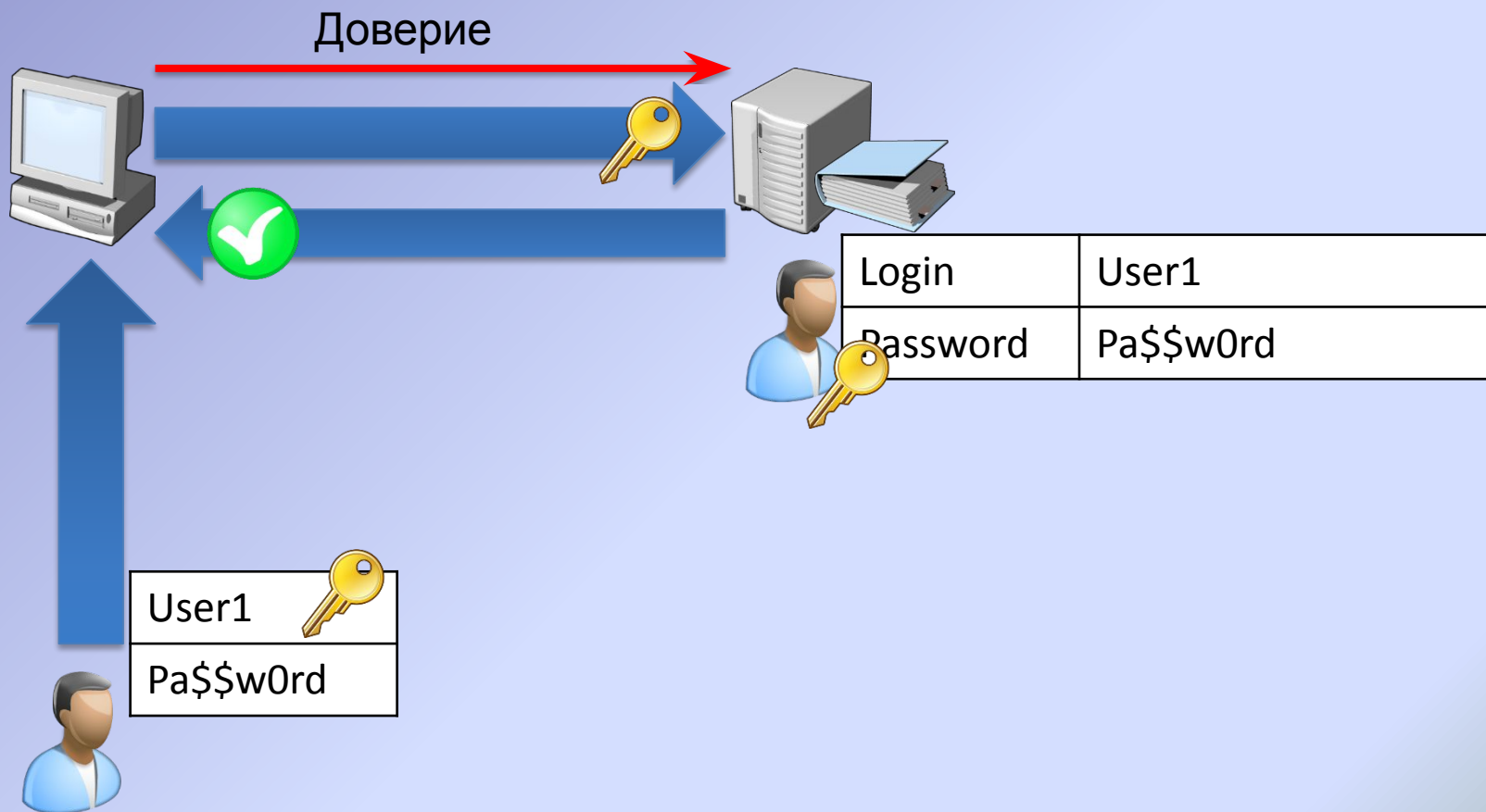
Учётные данные пользователя могут храниться  
на локальном компьютере

**Проблема:** потребуется создать учётные записи на  
каждом компьютере, к которому подключается  
пользователь

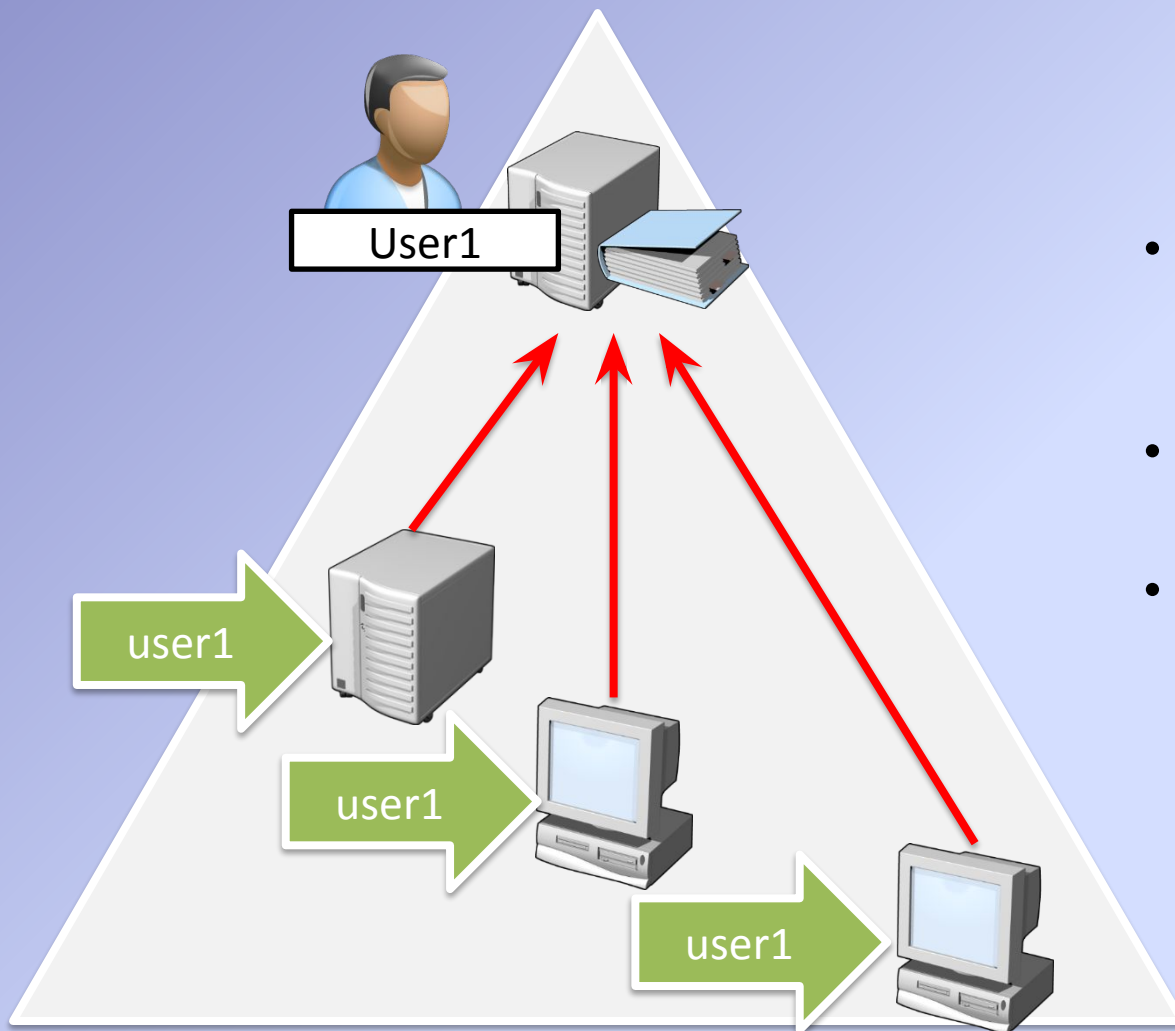
Решение: централизованное хранилище учётных данных

Служба каталогов Active Directory

# Отношение доверия



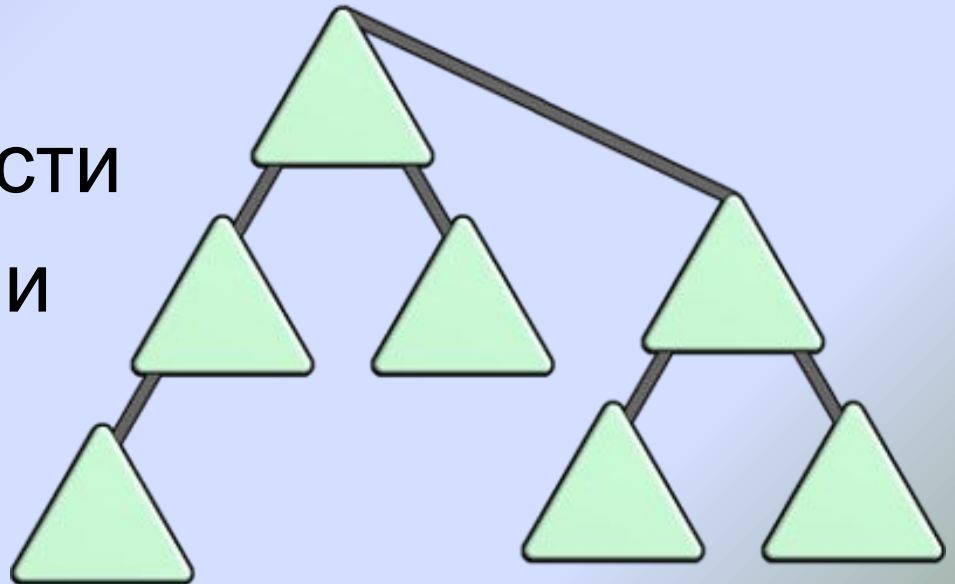
# Домен Windows NT



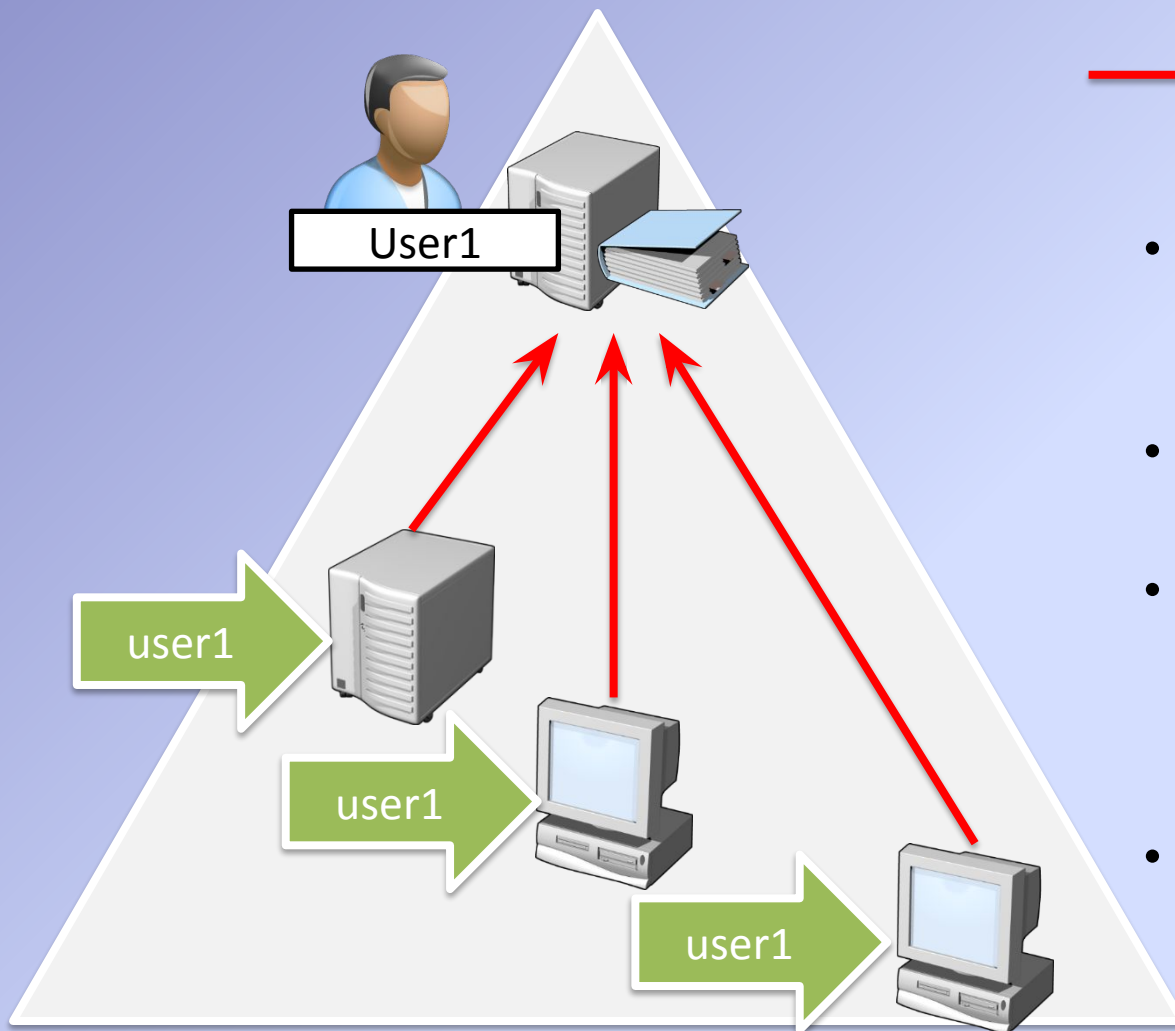
- Требуется наличие как минимум одного контроллера домена (PDC)
- Граница репликации домена
- Доверенный источник учётных данных: любой доменный контроллер (PDC и BDC) может провести аутентификацию в домене

# Лес Active Directory

- Состоит из одного и более доменов Active Directory
- Первый домен в лесу становится корнем
- Единая схема и конфигурация по всему лесу
- Граница безопасности
- Граница репликации



# Домен Active Directory

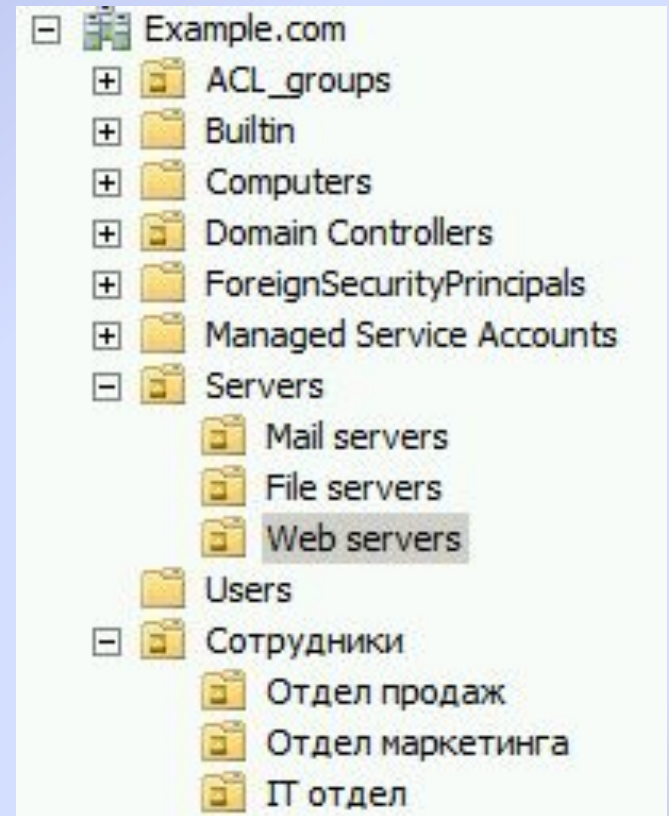


Отношения доверия

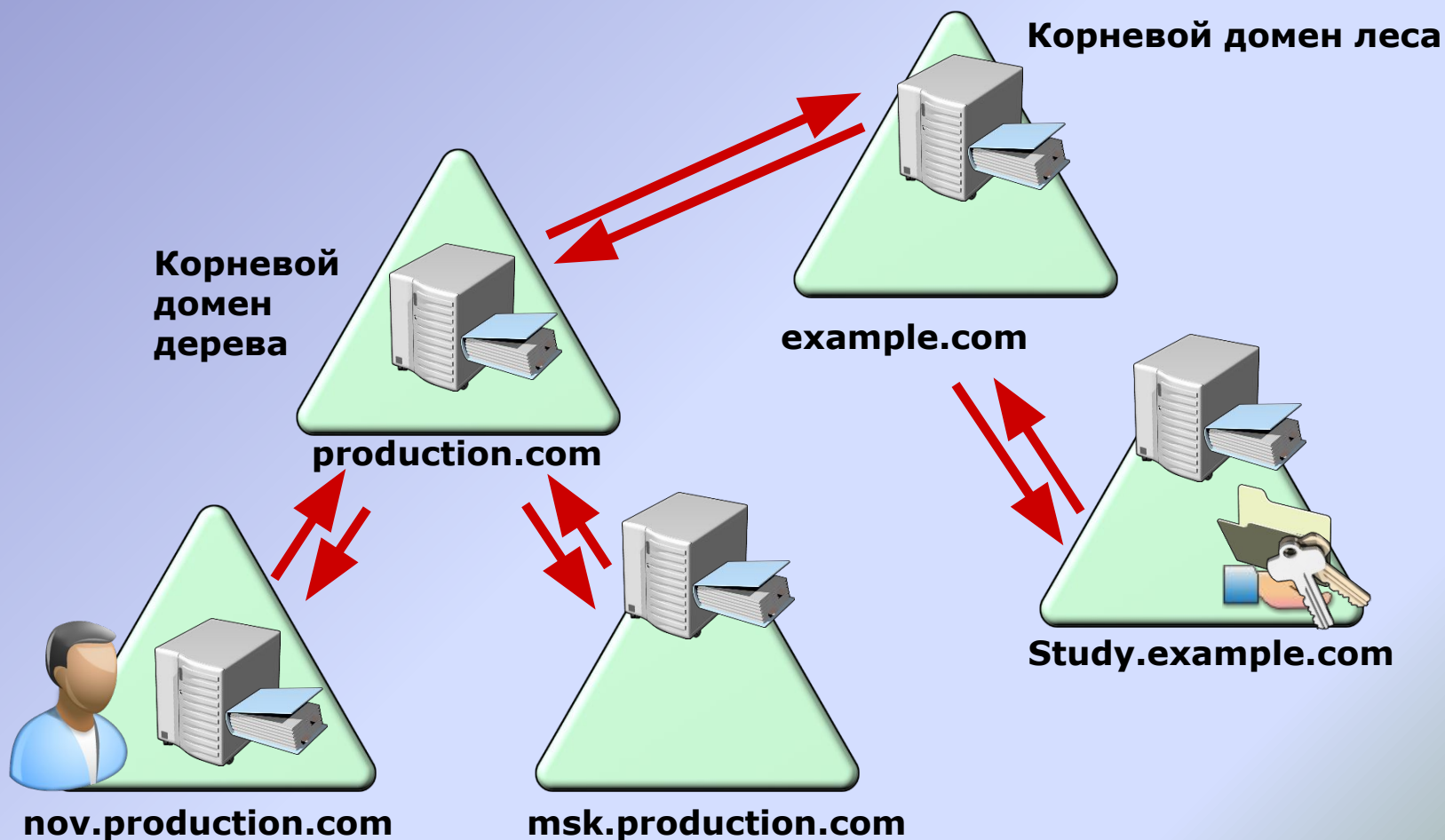
- Требует наличия как минимум одного контроллера домена
- Граница репликации доменного раздела
- Доверенный источник учётных данных: любой DC может провести аутентификацию в домене
- Граница применения политик

# Подразделения

- Объекты
  - Пользователи
  - Компьютеры
- Подразделения
  - Контейнеры для группировки объектов в домене
  - Подразделения создаются:
    - Для делегирования разрешений
    - Для назначения групповых политик

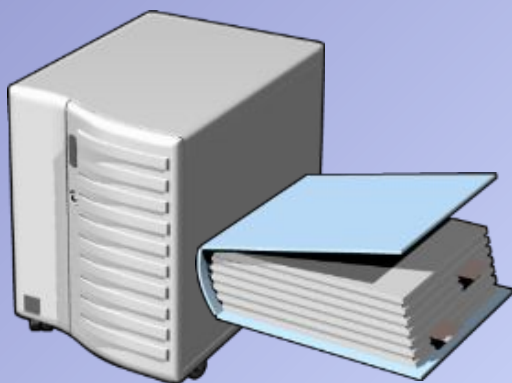


# Доверительные отношения в лесу Active Directory





# Роль контроллера домена при аутентификации



Хранилище учётных данных

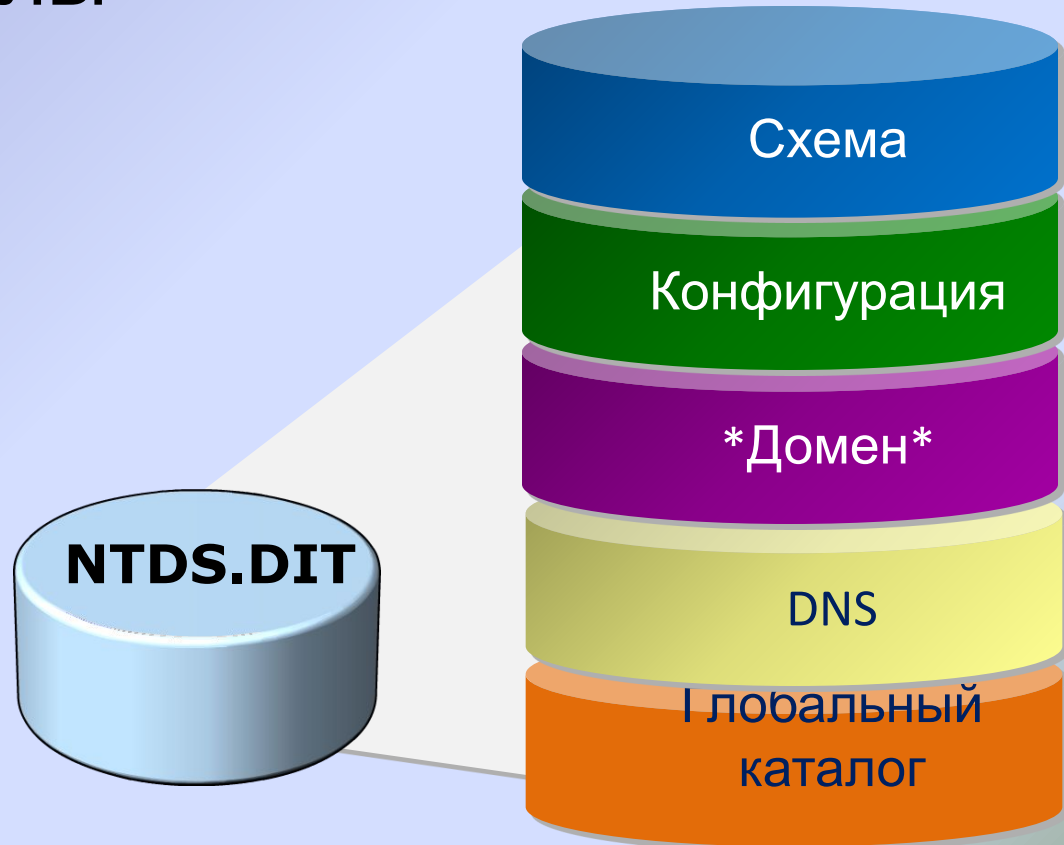
Login	User1	User2
Password	Pa\$\$w0rd	Pa\$\$word2



Проверка учётных данных

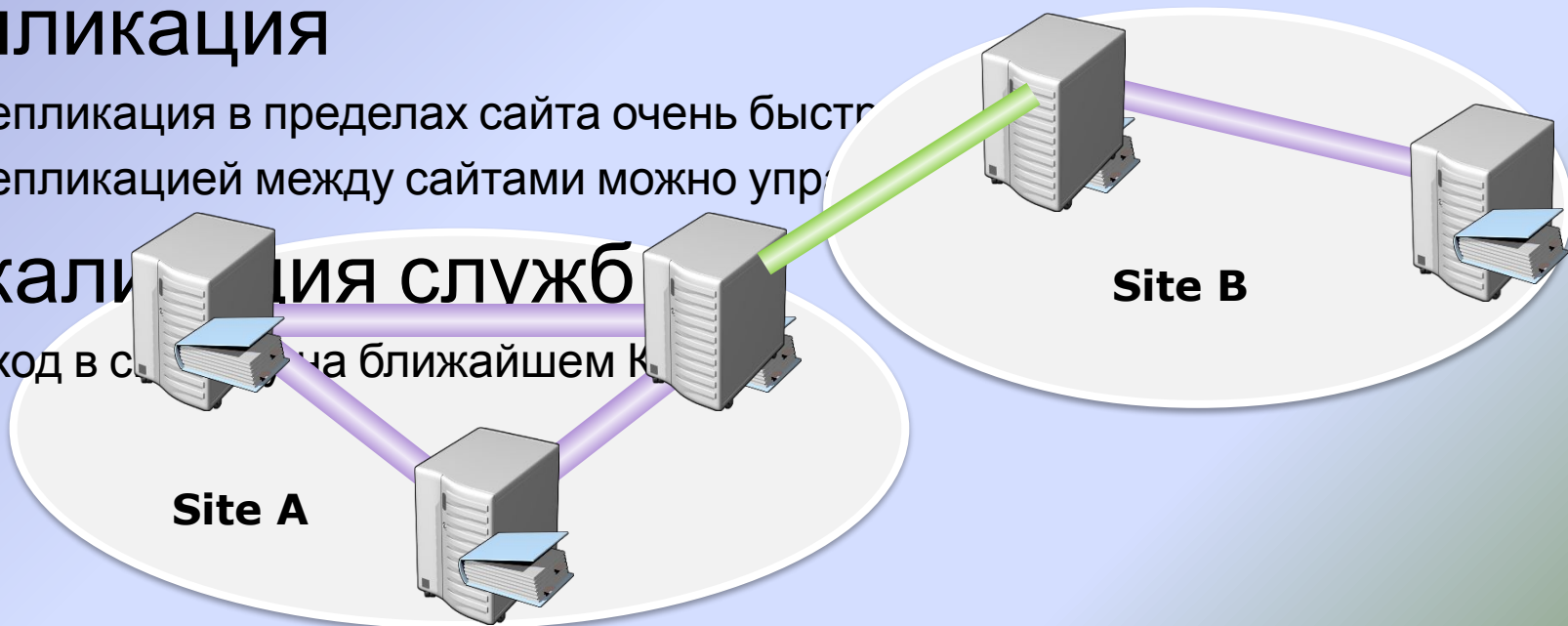
# Хранилище данных Active Directory

- %systemroot%\NTDS\ntds.dit
- Логические разделы
  - Домен
  - Схема
  - Конфигурация
  - Глобальный каталог
  - DNS
- SYSVOL
  - %systemroot%\SYSVOL
  - Скрипты входа в систему
  - Политики



# Сайты

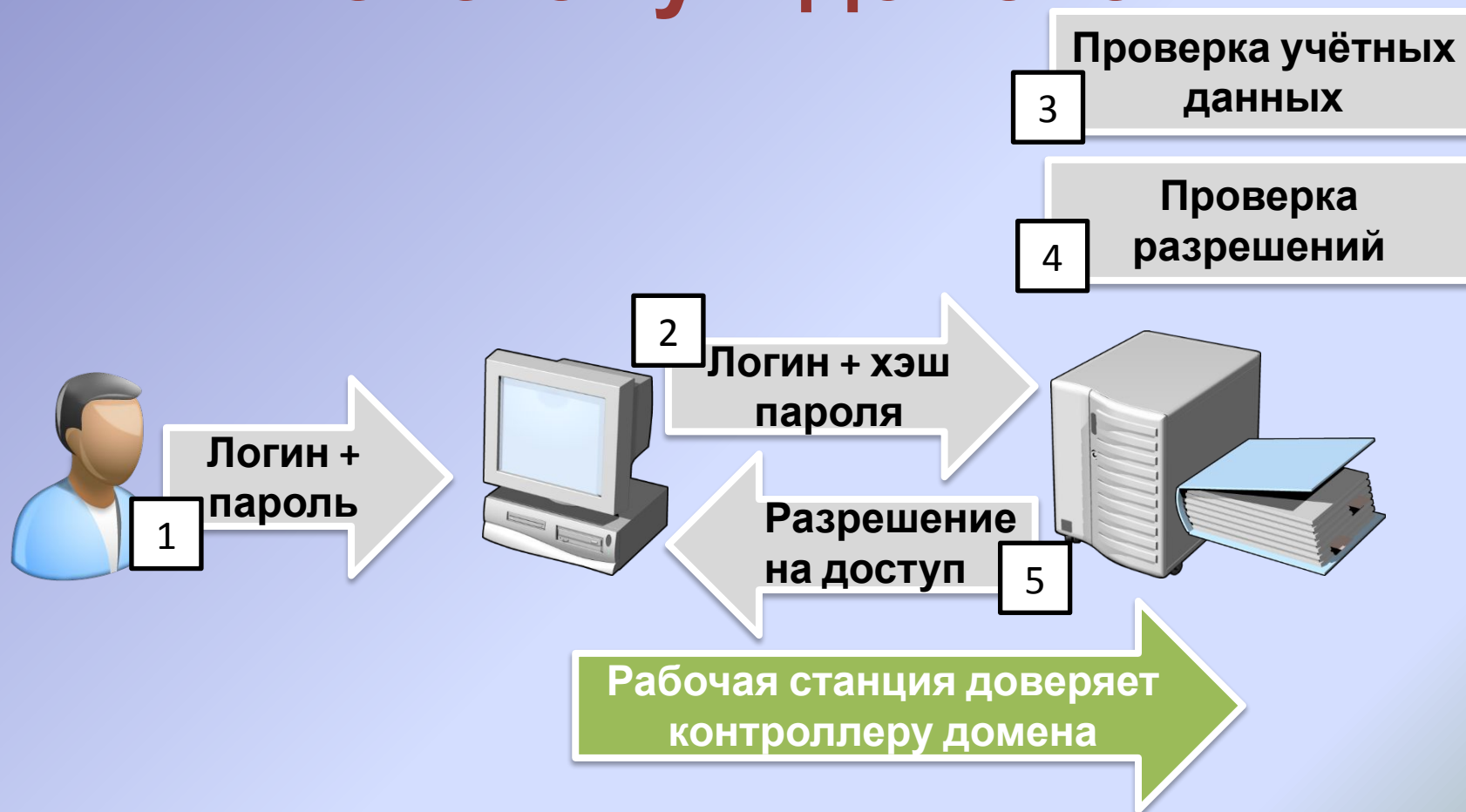
- Объекты Active Directory, представляющие сегменты сети с надёжным соединением
  - Ассоциируются с подсетями.
- Внутрисайтовая и межсайтовая репликация
  - Репликация в пределах сайта очень быстра
  - Репликацией между сайтами можно управлять
- Локализация служб
  - Вход в систему на ближайшем контроллере



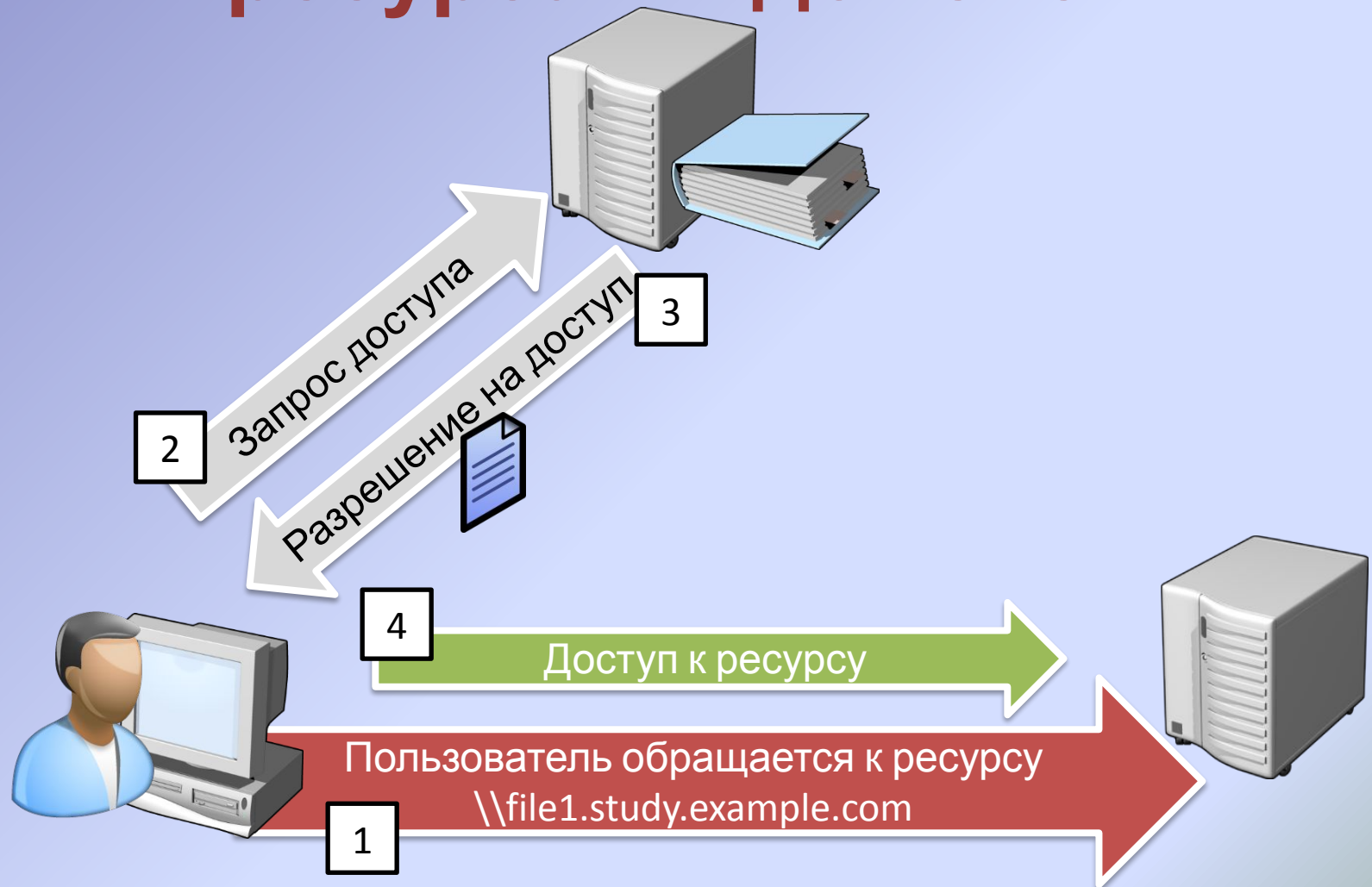
# Учётные записи пользователей

- Учётная запись пользователя:
  - Позволяет проводить аутентификацию пользователя с помощью атрибутов, например logon name и password
  - Является участником безопасности с уникальным идентификатором (SID), который позволяет предоставлять пользователю доступ к ресурсам
- Учётная запись пользователя может храниться:
  - В Active Directory, где позволяет осуществить вход в домен и получить доступ к любому ресурсу в домене
  - В локальной базе данных Security Account Manager, где позволяет осуществить локальный вход и получить доступ только к локальным ресурсам

# Процесс входа пользователя в систему в домене



# Процесс доступа к сетевым ресурсам в домене



# Использование групп для контроля доступа на основе ролей

Пользователь

Группа роли

Группа доступа

Ресурсы

Иван Иванов

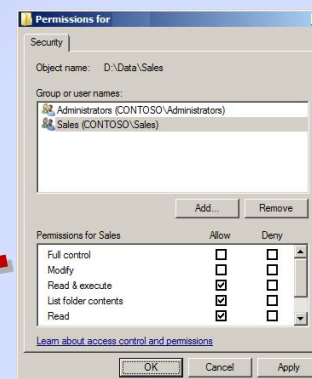
Пётр Петров

Василий Васильев

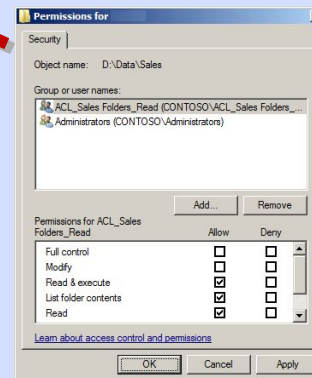
Sales

Auditors

ACL\_Sales\_read



SalesDocs



SalesShare



# Диапазоны применения групп

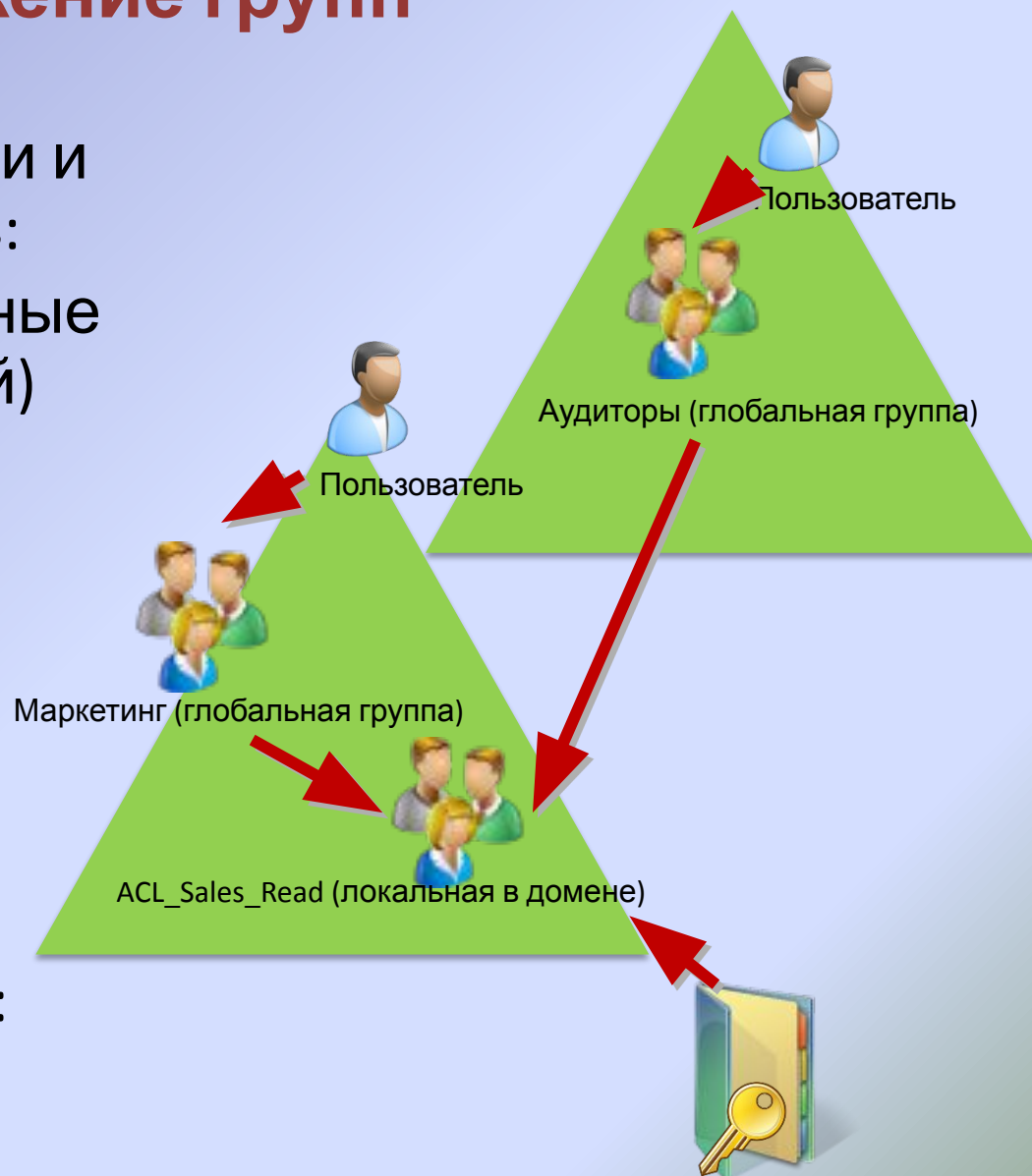
Диапазон	Члены из домена	Члены из другого домена в лесу	Члены из внешнего доверенного домена	Могут предоставлять разрешения
Локальная	U, C, GG, DLG, UG локальные пользователи	U, C, GG, UG	U, C, GG	Только на локальном компьютере
Локальная в домене	U, C, GG, DLG, UG	U, C, GG, UG	U, C, GG	Во всём домене
Универсальная	U, C, GG, UG	U, C, GG, UG	N/A	Во всём лесу
Глобальная	U, C, GG	N/A	N/A	Во всём домене или доверенном домене

U Пользователь      DLG Локальная группа в домене  
 C Компьютер      UG Универсальная группа  
 GG Глобальная группа



# Вложение групп

- Identities (пользователи и компьютеры) входят в:
- Global groups (глобальные группы – группы ролей) входят в:
- Domain Local groups (локальные в домене группы) предоставляют:
- Access (доступ к ресурсам)
- Мультидоменный лес: IGUDLA



# Типы групп

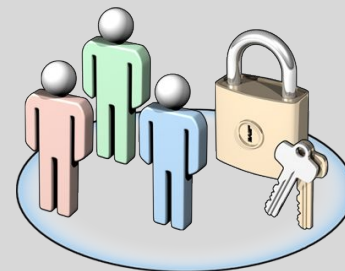
## Группы распространения

- Используются приложениями электронной почты
- Не имеют идентификатора безопасности



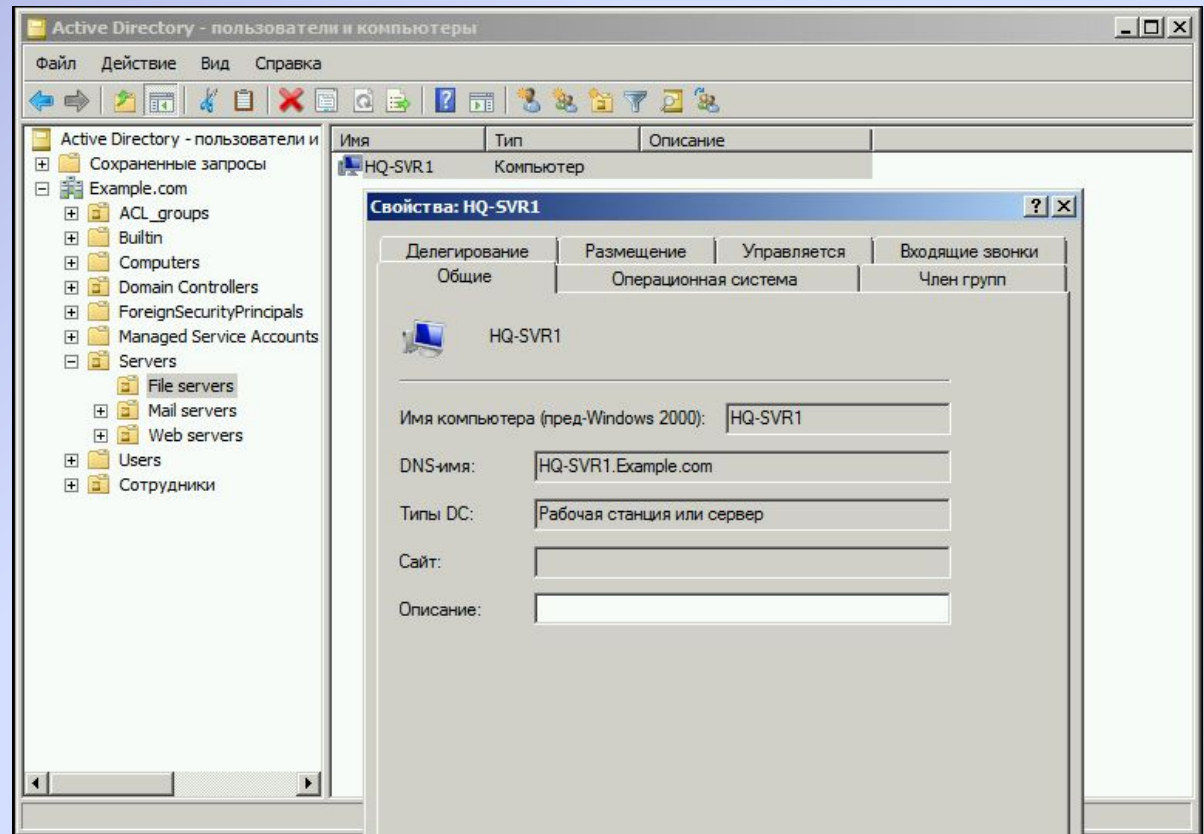
## Группы безопасности

- Имеют идентификатор безопасности, могут быть использованы для контроля доступа
- Также могут использоваться приложениями электронной почты

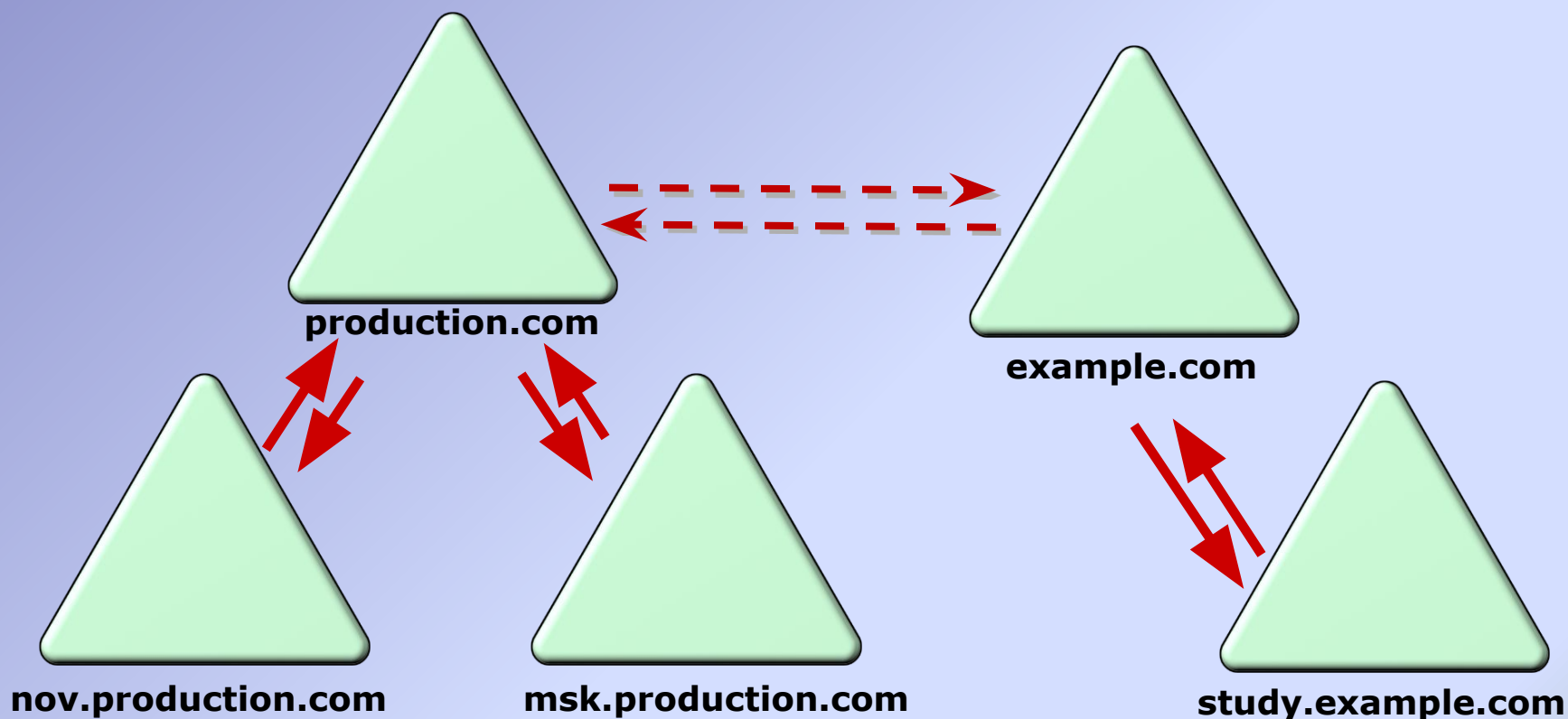


# Учётные записи компьютеров

- Компьютер является участником безопасности как и пользователь
- Учётная запись компьютера необходима для доверительных отношений



# Доверительные отношения между лесами



# **Взаимодействие с Интернет. Firewall (брандмауэр, межсетевой экран)**

# Модель эшелонированной обороны

Политики, процедуры,  
осведомленность

Физический  
доступ

Хранение

ACL EFS Bitlocker

Backup Mirror RAID SC

Обработка

APPs

Antivirus Updates

OS/.NET

Antispyware Autentification HIDS-HIPS

PKI

AD

Передача

Intranet

Routing

IPSec

RMS

NIDS-NIPS

Internet

Firewall

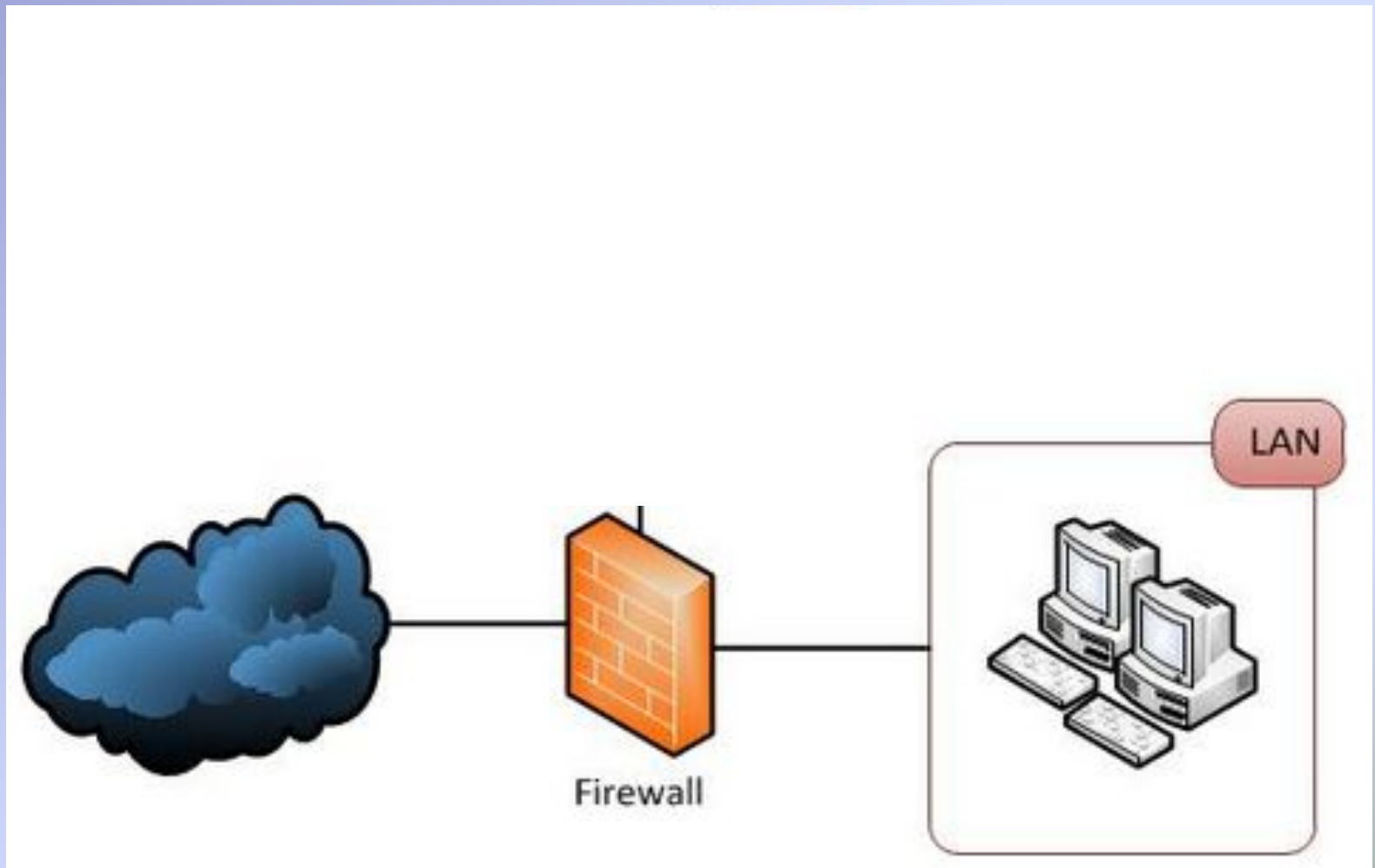
VPN

NAP

# Набор технологий

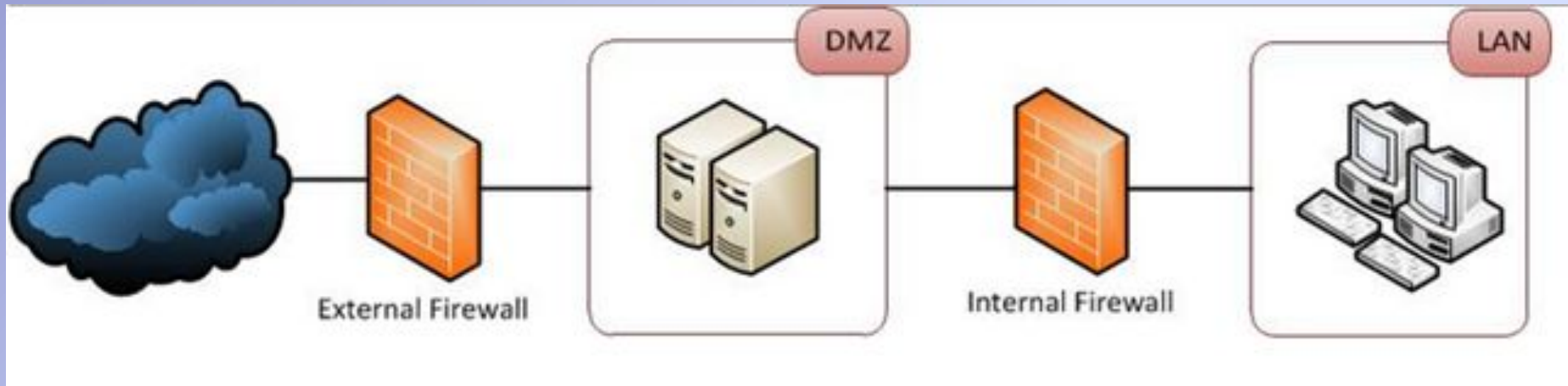
- |                              |   |
|------------------------------|---|
| • Proxy                      | 7 |
| • VPN                        | 6 |
| • Контентная фильтрация      | 5 |
| • Аутентификация             | 4 |
| • Трансляция сетевых адресов | 3 |
| • Пакетные фильтры           | 2 |

# Простые конфигурации





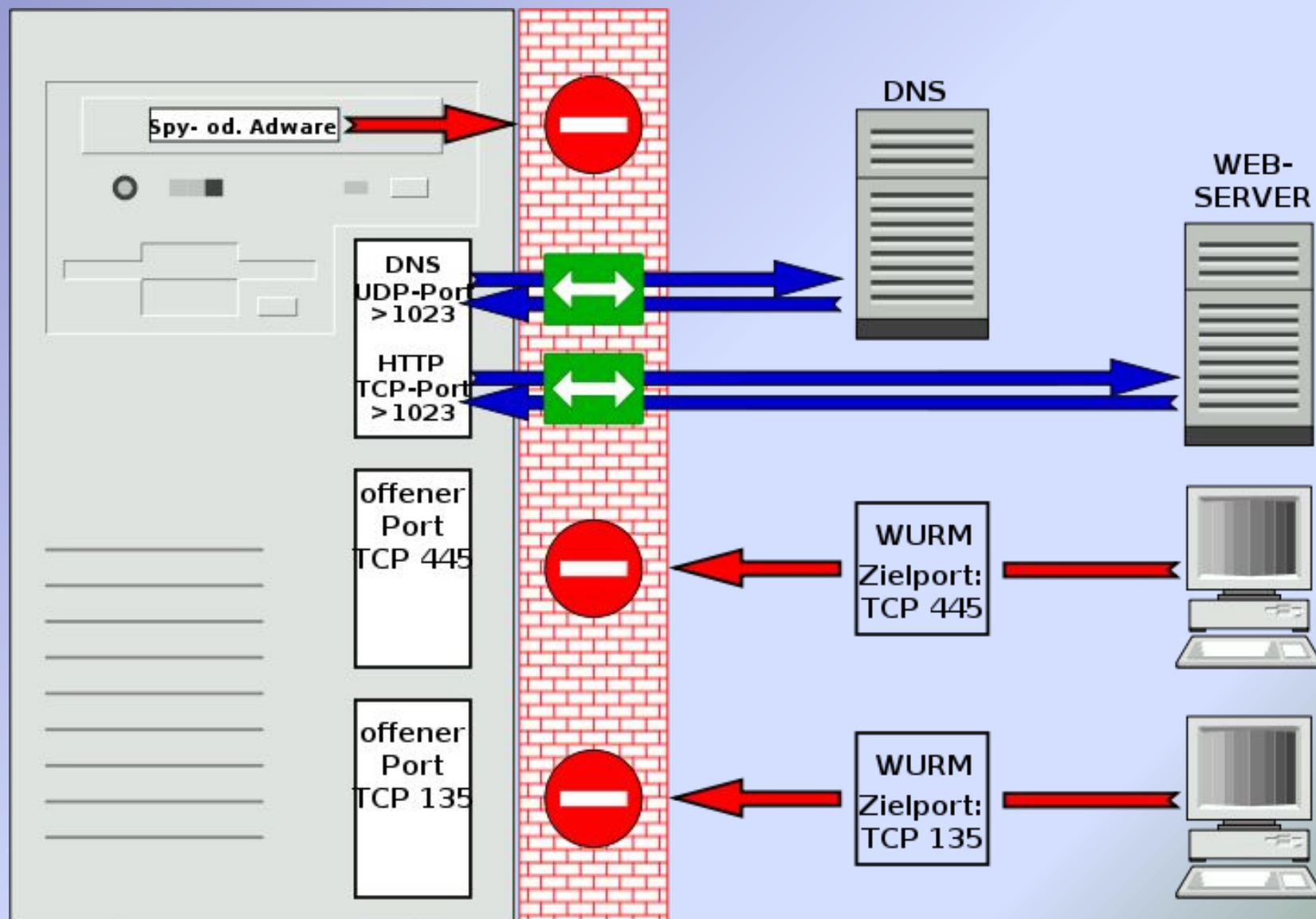
# Демилитаризованная зона (сеть периметра)



# Windows Firewall?

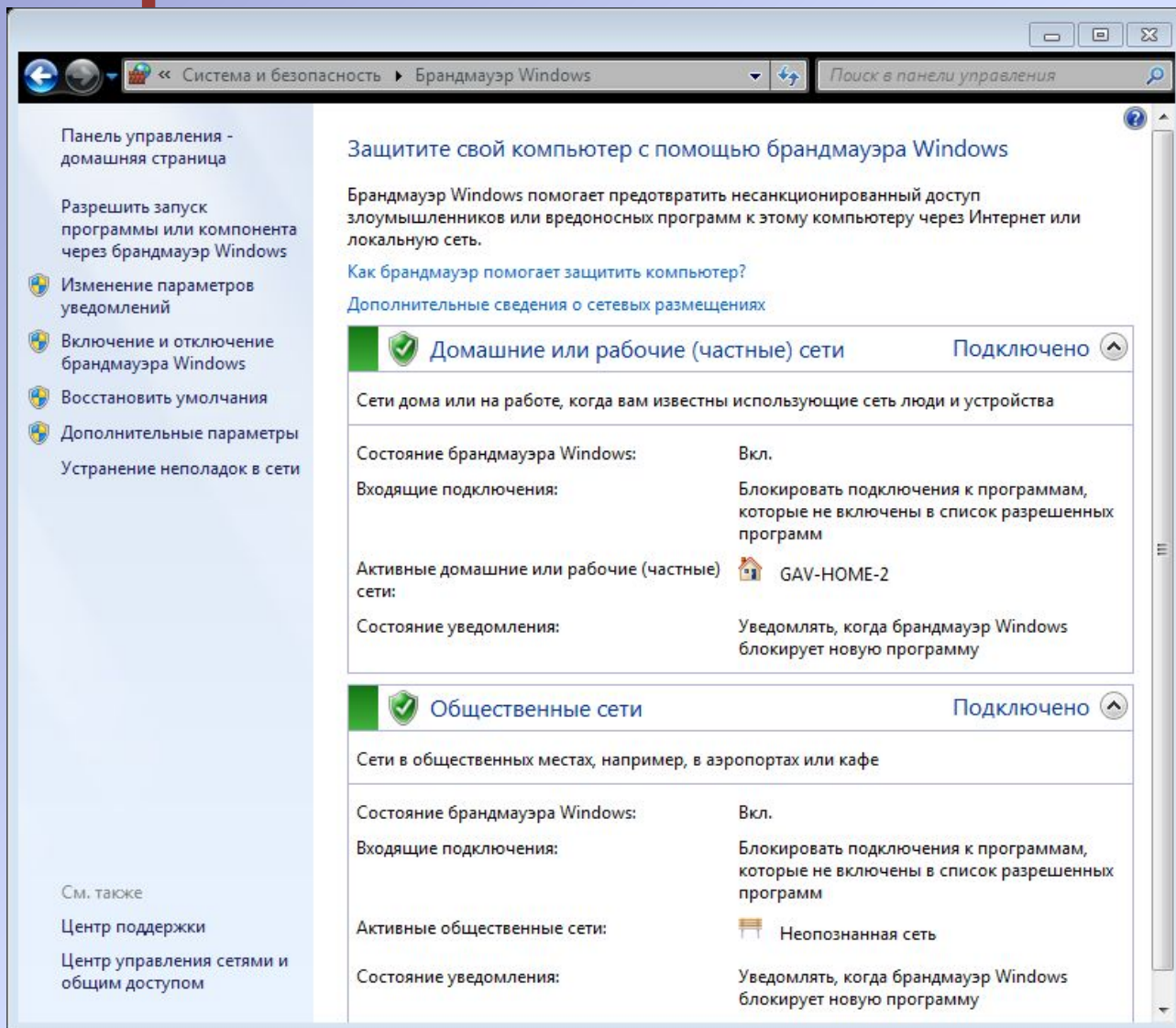


# Персональный брандмауэр

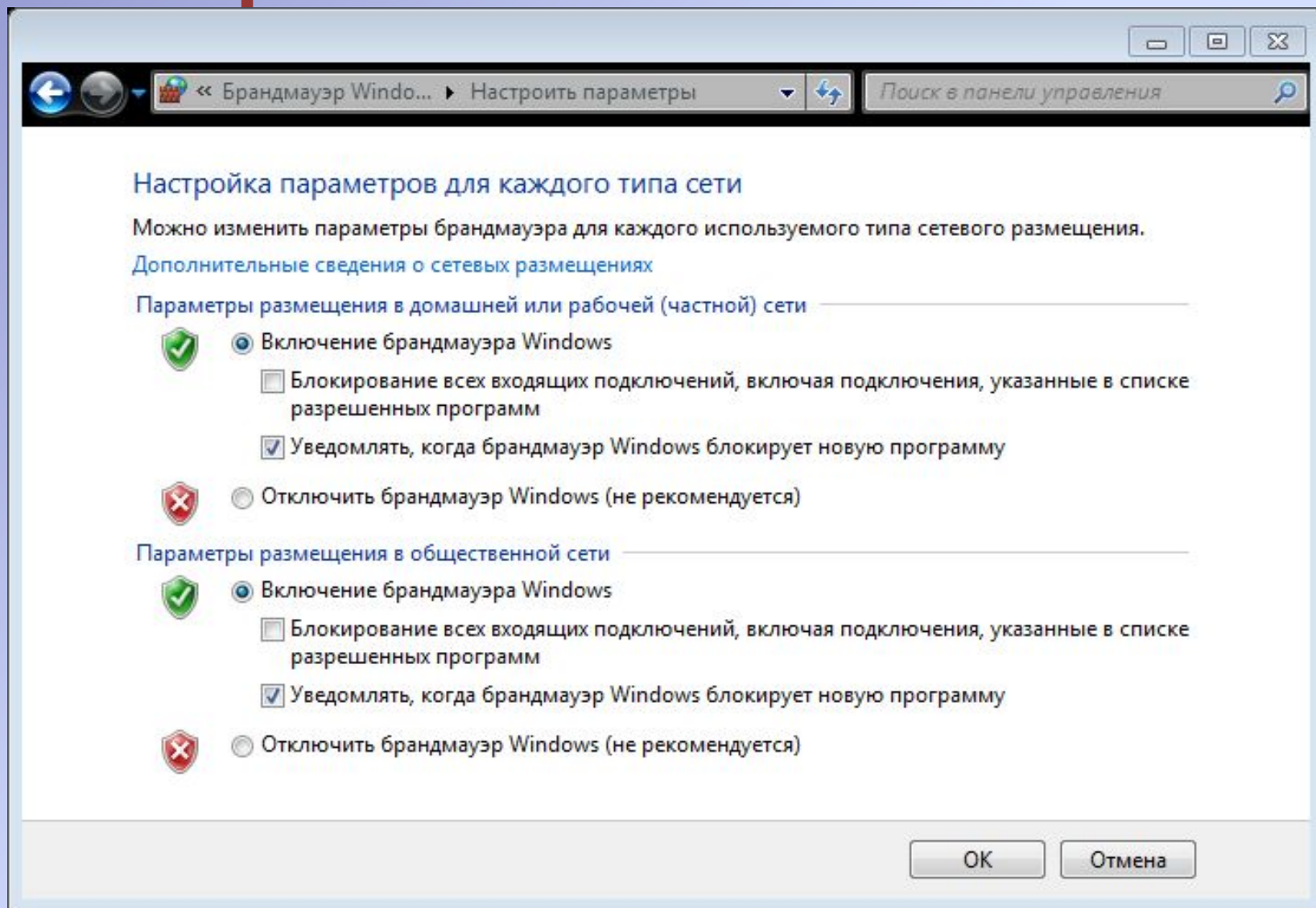




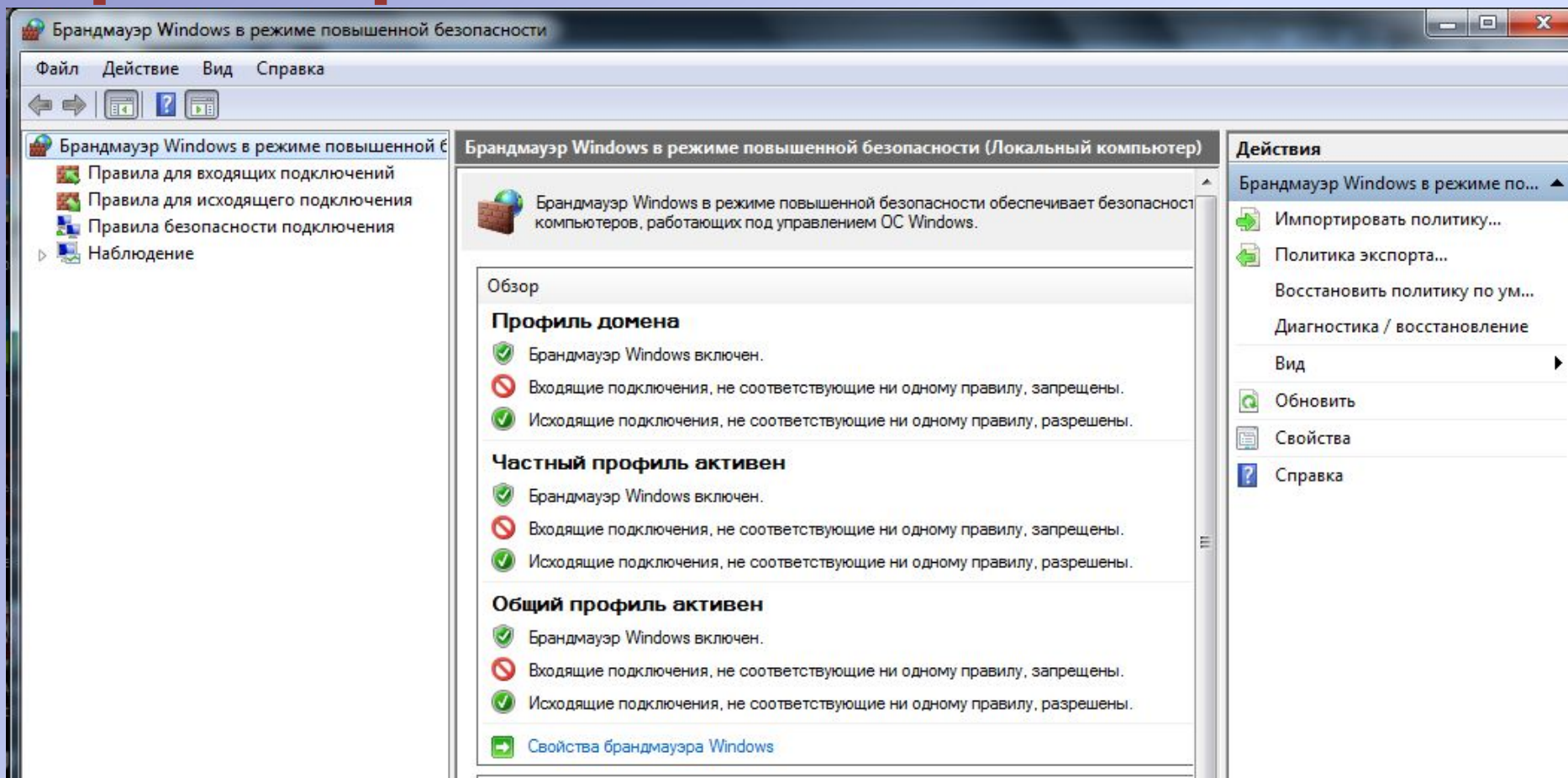
# Windows Firewall с расширенными возможностями



# Windows Firewall с расширенными возможностями

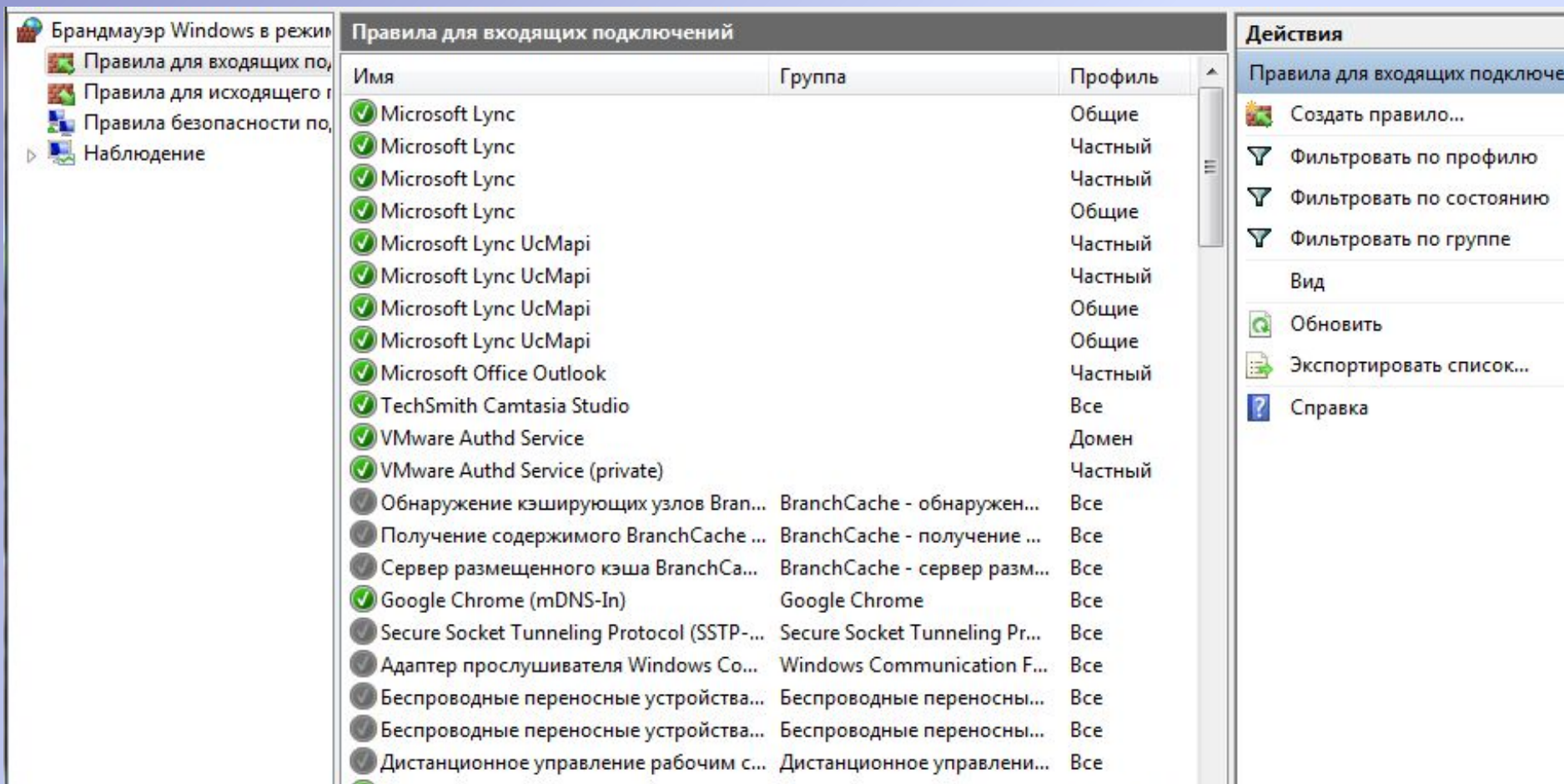


# Windows Firewall с расширенными возможностями

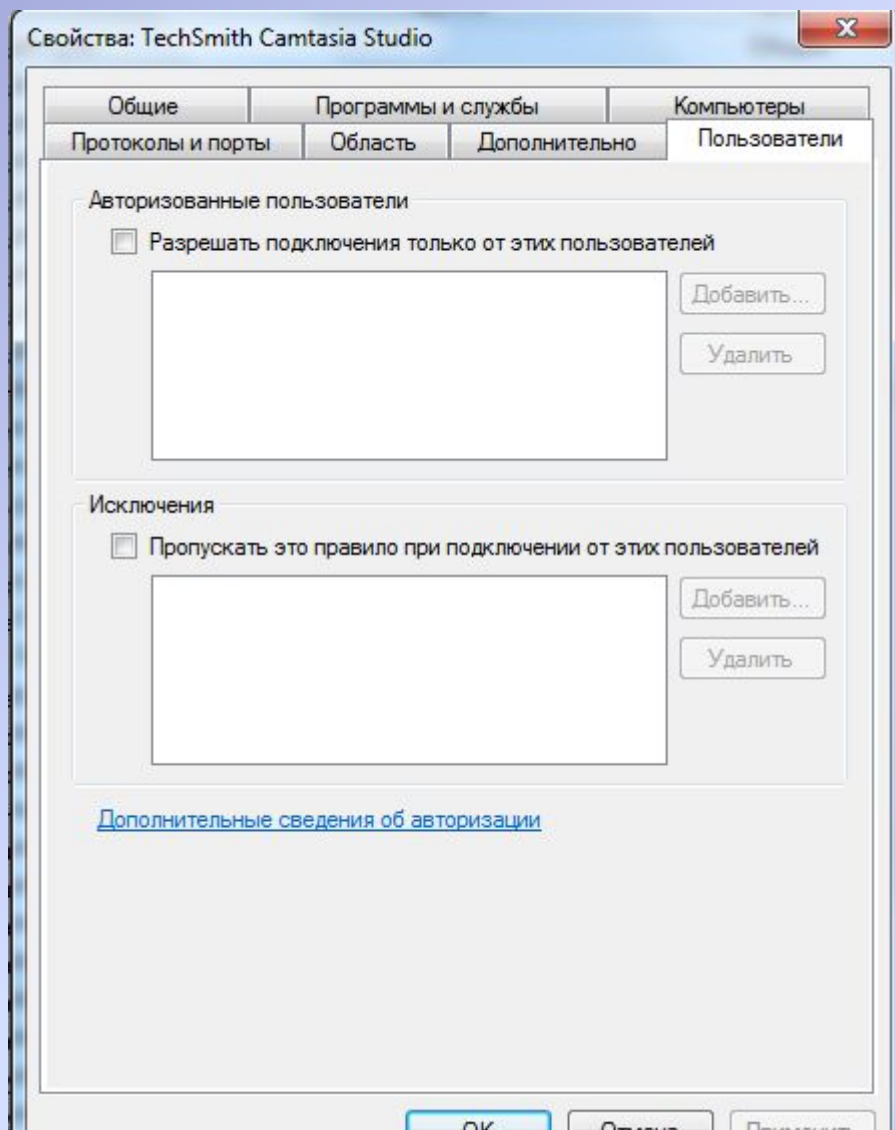




# Windows Firewall с расширенными возможностями

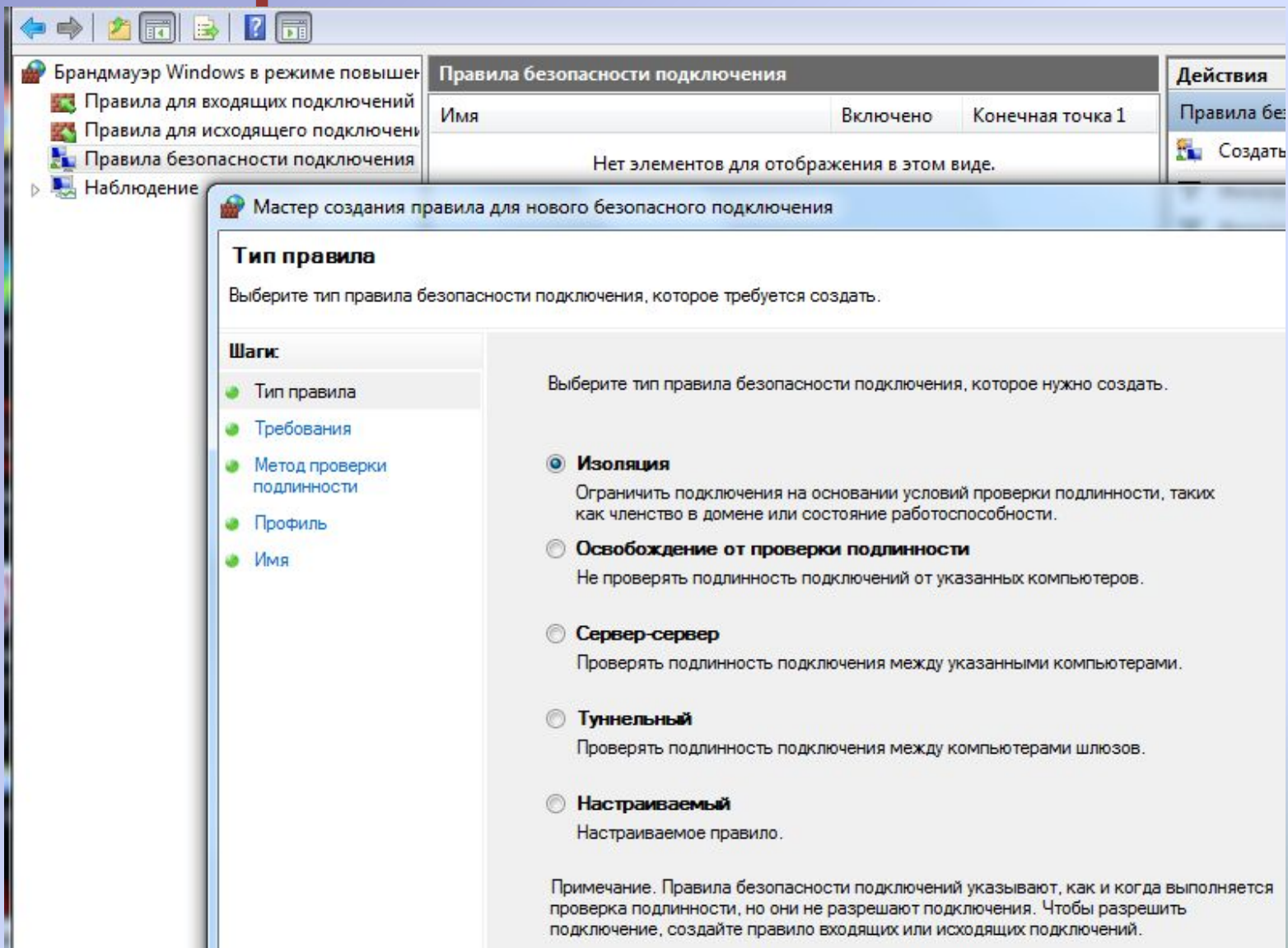


# Windows Firewall с расширенными возможностями





# Windows Firewall с расширенными возможностями



# Windows Firewall с расширенными возможностями

Мастер создания правила для нового безопасного подключения

## Требования

Укажите требования проверки подлинности для подключений, соответствующих данному правилу.

Шаги:	
<input checked="" type="radio"/> Тип правила	
<input checked="" type="radio"/> Конечные точки	
<input checked="" type="radio"/> Требования	
<input checked="" type="radio"/> Метод проверки подлинности	
<input checked="" type="radio"/> Протокол и порты	
<input checked="" type="radio"/> Профиль	
<input checked="" type="radio"/> Имя	

Когда выполнять проверку подлинности?

- ☒ **Запрашивать проверку подлинности для входящих и исходящих подключений**  
Проверять подлинность, когда возможно, но подтверждение подлинности не обязательно.
- ☐ **Требовать проверку подлинности для входящих подключений и запрашивать проверку подлинности для исходящих подключений**  
Входящие подключения разрешаются только после проверки подлинности. Проверять подлинность исходящих, когда возможно, но подтверждение подлинности не обязательно.
- ☐ **Требовать проверку подлинности для входящих и исходящих подключений**  
Входящие и исходящие подключения разрешаются только после выполнения проверки подлинности.
- ☐ **Не выполнять проверку подлинности**  
Подлинность подключений не проверяется.

# Windows Firewall с расширенными возможностями

Мастер создания правила для нового безопасного подключения

## Метод проверки подлинности

Укажите способ выполнения проверки подлинности для подключений, соответствующих данному правилу.

### Шаги:

- Тип правила
- Конечные точки
- Требования
- Метод проверки подлинности**
- Протокол и порты
- Профиль
- Имя

Выберите метод проверки подлинности.

☒ **По умолчанию**

Использовать методы проверки подлинности, указанные в параметрах IPsec.

☐ **Компьютер и пользователь (Kerberos V5)**

Разрешается передача данных только пользователям и компьютерам, входящим в состав домена. Предоставляет учетные данные для проверки подлинности указанных пользователей и компьютеров для правил входящих и исходящих подключений.

☐ **Компьютер (Kerberos V5)**

Разрешается передача данных только между компьютерами, подключенными к домену. Предоставляет учетные данные для проверки подлинности указанных компьютеров для правил входящих и исходящих подключений.

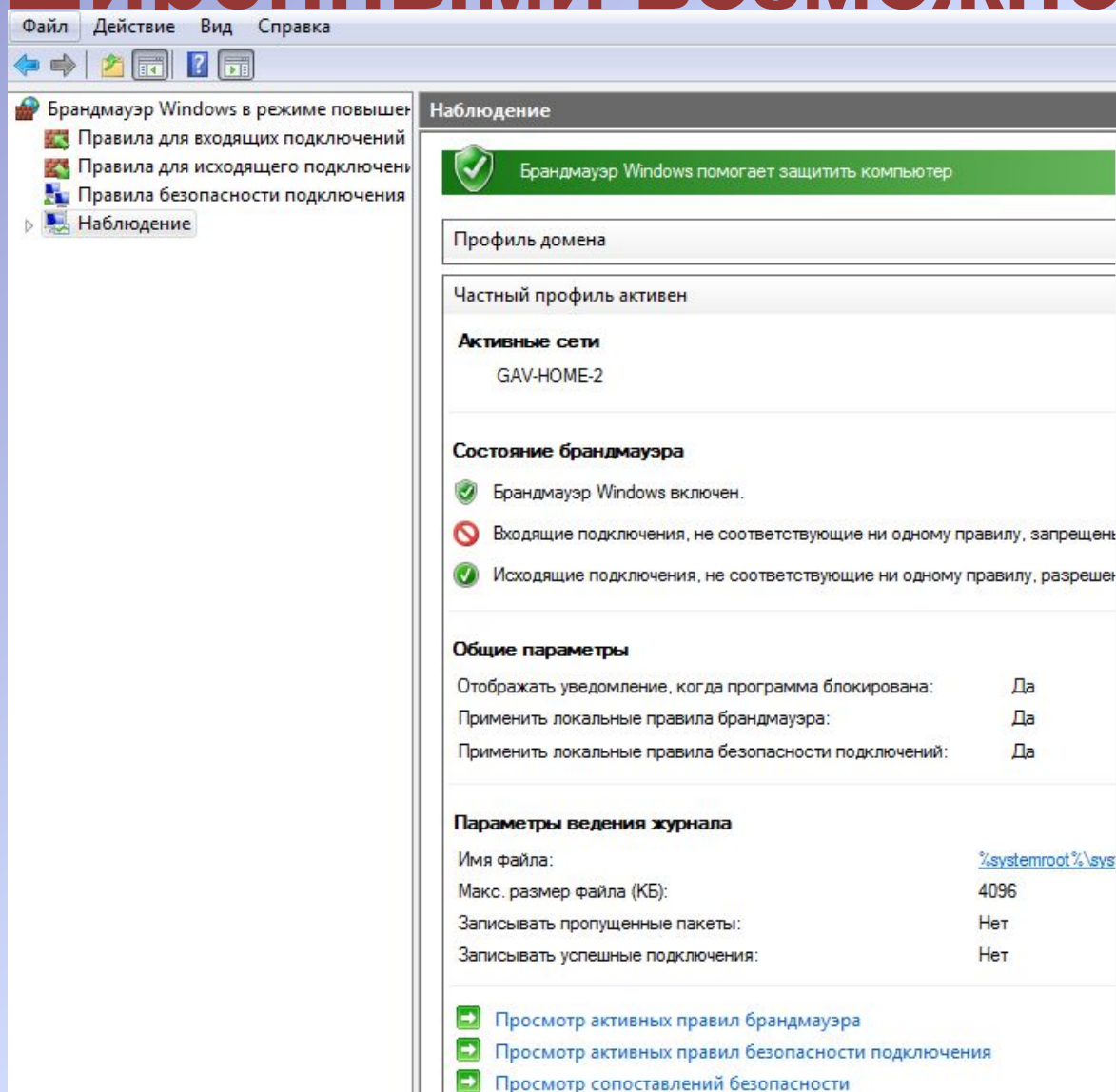
☐ **Дополнительно**

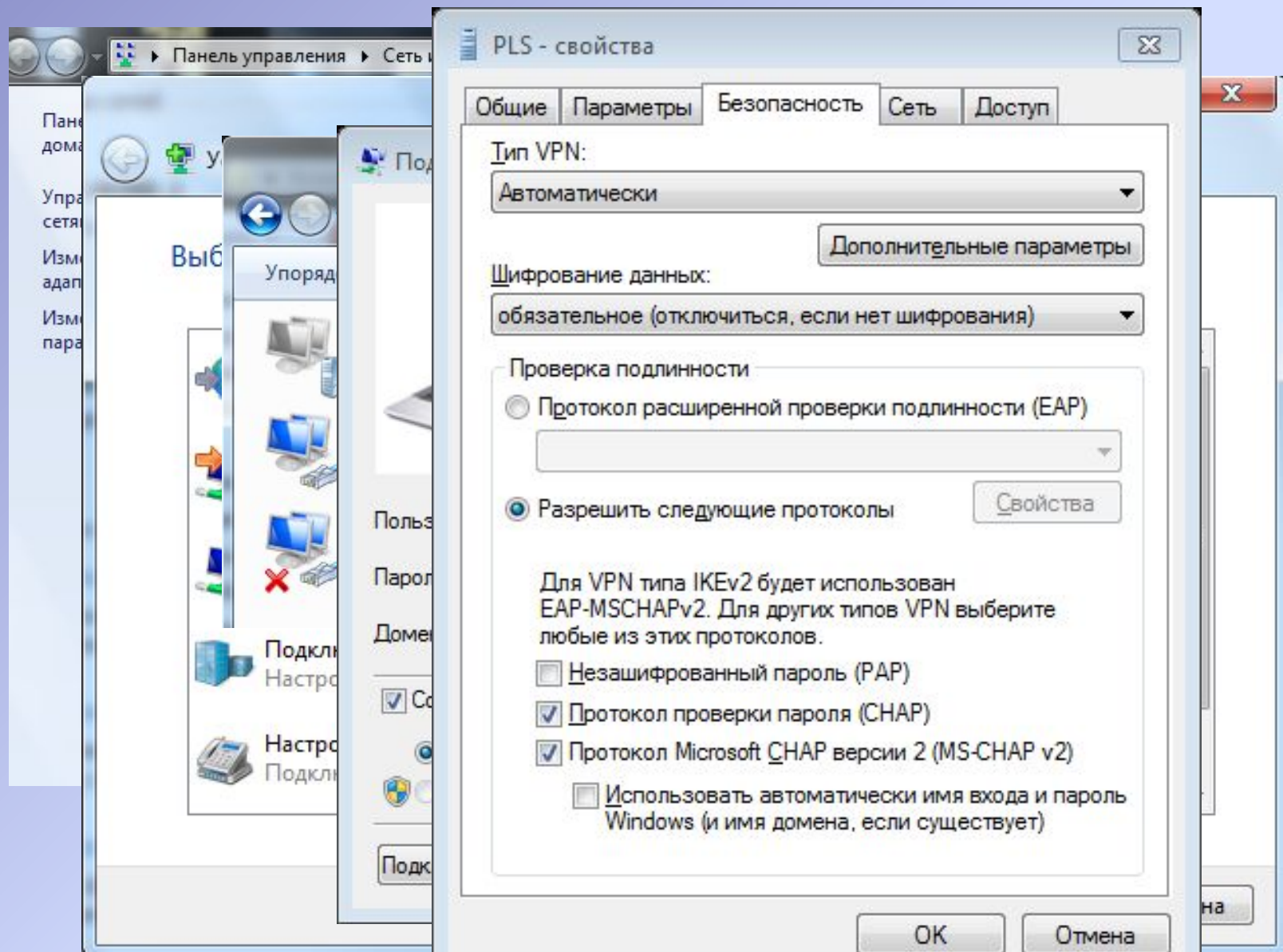
Выберите параметры первой и второй проверки подлинности.

Настроить..



# Windows Firewall с расширенными возможностями





## PLS - свойства

Общие | Параметры | **Безопасность** | Сеть | Доступ

Тип VPN:

Автоматически

Дополнительные параметры

Шифрование данных:

обязательное (отключиться, если нет шифрования)

Проверка подлинности

☐ Протокол расширенной проверки подлинности (EAP)

☒ Разрешить следующие протоколы

Свойства

Для VPN типа IKEv2 будет использован EAP-MSCHAPv2. Для других типов VPN выберите любые из этих протоколов.

☐ Незашифрованный пароль (PAP)

☒ Протокол проверки пароля (CHAP)

☒ Протокол Microsoft CHAP версии 2 (MS-CHAP v2)

☐ Использовать автоматически имя входа и пароль Windows (и имя домена, если существует)

OK

Отмена

C:\Users\Alexander&gt;ipconfig /all

## Настройка протокола IP для Windows

```

Имя компьютера . . . . . : Gav-WorkPlace
Основной DNS-суффикс . . . . . :
Тип узла. . . . . : Гибридный
IP-маршрутизация включена . . . . : Нет
WINS-прокси включен . . . . . : Нет

```

## Адаптер PPP PLS:

```

Имя компьютера . . . . . : Gav-WorkPlace
Основной DNS-суффикс . . . . . :
Тип узла. . . . . : Гибридный
IP-маршрутизация включена . . . . : Нет
WINS-прокси включен . . . . . : Нет
DNS-суффикс подключения . . . . . :
Описание. . . . . : PLS
Физический адрес. . . . . :
DHCP включен. . . . . : Нет
Автонастройка включена. . . . . : Да
IPv4-адрес. . . . . : 10.10.0.3(Основной)
Маска подсети . . . . . : 255.255.255.255
Основной шлюз. . . . . : 0.0.0.0
DNS-серверы. . . . . : 192.168.224.4
                        195.26.162.34
NetBios через TCP/IP. . . . . : Включен

```

## Адаптер беспроводной локальной сети Беспроводное сетевое соединение:

```

Имя компьютера . . . . . : Gav-WorkPlace
Основной DNS-суффикс . . . . . :
Тип узла. . . . . : Гибридный
IP-маршрутизация включена . . . . : Нет
WINS-прокси включен . . . . . : Нет
DNS-суффикс подключения . . . . . :
Описание. . . . . : Сетевое подключение Intel(R) PRO/Wireless
3945ABG
Физический адрес. . . . . : 00-1B-77-DE-01-59
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
IPv4-адрес. . . . . : 192.168.2.145(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 5 ноября 2015 г. 8:42:32
Срок аренды истекает. . . . . : 7 ноября 2015 г. 7:53:03
Основной шлюз. . . . . : 192.168.2.1
DHCP-сервер. . . . . : 192.168.2.1
DNS-серверы. . . . . : 192.168.2.1
NetBios через TCP/IP. . . . . : Включен

```

## Ethernet adapter Подключение по локальной сети:

```

Имя компьютера . . . . . : Gav-WorkPlace
Основной DNS-суффикс . . . . . :
Тип узла. . . . . : Гибридный
IP-маршрутизация включена . . . . : Нет
WINS-прокси включен . . . . . : Нет
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Сетевой адаптер Broadcom NetLink (TM) G
abit Ethernet
Физический адрес. . . . . : 00-16-D3-EE-1F-39
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

```

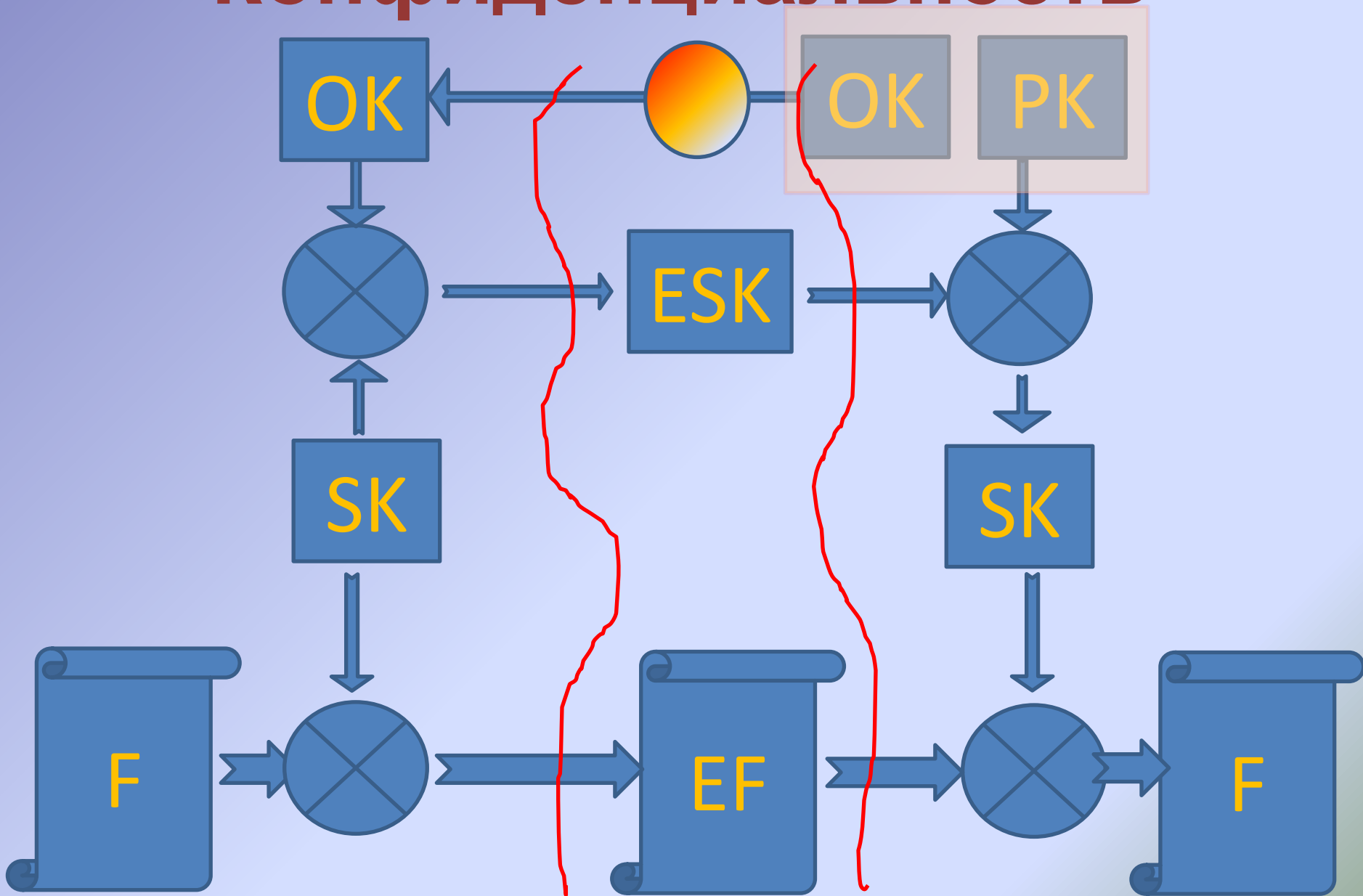
## Ethernet adapter VMware Network Adapter VMnet1:

```

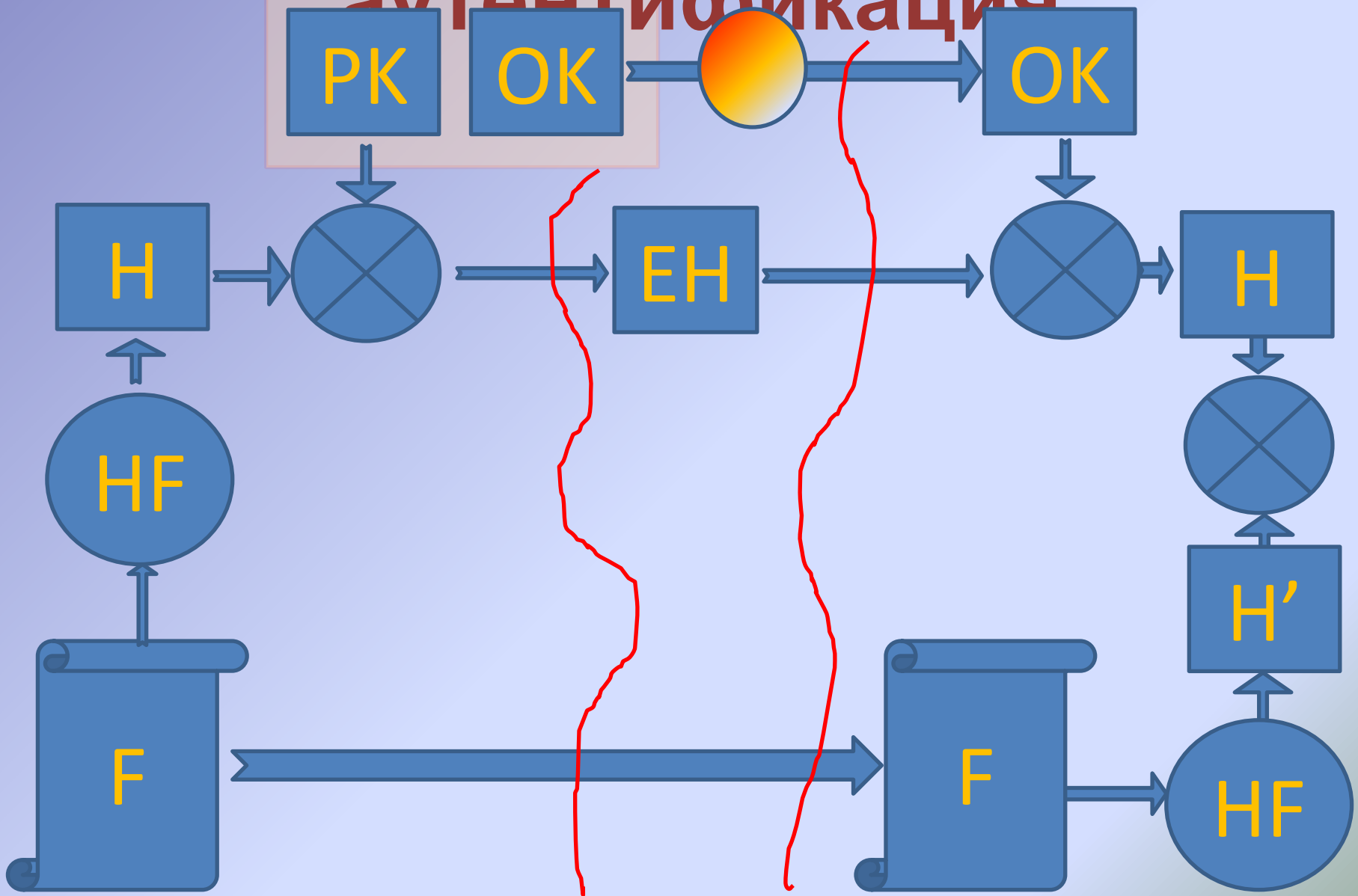
Имя компьютера . . . . . : Gav-WorkPlace
Основной DNS-суффикс . . . . . :
Тип узла. . . . . : Гибридный
IP-маршрутизация включена . . . . : Нет
WINS-прокси включен . . . . . : Нет
DNS-суффикс подключения . . . . . :
Описание. . . . . : VMware Virtual Ethernet Adapter for VMn

```

# Конфиденциальность



# Целостность и аутентификация





# Списки управления доступом

Горячев Александр Вадимович  
Доцент кафедры ИБ  
[avgoriachev@etu.ru](mailto:avgoriachev@etu.ru)

# модель эшелонированной обороны

Физический

Политики, процедуры,  
осведомленность

Хранилище

ACL EFS Bitlocker

Backup Mirror RAID SC

Обработка

APPs Antivirus Updates

OS/.NET Antispyware Autentification HIDS-HIPS

PKI

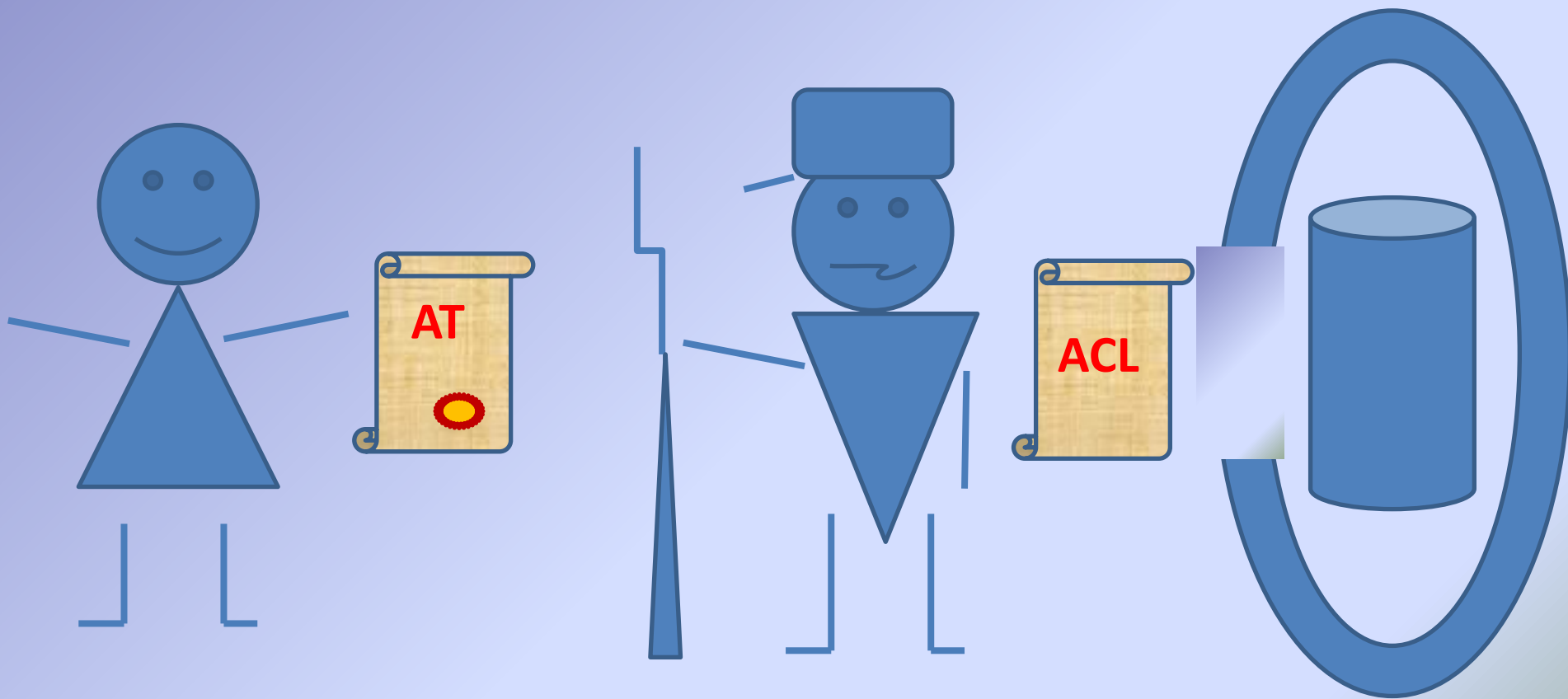
AD

Передача

Intranet Routing IPsec RMS NIDS-NIPS

Internet Firewall VPN NAP

# Список контроля доступа



# Список контроля доступа (ACL)

SID	Прав	A/D	I
SID O1	a R	A	
SID O2	RW	A	I
SID O3	RWM	D	

# Маркер доступа (AT)



# Обеспечение доступности информации при хранении

Горячев Александр Вадимович  
Доцент кафедры  
Информационной безопасности  
[avgoriachev@etu.ru](mailto:avgoriachev@etu.ru)

# Модель эшелонированной обороны

Физический  
доступ

Политики, процедуры,  
осведомленность

Хранение

ACL EFS Bitlocker

Backup Mirror RAID SC

Обработка

APPs

Antivirus Updates

OS/.NET

Antispyware Autentification HIDS-HIPS

PKI

AD

Передача

Intranet

Routing

IPSec

RMS

NIDS-NIPS

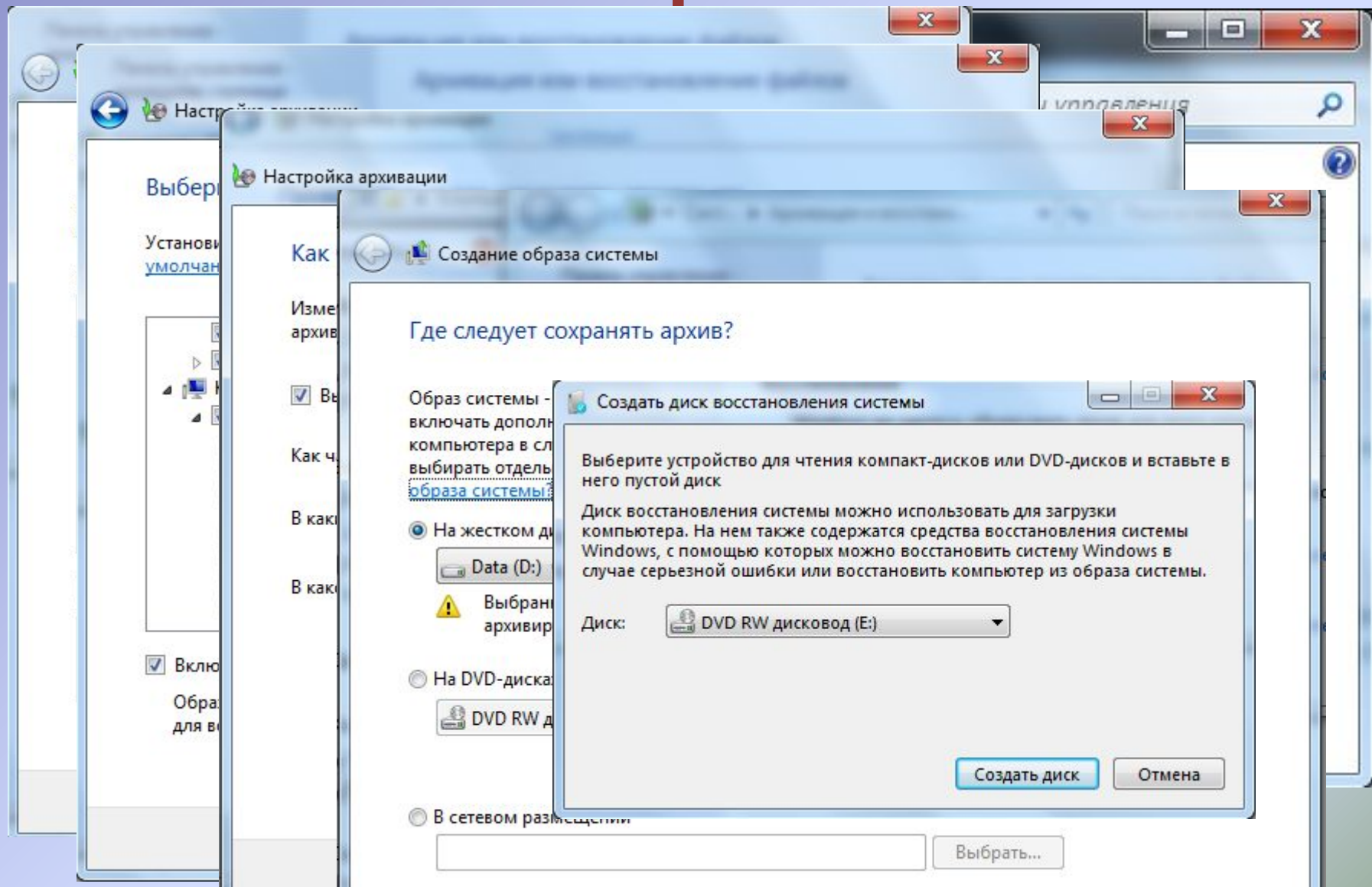
Internet

Firewall

VPN

NAP

# Резервное копирование. Настройка





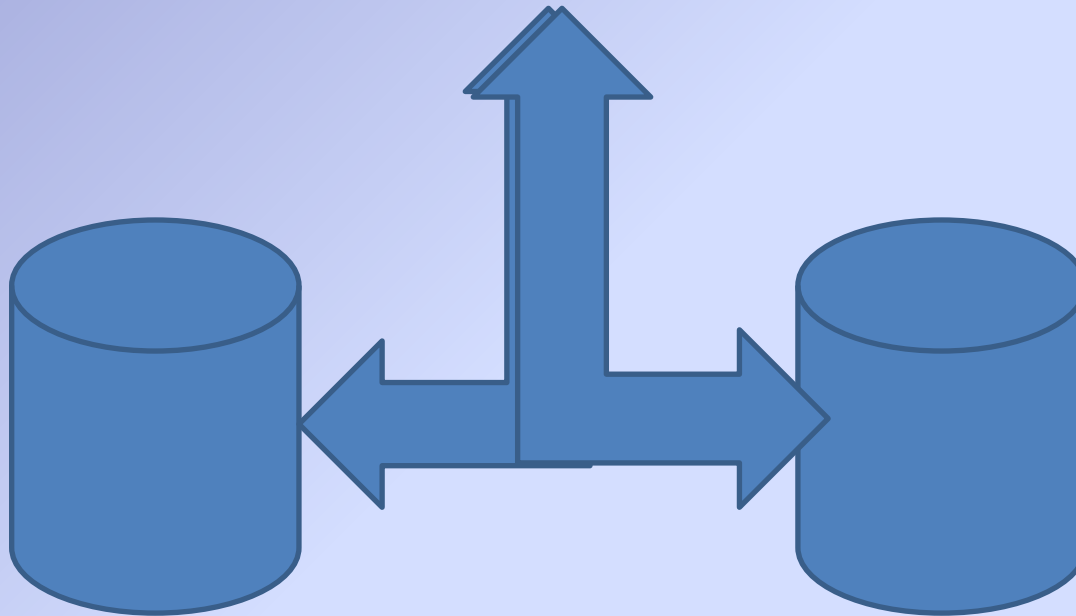
# Резервное копирование. Схемы

- Полная копирование
- Инкрементальное копирование
- Дифференциальное копирование
- Копирование на конкретную дату

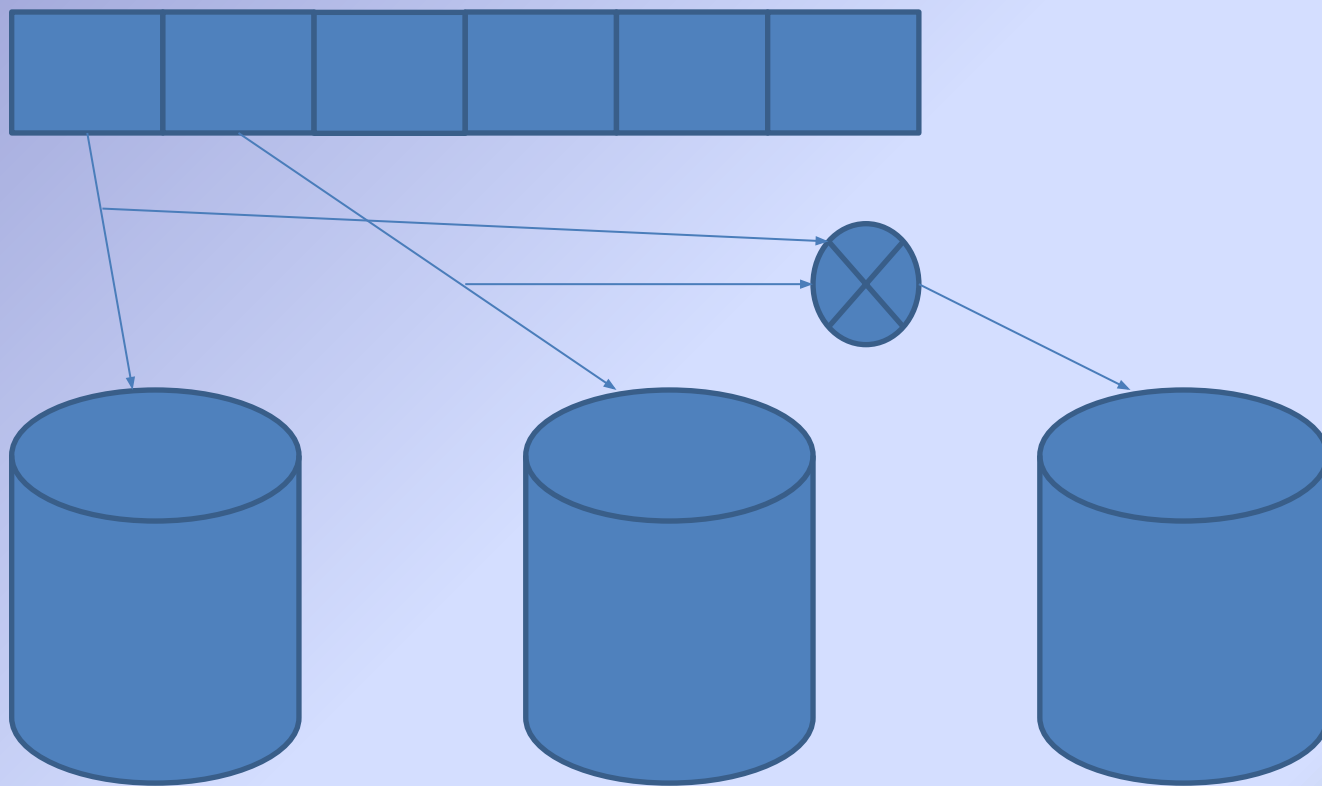
# Резервное копирование. Правила

- ТРИ экземпляра копии, один – «OffSite»
- Регулярная проверка целостности копии
- Резервная копия – находка для злодея

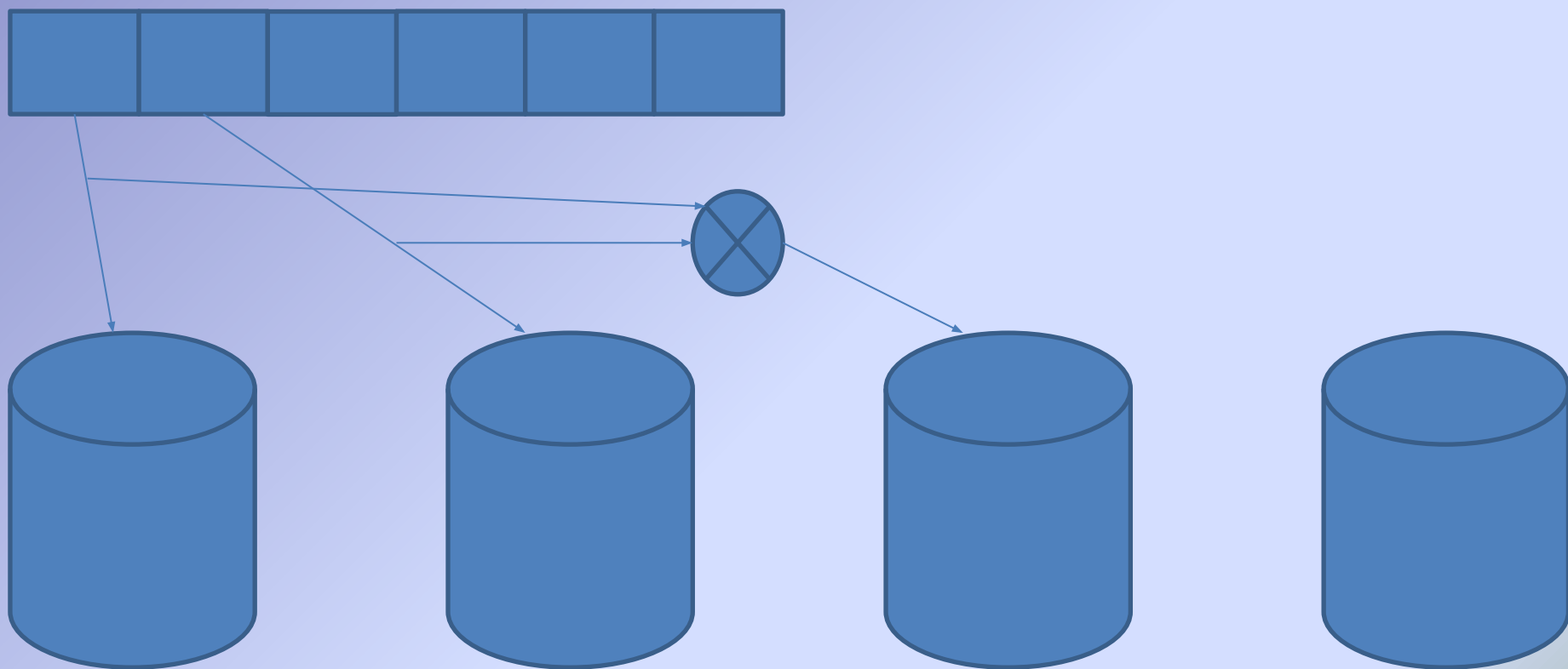
# Дисковые массивы. Зеркало



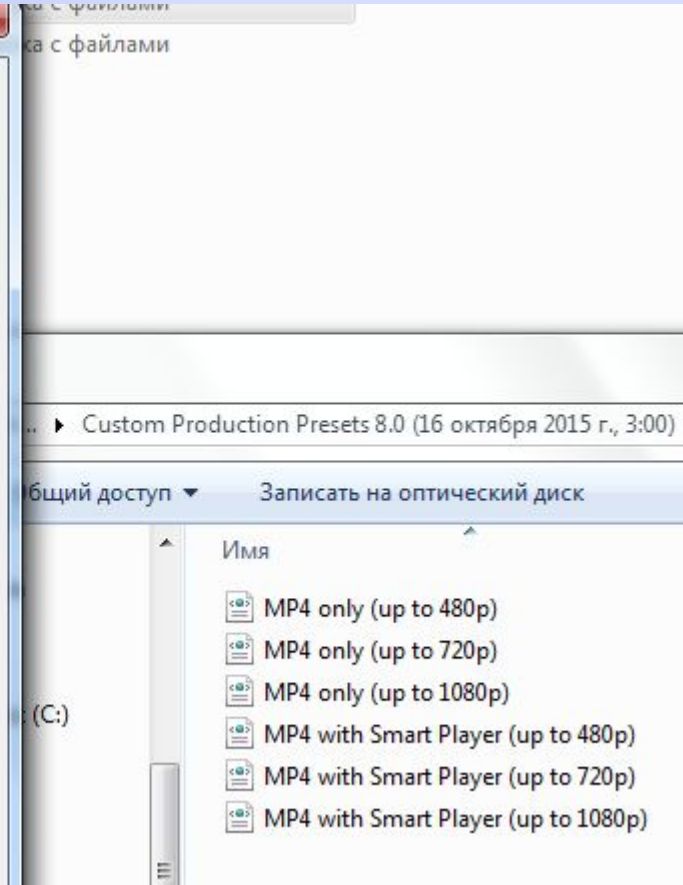
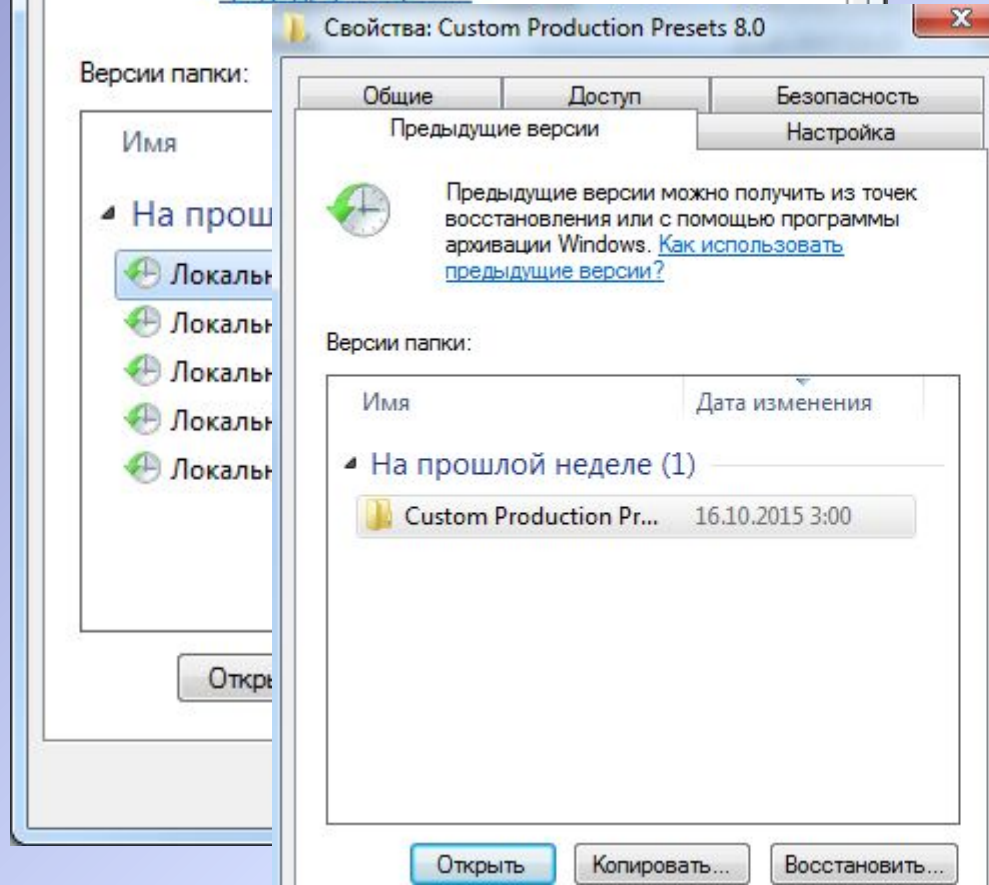
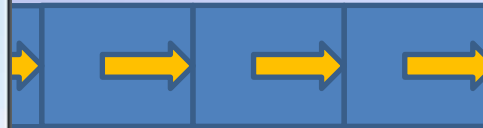
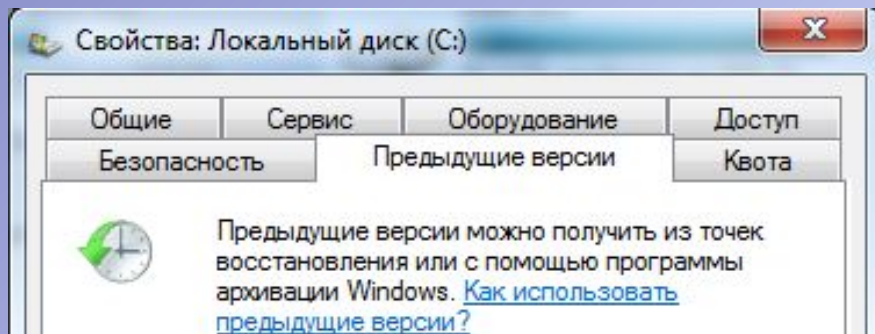
# Дисковые массивы. RAID 5



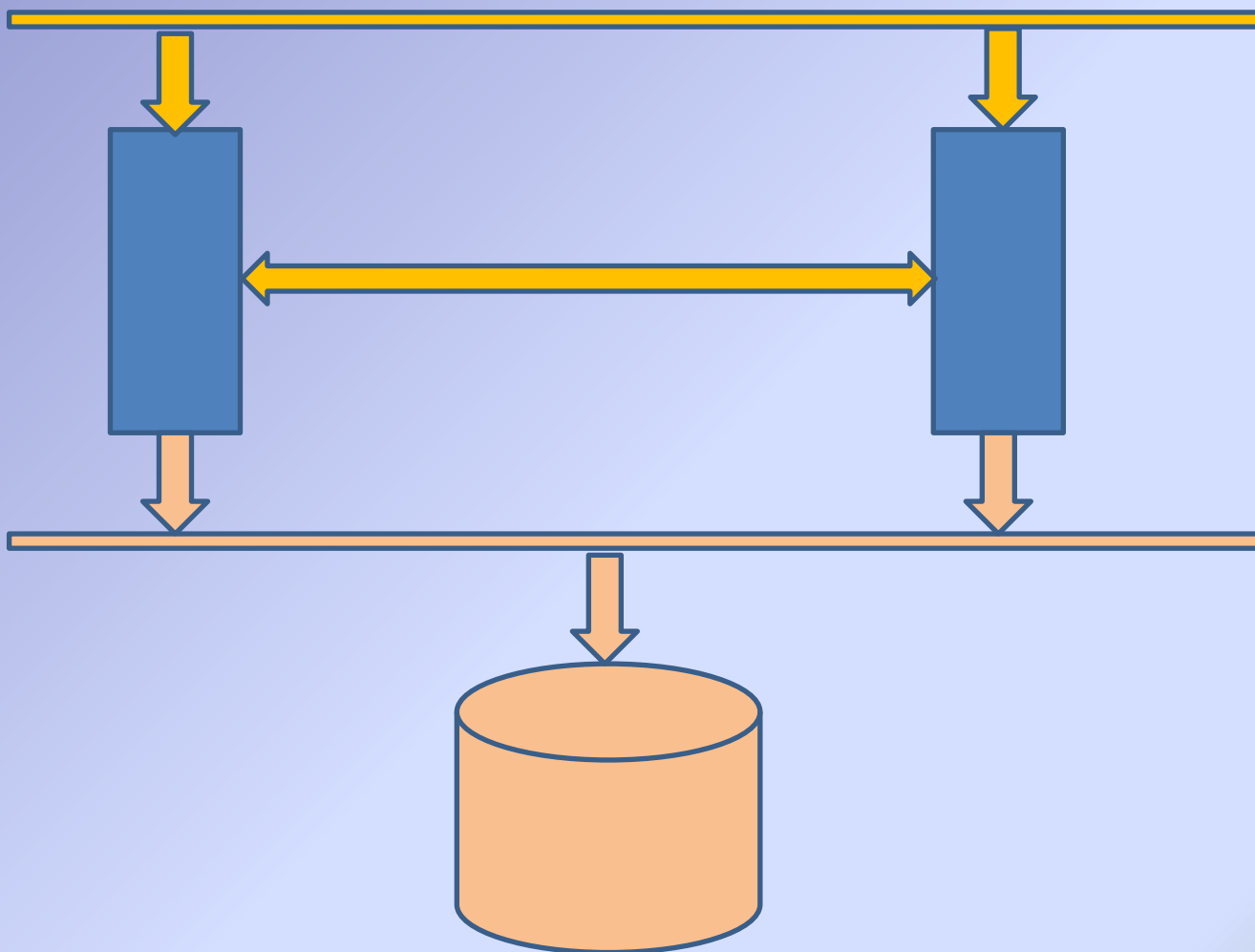
# Дисковые массивы. Hot Spare



# Shadow Copy



# Кластер надежности



# Групповые политики службы каталога Active Directory

Горячев Александр Вадимович  
Доцент кафедры  
Информационной безопасности  
[avgoriachev@etu.ru](mailto:avgoriachev@etu.ru)



# Модель эшелонированной обороны

Физический  
доступ

Политики, процедуры,  
осведомленность

Хранение

ACL EFS Bitlocker

Backup Mirror RAID SC

Обработка

APPs Antivirus Updates

OS/.NET Antispyware Autentification HIDS-HIPS

PKI

AD

Передача

Intranet Routing IPsec RMS NIDS-NIPS

Internet Firewall VPN NAP

# Локальная политика безопасности

Console Root	Policy	Security Setting
<ul style="list-style-type: none"><li>Security Templates<ul style="list-style-type: none"><li>C:\Users\Student\Documents\Security\Templates<ul style="list-style-type: none"><li>Temp1</li></ul></li></ul></li><li>Security Configuration and Analysis</li><li>Local Computer Policy<ul style="list-style-type: none"><li>Computer Configuration<ul style="list-style-type: none"><li>Software Settings</li><li>Windows Settings<ul style="list-style-type: none"><li>Name Resolution Policy</li><li>Scripts (Startup/Shutdown)</li><li>Security Settings<ul style="list-style-type: none"><li>Account Policies<ul style="list-style-type: none"><li><b>Password Policy</b></li><li>Account Lockout Policy</li></ul></li><li>Local Policies</li><li>Windows Firewall with Advanced Security</li><li>Network List Manager Policies</li><li>Public Key Policies</li><li>Software Restriction Policies</li><li>Application Control Policies</li><li>IP Security Policies on Local Computer</li><li>Advanced Audit Policy Configuration</li></ul></li><li>Policy-based QoS</li></ul></li><li>Administrative Templates</li></ul></li><li>User Configuration<ul style="list-style-type: none"><li>Software Settings</li><li>Windows Settings</li><li>Administrative Templates</li></ul></li></ul></li></ul>	<ul style="list-style-type: none"><li>Enforce password history</li><li>Maximum password age</li><li>Minimum password age</li><li>Minimum password length</li><li>Password must meet complexity requirements</li><li>Store passwords using reversible encryption</li></ul>	<ul style="list-style-type: none"><li>24 passwords remember...</li><li>42 days</li><li>1 days</li><li>7 characters</li><li>Enabled</li><li>Disabled</li></ul>


# Шаблоны безопасности

The screenshot displays the Windows Security Templates console. On the left, a tree view shows the hierarchy: Console Root > Security Templates > C:\Users\Student\Documents\Security\Templa > Temp1 > Account Policies > Password Policy. The main pane on the right lists several policies with their corresponding computer settings. The 'Password must meet complexity requirements' policy is highlighted. A pop-up window titled 'Password must meet complexity requirements Pro...' is open, showing the 'Template Security Policy Setting' tab. In this window, the checkbox 'Define this policy setting in the template' is checked, and the 'Enabled' radio button is selected.

Policy	Computer Setting
Enforce password history	Not Defined
Maximum password age	42 days
Minimum password age	30 days
Minimum password length	Not Defined
Password must meet complexity requirements	Not Defined
Store passwords using reversible encryption	Not Defined

**Password must meet complexity requirements Pro...**

Template Security Policy Setting Explain

 Password must meet complexity requirements

☒ Define this policy setting in the template

☒ Enabled

☐ Disabled

# Анализ и конфигурация безопасности

Console Root

Security Templates

C:\Users\Student\Documents\Security\Templ

Temp1

Security Configuration and Analysis

Account Policies

Password Policy

Account Lockout Policy

Local Policies

Event Log

Restricted Groups

System Services

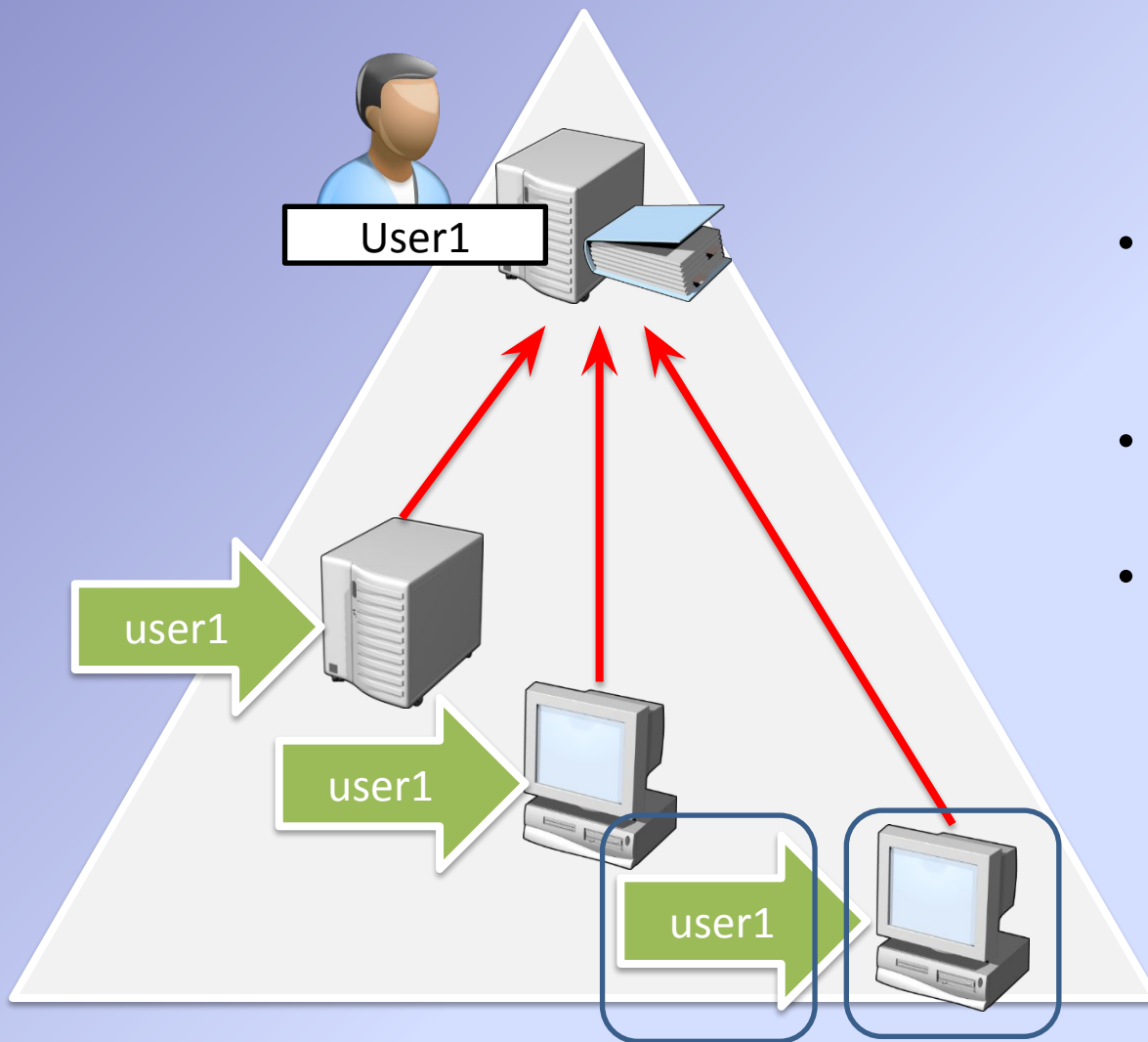
Registry

File System

Local Computer Policy

Policy	Database Setting	Computer Set
Enforce password history	Not Defined	24 passwords i
Maximum password age	42 days	42 days
Minimum password age	30 days	1 days
Minimum password length	Not Defined	7 characters
Password must meet complexity requirements	Not Defined	Enabled
Store passwords using reversible encryption	Not Defined	Disabled

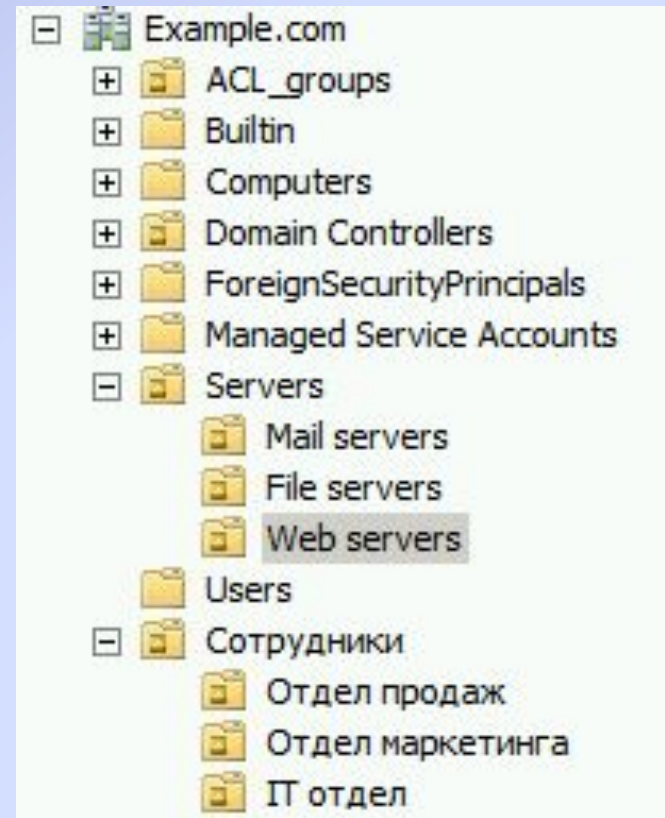
# Домен Windows NT



- Требует наличия как минимум одного контроллера домена (PDC)
  - Граница репликации домена
  - Доверенный источник учётных данных: любой доменный контроллер (PDC и BDC) может провести аутентификацию в домене
- Security Account Manager

# Подразделения (организационные единицы)

- Объекты
  - Пользователи
  - Компьютеры
- Подразделения
  - Контейнеры для группировки объектов в домене
  - Подразделения создаются:
    - Для делегирования разрешений
    - Для назначения групповых политик



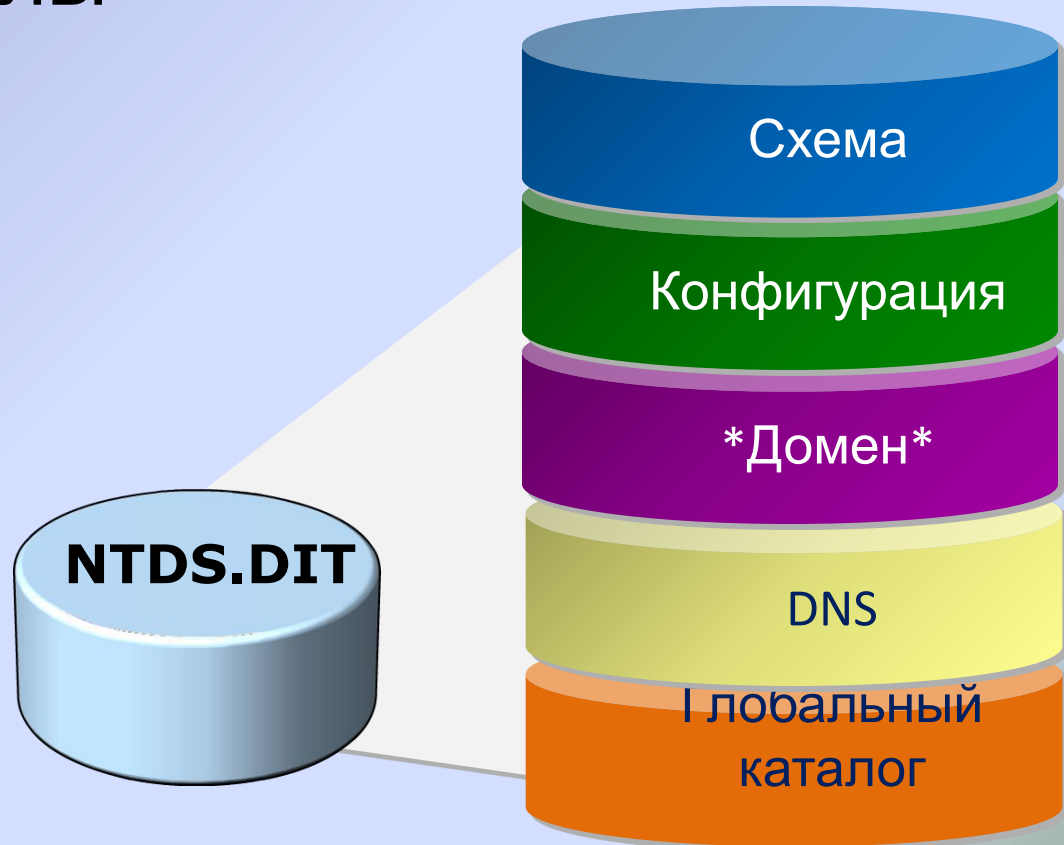


# Хранилище данных Active Directory

- %systemroot%\NTDS\ntds.dit
- Логические разделы
  - Домен
  - Схема
  - Конфигурация
  - Глобальный каталог
  - DNS

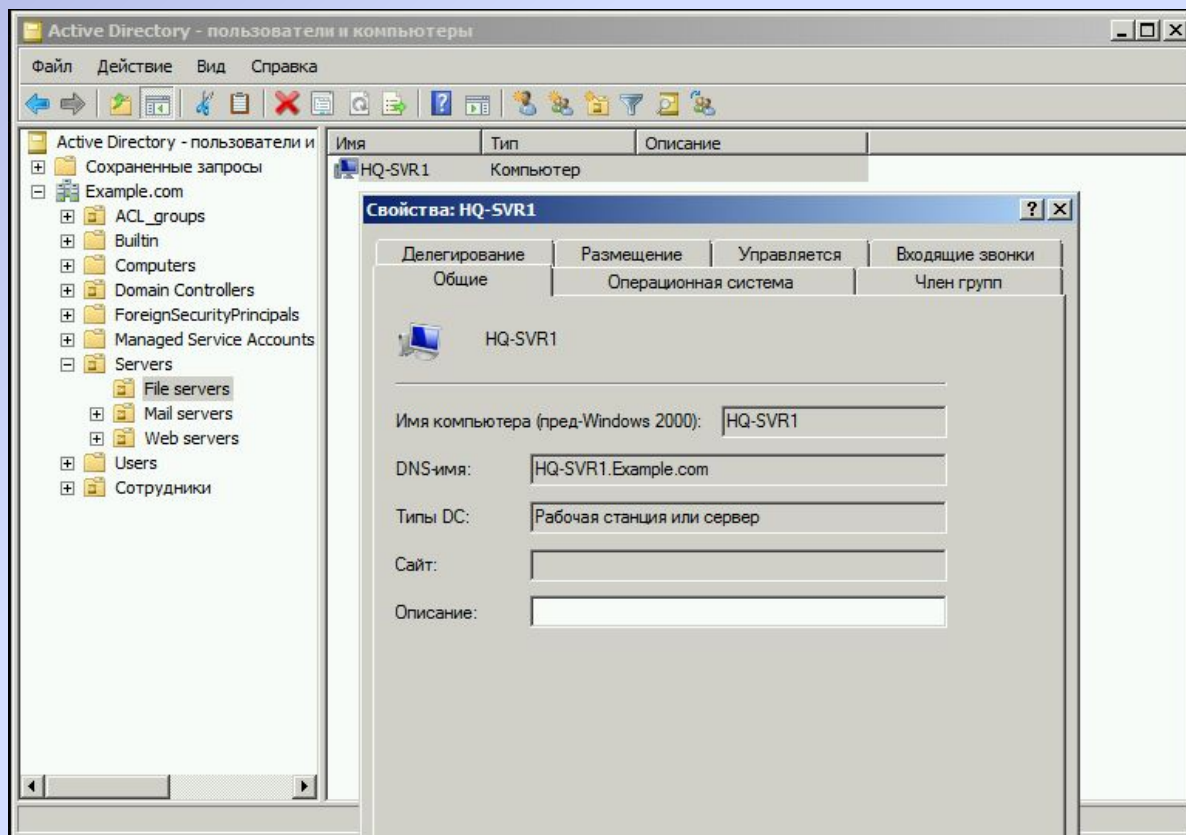
- **SYSVOL**

- %systemroot%\SYSVOL
- Скрипты входа в систему
- Политики



# Учётные записи компьютеров

- Компьютер является участником безопасности как и пользователь
- Учётная запись компьютера необходима для доверительных отношений



# Параметры групповой политики

- Детальное определение изменений в конфигурации

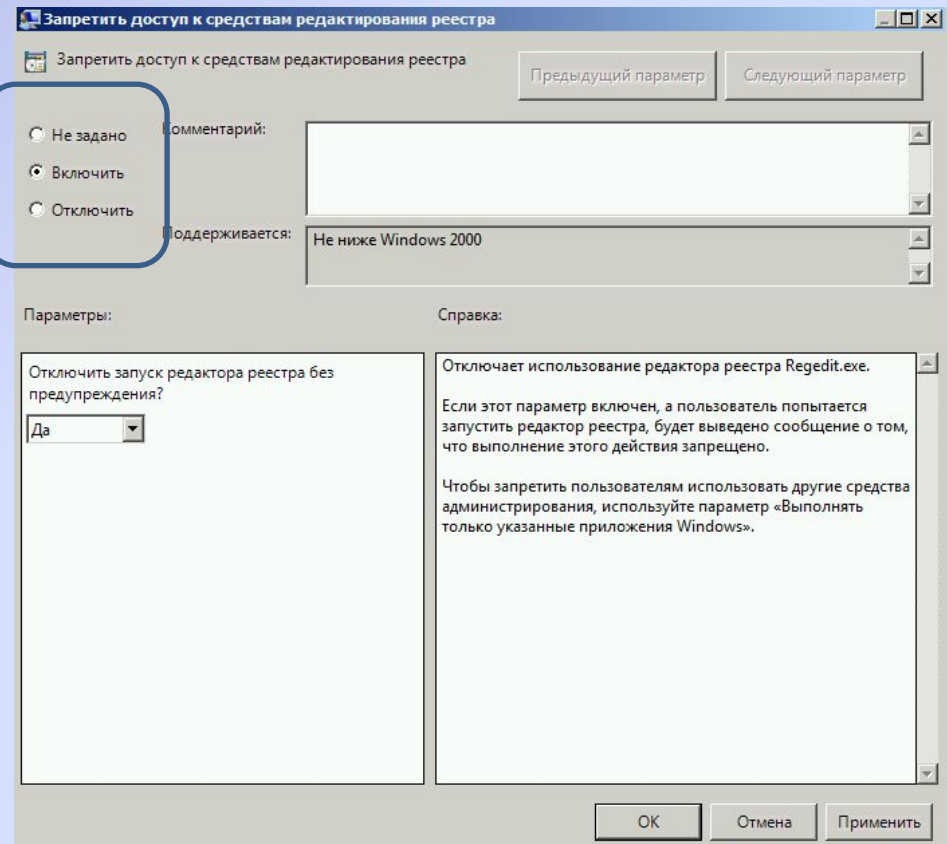
- Предотвратить доступ к реестру
- Назначить установку приложения
- Выполнить скрипт при включении компьютера

- Подразделяются на

- Конфигурацию пользователя
- Конфигурацию компьютера

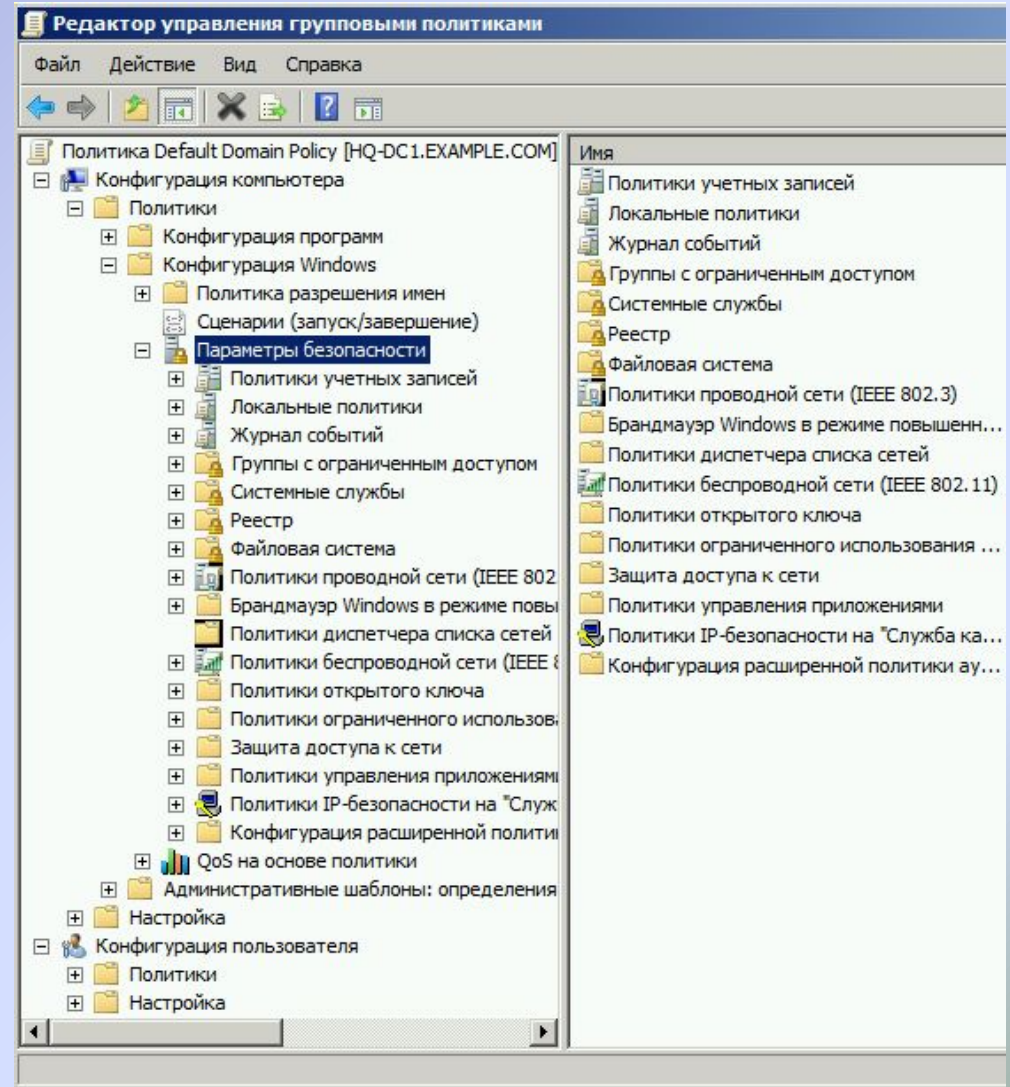
- Могут быть

- Не настроены (Not configured)
- Включены (Enabled)
- Выключены (Disabled)



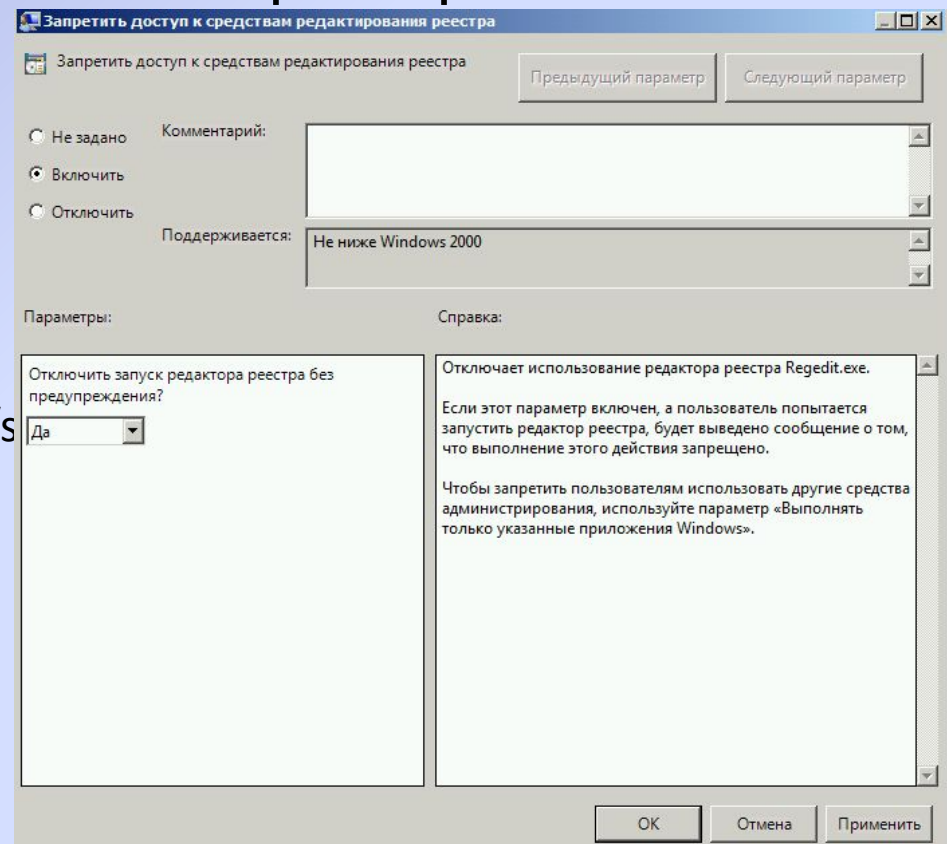
# Объекты групповой политики

- Контейнер для параметров групповой политики
- Применяется на определённом уровне иерархии Active Directory



# Административные шаблоны

- Параметры политик из Административных Шаблонов производят изменения в реестре
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
  - DisableRegeditMode
    - 1 – Отключить только UI
    - 2 – Также отключить regedit /s



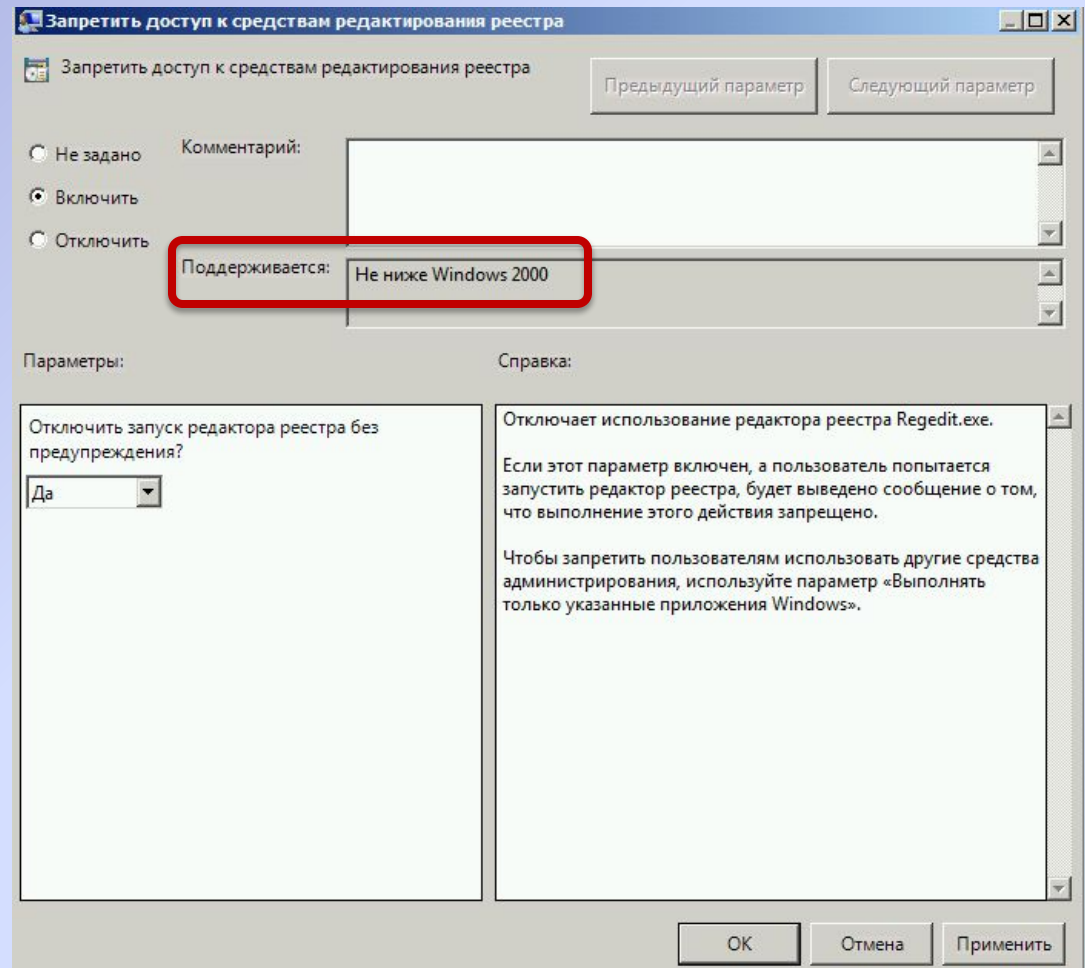


# Клиент групповой политики и Client-side extensions

1. Клиент групповой политики получает список GPO с порядком применения
2. GPO загружаются и кэшируются
3. CSEs обрабатывают настройки для применения изменений
  - Отдельный CSE для каждой крупной категории параметров: Security, registry, script, software installation, mapped drive preferences.
  - Большинство CSEs применяют изменения только если GPO изменился
    - Security CSE применяет настройки каждые 16 часов
  - Применение GPO инициируется клиентом

# Применение политик разными операционными системами

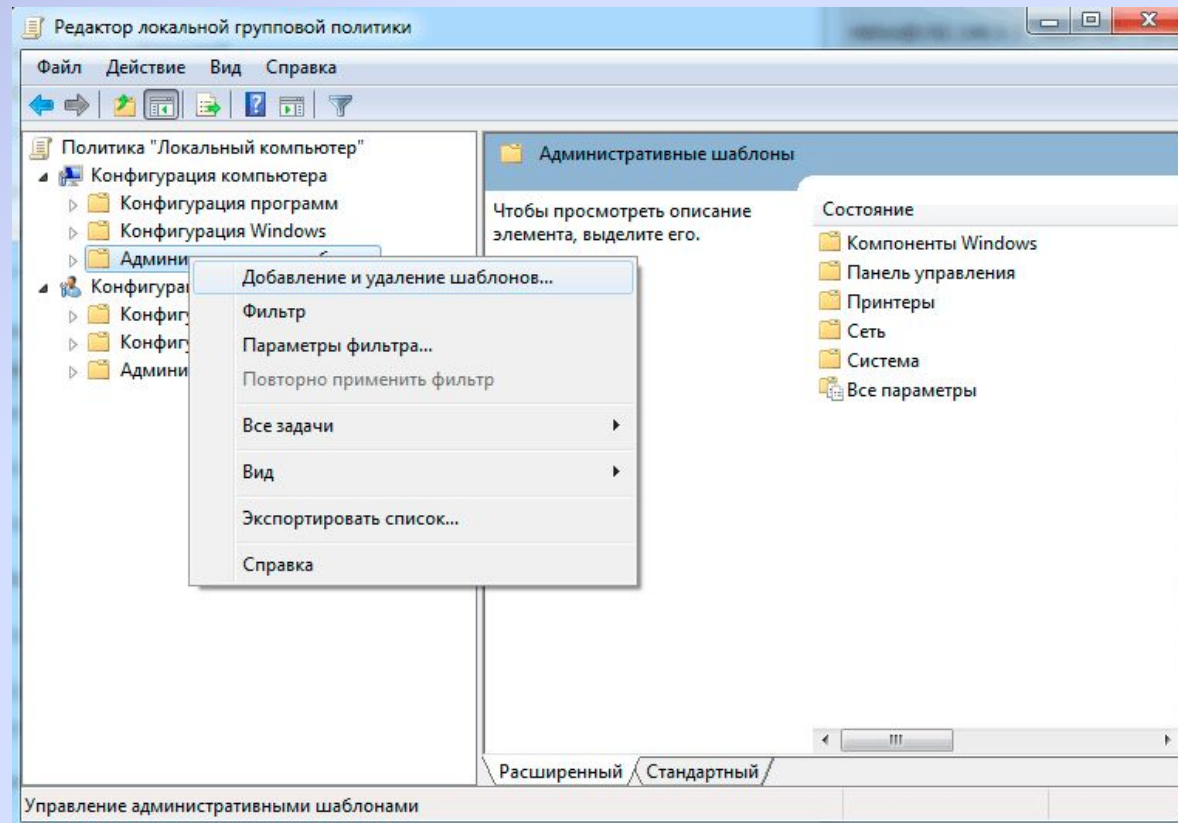
- Минимальный поддерживаемый уровень
- Client Side Extensions
- Синхронное и асинхронное применение политик



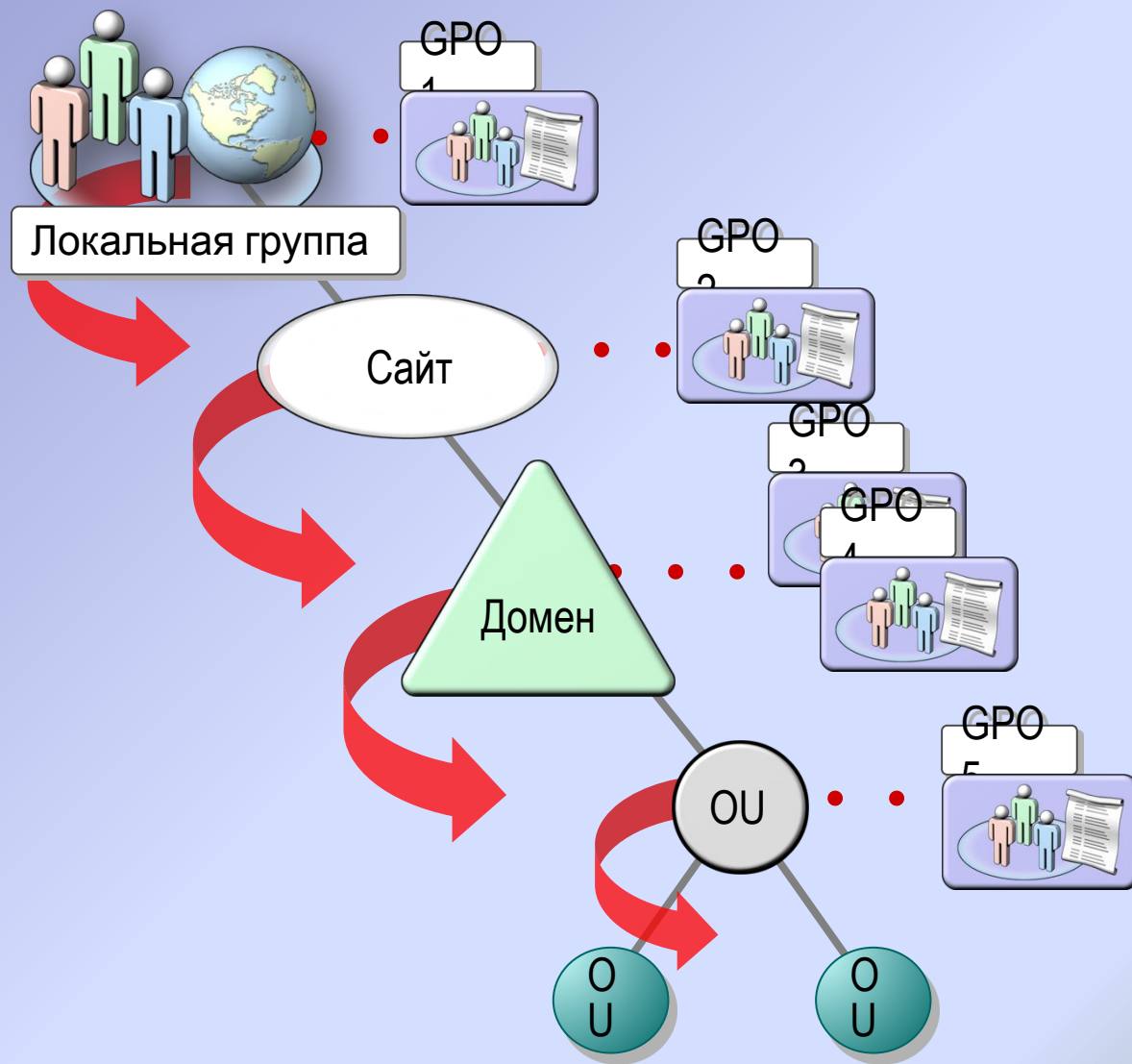


# Расширение функционала с помощью административных шаблонов

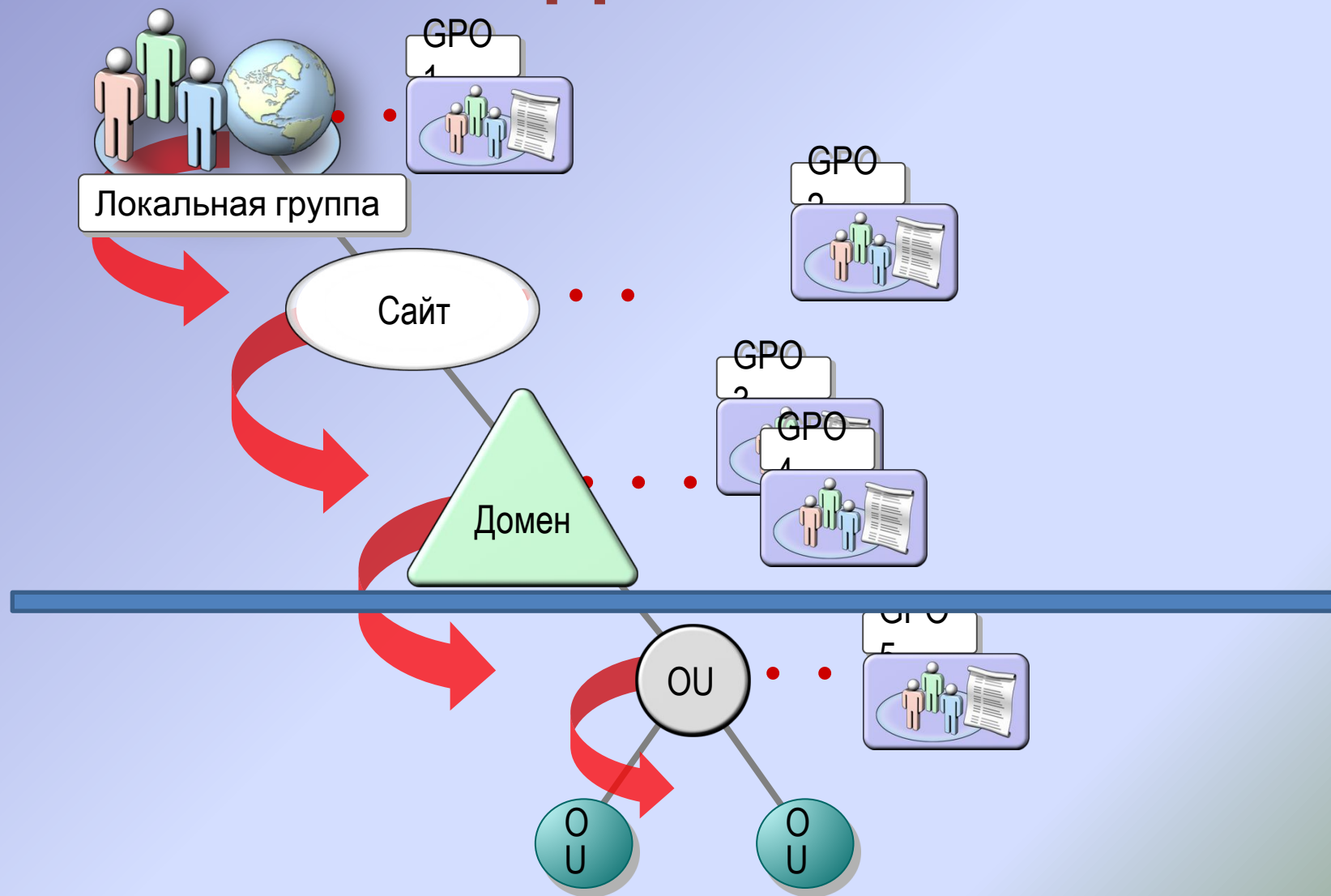
- Административные шаблоны позволяют централизованно управлять программным обеспечением:
  - Microsoft Office, Google Chrome, etc
- ADM
- ADMX/ADML



# Порядок применения GPO



# Блокирование наследования



# Фильтрация по безопасности

# Фильтрация WMI

# Область применения

- Область применения
  - Определение объектов (пользователей и компьютеров) к которым применяется GPO
- Связи GPO
  - GPO может быть привязан к нескольким доменам, сайтам, подразделениям (OU)
  - Связь GPO определяет максимальную область применения GPO
- Фильтрация безопасности
  - Разрешает или запрещает применение GPO членами глобальной группы безопасности
  - Позволяет фильтровать применение GPO в рамках связи
- WMI Фильтрация
  - Позволяет изменять область применения на основе WMI запроса

# Обновление групповых ПОЛИТИК

- Когда применяются параметры GPO
- Конфигурация компьютера
  - Включение
  - Каждые 90-120 минут
  - GPOupdate
- Конфигурация пользователя
  - Вход в систему
  - Каждые 90-120 минут
  - GPOupdate



# Предпочтения групповой политики

Предпочтения групповых политик расширяют диапазон настраиваемых параметров GPO и:

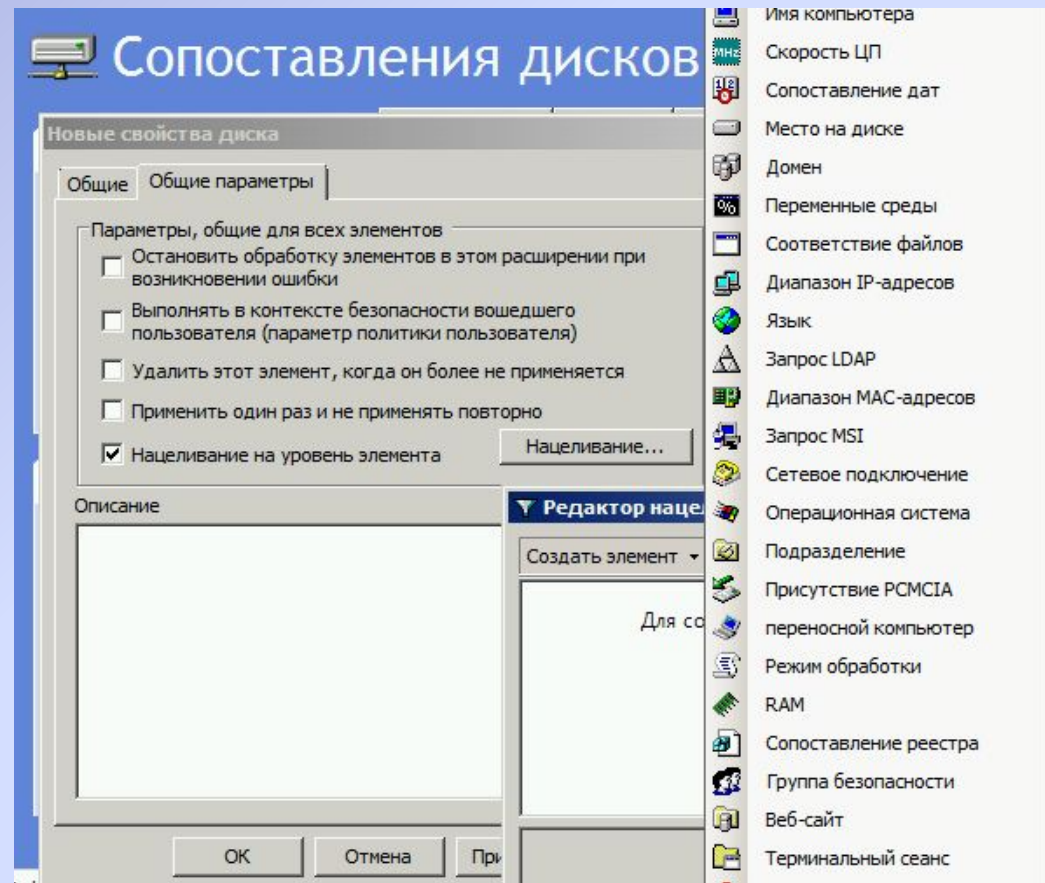
- Не блокируют настройки от изменения пользователем
- Позволяют настраивать параметры операционной системы и ПО
- иначе управляемые загрузочными скриптами (создавать ярлыки,
- подключать сетевые диски и т.д.

Способы применения предпочтений групповой политики:

- Create: Создать новый объект на целевом компьютере
- Delete: Удалить существующий объект с целевого компьютера
- Replace: Удалить и создать заново объект на целевом компьютере
- Update: Модифицировать объект на целевом компьютере

# Нацеливание предпочтений групповой политики

- Нацеливание на уровень элемента
  - В одном GPO может быть несколько настроек для разных пользователей и компьютеров
  - Доступно только для предпочтений
- Множество готовых WMI фильтров



# Loopback policy processing

- При входе пользователя в систему применяются пользовательские параметры GPO нацеленные на компьютер
  - Позволяет обеспечить единообразную среду на компьютере, независимо от вошедшего в систему пользователя.
  - Подходит для переговорных, публичных компьютеров, VDI, RDS, и т.д.
- Конфигурация компьютера\Политики\Административные шаблоны\Система\Групповая политика
  - Режим обработки замыкания пользовательской групповой политики
- Режим замещения
  - Применяются только пользовательские настройки нацеленные на компьютер
- Режим слияния
  - Сначала применяются пользовательские настройки нацеленные на пользователя, затем настройки нацеленные на компьютер.

# Обработка групповых политик при медленном соединении

- Клиент групповой политики определяет, находится ли контроллер домена, предоставляющий GPO за медленным соединением
  - По умолчанию медленным считается соединение менее 500 kbps
- Каждый CSE использует определение медленного соединения
  - По умолчанию при медленном соединении не производится установка ПО
- Можно изменить поведение каждого CSE при обнаружении медленного соединения
  - Computer Configuration\Policies\Administrative Templates\System\Group Policy
- Можно изменить пороговое значение медленного соединения
  - Computer [or User] Configuration\Policies\Administrative Templates\System\Group Policy

# Подводя итог

- Групповые политики АД – мощный инструмент управления конфигурацией компьютера
- Применение требует тщательного проектирования и контроля

# Шифрованная файловая система (EFS)

Горячев Александр Вадимович  
Доцент кафедры  
Информационной безопасности  
[avgoriachev@etu.ru](mailto:avgoriachev@etu.ru)

# Модель эшелонированной обороны

Физический  
доступ

Политики, процедуры,  
осведомленность

Хранение

ACL EFS Bitlocker

Backup Mirror RAID SC

Обработка

APPs Antivirus Updates

OS/.NET Antispyware Autentification HIDS-HIPS

PKI

AD

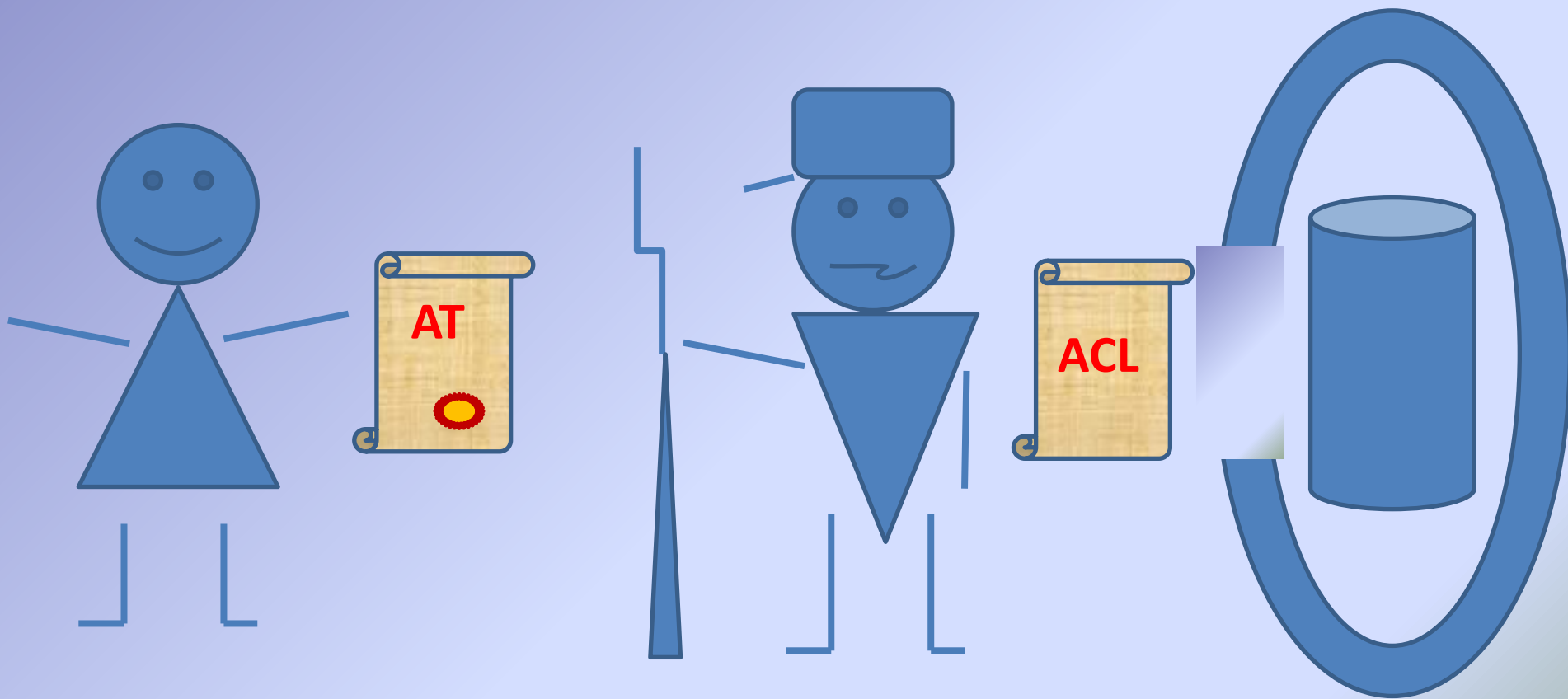
Передача

Intranet Routing IPsec RMS NIDS-NIPS

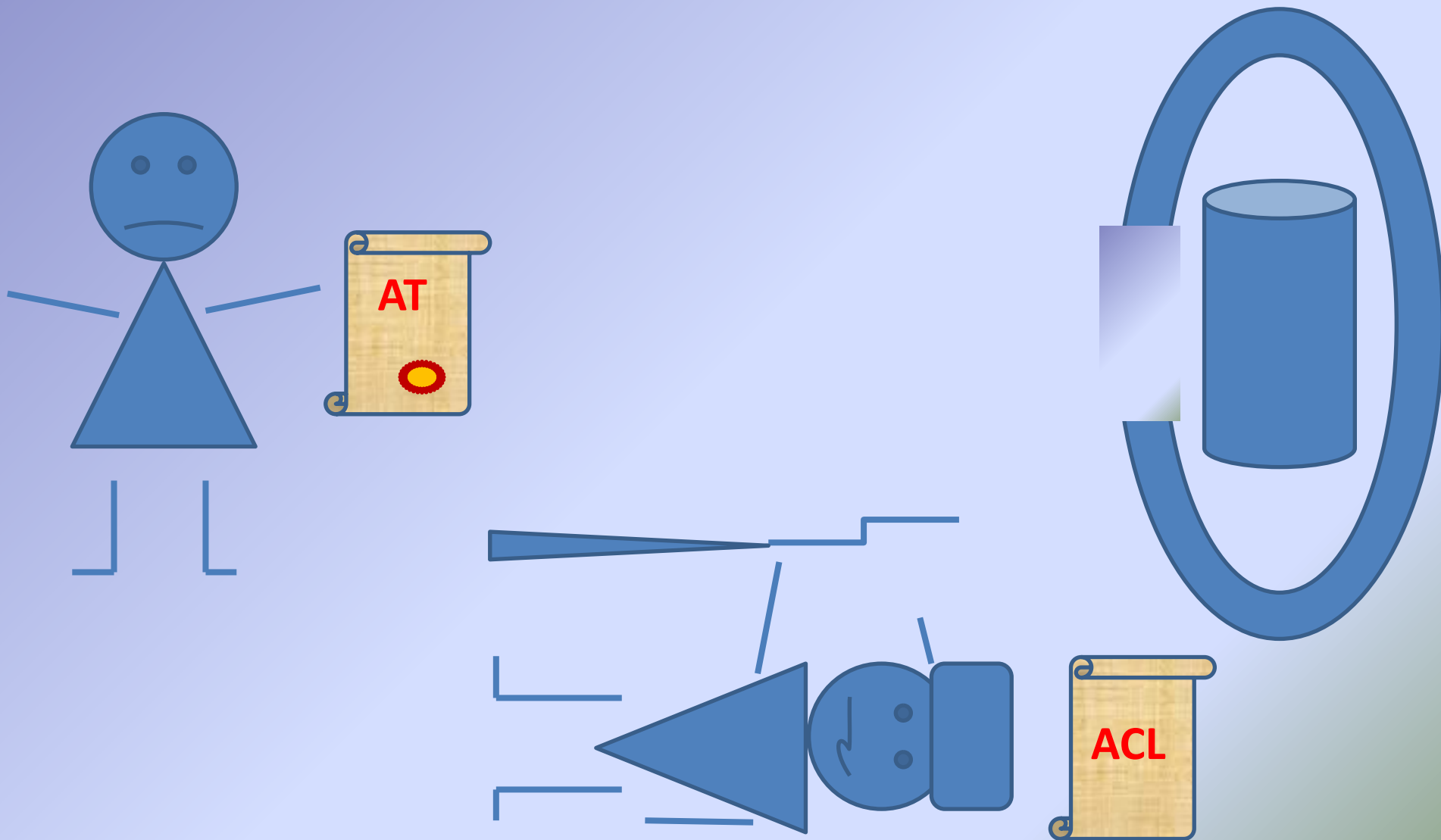
Internet Firewall VPN NAP



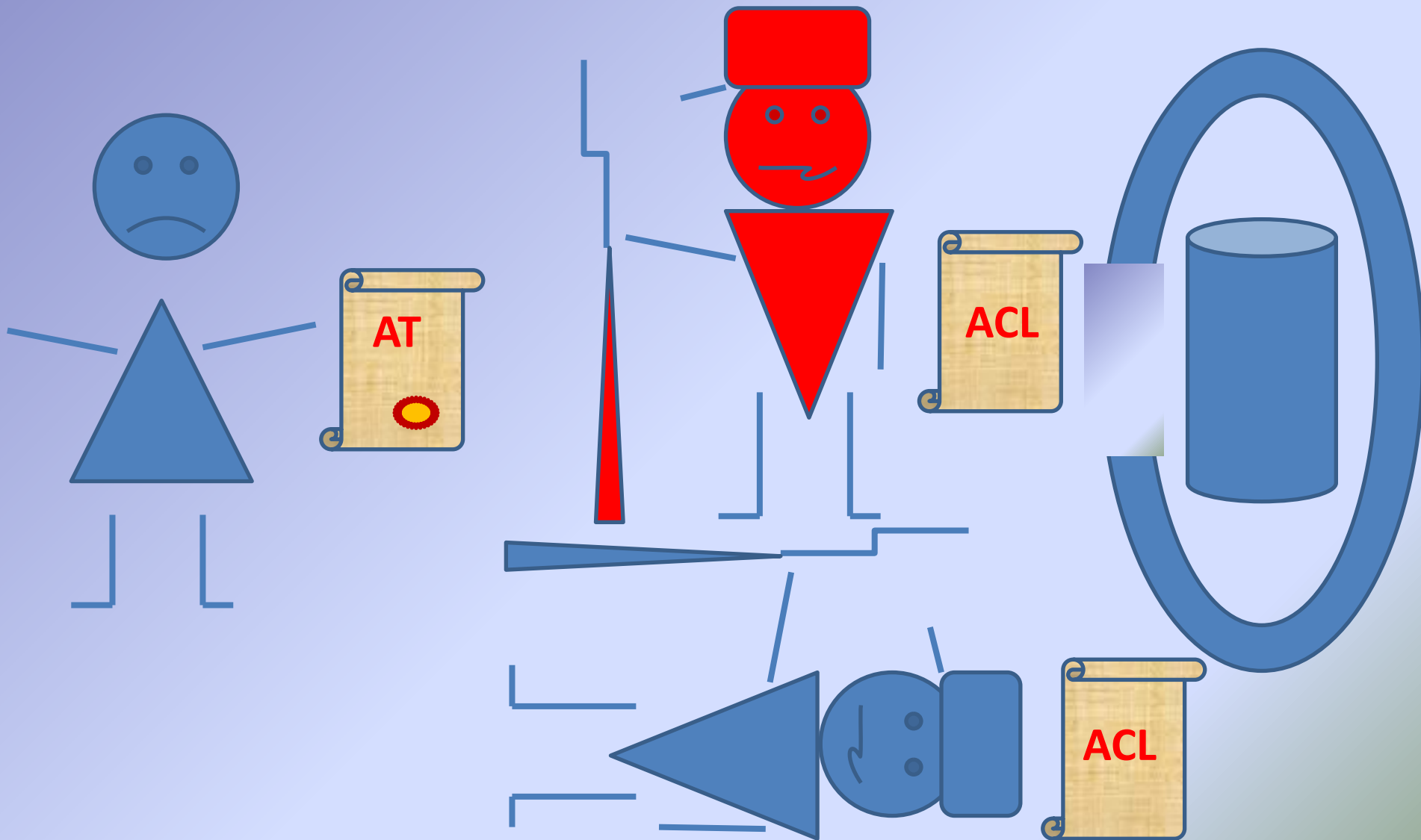
# Список контроля доступа



# Список контроля доступа



# Список контроля доступа

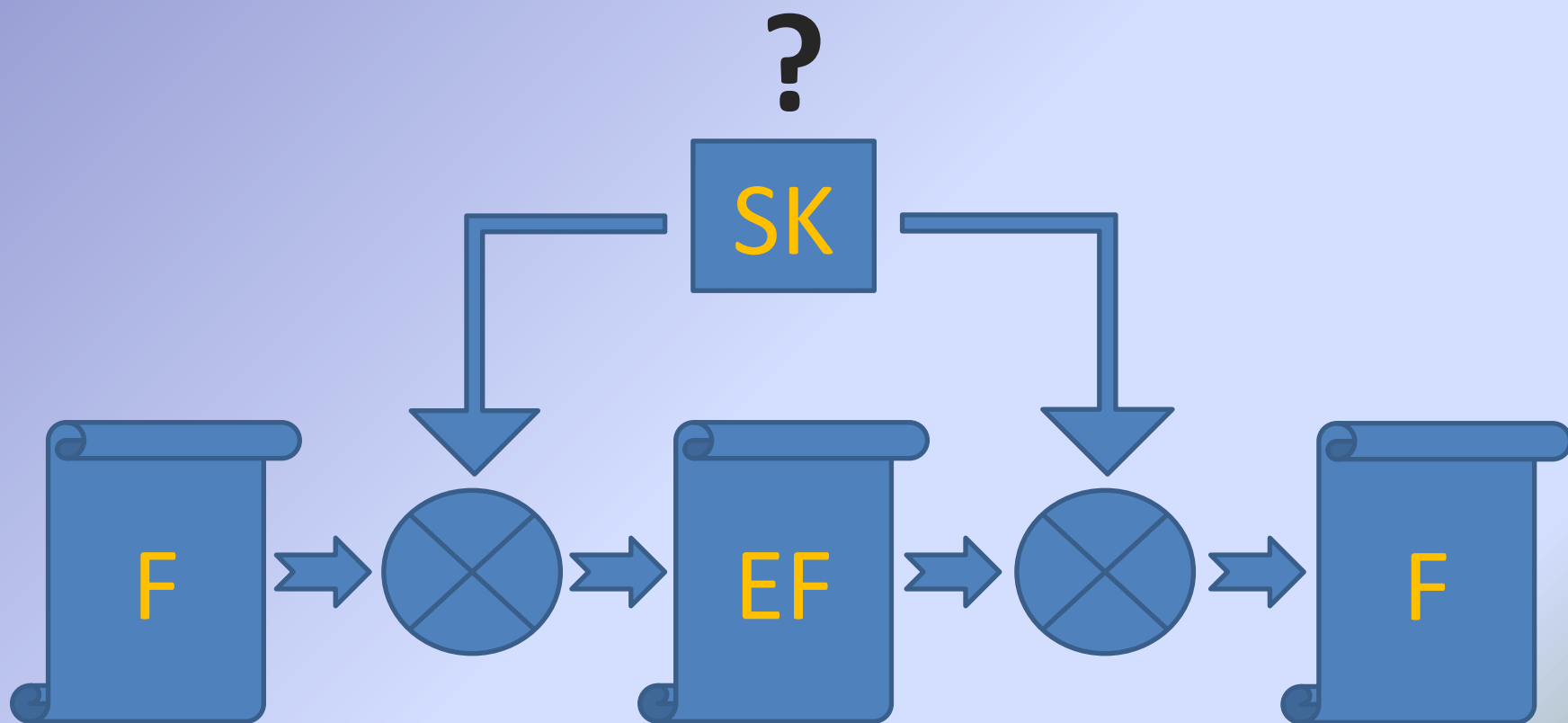


# Шифрование с симметричным ключом

$$T(a, x) = e$$

$$T^{-1}(e, x) = a$$

# Простейший вариант



# Шифрование с асимметричным ключом (открытым и закрытым ключами)

$$G \rightarrow (o, p)$$

$$T(a, o) = e$$

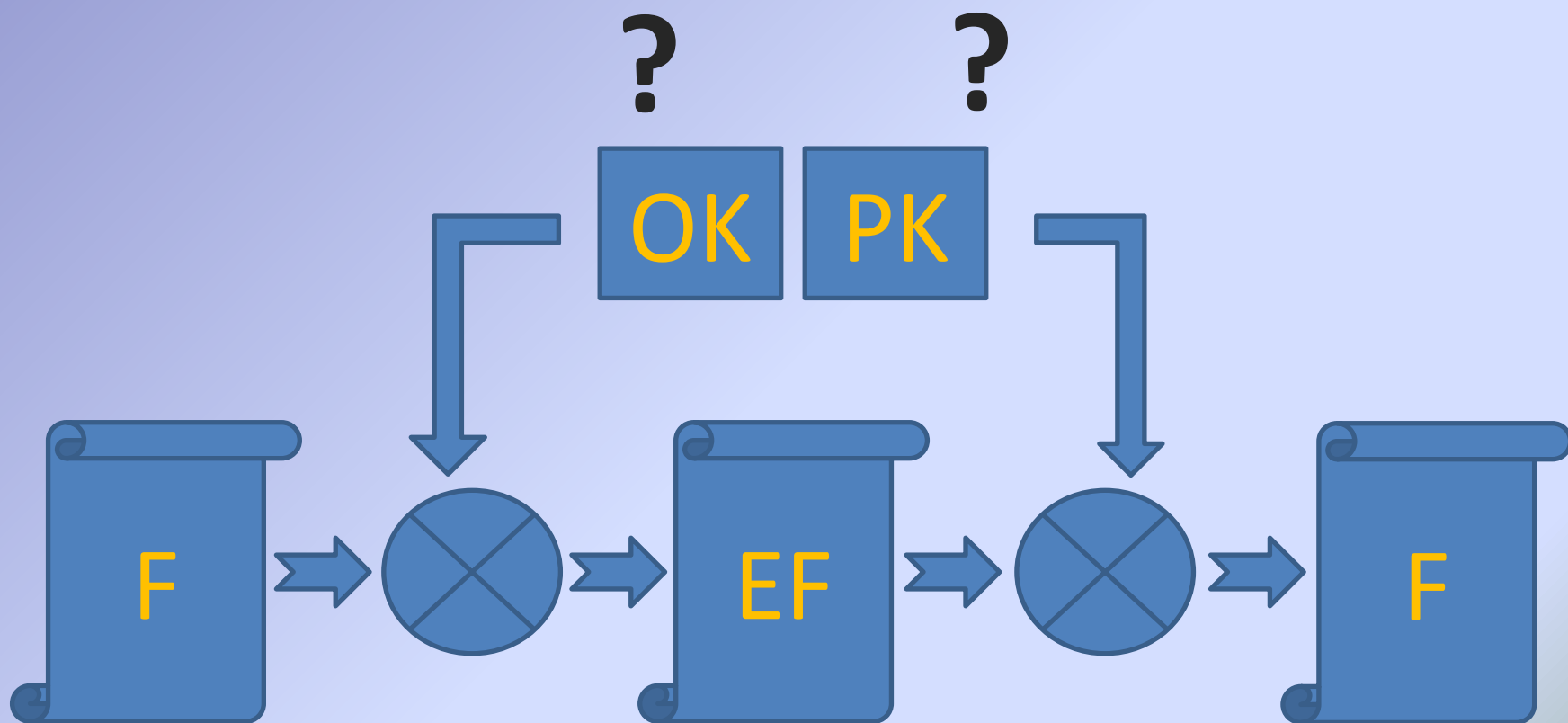
$$T^{-1}(e, p) = a$$

$$G \rightarrow (o, p)$$

$$T(a, p) = e$$

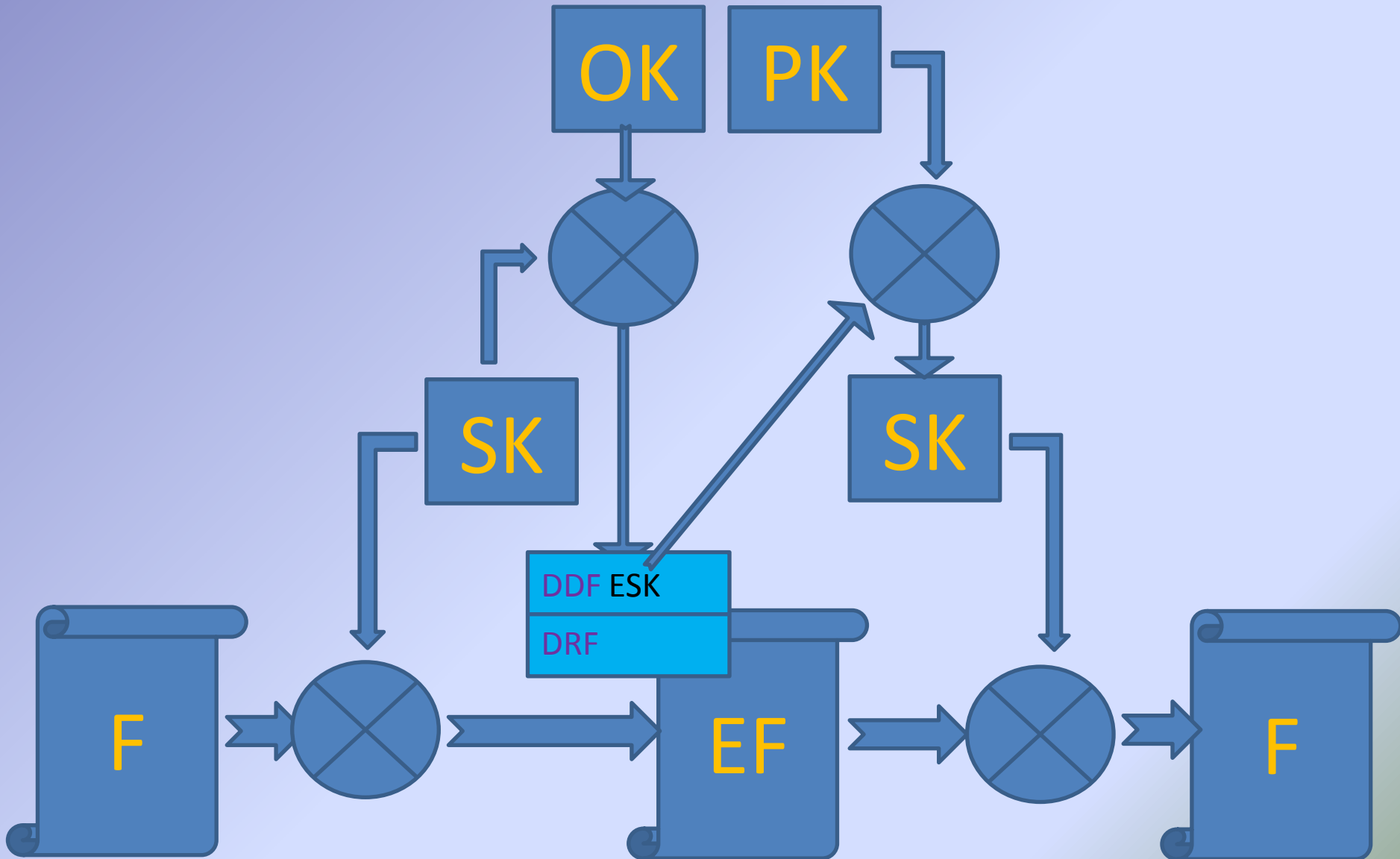
$$T^{-1}(e, o) = a$$

# А можно так?

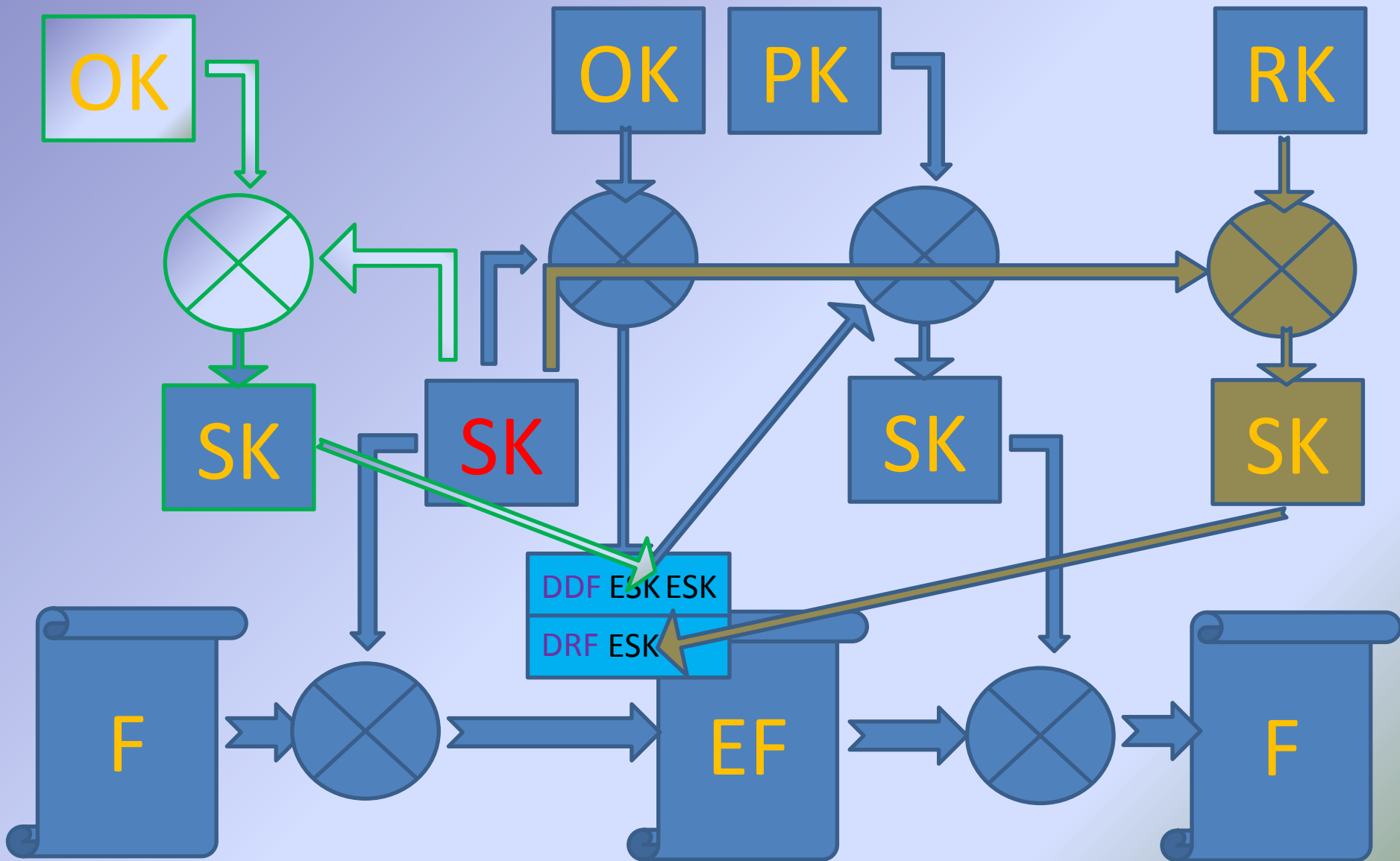




# Уже правильнее



# EFS



# Формирование сертификата

Заявка на

сертификат

О  
К

Кто?

Зачем  
?

?

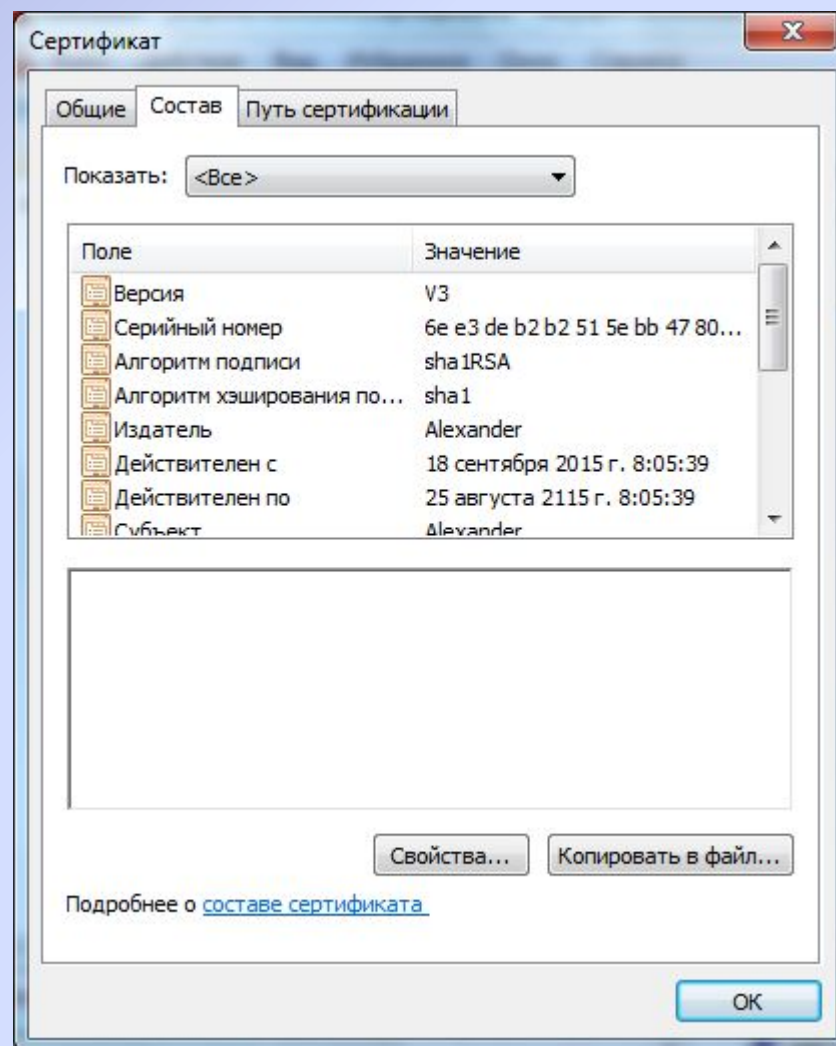
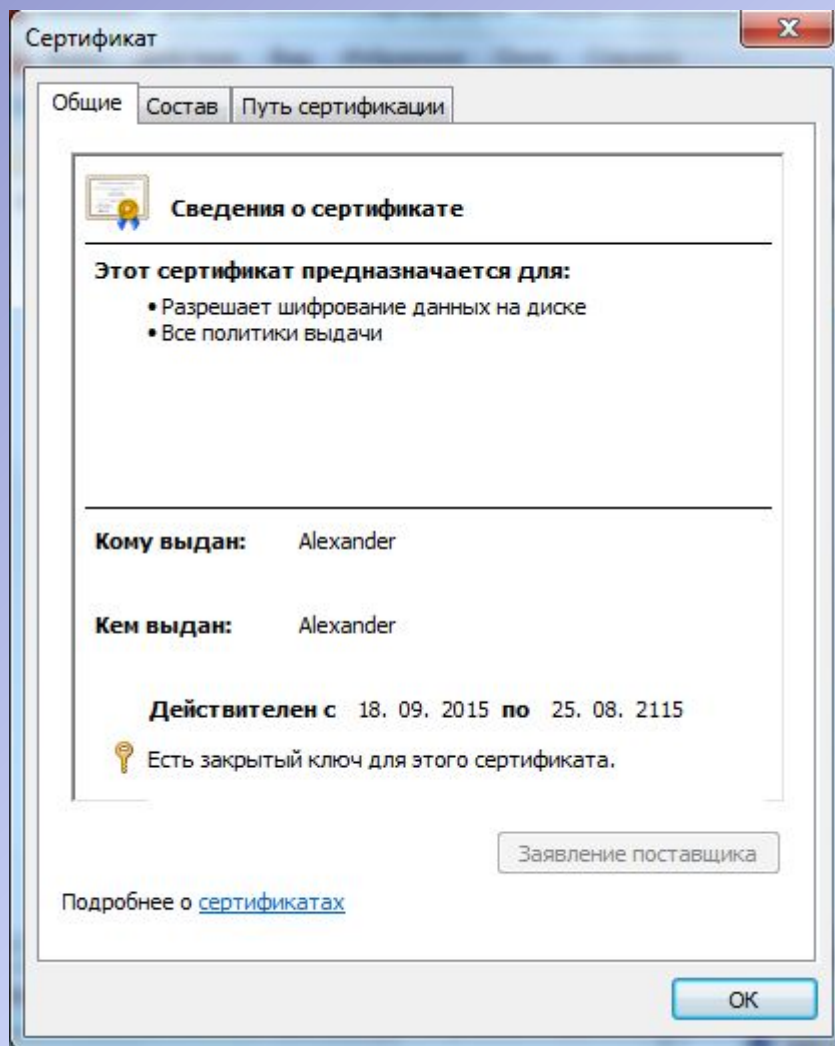
С  
А

Инф  
о

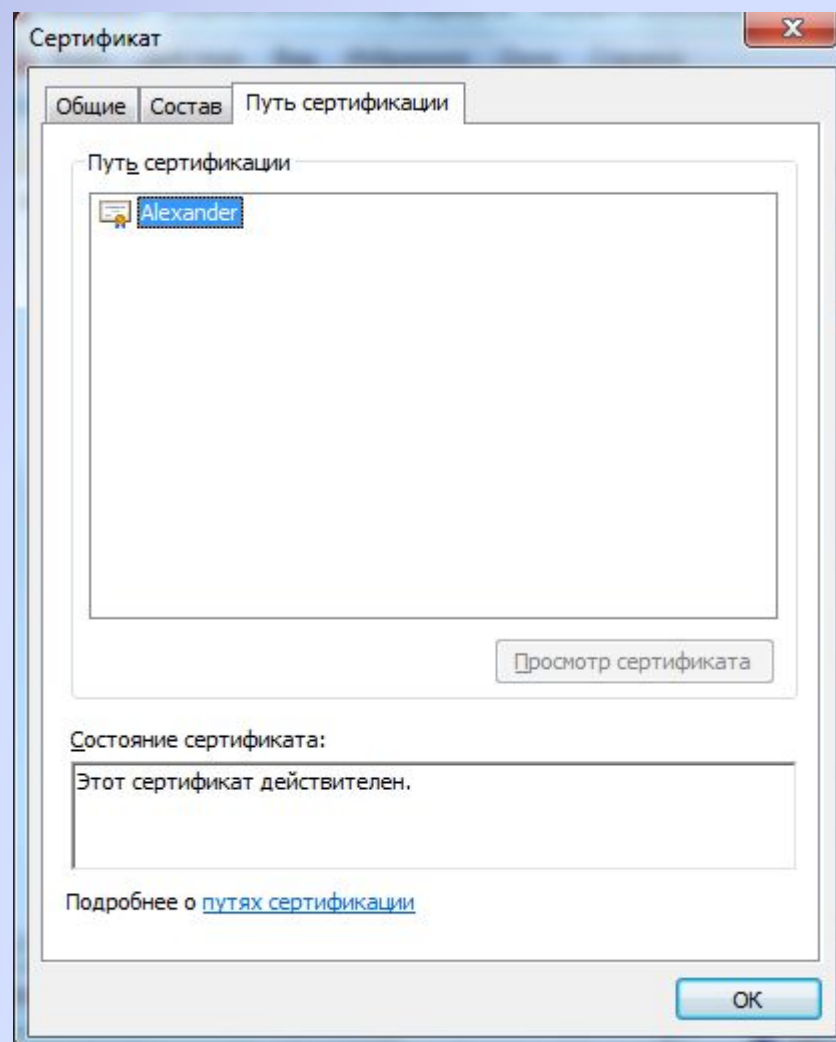
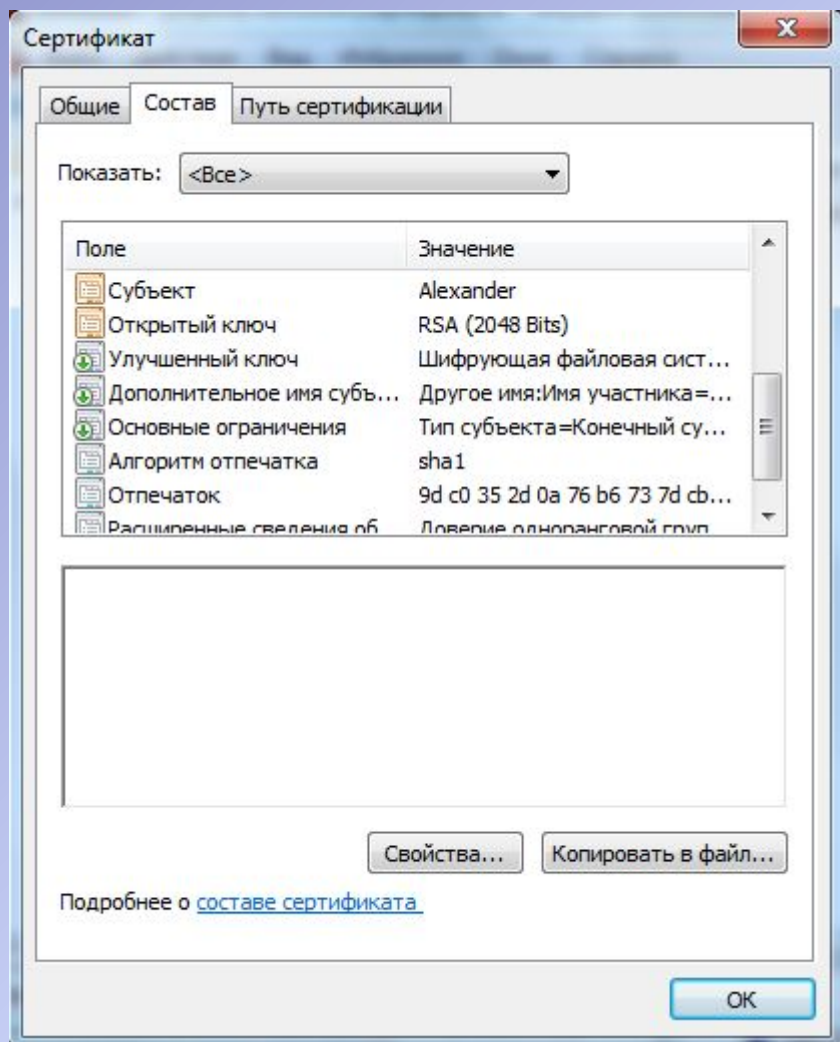
S

CA

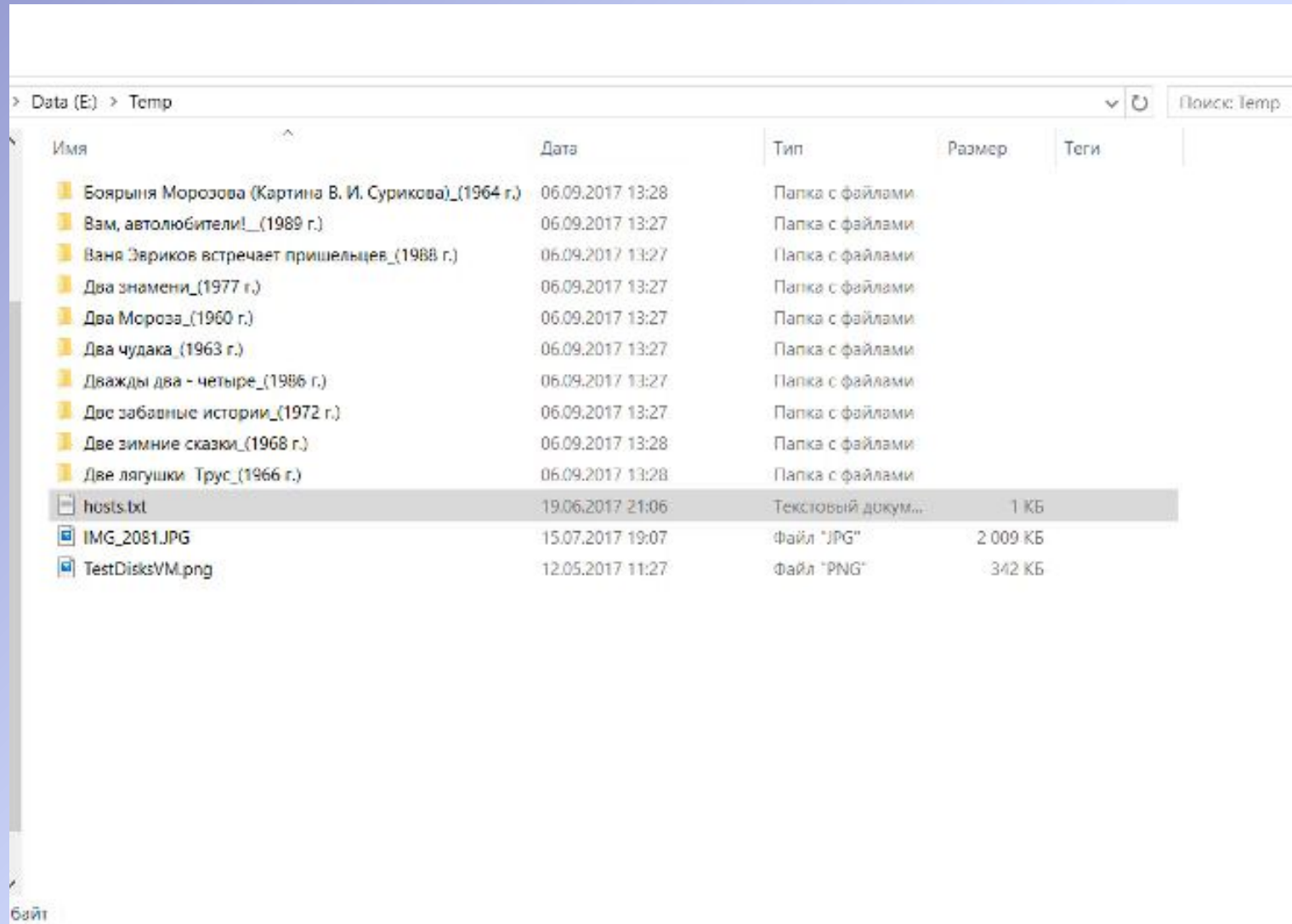
# Сертификат



# Сертификат



# Интерфейс управления EFS



**Взаимодействие внутри  
корпоративной сети.  
IPsecurity. SSL.**



# Модель эшелонированной обороны

Политики, процедуры,  
осведомленность

Физический  
доступ

Хранение

ACL EFS Bitlocker

Backup Mirror RAID SC

Обработка

APPs Antivirus Updates

OS/.NET Antispyware Autentification HIDS-HIPS

PKI

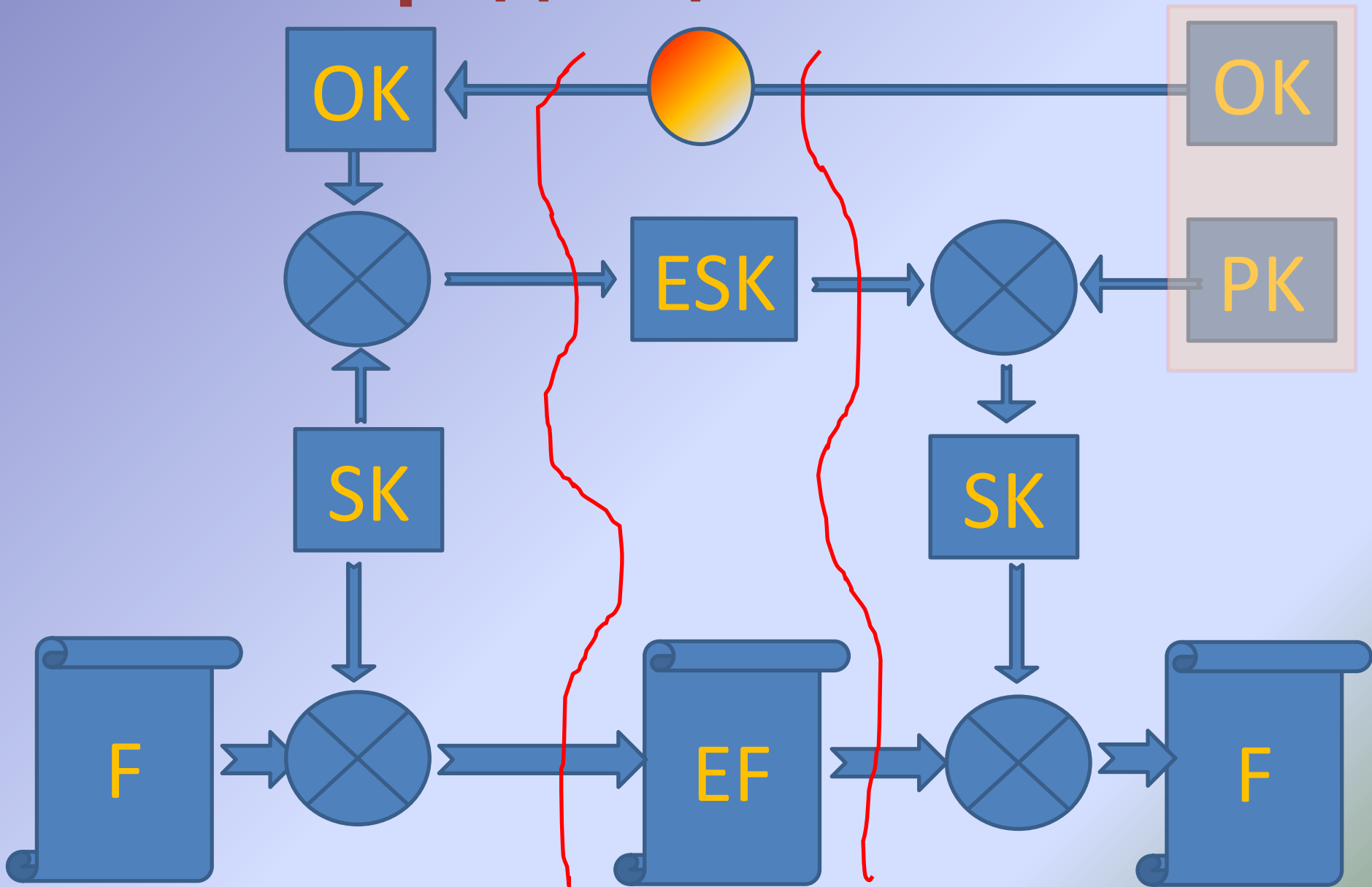
AD

Передача

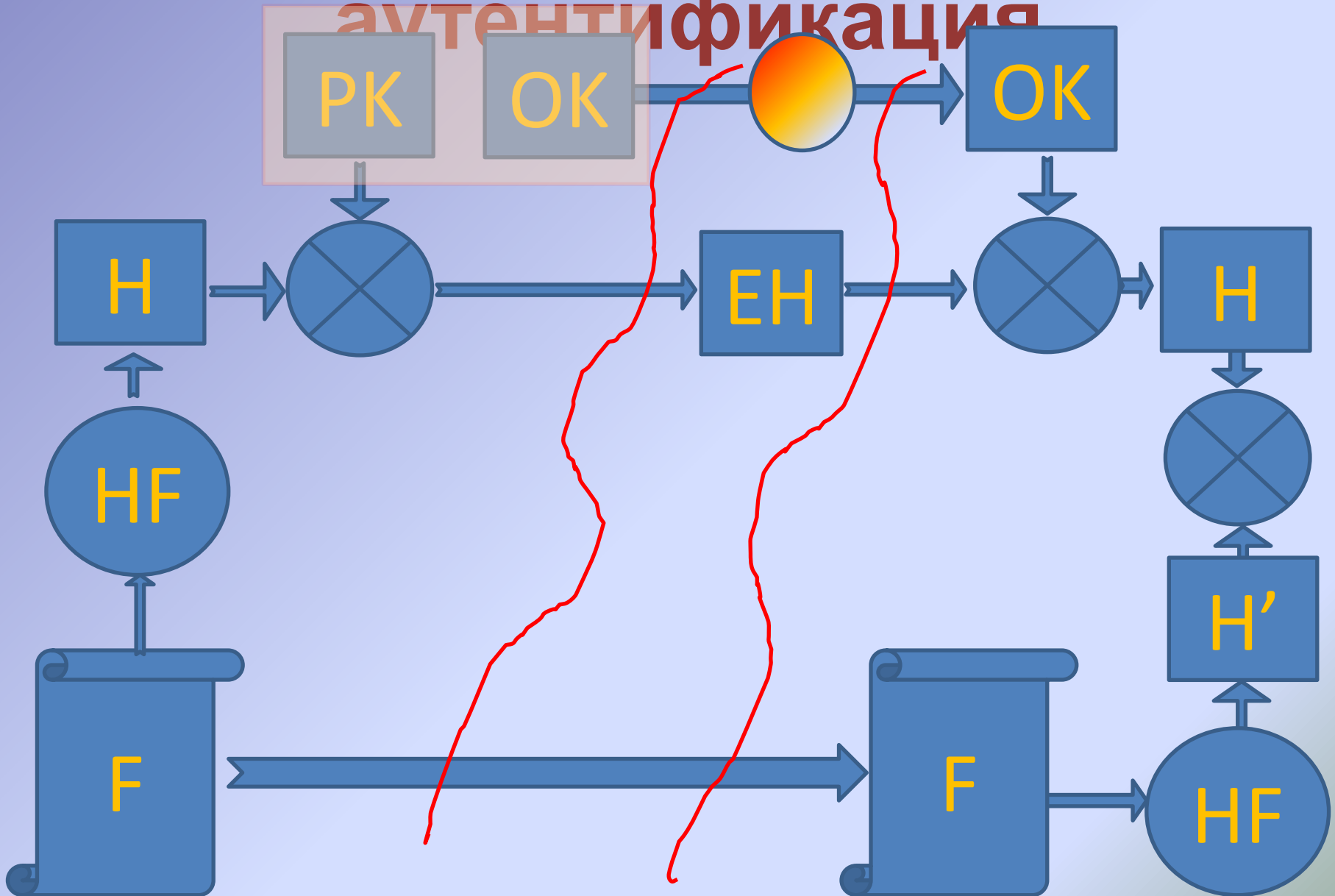
Intranet Routing IPsec SSL RMS NIDS-NIPS

Internet Firewall VPN NAP

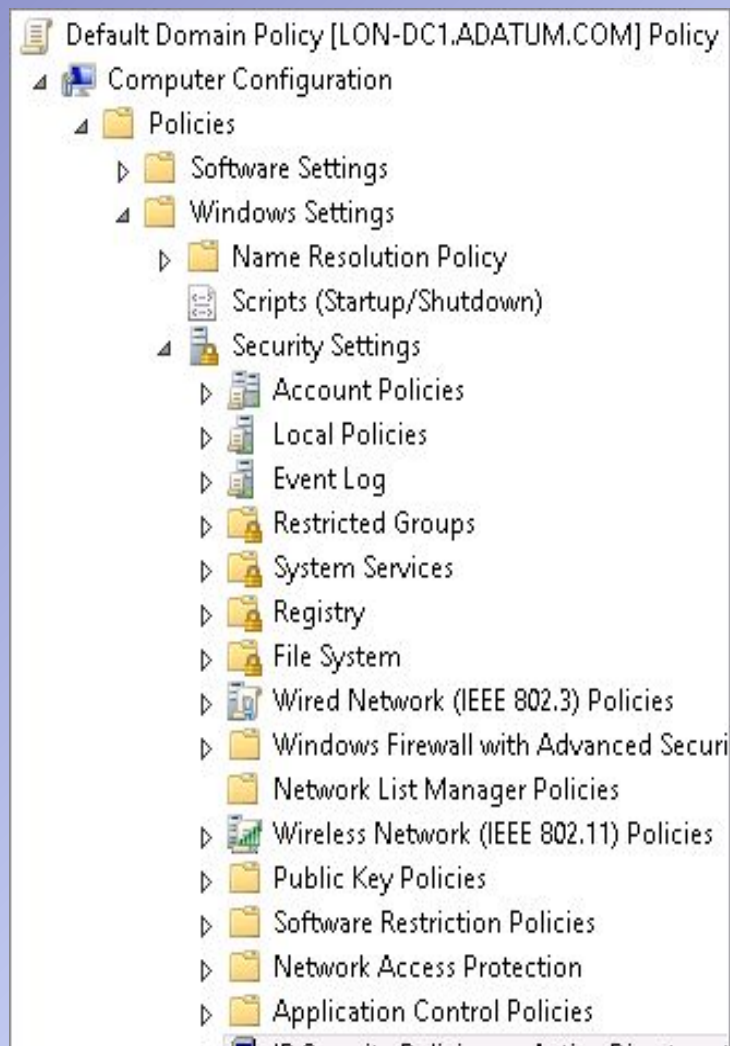
# Конфиденциальность



# Целостность и аутентификация

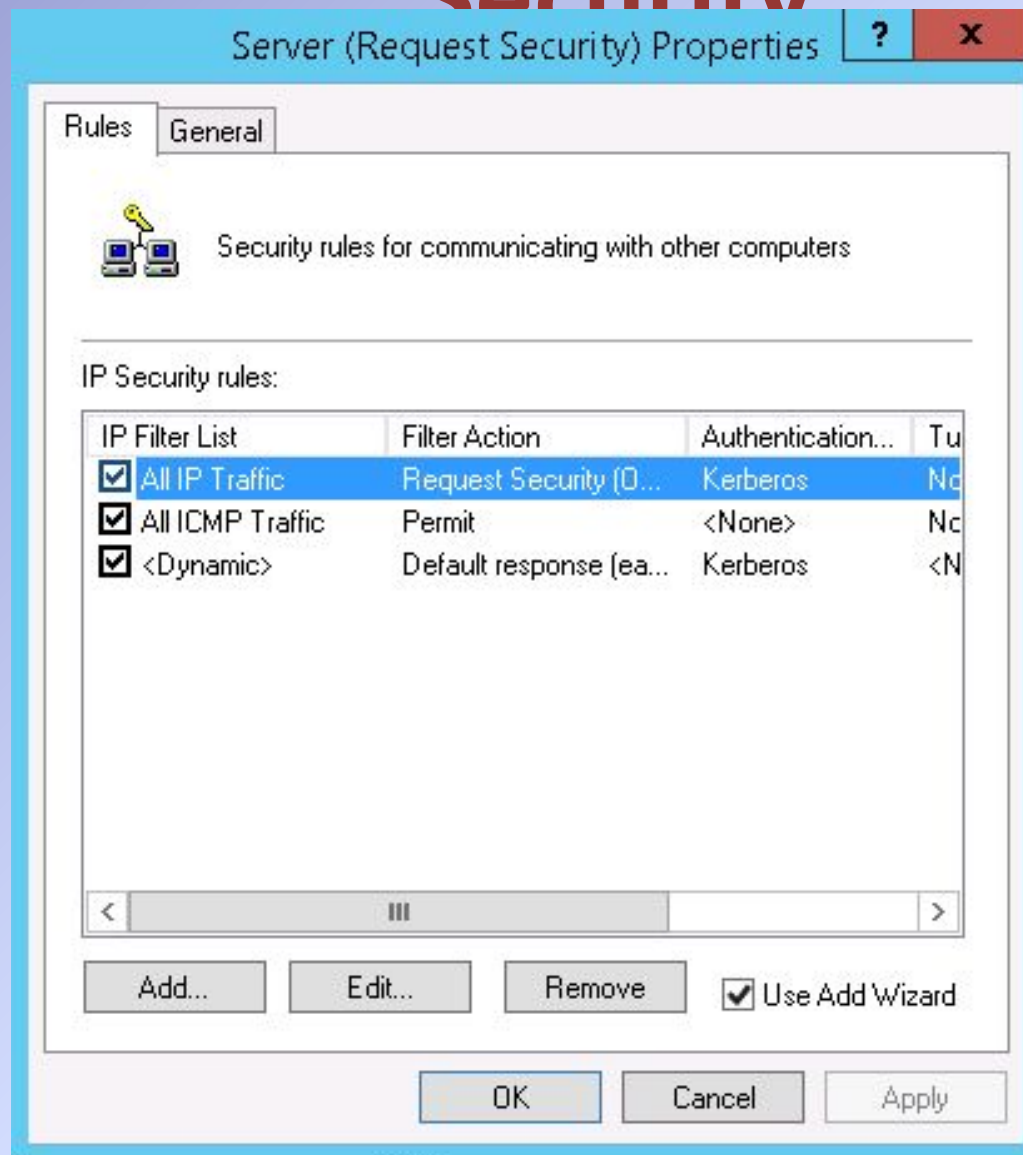


# Настройка IP Security



Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (unsecured). Use t...	No
Secure Server (Require Security)	For all IP traffic, always require security usin...	No
Server (Request Security)	For all IP traffic, always request security usi...	No


# Настройка политики IP Security



# Настройка правил IP Security

Edit Rule Properties

IP Filter List		Filter Action
Authentication Methods	Tunnel Setting	Connection Type

 This rule only applies to network traffic over connections of the selected type.

---

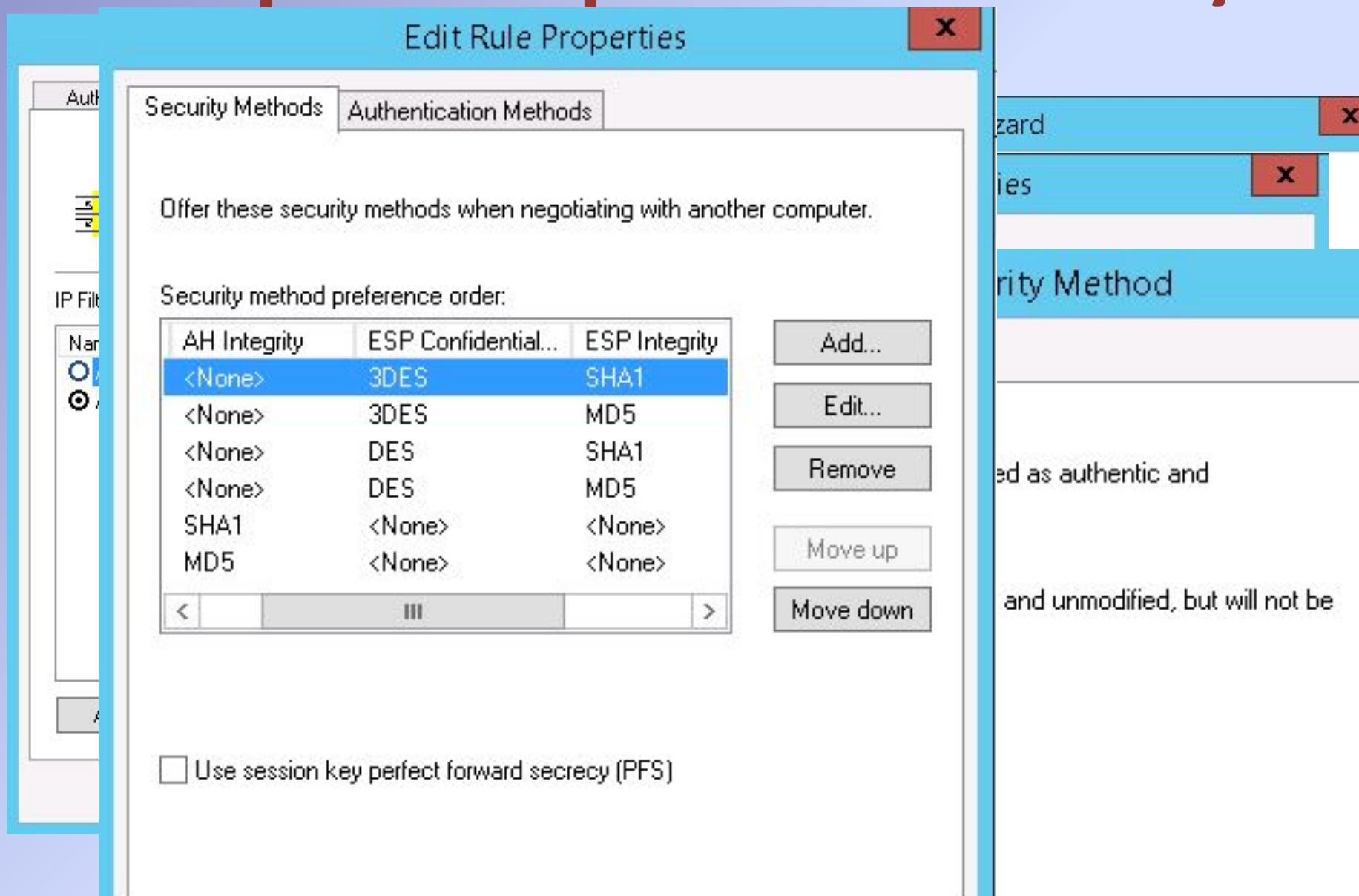
☒ All network connections

☐ Local area network (LAN)

☐ Remote access

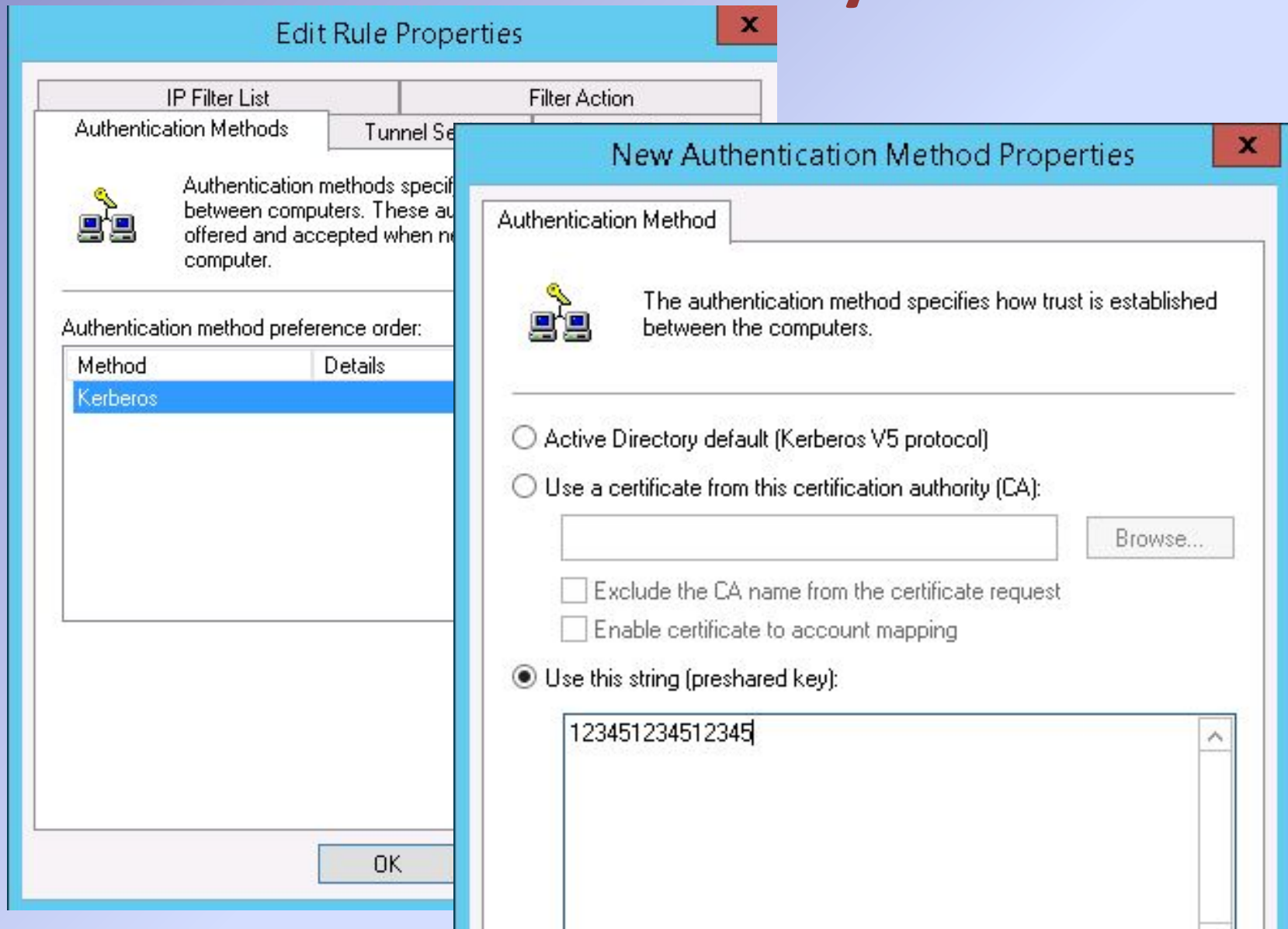
OK Cancel Apply

# Настройка правил IP Security





# Настройка аутентификации IP Security



# Мониторинг IPSecurity

Консоль1 - [Корень консоли\Монитор IP-безопасности\GAV-WORKPLACE\Быстрый режим: \Статистика]

Файл Действие Вид Избранное Окно Справка

Корень консоли

- Монитор IP-безопасности
  - GAV-WORKPLACE
    - Активная политика
      - Основной режим
        - Универсальные фильтры
        - Специальные фильтры
        - Политики IKE
        - Статистика
        - Сопоставления безопасност...
      - Быстрый режим:
        - Универсальные фильтры
        - Специальные фильтры
        - Политики согласования
        - Статистика
        - Сопоставления безопасност...

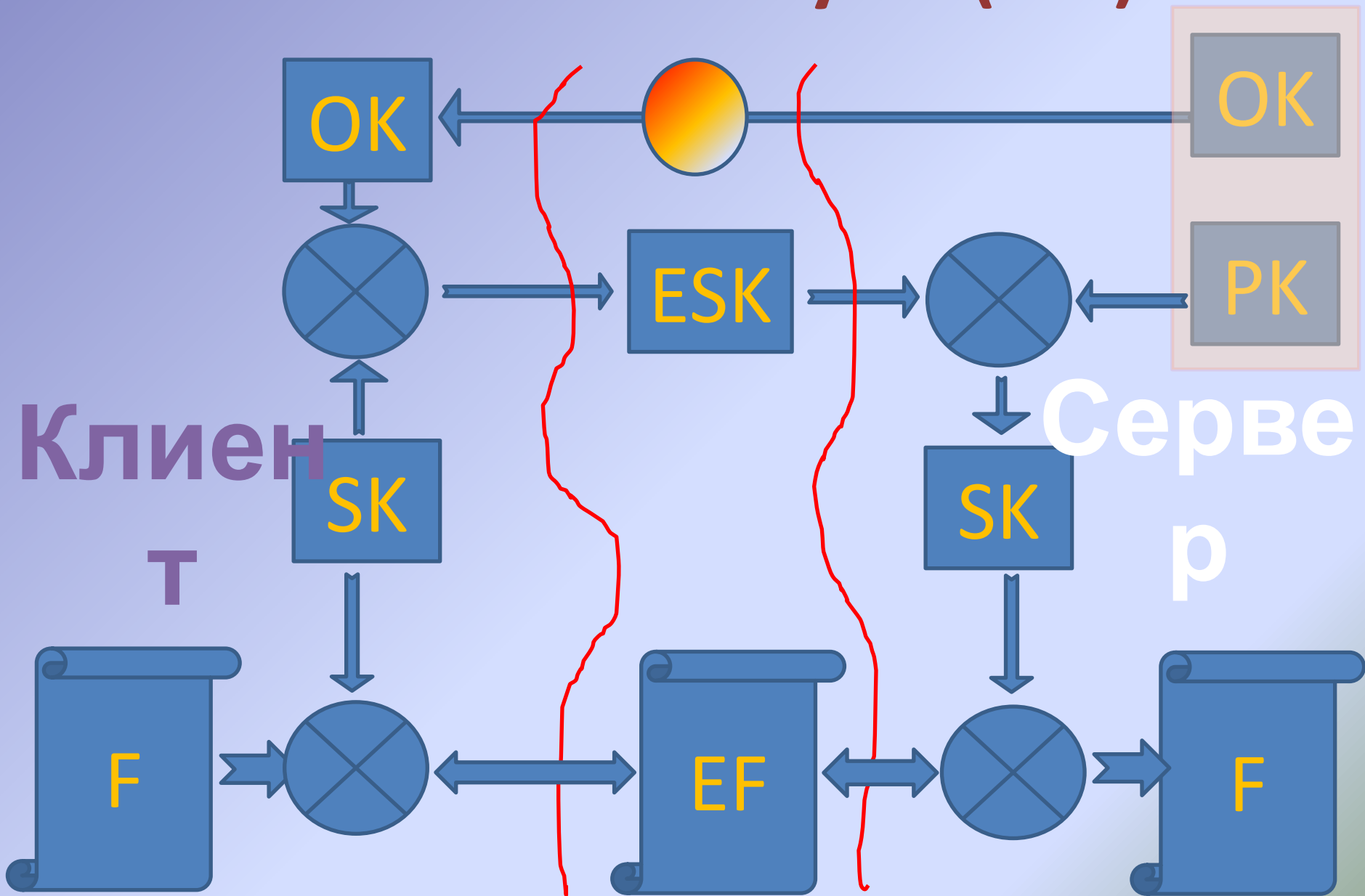
Параметры	Статистика
Активных сопоставлений безопаснос...	0
Разгруженные операции сопоставлен...	0
Не законченные операции с ключами	0
Дополнения по ключам	0
Удалений ключей	0
Повторное создание ключей	0
Активных туннелей	0
Сбойных пакетов SPI	0
Незашифрованных пакетов	0
Непроверенных пакетов	0
Пакеты с определением ответа	0
Послано байт (секретных)	0
Получено байт (секретных)	0
Послано байт (проверенных)	0
Получено байт (проверенных)	0
Транспортных байтов отправлено	0
Получено транспортных байтов	0
Отправлено в туннель, байт	0
Получено из туннеля, байт	0
Отправлено разгруженных байтов	0
Получено разгруженных байтов	0

Действия

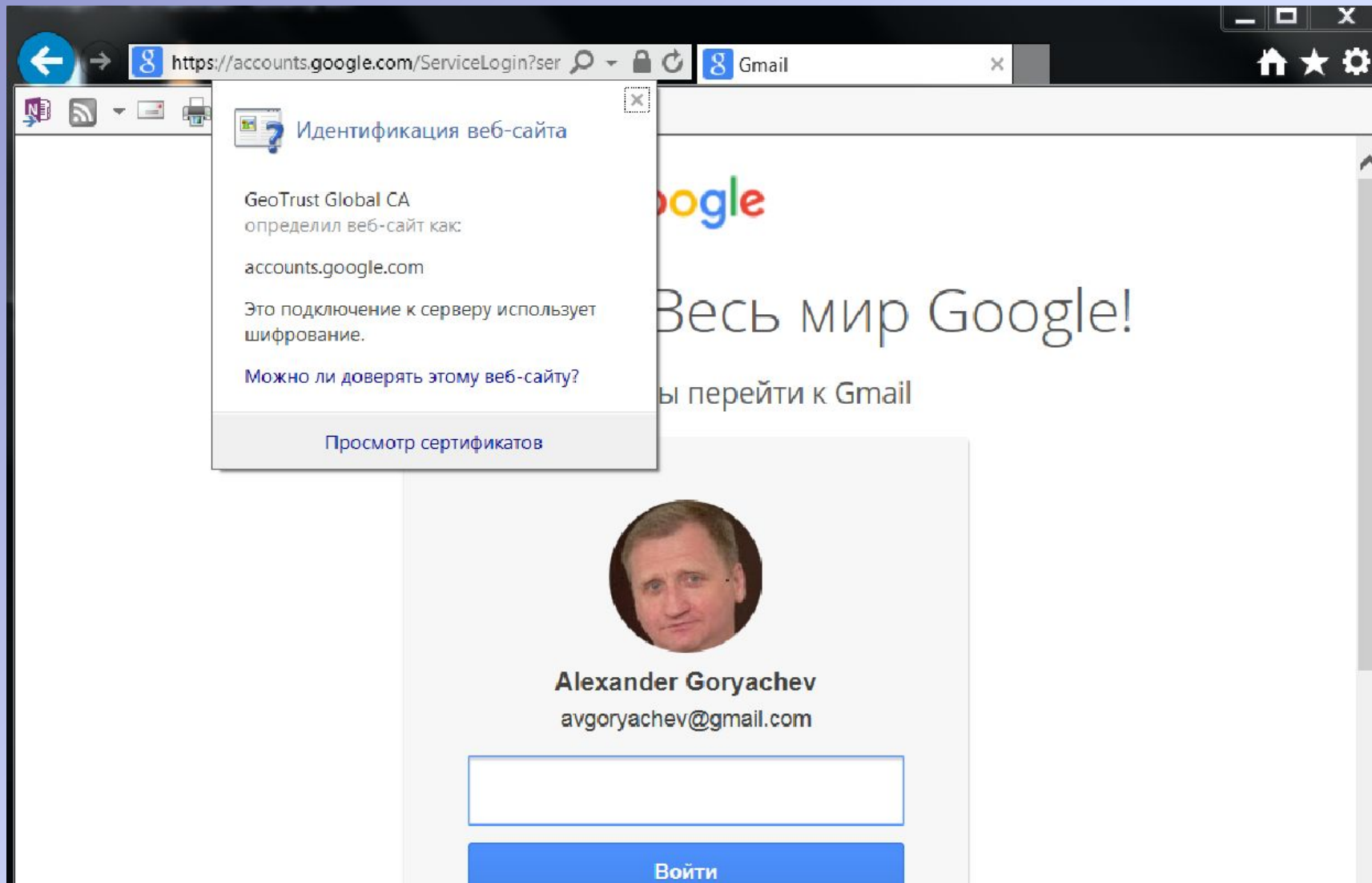
Статистика

Дополнительные дей...

# Secure Socket Layers (SSL)

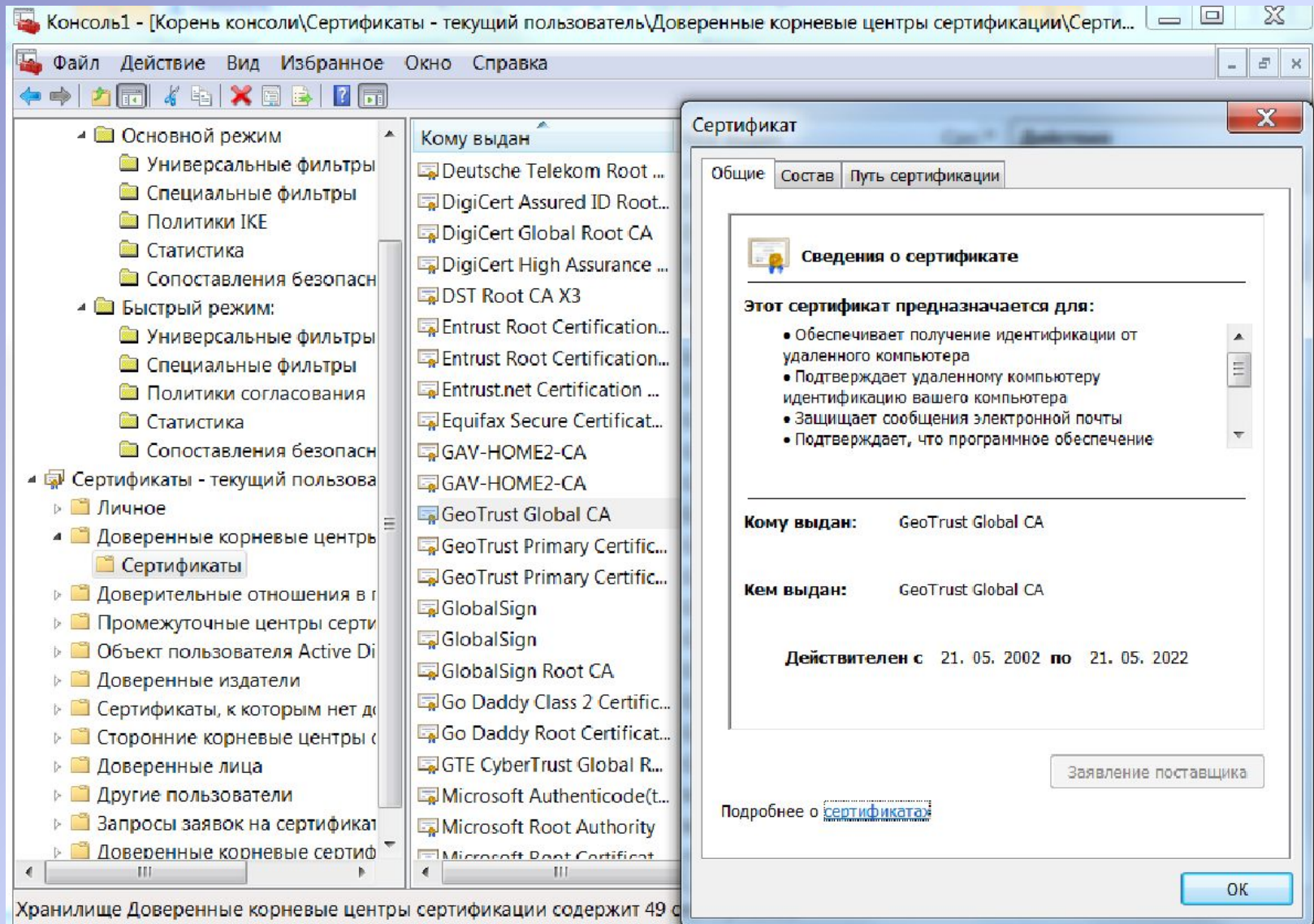


# Установка соединения SSL





# Сертификаты SSL



# Сертификаты SSL

Параметры



## Безопасность

- ☐ SSL 2.0
- ☒ SSL 3.0
- ☒ TLS 1.0
- ☐ Блокировать небезопасные рисунки и другой смешанный контент
- ☒ Включить внутреннюю поддержку XMLHTTP
- ☒ Включить защиту памяти для снижения риска интернет-атак
- ☐ Включить строгую проверку P3P\*
- ☒ Включить фильтр SmartScreen
- ☒ Включить хранилище DOM
- ☒ Использовать TLS 1.1
- ☒ Использовать TLS 1.2
- ☐ Не сохранять зашифрованные страницы на диск
- ☒ Отправлять на посещаемые через Internet Explorer веб-сайты

\* Изменения будут применены после перезапуска компьютера

Intended purpose:

<All>

Intermediate Certification A

Issued To

- AddTrust External ...
- Baltimore CyberTru...
- Class 2 Primary CA
- Class 3 Public Prima...
- Copyright (c) 1997 ...
- DigiCert Assured ID...
- DigiCert High Assur...
- Equifax Secure Cer...
- GAV-HOME2

Import...

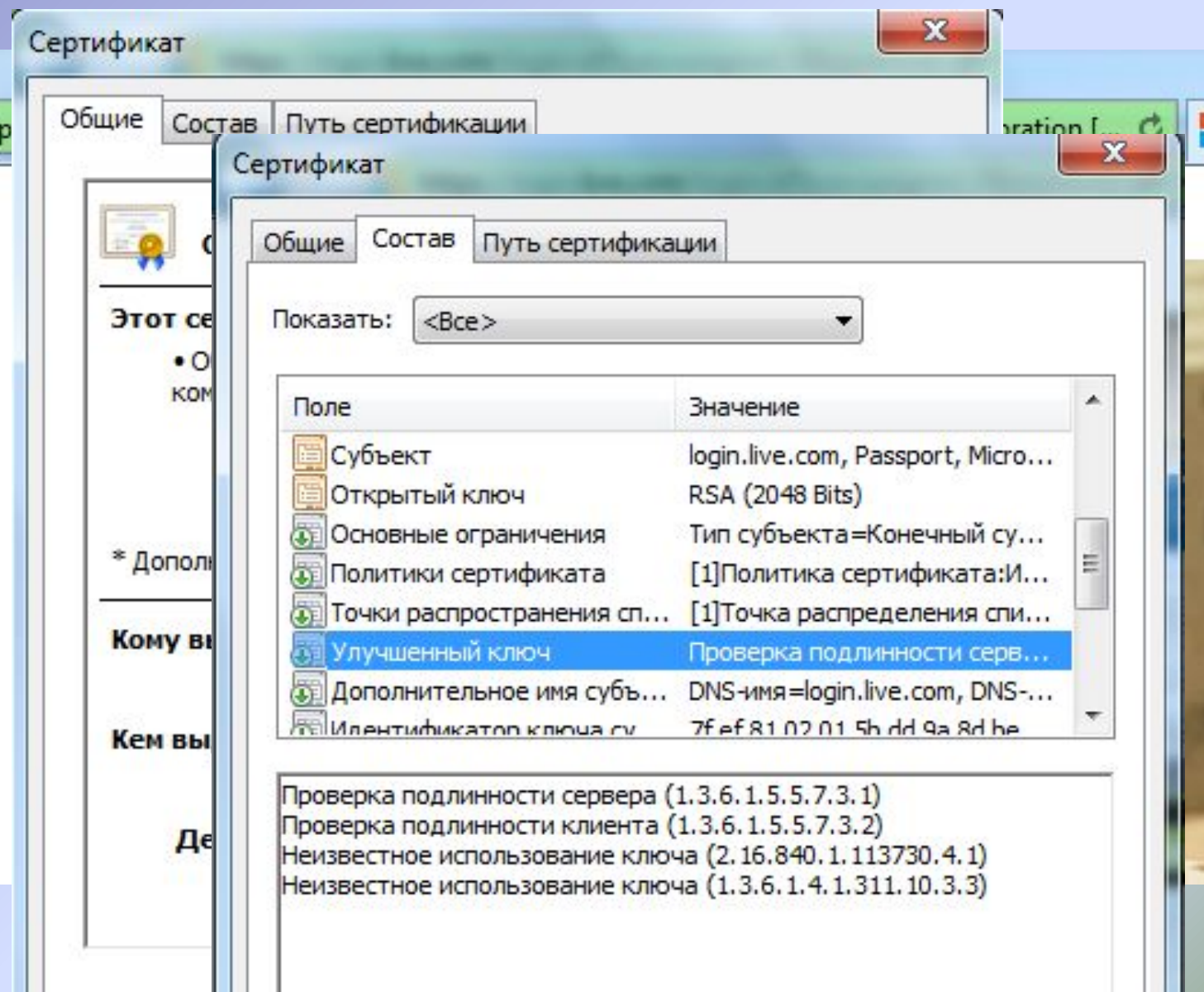
Export...

Remove

Advanced

Certificate intended purposes

# Работа с SSL





**VPN**

Горячев Александр Вадимович  
Доцент кафедры ИБ  
[avgoriachev@etu.ru](mailto:avgoriachev@etu.ru)

# Модель эшелонированной обороны

Политики, процедуры,  
осведомленность

Физический  
доступ

Хранилище

ACL EFS Bitlocker

Backup Mirror RAID SC

Обработка

APPs Antivirus Updates

OS/.NET Antispyware Autentification HIDS-HIPS

PKI

AD

Передача

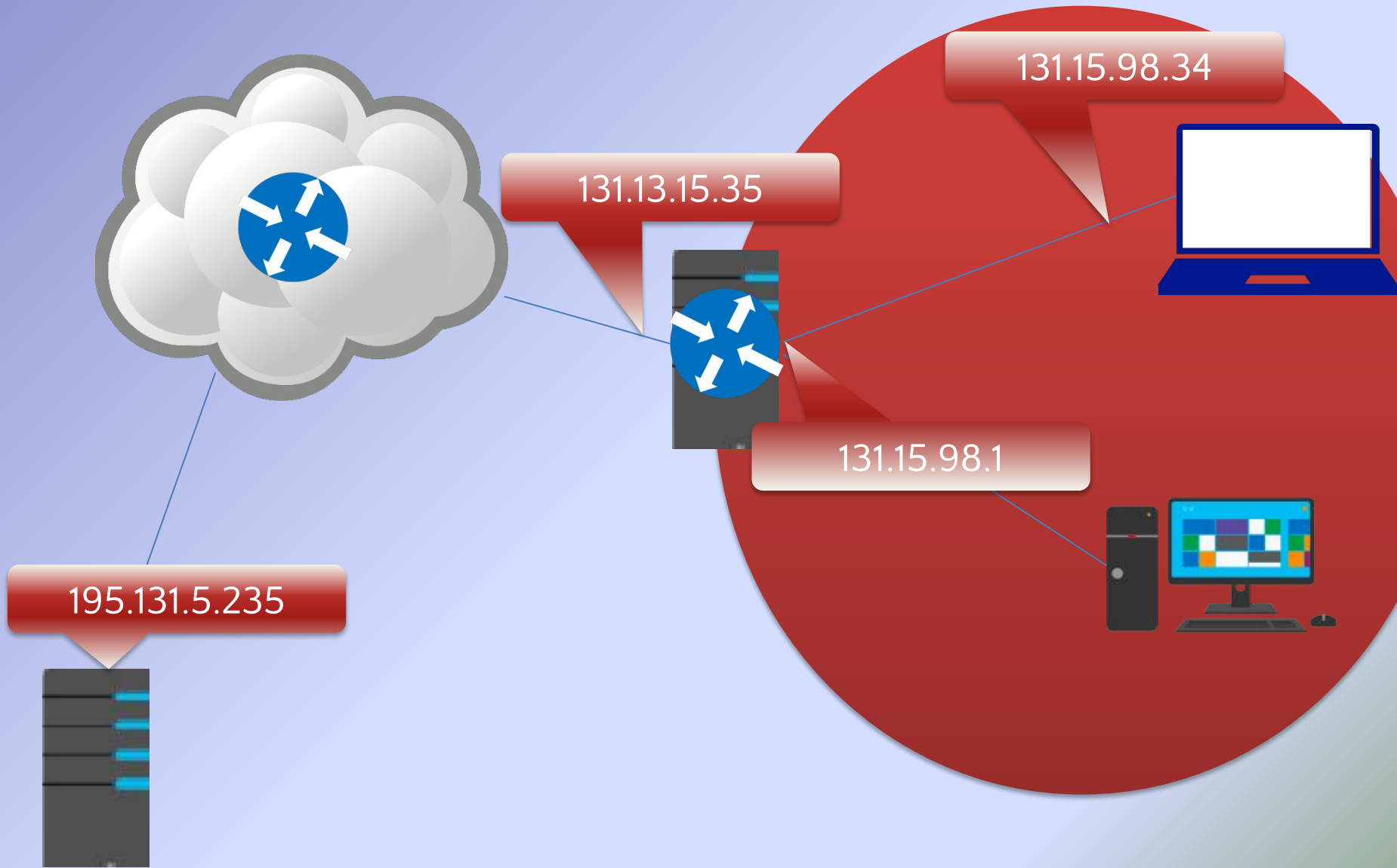
Intranet Routing IPsec SSL RMS NIDS-NIPS

Internet Firewall VPN NAP

# Технологии выхода в Интернет из корпоративной сети

- Маршрутизация
- Статическая трансляция адресов  
(публикация ресурсов)
- Динамическая трансляция адресов
- Прокси (Proxy)

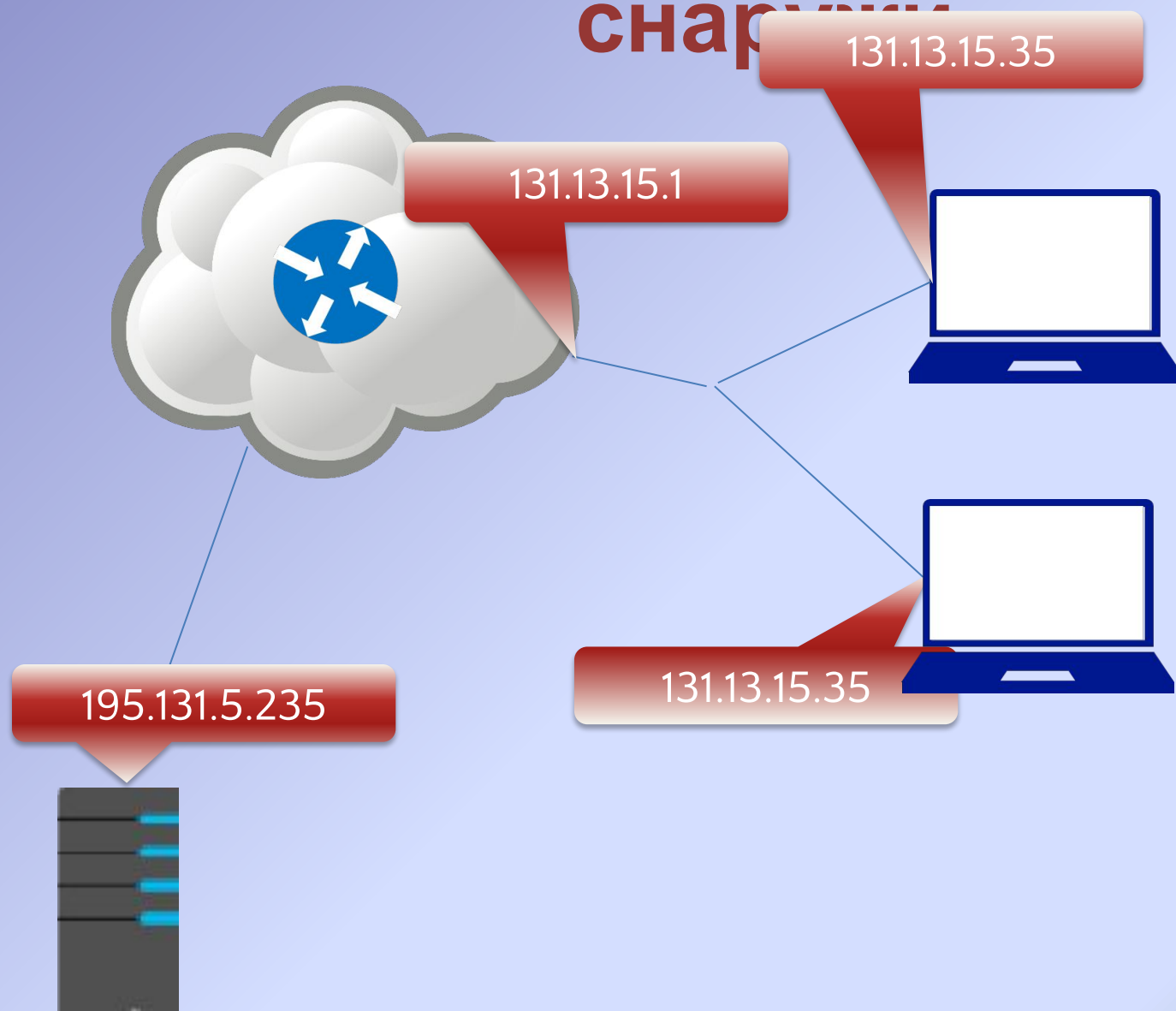
# Маршрутизация



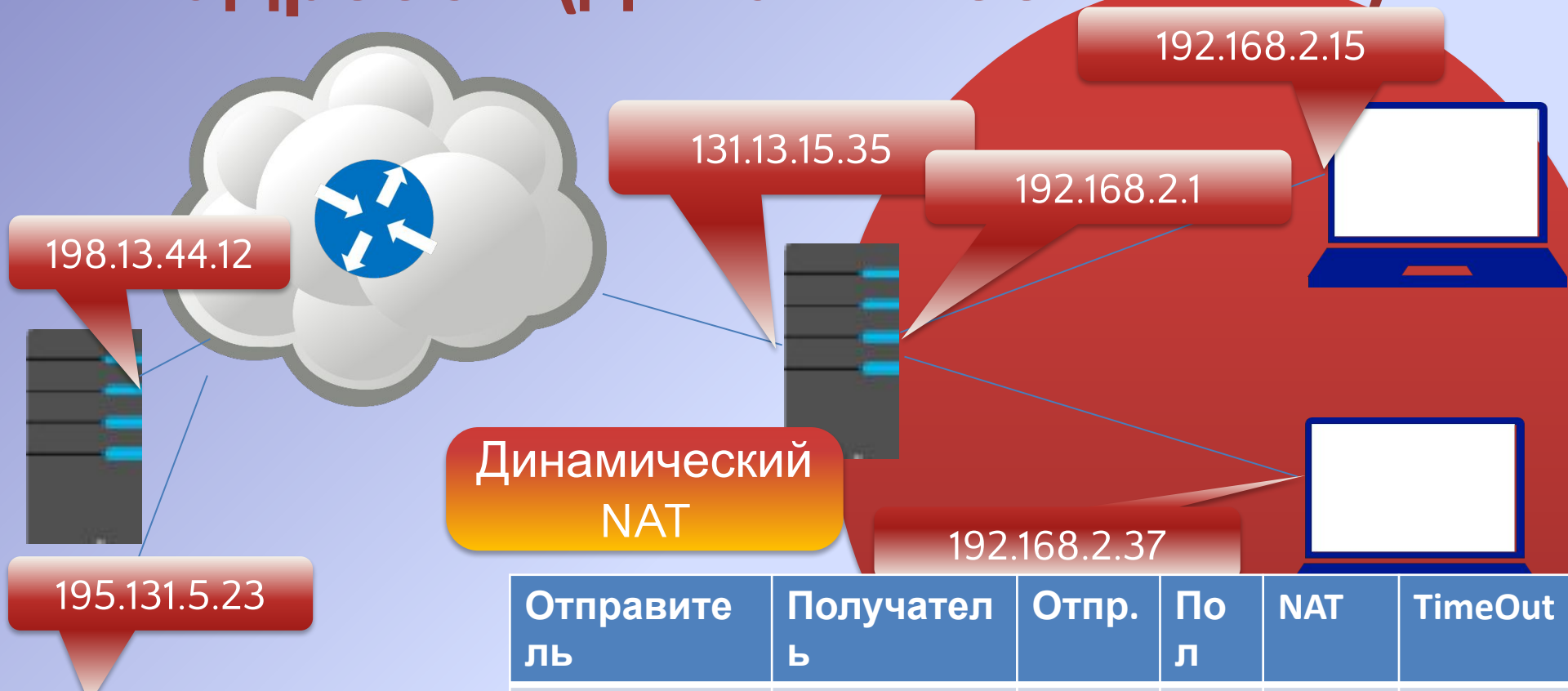
# Статическая трансляция адресов (статический NAT)



# Статический NAT – как выглядит схема



# Динамическая трансляция адресов (динамический NAT)



Отправитель	Получатель	Отпр.	Пол	NAT	TimeOut
198.13.44.12	131.13.15.35	12345	80	34555	
195.131.5.23	131.13.15.35	32256	80	34556	

Пакет прямой:

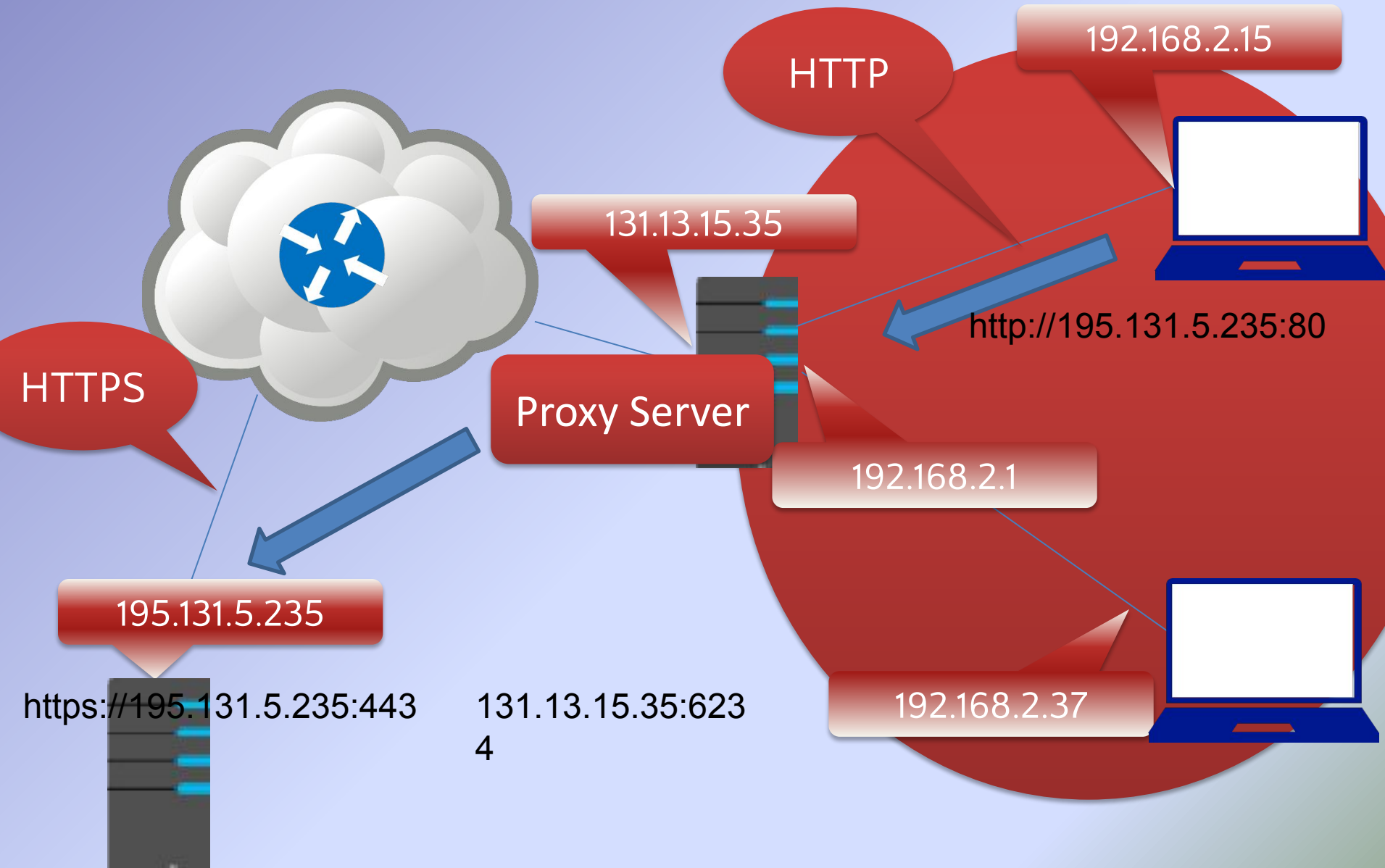
Пакет ответный:

Отправитель: 198.13.44.12:80

Получатель: 131.13.15.35:34555



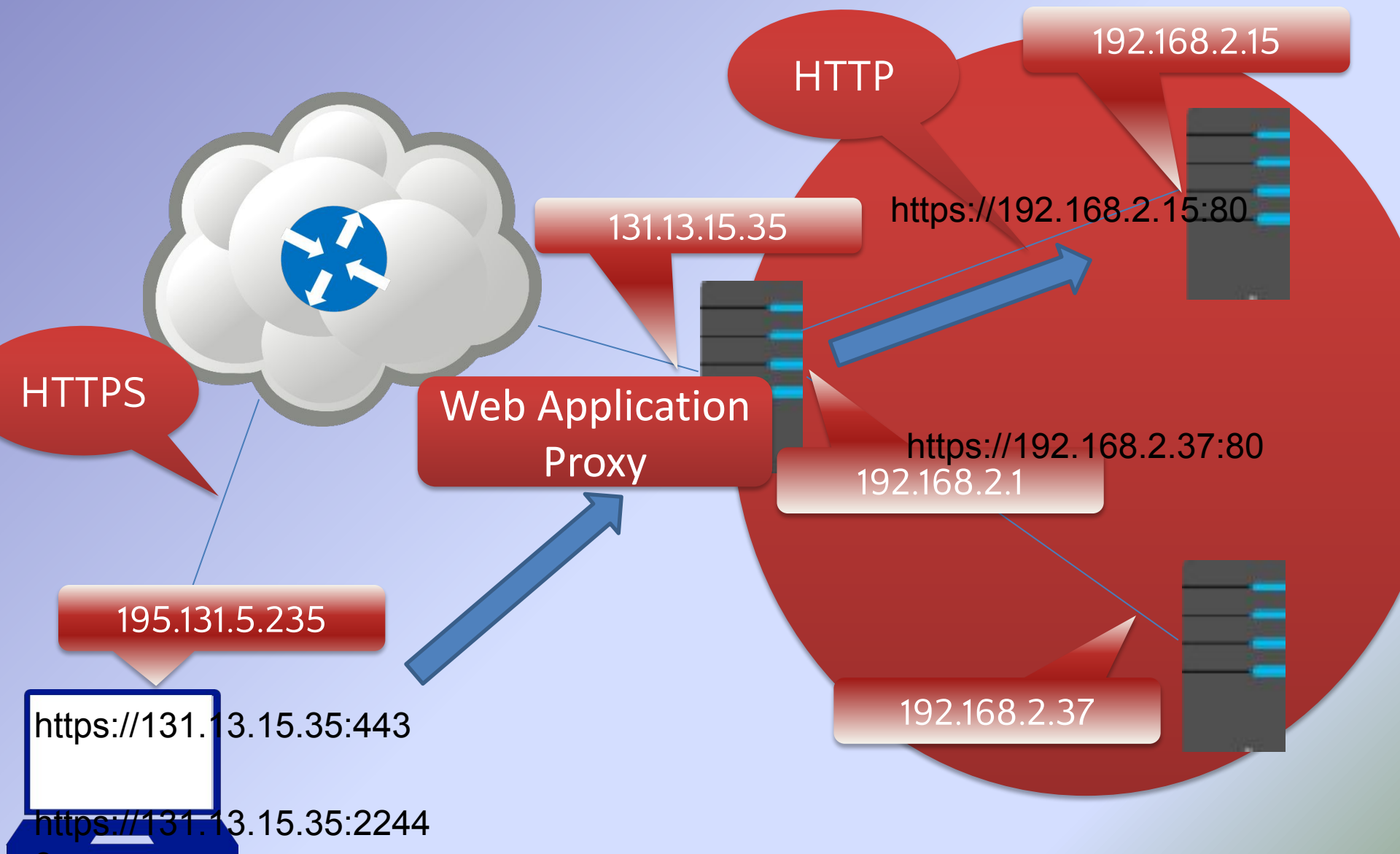
# Прокси (Proxy)



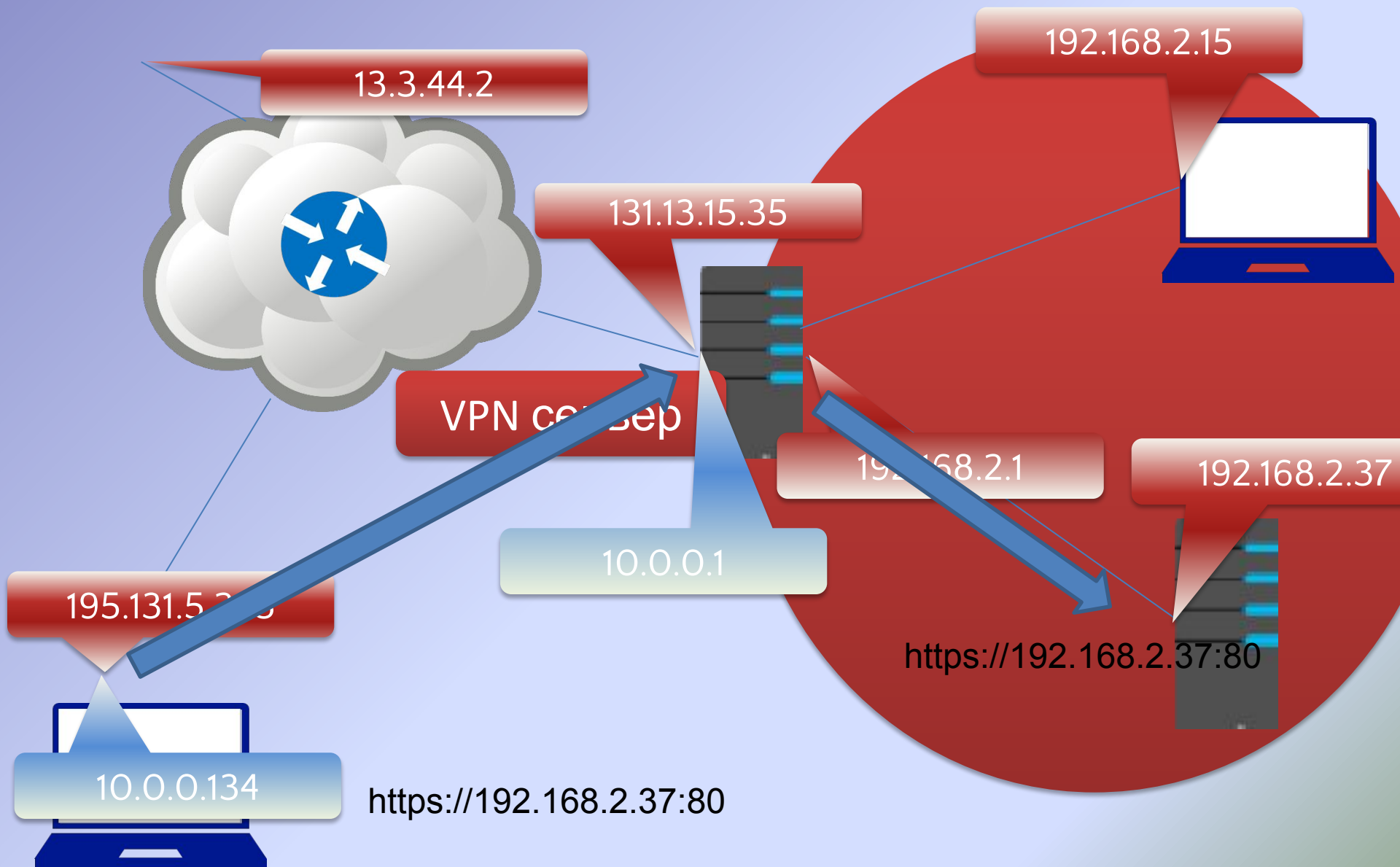
# Технологии доступа из Интернет к ресурсам корпоративной сети

- Статическая трансляция адресов (публикация)
- Обратный прокси (Application Proxy)
- VPN (Виртуальные частные сети)
- Терминальный доступ

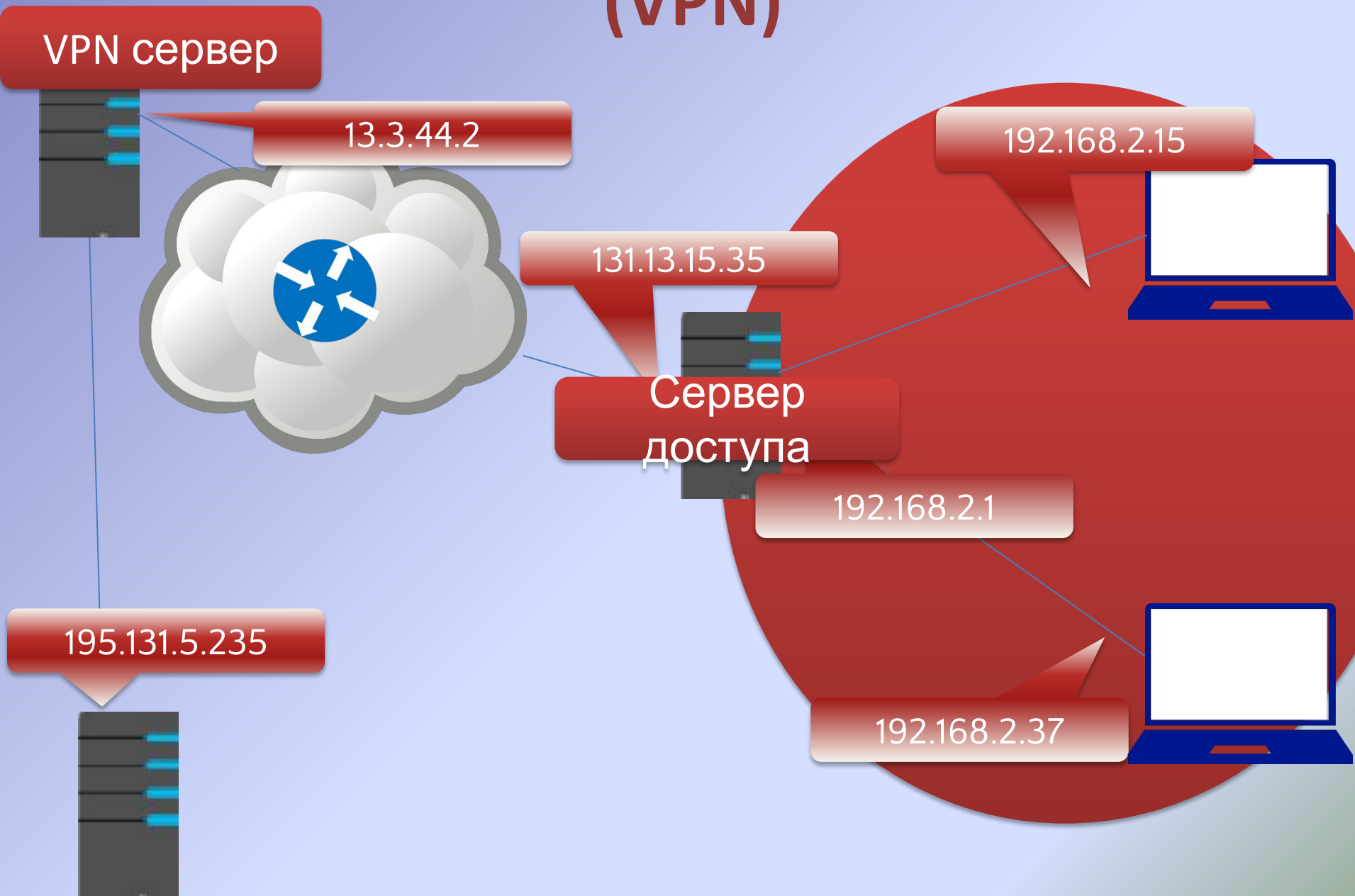
# прокси)



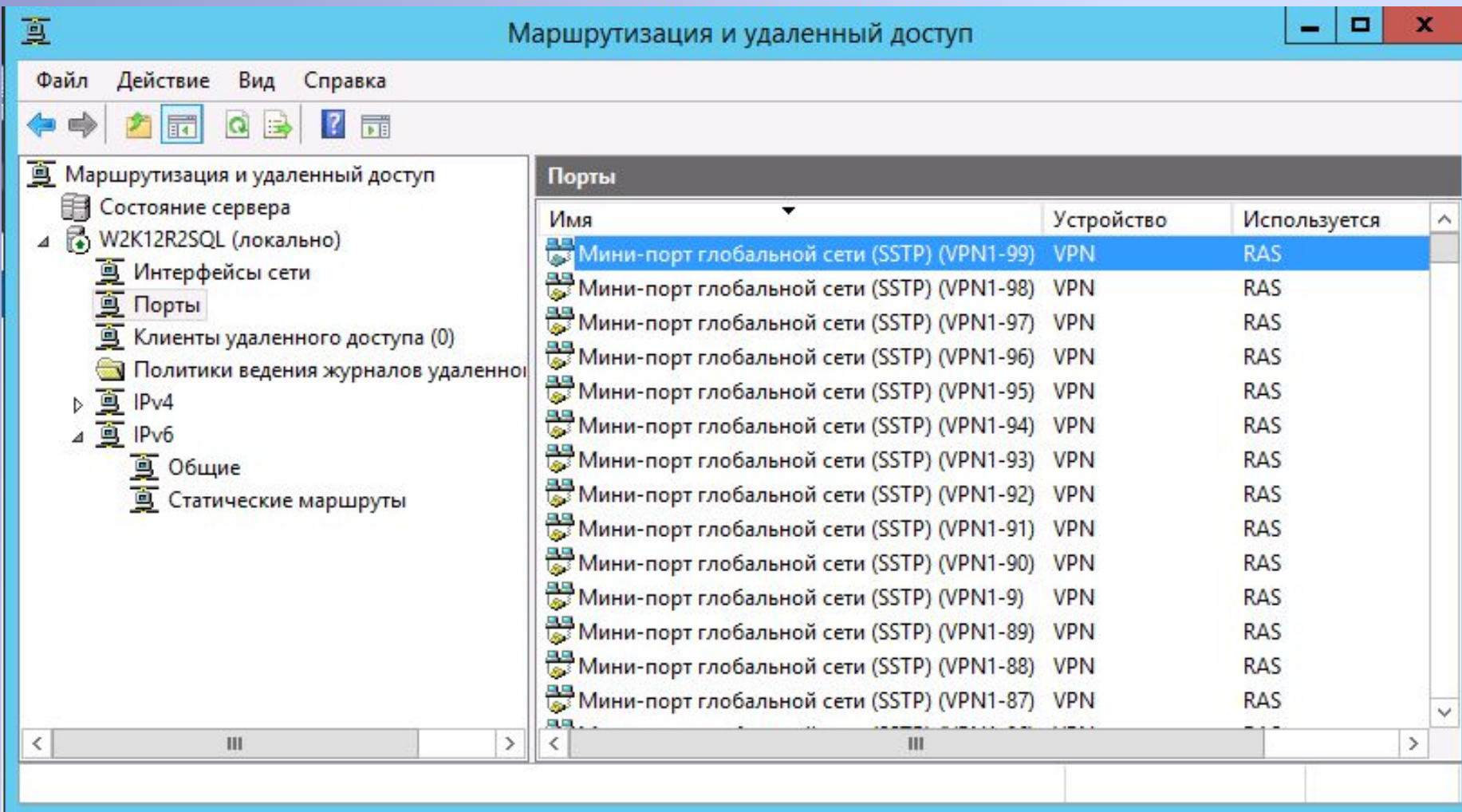
# Виртуальные частные сети (VPN)



# Виртуальные частные сети (VPN)



# Настройка VPN в RRAS



Маршрутизация и удаленный доступ

Файл Действие Вид Справка

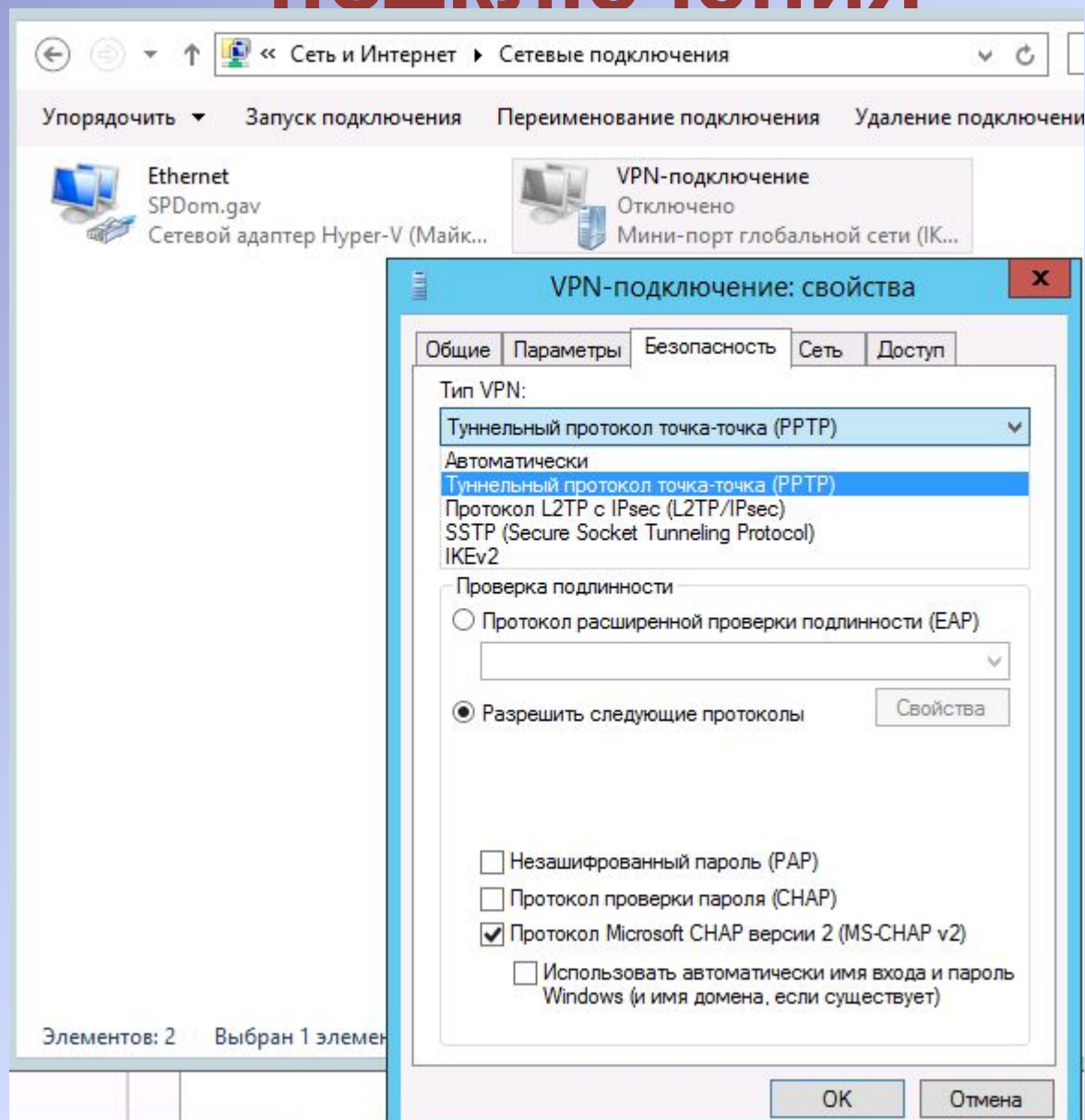
Маршрутизация и удаленный доступ

- Состояние сервера
- W2K12R2SQL (локально)
  - Интерфейсы сети
  - Порты**
  - Клиенты удаленного доступа (0)
  - Политики ведения журналов удаленного доступа
  - IPv4
  - IPv6
    - Общие
    - Статические маршруты

Имя	Устройство	Используется
Мини-порт глобальной сети (SSTP) (VPN1-99)	VPN	RAS
Мини-порт глобальной сети (SSTP) (VPN1-98)	VPN	RAS
Мини-порт глобальной сети (SSTP) (VPN1-97)	VPN	RAS
Мини-порт глобальной сети (SSTP) (VPN1-96)	VPN	RAS
Мини-порт глобальной сети (SSTP) (VPN1-95)	VPN	RAS
Мини-порт глобальной сети (SSTP) (VPN1-94)	VPN	RAS
Мини-порт глобальной сети (SSTP) (VPN1-93)	VPN	RAS
Мини-порт глобальной сети (SSTP) (VPN1-92)	VPN	RAS
Мини-порт глобальной сети (SSTP) (VPN1-91)	VPN	RAS
Мини-порт глобальной сети (SSTP) (VPN1-90)	VPN	RAS
Мини-порт глобальной сети (SSTP) (VPN1-9)	VPN	RAS
Мини-порт глобальной сети (SSTP) (VPN1-89)	VPN	RAS
Мини-порт глобальной сети (SSTP) (VPN1-88)	VPN	RAS
Мини-порт глобальной сети (SSTP) (VPN1-87)	VPN	RAS

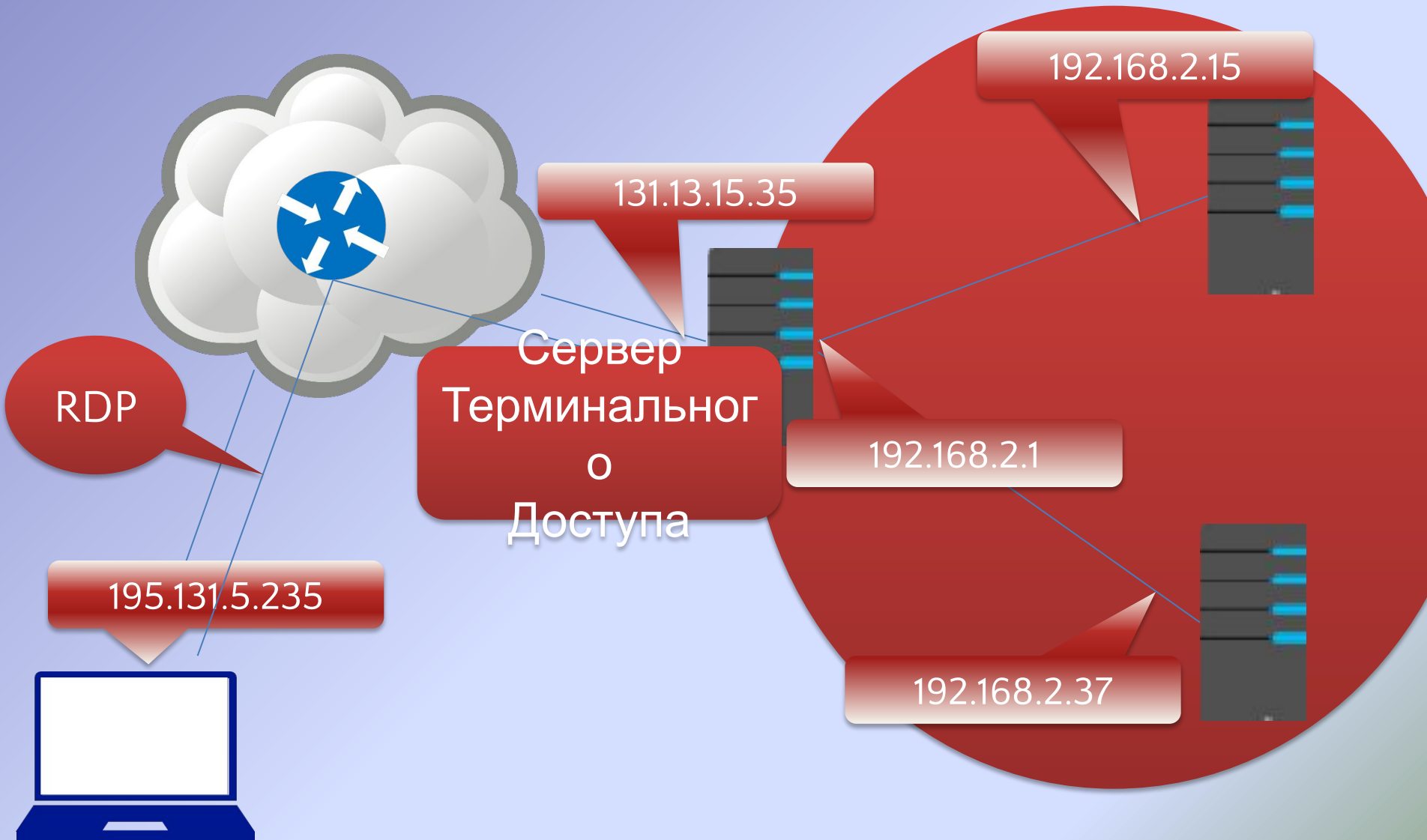


# Настройка параметров подключения

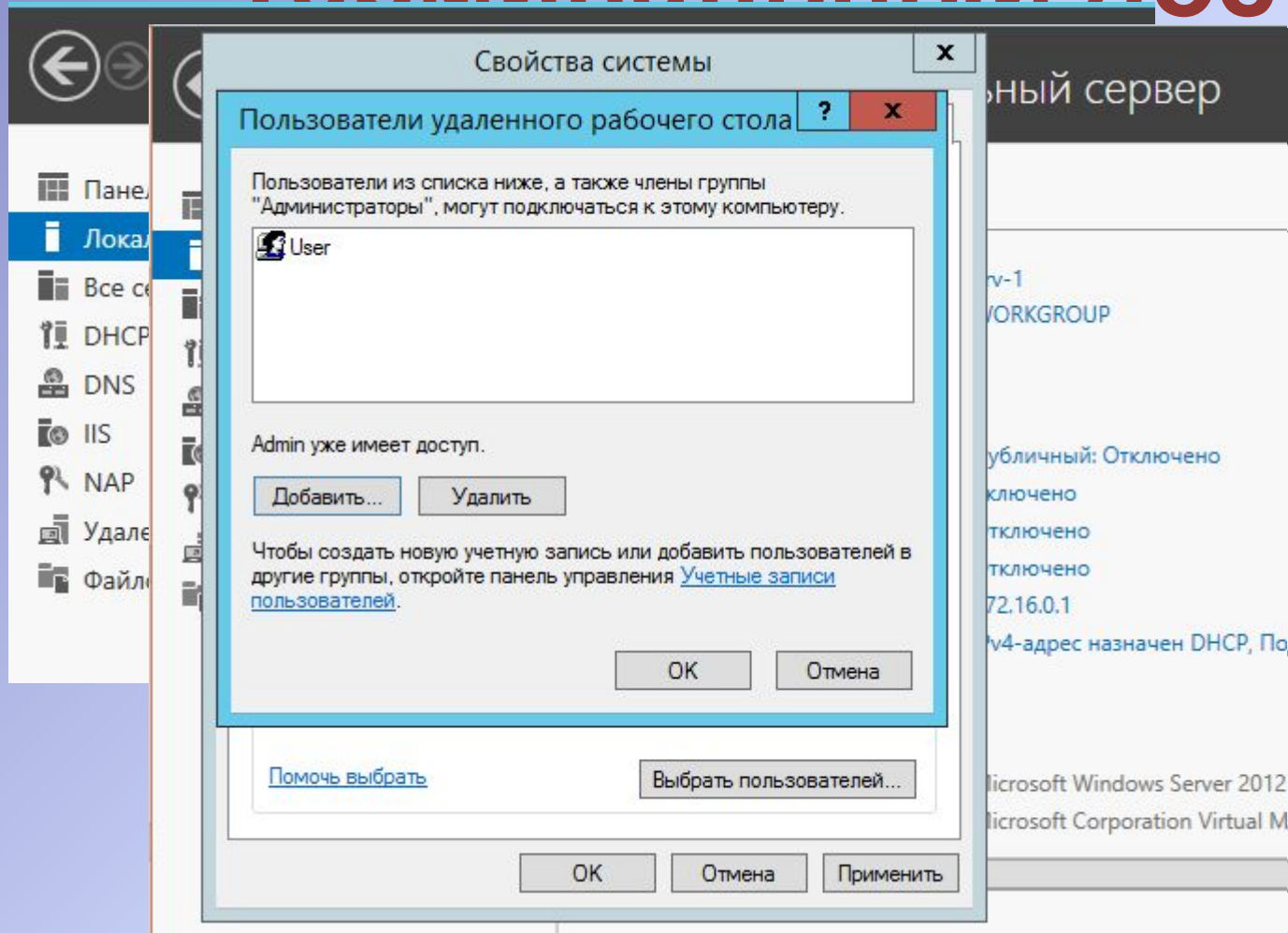




# Терминальный доступ



# Терминальный доступ



# Терминальный доступ



Подключение к удаленному рабочему с...

Подключение к удаленному

Параметры сервера шлюза удаленных рабочих столов

Подключение к удаленному рабочему столу

Параметры подключения

☐ Автоматически определять параметры сервера шлюза удаленных рабочих столов

☐ Использовать следующие параметры сервера шлюза удаленных рабочих столов:

Имя сервера:

Метод входа:

☒ Не использовать сервер шлюза удаленных рабочих столов для локальных адресов

☒ Не использовать сервер шлюза удаленных рабочих столов

Параметры входа

Пользователь:

Шлюз удаленных рабочих столов не будет использоваться для подключения к удаленному компьютеру.

☐ Использовать мои учетные данные шлюза удаленных рабочих столов для удаленного компьютера

OK Отмена



Корзина

## Командная строка

Microsoft Windows [Version 6.3.9600]  
(c) Корпорация Майкрософт (Microsoft Corporation), 2013. Все права защищены.

C:\Users\User>ipconfig /all

### Настройка протокола IP для Windows

Имя компьютера . . . . . : srv-1  
Основной DNS-суффикс . . . . . :  
Тип узла . . . . . : Гибридный  
IP-маршрутизация включена . . . . . : Нет  
WINS-прокси включен . . . . . : Нет  
Порядок просмотра суффиксов DNS . . . . . : mshome.net  
sapr.etu.ru

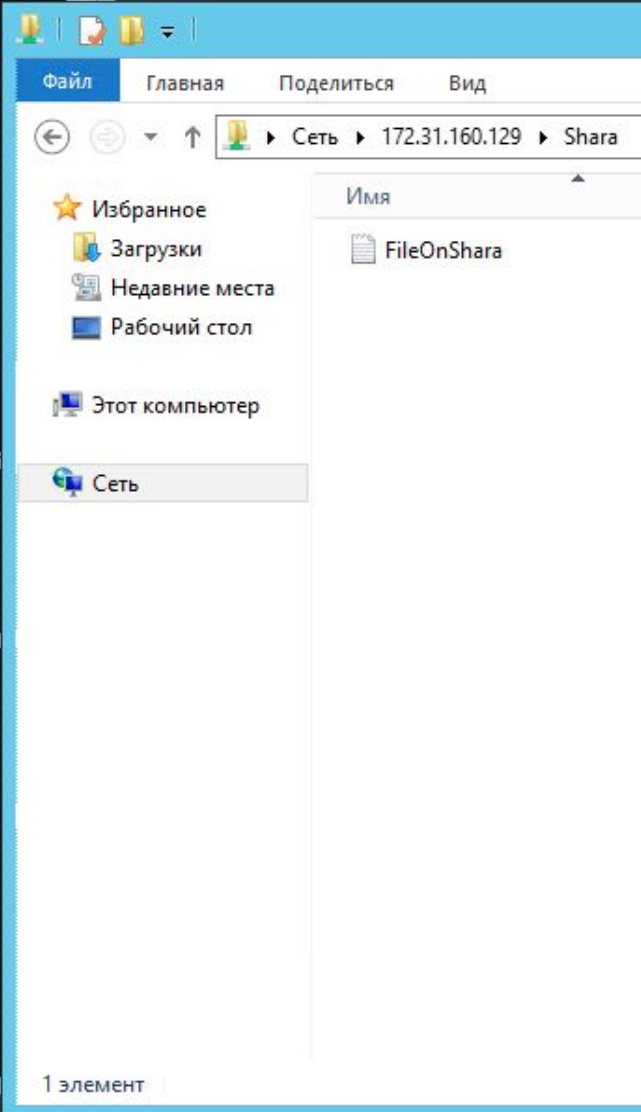
### Ethernet adapter Ethernet 2:

DNS-суффикс подключения . . . . . : mshome.net  
Описание . . . . . : Сетевой адаптер Nupur-U (Майкрософт)  
Физический адрес . . . . . : 00-15-5D-2B-A5-0D  
DHCP включен . . . . . : Да  
Автонастройка включена . . . . . : Да  
Локальный IPv6-адрес канала . . . . . : fe80::c005:26d2:d4a0:1529%14(Основной)  
IPv4-адрес . . . . . : 172.31.160.135(Основной)  
Маска подсети . . . . . : 255.255.255.240  
Аренда получена . . . . . : 12 апреля 2018 г. 8:47:09  
Срок аренды истекает . . . . . : 13 апреля 2018 г. 8:57:09  
Основной шлюз . . . . . : 172.31.160.129  
DHCP-сервер . . . . . : 172.31.160.129  
IAID DHCPv6 . . . . . : 369104221  
DUID клиента DHCPv6 . . . . . : 00-01-00-01-22-17-12-8E-00-15-5D-2B-A

DNS-серверы . . . . . : 172.31.160.129  
NetBios через TCP/IP . . . . . : Включен

### Ethernet adapter Ethernet:

DNS-суффикс подключения . . . . . : sapr.etu.ru  
Описание . . . . . : Сетевой адаптер Nupur-U (Майкрософт)  
Физический адрес . . . . . : 00-15-5D-2B-A5-0C  
DHCP включен . . . . . : Нет  
Автонастройка включена . . . . . : Да  
IPv4-адрес . . . . . : 172.16.0.1(Основной)  
Маска подсети . . . . . : 255.255.0.0  
Основной шлюз . . . . . :  
DNS-серверы . . . . . : 172.16.0.1  
192.168.3.15  
8.8.8.8  
Основной WINS-сервер . . . . . : 172.16.0.1  
NetBios через TCP/IP . . . . . : Включен





Корзина

Microsoft Windows [C:\>]  
(c) Корпорация Майкрософт

C:\>\Users\User>ipconfig

Настройка протокола

Имя компьютера  
Основной DNS-суффикс  
Тип узла . . . . .  
IP-маршрутизация  
WINS-прокси включен  
Порядок просмотра

Ethernet adapter Ethernet

DNS-суффикс подсети  
Описание . . . . .  
Физический адрес  
DHCP включен . . . .  
Автонастройка включена  
Локальный IPv6-адрес  
IPv4-адрес . . . . .  
Маска подсети . . . .  
Аренда получена  
Срок аренды истекает  
Основной шлюз . . . .  
DHCP-сервер . . . . .  
IAID DHCPv6 . . . . .  
DUID клиента DHCPv6

DNS-серверы . . . . .  
NetBios через TCP/IP

Ethernet adapter Ethernet

DNS-суффикс подсети  
Описание . . . . .  
Физический адрес  
DHCP включен . . . .  
Автонастройка включена  
IPv4-адрес . . . . .  
Маска подсети . . . .  
Основной шлюз . . . .  
DNS-серверы . . . . .

Основной WINS-сервер . . . . .  
NetBios через TCP/IP . . . . .

Отмена



Shara

Файл

Главная

Поделиться

Вид



Сеть > 172.31.160.129 > Shara

Избранное

Загрузки

Недавние места

Рабочий стол

Этот компьютер

Сеть

1 элемент

Имя

Дата изменения

Тип

FileOnShara

12.04.2018 9:05

Текстовый документ

Диспетчер задач



Файл Параметры Вид

Процессы

Производительность

Пользователи

Подробности

Службы

Пользователь

Состояние

4%

81%

ЦП

Память

4 User (10)



Диспетчер задач



Диспетчер окон рабочег...



Обработчик команд Win...



Обработчик команд Win...



Окно консоли узла



Окно консоли узла



Проводник



Программа входа в систе...



Процесс исполнения кли...



Хост-процесс для задач ...

0%

64,8 МБ

0%

5,8 МБ

0%

15,6 МБ

0%

0,3 МБ

0%

0,3 МБ

0%

0,8 МБ

0%

0,9 МБ

0%

37,0 МБ

0%

0,8 МБ

0%

1,0 МБ

0%

2,1 МБ

**Спасибо за внимание!**

# Сертификаты. Инфраструктура шифрования с открытым ключом (PKI)

Горячев Александр Вадимович  
Доцент кафедры ИБ  
[avgoriachev@etu.ru](mailto:avgoriachev@etu.ru)



# Модель эшелонированной обороны

Физический  
доступ

Политики, процедуры,  
осведомленность

Хранилище

ACL EFS Bitlocker

Backup Mirror RAID SC

Обработка

APPs

Antivirus Updates

OS/.NET

Antispyware Autentification HIDS-HIPS

PKI

AD

Передача

Intranet

Routing

IPSec

RMS

NIDS-NIPS

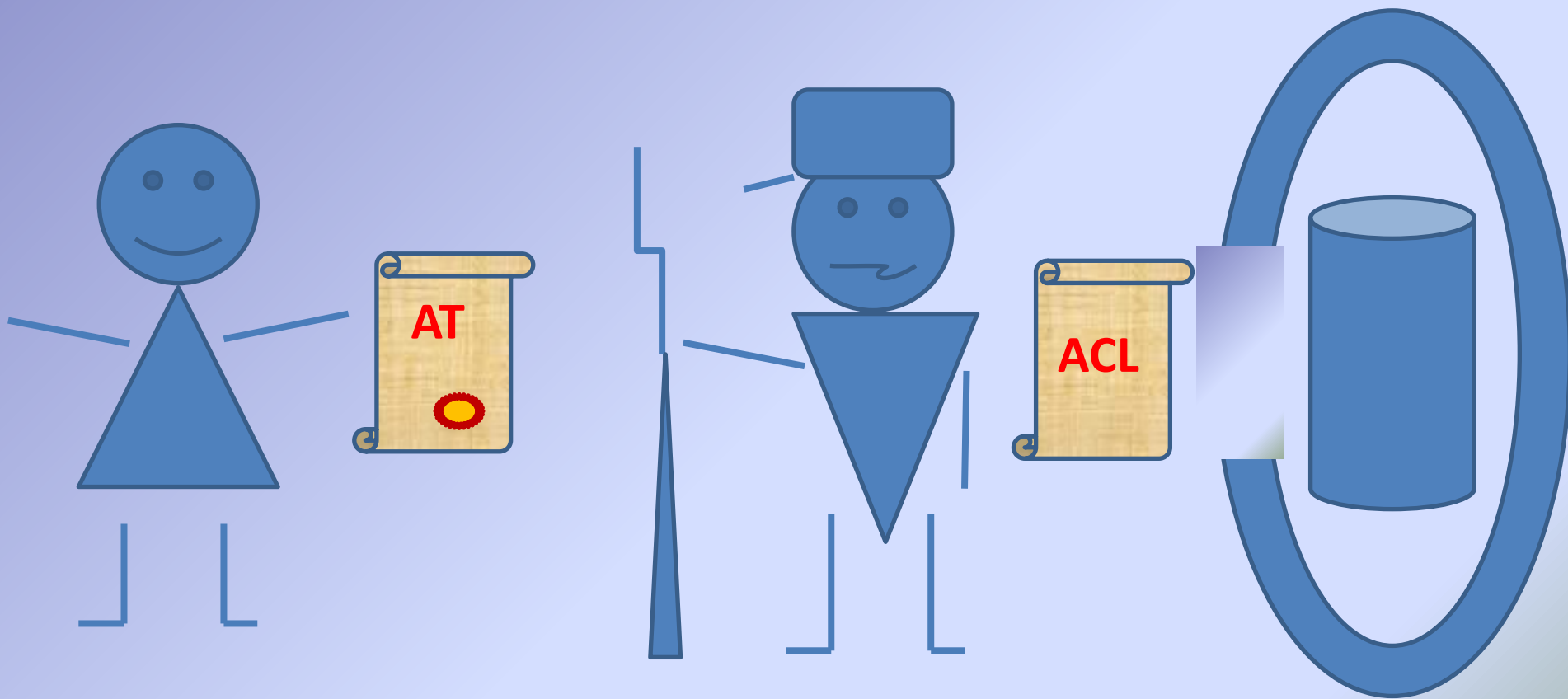
Internet

Firewall

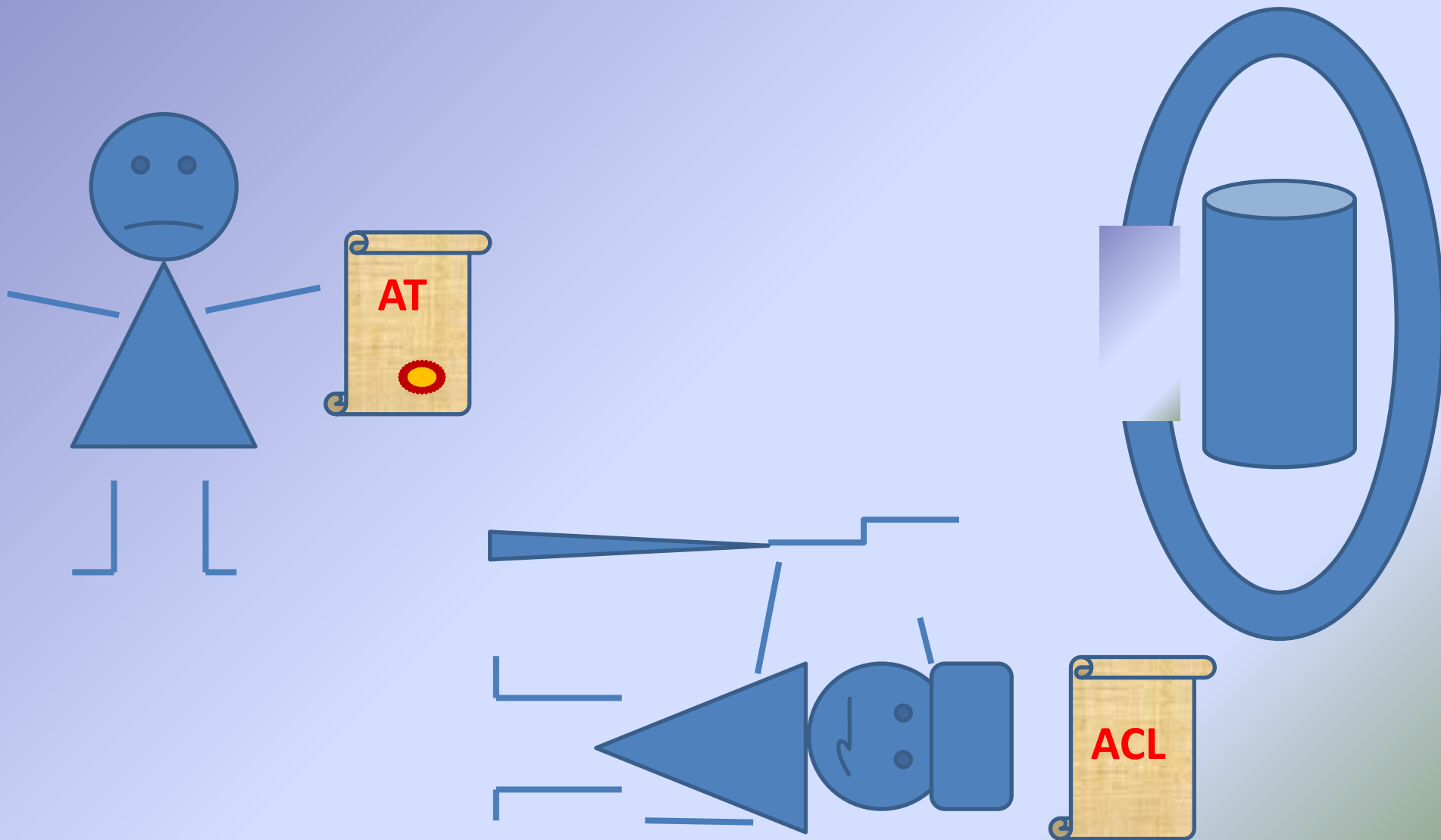
VPN

NAP

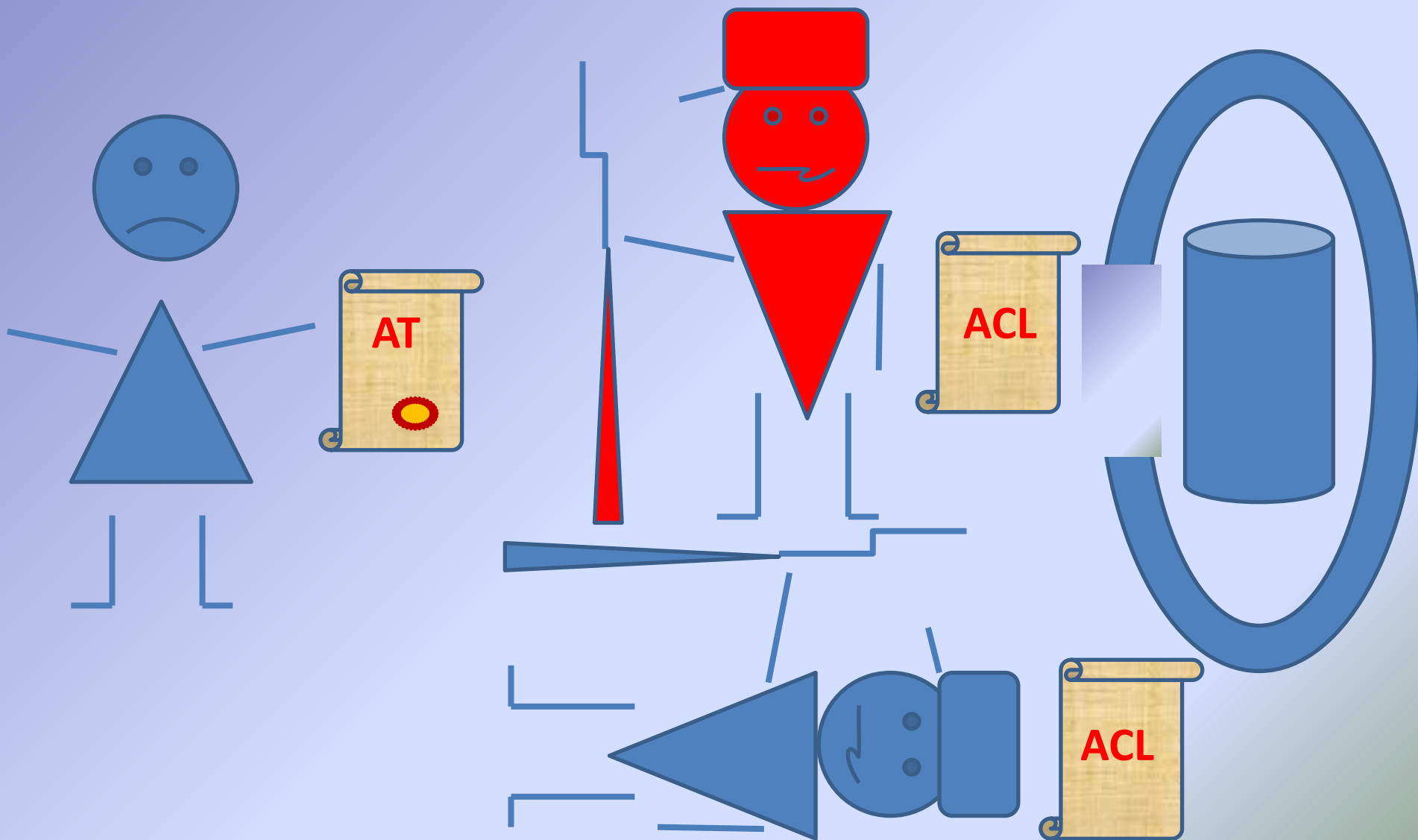
# Список контроля доступа



# Список контроля доступа



# Список контроля доступа

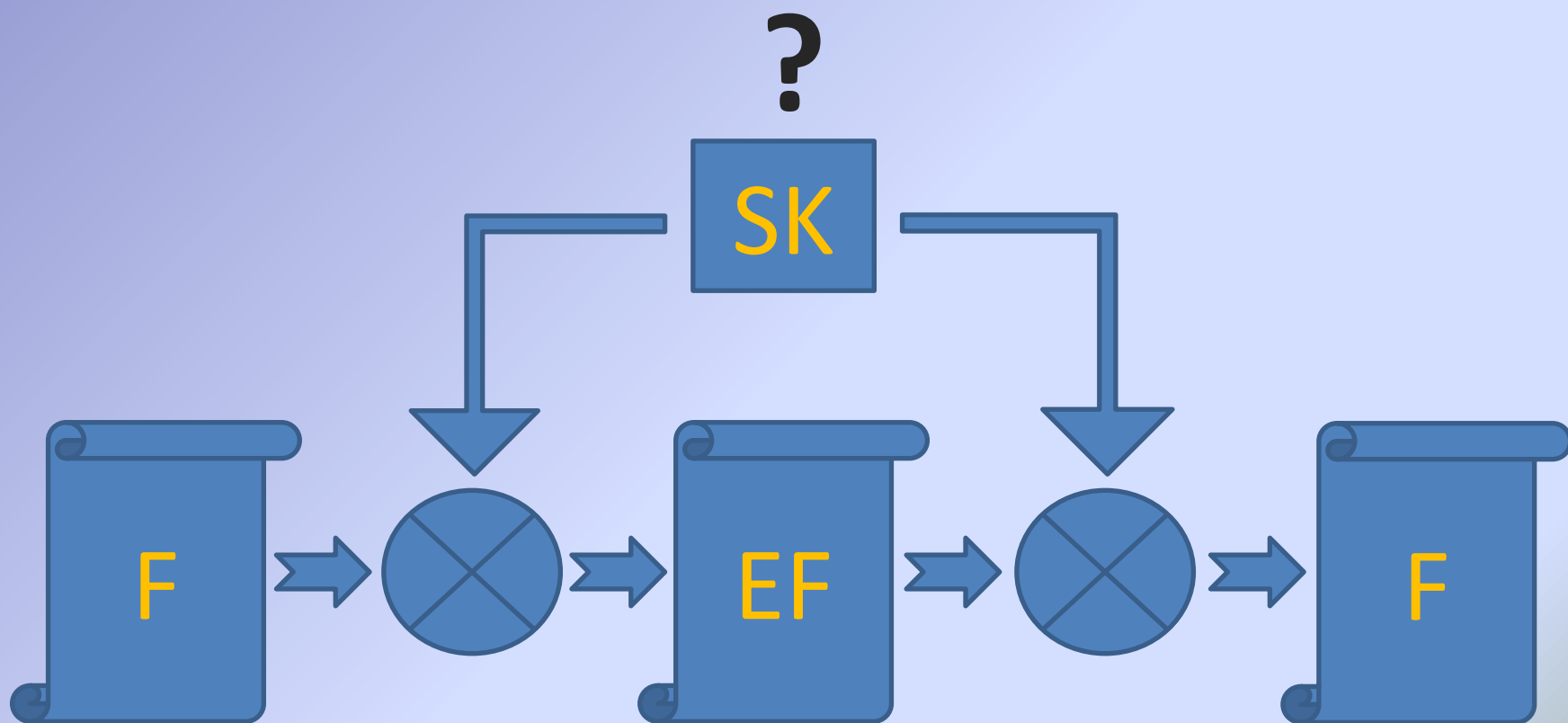


# Шифрование с симметричным ключом

$$T(a, x) = e$$

$$T^{-1}(e, x) = a$$

# Простейший вариант



# Шифрование с асимметричным ключом (открытым и закрытым ключами)

$$G \rightarrow (o, p)$$

$$T(a, o) = e$$

$$T^{-1}(e, p) = a$$

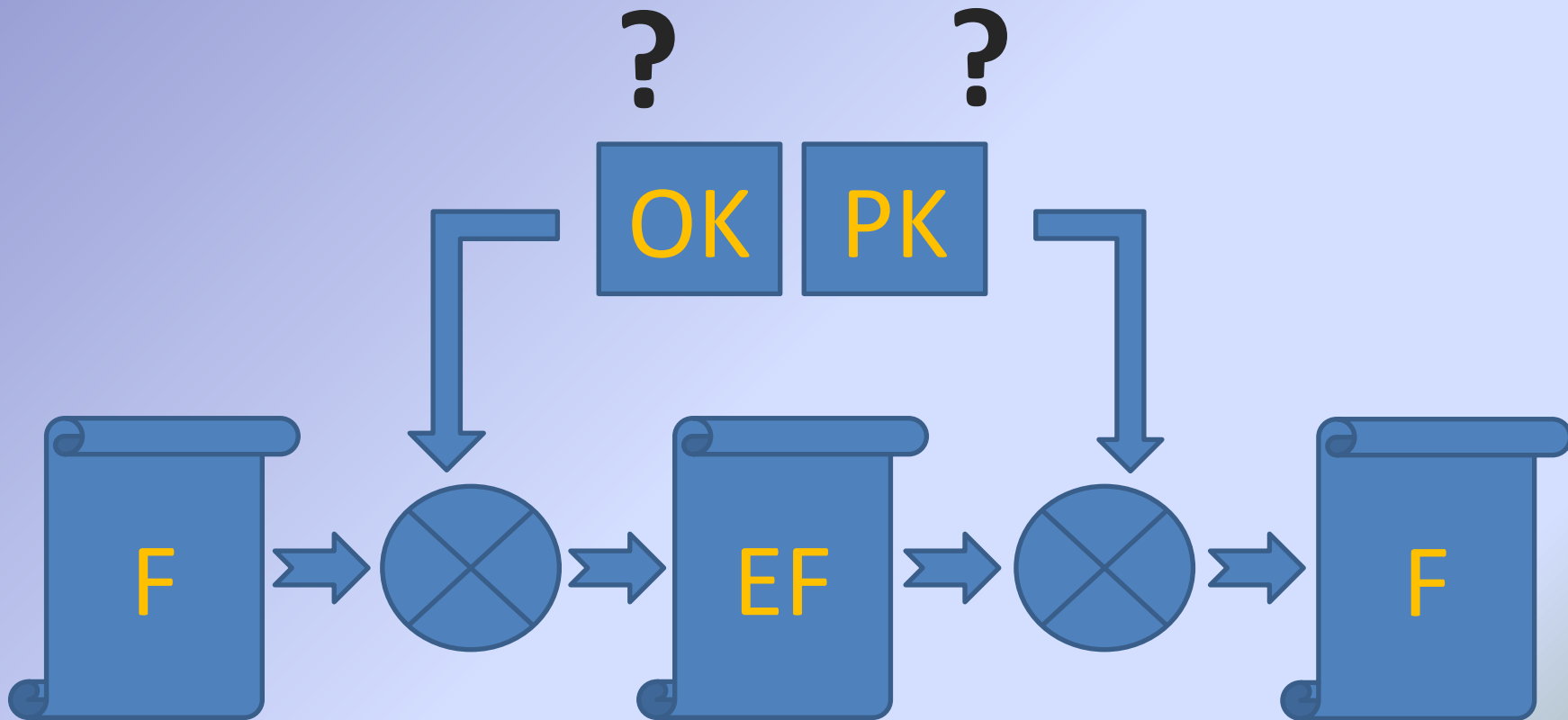
$$G \rightarrow (o, p)$$

$$T(a, p) = e$$

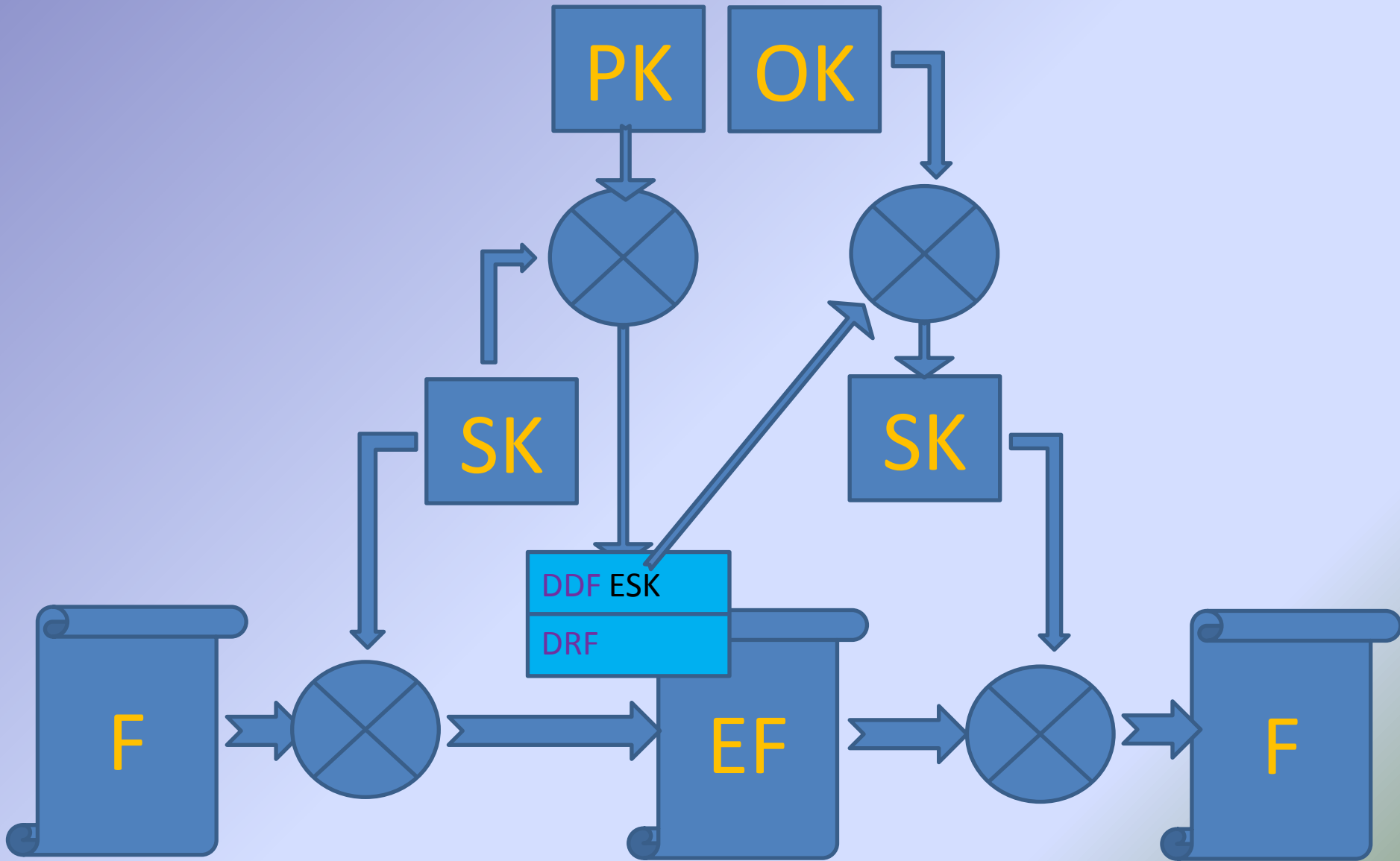
$$T^{-1}(e, o) = a$$



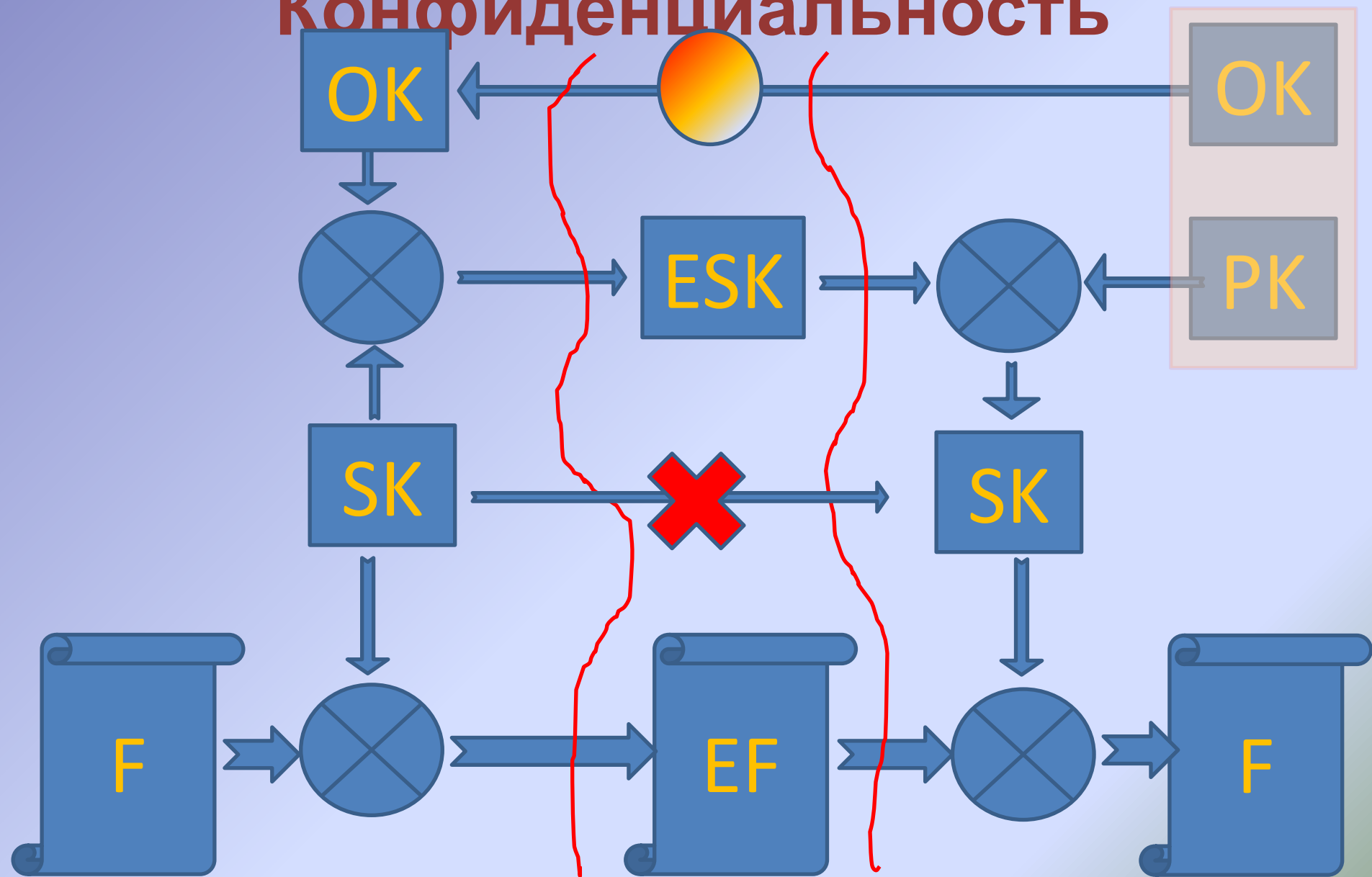
# А можно так?



# Уже правильнее

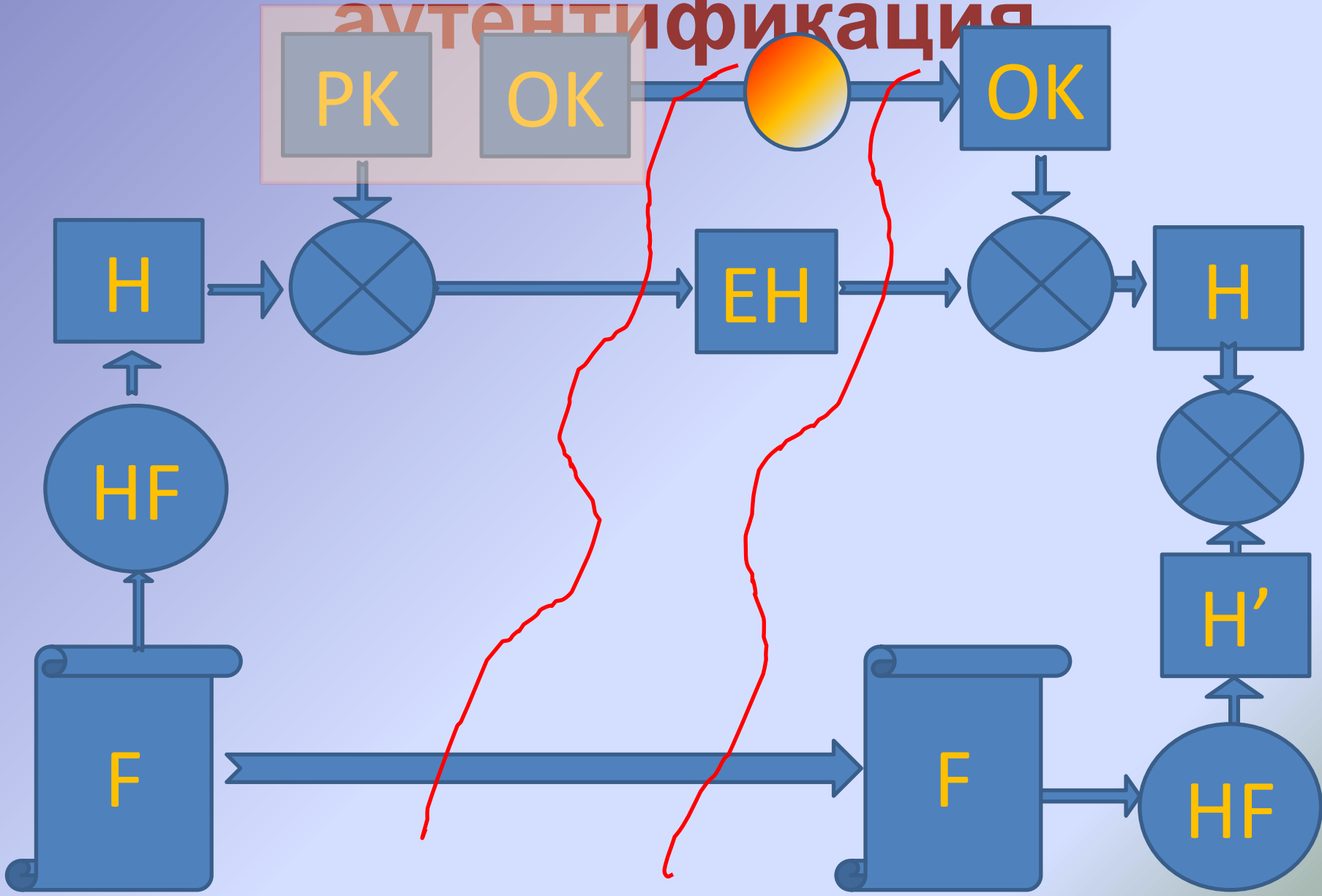


# Передача - Конфиденциальность



# Целостность и

## аутентификация



# Формирование сертификата

Заявка на

сертификат

Зачем

Кто?

?

?

С

Инф

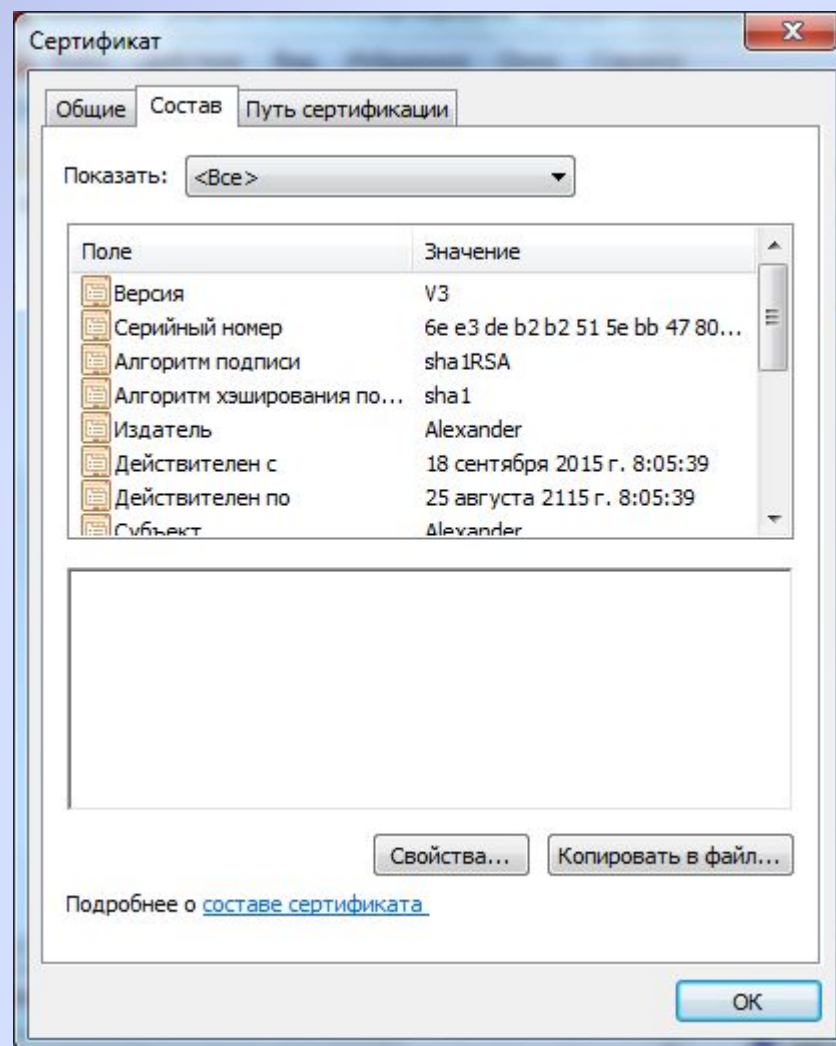
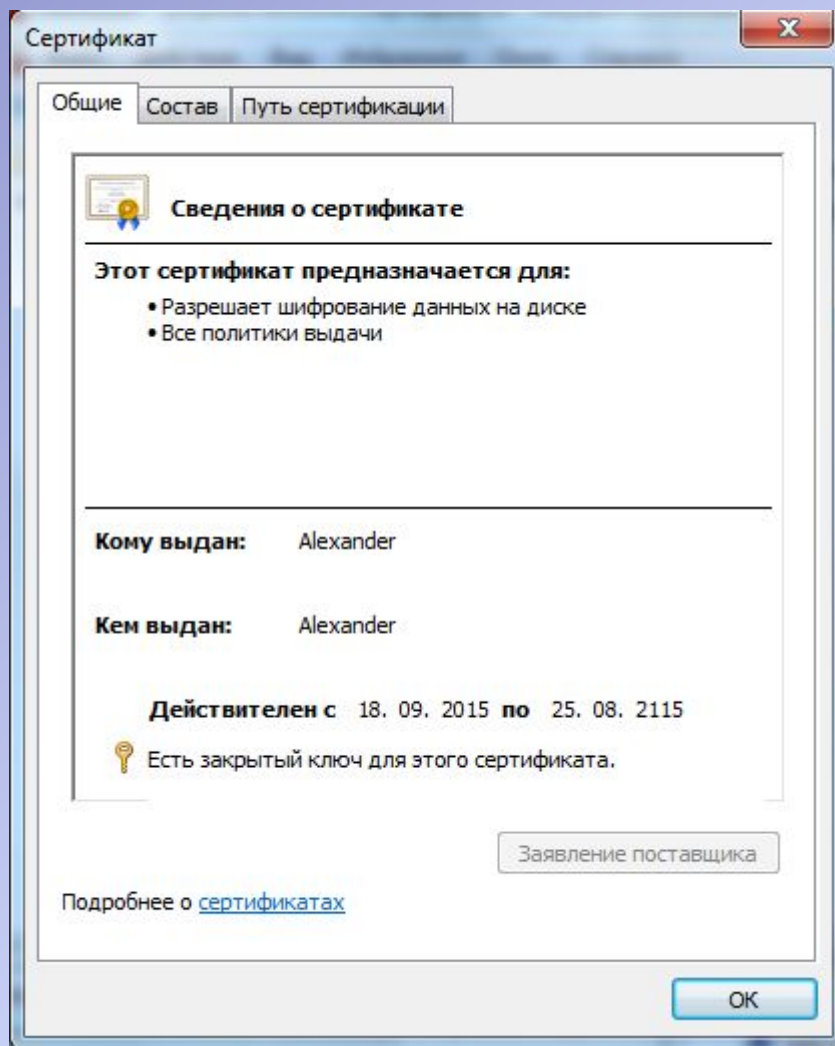
S

А

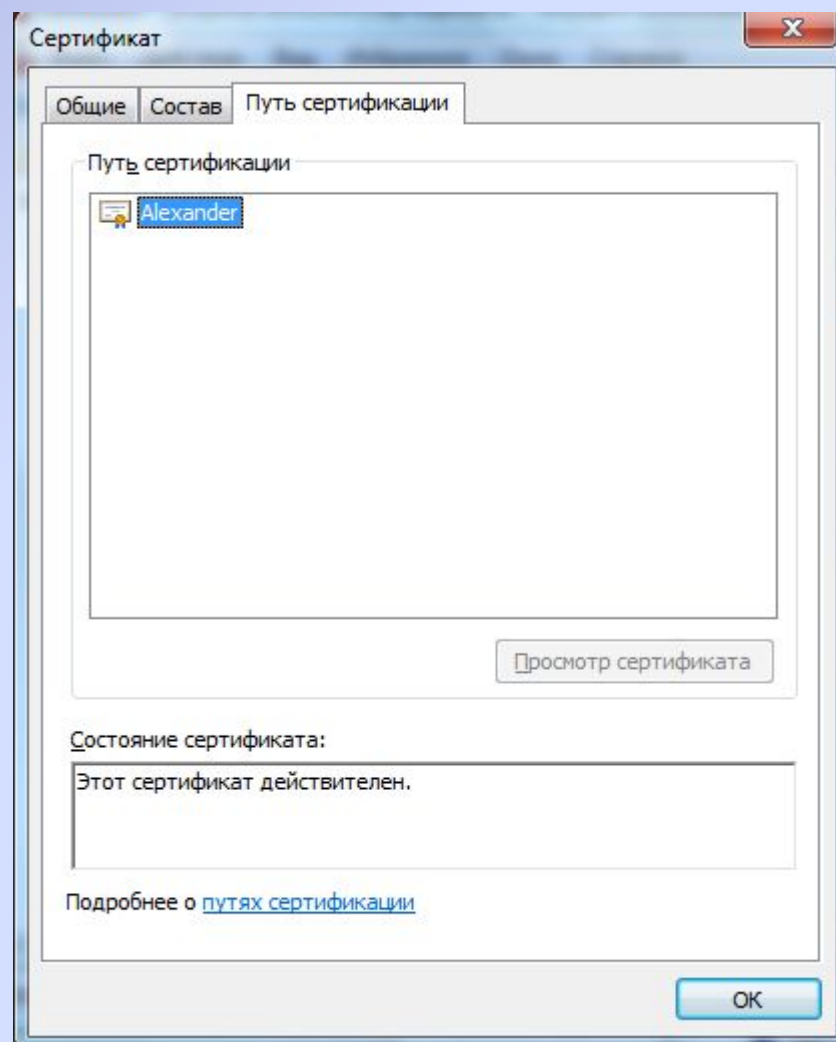
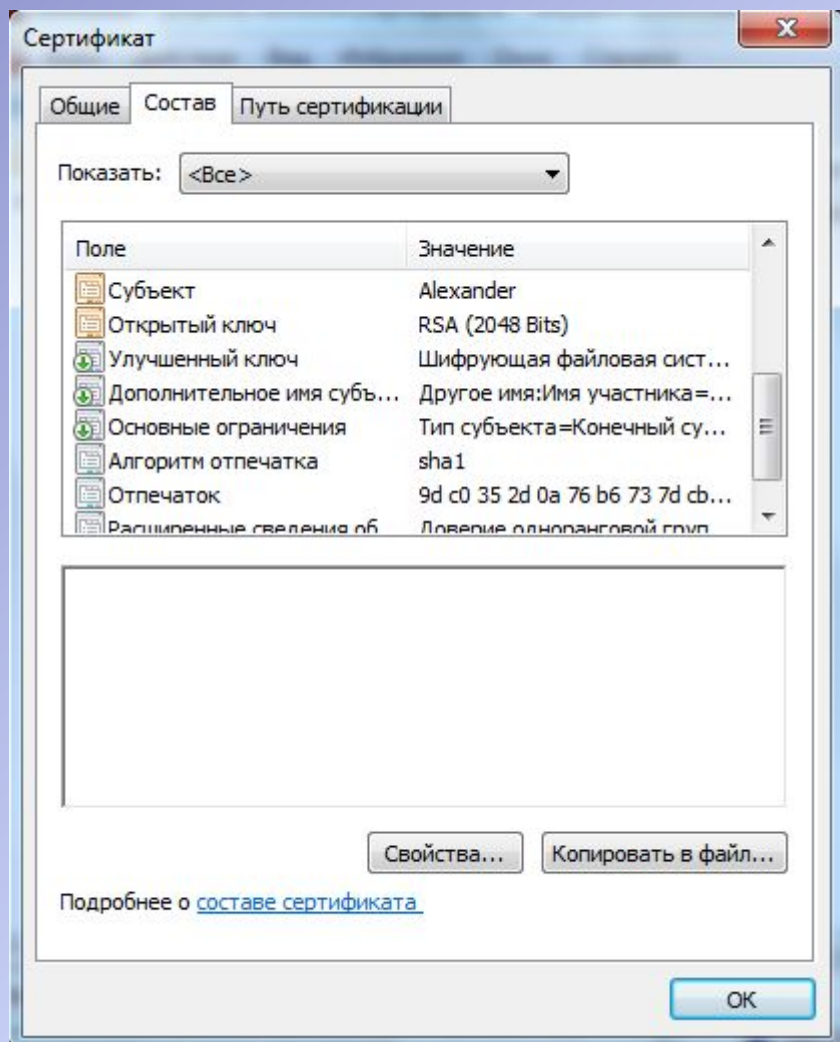
о

СА

# Сертификат

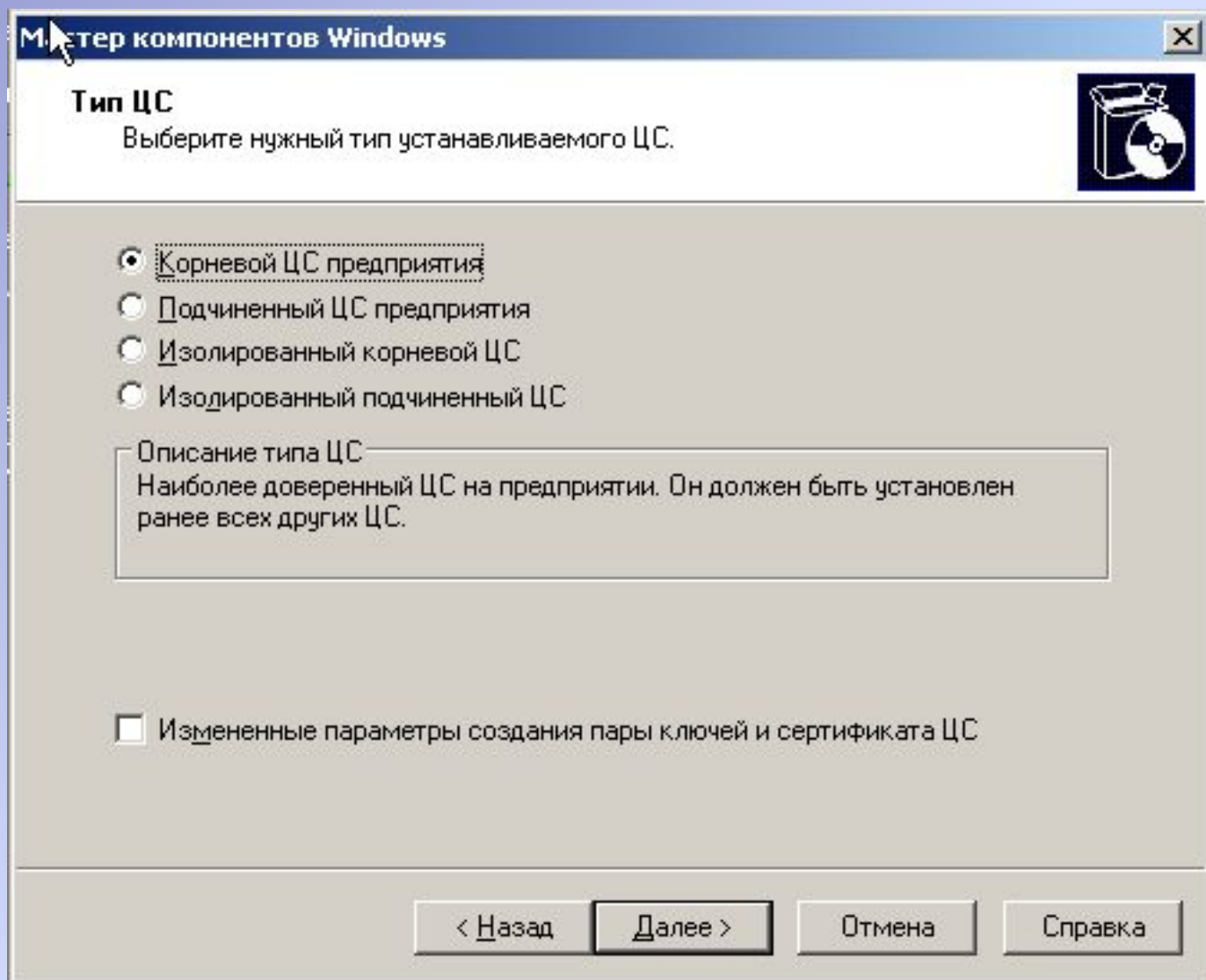


# Сертификат





# Типы СА



# Имя и сертификат

Мастер компонентов Windows

**Сведения о центре сертификации**  
Введите сведения об этом центре сертификации

Общее имя для этого ЦС:  
DC1

Суффикс различающегося имени:  
DC=sapr,DC=etu,DC=ru

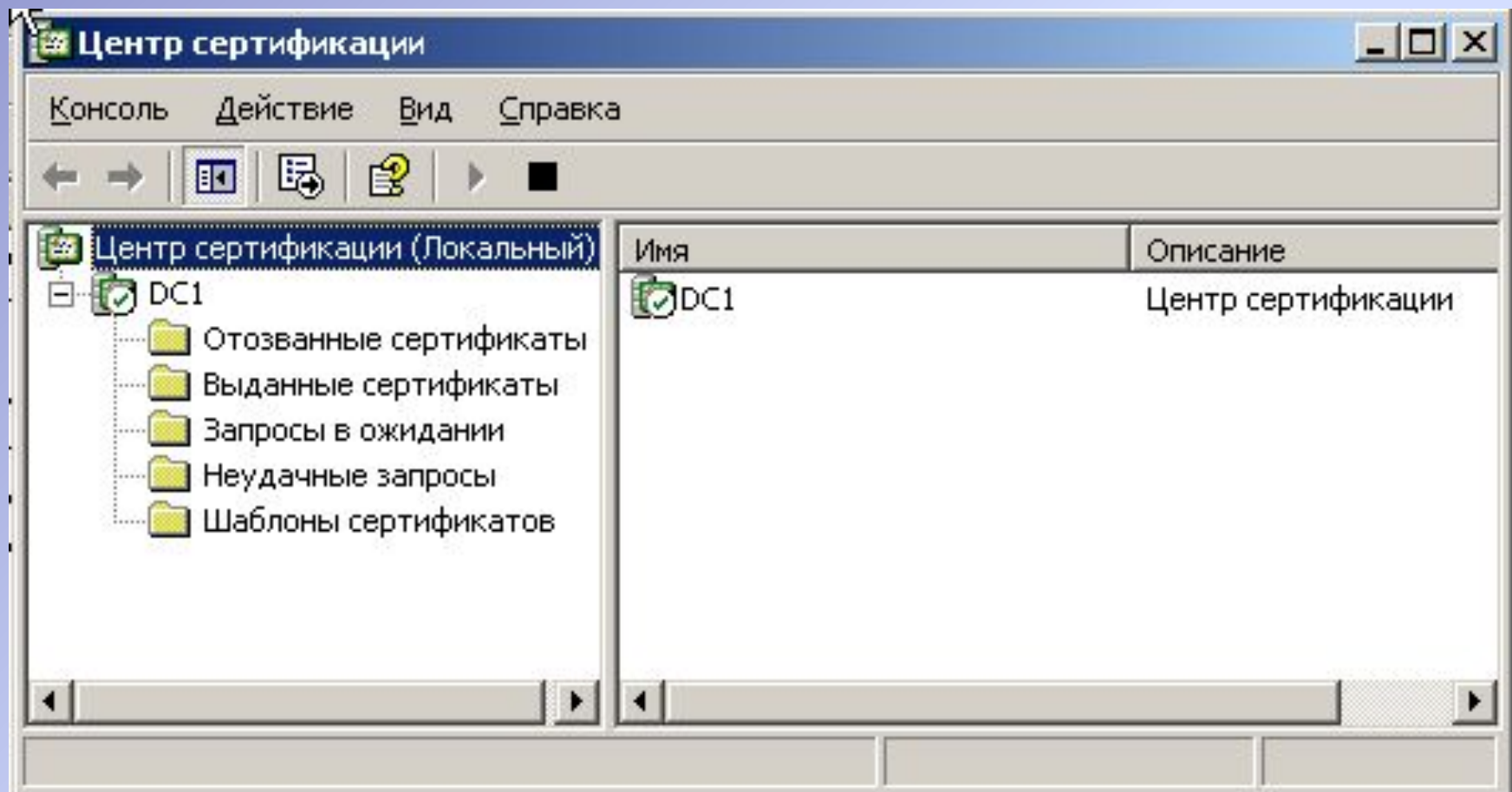
Просмотр различающегося имени:  
CN=DC1,DC=sapr,DC=etu,DC=ru

Срок действия:  
5 лет

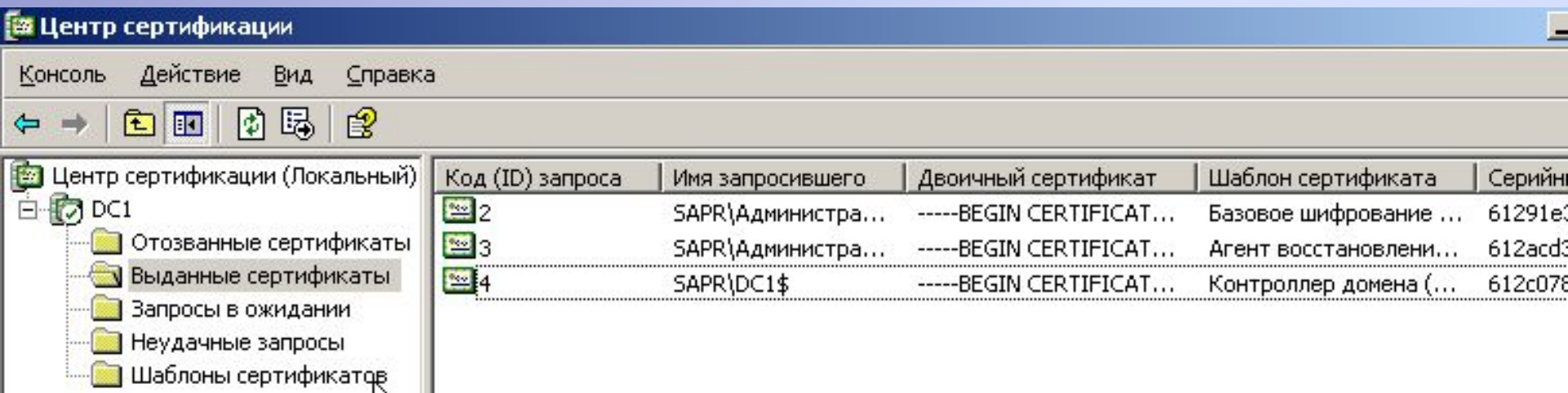
Истекает:  
25.09.2020 6:53

< Назад    Далее >    Отмена    Справка

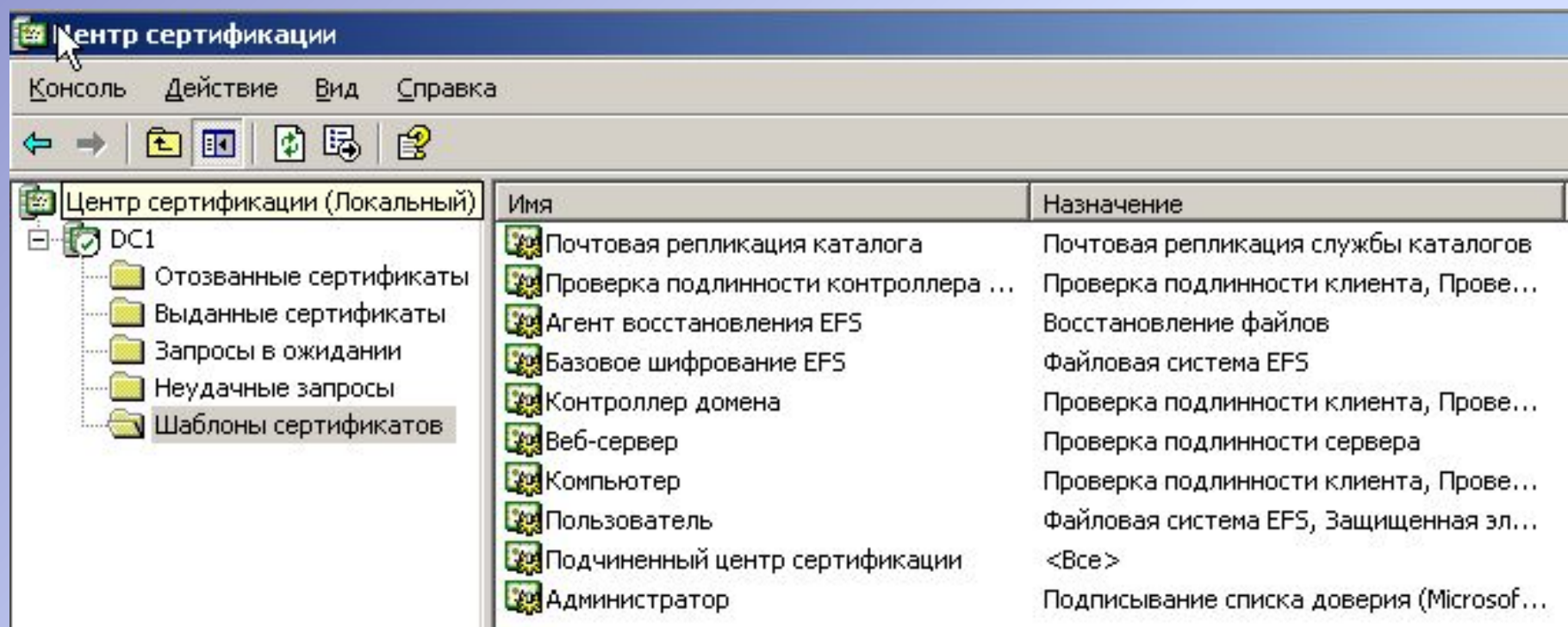
# Консоль центра сертификатов



# Выданные сертификаты



# Шаблоны сертификатов



Центр сертификации

Консоль Действие Вид Справка

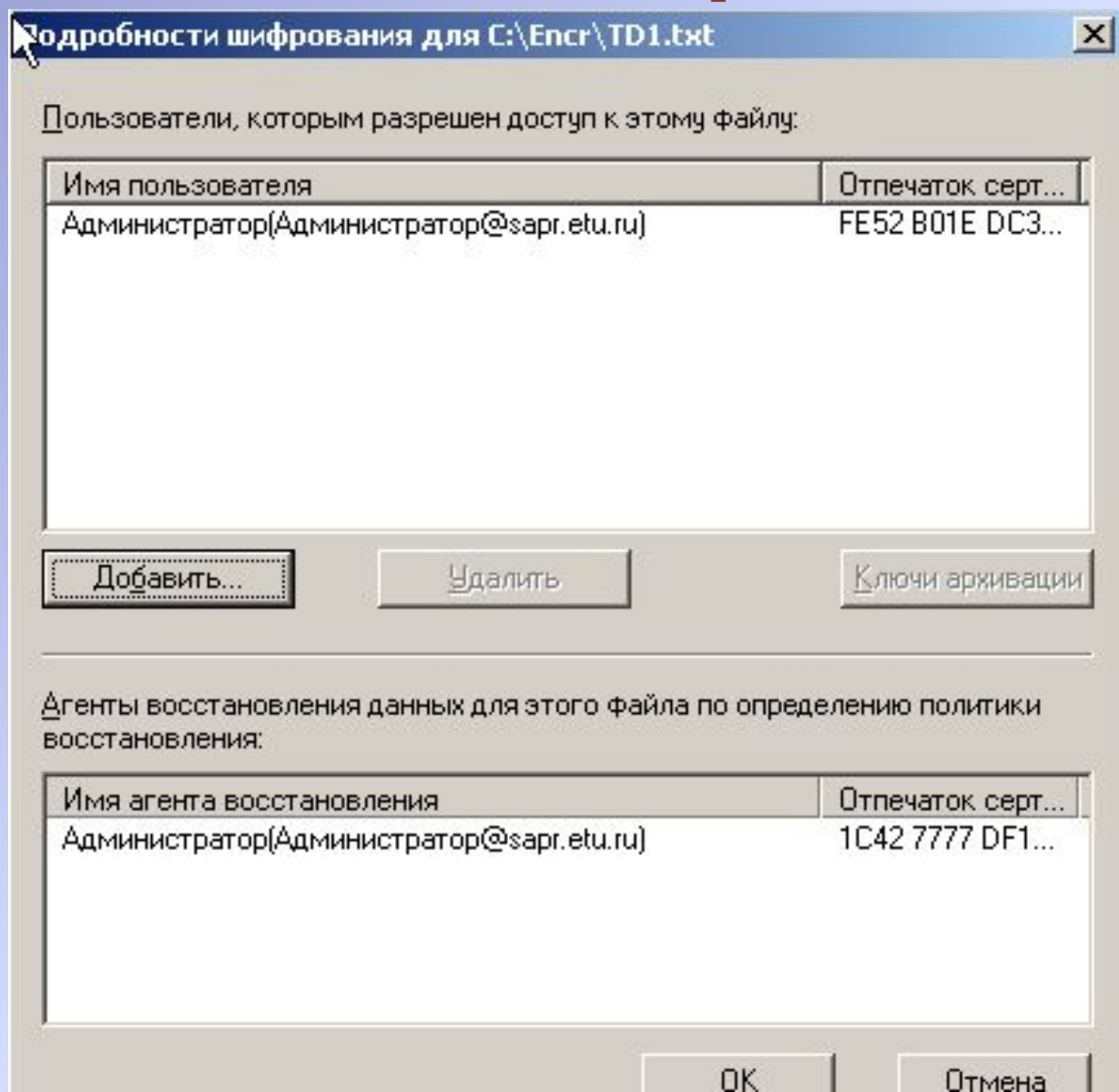
← → [Иконки]

Центр сертификации (Локальный)

- DC1
  - Отозванные сертификаты
  - Выданные сертификаты
  - Запросы в ожидании
  - Неудачные запросы
  - Шаблоны сертификатов**

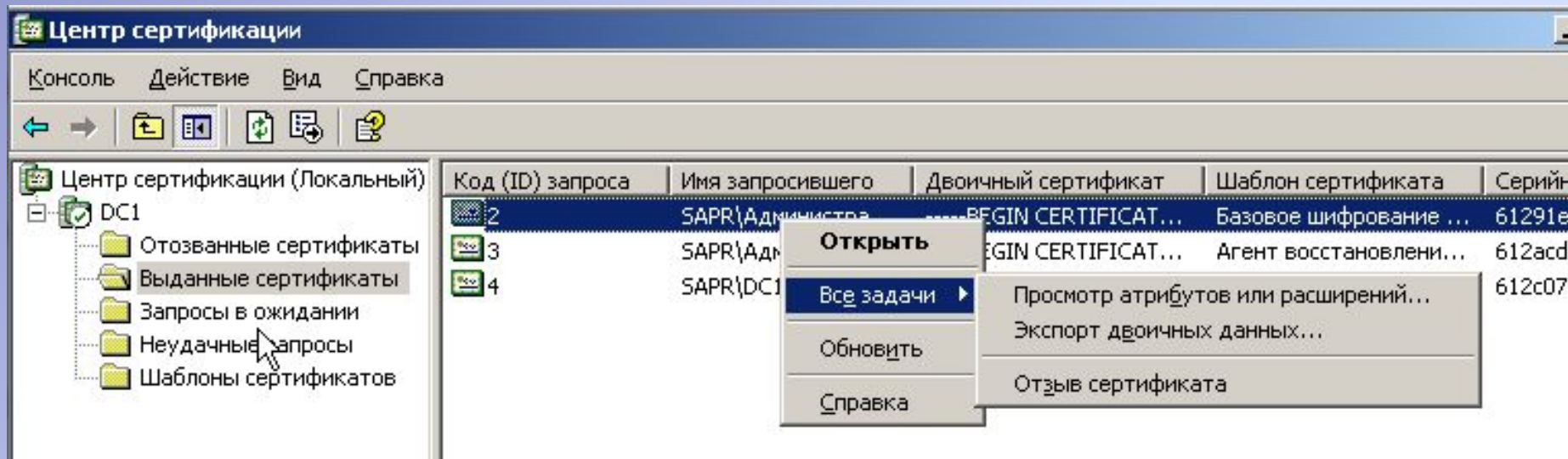
Имя	Назначение
Почтовая репликация каталога	Почтовая репликация службы каталогов
Проверка подлинности контроллера ...	Проверка подлинности клиента, Прове...
Агент восстановления EFS	Восстановление файлов
Базовое шифрование EFS	Файловая система EFS
Контроллер домена	Проверка подлинности клиента, Прове...
Веб-сервер	Проверка подлинности сервера
Компьютер	Проверка подлинности клиента, Прове...
Пользователь	Файловая система EFS, Защищенная эл...
Подчиненный центр сертификации	<Все>
Администратор	Подписывание списка доверия (Microsof...

# Заголовок файла



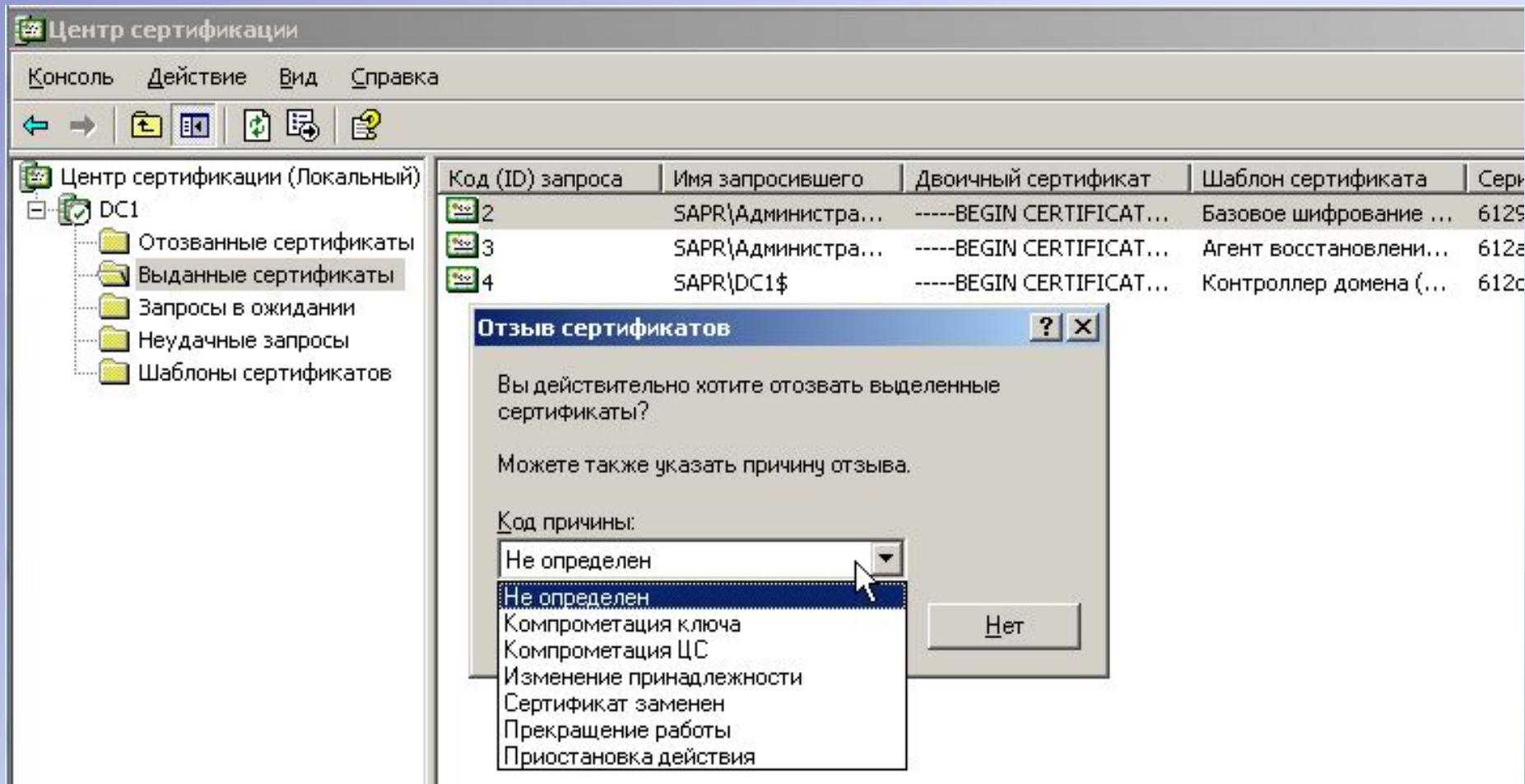


# Отзыв сертификата

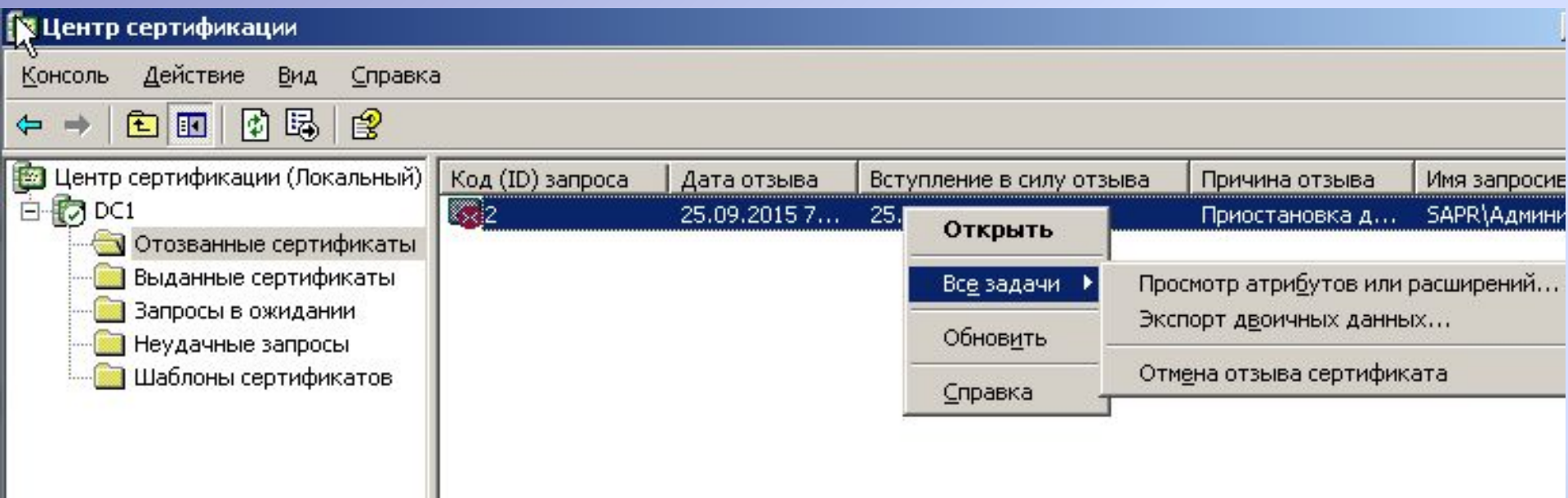




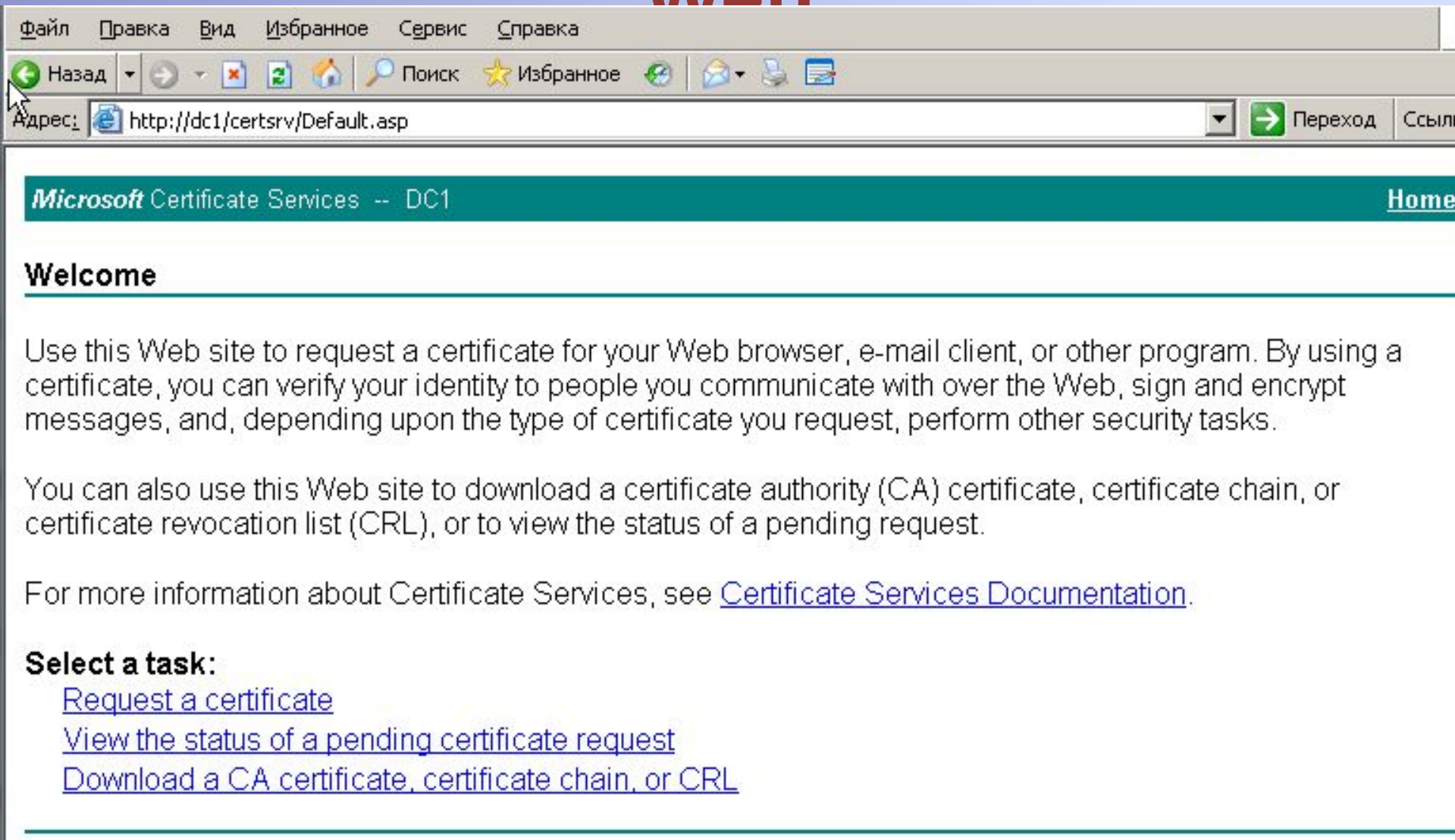
# Отзыв сертификата - причина



# Отмена отзыва сертификата



# Запрос сертификата через Web



The screenshot shows a Microsoft Internet Explorer browser window. The address bar displays the URL `http://dc1/certsrv/Default.asp`. The page title is "Microsoft Certificate Services -- DC1". The main content area has a "Welcome" heading and explains the purpose of the site: to request a certificate for a web browser, email client, or other program. It also mentions that users can download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL). At the bottom, there is a section titled "Select a task:" with three links: "Request a certificate", "View the status of a pending certificate request", and "Download a CA certificate, certificate chain, or CRL".

Файл Правка Вид Избранное Сервис Справка

Назад Поиск Избранное

Адрес: `http://dc1/certsrv/Default.asp` Переход Ссылки

**Microsoft** Certificate Services -- DC1 [Home](#)

## Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

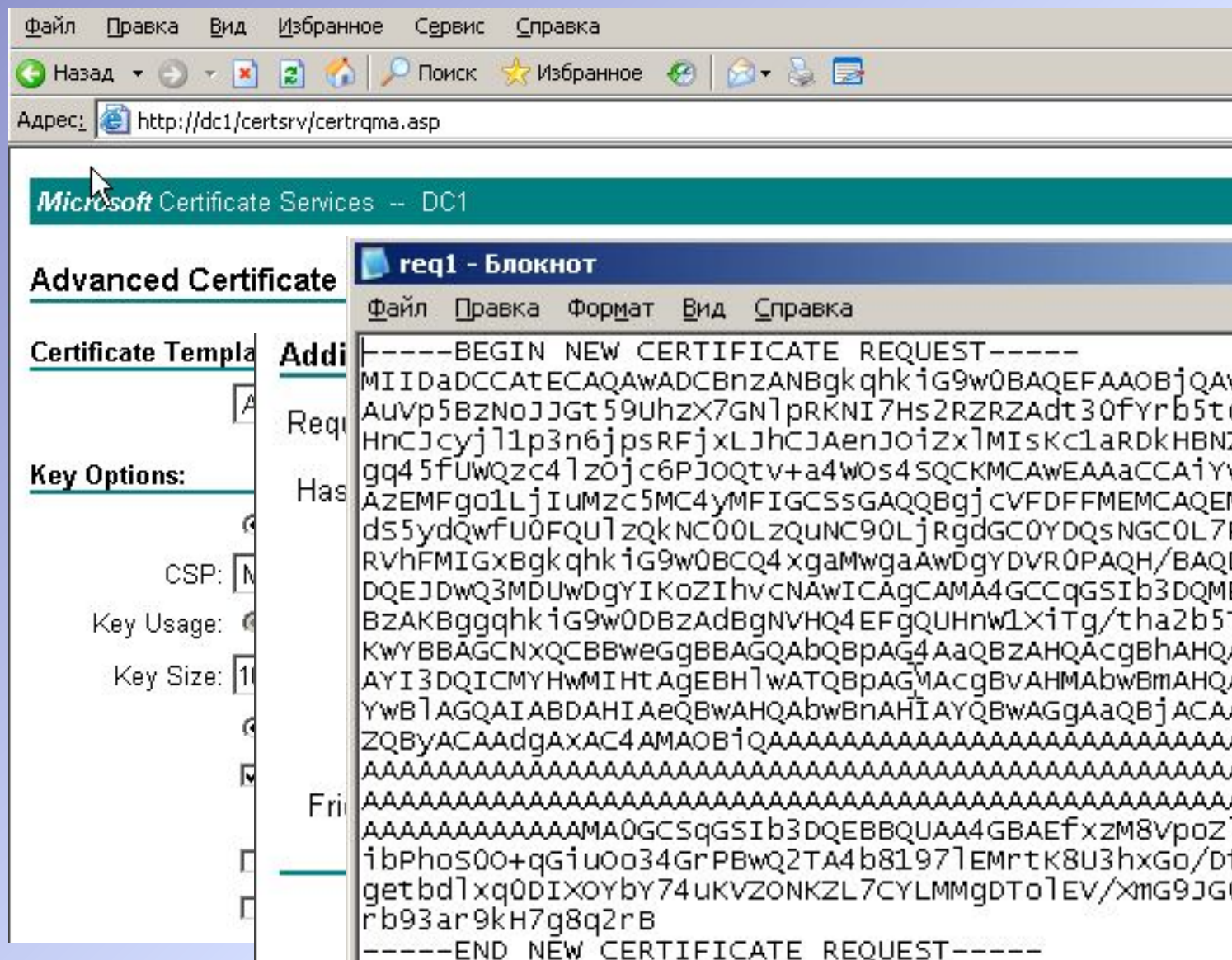
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see [Certificate Services Documentation](#).

**Select a task:**

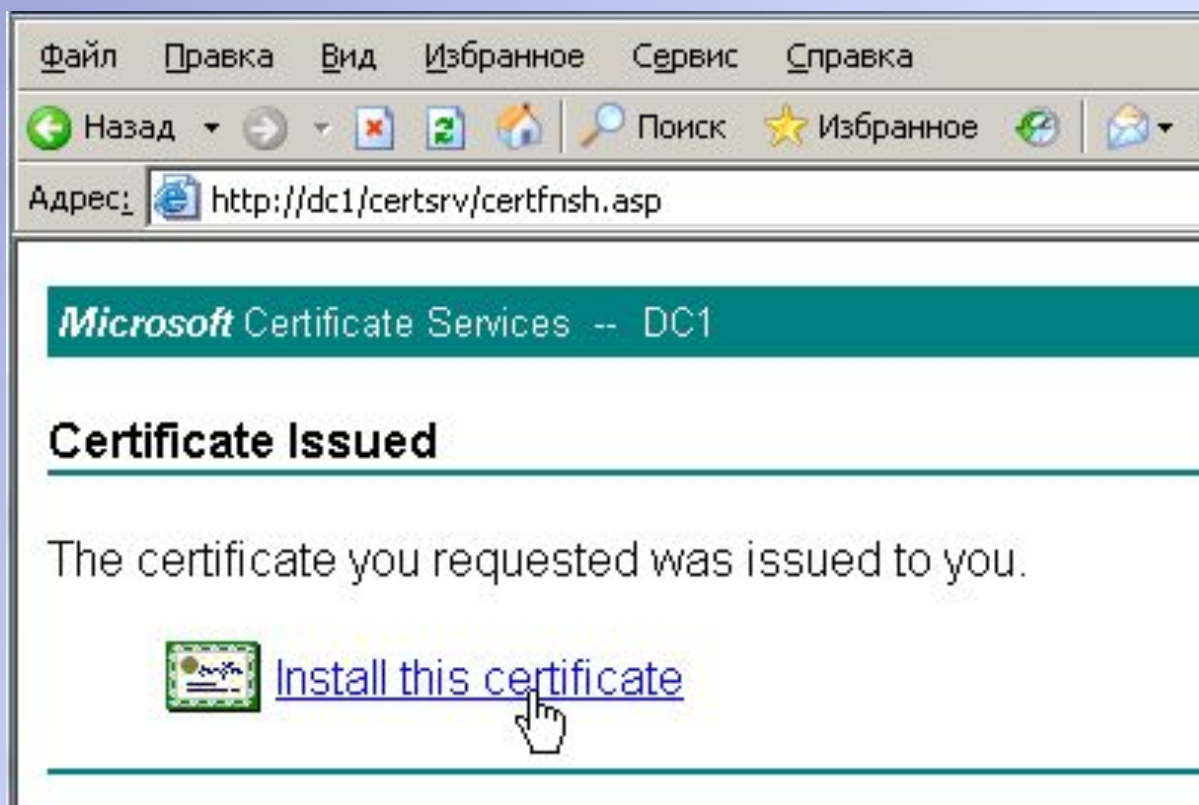
- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

# Детали запроса





# Установка готового сертификата



# Личные сертификаты

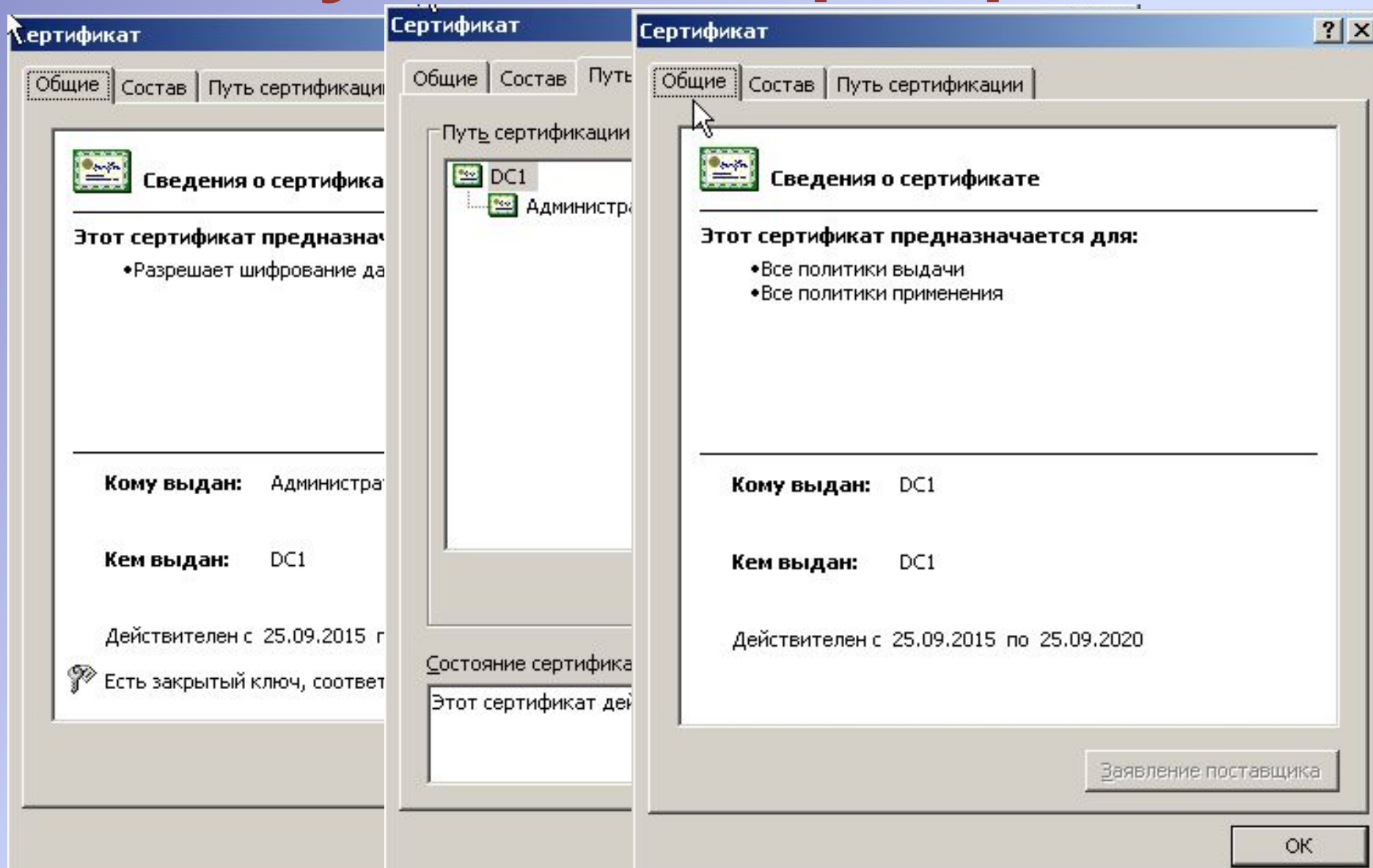
Консоль 1 - [Корень консоли\Сертификаты - текущий пользователь\Личные\Сертификаты]

Консоль Действие Вид Избранное Окно Справка

← → ↗ ↖ ↕ ↘ ↙ ↻ ↺ ↻ ↺

Корень консоли	Кому выдан	Кем выдан	Срок действия	Назначения
[-] Сертификаты - текущий пользователь	Администратор	DC1	24.09.2016	Файловая система EFS
[-] Личные	Администратор	Администра...	12.03.2013	Восстановление файлов
[-] Сертификаты	Администратор	DC1	25.09.2017	Восстановление файлов
[+] Доверенные корневые центры сертификации	Администратор	DC1	24.09.2016	Подписывание списка доверия (M)
[+] Доверительные отношения				
[+] Промежуточные центры сертификации				
[+] Объект пользователя				
[+] Доверенные издатели				
[+] Сертификаты, к которым относятся доверительные отношения				
[+] Сторонние корневые центры сертификации				
[+] Доверенные лица				
[+] Запросы заявок на сертификаты				

# Полученный сертификат





# Доверенные сертификаты

Консоль 1 - [Корень консоли\Сертификаты - текущий пользователь\Доверенные корневые цен...

Консоль Действие Вид Избранное Окно Справка

Корень консоли

- Сертификаты - текущий пользователь
  - Личные
  - Доверенные корневые центры сертификации
    - Сертификаты
  - Доверительные отношения в предприятии
  - Промежуточные центры сертификации
  - Объект пользователя Active Directory
  - Доверенные издатели
  - Сертификаты, к которым нет доверия
  - Сторонние корневые центры сертификации
  - Доверенные лица
  - Запросы заявок на сертификат

Кому выдан	Кем выдан	Срок действия	На...
Copyright (c) 1997 M...	Copyright (c)...	31.12.1999	Ус...
DC1	DC1	13.03.2011	Пр...
DC1	DC1	25.09.2020	<В...
DC1	DC1	25.09.2020	<В...
DC1.sapr.etu.ru	DC1.sapr.et...	13.03.2011	Пр...
DC2	DC2	13.03.2011	Пр...
Deutsche Telekom R...	Deutsche Tel...	10.07.2019	За...
Deutsche Telekom R...	Deutsche Tel...	10.07.2019	За...
DST (ANX Network) CA	DST (ANX Ne...	09.12.2018	За...
DST (NRF) RootCA	DST (NRF) R...	08.12.2008	За...
DST (UPS) RootCA	DST (UPS) R...	07.12.2008	За...
DST RootCA X1	DST RootCA X1	28.11.2008	За...
DST RootCA X2	DST RootCA X2	28.11.2008	За...
DSTCA E1	DSTCA E1	10.12.2018	За...
DSTCA E2	DSTCA E2	09.12.2018	За...
DST-Entrust GTI CA	DST-Entrust ...	09.12.2018	За...

Хранилище Доверенные корневые центры сертификации содержит 109 сертификата

# **Защита компьютерной информации. Защита информации на уровне кода**

Горячев Александр Вадимович  
Доцент кафедры Информационной  
безопасности

[Avgoriachev@etu.ru](mailto:Avgoriachev@etu.ru)

# модель эшелонированной обороны

Физический  
доступ

Политики, процедуры,  
осведомленность

Хранилища

Хранилища

Обработка

Приложения Обновления Контроль

ОС/.NET Обновления Аутентификация

Антивирус

AD

PKI

Передача

Intranet

Internet

# Обновления – какие проблемы?

- Ошибки изначального кода
- Уязвимости

## Как бороться?

- «Заплатки» (Patch)
- Замена кода



# Все ли изменения нужны?

- Security – ДА!!!
- ...
- Feature-pack – Нет!

# Центр обновлений Windows

Параметры

Главная

Найти параметр

Обновление и безопасность

Центр обновления Windows

Оптимизация доставки

Безопасность Windows

Служба архивации

Устранение неполадок

Восстановление

Активация

Поиск устройства

Для разработчиков

Программа предварительной оценки Windows

Центр обновления Windows

У вас установлены все последние обновления

Время последней проверки: сегодня, 14:18

Проверить наличие обновлений

Просмотреть необязательные обновления

Обновление функций до Windows 10, версия 21H2

Доступна версия Windows с новыми функциями и улучшениями системы безопасности. Когда вы будете готовы установить обновление, выберите пункт "Загрузить и установить".

Загрузить и установить   Ознакомьтесь с содержимым этого обновления

Этот компьютер в настоящее время не соответствует минимальным требованиям к системе для запуска Windows 11

Получите дополнительные сведения и узнайте, что можно сделать в приложении "Проверка работоспособности ПК".

Проверка работоспособности ПК

Приостановить обновления на 7 дн.

Для изменения периода приостановки перейдите в раздел дополнительных параметров

Изменить период активности

С 8:00 до 17:00

# Типы атак

Атака	Характеристики
Eavesdropping	<ul style="list-style-type: none"><li>• «Подсматривание» коммуникаций.</li></ul>
Data Modification	<ul style="list-style-type: none"><li>• Изменение пакетов данных.</li></ul>
Identity Spoofing	<ul style="list-style-type: none"><li>• Атака с чужого адреса или под чужой личиной.</li></ul>
Password Based	<ul style="list-style-type: none"><li>• Получение чужого пароля.</li></ul>
Denial of Service	<ul style="list-style-type: none"><li>• Прекращение нормальной работы объекта-цели.</li></ul>
Man in the Middle	<ul style="list-style-type: none"><li>• «Испорченный телефон».</li></ul>
Compromised Key	<ul style="list-style-type: none"><li>• Добыча чужого ключа.</li></ul>
Sniffer	<ul style="list-style-type: none"><li>• Мониторинг сети.</li></ul>
Application Layer	<ul style="list-style-type: none"><li>• Атака на приложение.</li></ul>



# Phishing

Получение паролей, PIN-кодов и пр.

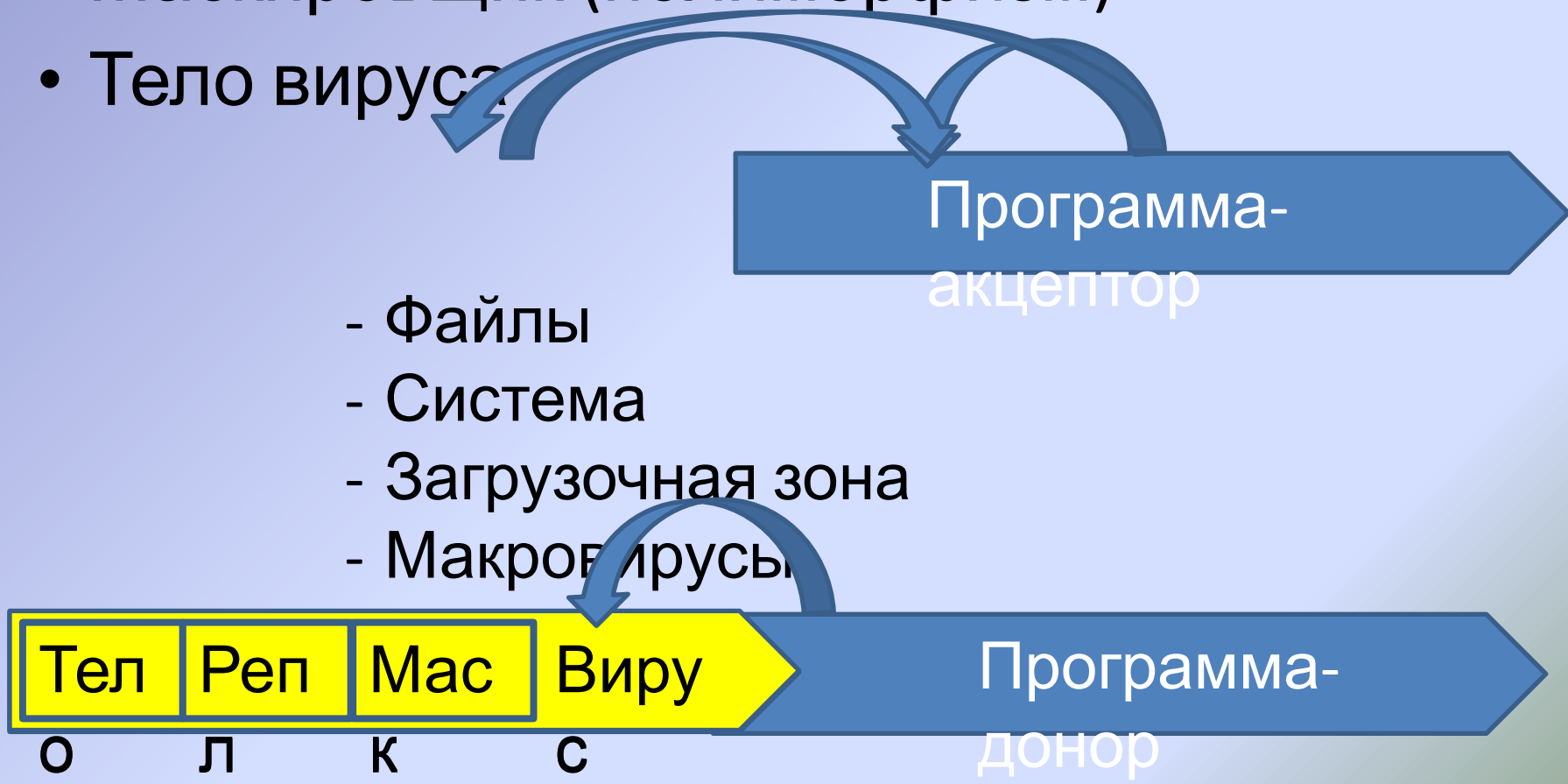
- Пассивное наблюдение
- Спровоцировать передачу неавторизованному участнику
- Проникновение с кражей

# USB-флэш атака

- Из 30 разбросанных по территории предприятия флэшек 20 «откликнулись» в течении часа

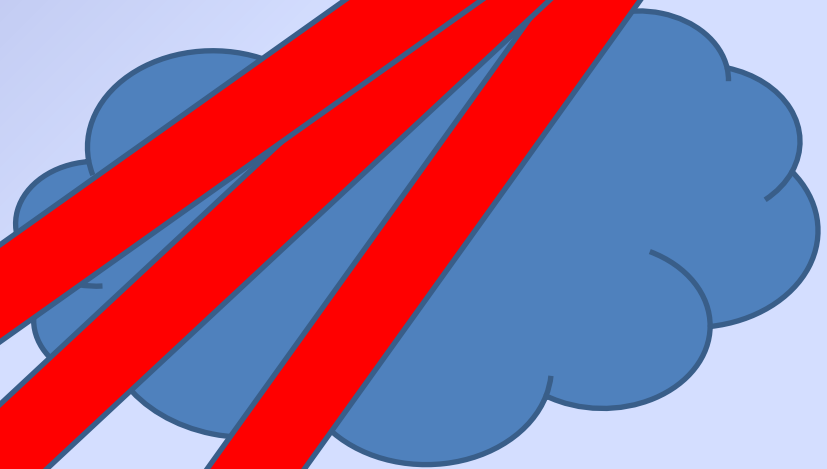
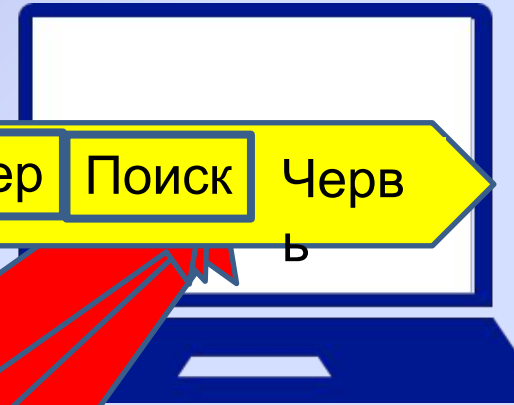
# Вирус

- Репликатор
- Маскировщик (полиморфизм)
- Тело вируса



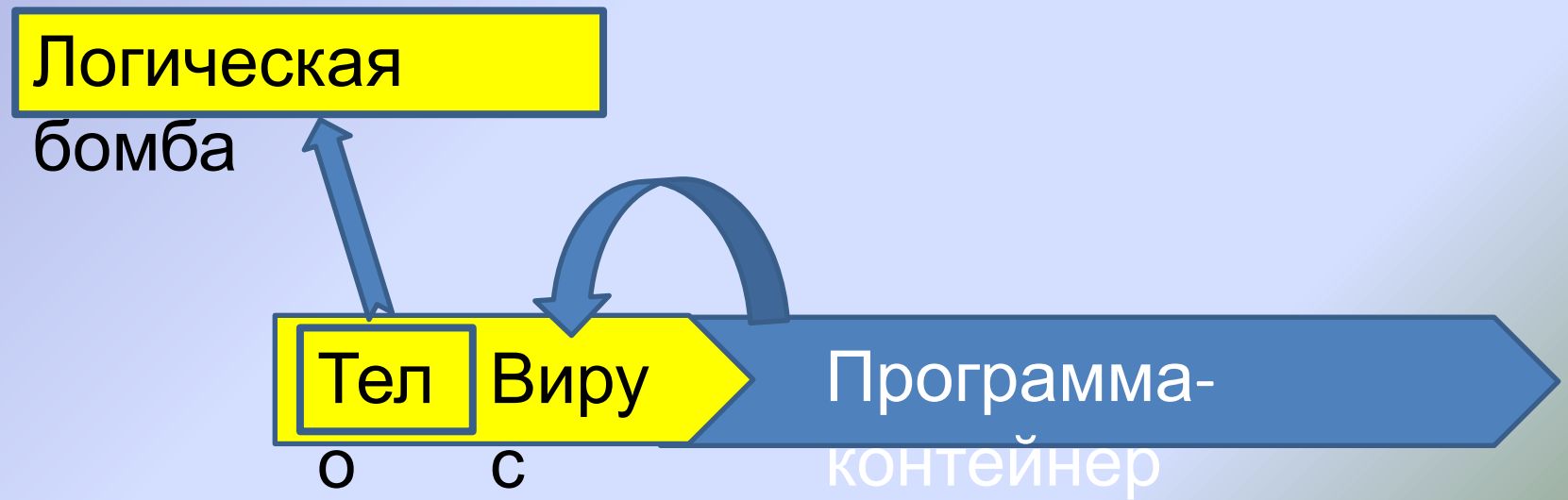
# Черви

- Средство проникновения
- Инсталлятор
- Средство поиска
- Сканнер
- Тело червя



# Троян

- Контейнер – полезная программа
- Тело трояна



# Root Kit

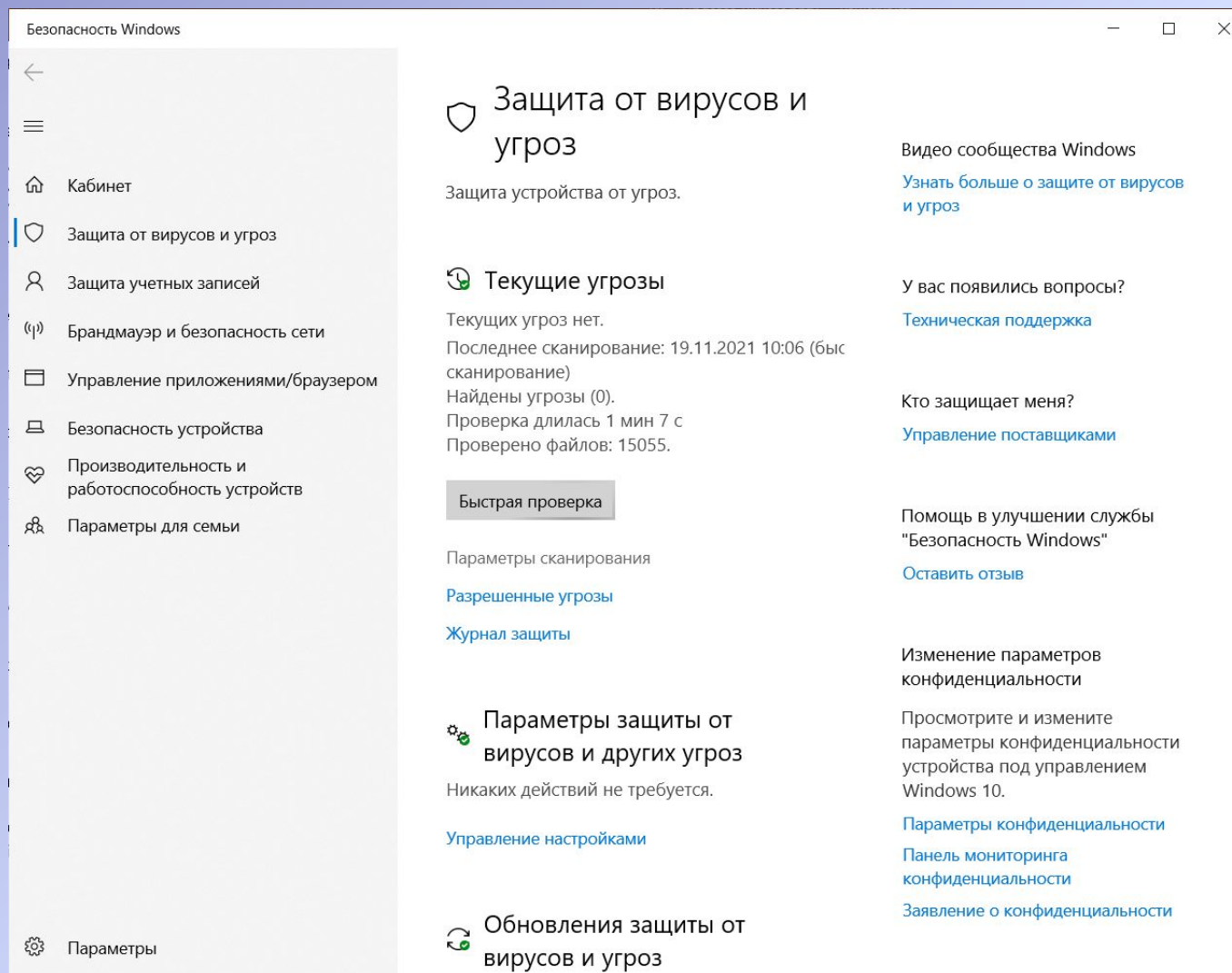
- Встраивается на уровне драйверов операционной системы
- Очень сложно обнаружить

# Методы обнаружения угроз ПО

- Обнаружение по маске – сканирование
- Анализ логов
- Обнаружение по маске при запуске ПО
- Поведенческий анализ «на лету»
- Принцип минимальных привилегий



# Защита от вирусов и...



Безопасность Windows

←

☰

🏠 Кабинет

🛡️ **Защита от вирусов и угроз**

👤 Защита учетных записей

🔒 Брандмауэр и безопасность сети

📁 Управление приложениями/браузером

💻 Безопасность устройства

💓 Производительность и работоспособность устройств

👨‍👩‍👧‍👦 Параметры для семьи

⚙️ Параметры

## 🛡️ Защита от вирусов и угроз

Защита устройства от угроз.

### 🔄 Текущие угрозы

Текущих угроз нет.  
Последнее сканирование: 19.11.2021 10:06 (быстрое сканирование)  
Найдены угрозы (0).  
Проверка длилась 1 мин 7 с  
Проверено файлов: 15055.

**Быстрая проверка**

Параметры сканирования

[Разрешенные угрозы](#)

[Журнал защиты](#)

### ⚙️ Параметры защиты от вирусов и других угроз

Никаких действий не требуется.

[Управление настройками](#)

### 🔄 Обновления защиты от вирусов и угроз

Видео сообщества Windows

[Узнать больше о защите от вирусов и угроз](#)

У вас появились вопросы?

[Техническая поддержка](#)

Кто защищает меня?

[Управление поставщиками](#)

Помощь в улучшении службы "Безопасность Windows"

[Оставить отзыв](#)

Изменение параметров конфиденциальности

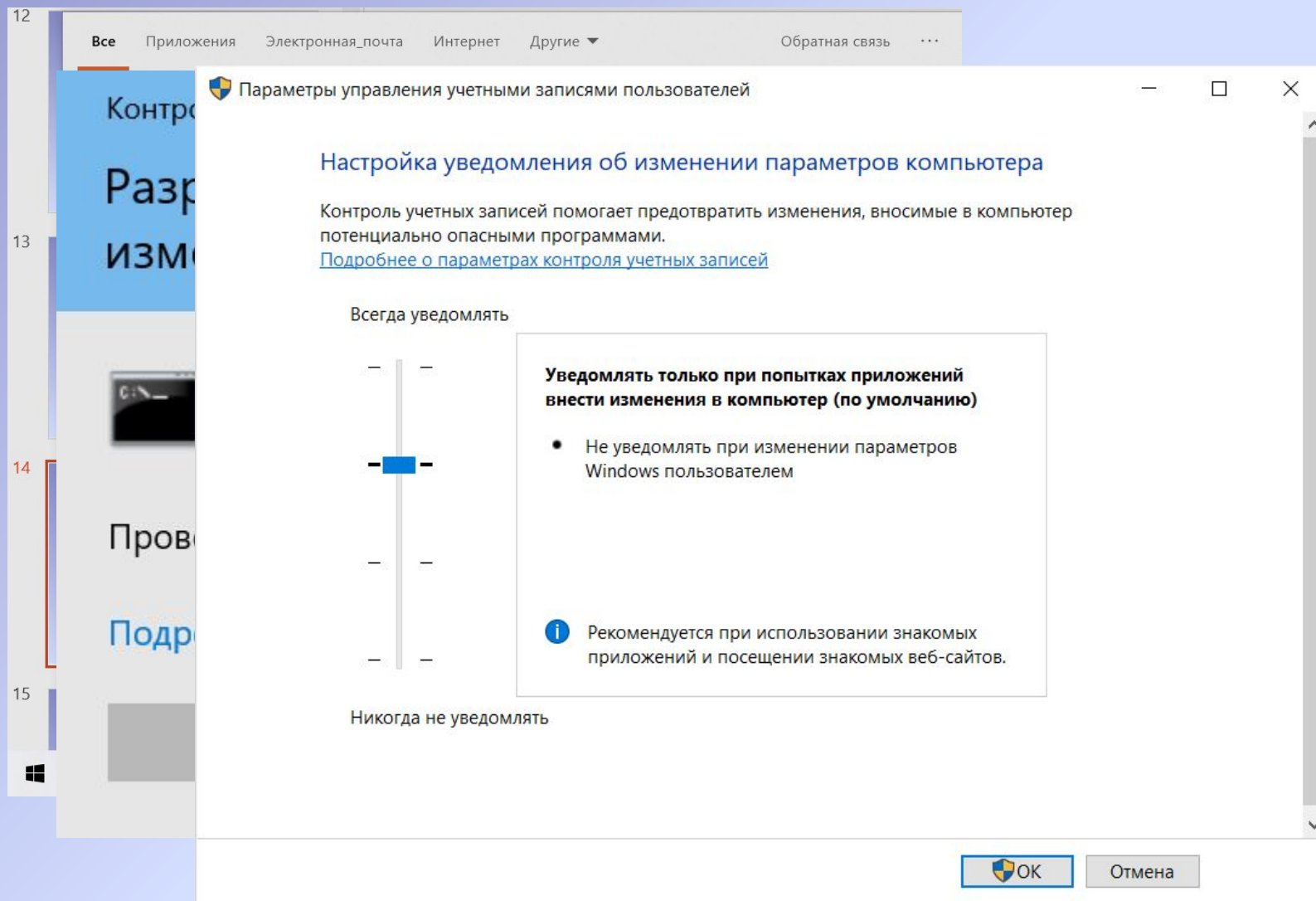
Просмотрите и измените параметры конфиденциальности устройства под управлением Windows 10.

[Параметры конфиденциальности](#)

[Панель мониторинга конфиденциальности](#)

[Заявление о конфиденциальности](#)

# Контроль доступа (UAC)

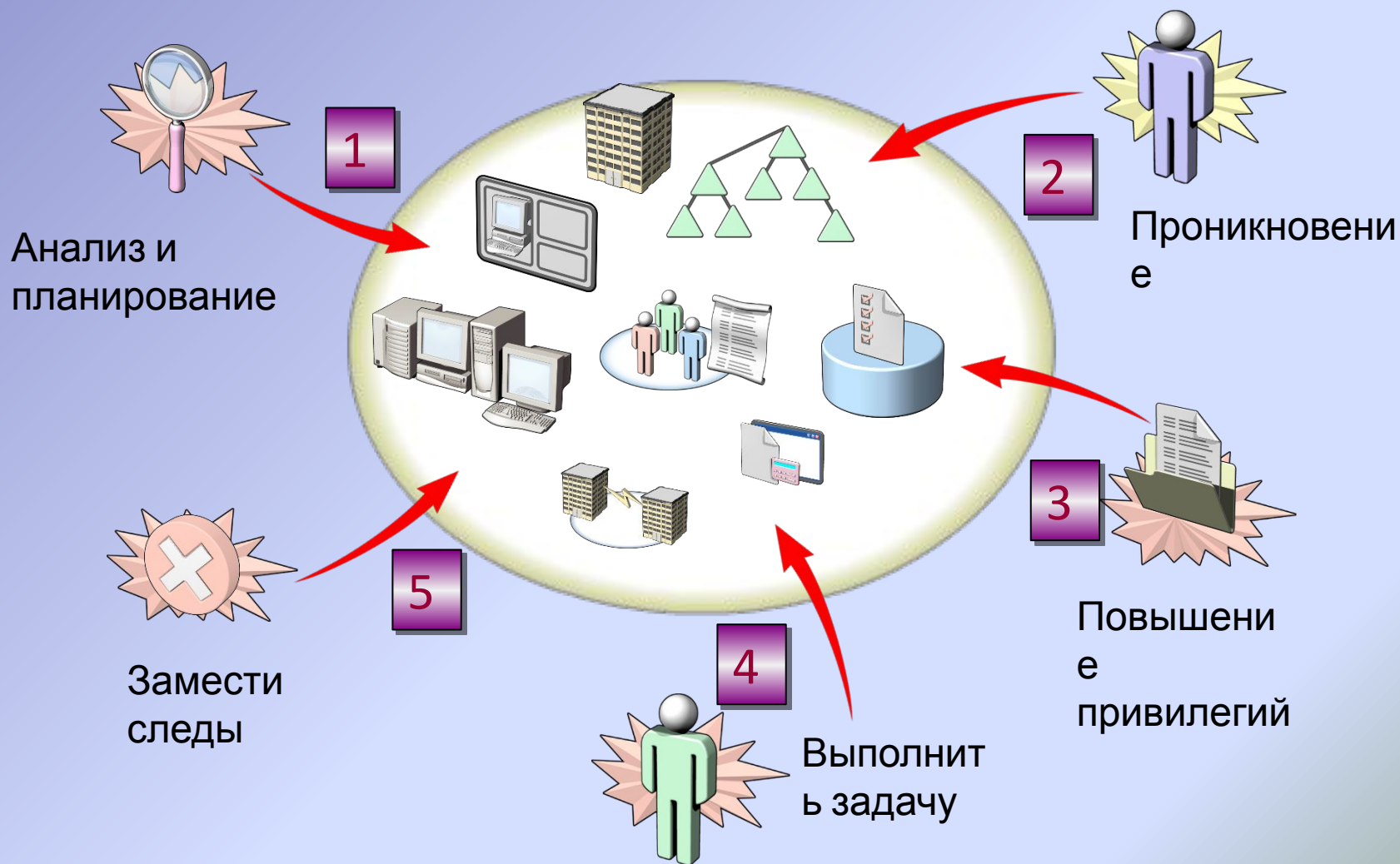


# **Обеспечение качества кода в ходе разработки**

# Модель угроз STRIDE

Spoofing	Работа от чужого имени
Tampering	Неавторизованное изменение данных
Repudiation	Возможность «отбрехаться» от того, что что-то сделал нехорошее
Information disclosure	Несанкционированное раскрытие информации
Denial of service	Приложение делается недоступным
Elevation of privilege	Получение полномочий привилегированного пользователя

# Анатомия атаки



# Борьба...

Категории	Примеры мер
<b>Spoofing</b>	<ul style="list-style-type: none"><li>• Строгая аутентификация.</li><li>• Не хранить секреты на виду.</li><li>• Не передавать секреты открытым текстом.</li></ul>
<b>Tampering</b>	<ul style="list-style-type: none"><li>• Подписывать данные.</li><li>• Использовать строгую аутентификацию</li><li>• Использовать устойчивые протоколы.</li></ul>
<b>Repudiation</b>	<ul style="list-style-type: none"><li>• Аудит!!!.</li><li>• Подписывать.</li></ul>
<b>Information disclosure</b>	<ul style="list-style-type: none"><li>• Использовать строгую аутентификацию.</li><li>• Защищать коммуникации.</li><li>• Не хранить секреты на виду.</li></ul>
<b>Denial of service</b>	<ul style="list-style-type: none"><li>• Использовать технологию контроля полосы трафика.</li><li>• Контролировать входящий трафик.</li></ul>
<b>Elevation of privilege</b>	<ul style="list-style-type: none"><li>• Принцип минимальных привилегий.</li></ul>

# Модель эшелонированной обороны

Физический  
доступ

Политики, процедуры,  
осведомленность

Хранение

ACL EFS Bitlocker

Backup Mirror RAID SC

Обработка

APPs Antivirus Updates

OS/.NET Antispyware Autentification HIDS-HIPS

PKI

AD

Передача

Intranet Routing IPsec RMS NIDS-NIPS

Internet Firewall VPN NAP