Служба каталога Active Directory (AD)

Горячев Александр Вадимович
Доцент кафедры
Информационной безопасности
avgoriachev@etu.ru

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

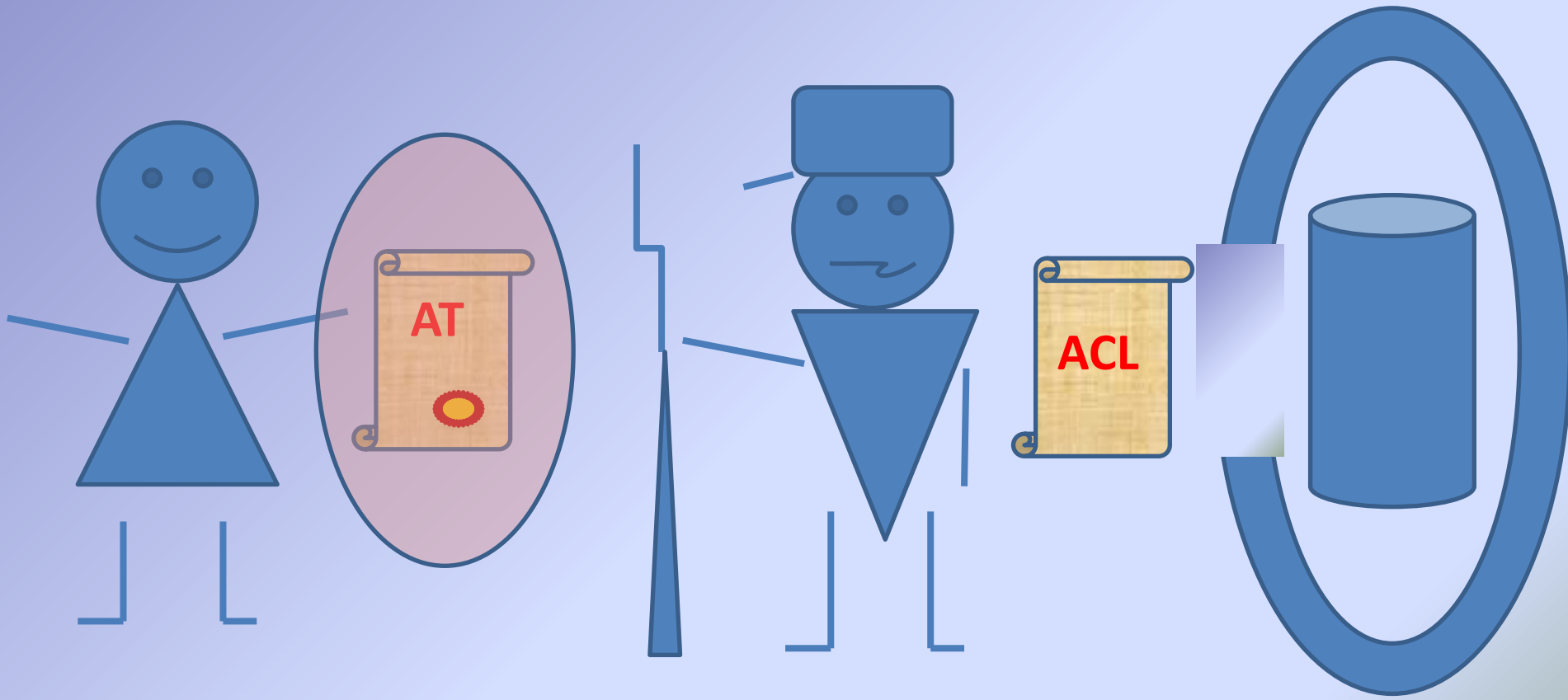
AD

Передача

Intranet Routing IPSec RMS NIDS-NIPS

Internet Firewall VPN NAP

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

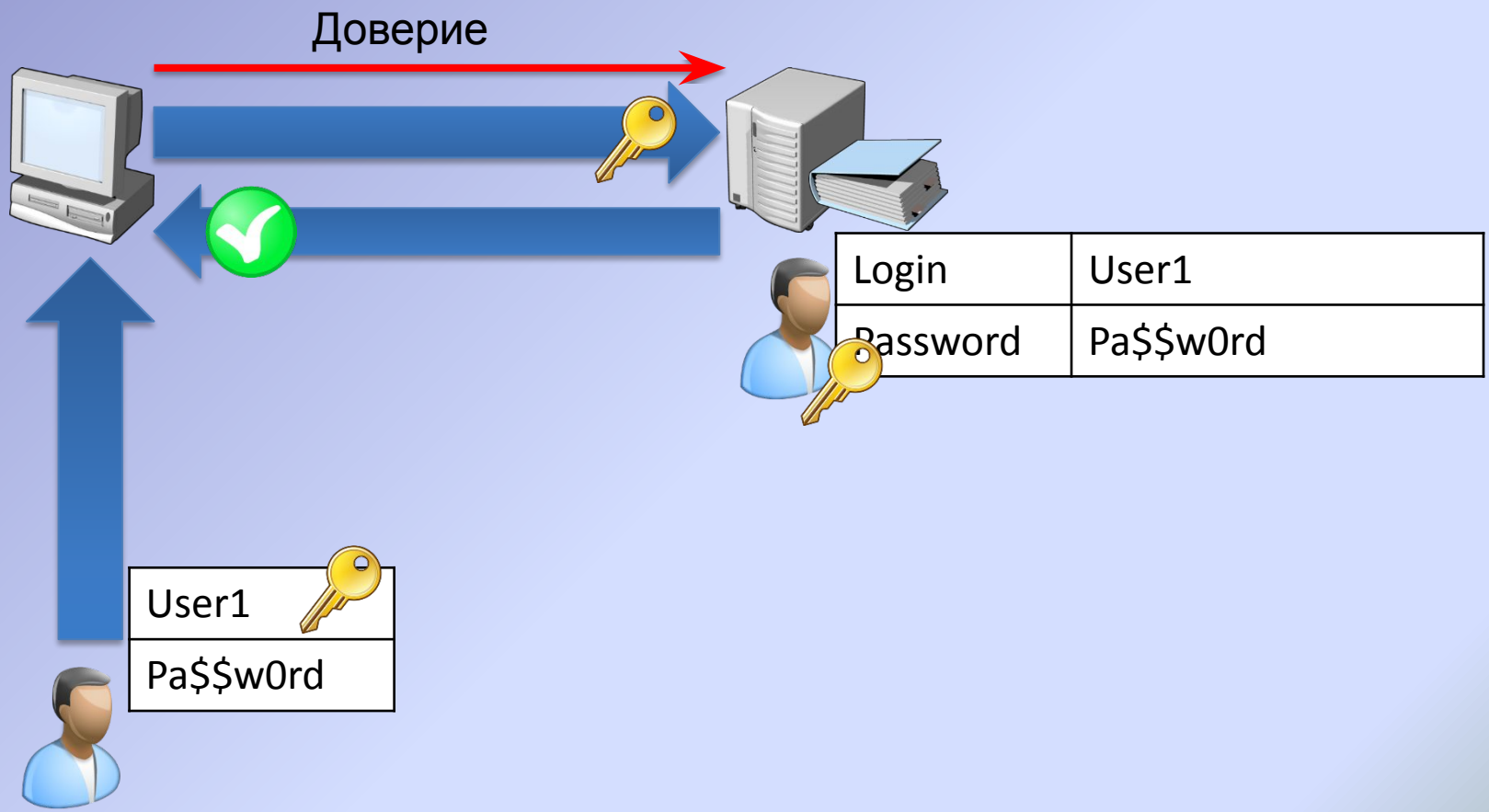
Учётные данные пользователя могут храниться на локальном компьютере

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

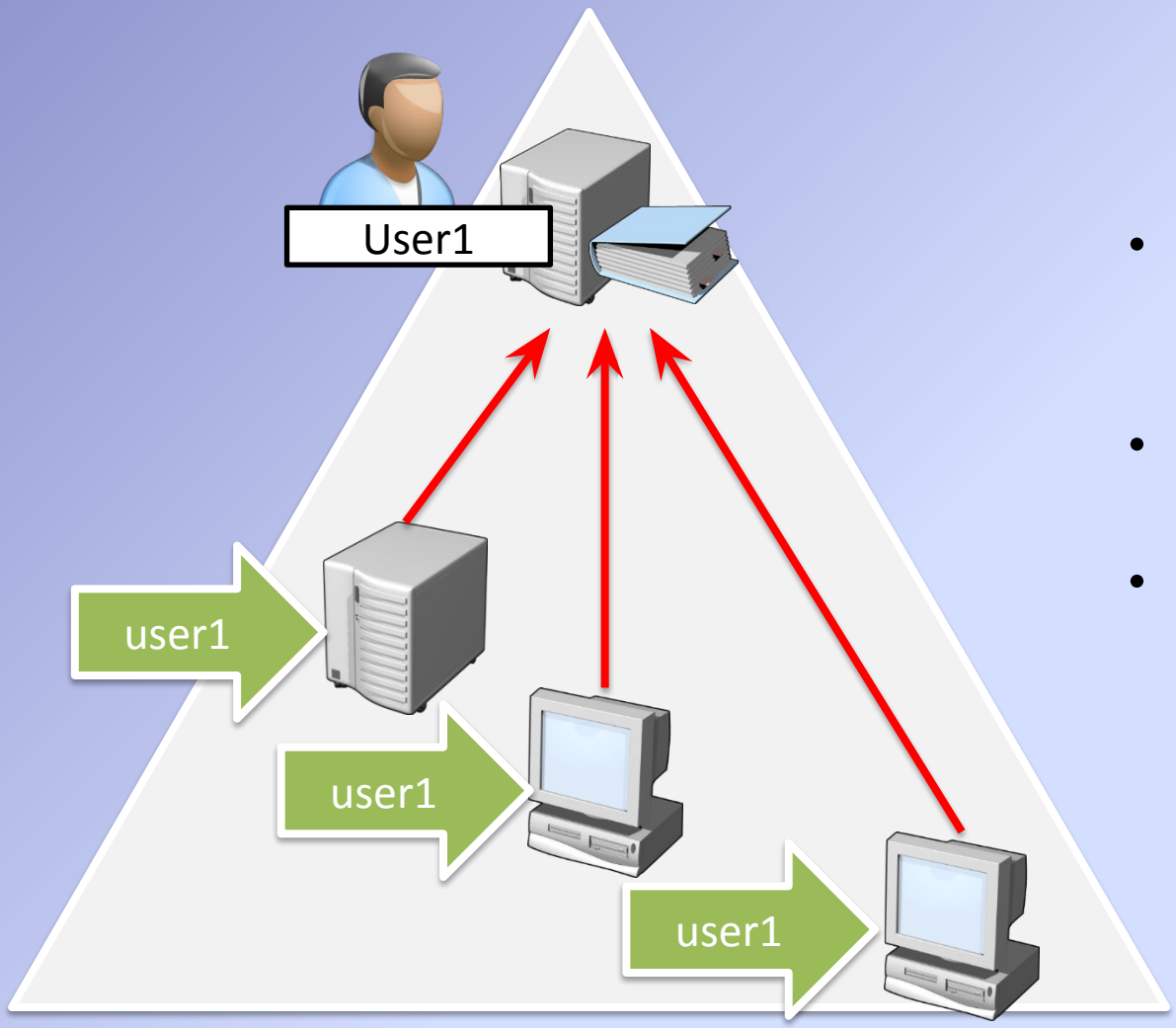
Решение: централизованное хранилище учётных данных

Служба каталогов Active Directory

Отношение доверия



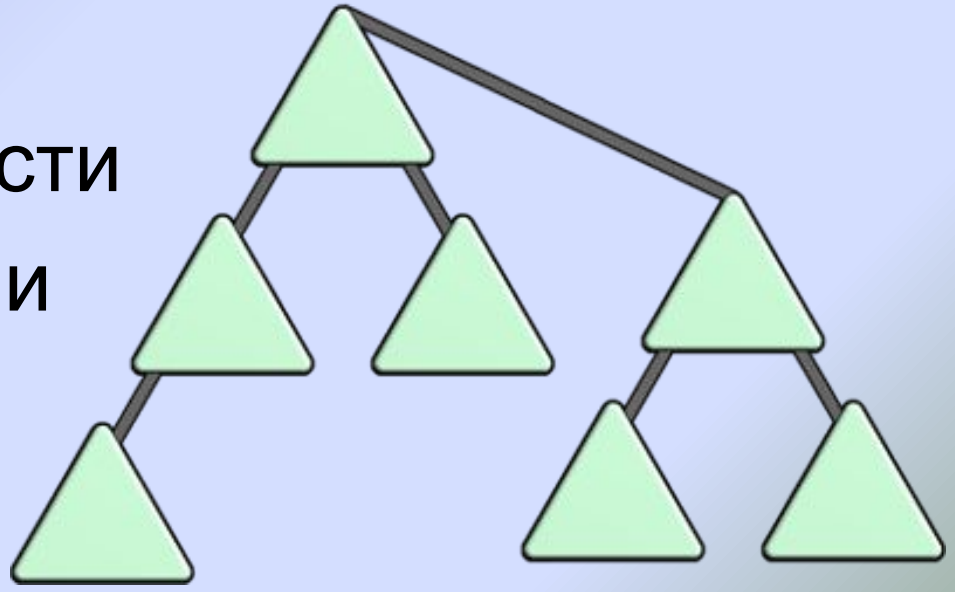
Домен Windows NT



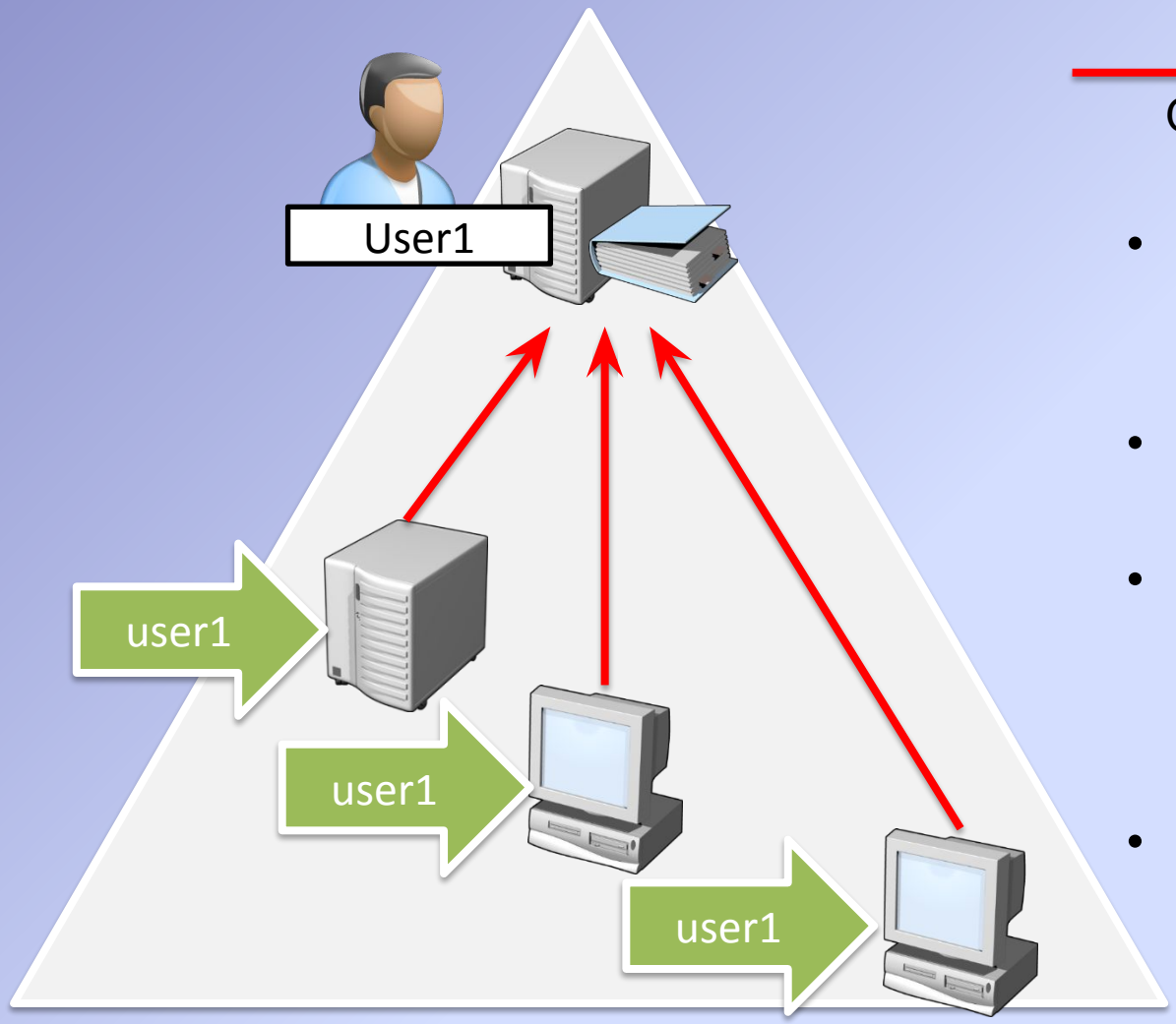
- Требует наличия как минимум одного контроллера домена (PDC)
- Граница репликации домена
- Доверенный источник учётных данных: любой доменный контроллер (PDC и BDC) может провести аутентификацию в домене

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

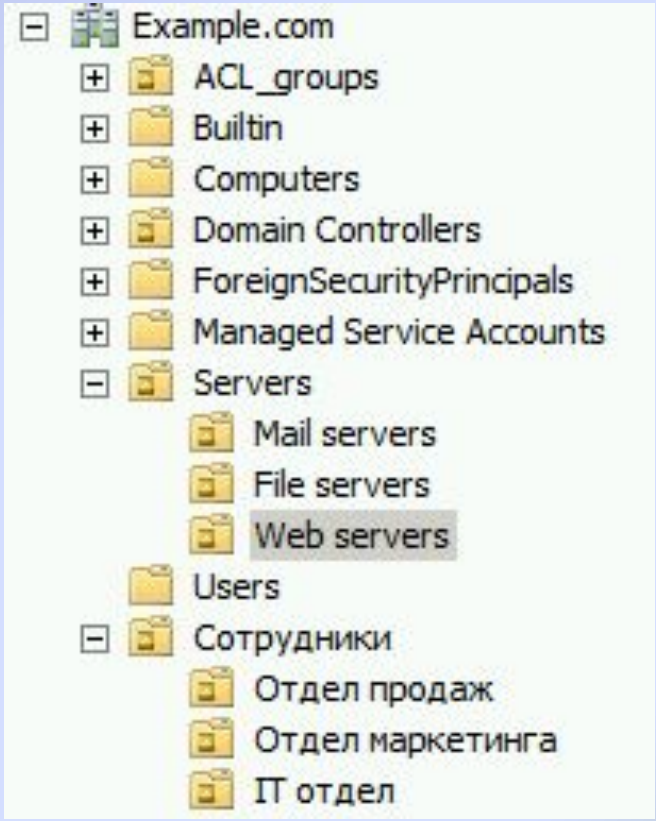


Отношения доверия

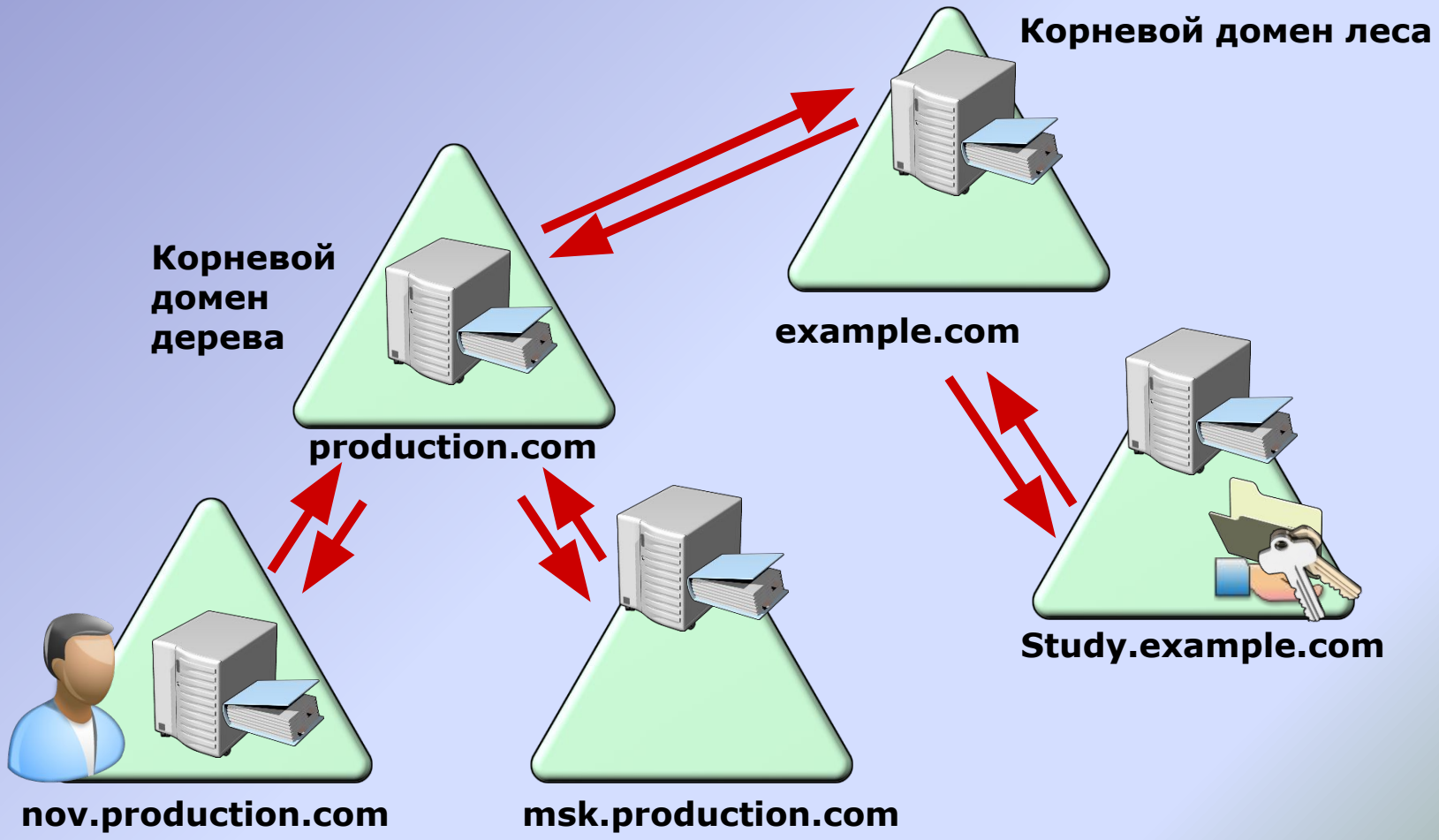
- Требует наличия как минимум одного контроллера домена
- Граница репликации доменного раздела
- Доверенный источник учётных данных: любой DC может провести аутентификацию в домене
- Граница применения политик

Подразделения

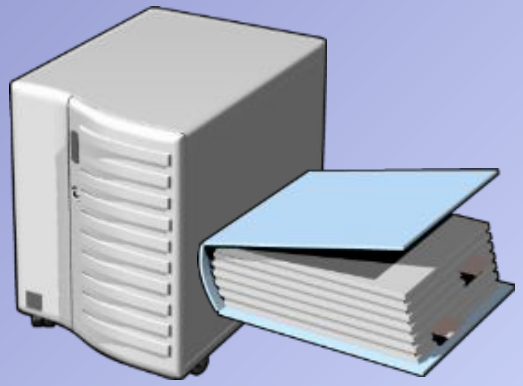
- Объекты
  - Пользователи
  - Компьютеры
- Подразделения
  - Контейнеры для группировки объектов в домене
  - Подразделения создаются:
    - Для делегирования разрешений
    - Для назначения групповых политик



Доверительные отношения в лесу Active Directory



Роль контроллера домена при аутентификации



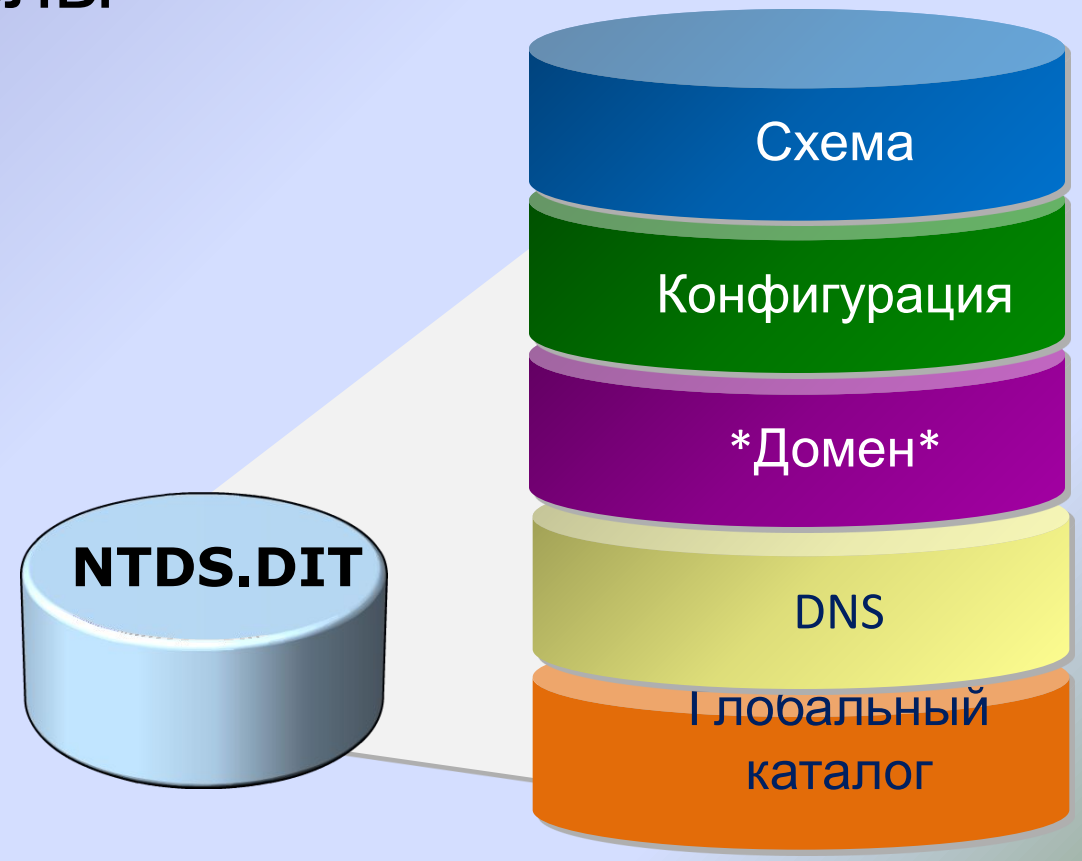
Хранилище учётных данных

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



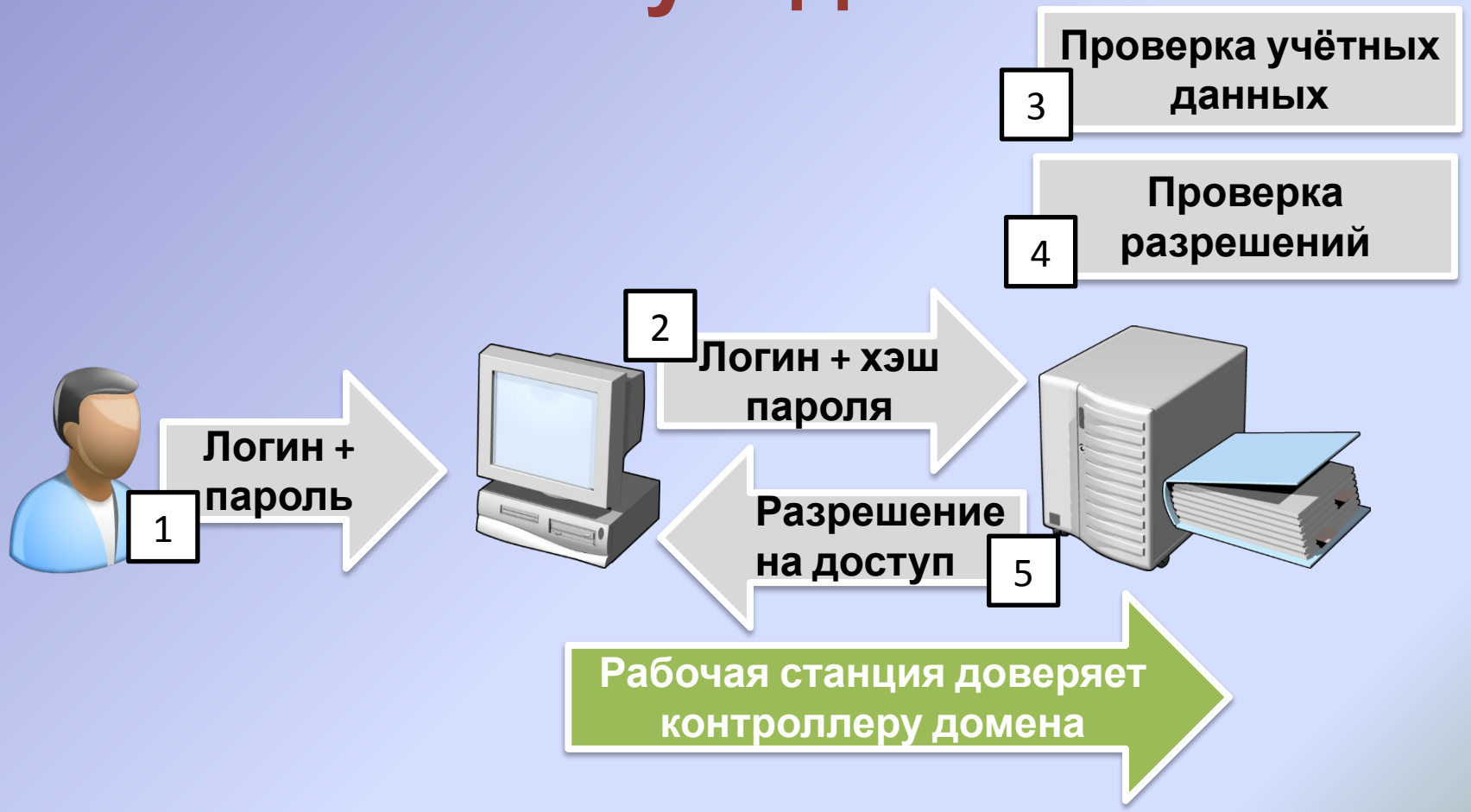
Сайты

- Объекты Active Directory, представляющие сегменты сети с надёжным соединением
  - Ассоциируются с подсетями.
- Внутрисайтовая и межсайтовая репликация
  - Репликация в пределах сайта очень быстр
  - Репликацией между сайтами можно упр
- Локали ция служб
  - Вход в с на ближайшем К

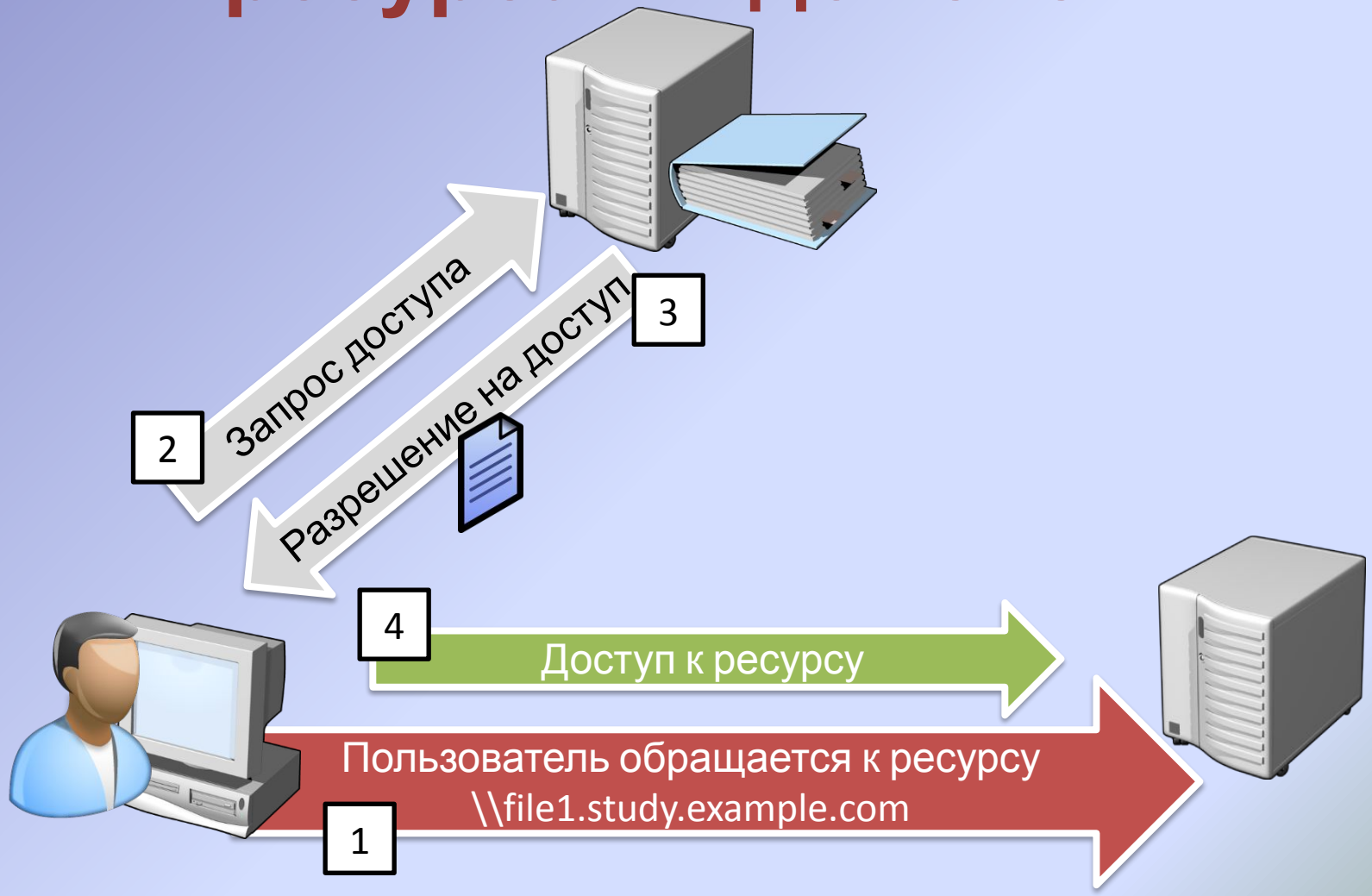
Учётные записи пользователей

- 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

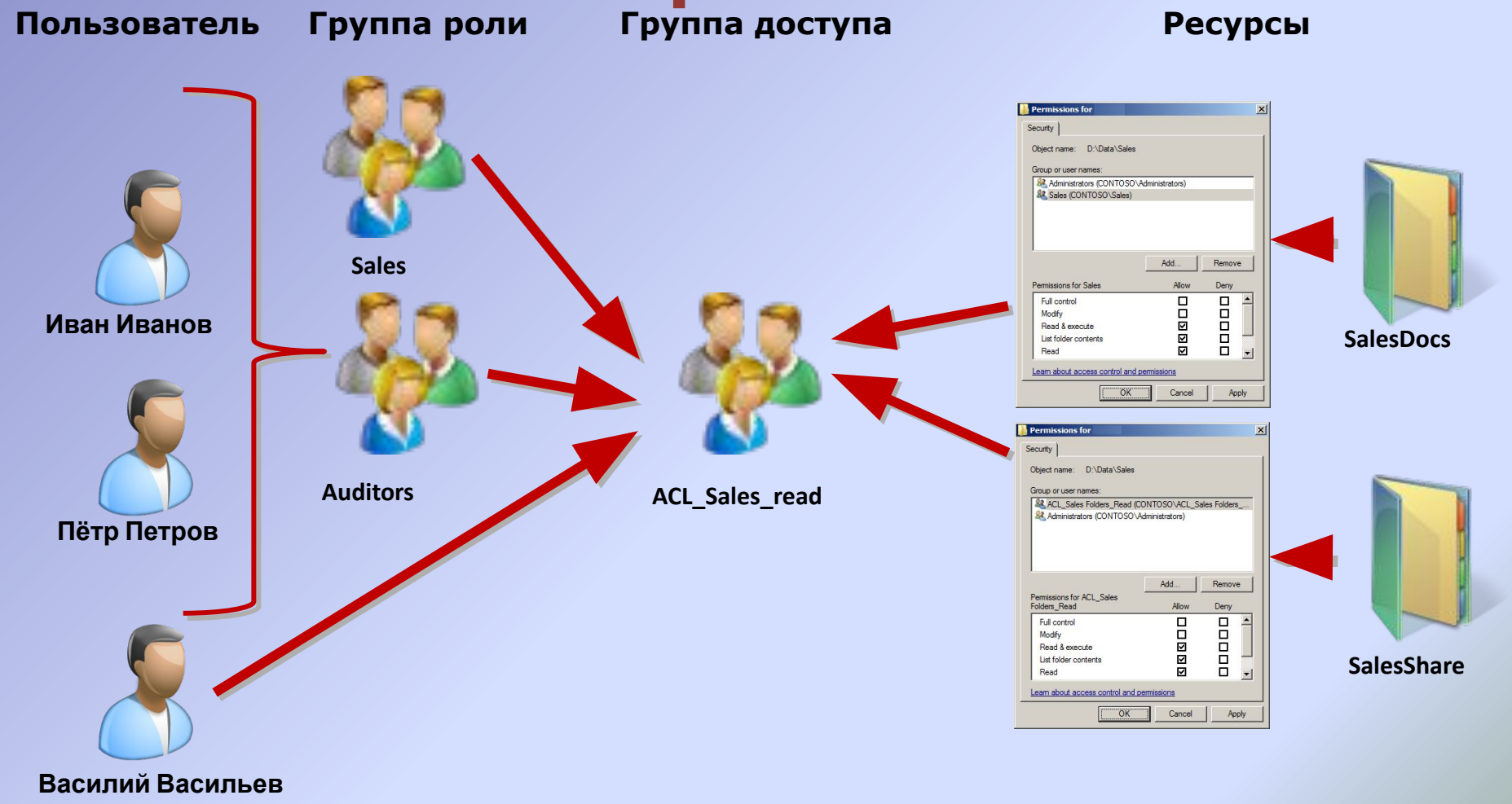
Процесс входа пользователя в систему в домене



Процесс доступа к сетевым ресурсам в домене



Использование групп для контроля доступа на основе ролей



Диапазоны применения групп

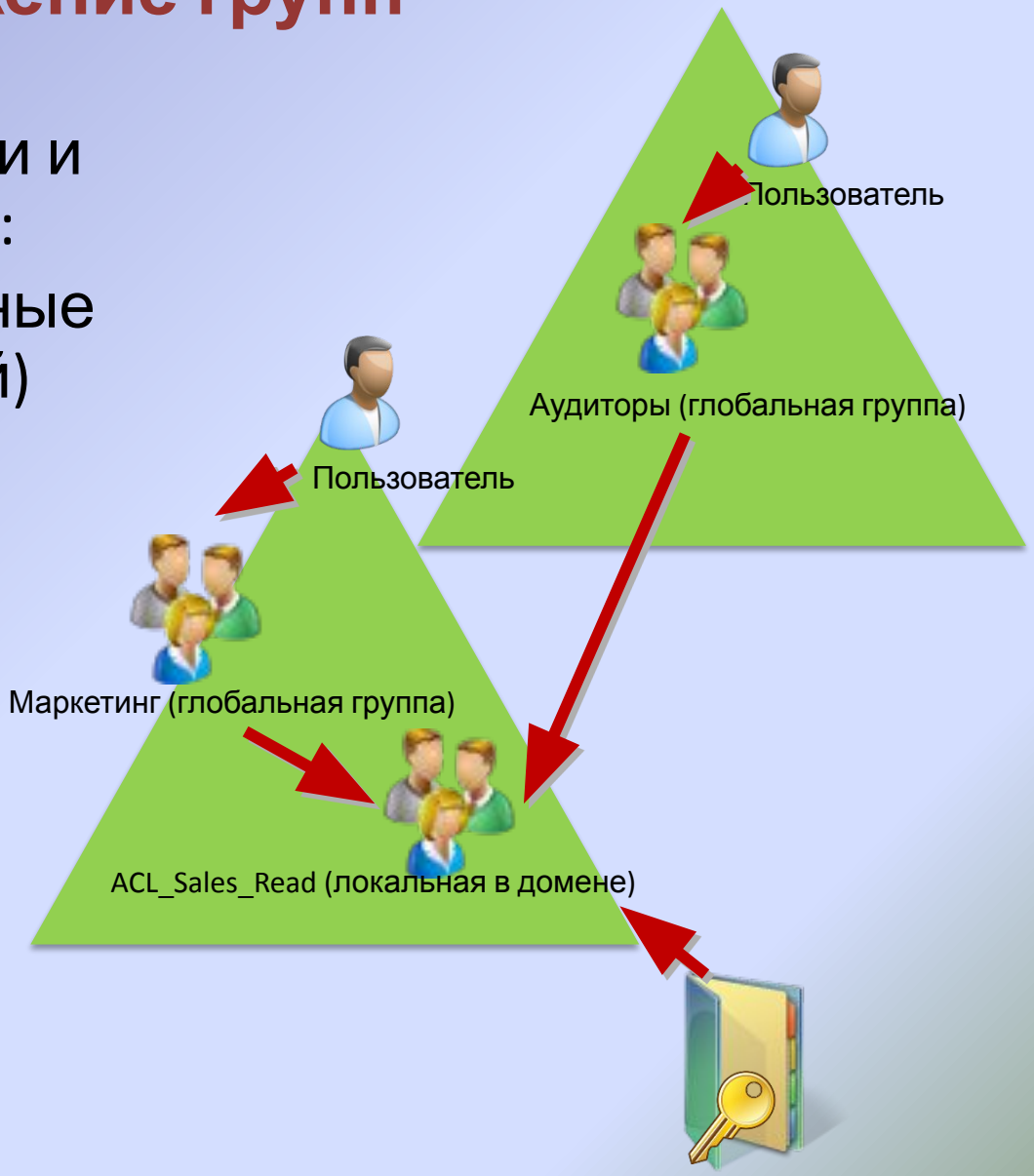
Диапазон	Члены из домена	Члены из другого домена в лесу	Члены из внешнего доверенного домена	Могут предоставлять разрешения
Локальная	U, C, GG, DLG, UG локальные пользователи	U, C, GG, UG	U, C, GG	Только на локальном компьютере
Локальная в домене	U, C, GG, DLG, UG	U, C, GG, UG	U, C, GG	Во всём домене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

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

Вложение групп

- **I**dentities (пользователи и компьютеры) входят в:
- **G**lobal groups (глобальные группы – группы ролей) входят в:
- **D**omain **L**ocal groups (локальные в домене группы)

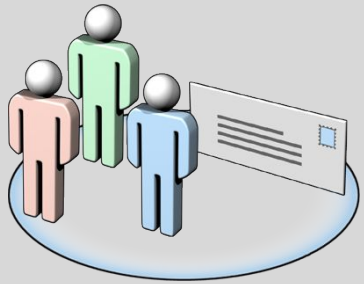
  предоставляют:
- **A**ccess (доступ к ресурсам)
- Мультидоменный лес: IG**U**DLA



Типы групп

Группы распространения

- Используются приложениями электронной почты
- Не имеют идентификатора безопасности

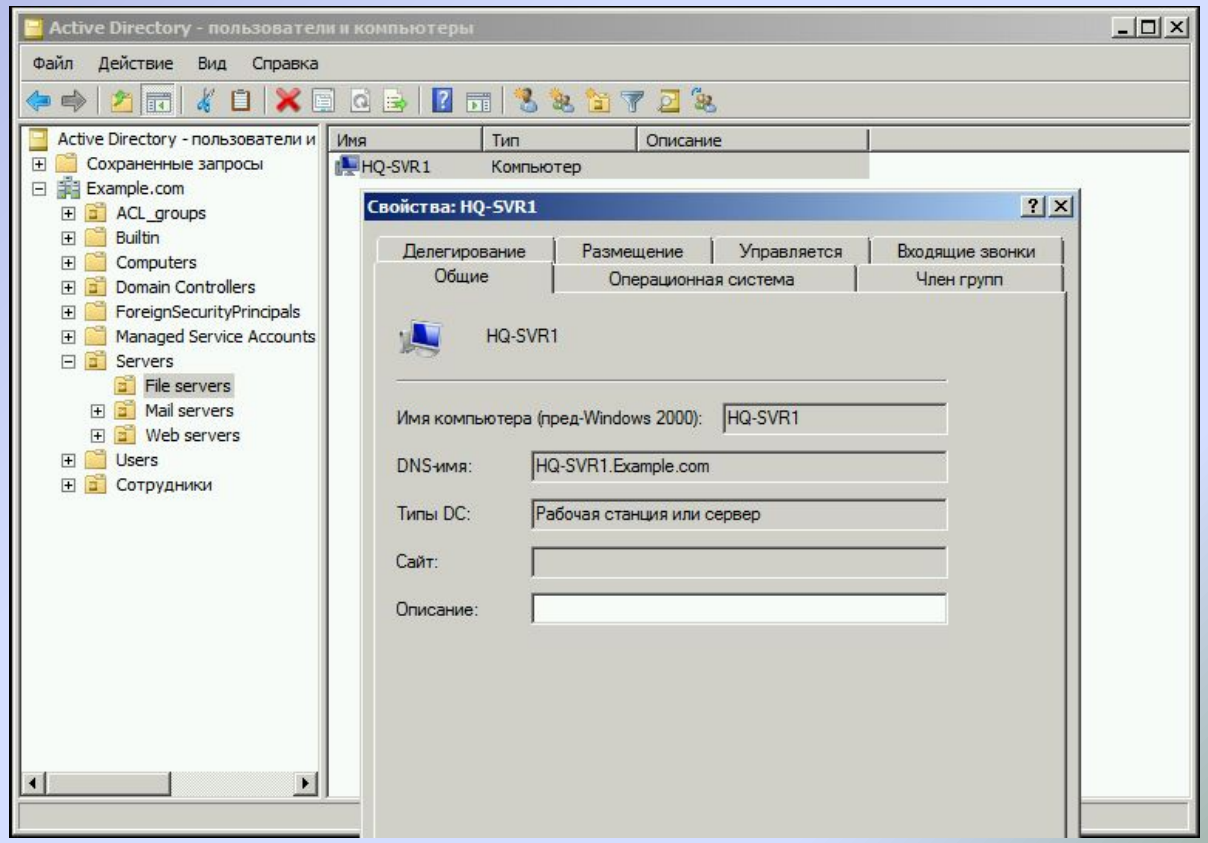


Группы безопасности

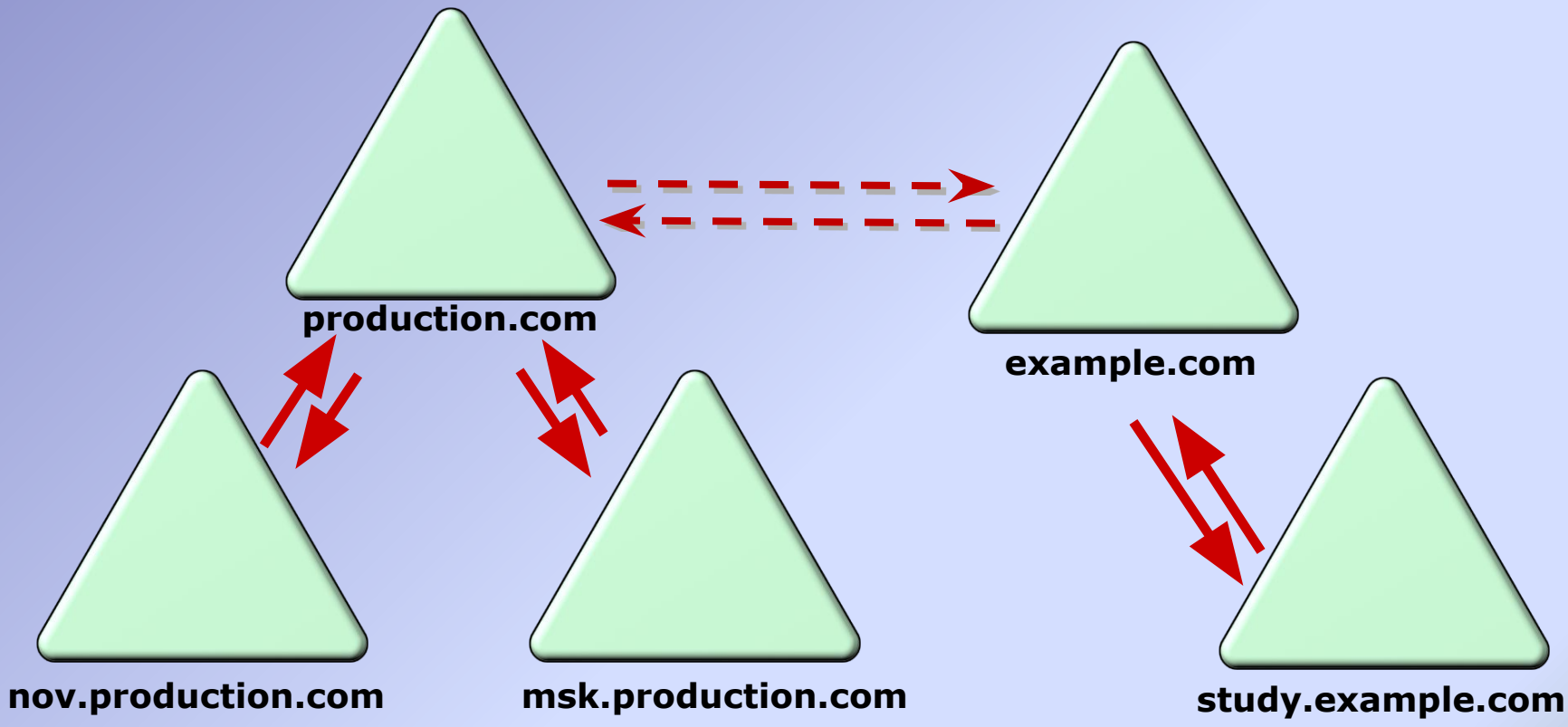
- Имеют идентификатор безопасности, могут быть использованы для контроля доступа
- Также могут использоваться приложениями электронной почты

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

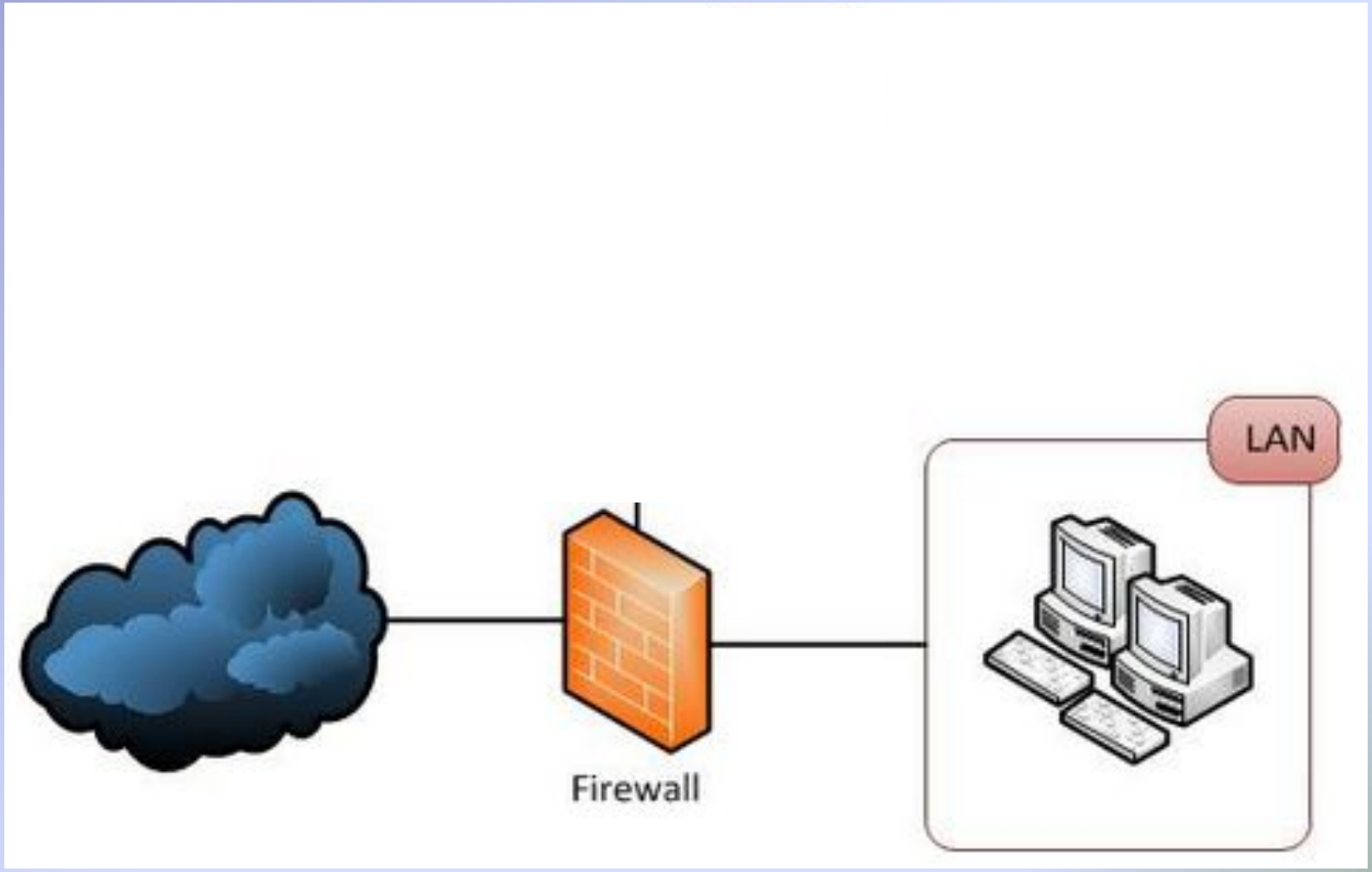
Internet Firewall VPN NAP

Набор технологий

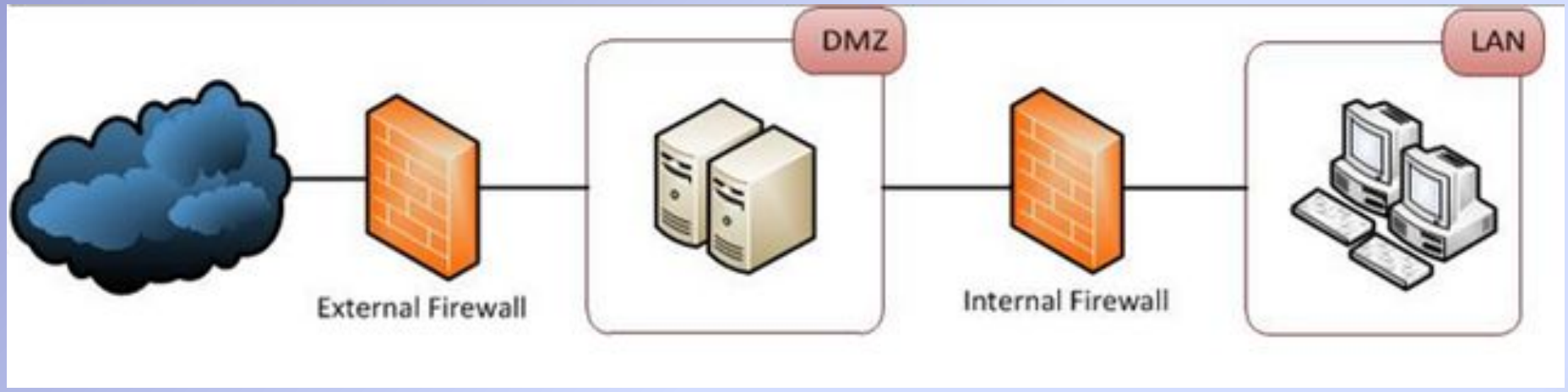
- Proxy 7
- VPN 6
- Контентная фильтрация 5
- Аутентификация 4
- Трансляция сетевых адресов 3
- Пакетные фильтры 2

1

Простые конфигурации

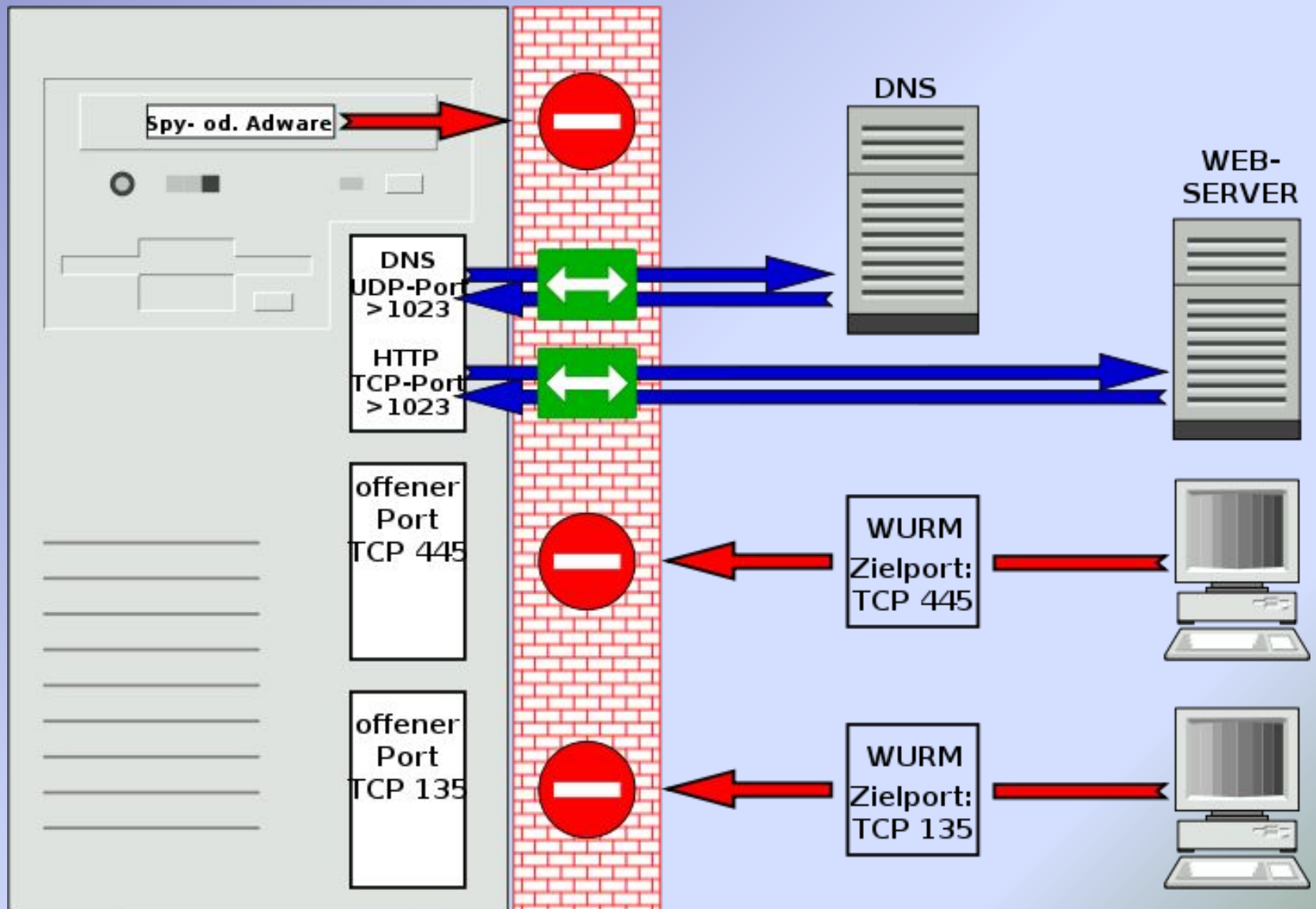


Демилиторизованная зона (сеть периметра)

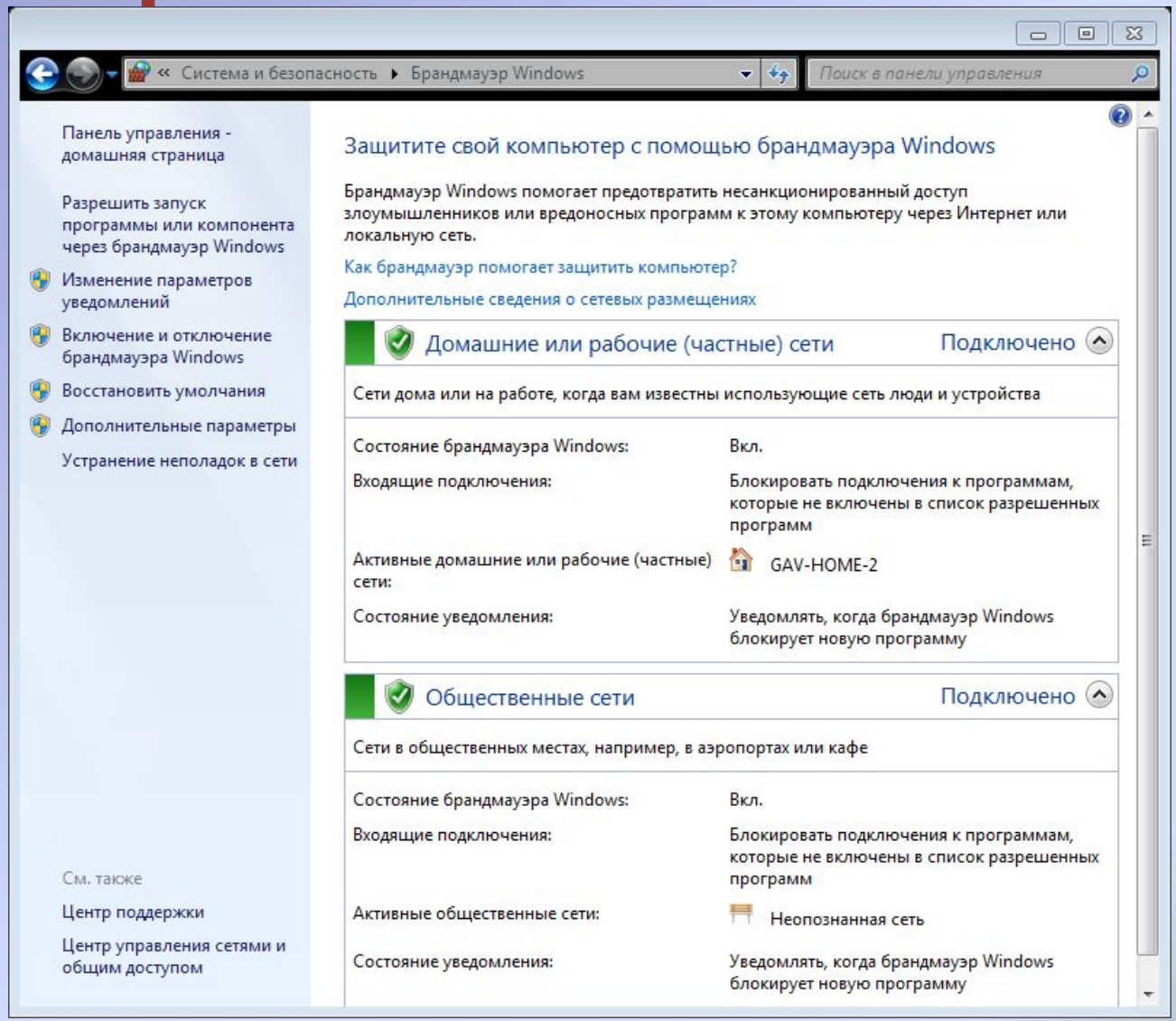


Windows Firewall?

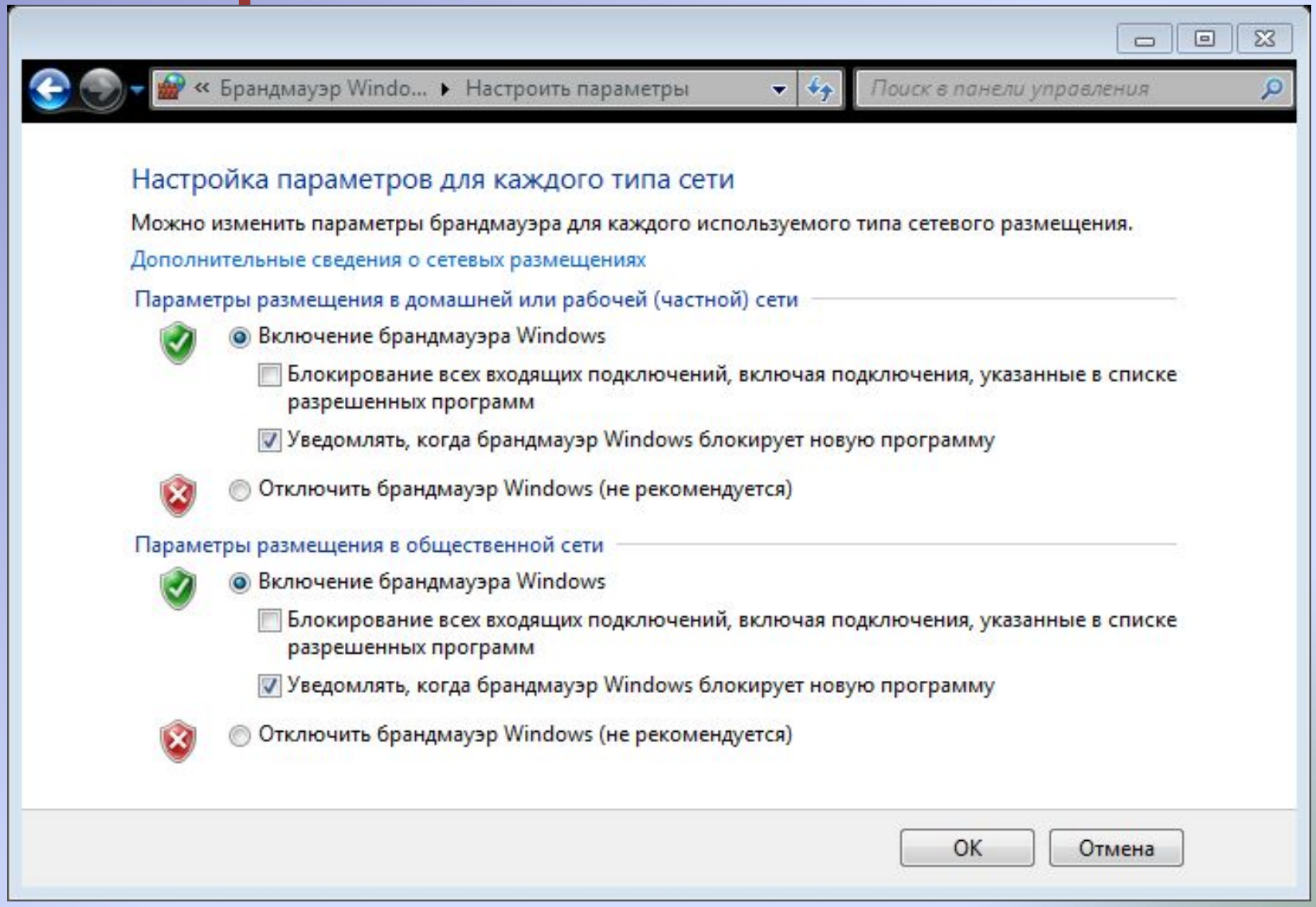
Персональный брандмауэр



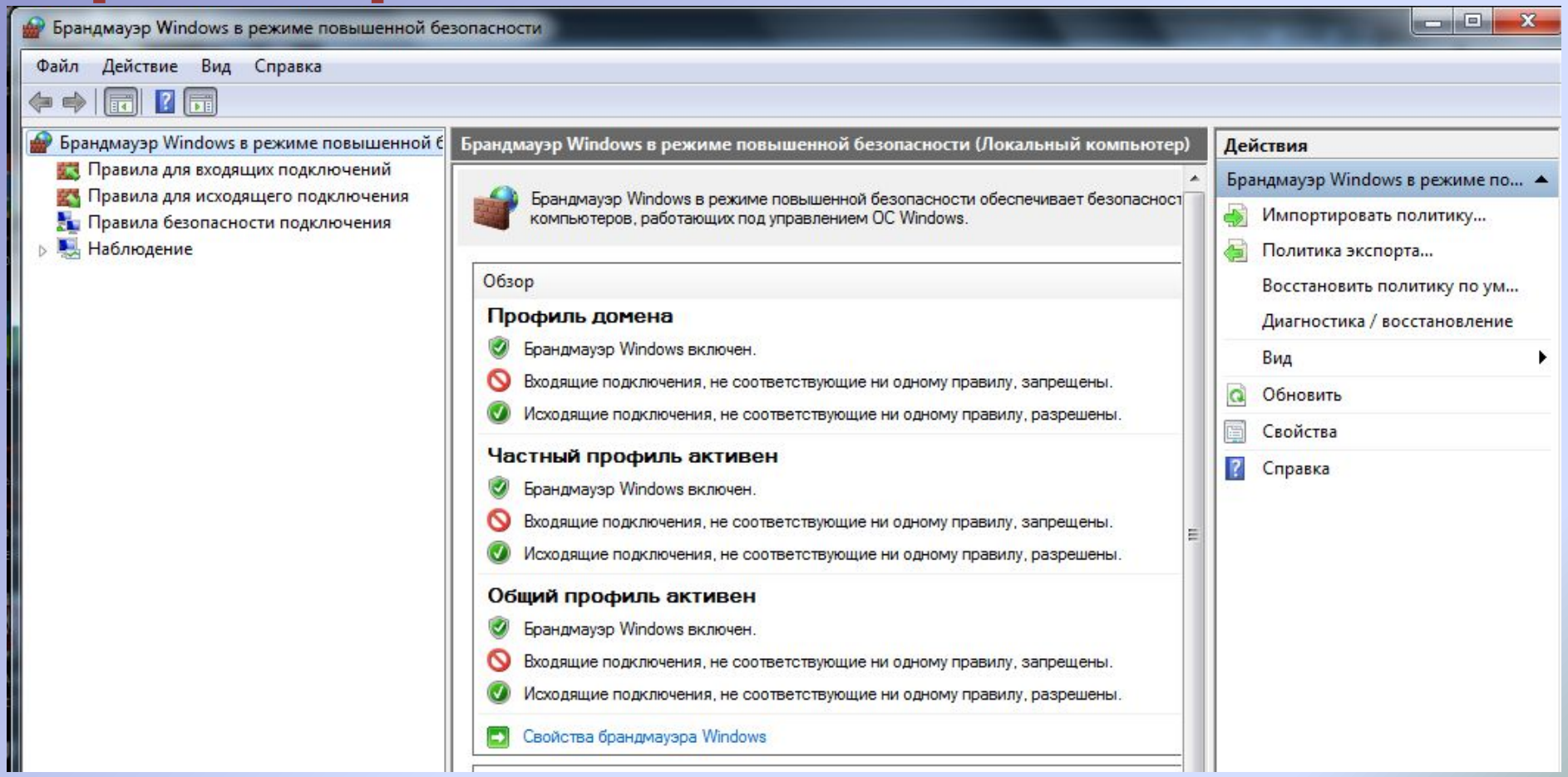
Windows Firewall с расширенными возможностями



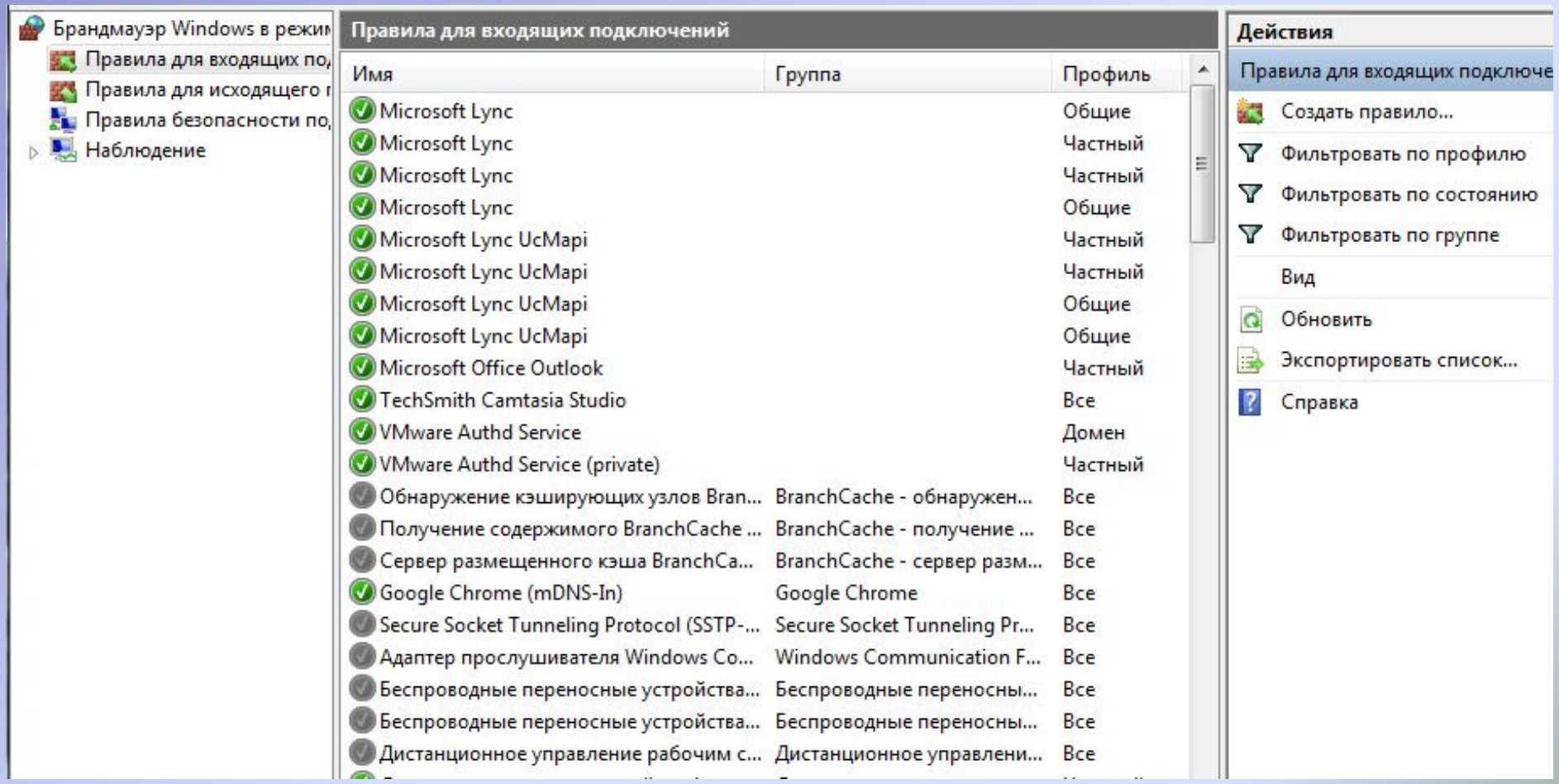
Windows Firewall с расширенными возможностями



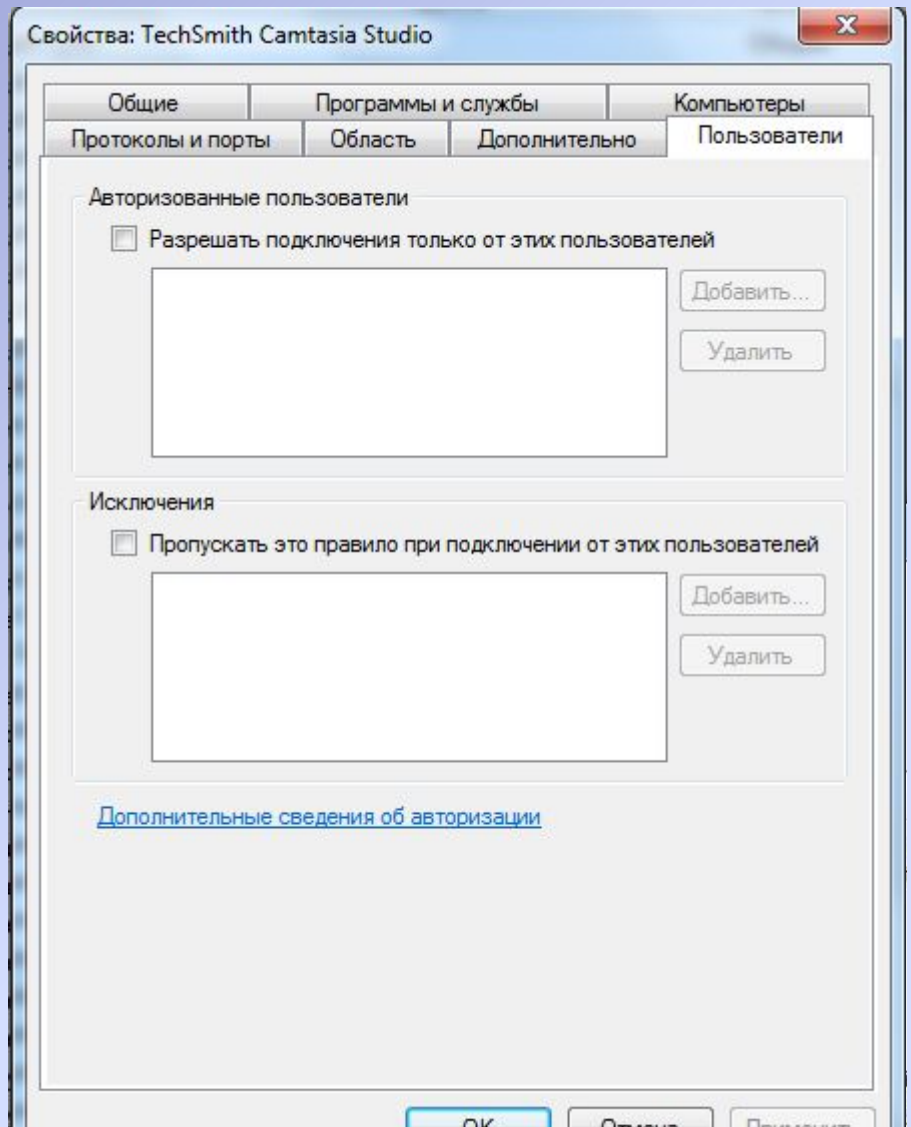
Windows Firewall с расширенными возможностями



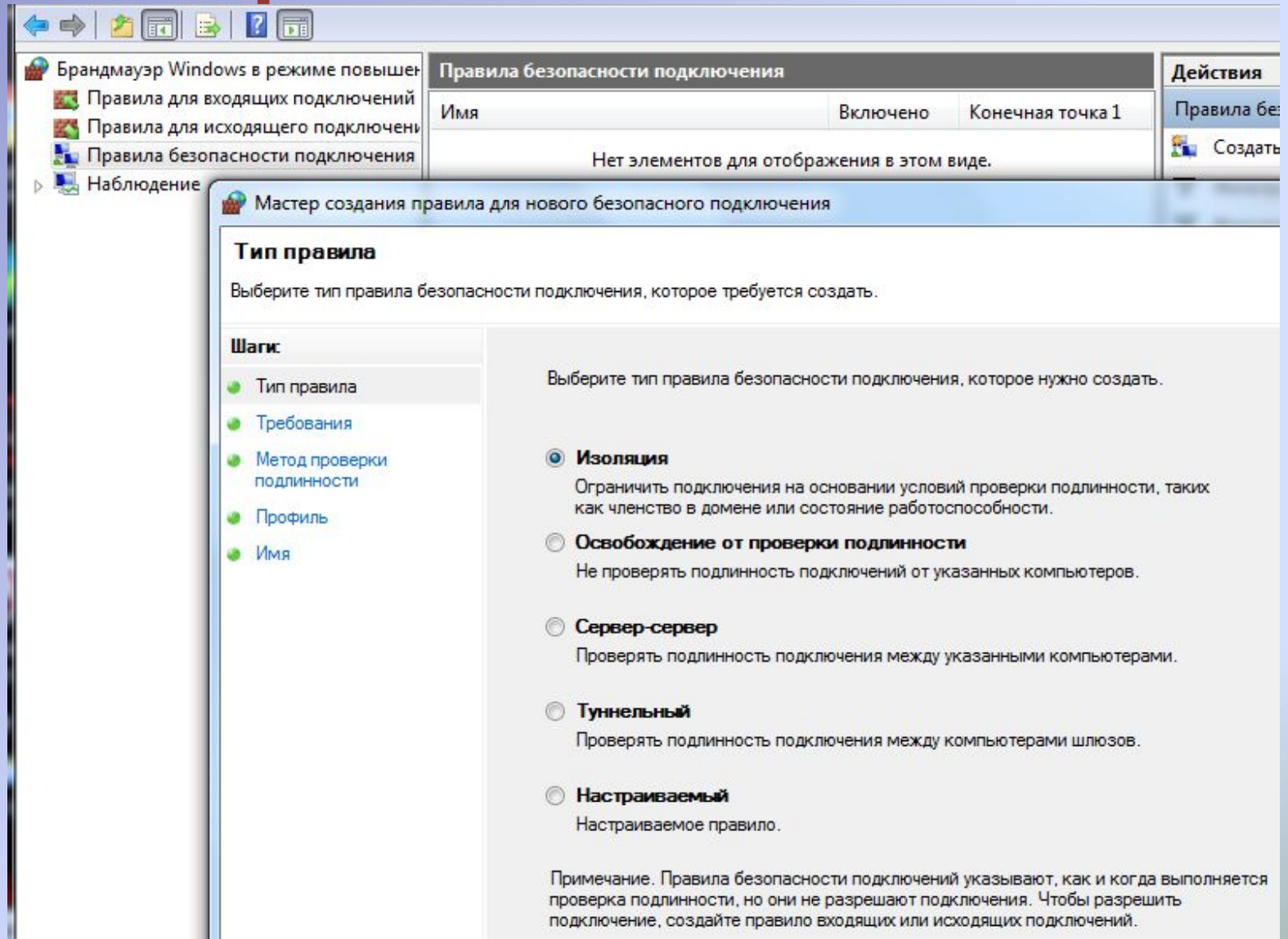
Windows Firewall с расширенными возможностями



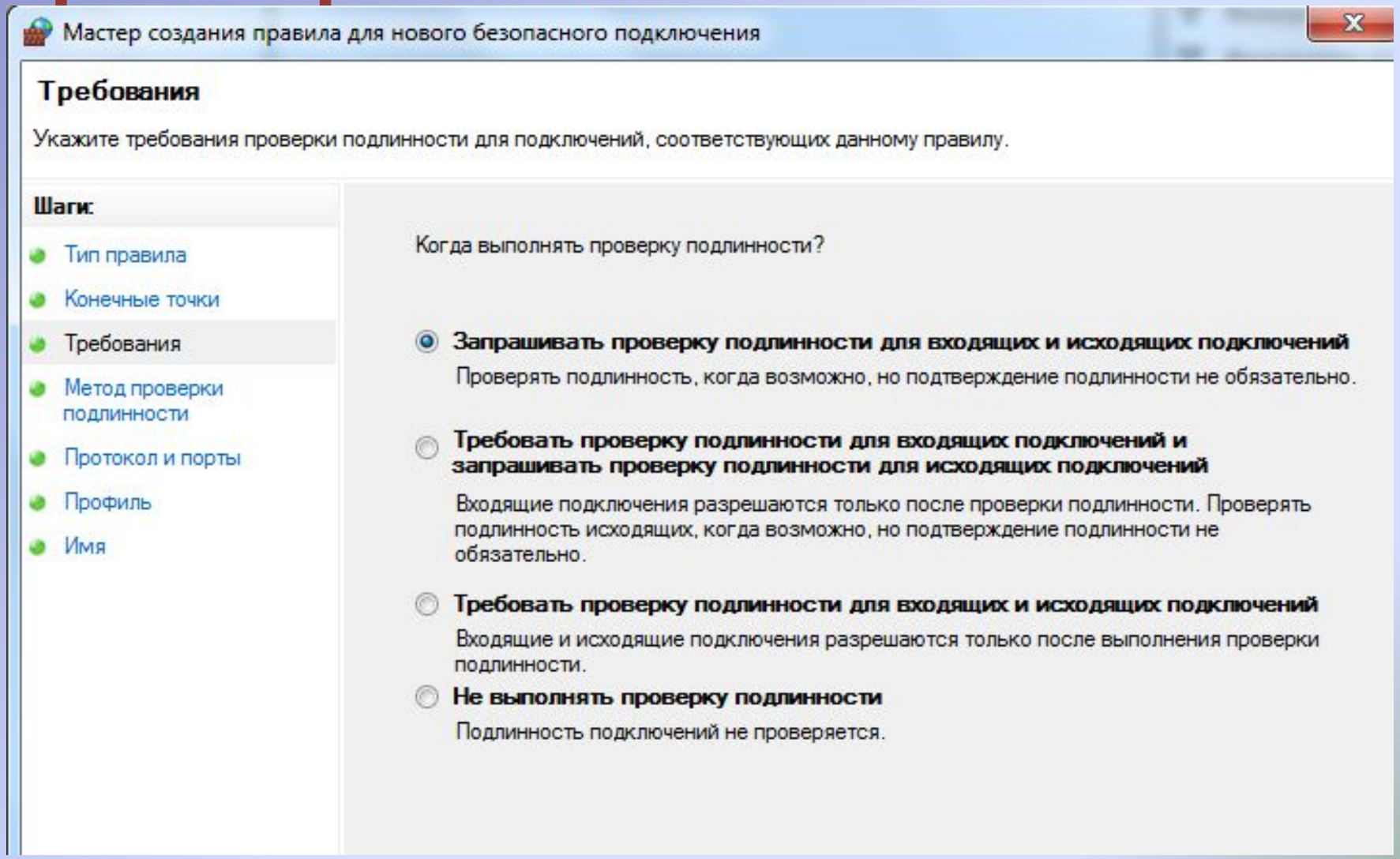
Windows Firewall с расширенными возможностями



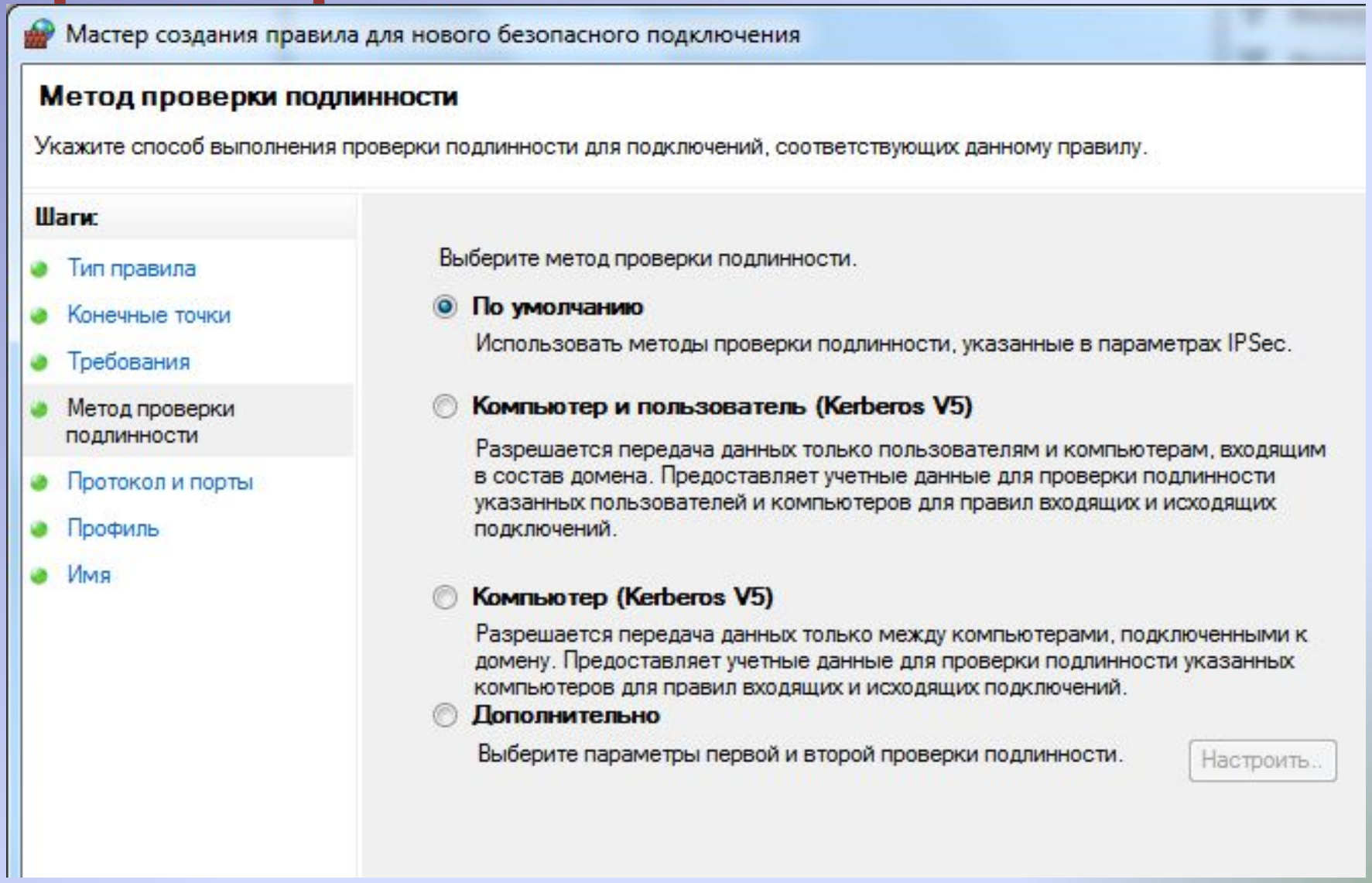
Windows Firewall с расширенными возможностями



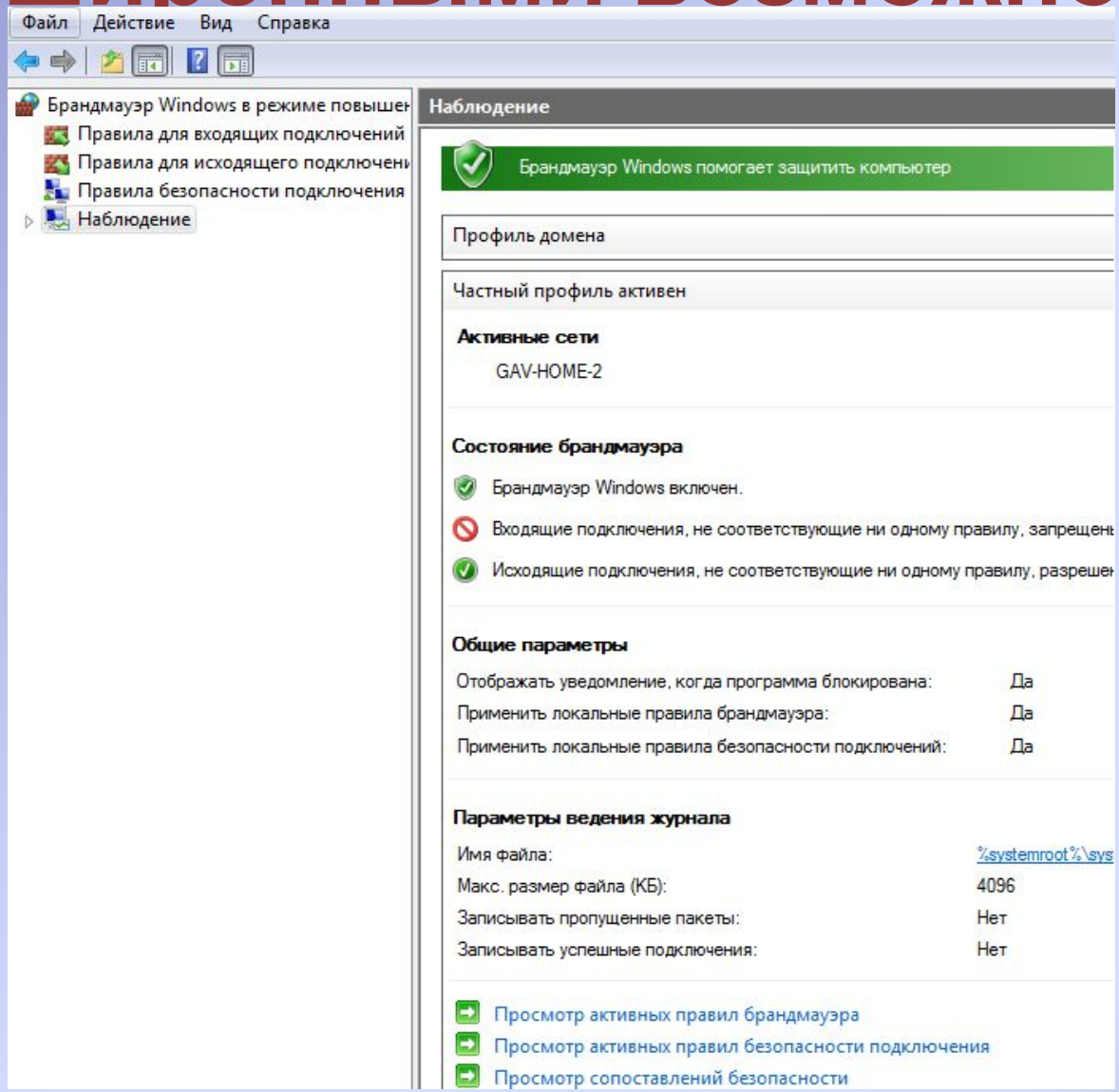
Windows Firewall с расширенными возможностями

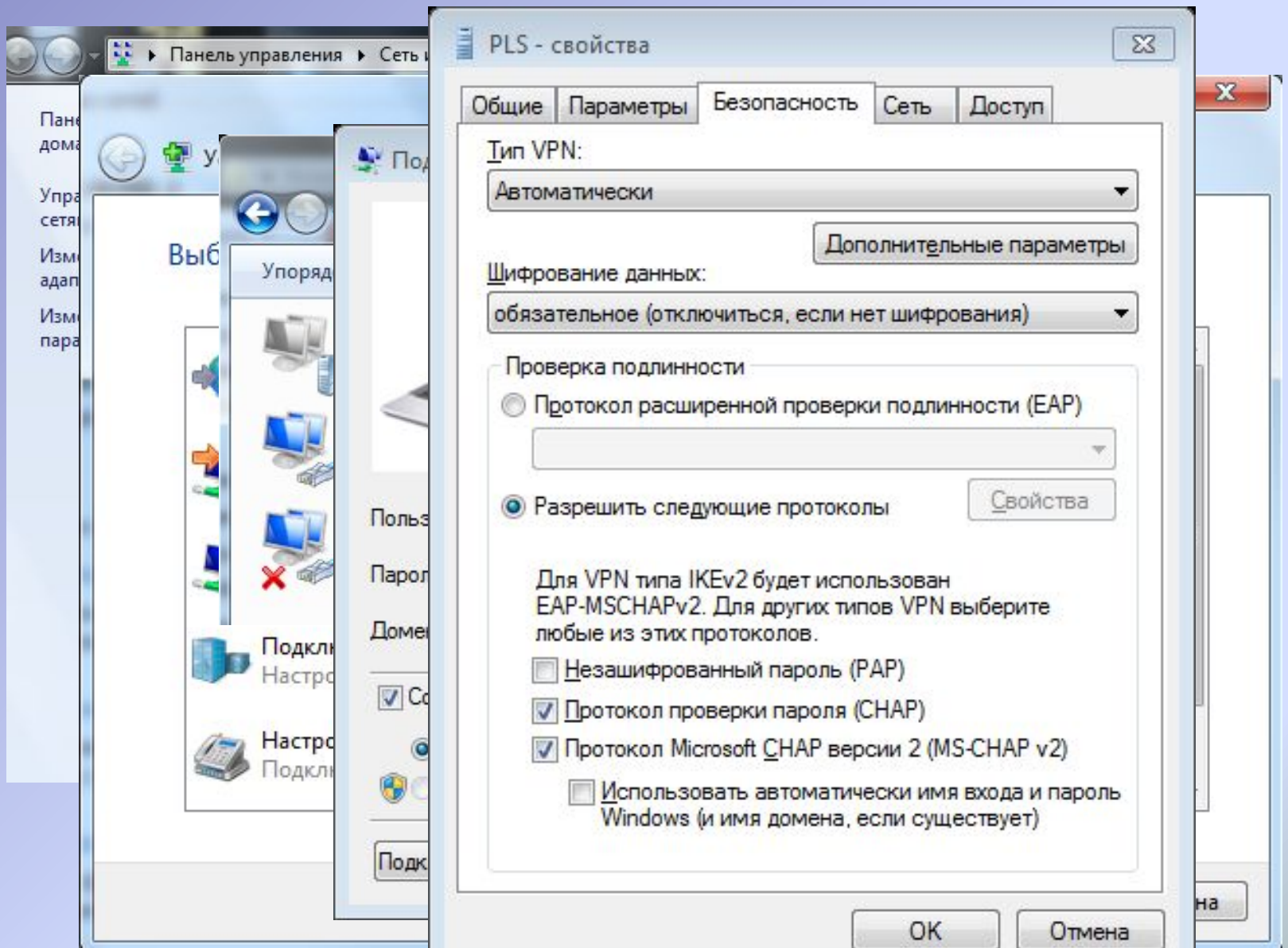


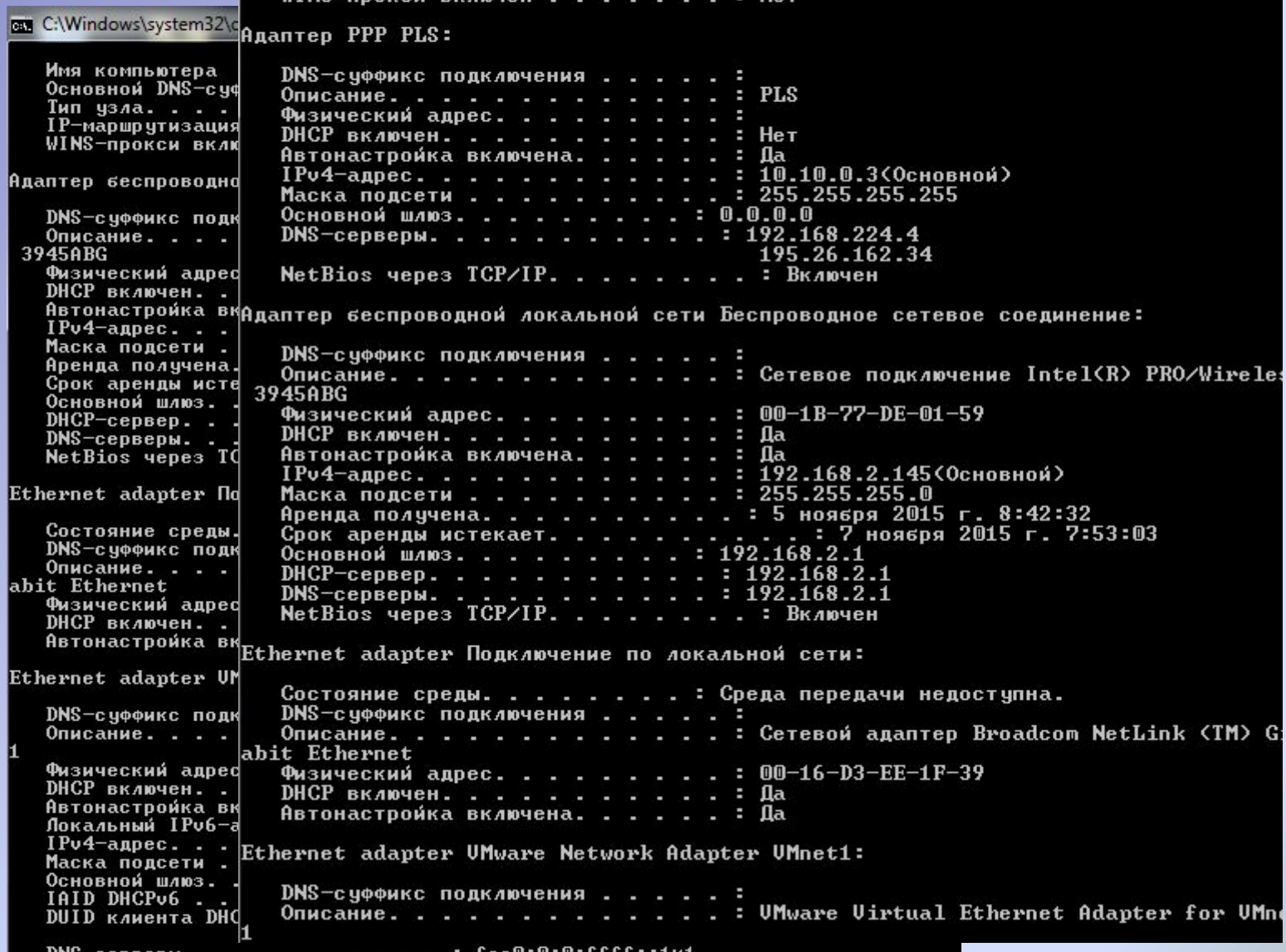
Windows Firewall с расширенными возможностями



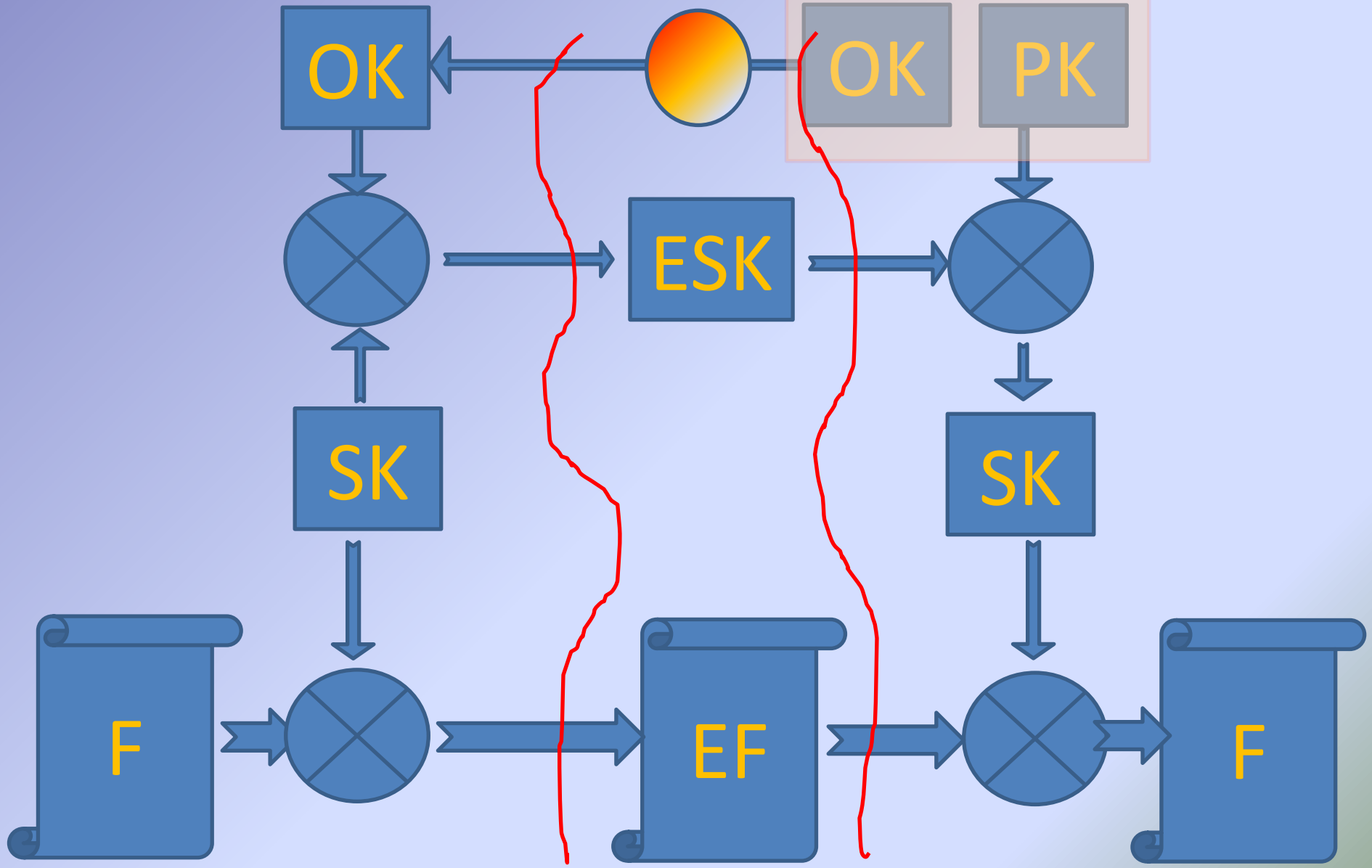
Windows Firewall с расширенными возможностями



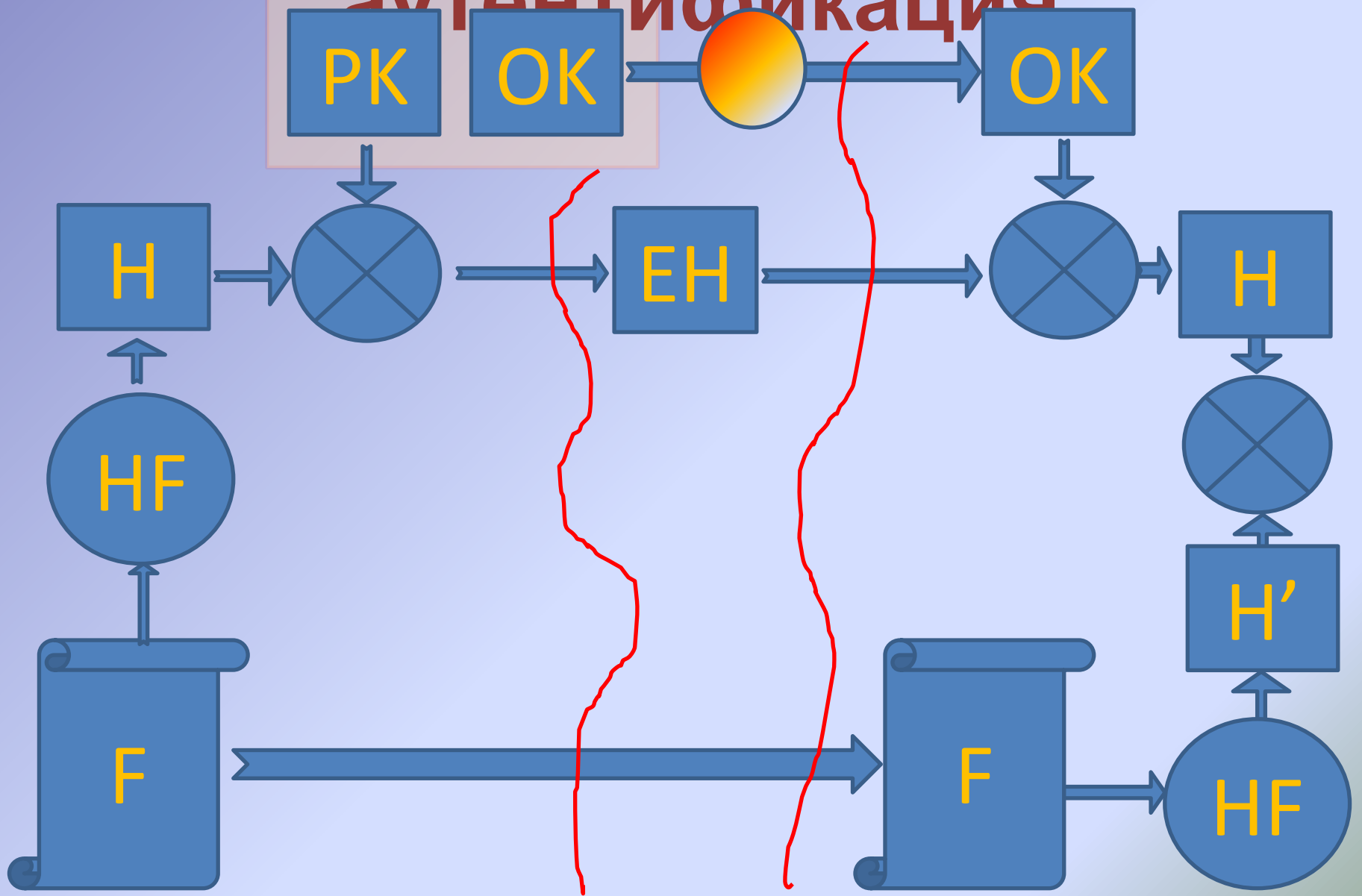

Панель управления
PLS - свойства
Общие
Параметры
Безопасность
Сеть
Доступ
Тип VPN:
Автоматически
Дополнительные параметры
Шифрование данных:
обязательное (отключиться, если нет шифрования)
Проверка подлинности
Протокол расширенной проверки подлинности (EAP)
Разрешить следующие протоколы
Свойства
Для 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:\Windows\system32\cmd.exe
C:\Users\Alexander>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:
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:
DNS-суффикс подключения . . . . . :
Описание. . . . . : Сетевое подключение Intel(R) PRO/Wireles
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:
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:
DNS-суффикс подключения . . . . . :
Описание. . . . . : VMware Virtual Ethernet Adapter for VMn
1

Конфиденциальность



Целостность и аутентификация



Списки управления доступом

Горячев Александр Вадимович
Доцент кафедры ИБ
avgoriachev@etu.ru

Модель эшелонированной обороны

Физический

Политики, процедуры, осведомленность

Хранение

ACL EFS Bitlocker Backup Mirror RAID SC

Обработка

APPs Antivirus Updates

OS/.NET Antispyware Autentification HIDS-HIPS

PKI

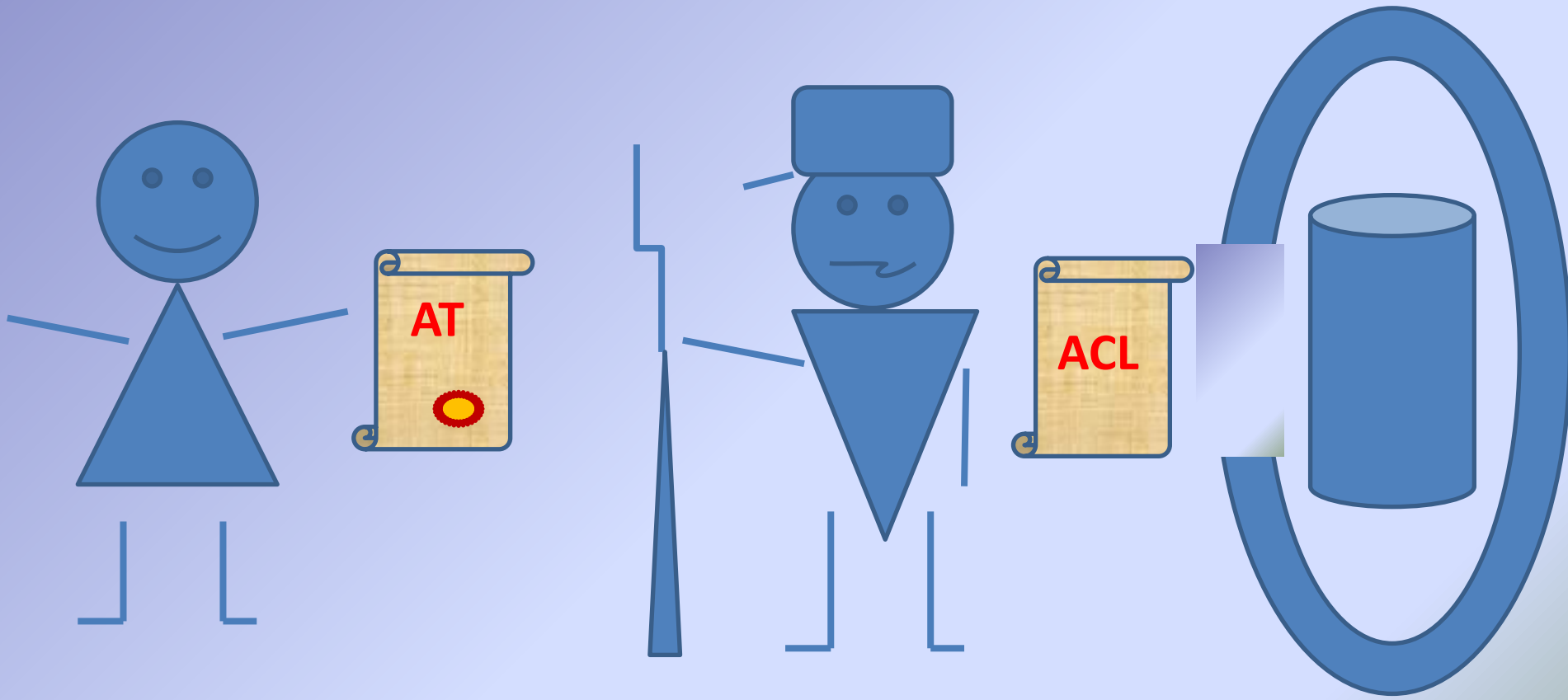
AD

Передача

Intranet Routing IPSec RMS NIDS-NIPS

Internet Firewall VPN NAP

Список контроля доступа



Список контроля доступа (ACL)

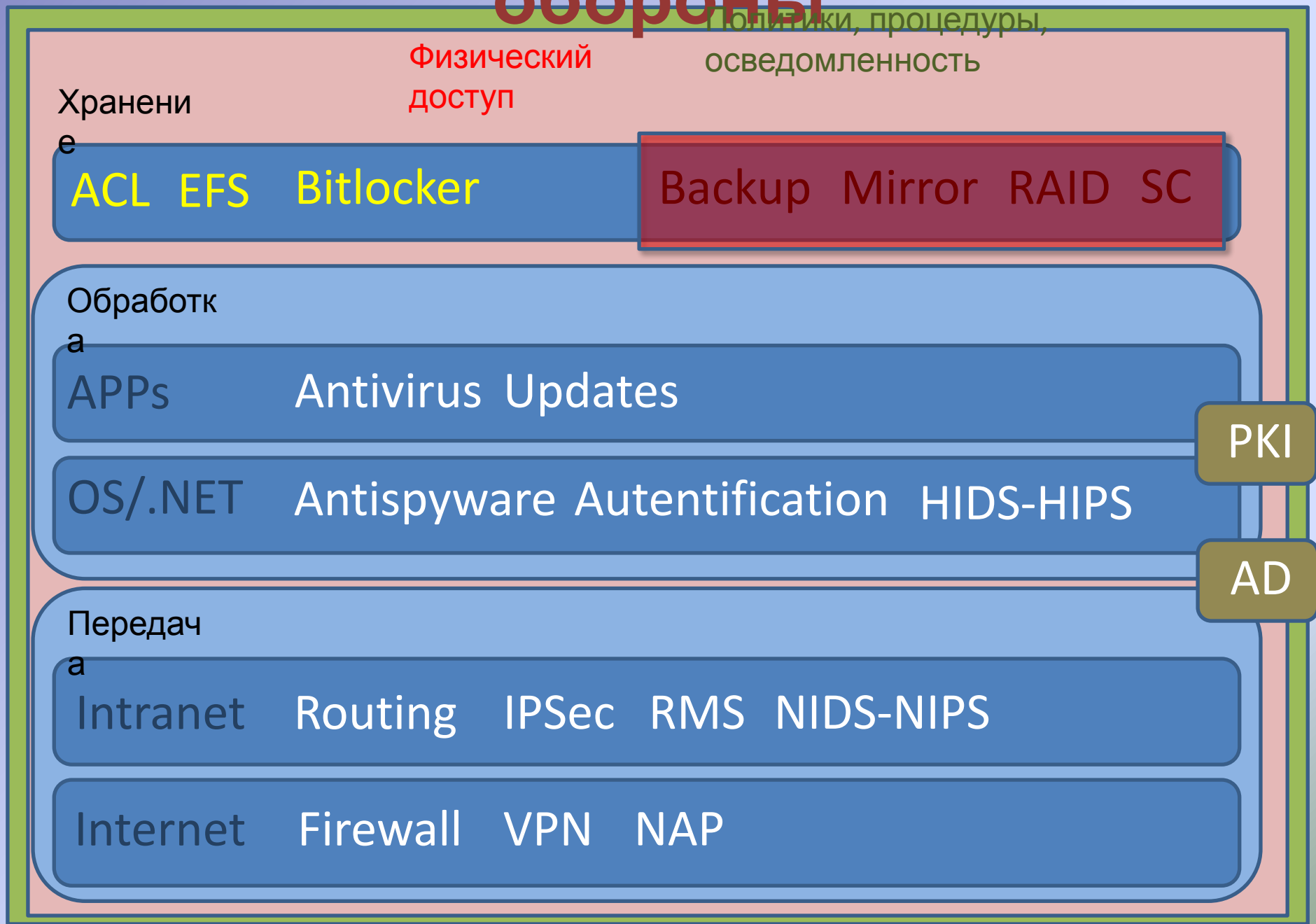
SID	Прав	A/D	I
SID O1	R	A	
SID O2	RW	A	I
SID O3	RWM	D	

Маркер доступа (AT)

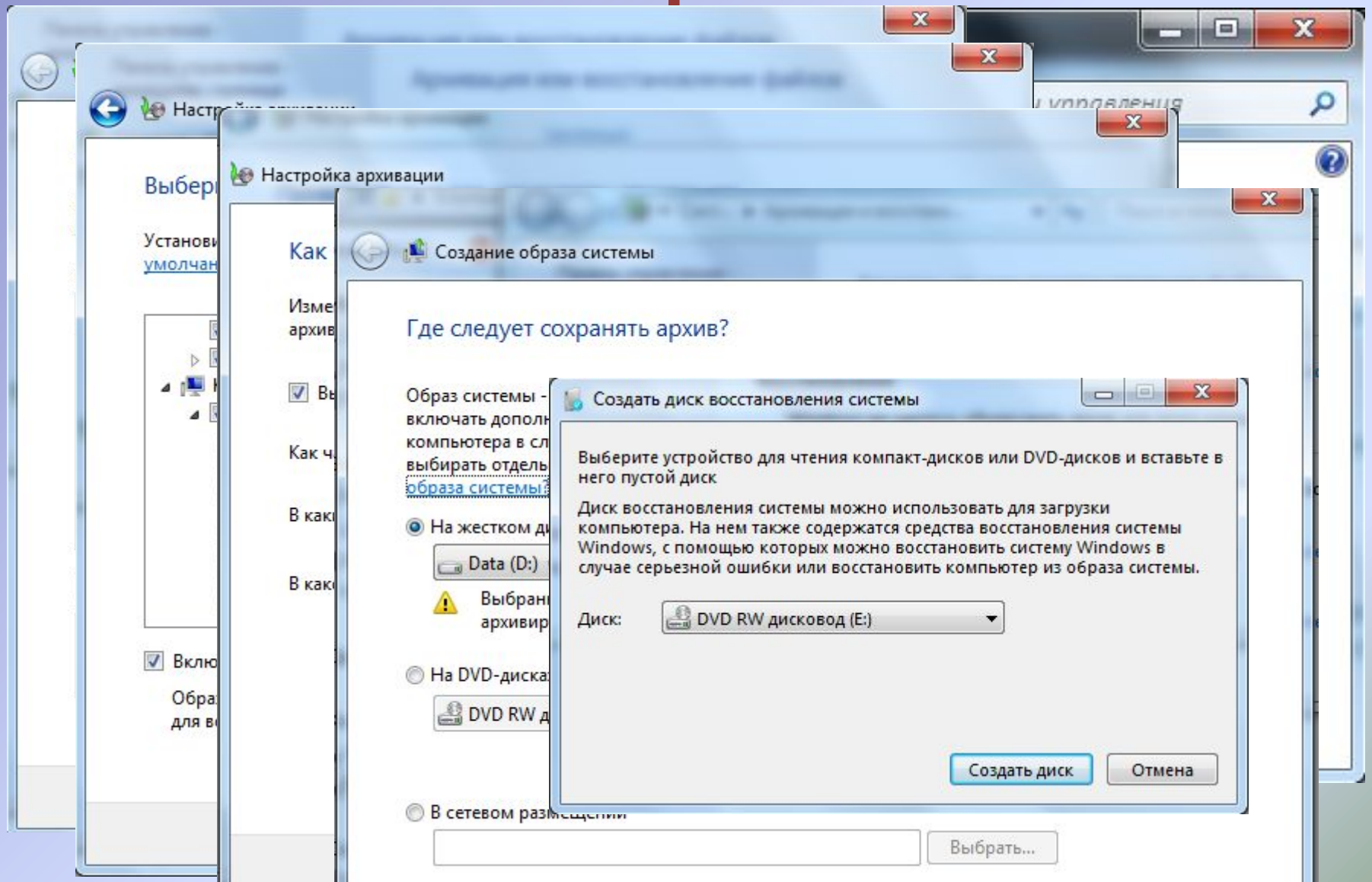
Обеспечение доступности информации при хранении

Горячев Александр Вадимович
Доцент кафедры
Информационной безопасности
avgoriachev@etu.ru

Модель эшелонированной обороны



Резервное копирование. Настройка



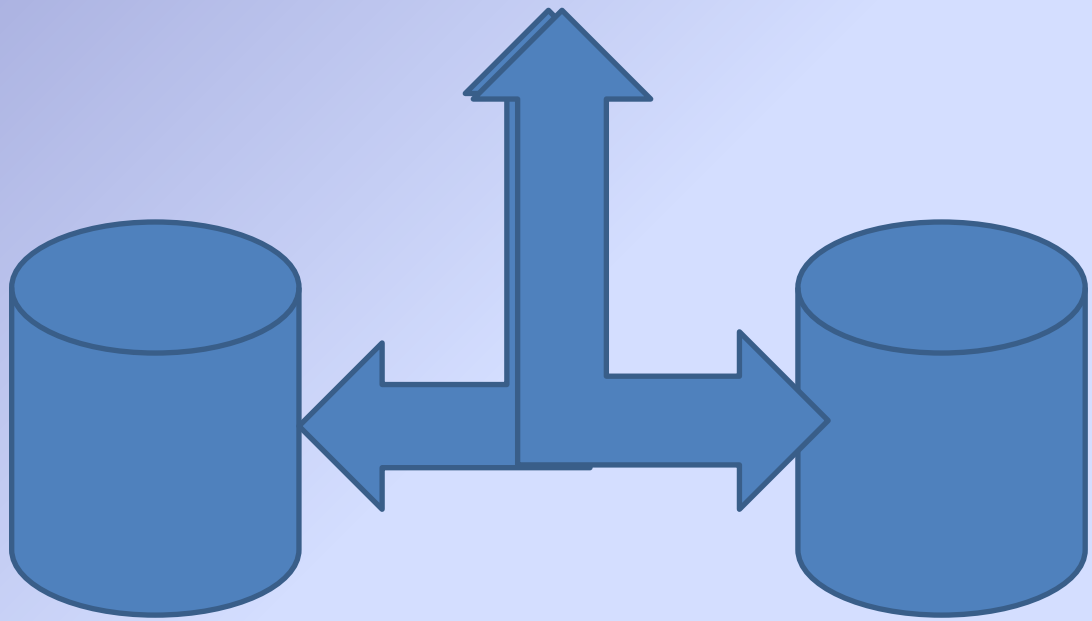
Резервное копирование. Схемы

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

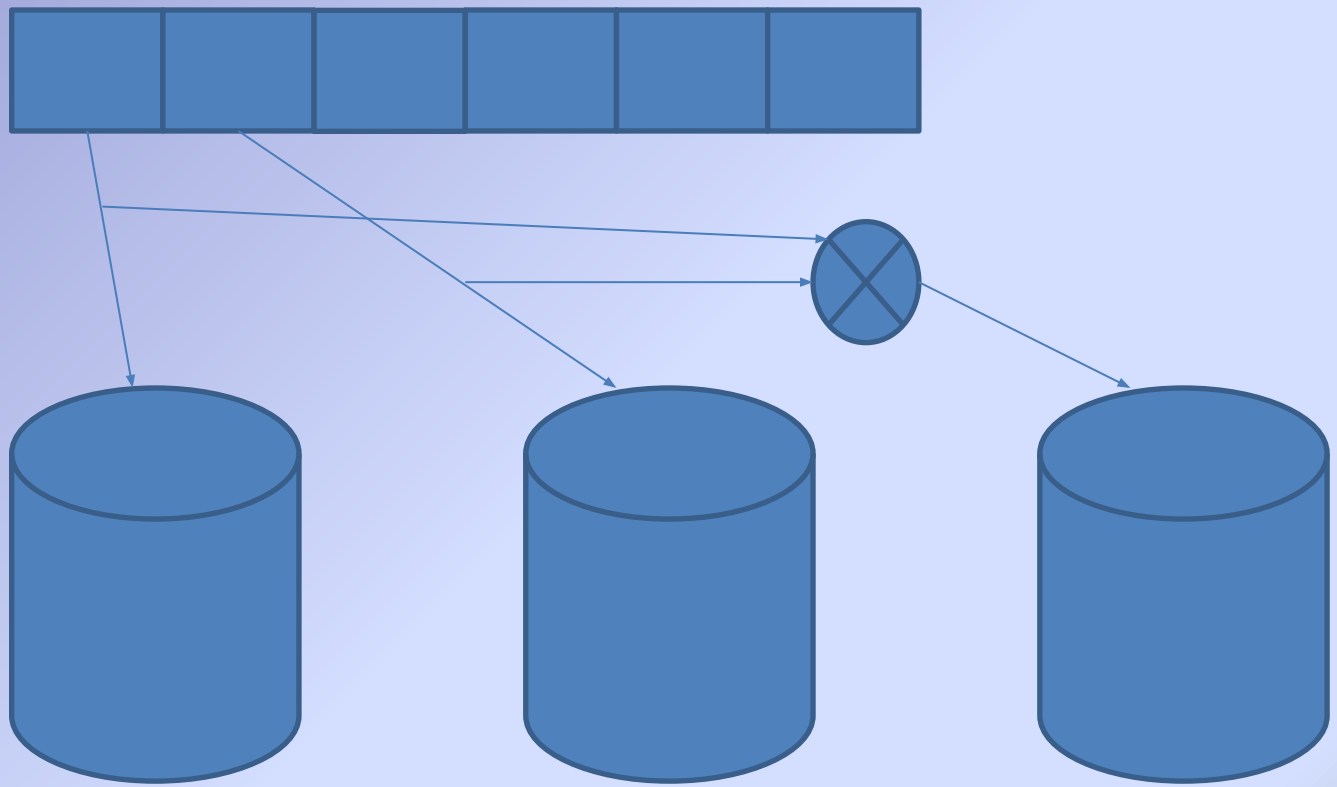
Резервное копирование. Правила

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

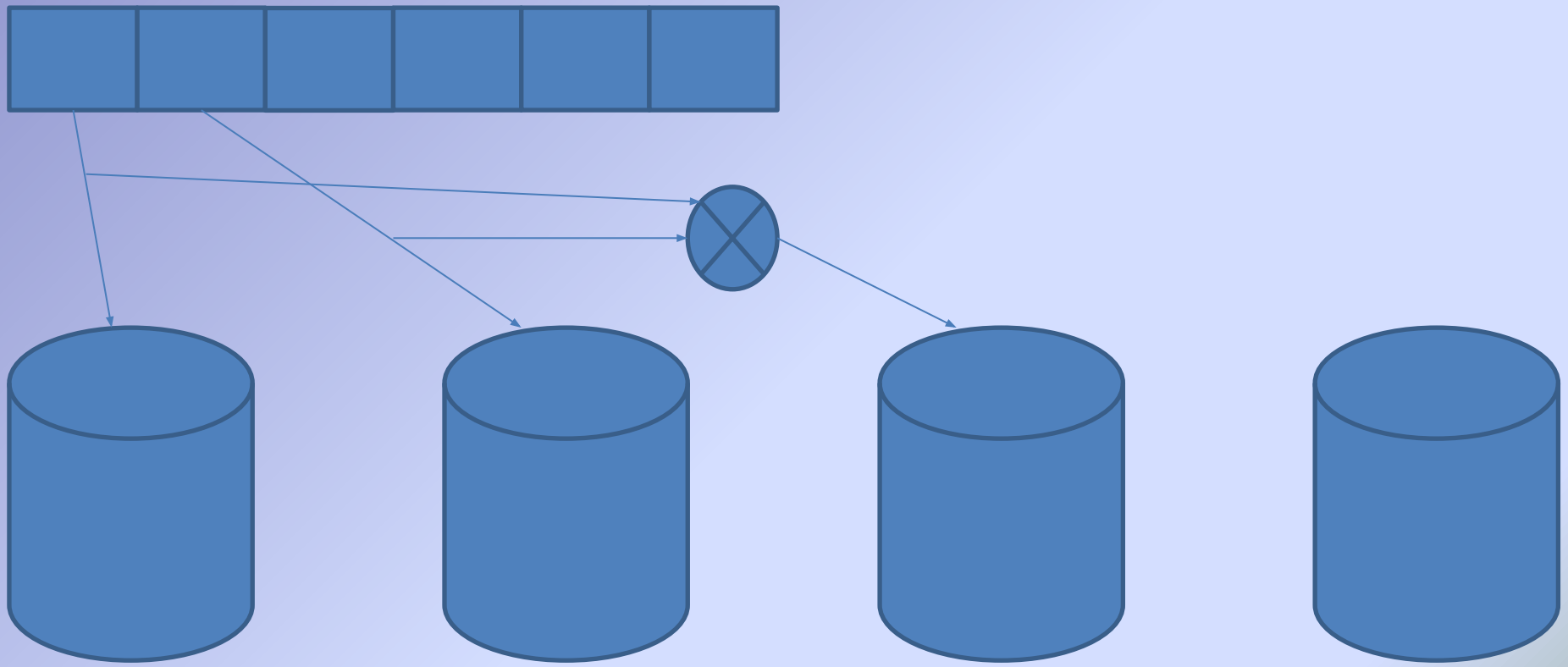
Дисковые массивы. Зеркало



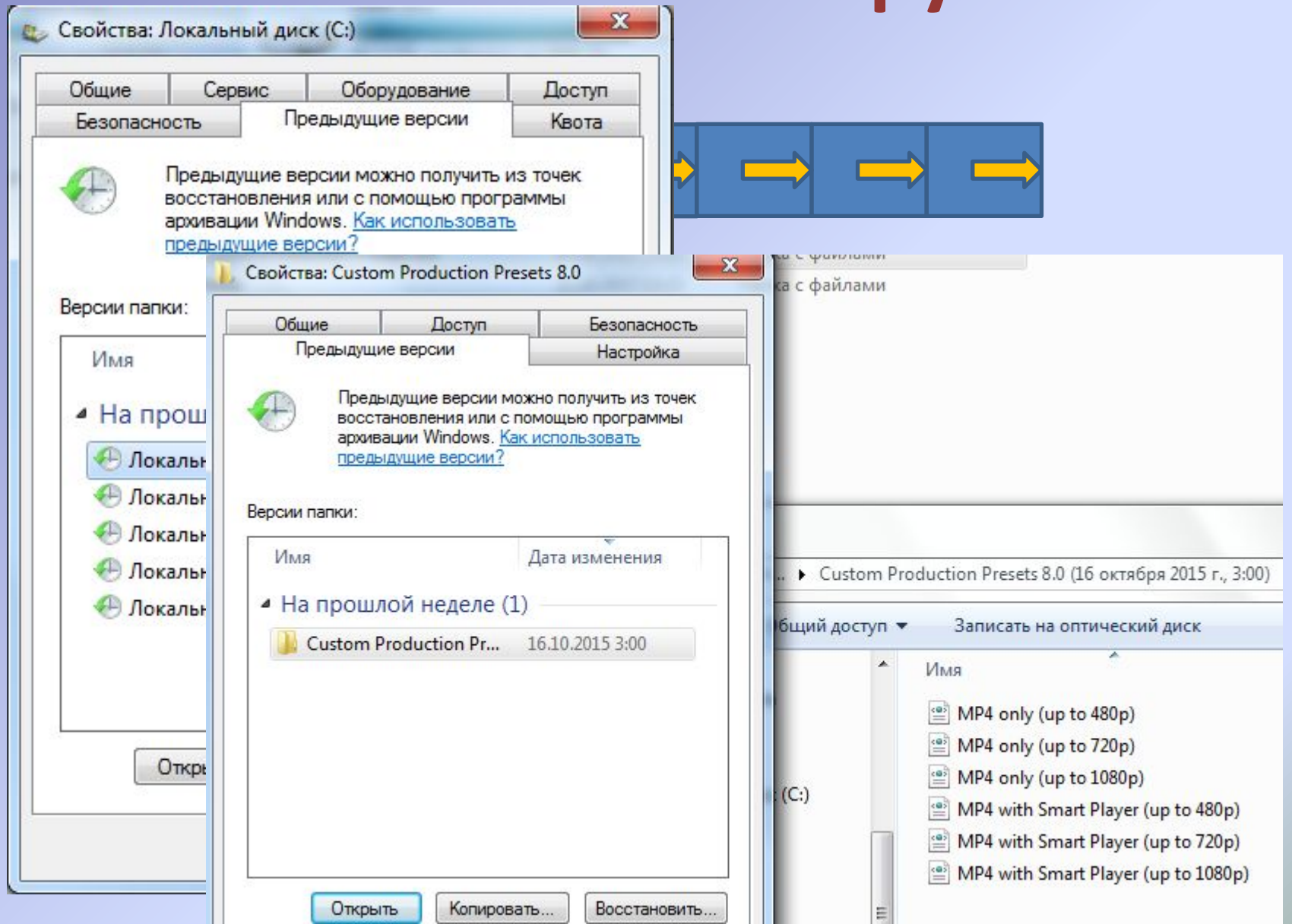
Дисковые массивы. RAID 5



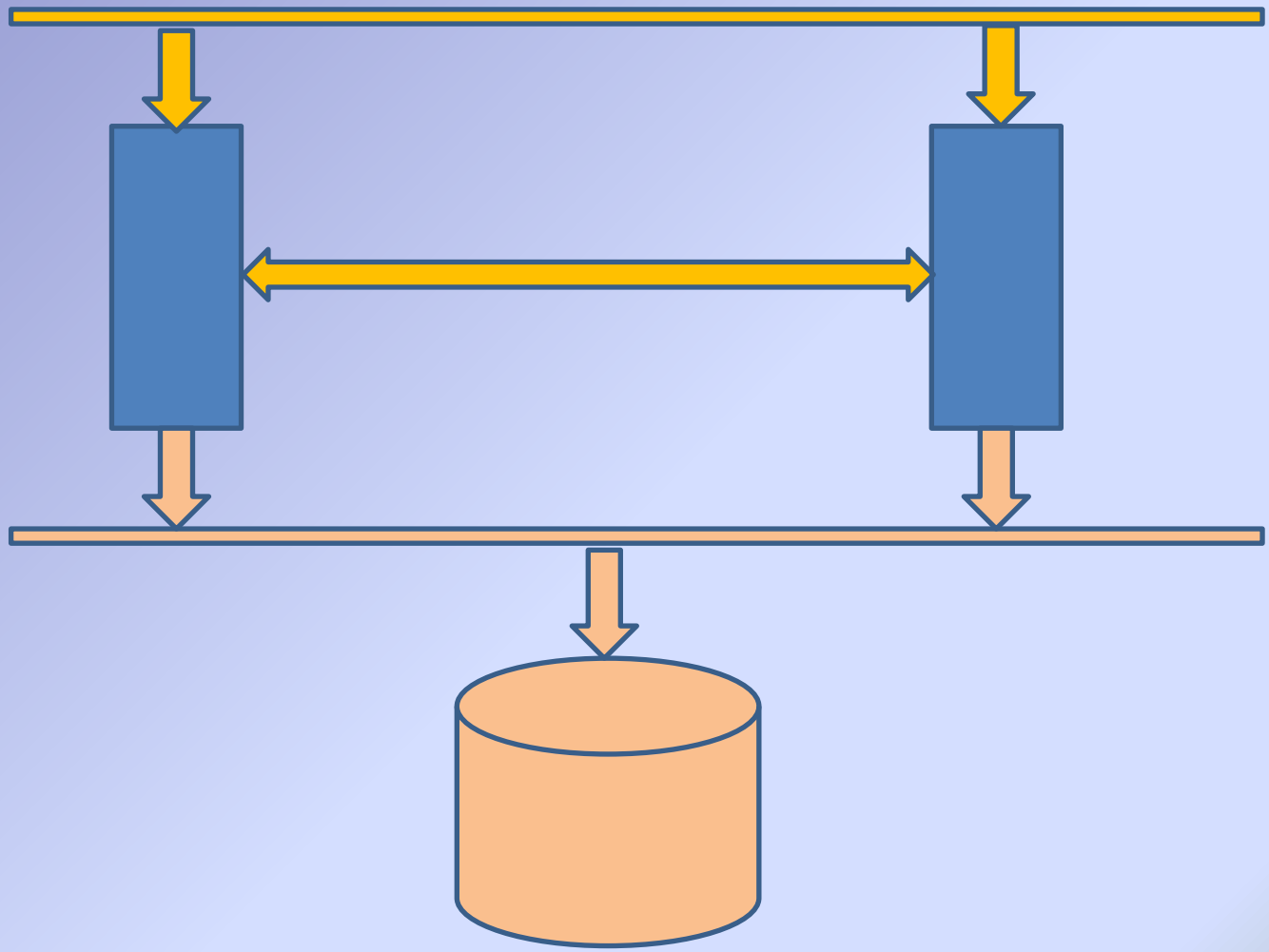
Дисковые массивы. Hot Spare



Shadow Copy


Свойства: Локальный диск (C:)
Общие
Сервис
Оборудование
Доступ
Безопасность
Предыдущие версии
Квота
Предыдущие версии можно получить из точек восстановления или с помощью программы архивации Windows. Как использовать предыдущие версии?
Версии папки:
Имя
Свойства: Custom Production Presets 8.0
Общие
Доступ
Безопасность
Предыдущие версии
Настройка
Предыдущие версии можно получить из точек восстановления или с помощью программы архивации Windows. Как использовать предыдущие версии?
Версии папки:
Имя
Дата изменения
На прошлой неделе (1)
Custom Production Pr...
16.10.2015 3:00
Открыть
Копировать...
Восстановить...
Custom Production Presets 8.0 (16 октября 2015 г., 3:00)
Общий доступ
Записать на оптический диск
Имя
MP4 only (up to 480p)
MP4 only (up to 720p)
MP4 only (up to 1080p)
MP4 with Smart Player (up to 480p)
MP4 with Smart Player (up to 720p)
MP4 with Smart Player (up to 1080p)

Кластер надежности



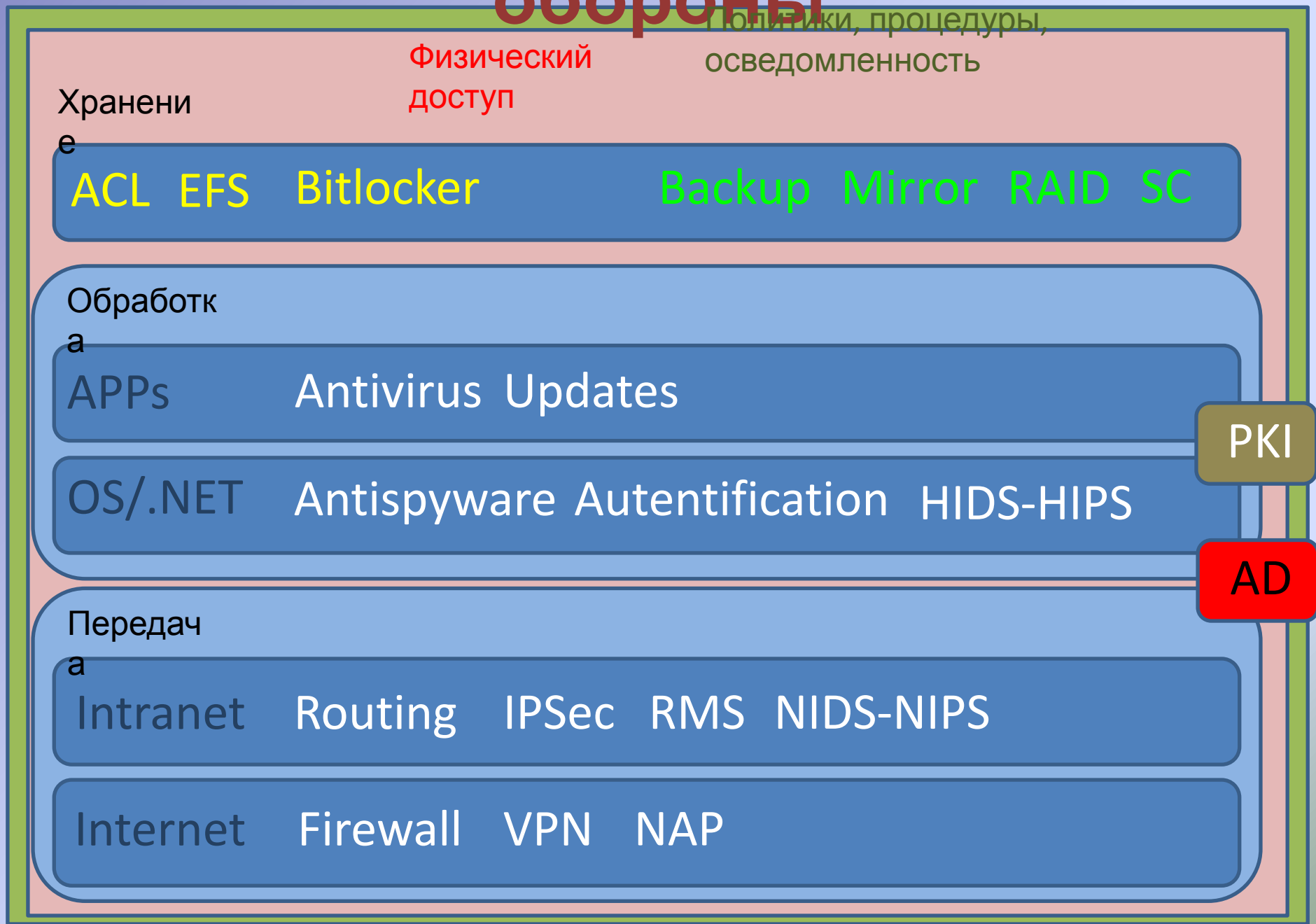
Групповые политики службы каталога Active Directory

Горячев Александр Вадимович

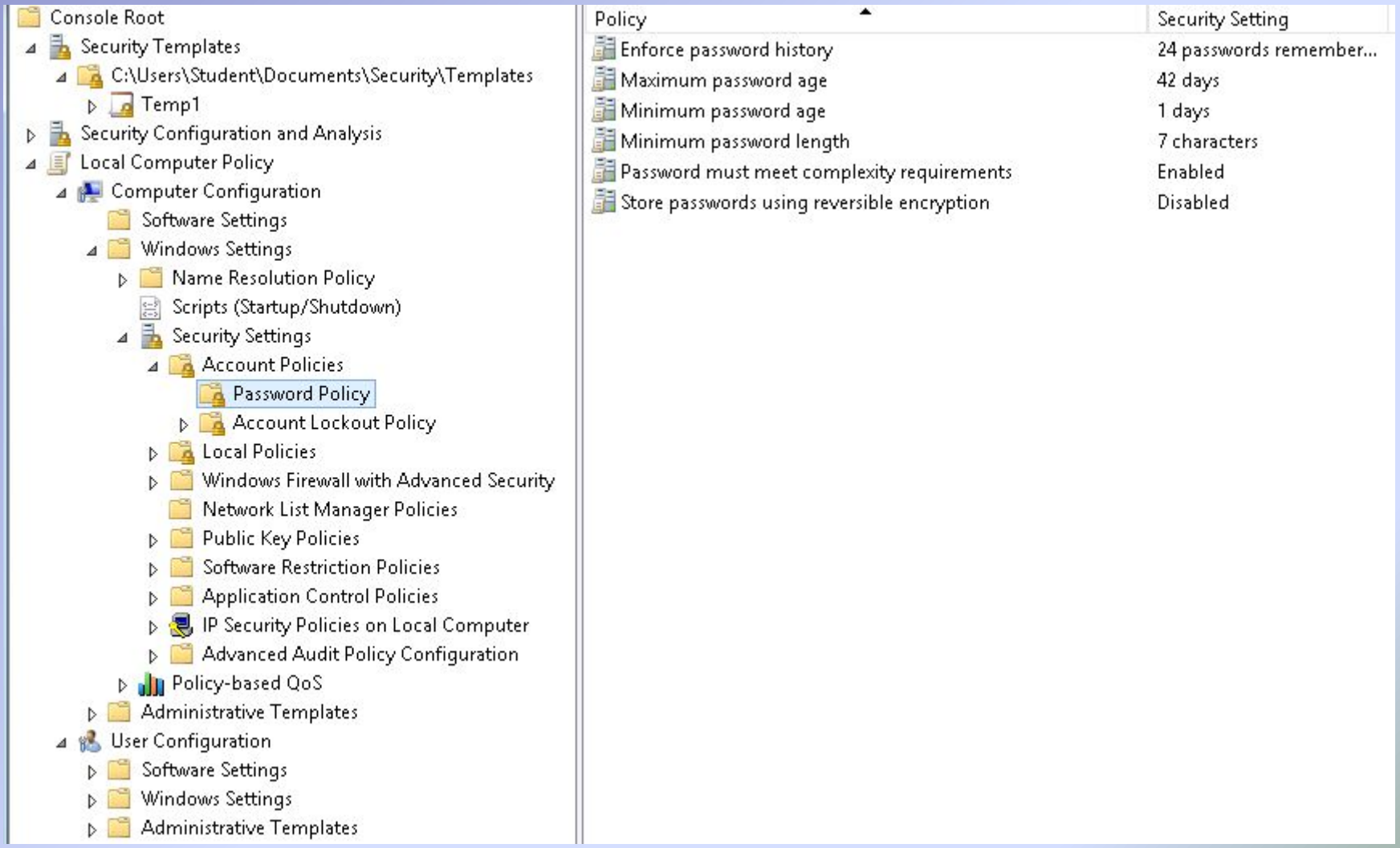
Доцент кафедры
Информационной безопасности

avgoriachev@etu.ru

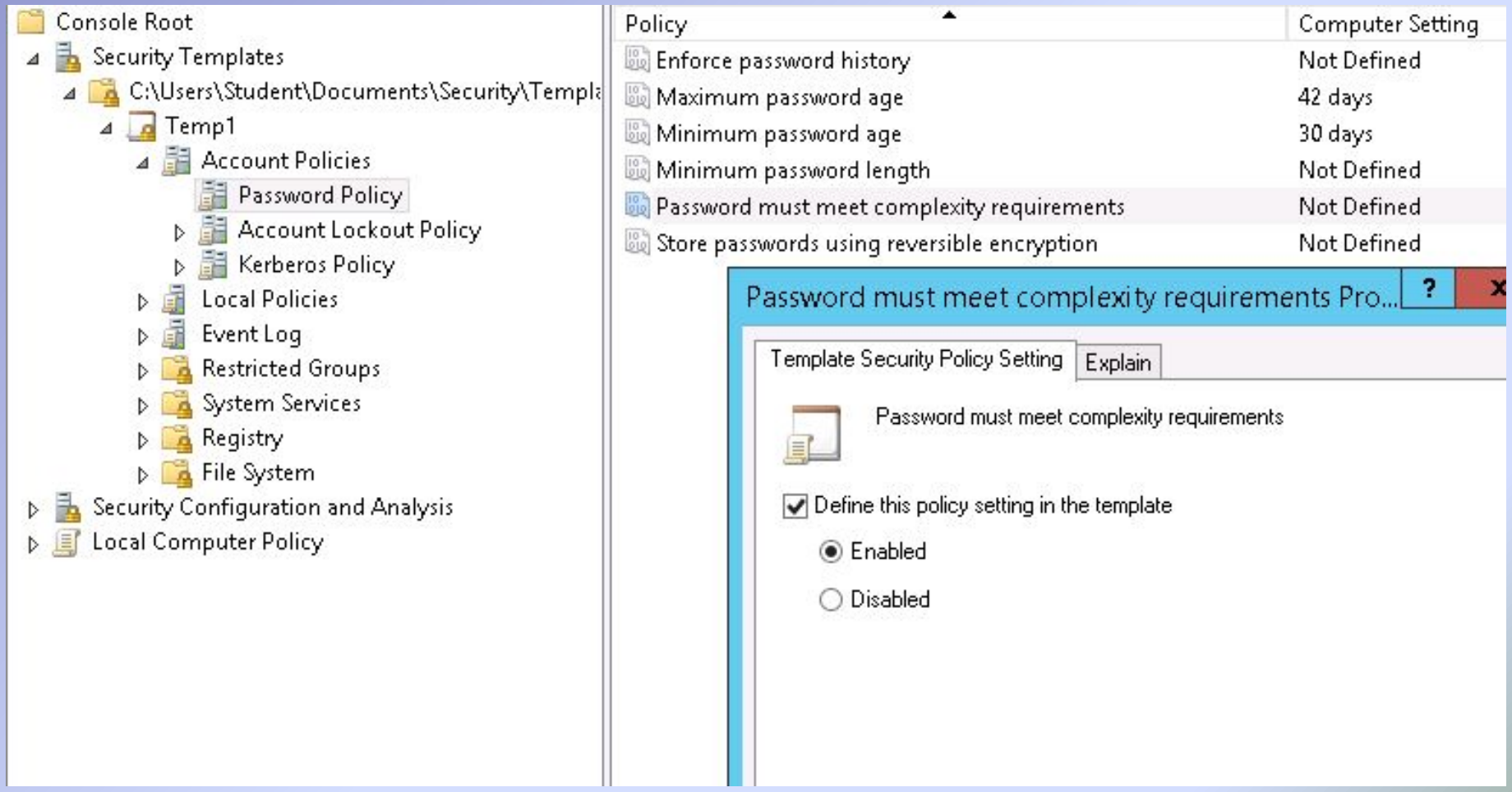
Модель эшелонированной обороны



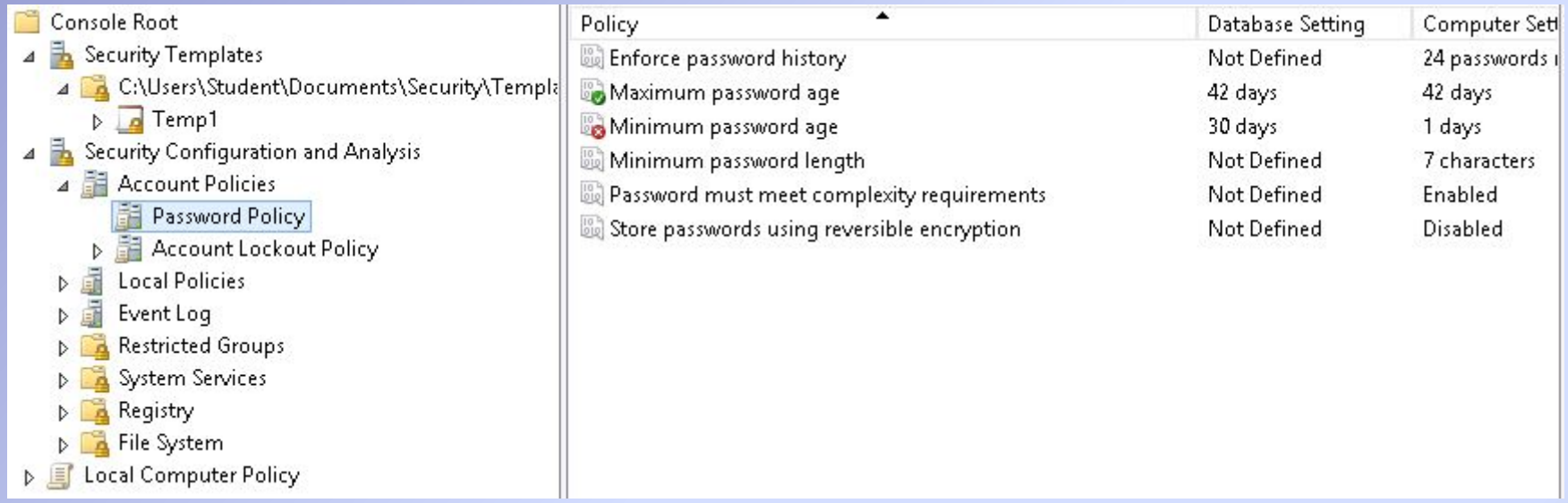
Локальная политика безопасности



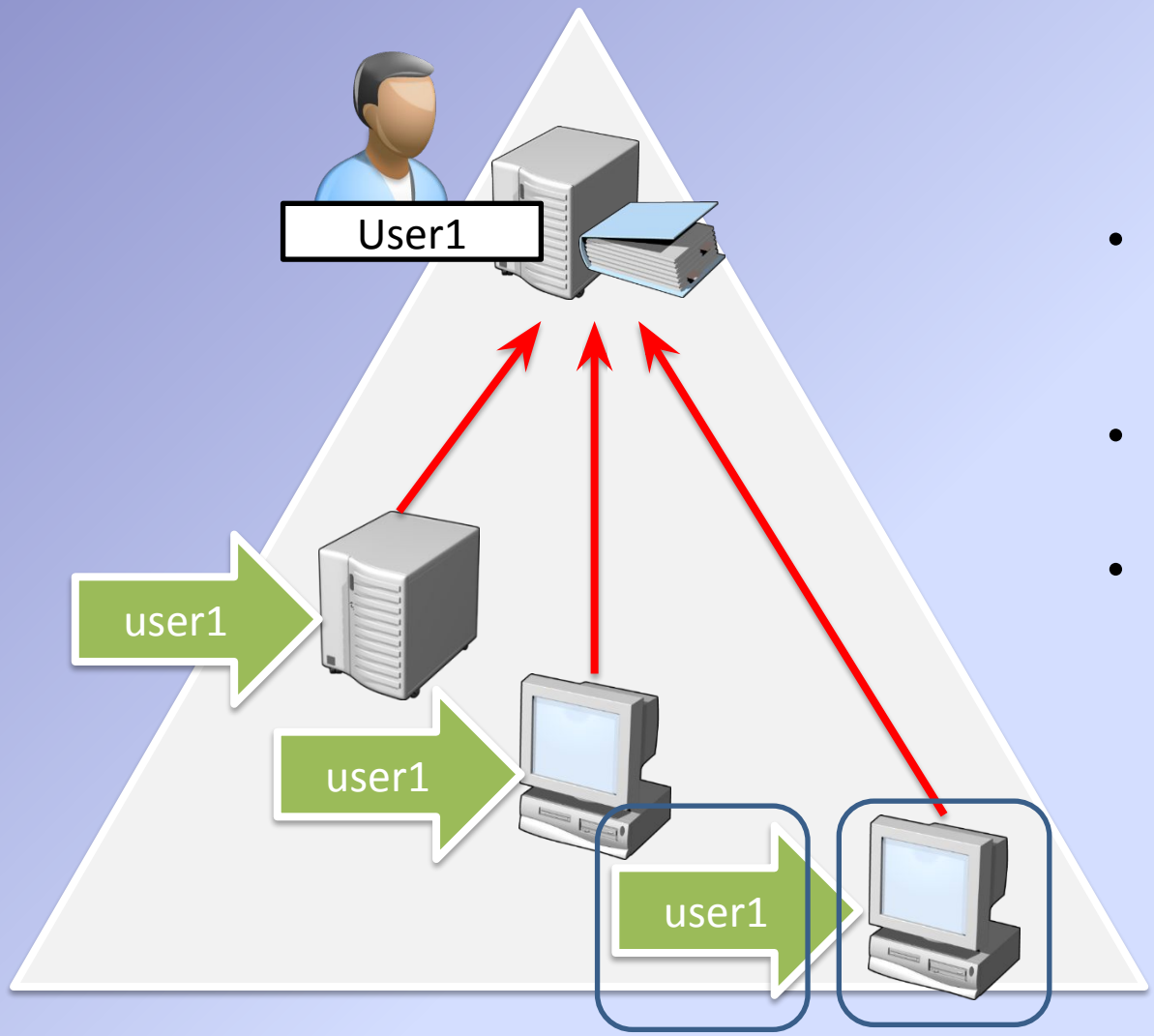
Шаблоны безопасности



Анализ и конфигурация безопасности



Домен Windows NT

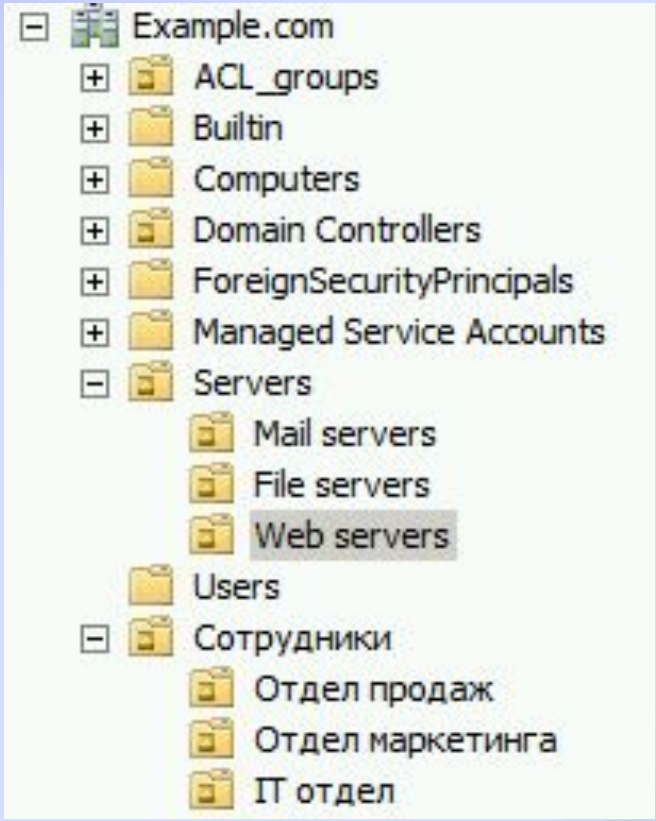


- Требует наличия как минимум одного контроллера домена (PDC)
- Граница репликации домена
- Доверенный источник учётных данных: любой доменный контроллер (PDC и BDC) может провести аутентификацию в домене

Security Account Manager

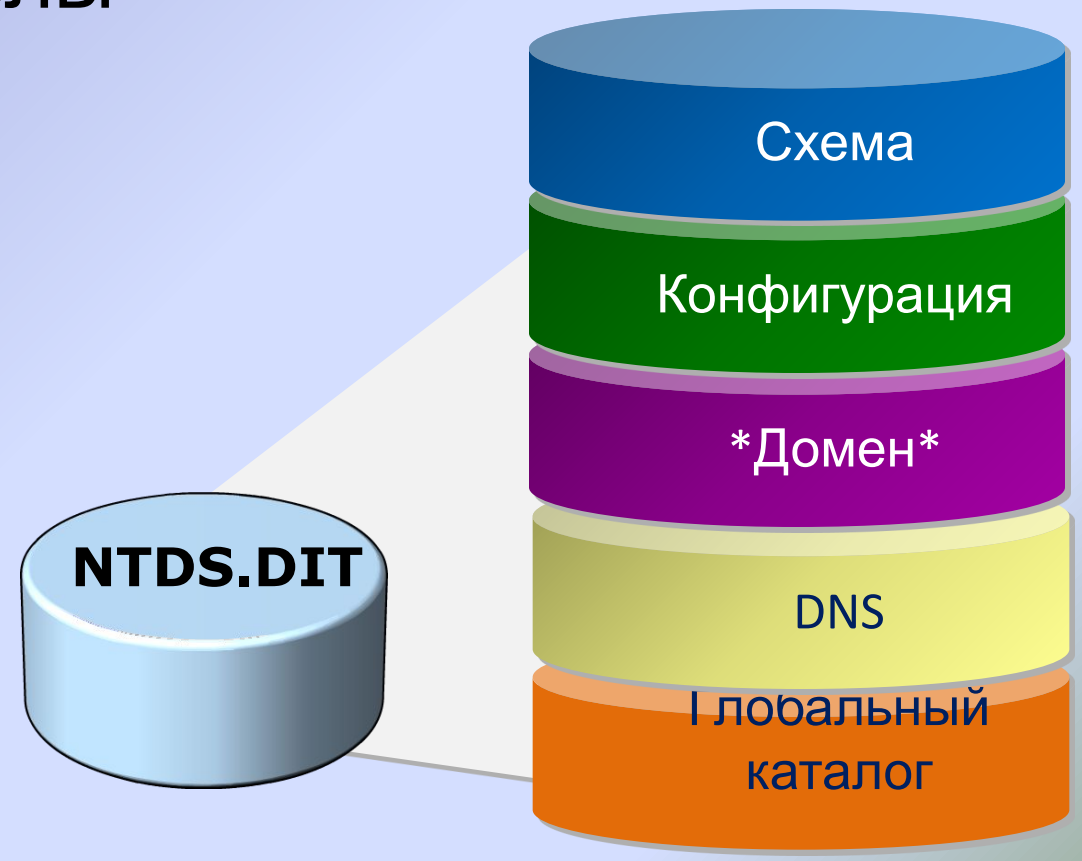
Подразделения (организационные единицы)

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



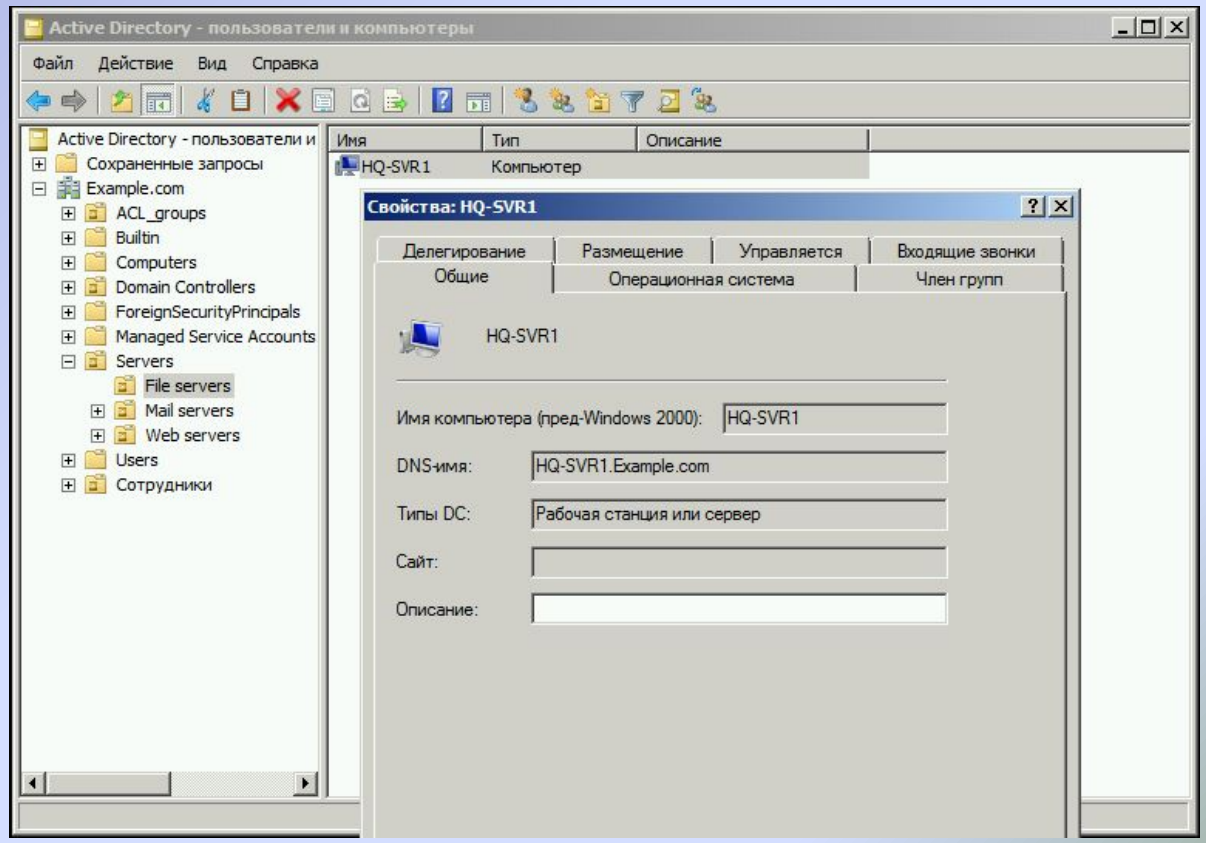
Хранилище данных Active Directory

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



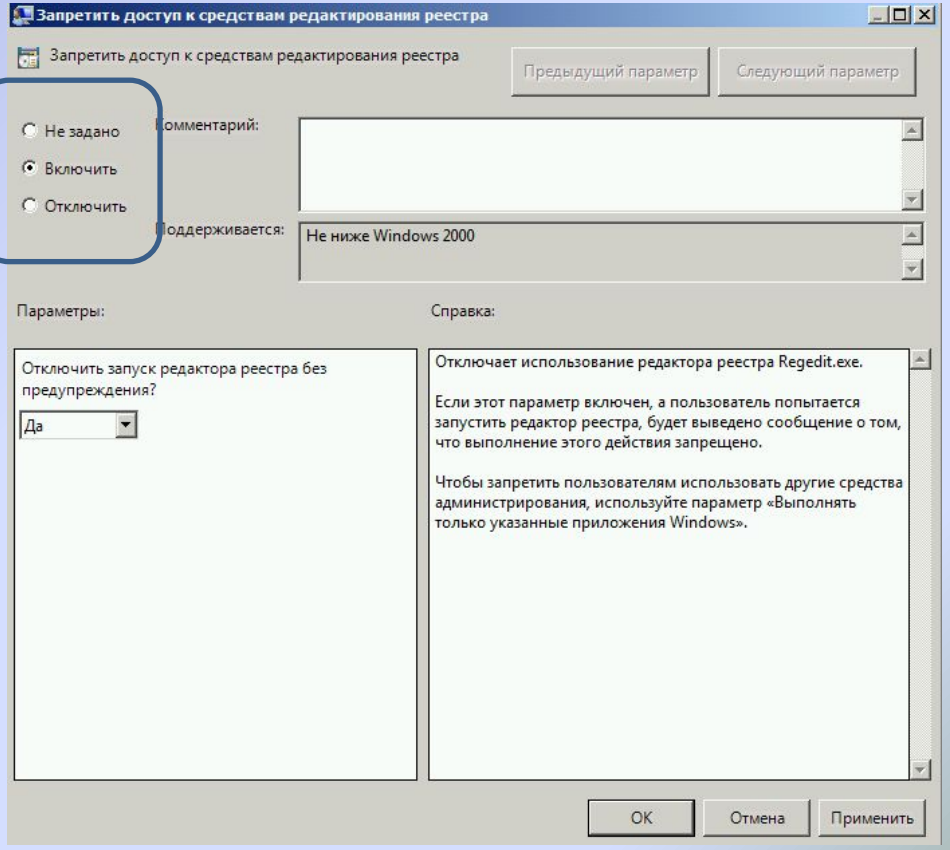
Учётные записи компьютеров

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



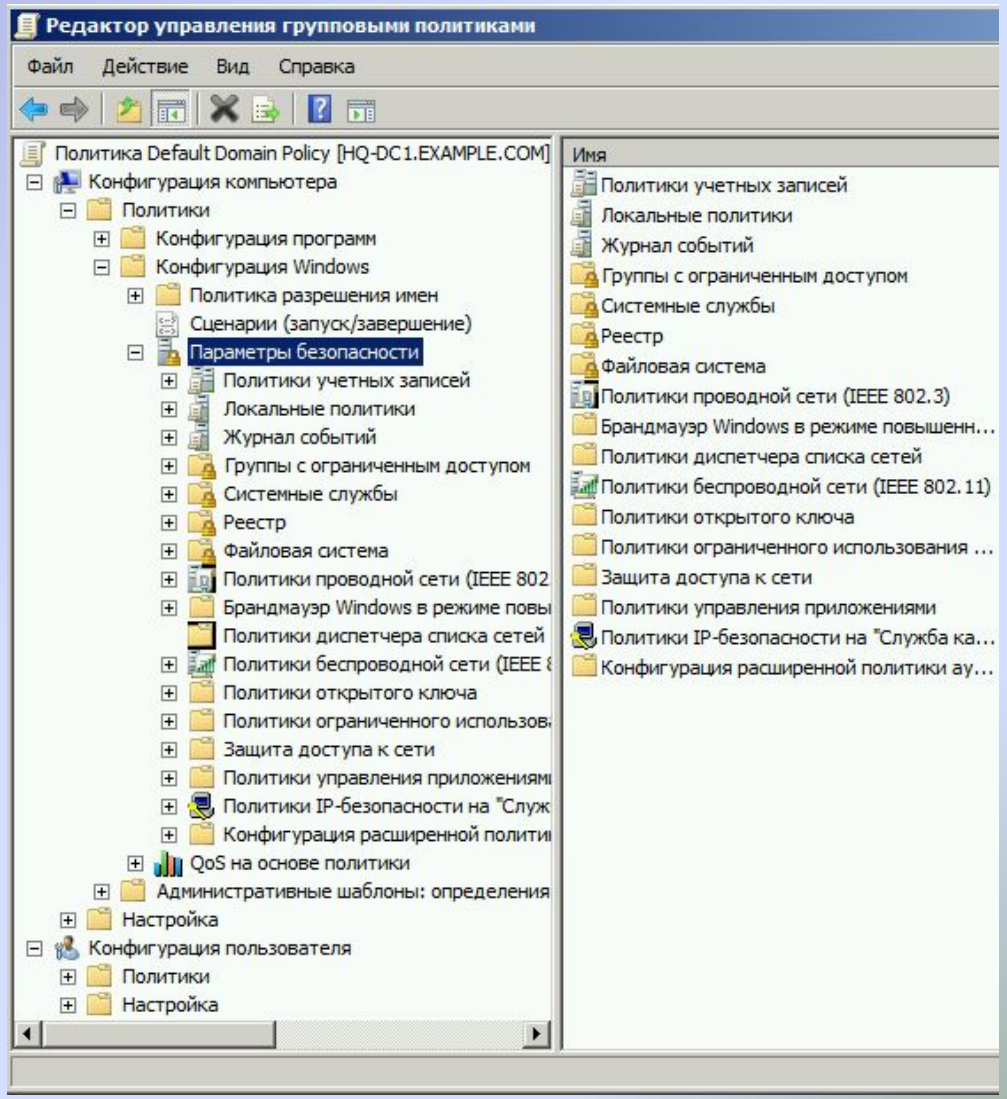
Параметры групповой политики

- 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)



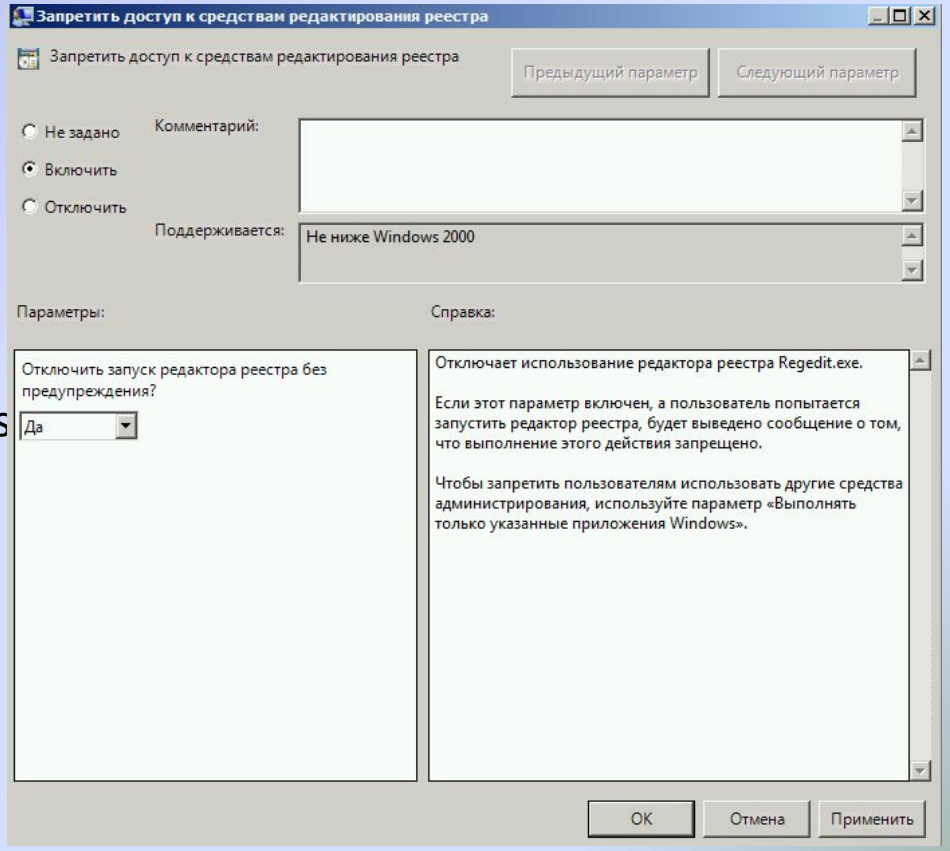
Объекты групповой политики

- 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

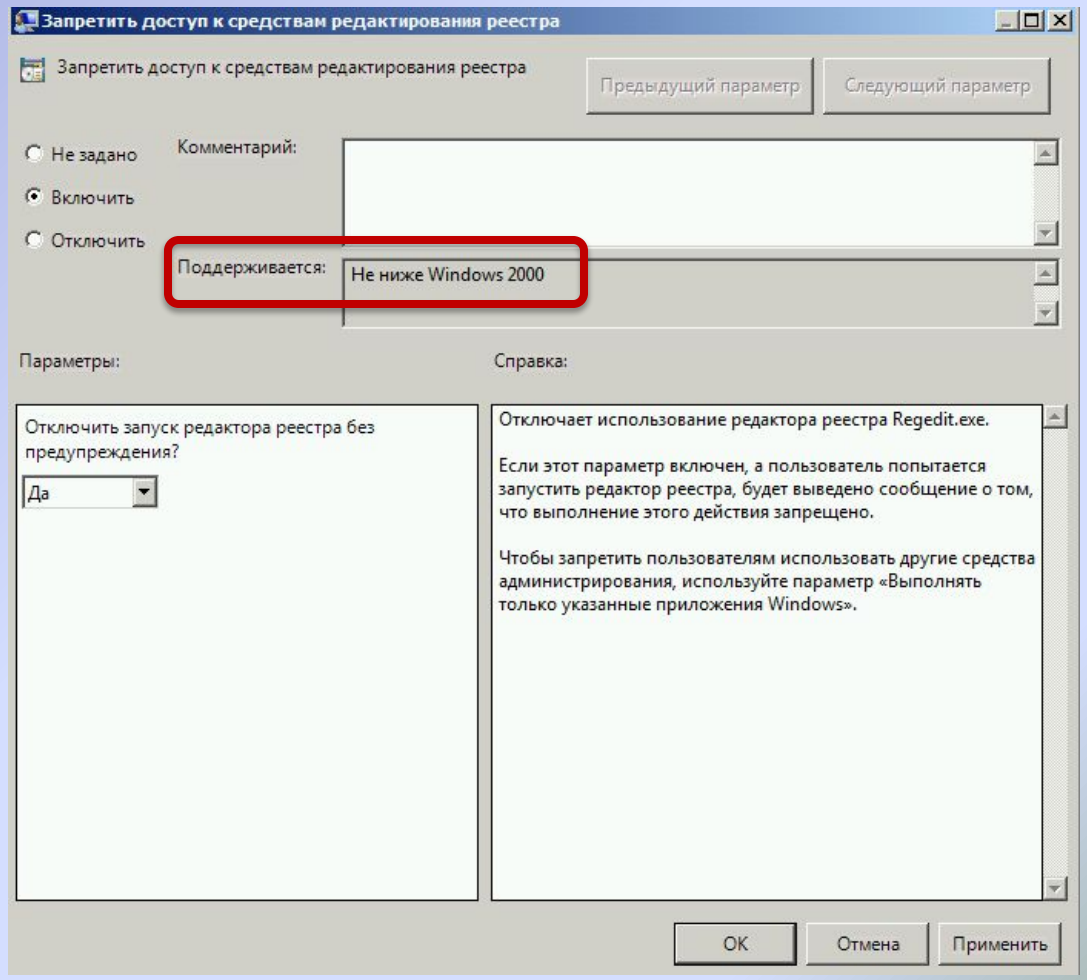


Клиент групповой политики и Client-side extensions

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

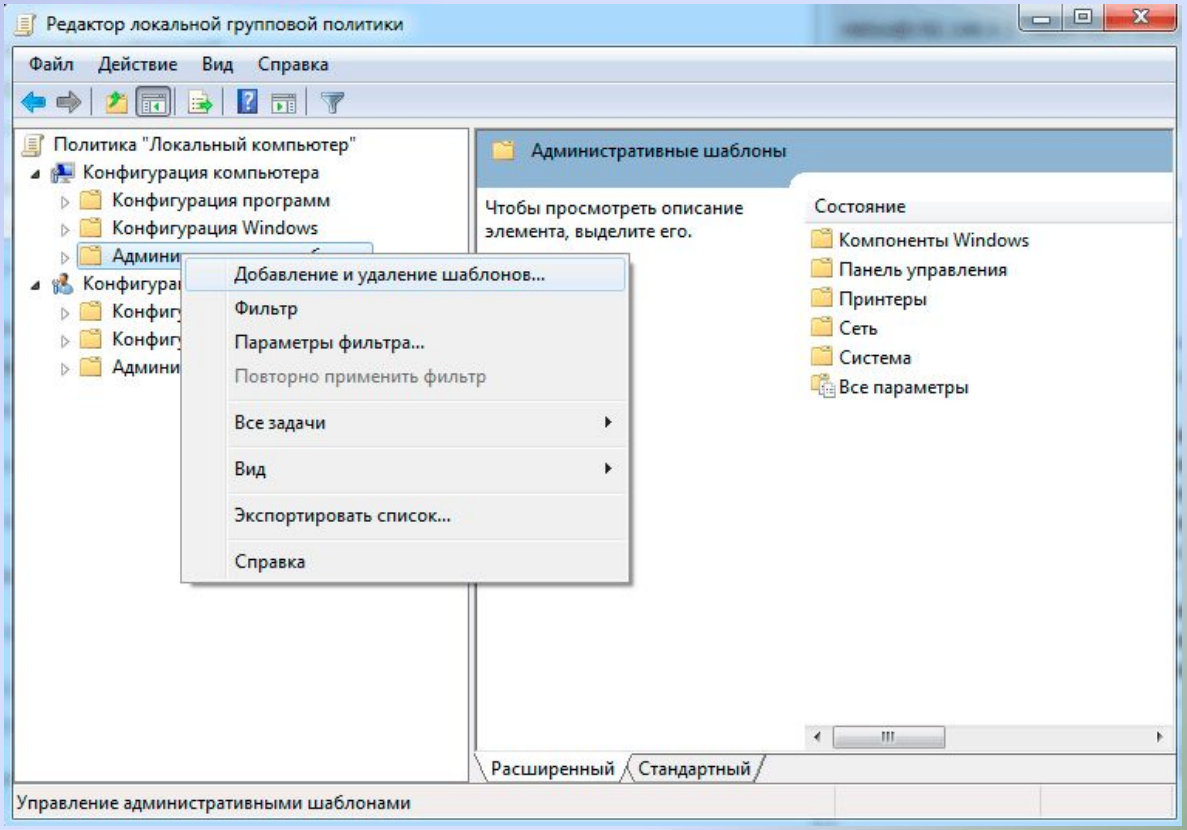
Применение политик разными операционными системами

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

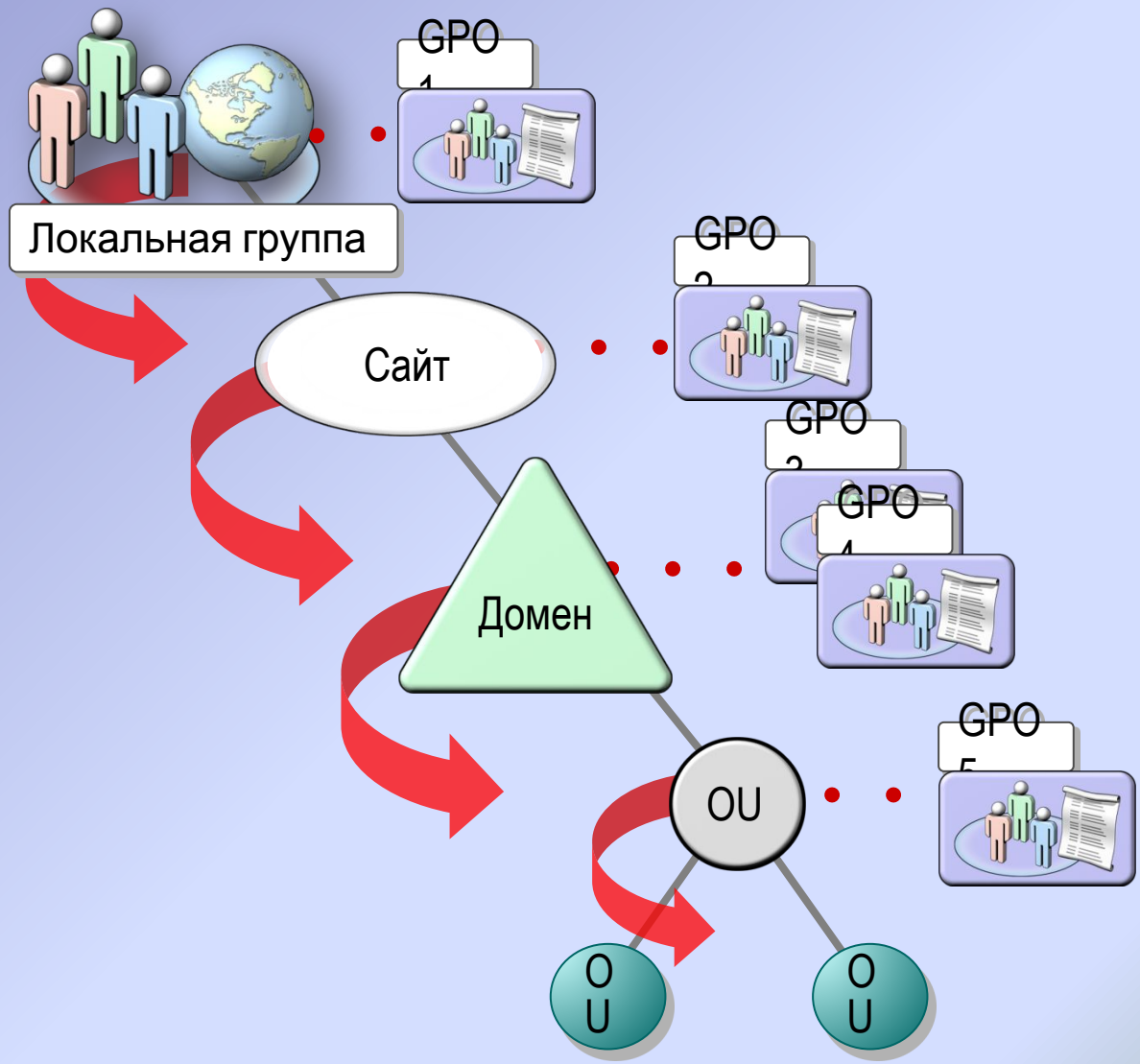


Расширение функционала с помощью административных шаблонов

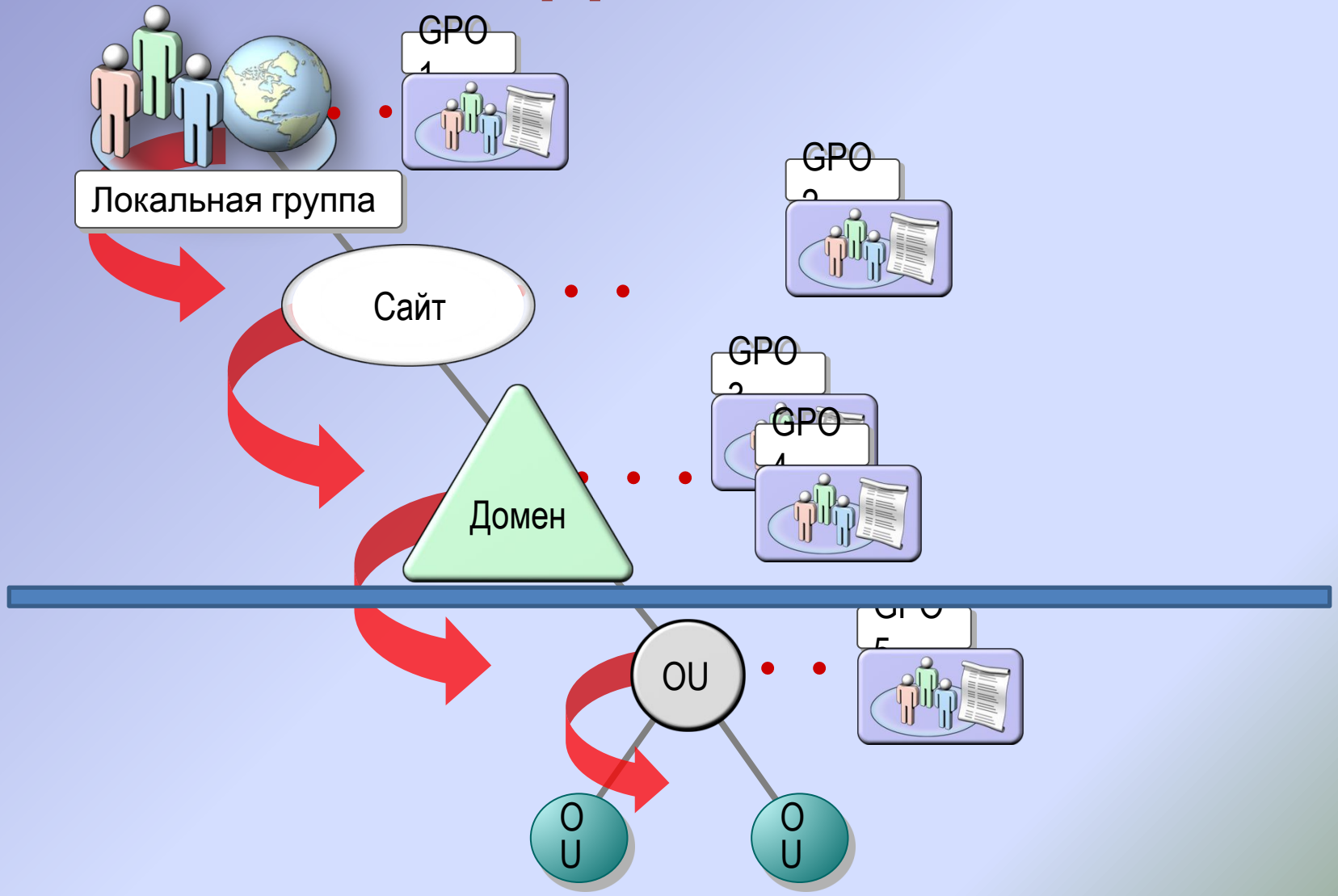
- Административные шаблоны позволяют централизованно управлять программным обеспечением:
  - Microsoft Office, Google Chrome, etc
- ADM
- ADMX/ADML



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
  - GPUpdate
- Конфигурация пользователя
  - Вход в систему
  - Каждые 90-120 минут
  - GPUpdate

Предпочтения групповой политики

Предпочтения групповых политик расширяют диапазон настраиваемых параметров GPO и:

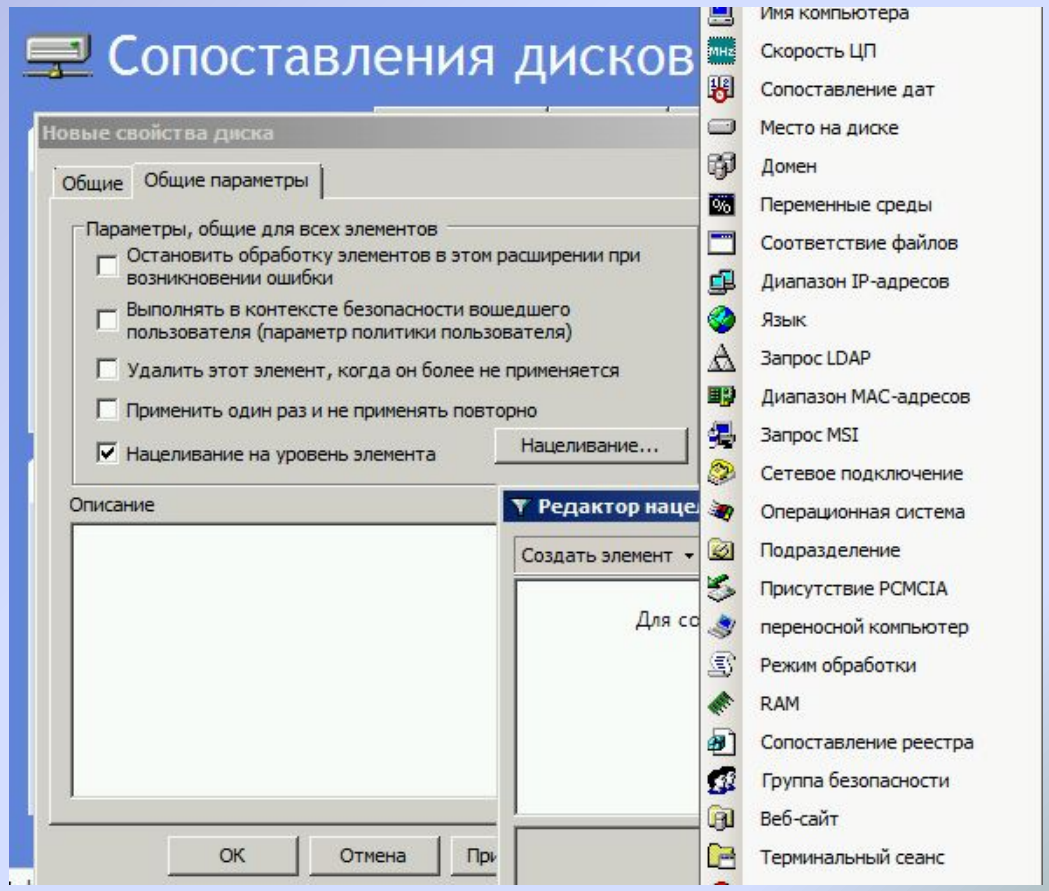
- Не блокируют настройки от изменения пользователем
- Позволяют настраивать параметры операционной системы и ПО
- иначе управляемые загрузочными скриптами (создавать ярлыки,
- подключать сетевые диски и т.д.

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

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

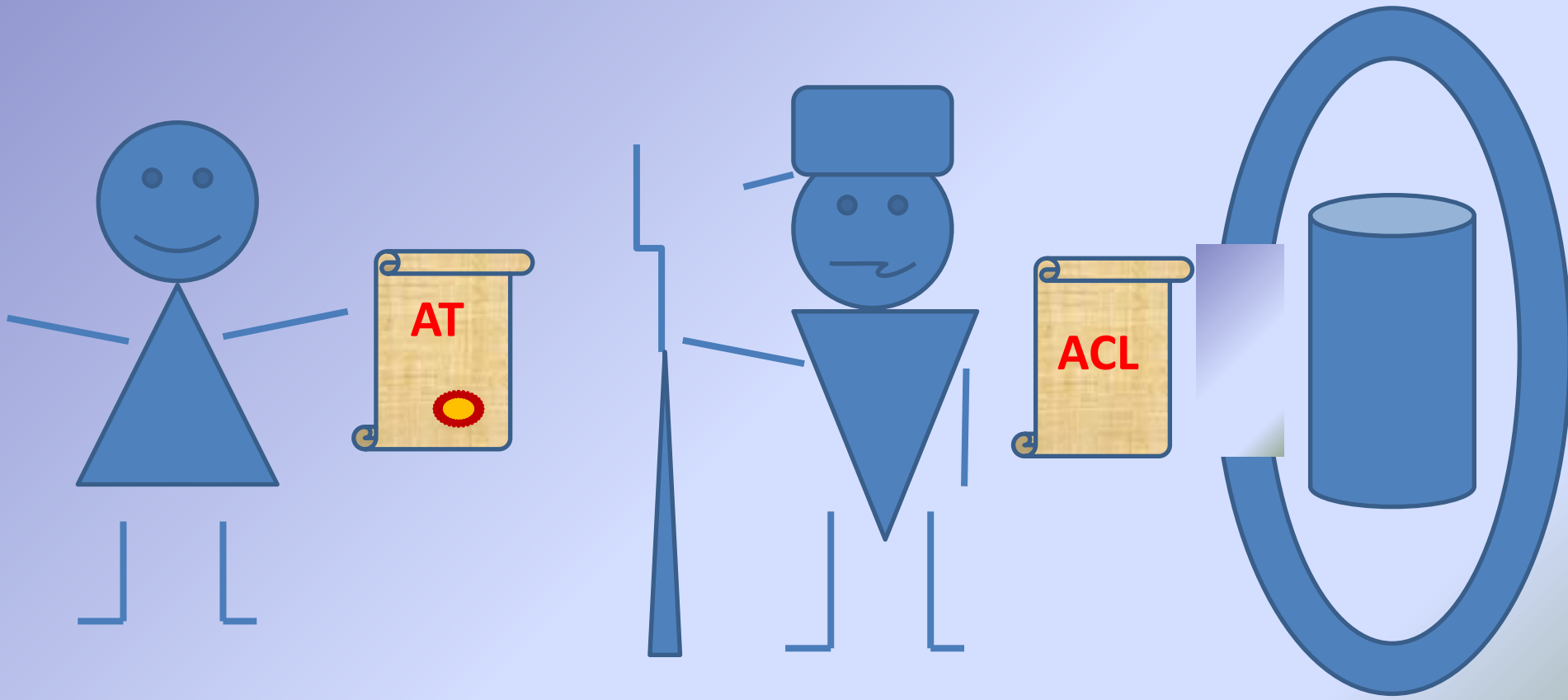
AD

Передача

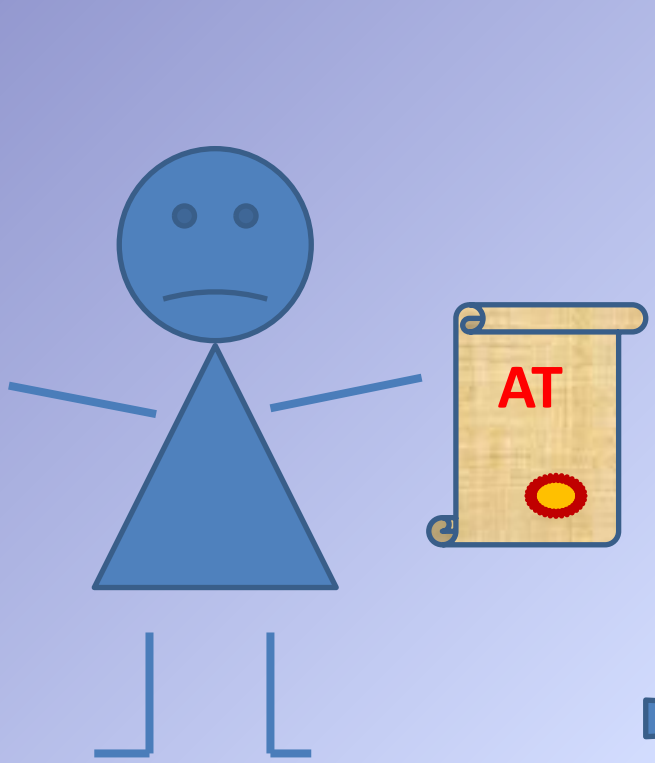
Intranet Routing IPSec RMS NIDS-NIPS

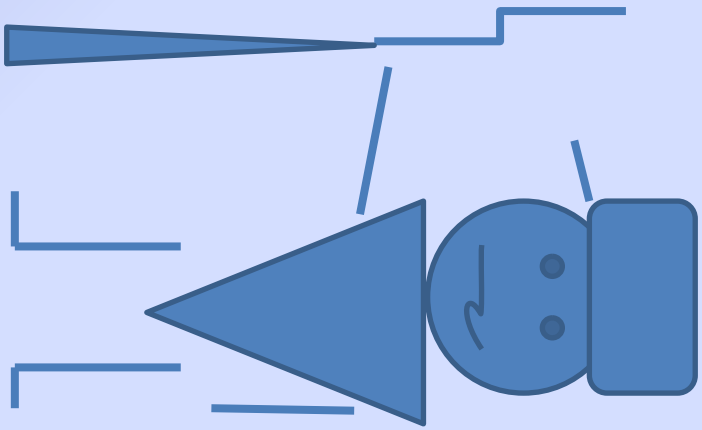
Internet Firewall VPN NAP

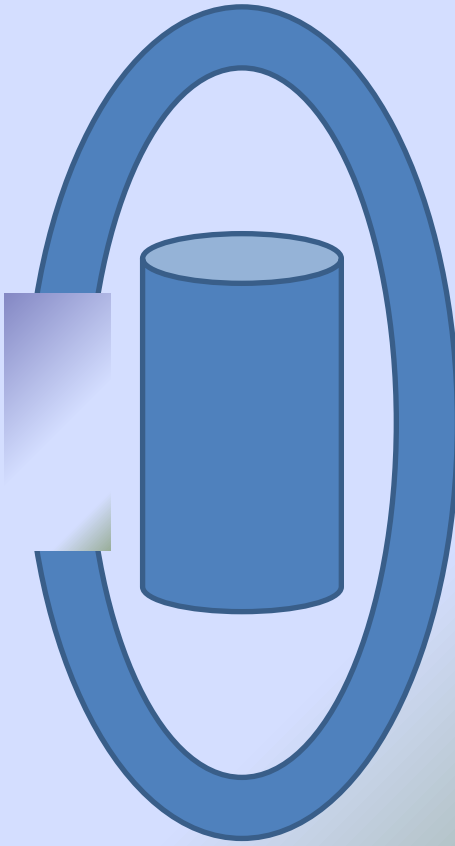
Список контроля доступа



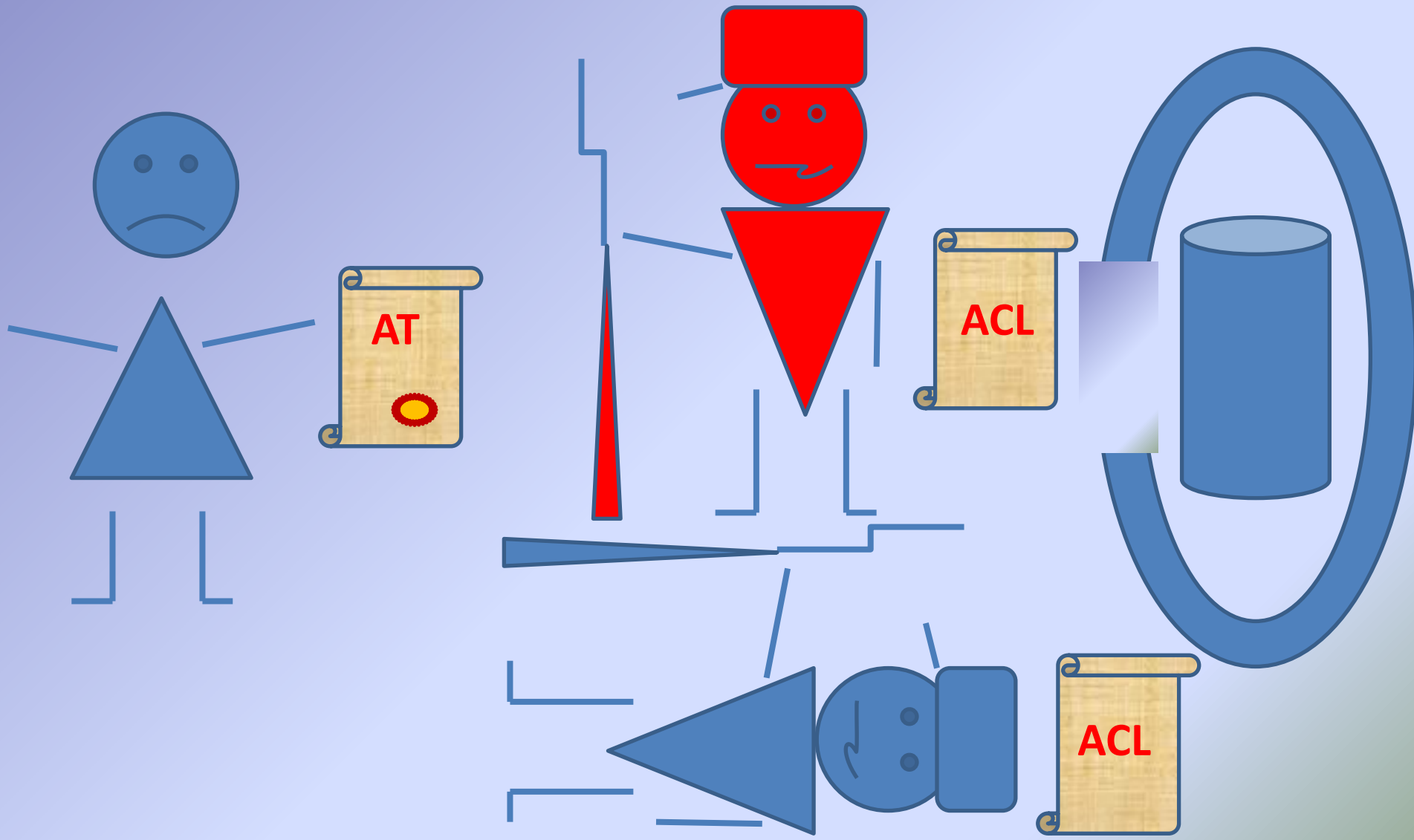
Список контроля доступа







Список контроля доступа

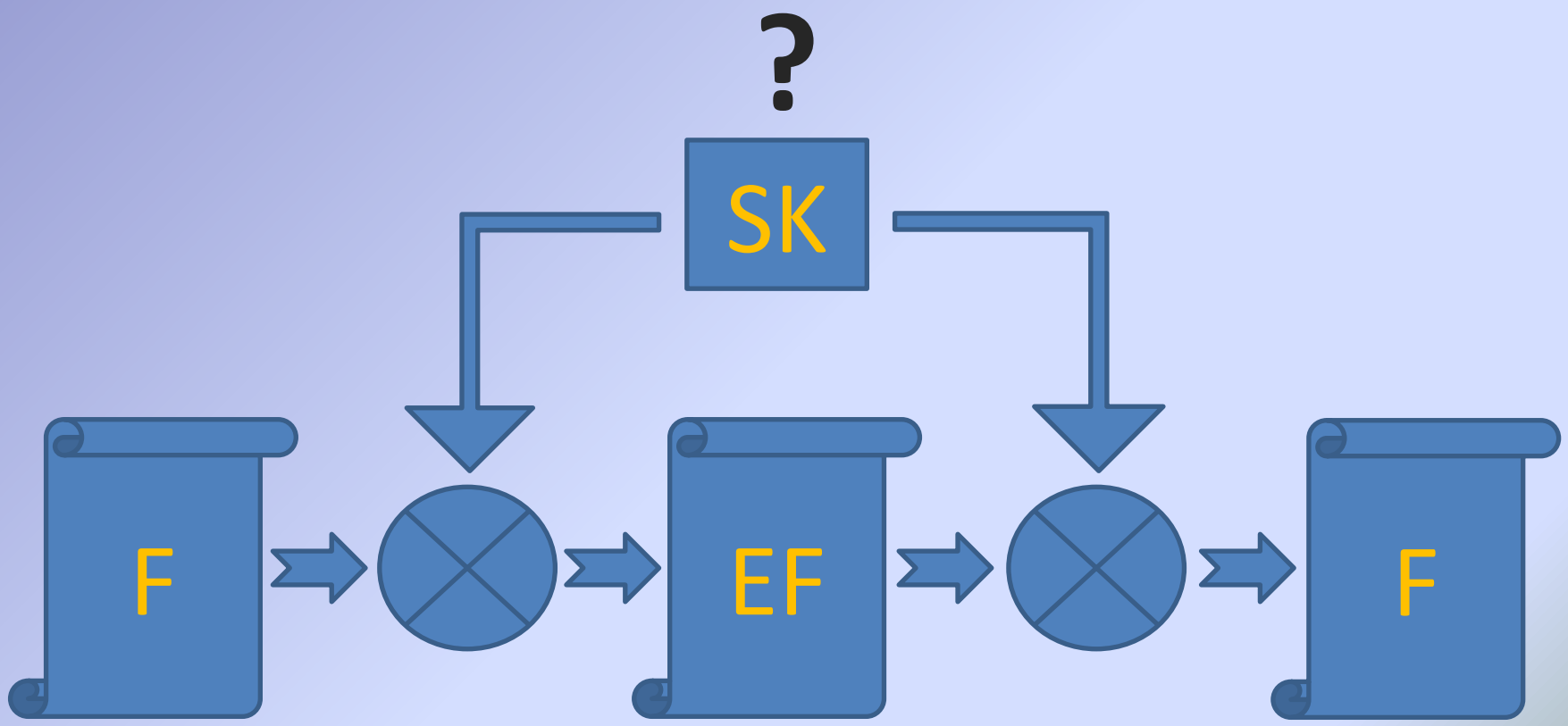


Шифрование с симметричным ключом

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

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

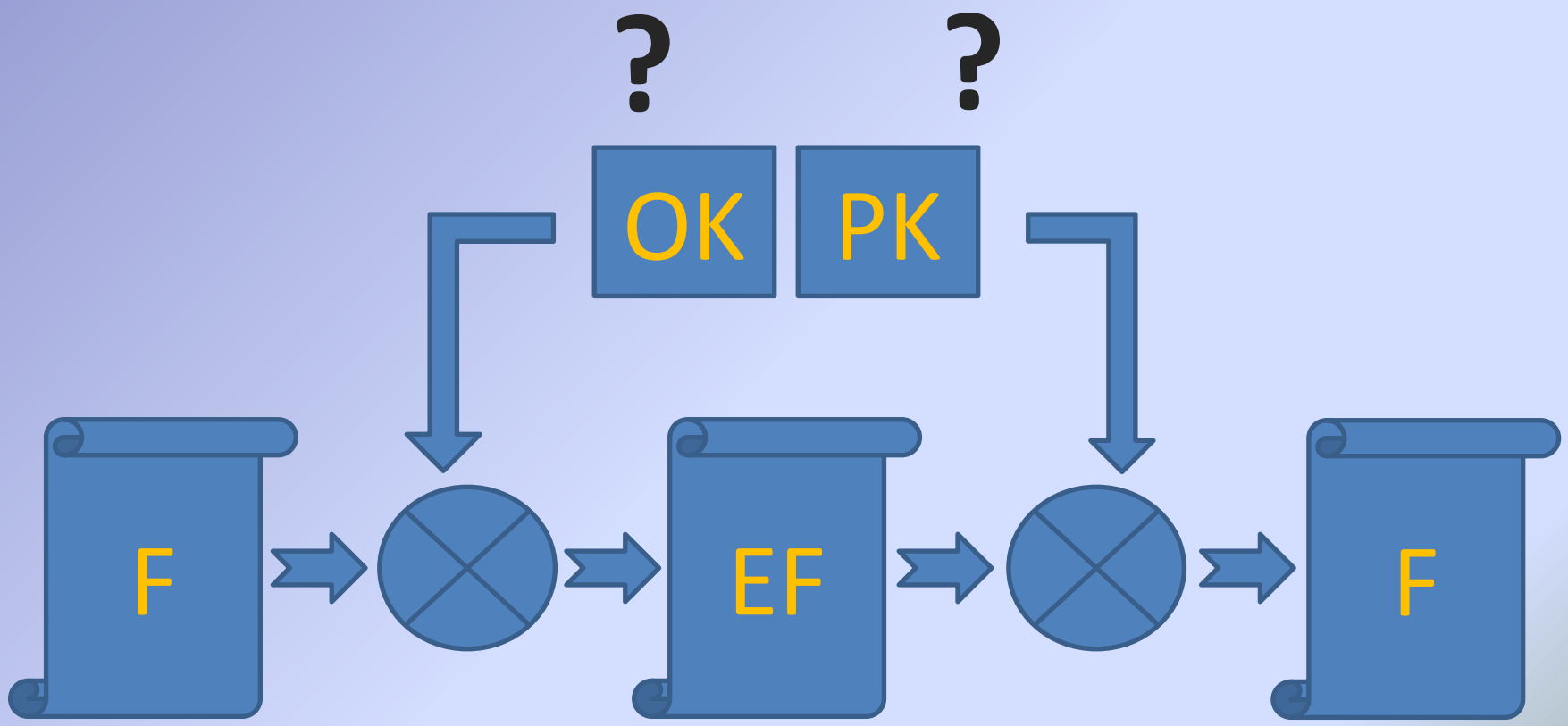
Простейший вариант



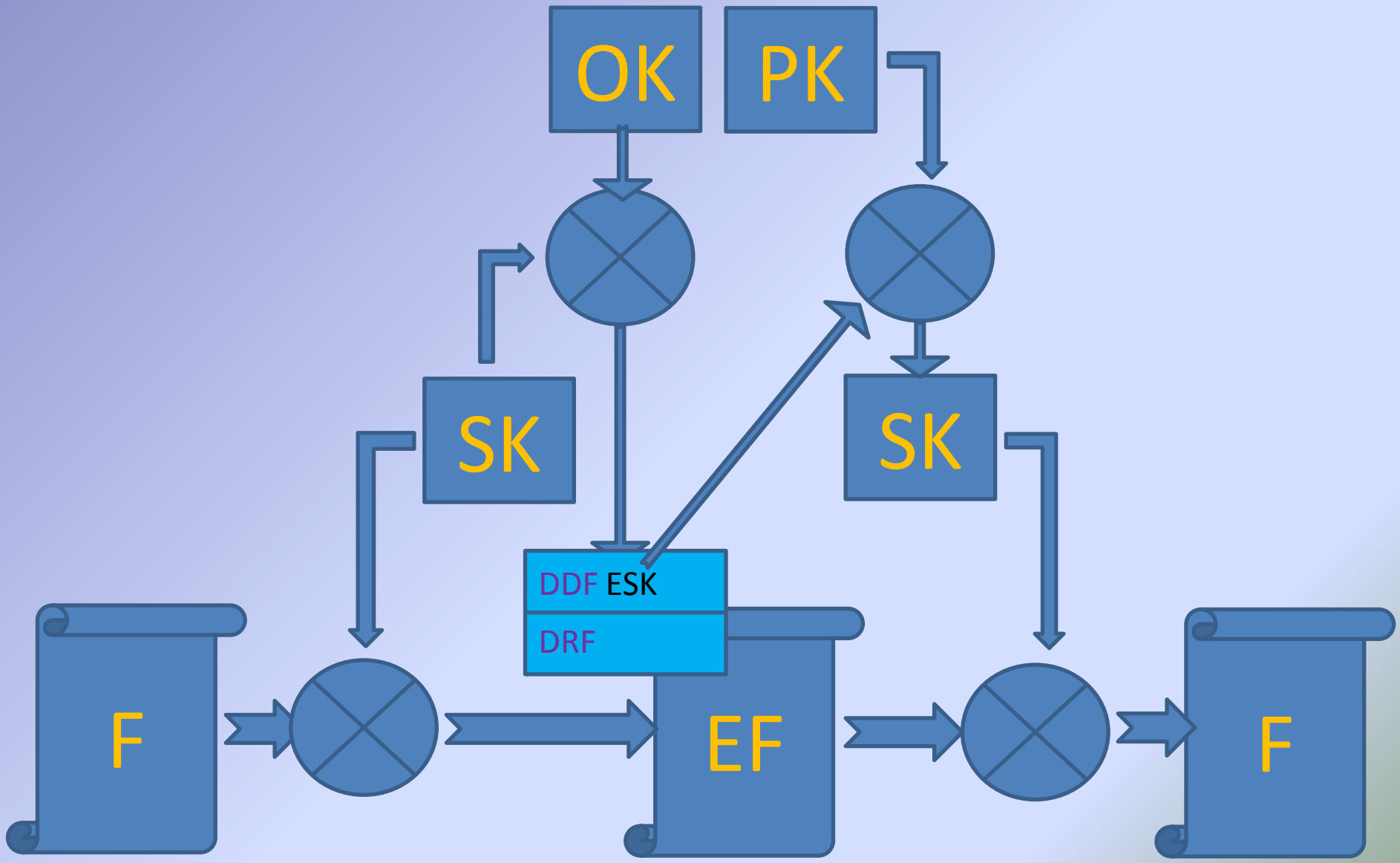
Шифрование с асимметричным ключом (открытым и закрытым ключами)

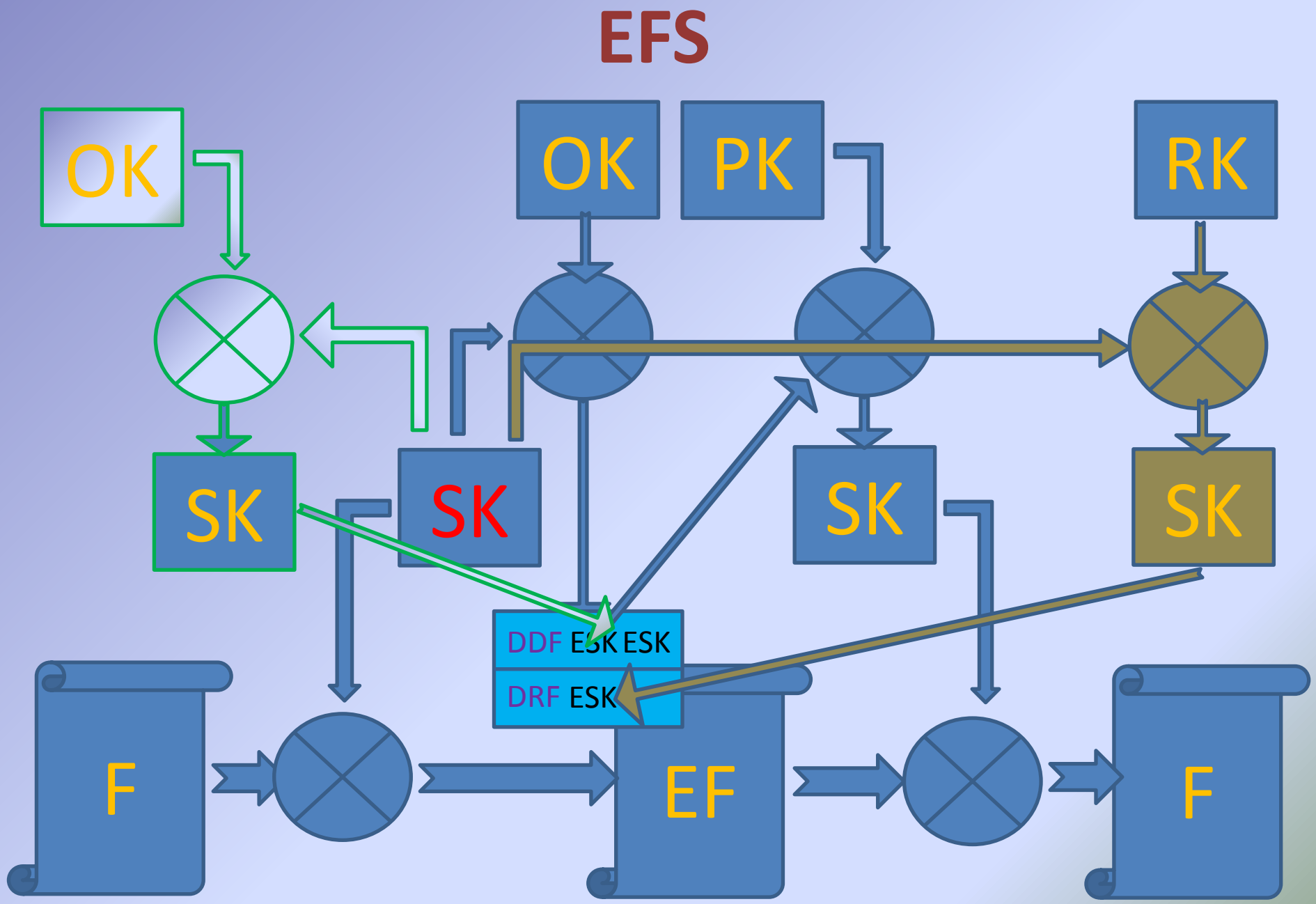
G->(o,p)	G->(o,p)
T(a,o) = e	T(a,p) = e
T^{-1}(e,p) = a	T^{-1}(e,o) = a

А можно так?

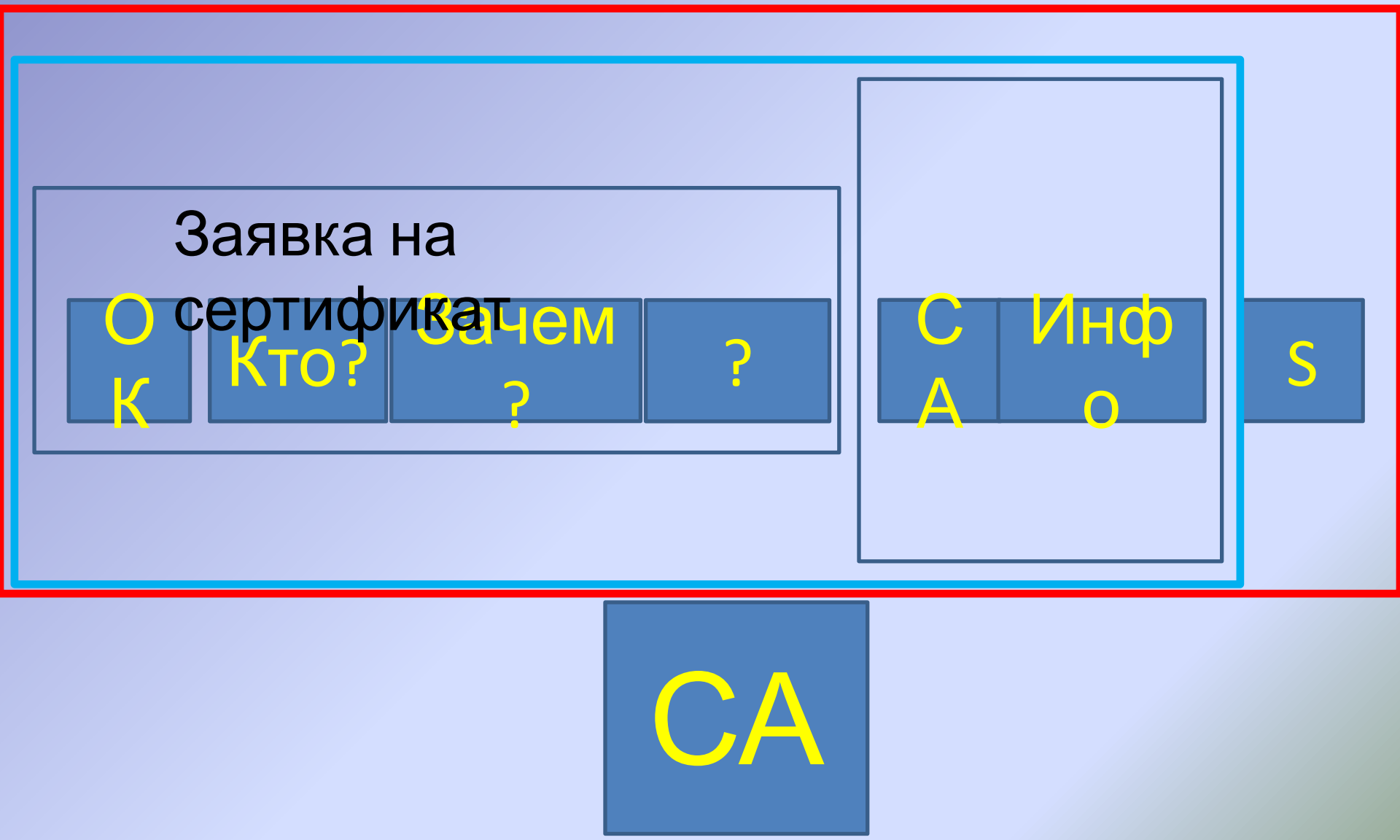


Уже правильнее

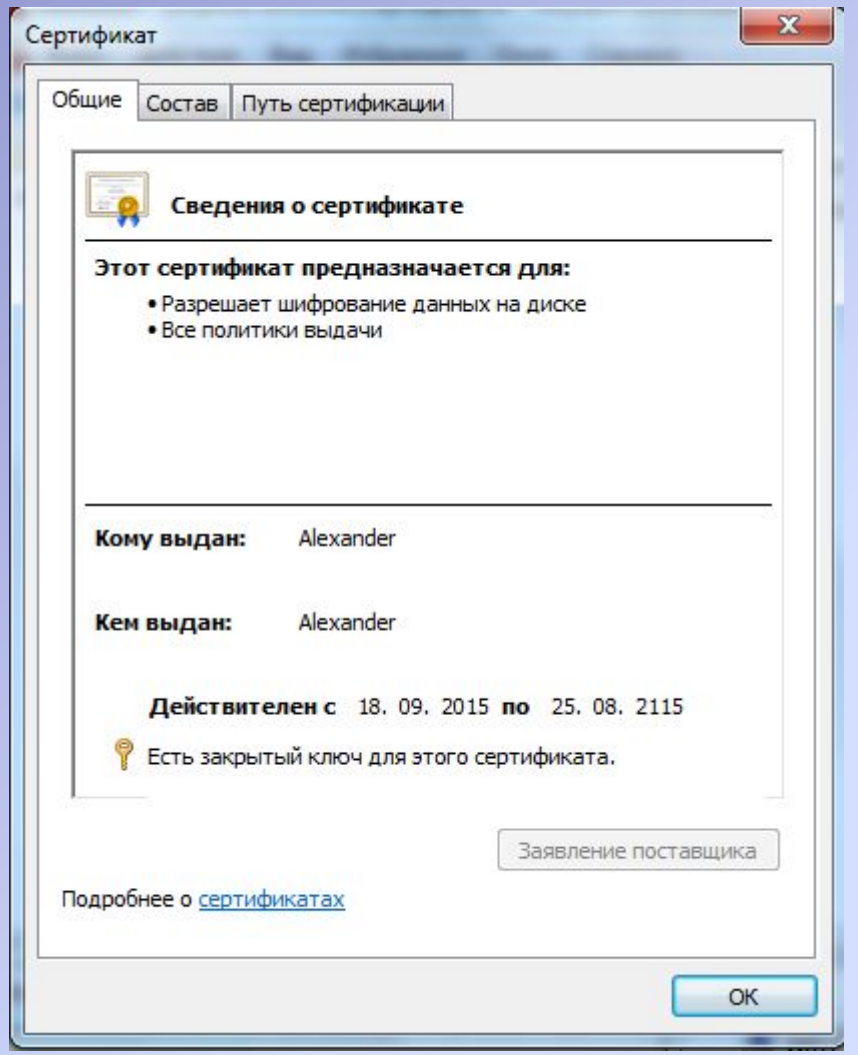


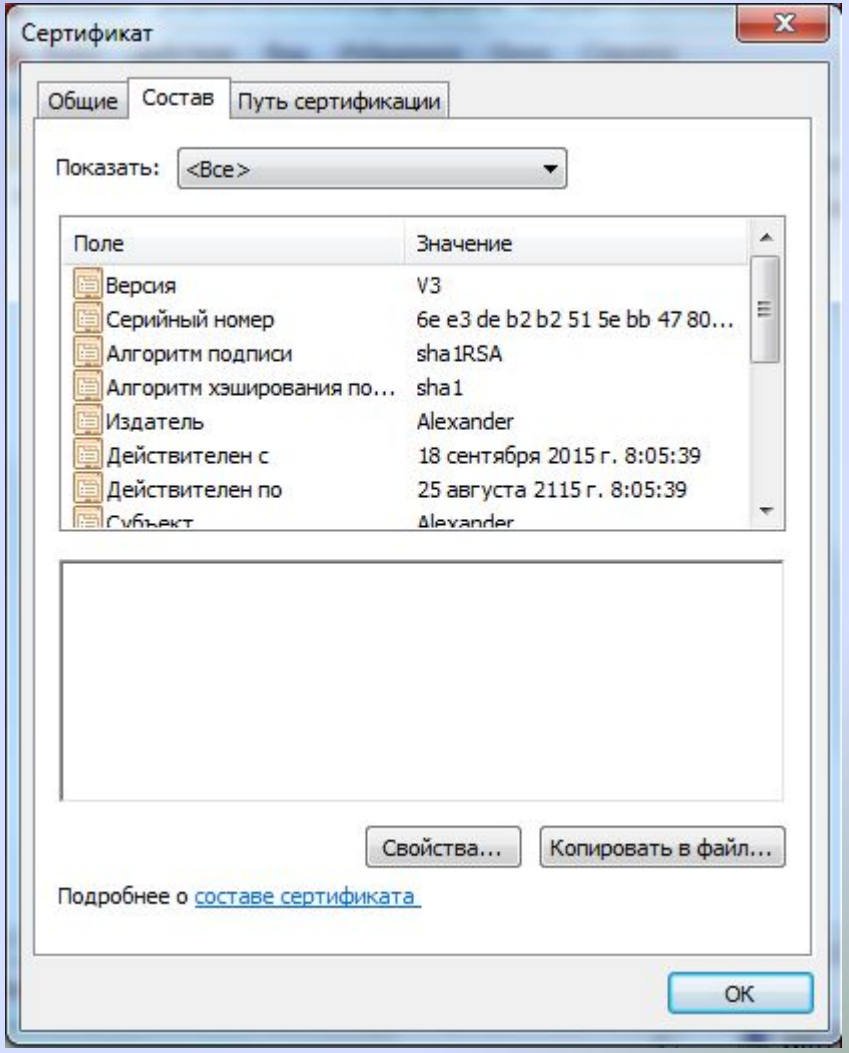

EFS
OK
OK
PK
RK
SK
SK
SK
SK
DDF ESK ESK
DRF ESK
F
EF
F

Формирование сертификата

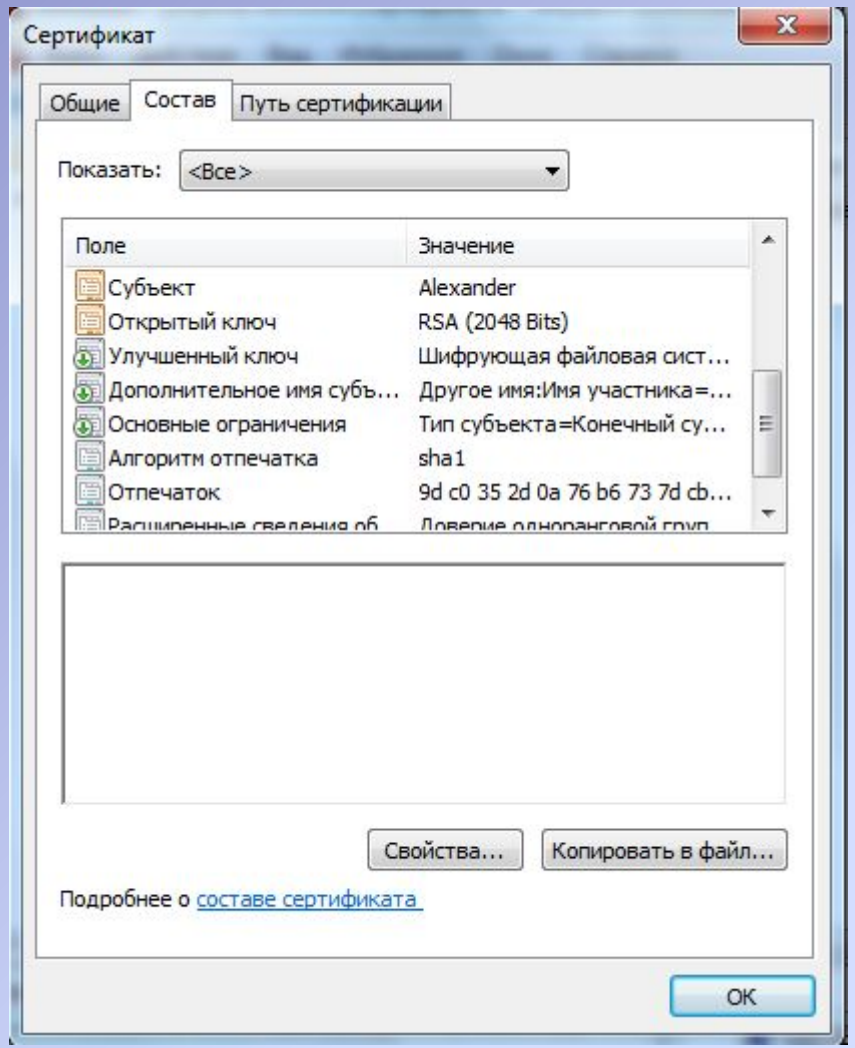


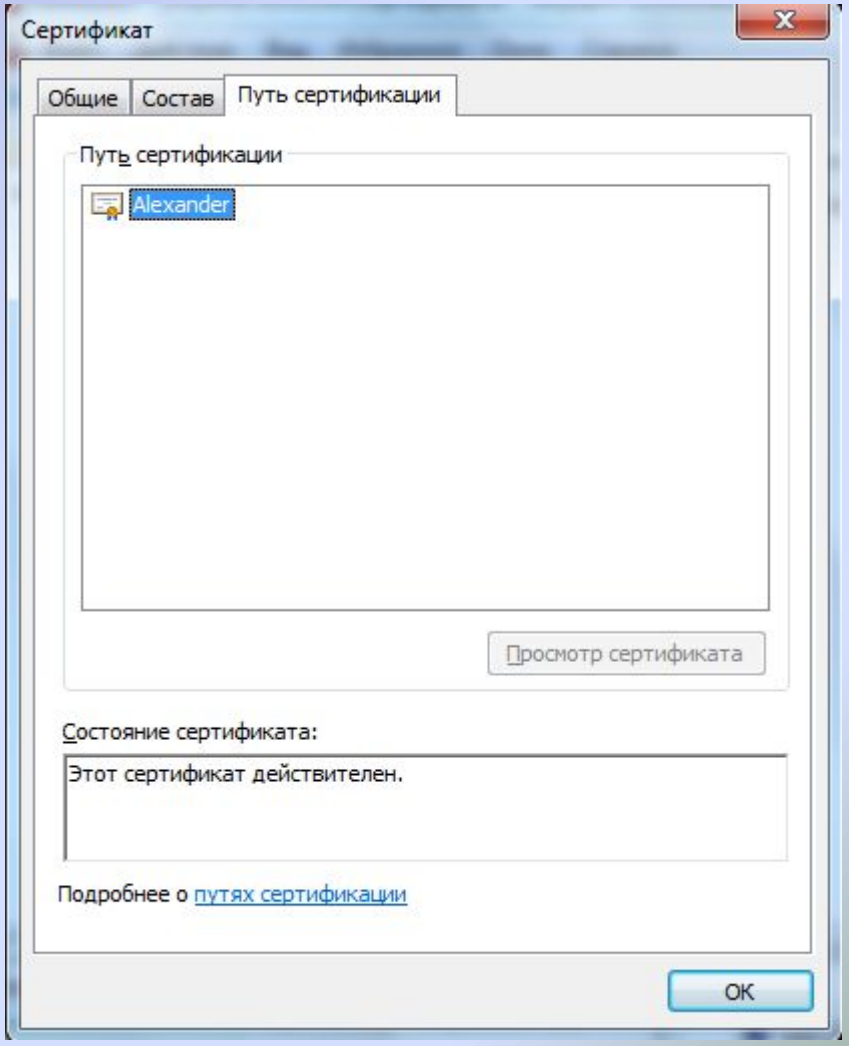
Сертификат


Сертификат
Общие
Состав
Путь сертификации
Сведения о сертификате
Этот сертификат предназначается для:
• Разрешает шифрование данных на диске
• Все политики выдачи
Кому выдан: Alexander
Кем выдан: Alexander
Действителен с 18. 09. 2015 по 25. 08. 2115
Есть закрытый ключ для этого сертификата.
Заявление поставщика
Подробнее о сертификатах
OK

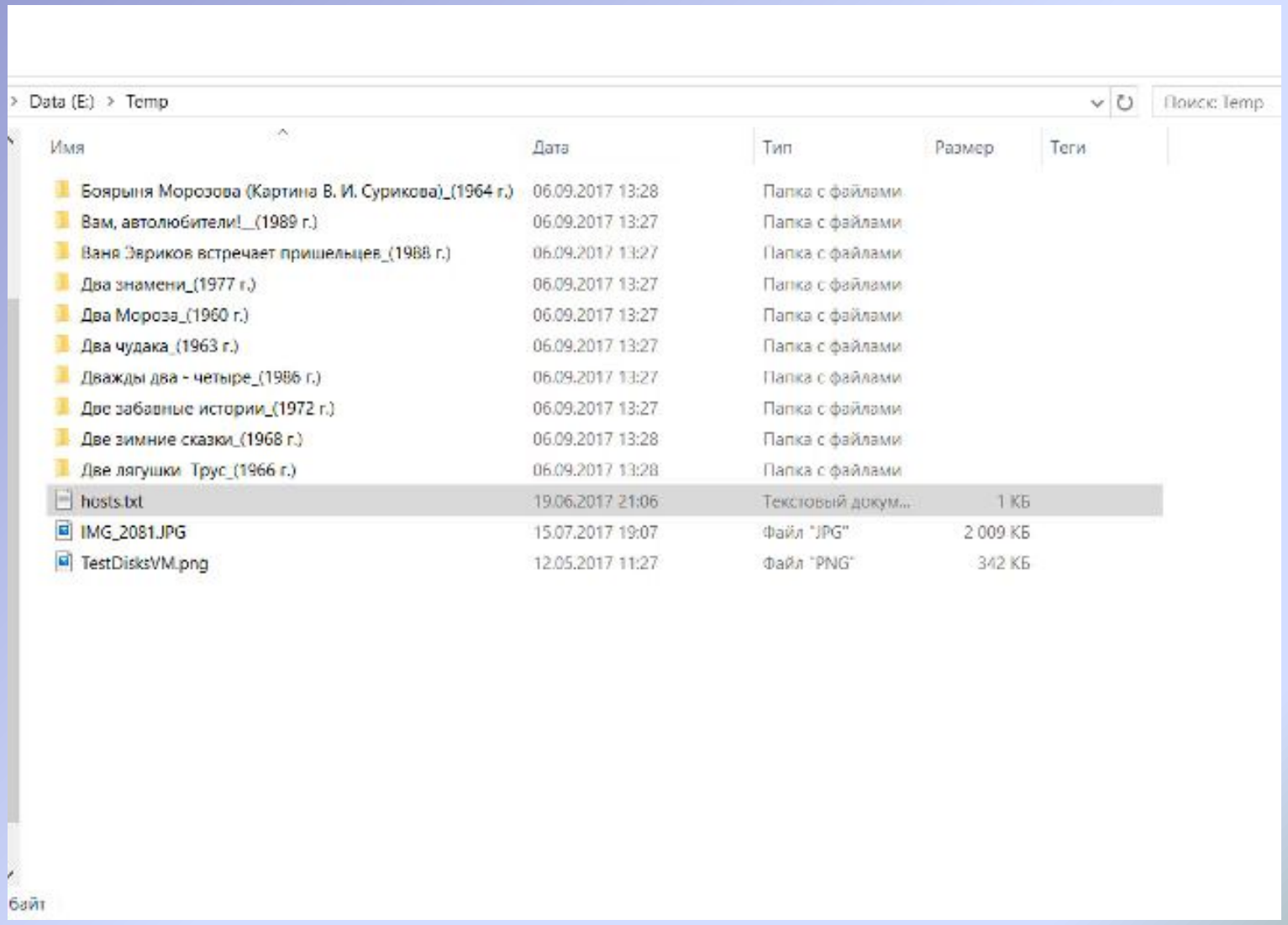

Сертификат
Общие
Состав
Путь сертификации
Показать: <Все>
Поле
Значение
Версия V3
Серийный номер 6e e3 de b2 b2 51 5e bb 47 80...
Алгоритм подписи sha1RSA
Алгоритм хэширования по... sha1
Издатель Alexander
Действителен с 18 сентября 2015 г. 8:05:39
Действителен по 25 августа 2115 г. 8:05:39
Субъект Alexander
Свойства...
Копировать в файл...
Подробнее о составе сертификата
OK

Сертификат


Сертификат
Общие
Состав
Путь сертификации
Показать:
<Все>
Поле
Значение
Субъект
Alexander
Открытый ключ
RSA (2048 Bits)
Улучшенный ключ
Шифрующая файловая сист...
Дополнительное имя субъ...
Другое имя:Имя участника=...
Основные ограничения
Тип субъекта=Конечный су...
Алгоритм отпечатка
sha1
Отпечаток
9d c0 35 2d 0a 76 b6 73 7d cb...
Свойства...
Копировать в файл...
Подробнее о составе сертификата
OK


Сертификат
Общие
Состав
Путь сертификации
Путь сертификации
Alexander
Просмотр сертификата
Состояние сертификата:
Этот сертификат действителен.
Подробнее о путях сертификации
OK

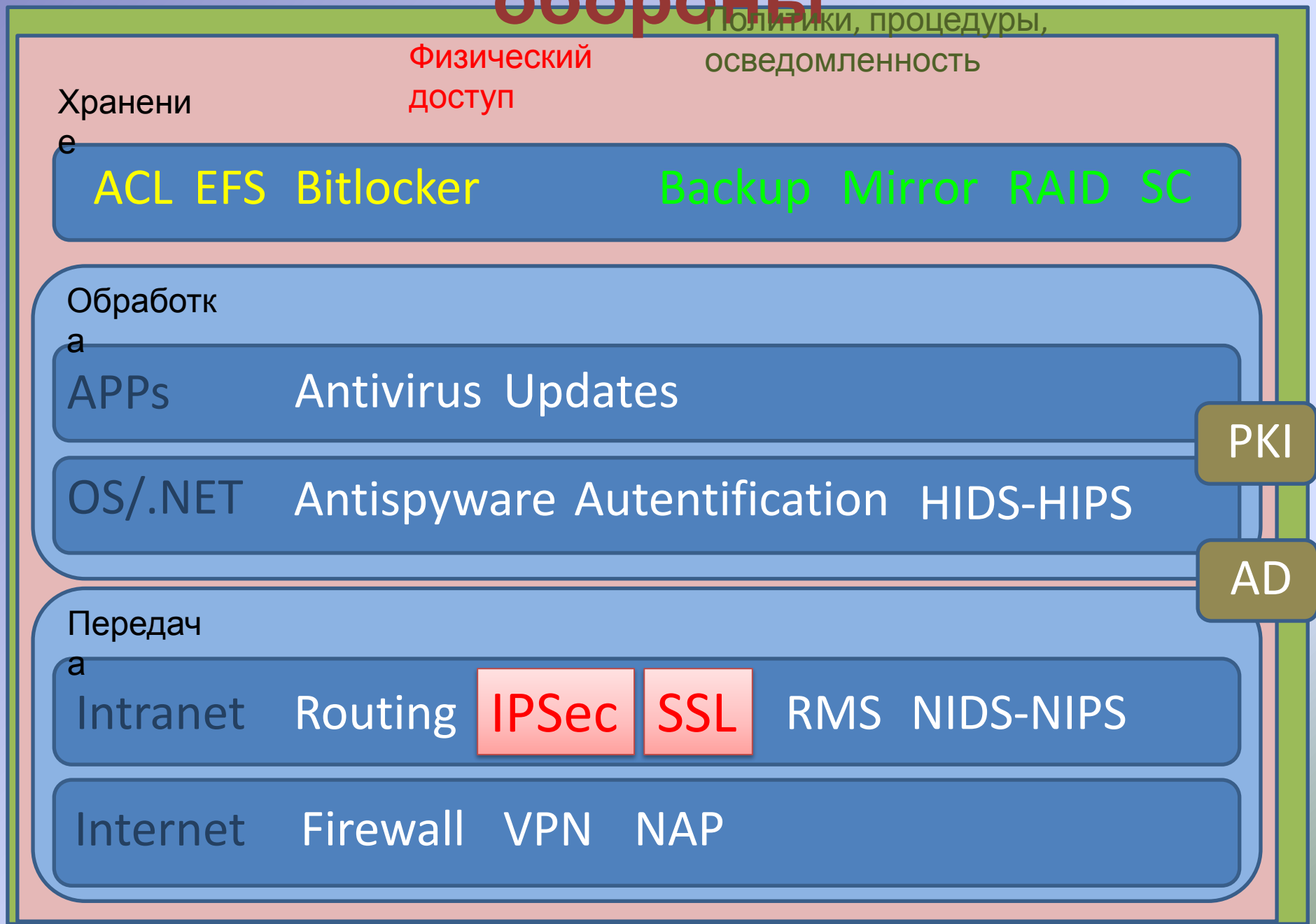
Интерфейс управления EFS



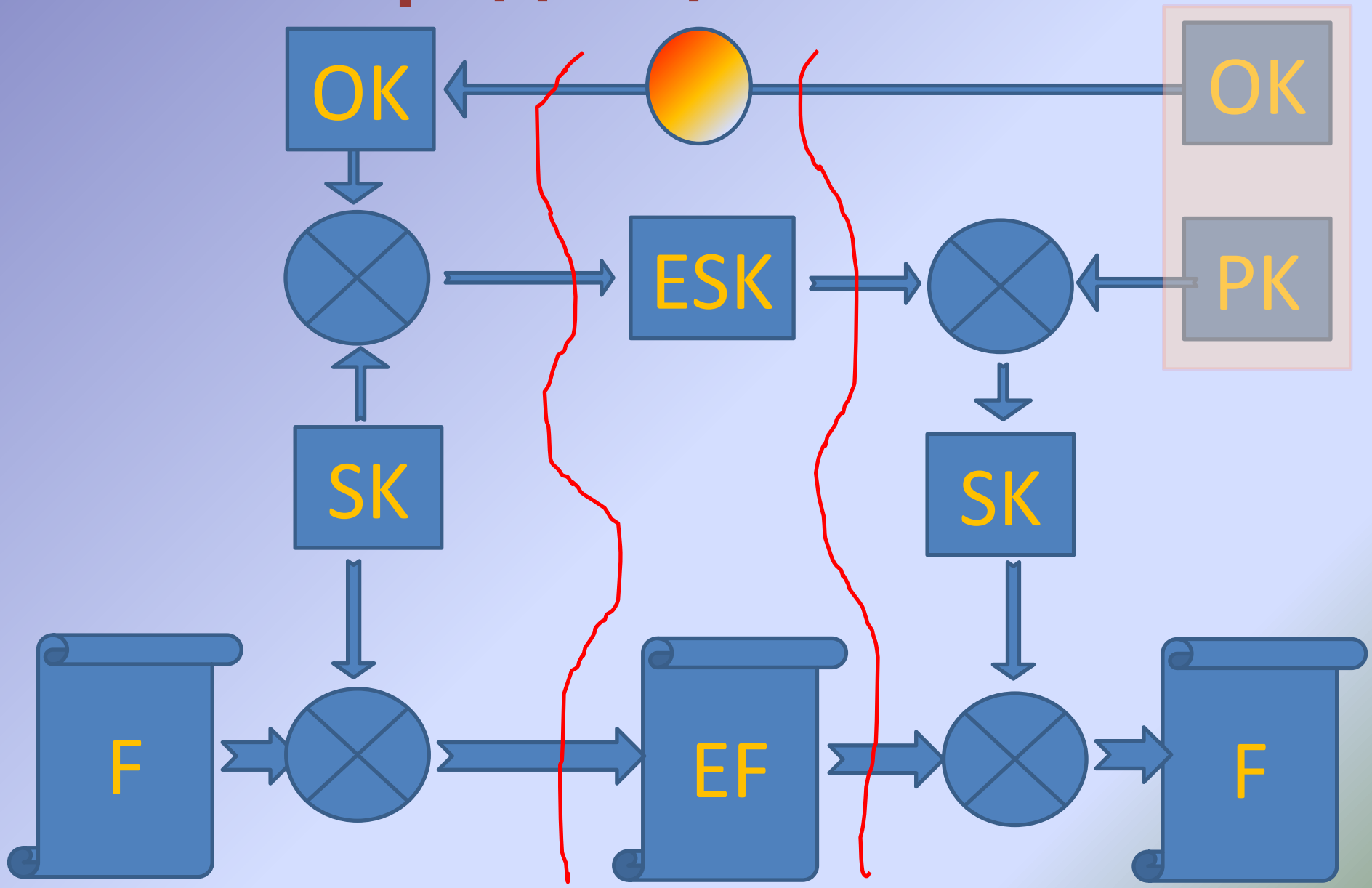
Взаимодействие внутри корпоративной сети.

IPsecurity. SSL.

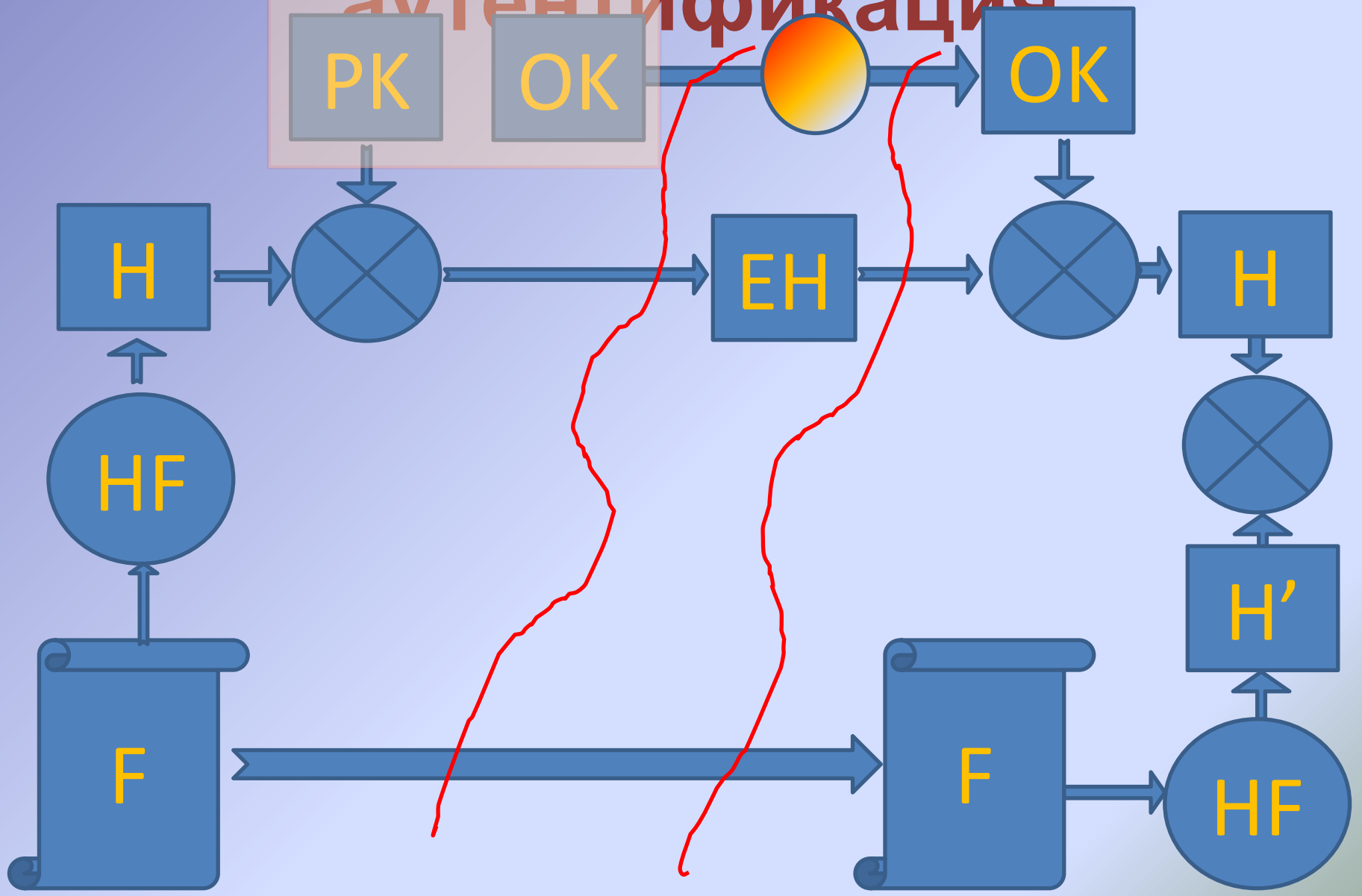
Модель эшелонированной обороны



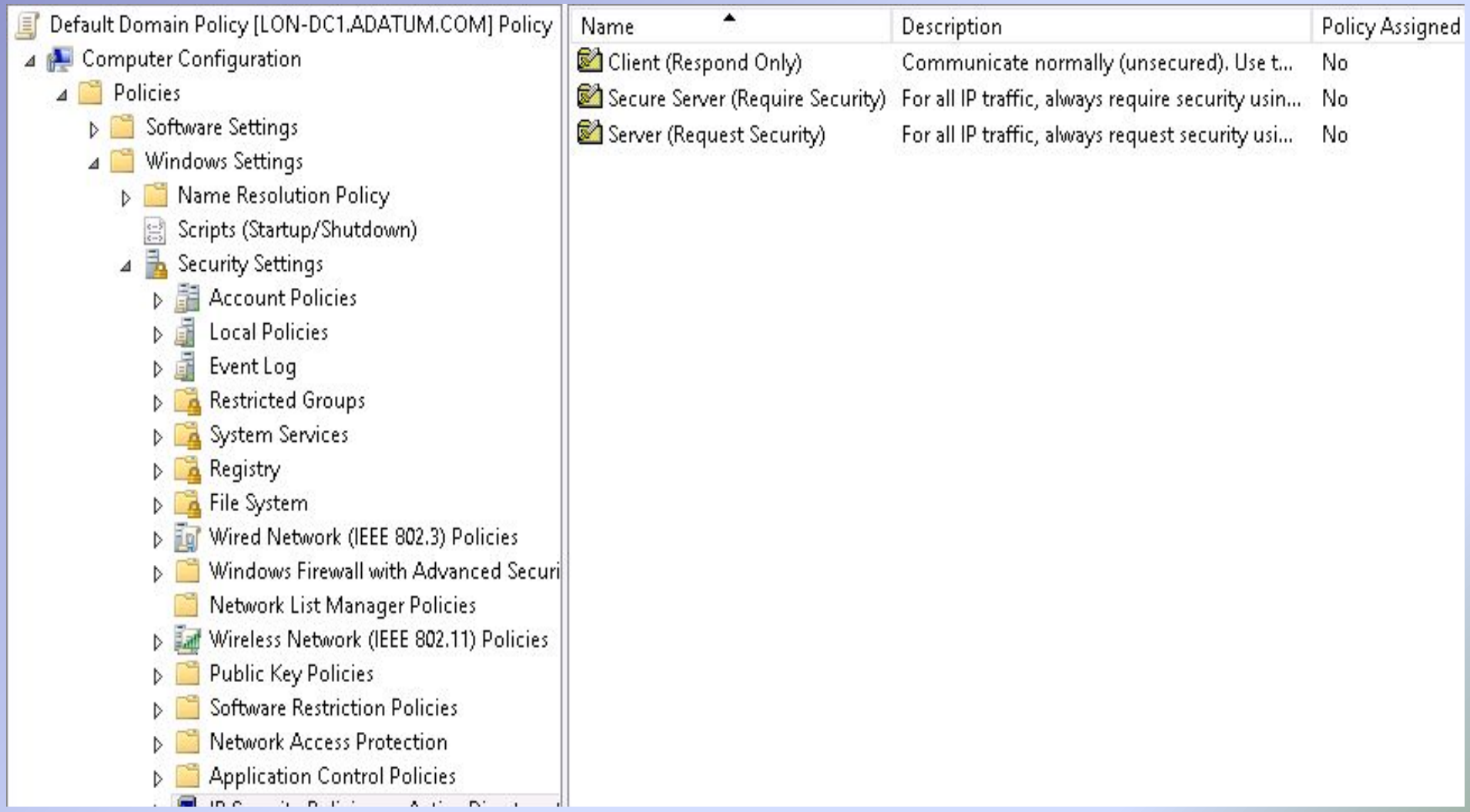
Конфиденциальность



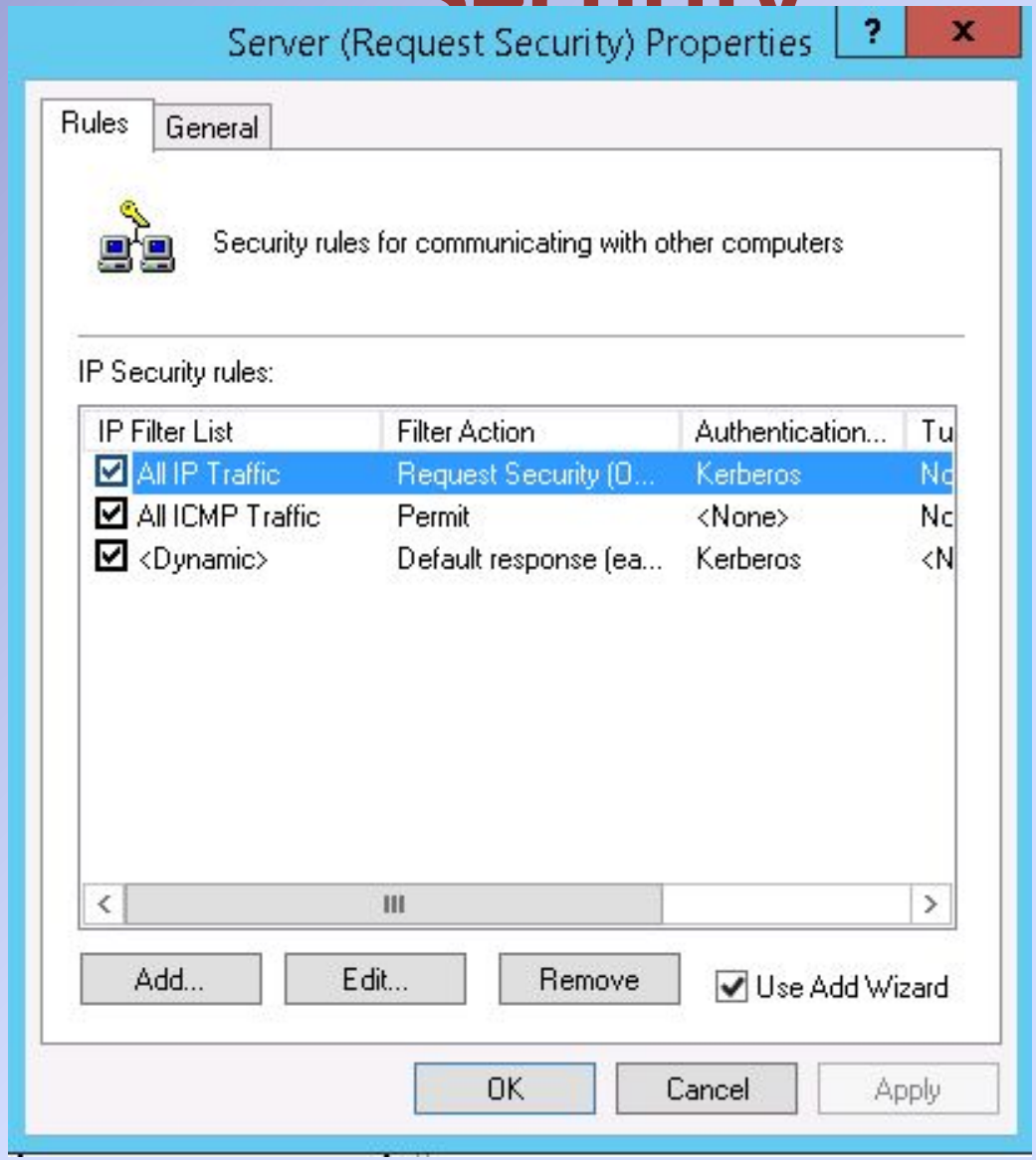
Целостность и аутентификация



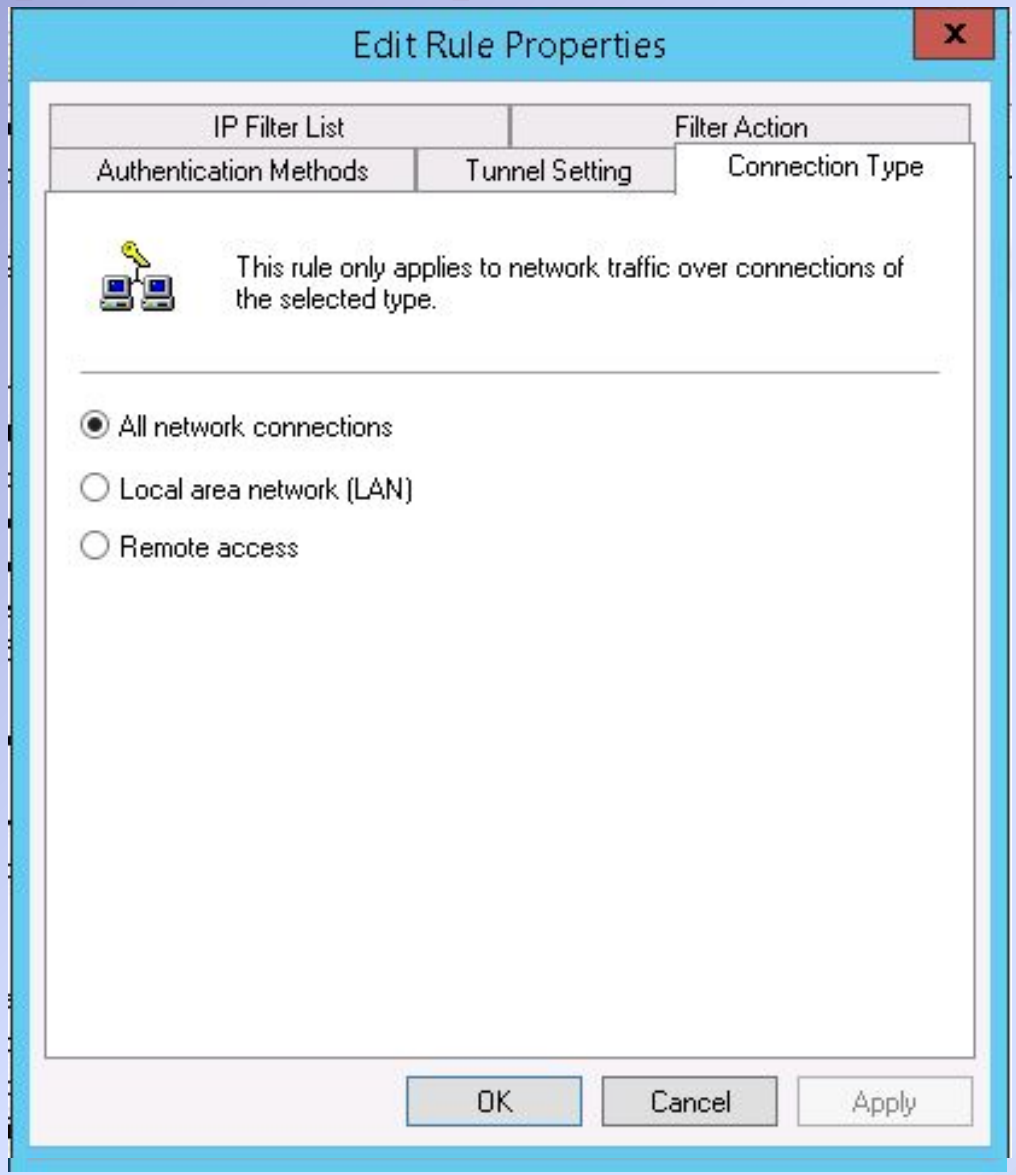
Настройка IP Security



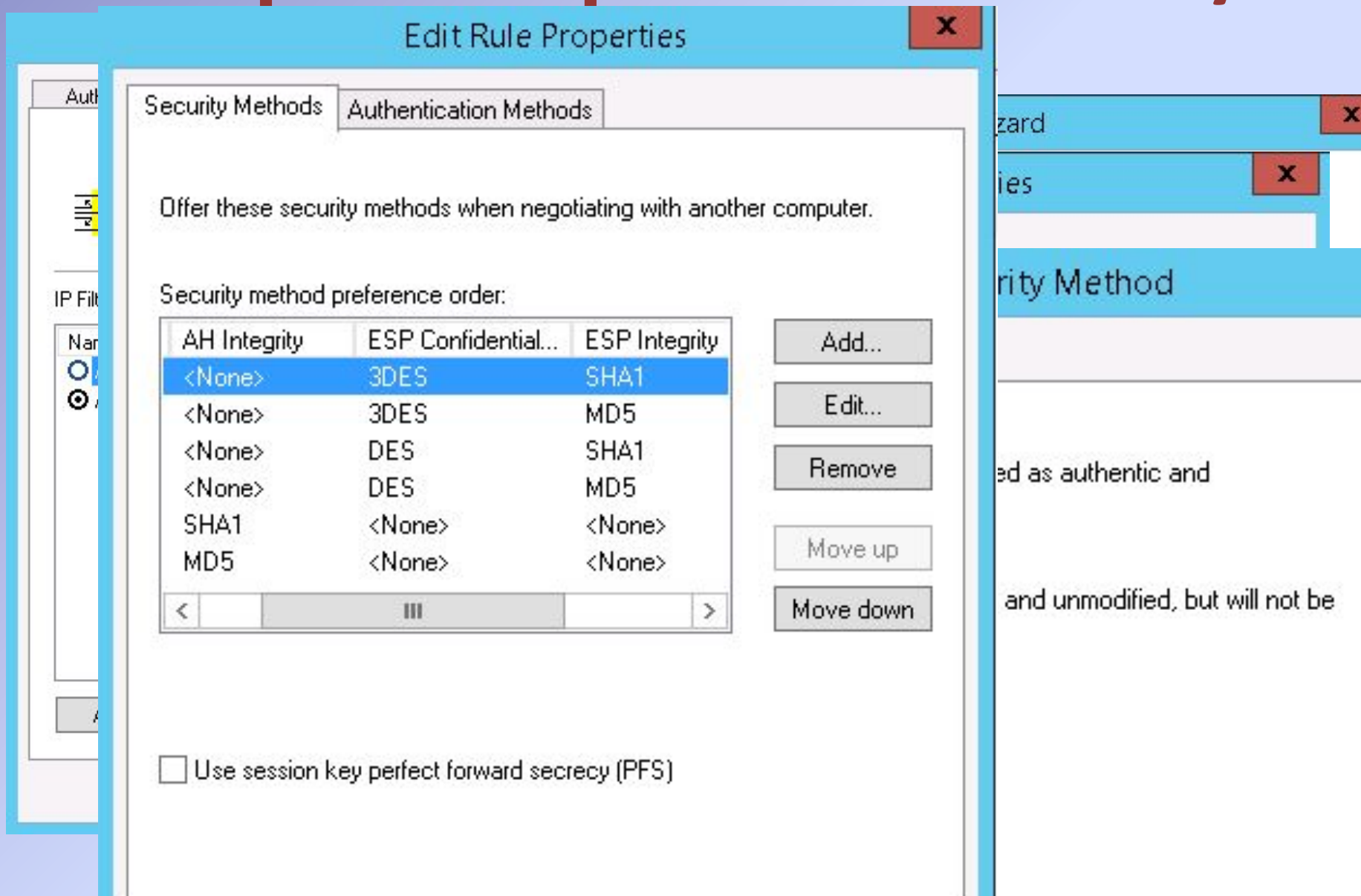
Настройка политики IP Security



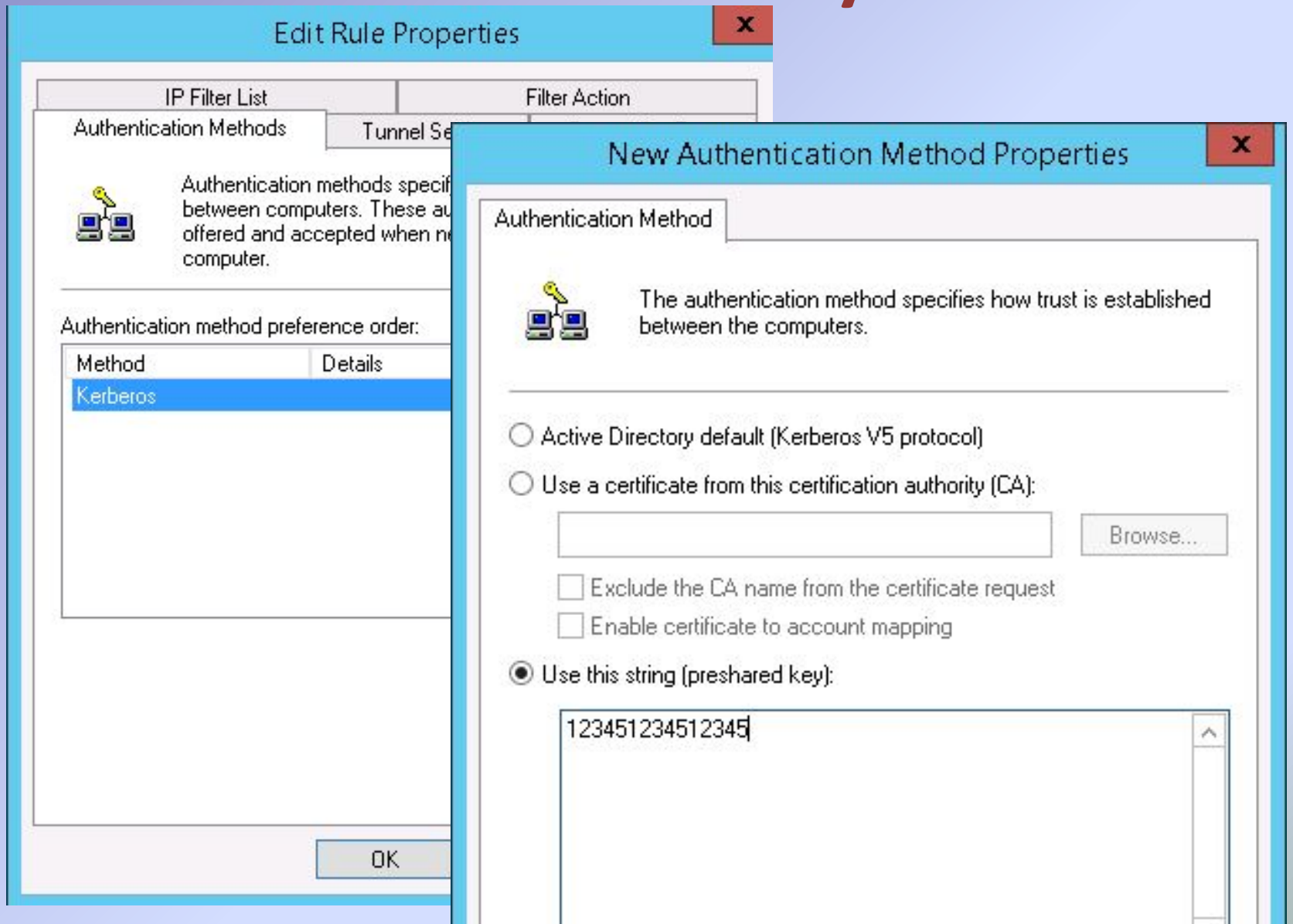
Настройка правил IP Security



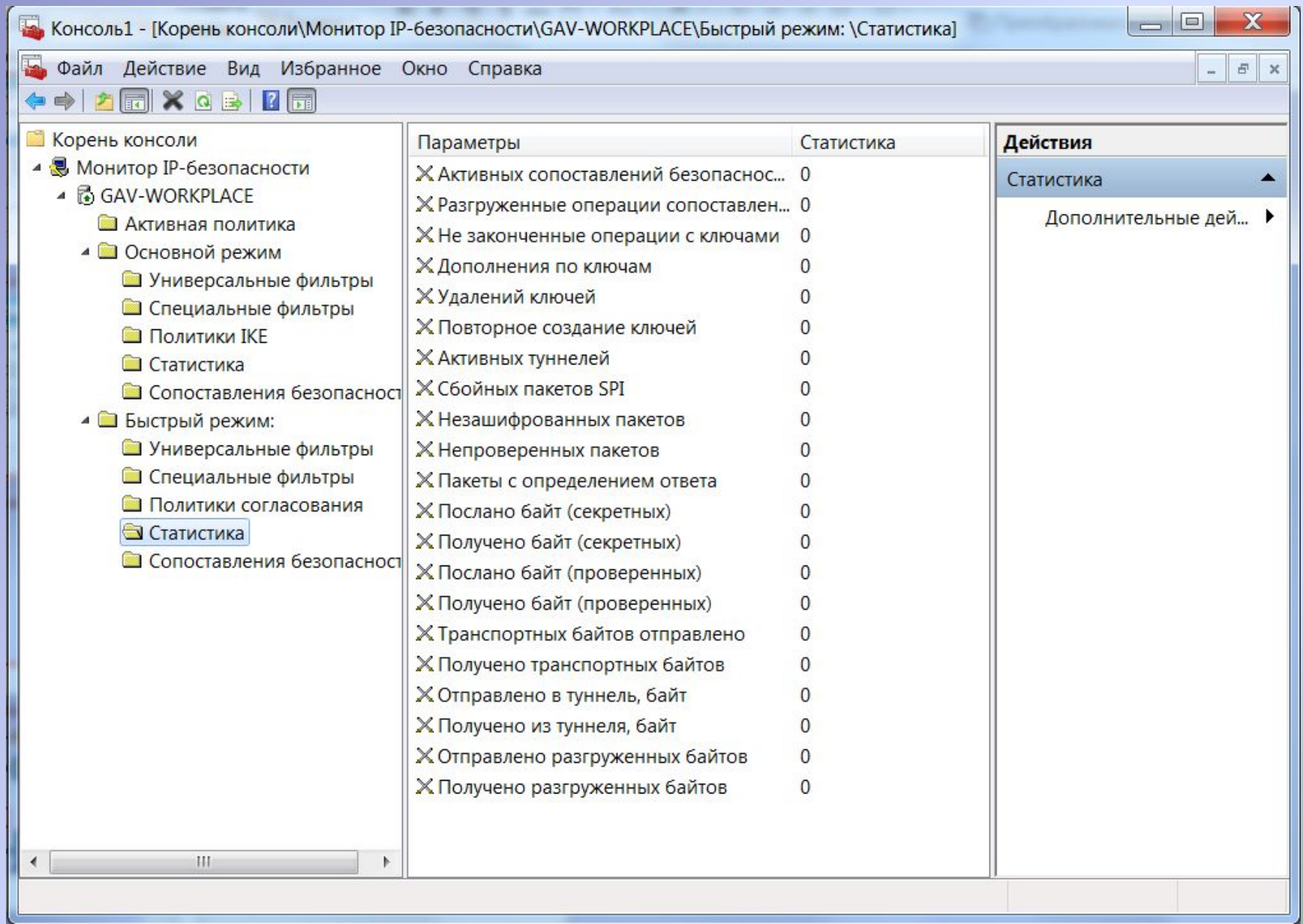
Настройка правил IP Security



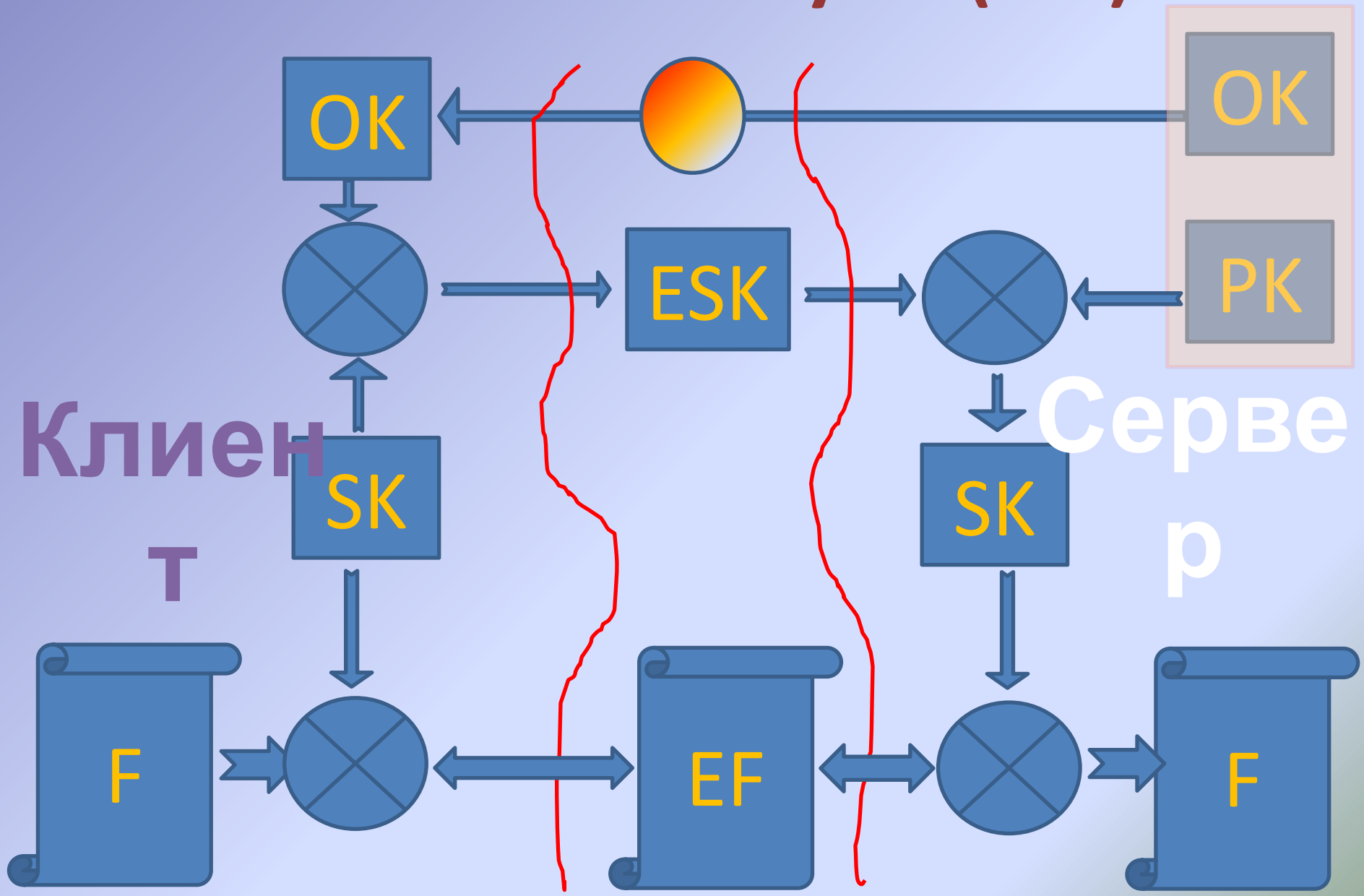
Настройка аутентификации IP Security



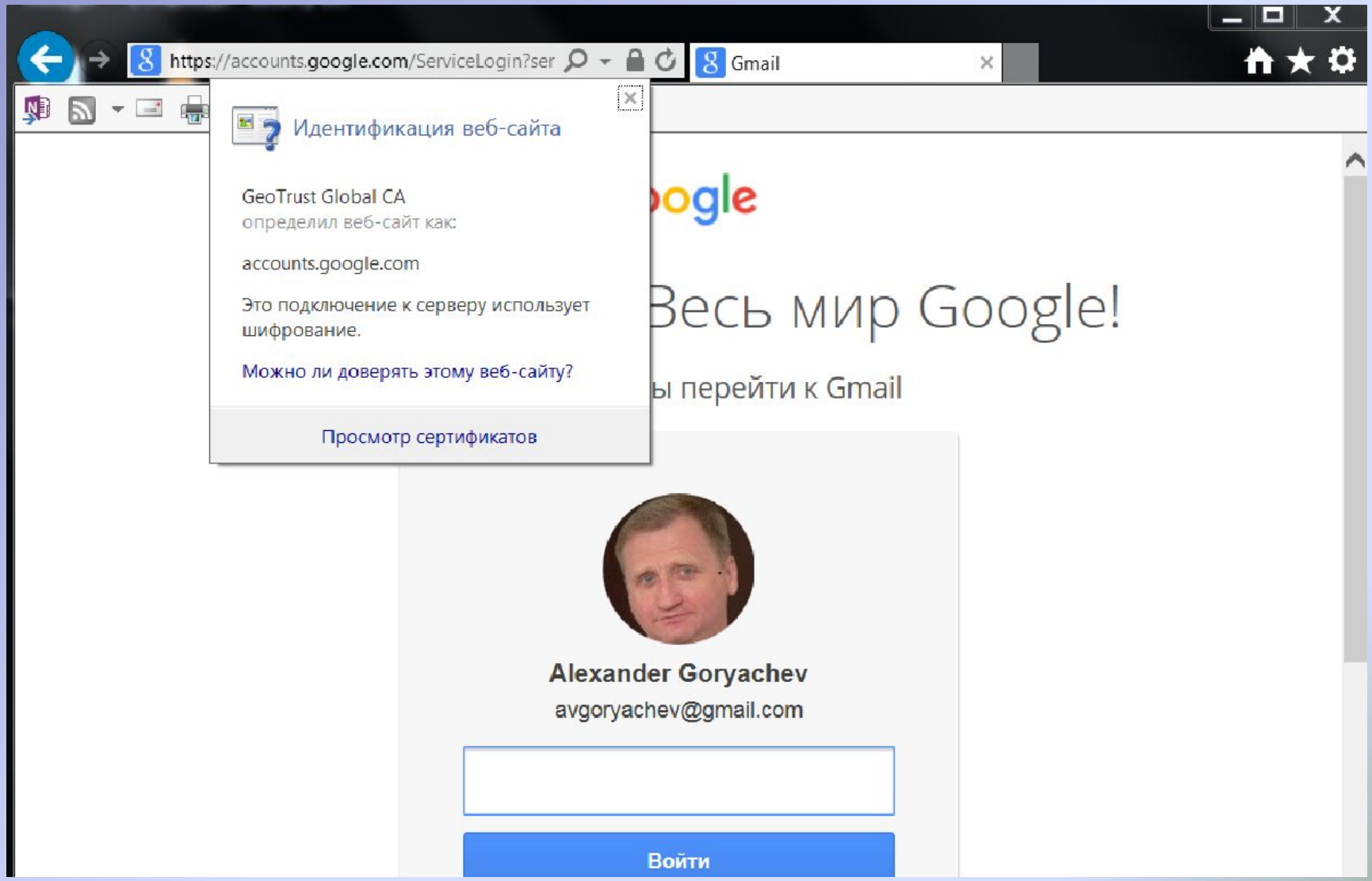
Мониторинг IPSecurity



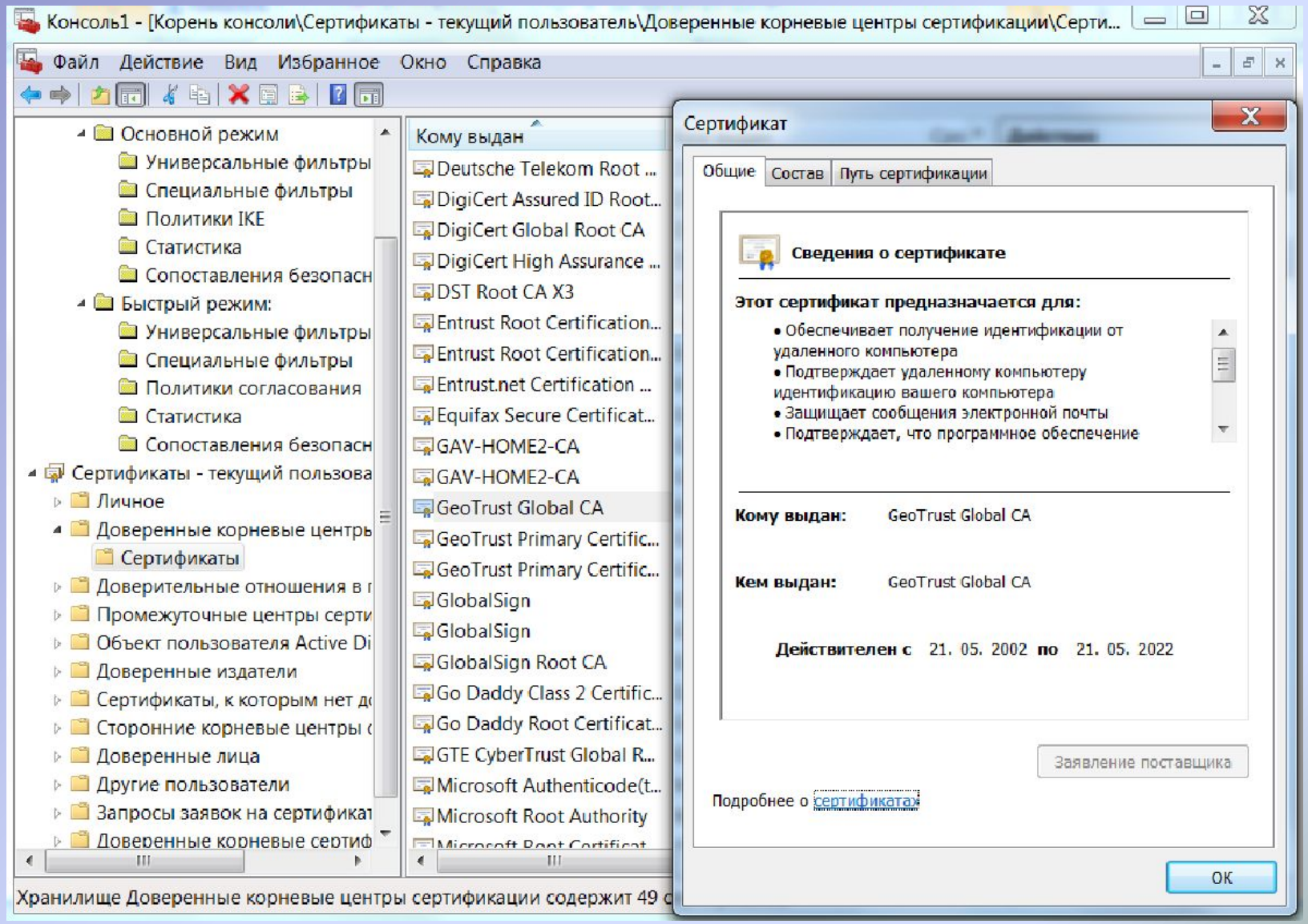
Secure Socket Layers (SSL)



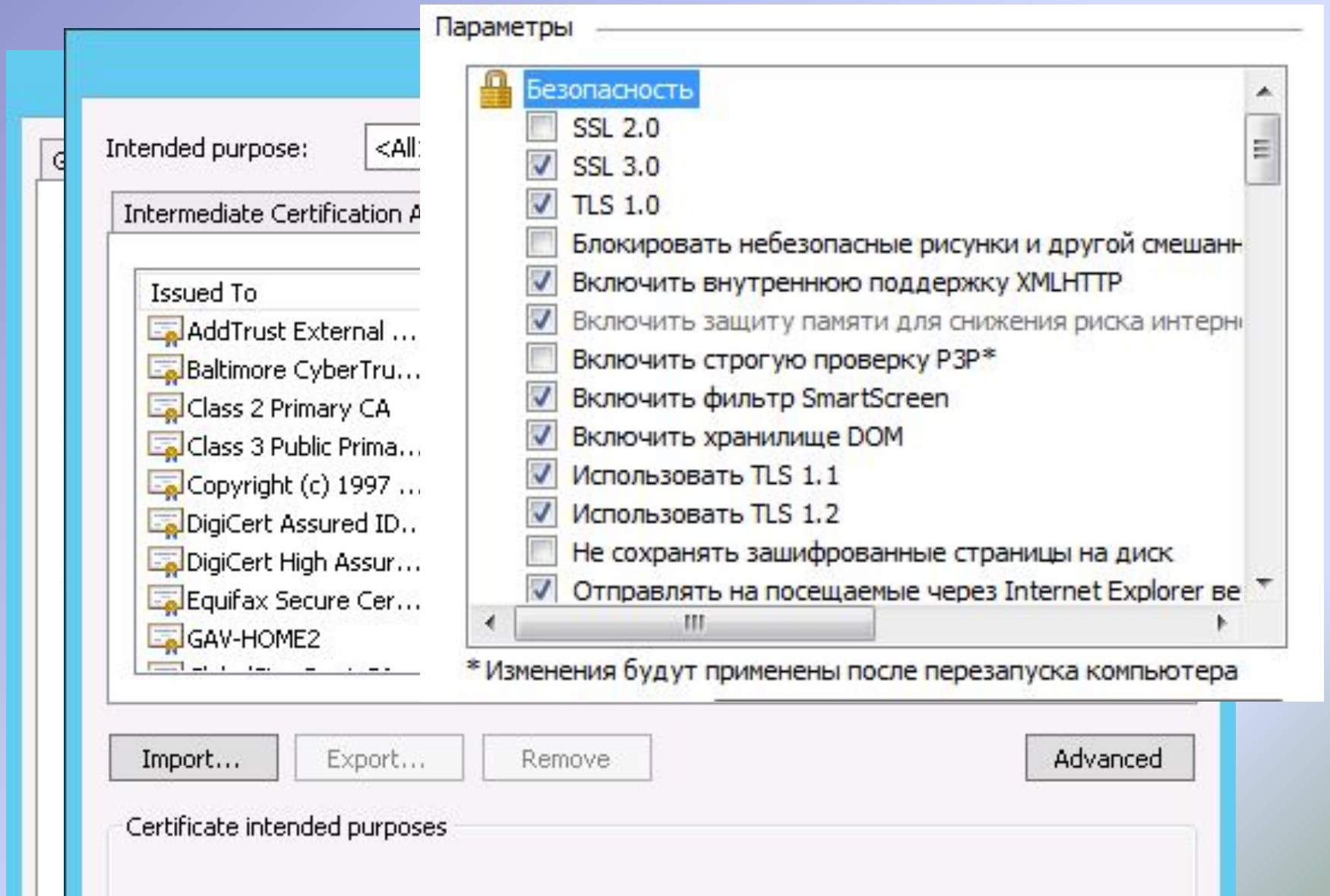
Установка соединения SSL



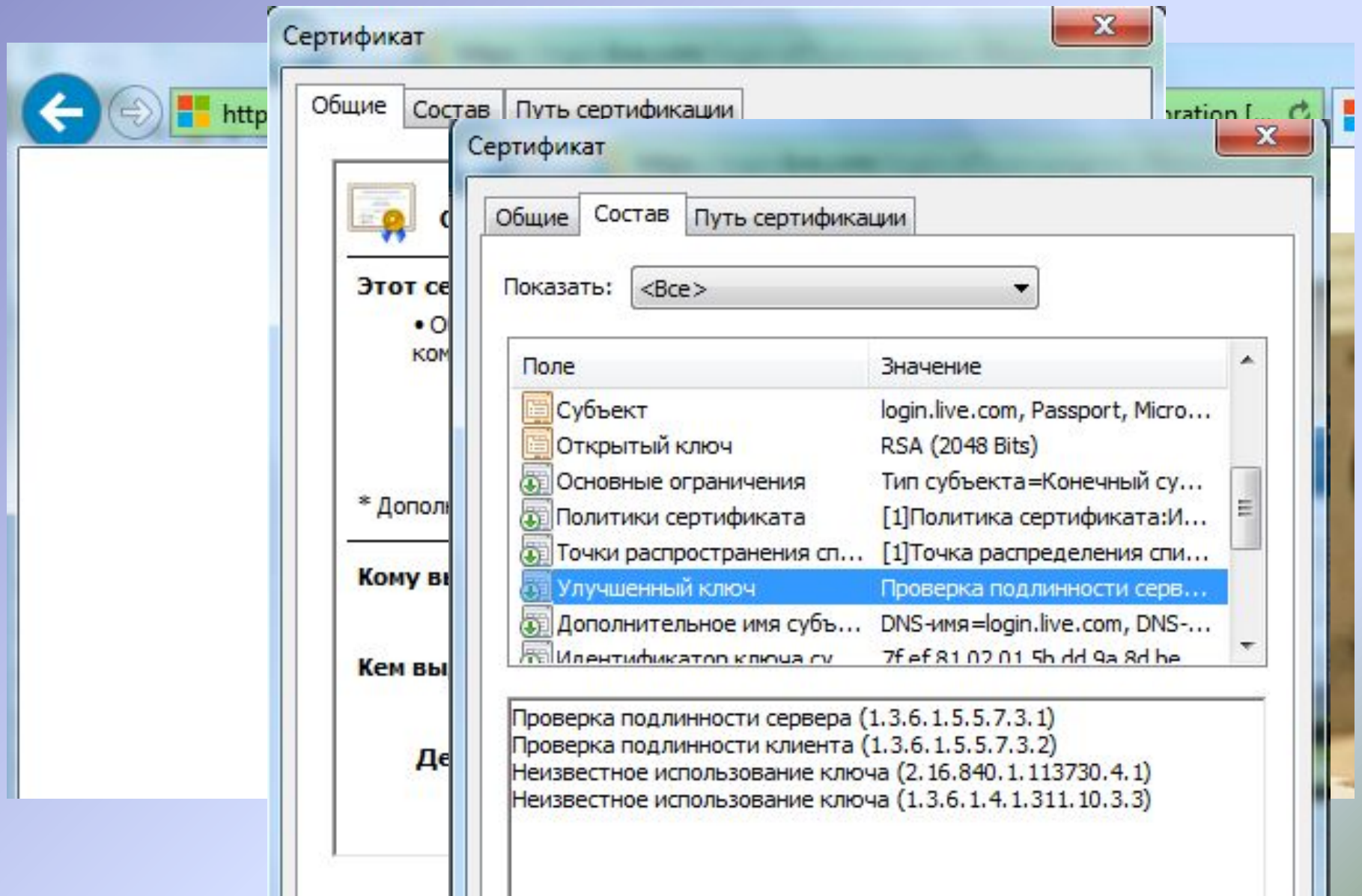
Суртификаты SSL



Сертификаты SSL



Работа с SSL


Сертификат
Общие
Состав
Путь сертификации
Сертификат
Общие
Состав
Путь сертификации
Показать:
<Все>
Поле
Значение
Субъект
login.live.com, Passport, Micro...
Открытый ключ
RSA (2048 Bits)
Основные ограничения
Тип субъекта=Конечный су...
Политики сертификата
[1]Политика сертификата:И...
Точки распространения сп...
[1]Точка распределения спи...
Улучшенный ключ
Проверка подлинности серв...
Дополнительное имя субъ...
DNS-имя=login.live.com, DNS-...
Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)
Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
Неизвестное использование ключа (2.16.840.1.113730.4.1)
Неизвестное использование ключа (1.3.6.1.4.1.311.10.3.3)

VPN

Горячев Александр Вадимович
Доцент кафедры ИБ
avgoriachev@etu.ru

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

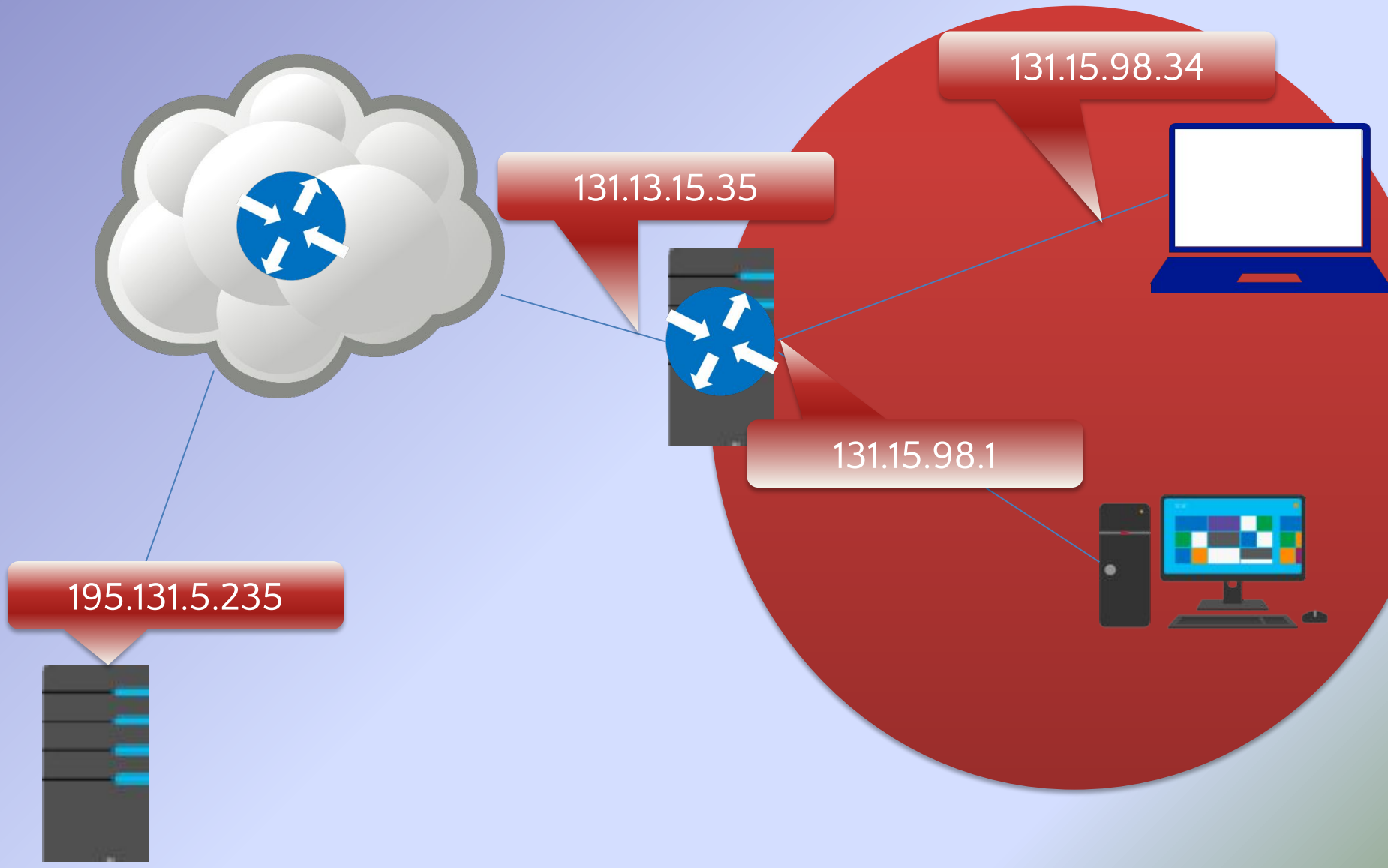
Intranet Routing IPSec SSL RMS NIDS-NIPS

Internet Firewall VPN NAP

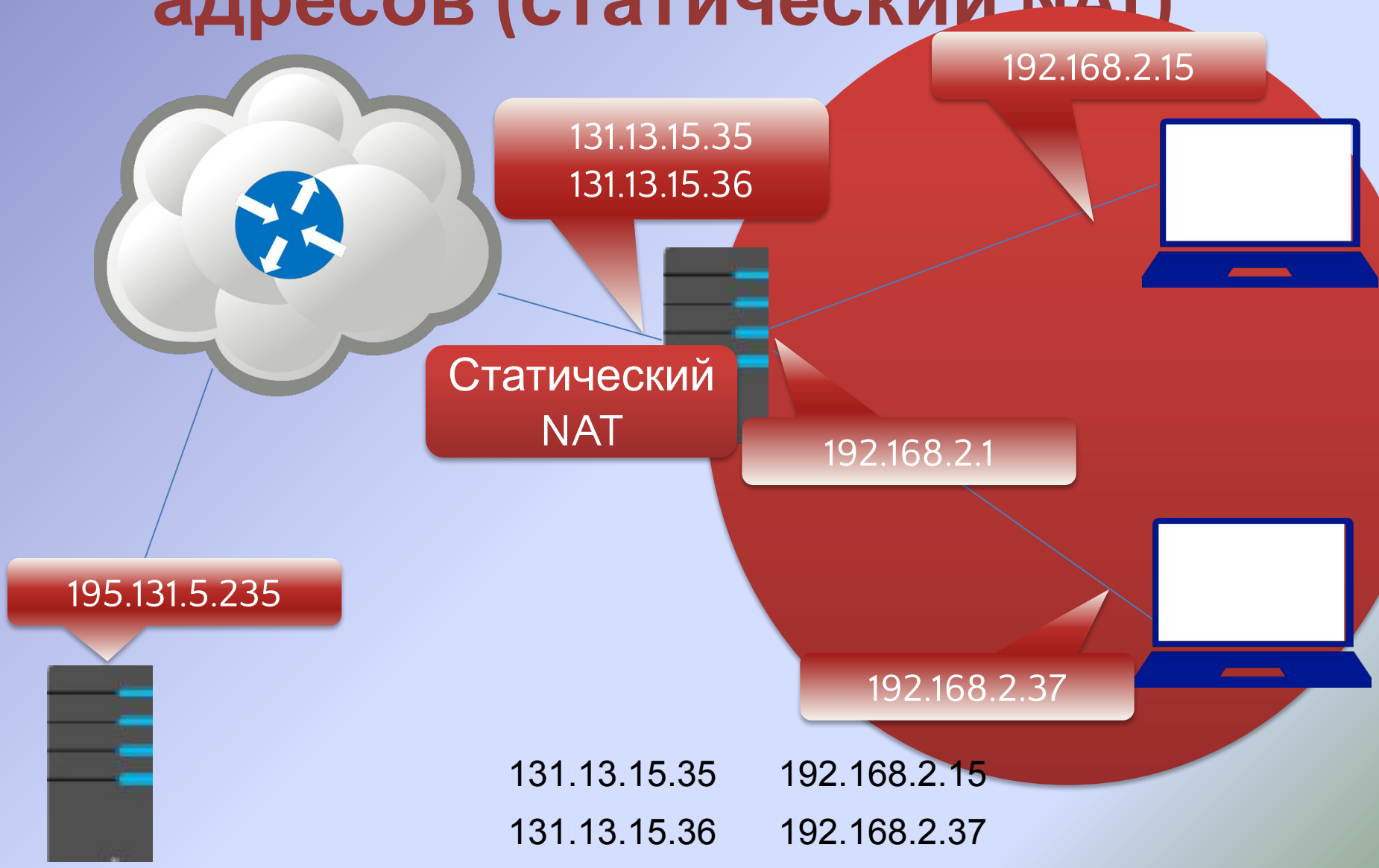
Технологии выхода в Интернет из корпоративной сети

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

Маршрутизация

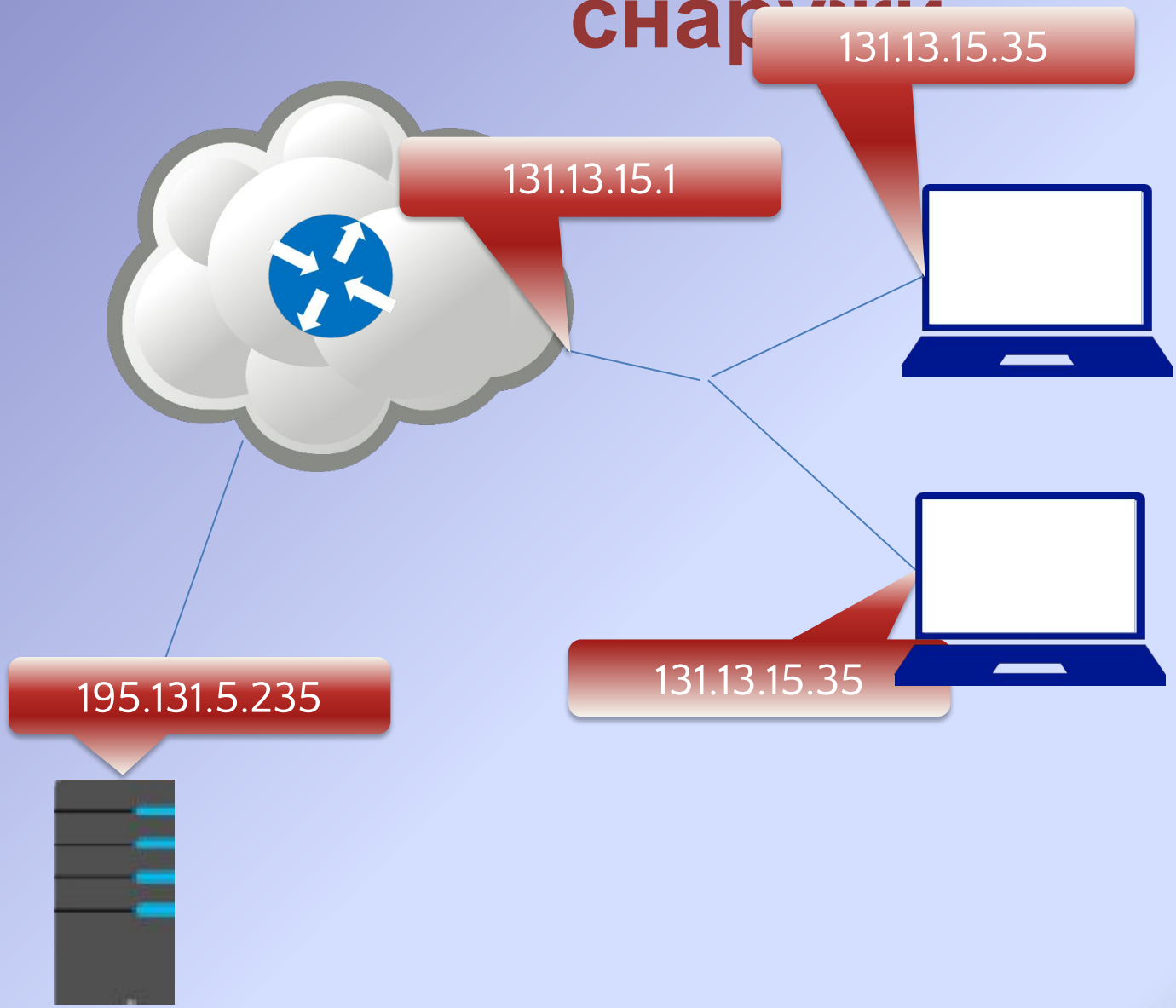


Статическая трансляция адресов (статический NAT)

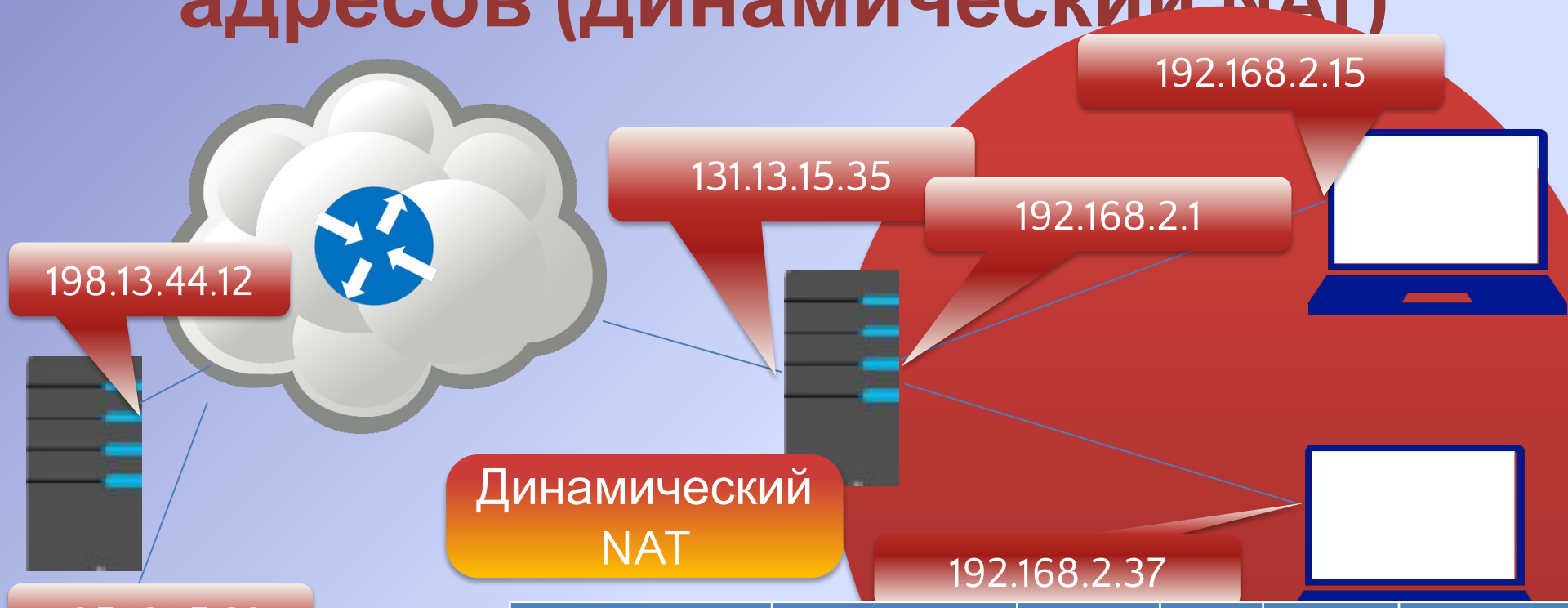


131.13.15.35	192.168.2.15
131.13.15.36	192.168.2.37

Статический NAT – как выглядит снаружи



Динамическая трансляция адресов (динамический NAT)



Отправитель	Получатель	Отпр.	Пол	NAT	TimeOut
	198.13.44.12	12345	80	34555	
	95.131.5.23	32256	80	34556	

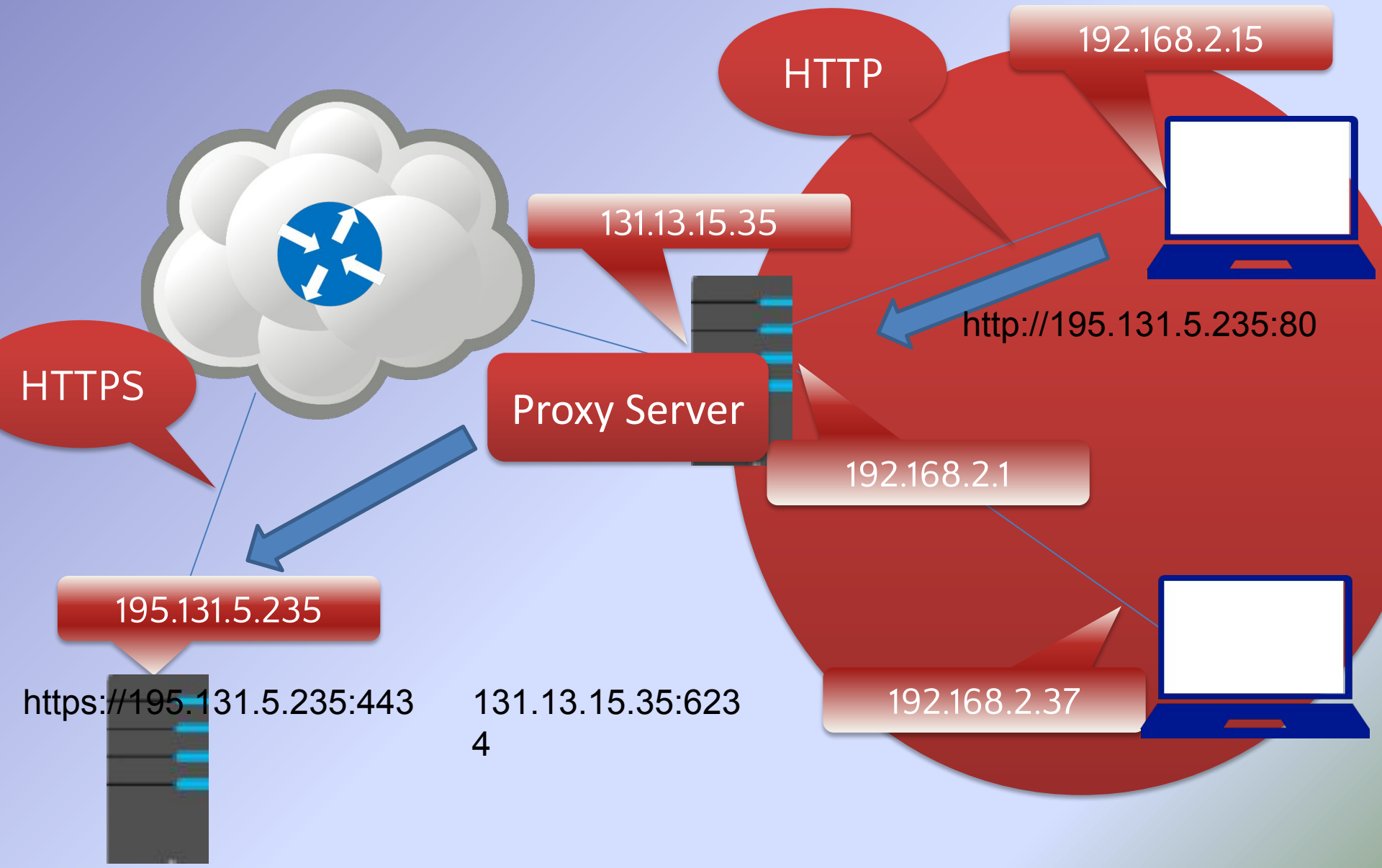
Пакет прямой:

Пакет ответный:

Отправитель: 198.13.44.12:80

Получатель: 131.13.15.35:34555

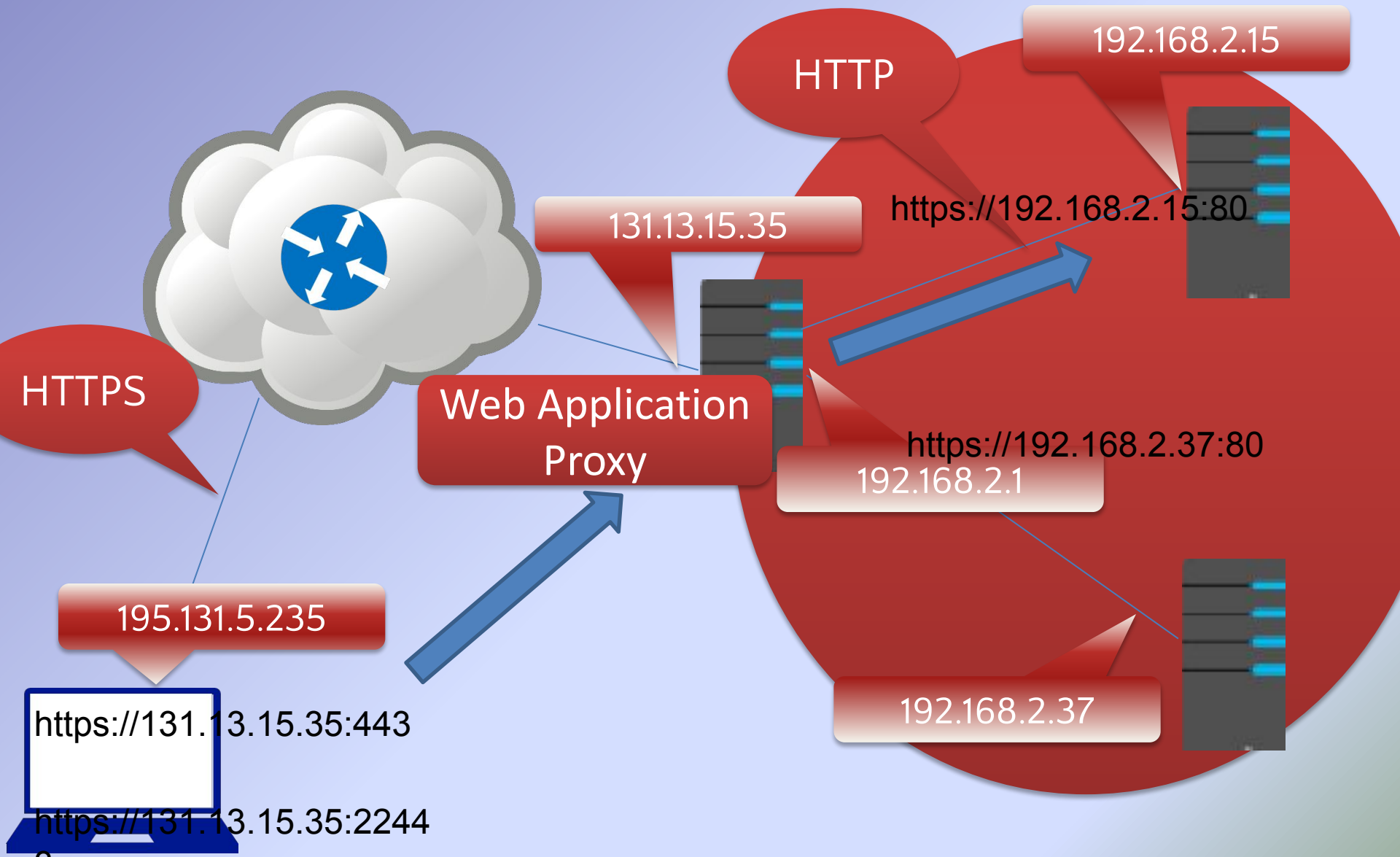
Прокси (Proxy)



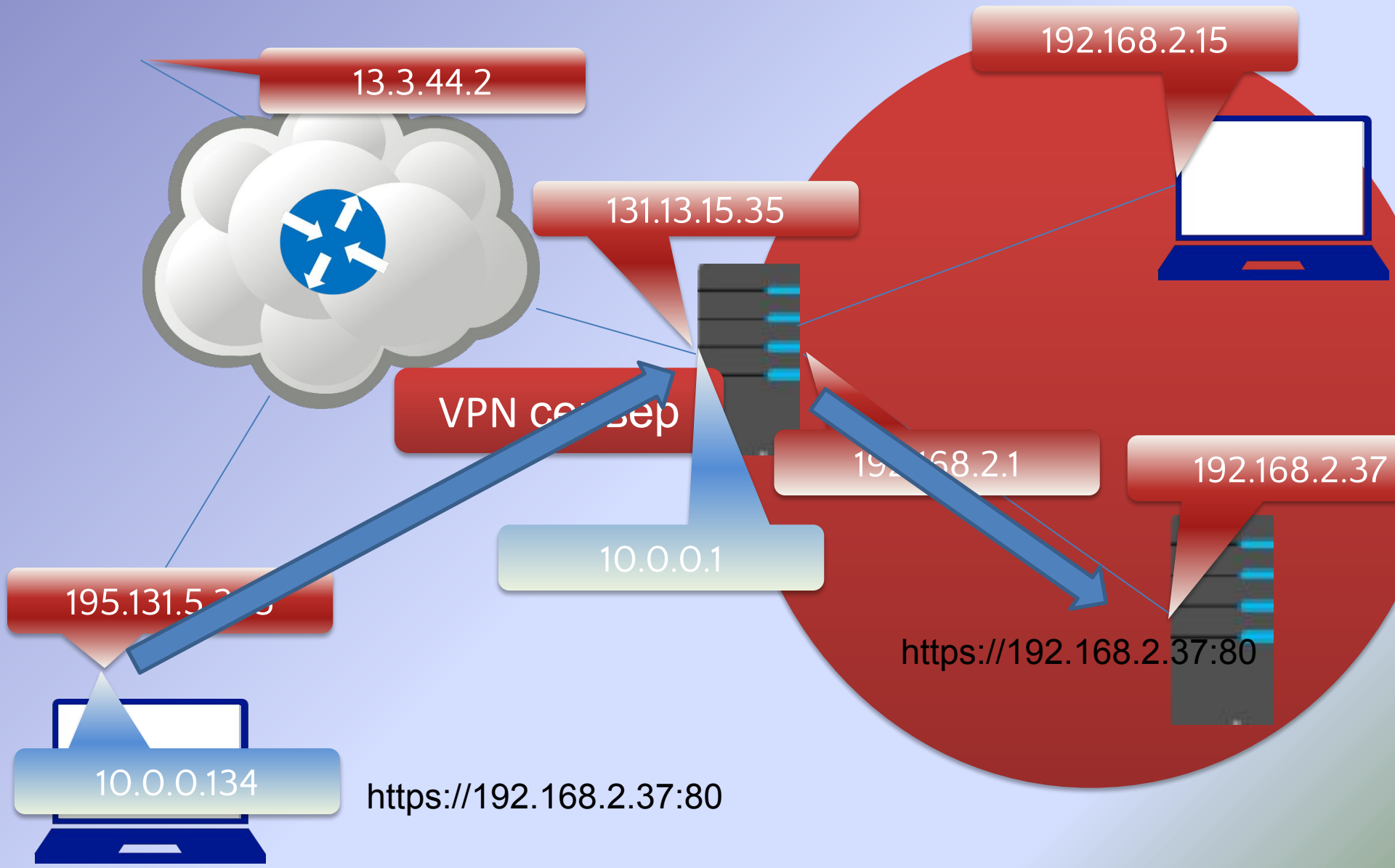
Технологии доступа из Интернет к ресурсам корпоративной сети

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

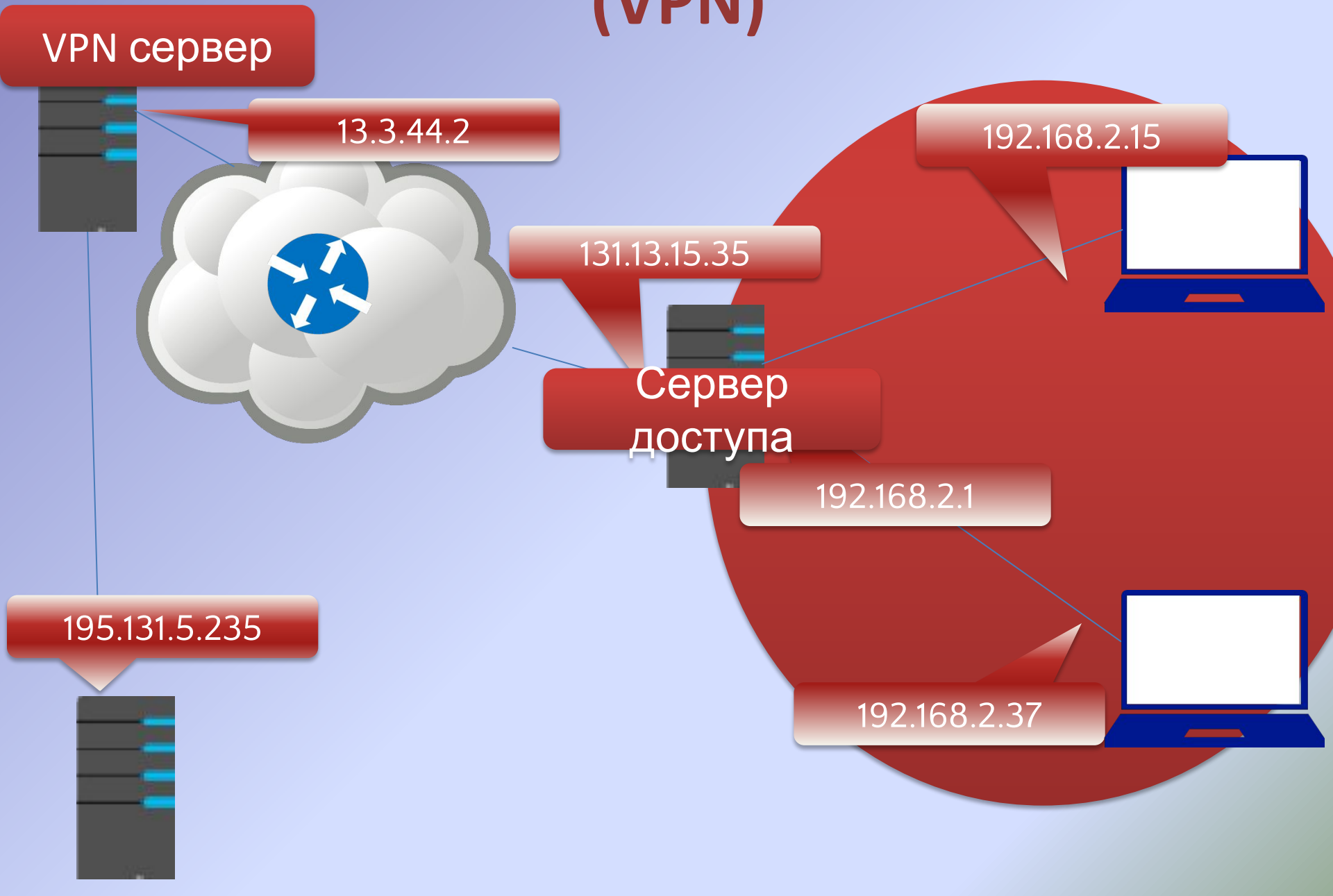
Web Application Proxy (Обратный прокси)



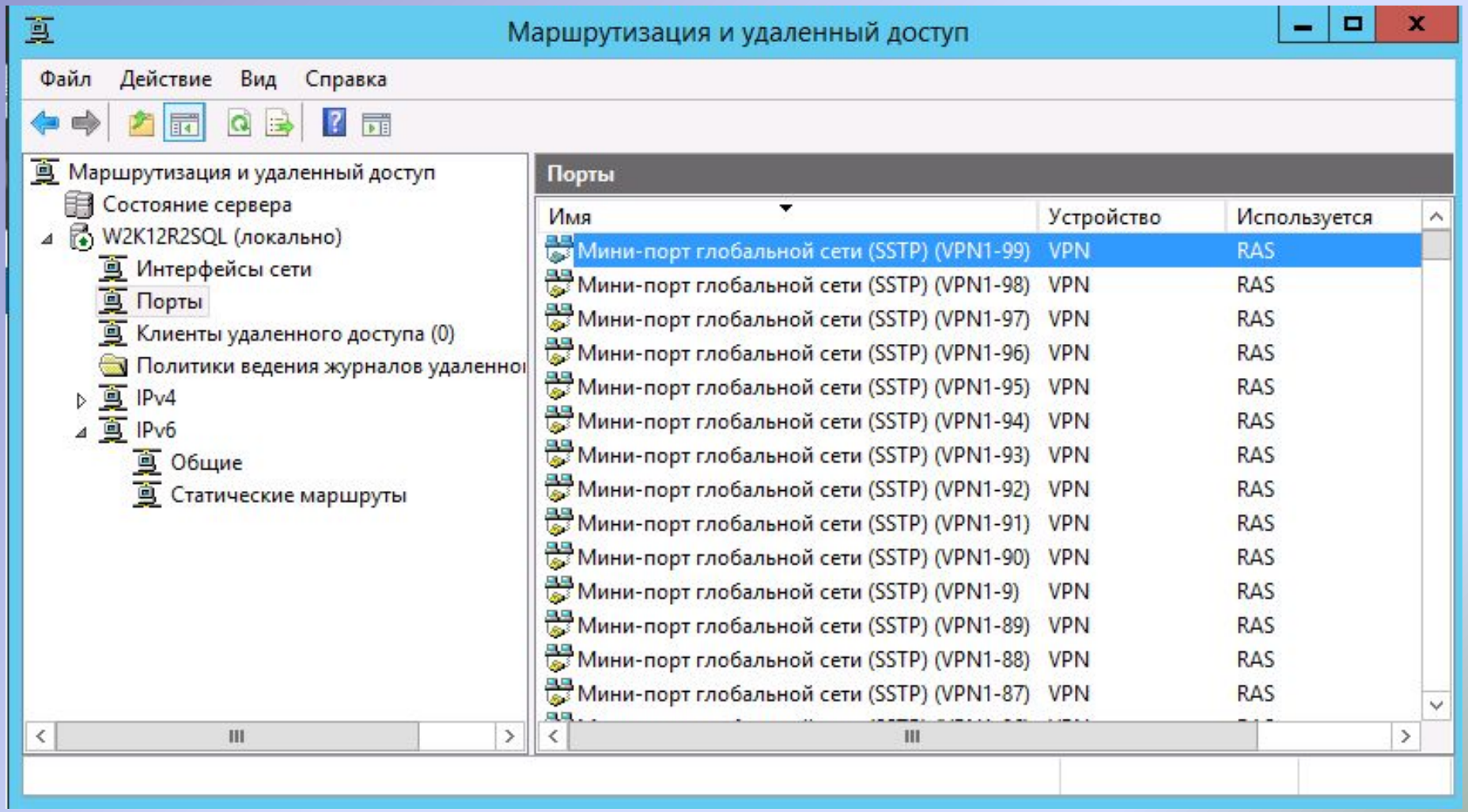
Виртуальные частные сети (VPN)



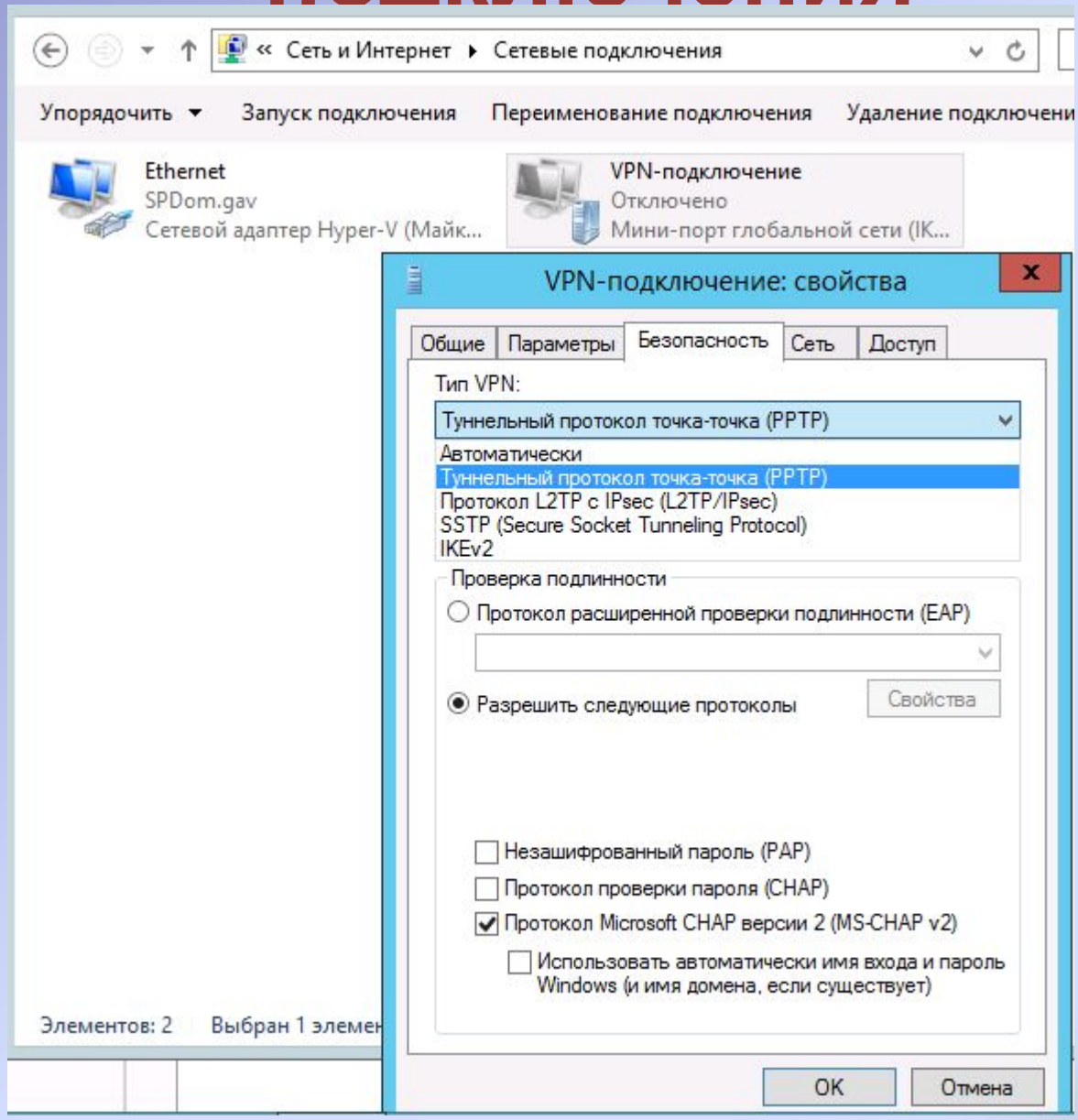
Виртуальные частные сети (VPN)



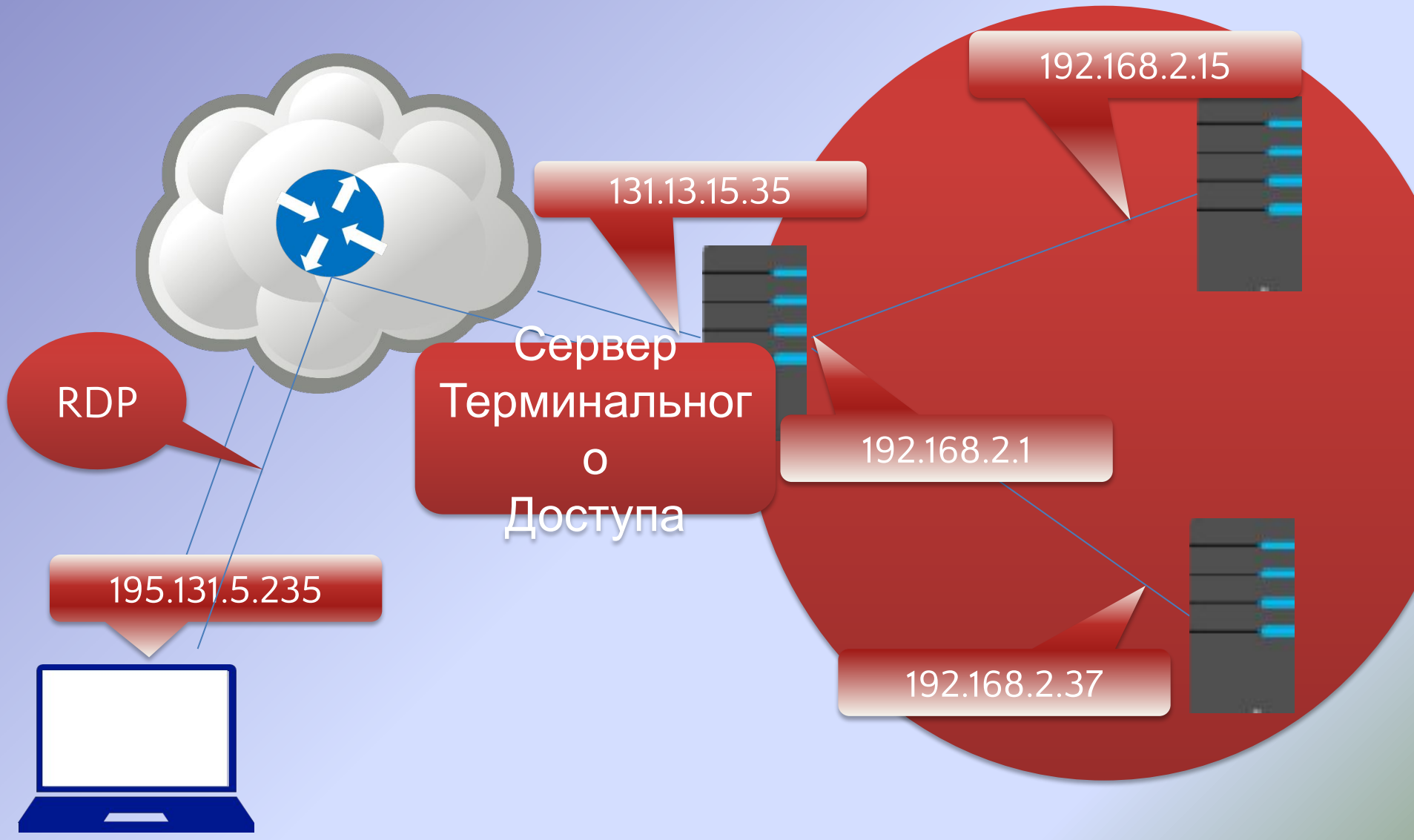
Настройка VPN в RRAS



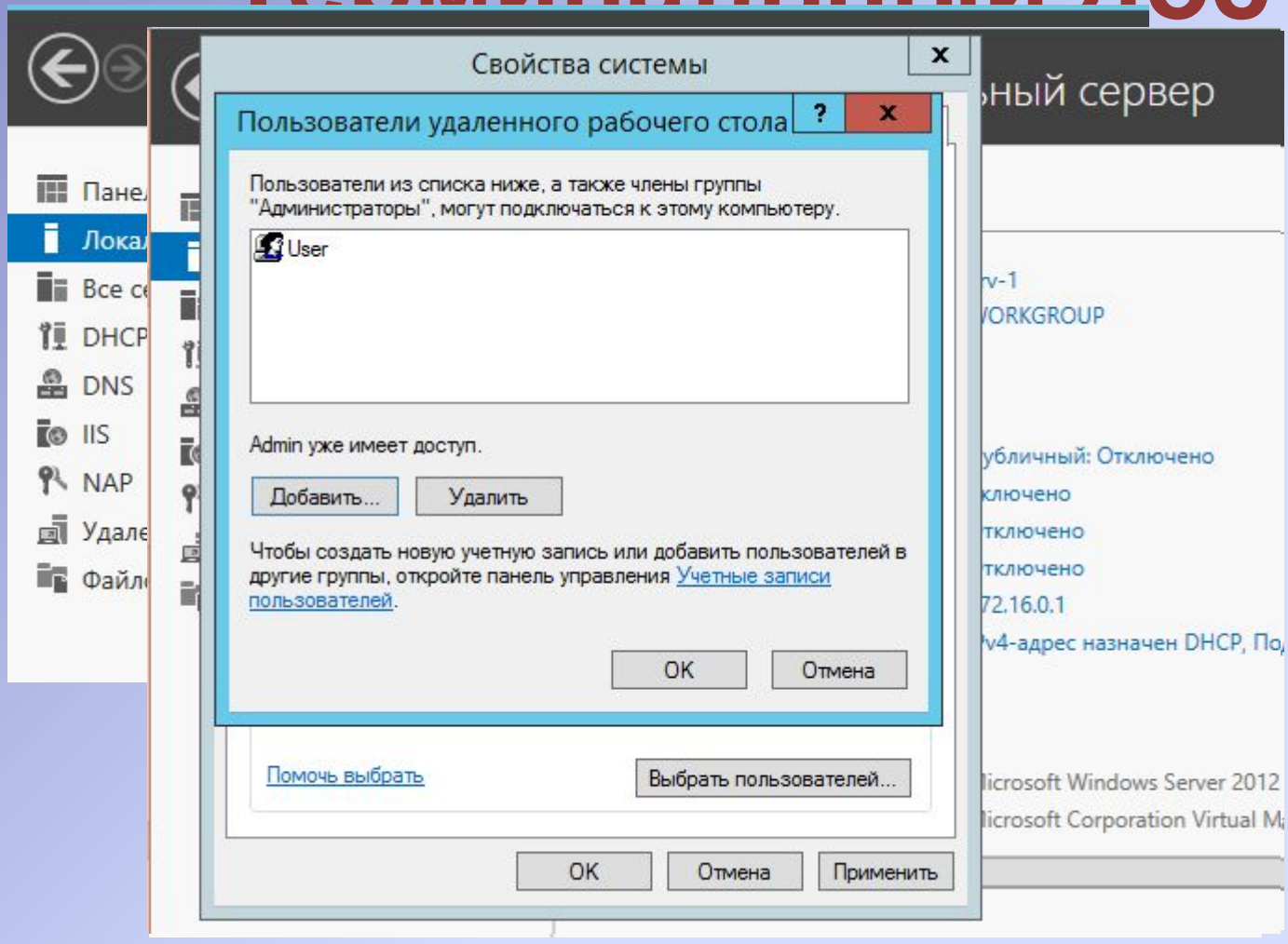
Настройка параметров подключения



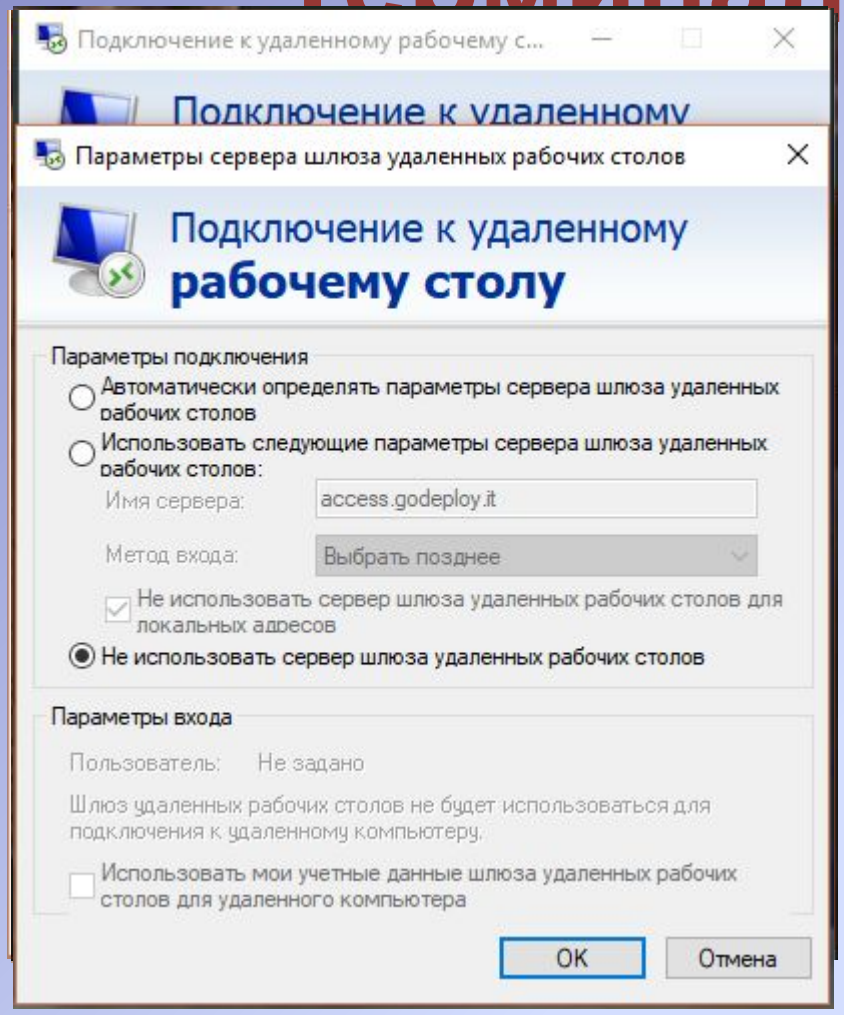
Терминальный доступ

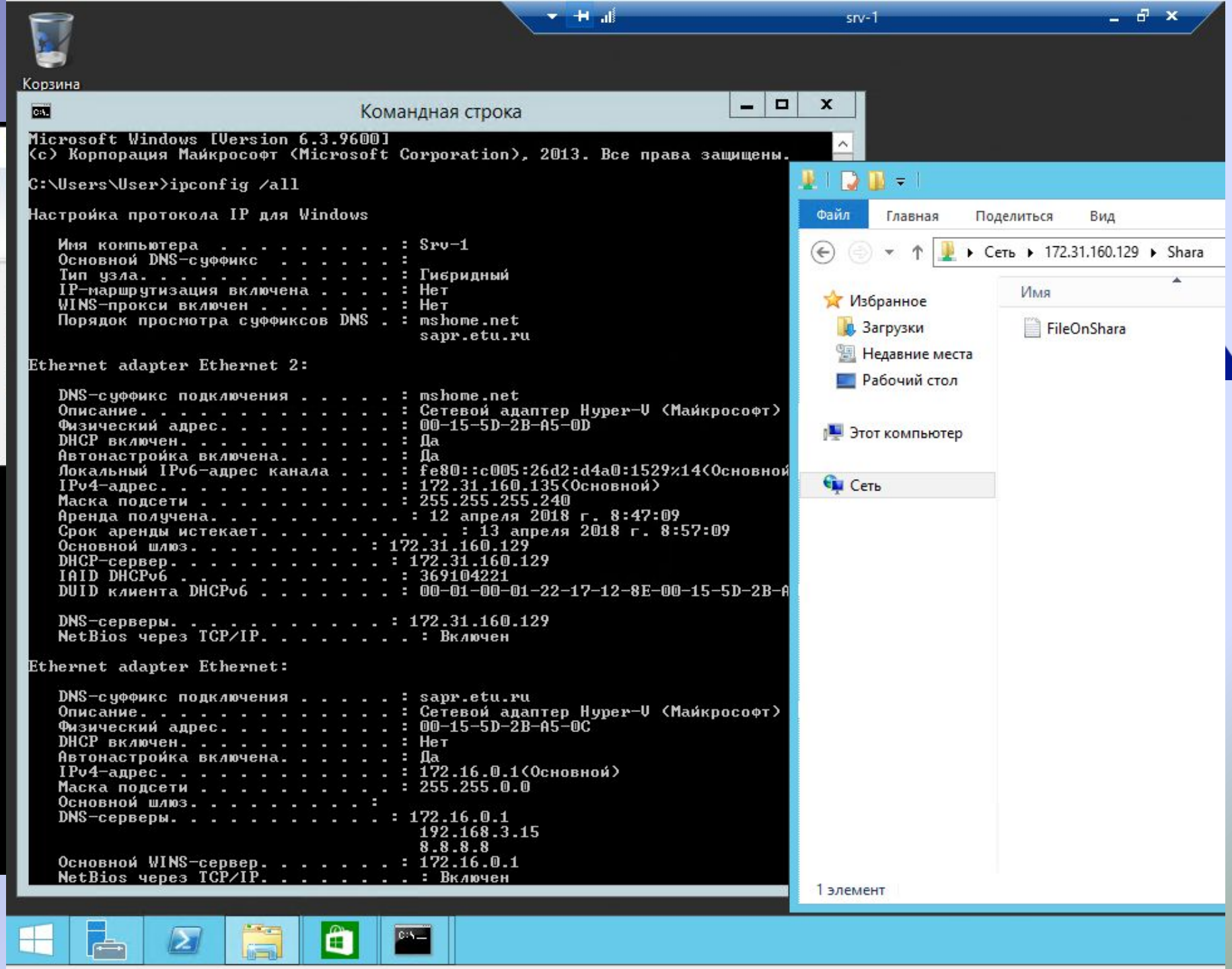


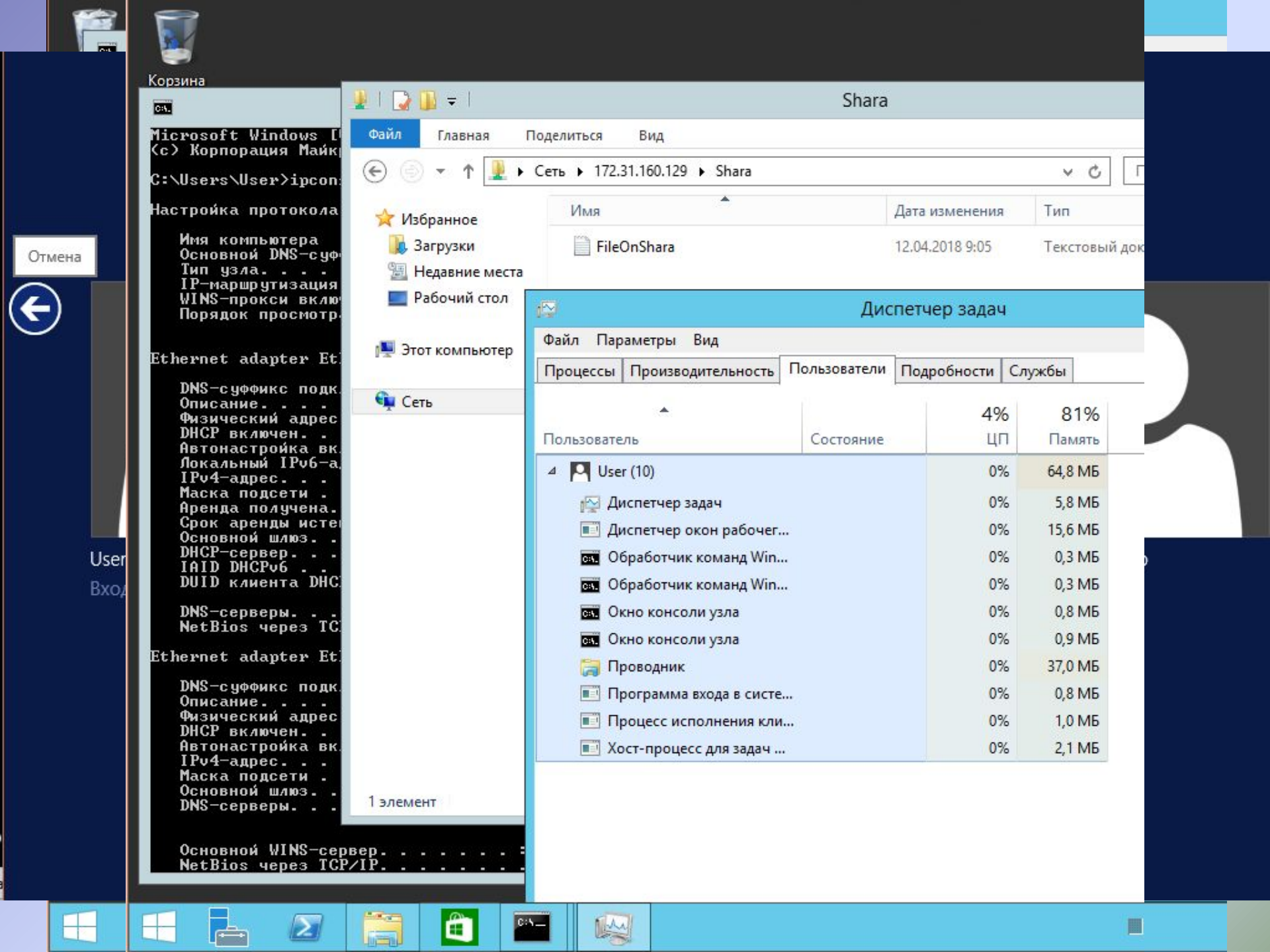
Терминальный доступ



Терминальный доступ




srv-1
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 Hyper-V (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 Hyper-V (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
Файл
Главная
Поделиться
Вид
Сеть ▸ 172.31.160.129 ▸ Shara
Избранное
Загрузки
Недавние места
Рабочий стол
Этот компьютер
Сеть
Имя
FileOnShara
1 элемент

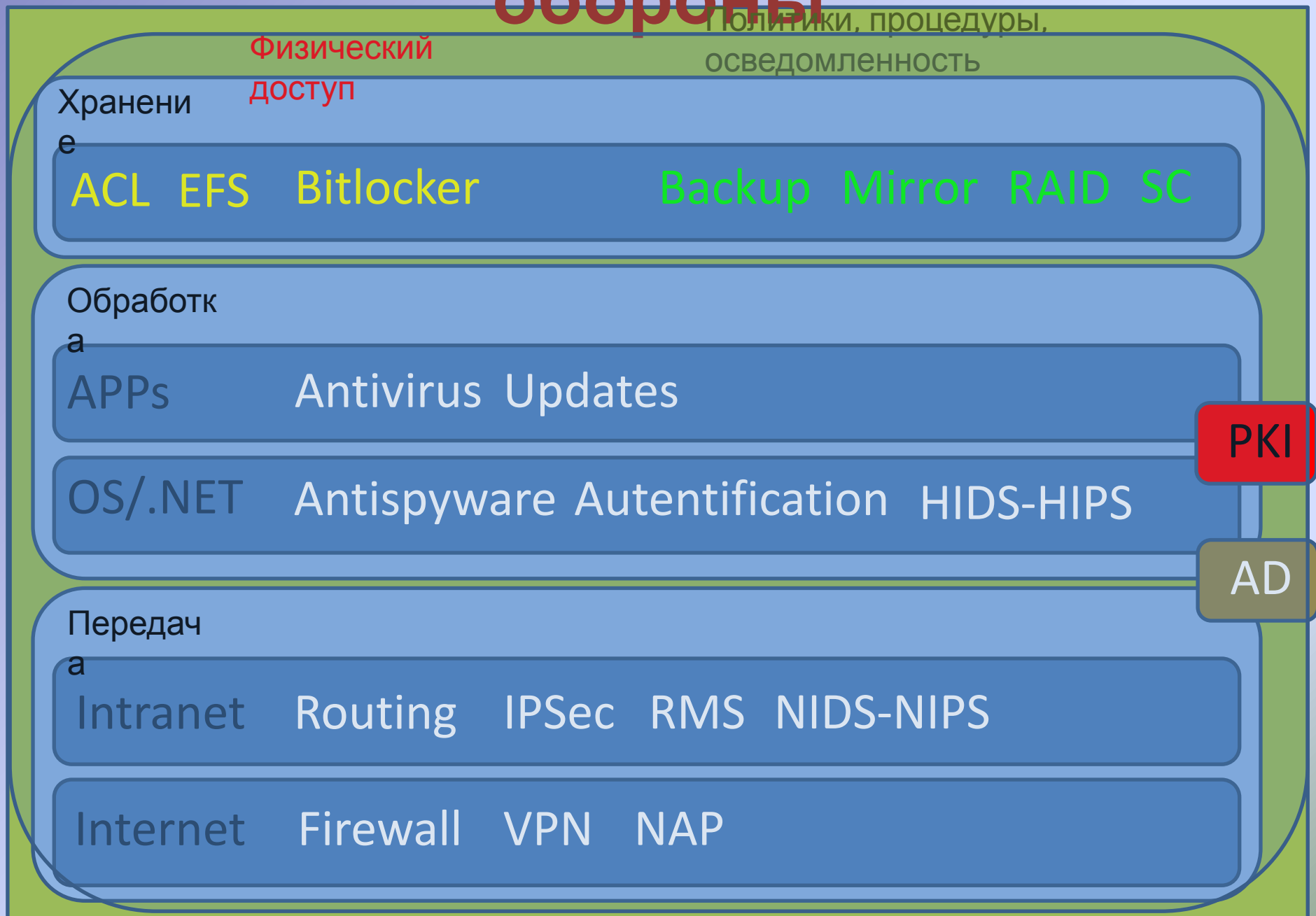

Корзина
Microsoft Windows [
(c) Корпорация Майк
C:\Users\User>ipcon
Настройка протокола
Имя компьютера
Основной DNS-суф
Тип узла. . . .
IP-маршрутизация
WINS-прокси вклю
Порядок просмотр
Ethernet adapter Et
DNS-суффикс подк
Описание. . . .
Физический адрес
DHCP включен. .
Автонастройка вк
Локальный IPv6-а
IPv4-адрес. . .
Маска подсети .
Аренда получена.
Срок аренды исте
Основной шлюз. .
DHCP-сервер. . .
IAID DHCPv6 . .
DUID клиента DHC
DNS-серверы. . .
NetBios через TC
Ethernet adapter Et
DNS-суффикс подк
Описание. . . .
Физический адрес
DHCP включен. .
Автонастройка вк
IPv4-адрес. . .
Маска подсети .
Основной шлюз. .
DNS-серверы. . .
Основной WINS-сервер. . . . . :
NetBios через TCP/IP. . . . . :
Shara
Файл
Главная
Поделиться
Вид
Сеть ▸ 172.31.160.129 ▸ Shara
Избранное
Загрузки
Недавние места
Рабочий стол
Этот компьютер
Сеть
Имя
Дата изменения
Тип
FileOnShara
12.04.2018 9:05
Текстовый док
1 элемент
Диспетчер задач
Файл
Параметры
Вид
Процессы
Производительность
Пользователи
Подробности
Службы
4%
ЦП
81%
Память
Пользователь
Состояние
User (10)
0%
64,8 МБ
Диспетчер задач
0%
5,8 МБ
Диспетчер окон рабочег...
0%
15,6 МБ
Обработчик команд Win...
0%
0,3 МБ
Обработчик команд Win...
0%
0,3 МБ
Окно консоли узла
0%
0,8 МБ
Окно консоли узла
0%
0,9 МБ
Проводник
0%
37,0 МБ
Программа входа в систе...
0%
0,8 МБ
Процесс исполнения кли...
0%
1,0 МБ
Хост-процесс для задач ...
0%
2,1 МБ
Отмена

Спасибо за внимание!

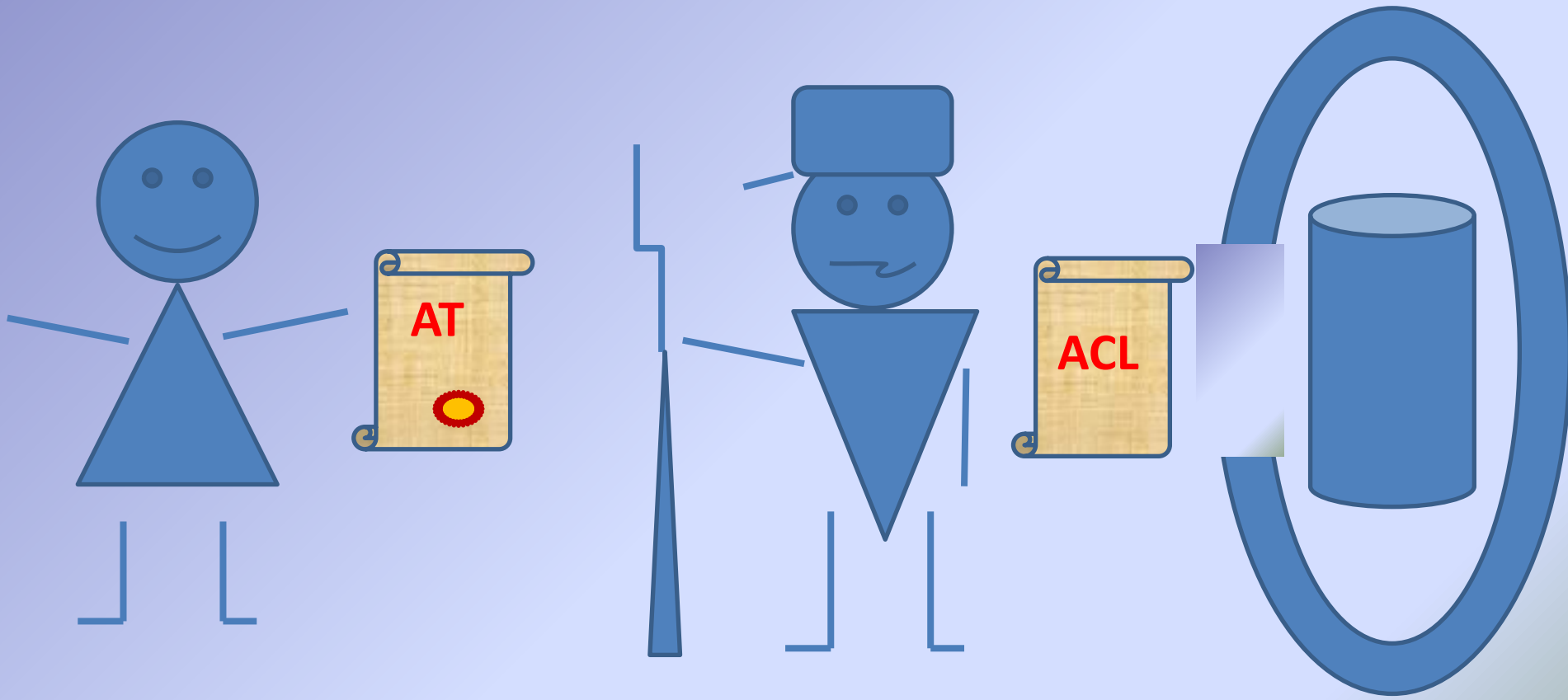
Сертификаты. Инфраструктура шифрования с открытым ключом (PKI)

Горячев Александр Вадимович
Доцент кафедры ИБ
avgoriachev@etu.ru

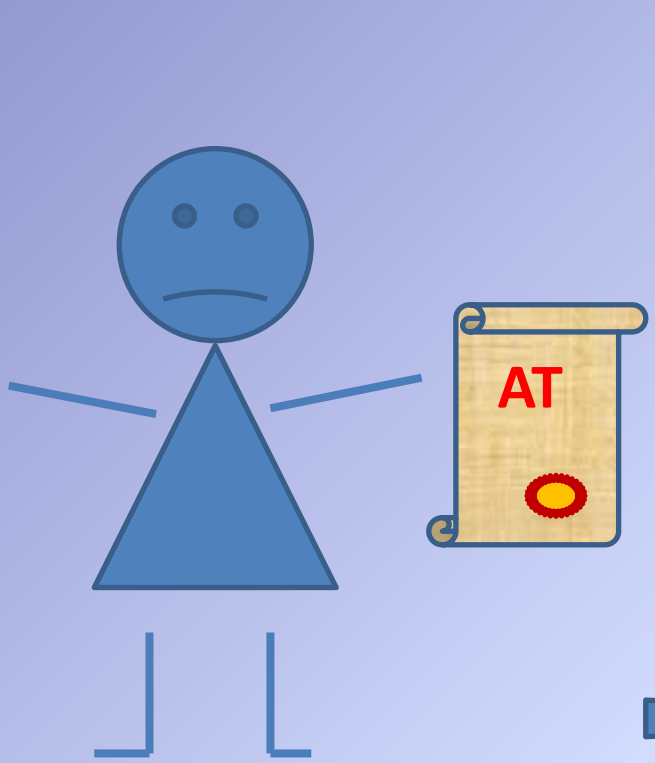
Модель эшелонированной обороны

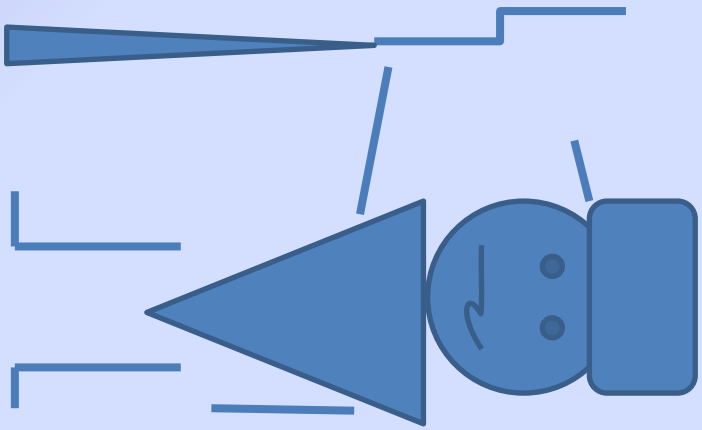


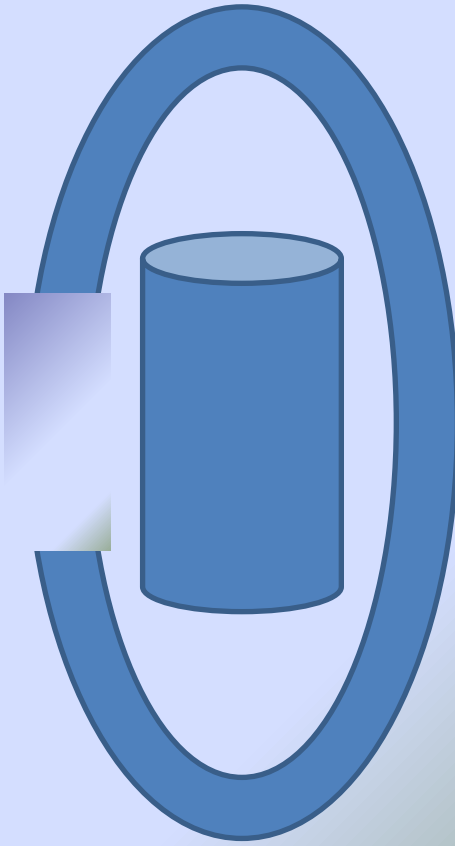
Список контроля доступа



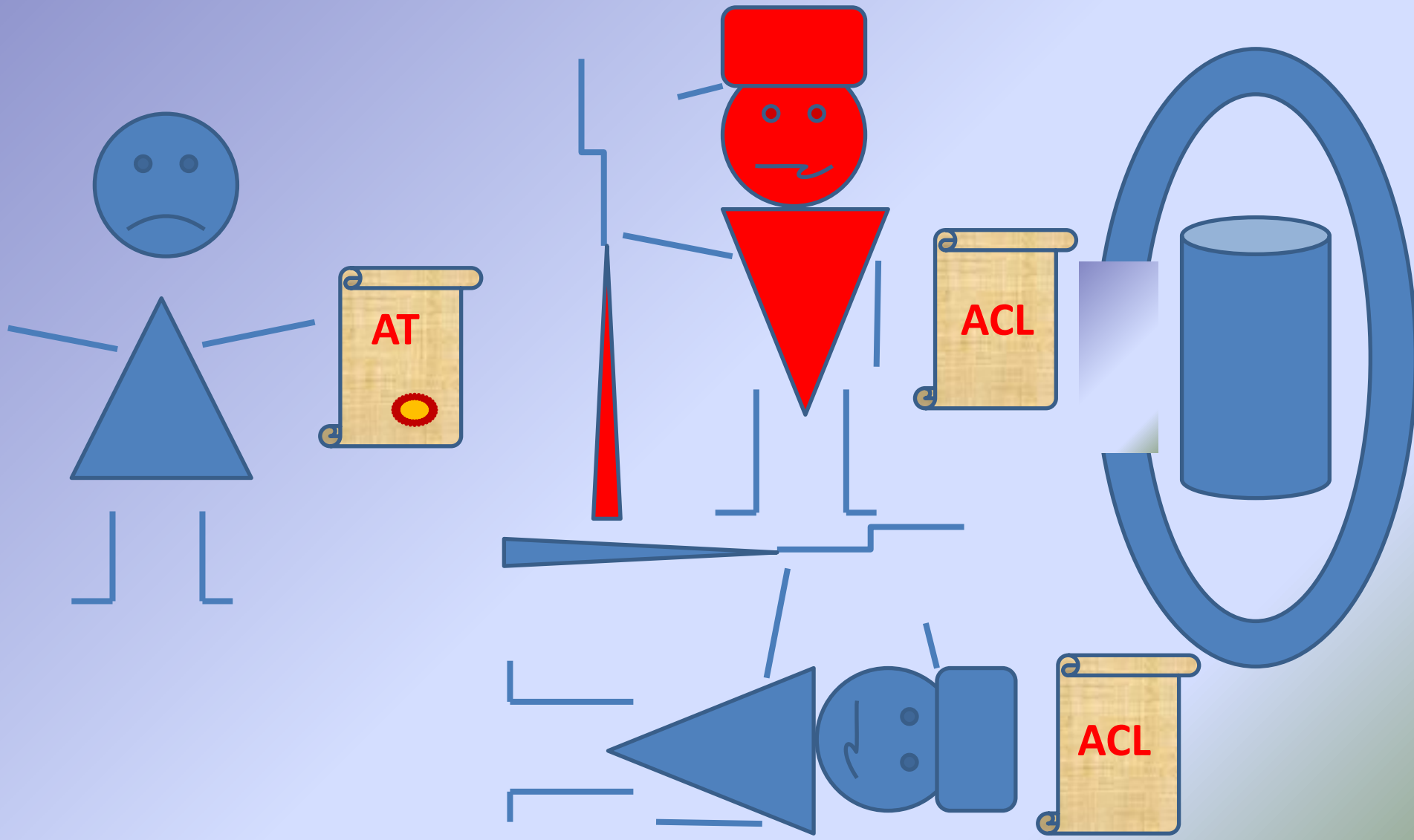
Список контроля доступа







Список контроля доступа

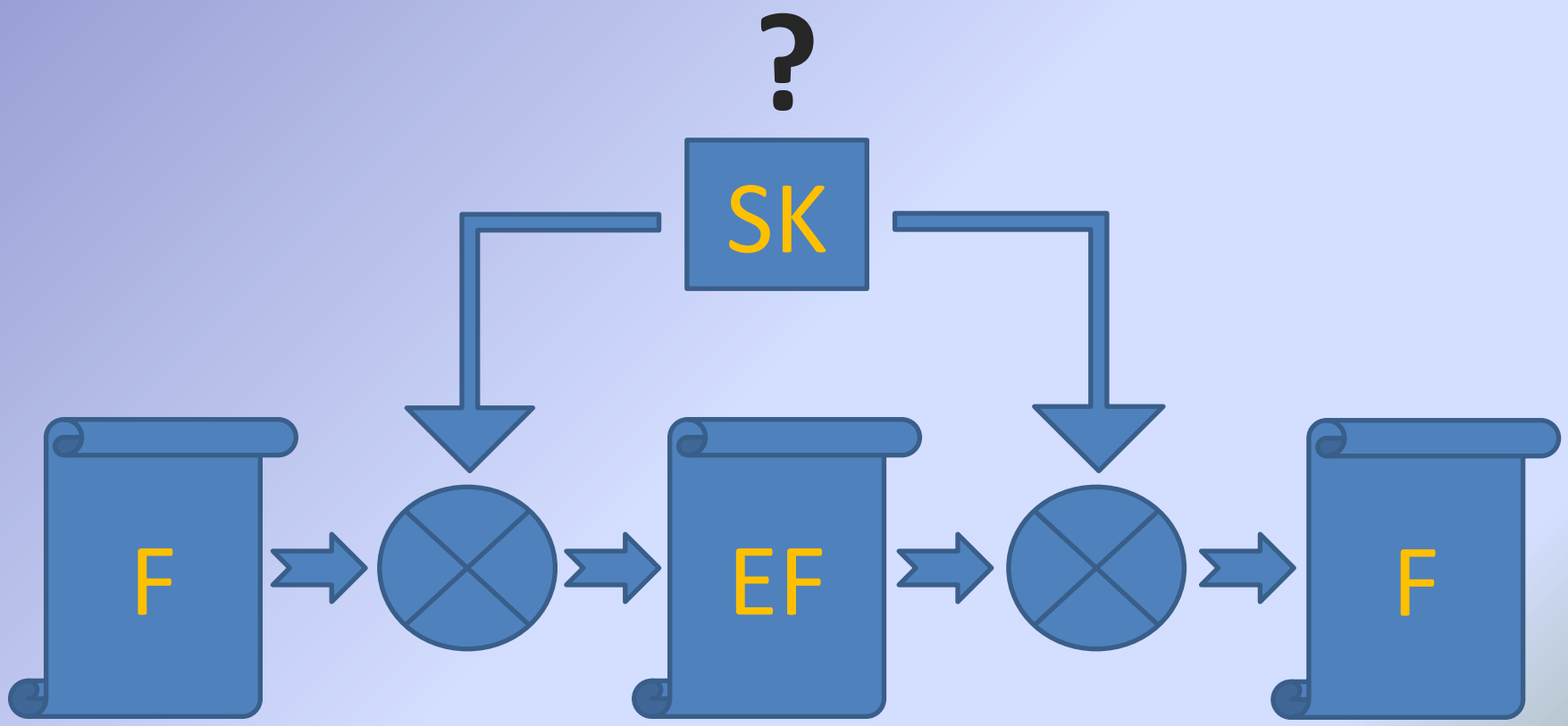


Шифрование с симметричным ключом

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

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

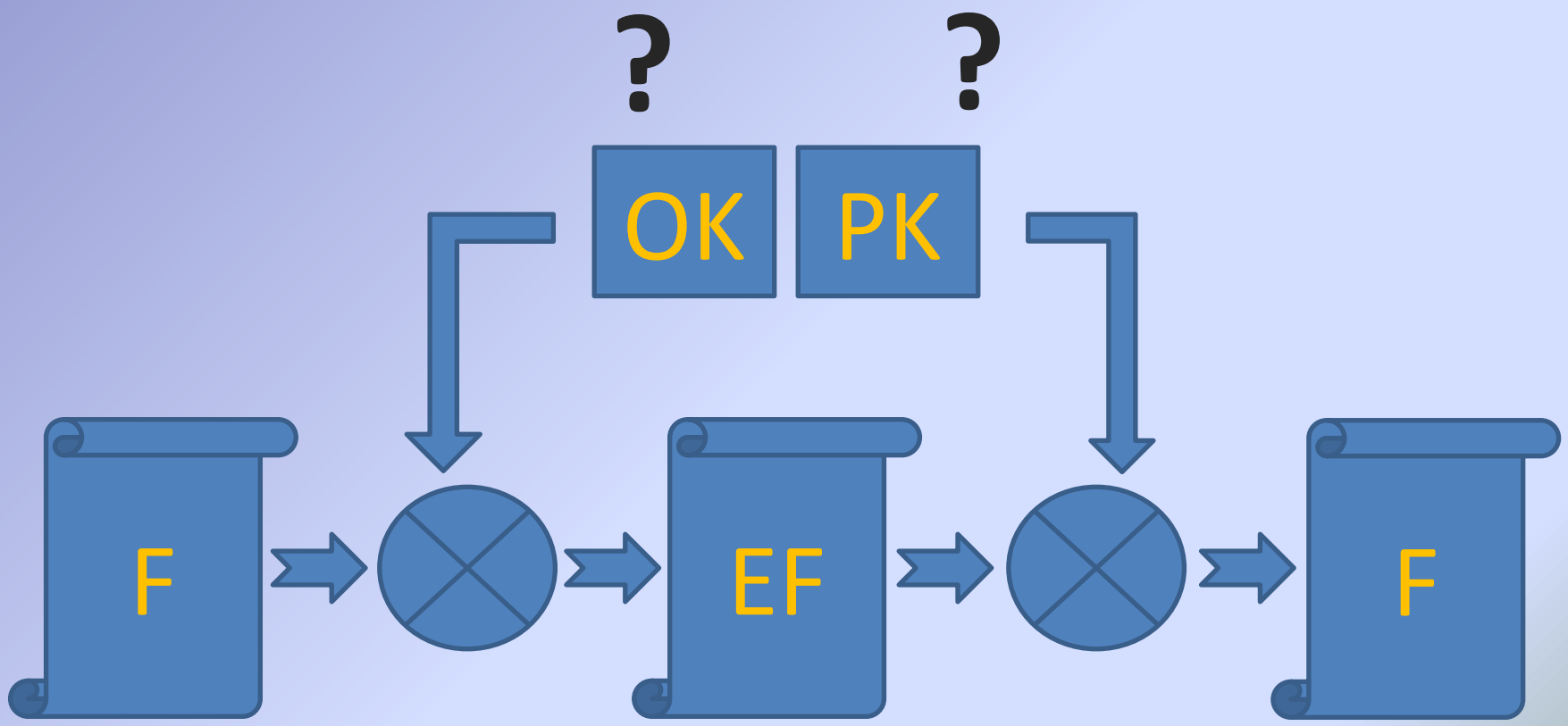
Простейший вариант



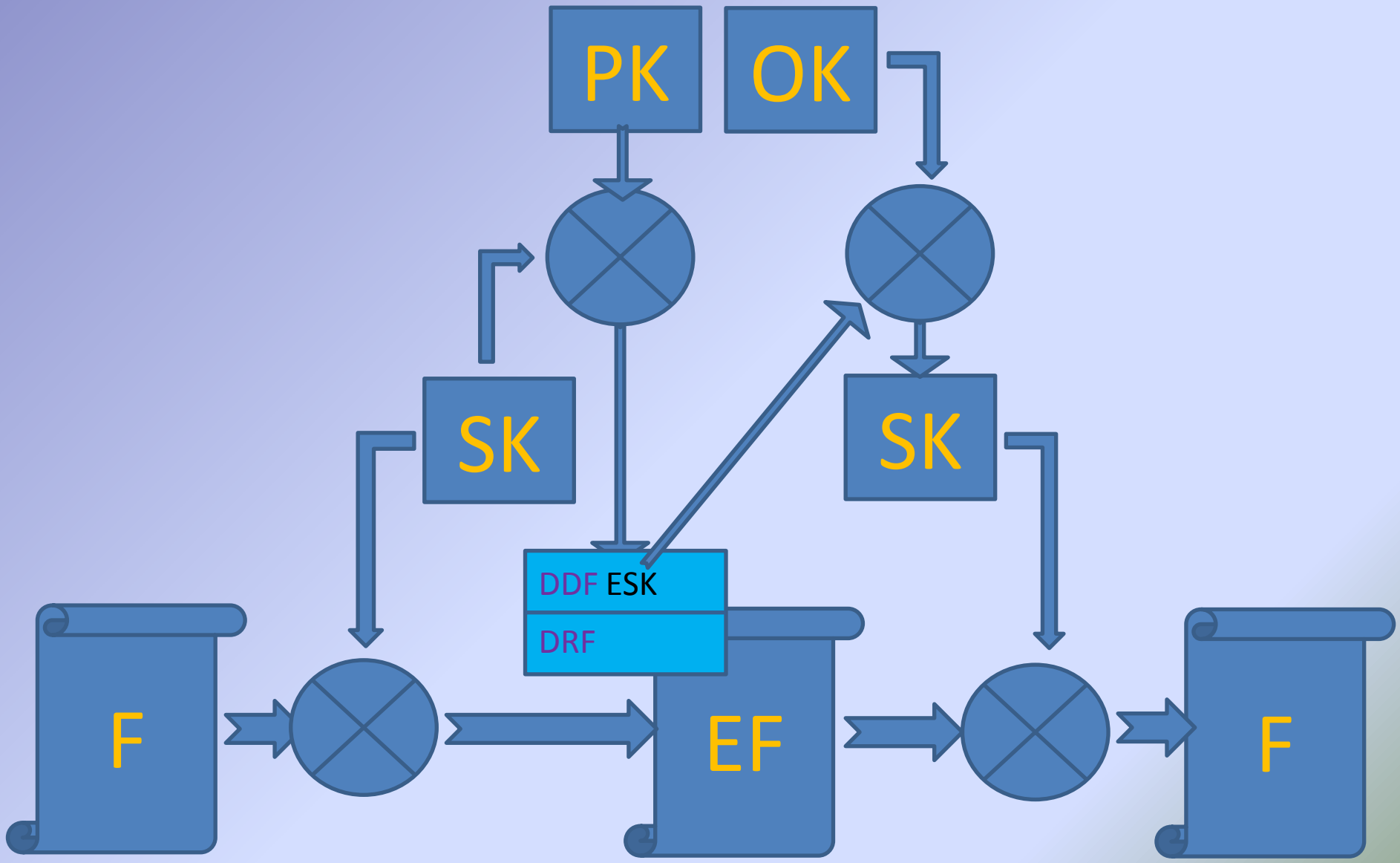
Шифрование с асимметричным ключом (открытым и закрытым ключами)

G->(o,p)	G->(o,p)
T(a,o) = e	T(a,p) = e
T^{-1}(e,p) = a	T^{-1}(e,o) = a

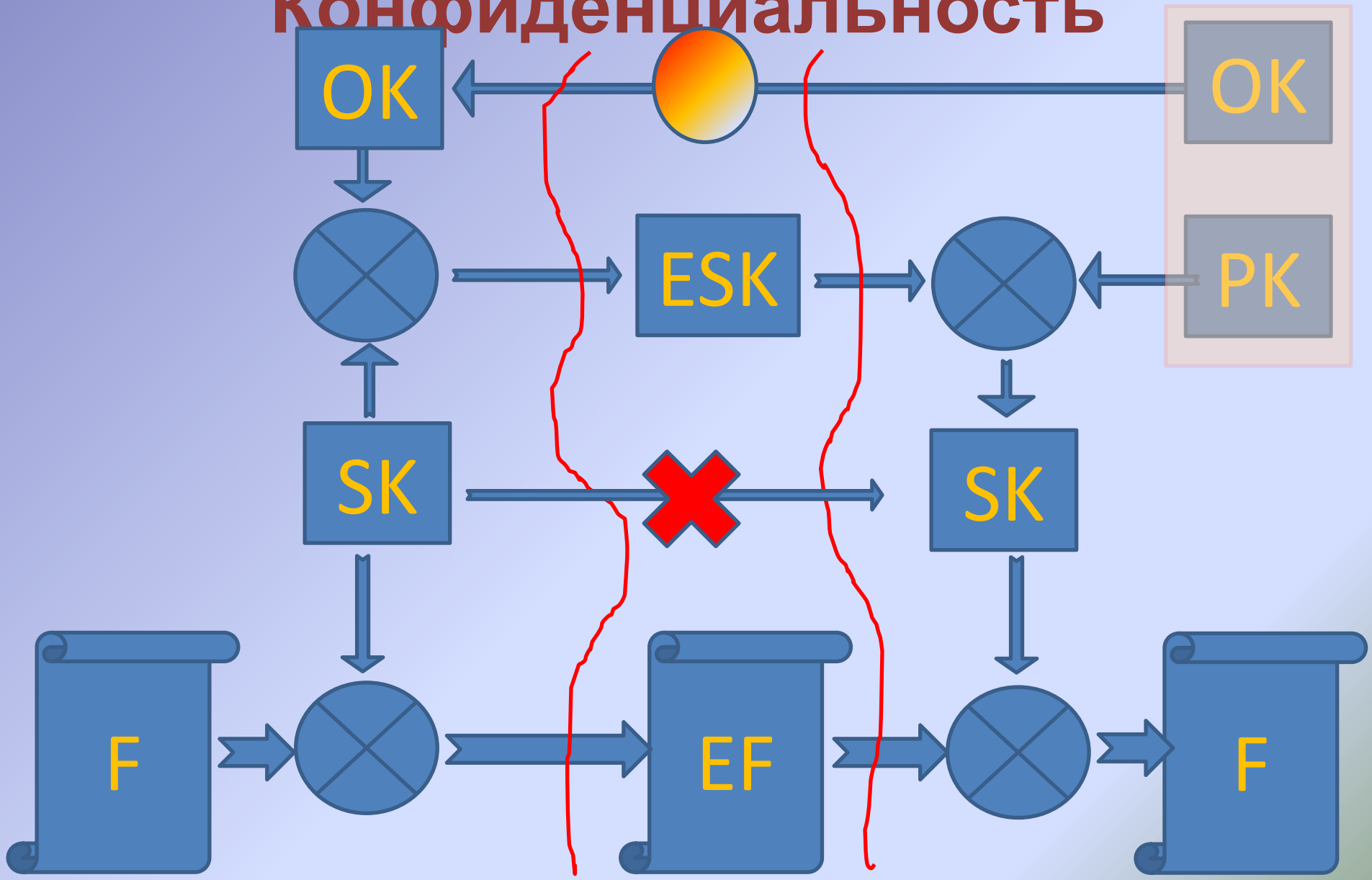
А можно так?



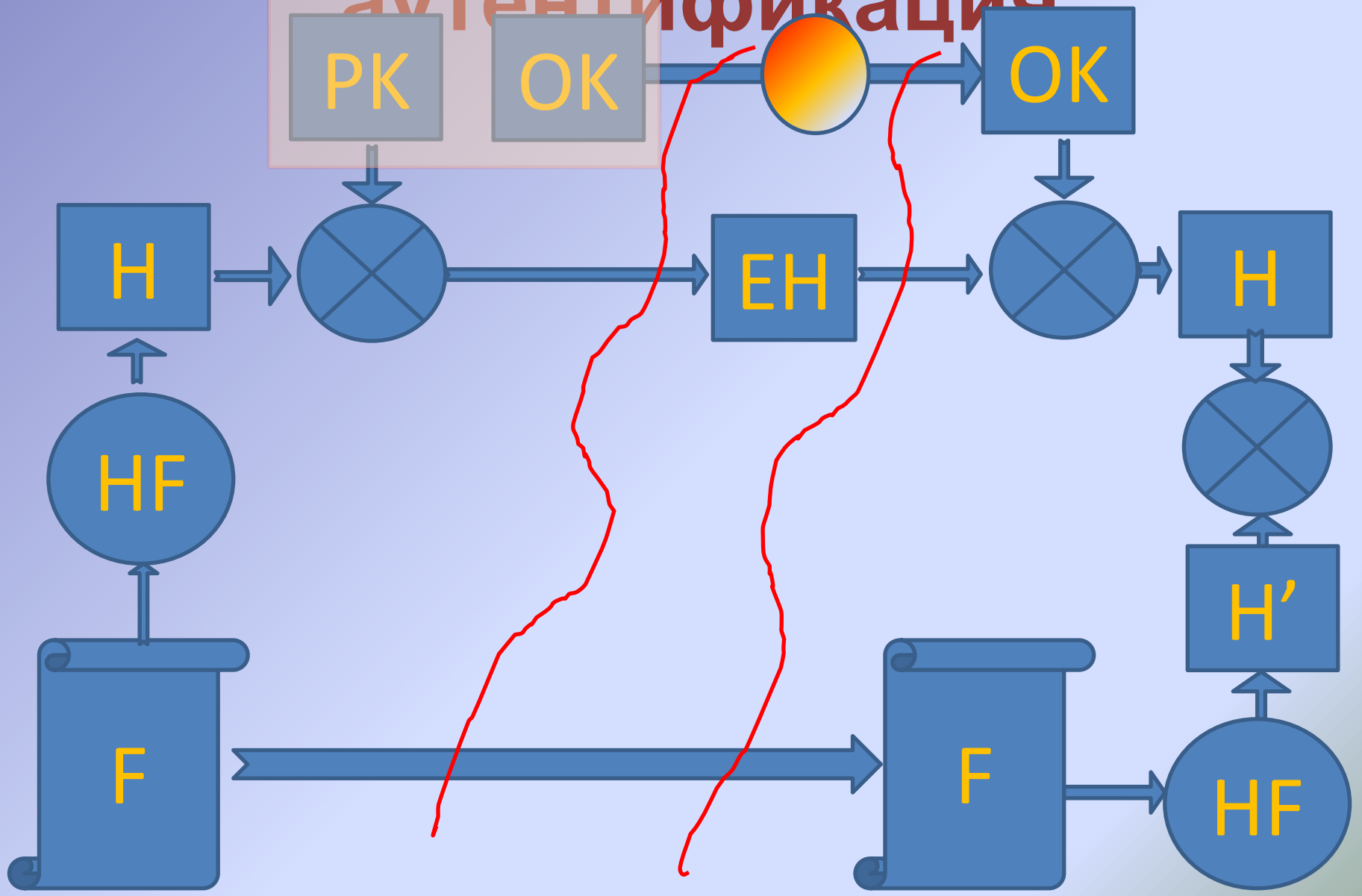
Уже правильнее



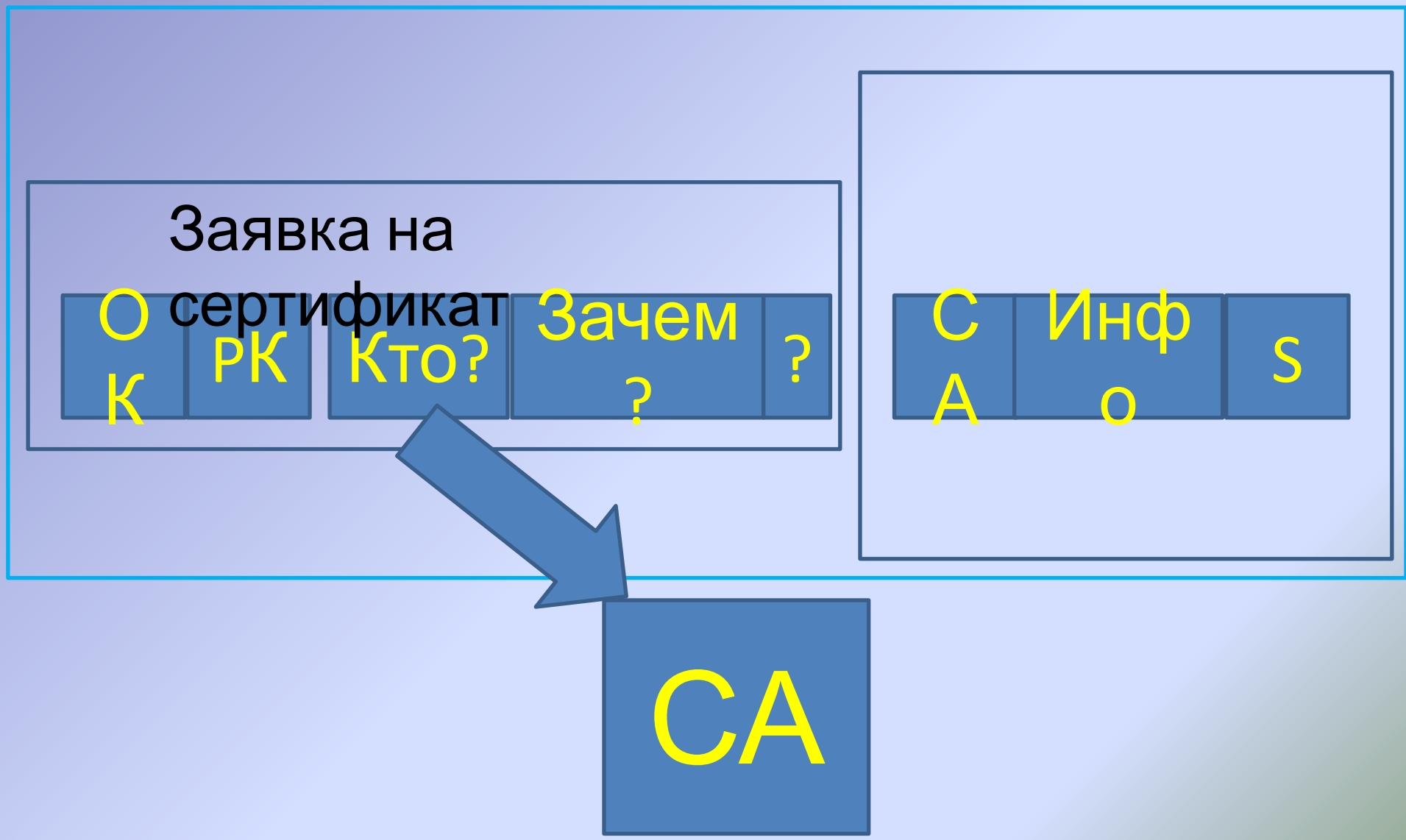
Передача - Конфиденциальность



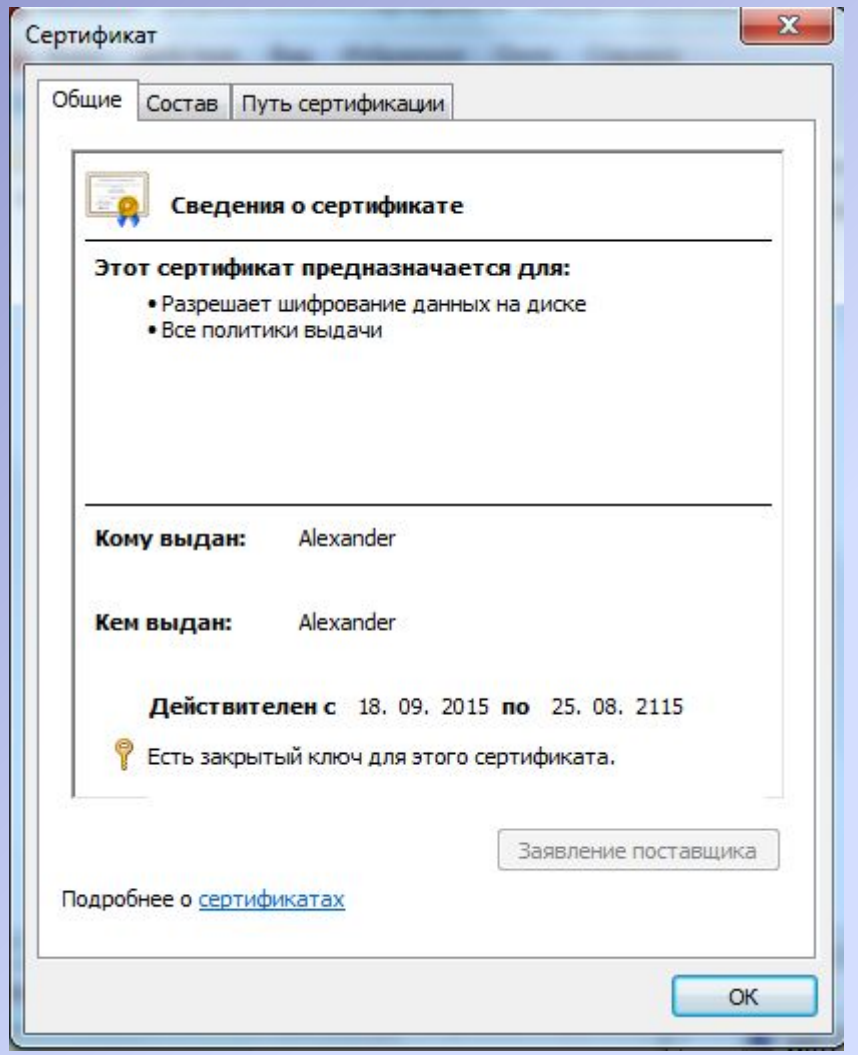
Целостность и аутентификация

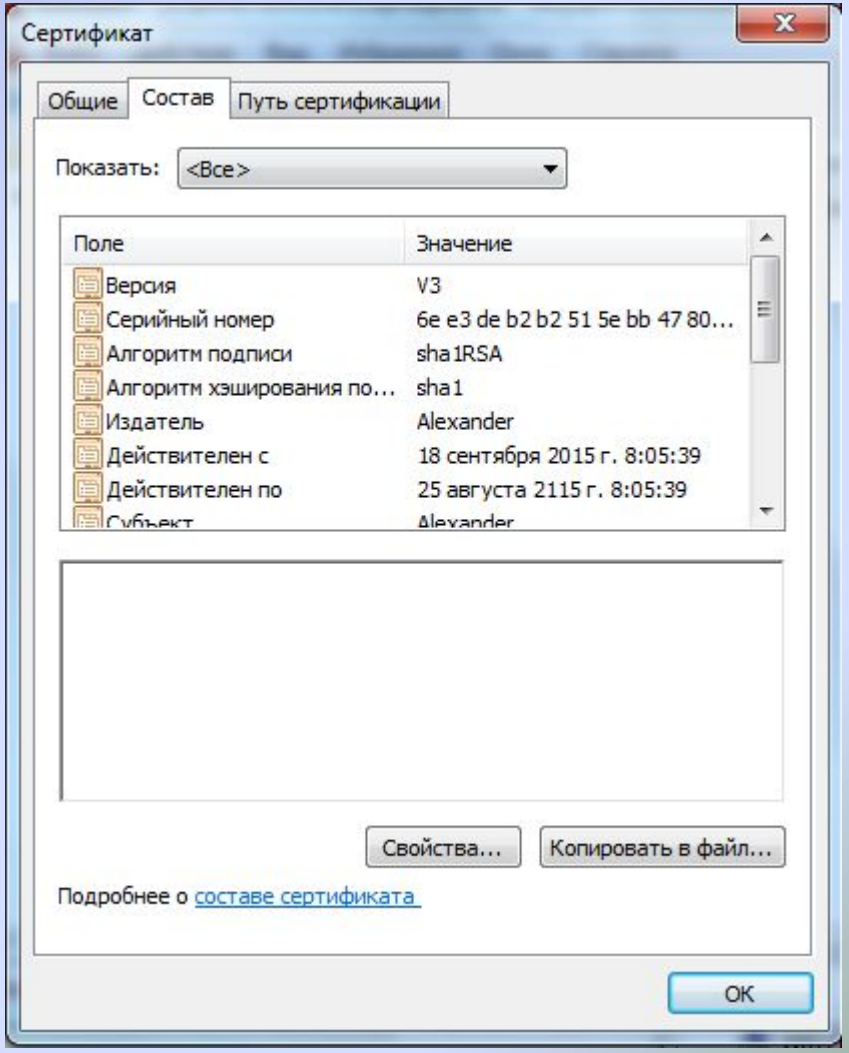


Формирование сертификата

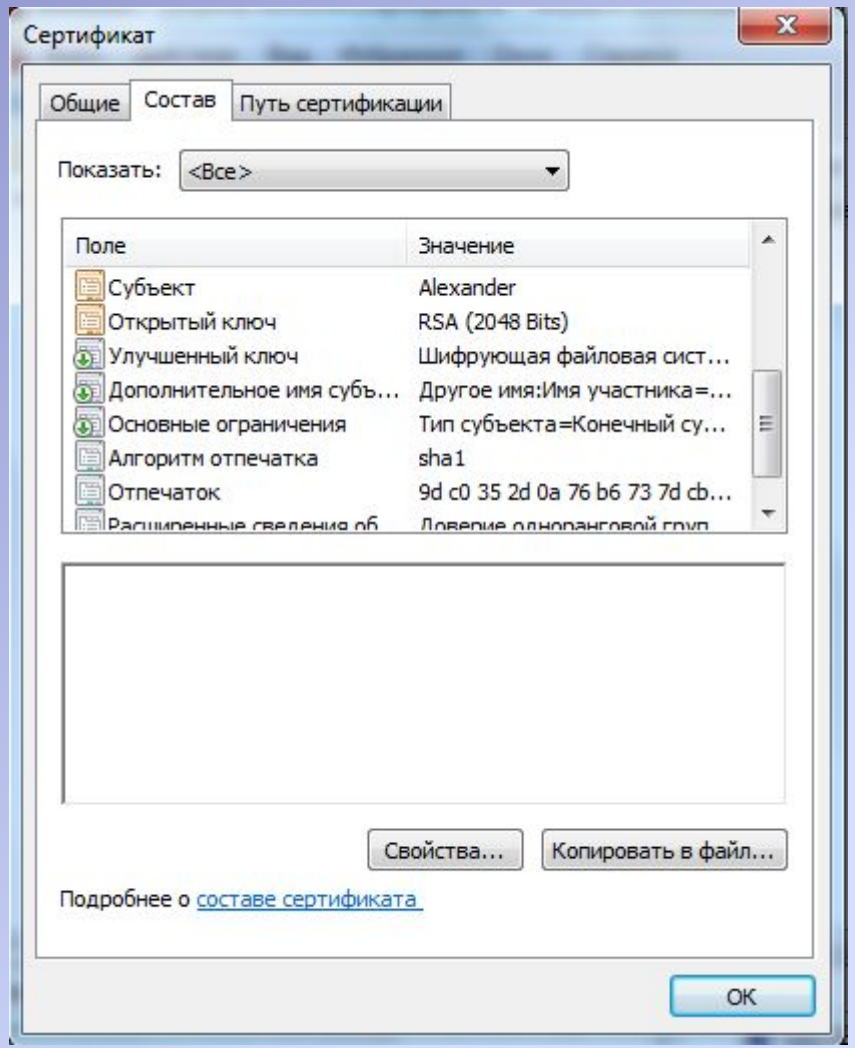


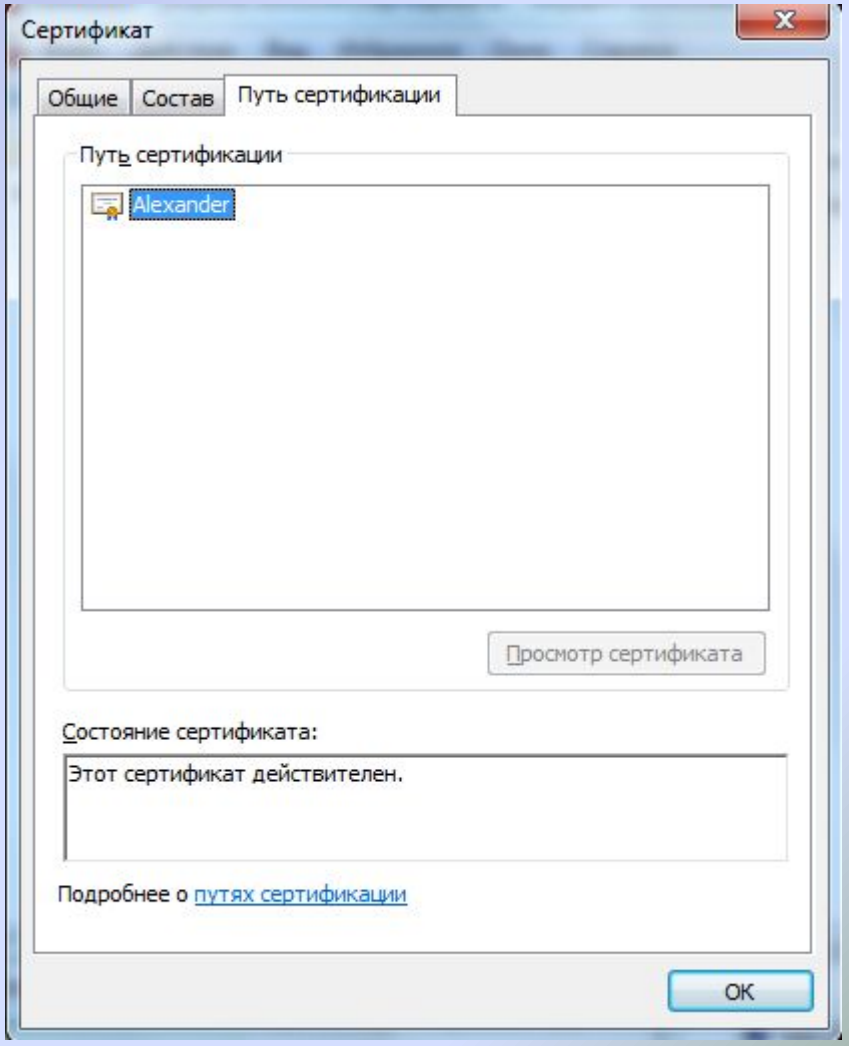
Сертификат


Сертификат
Общие
Состав
Путь сертификации
Сведения о сертификате
Этот сертификат предназначается для:
• Разрешает шифрование данных на диске
• Все политики выдачи
Кому выдан: Alexander
Кем выдан: Alexander
Действителен с 18. 09. 2015 по 25. 08. 2115
Есть закрытый ключ для этого сертификата.
Заявление поставщика
Подробнее о сертификатах
OK

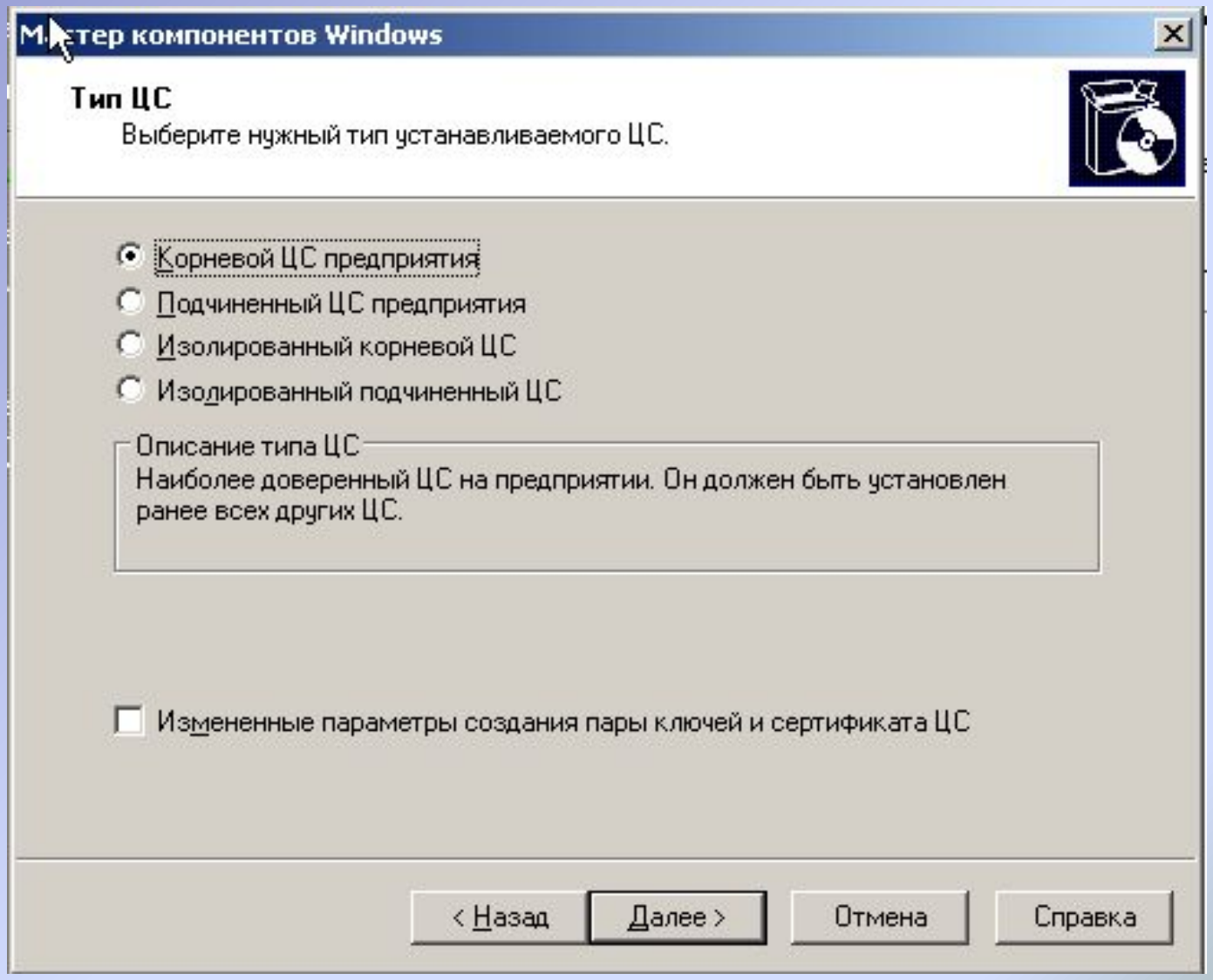

Сертификат
Общие
Состав
Путь сертификации
Показать: <Все>
Поле
Значение
Версия V3
Серийный номер 6e e3 de b2 b2 51 5e bb 47 80...
Алгоритм подписи sha1RSA
Алгоритм хэширования по... sha1
Издатель Alexander
Действителен с 18 сентября 2015 г. 8:05:39
Действителен по 25 августа 2115 г. 8:05:39
Субъект Alexander
Свойства...
Копировать в файл...
Подробнее о составе сертификата
OK

Сертификат

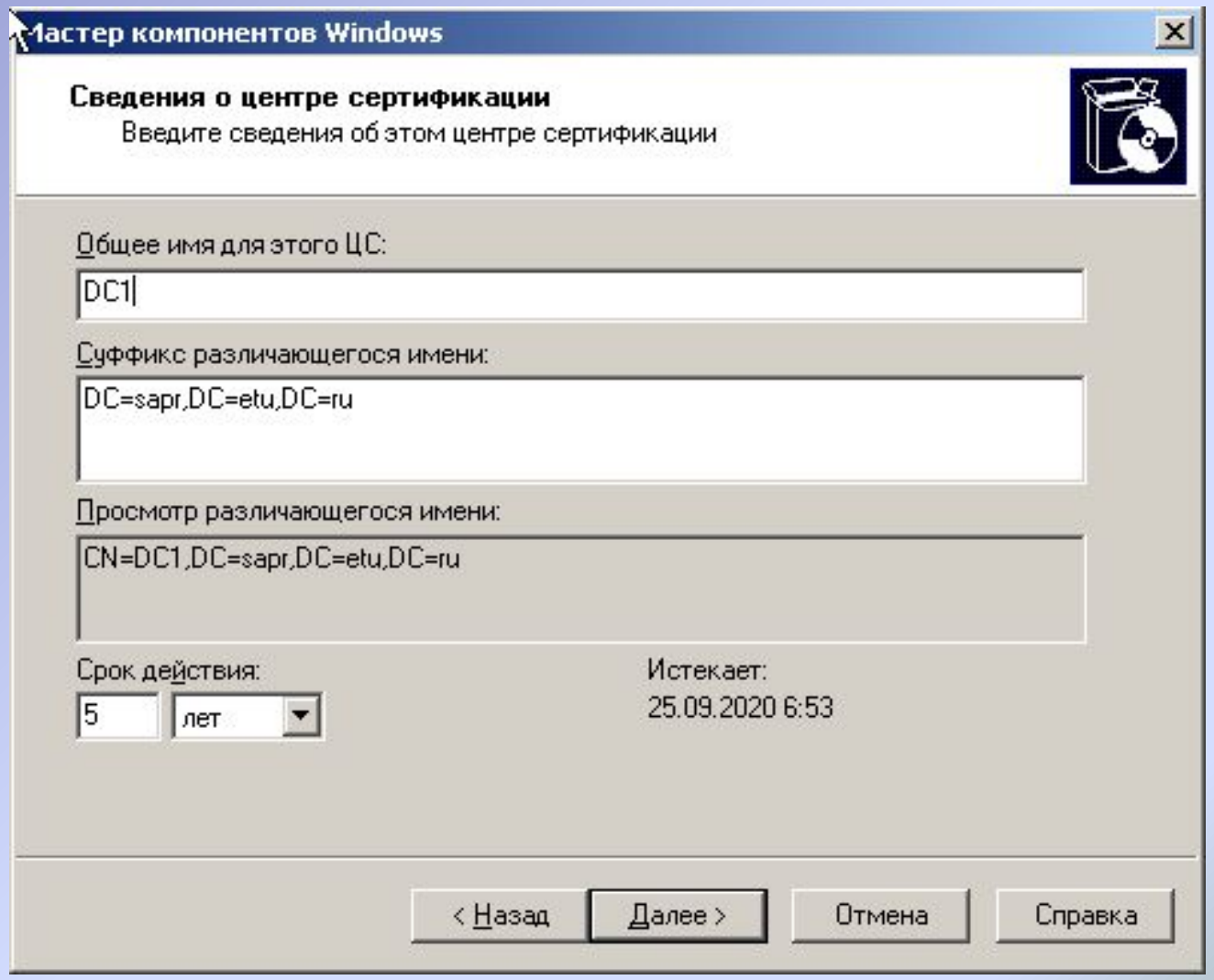

Сертификат
Общие
Состав
Путь сертификации
Показать:
<Все>
Поле
Значение
Субъект
Alexander
Открытый ключ
RSA (2048 Bits)
Улучшенный ключ
Шифрующая файловая сист...
Дополнительное имя субъ...
Другое имя:Имя участника=...
Основные ограничения
Тип субъекта=Конечный су...
Алгоритм отпечатка
sha1
Отпечаток
9d c0 35 2d 0a 76 b6 73 7d cb...
Свойства...
Копировать в файл...
Подробнее о составе сертификата
OK


Сертификат
Общие
Состав
Путь сертификации
Путь сертификации
Alexander
Просмотр сертификата
Состояние сертификата:
Этот сертификат действителен.
Подробнее о путях сертификации
OK

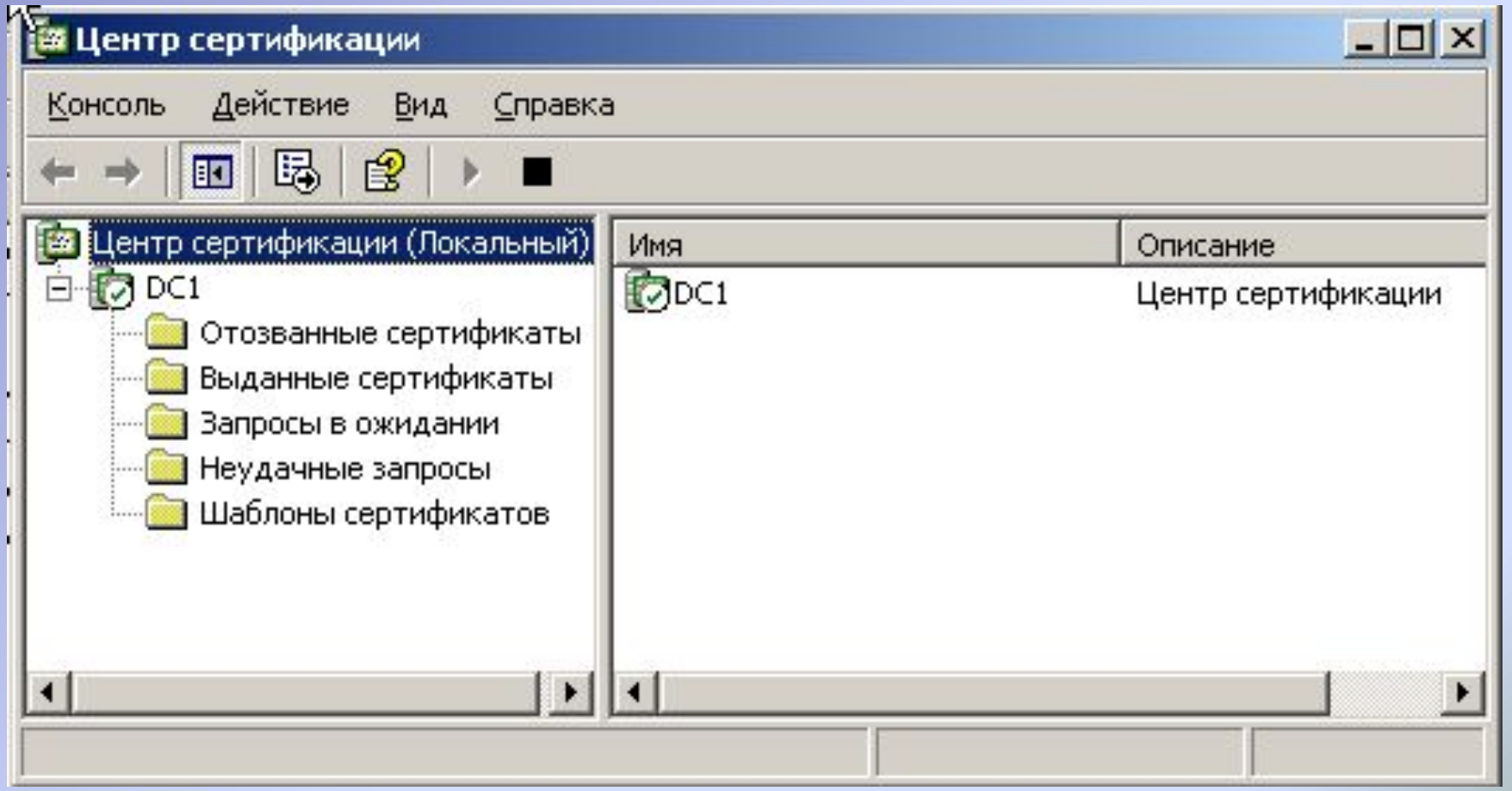
Типы CA


Мастер компонентов Windows
Тип ЦС
Выберите нужный тип устанавливаемого ЦС.
Корневой ЦС предприятия
Подчиненный ЦС предприятия
Изолированный корневой ЦС
Изолированный подчиненный ЦС
Описание типа ЦС
Наиболее доверенный ЦС на предприятии. Он должен быть установлен ранее всех других ЦС.
Измененные параметры создания пары ключей и сертификата ЦС
< Назад
Далее >
Отмена
Справка

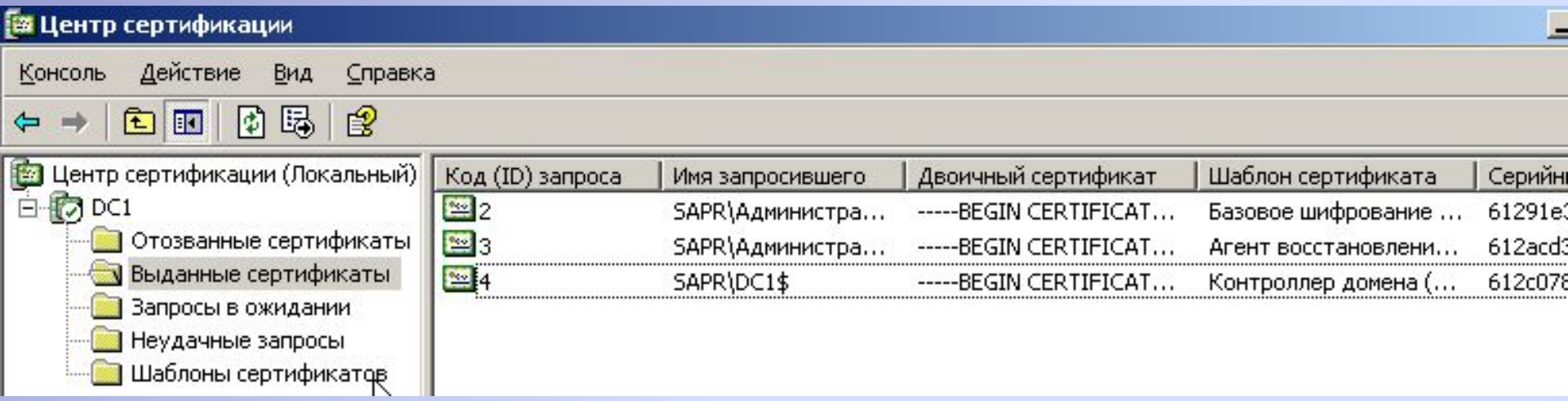
Имя и сертификат



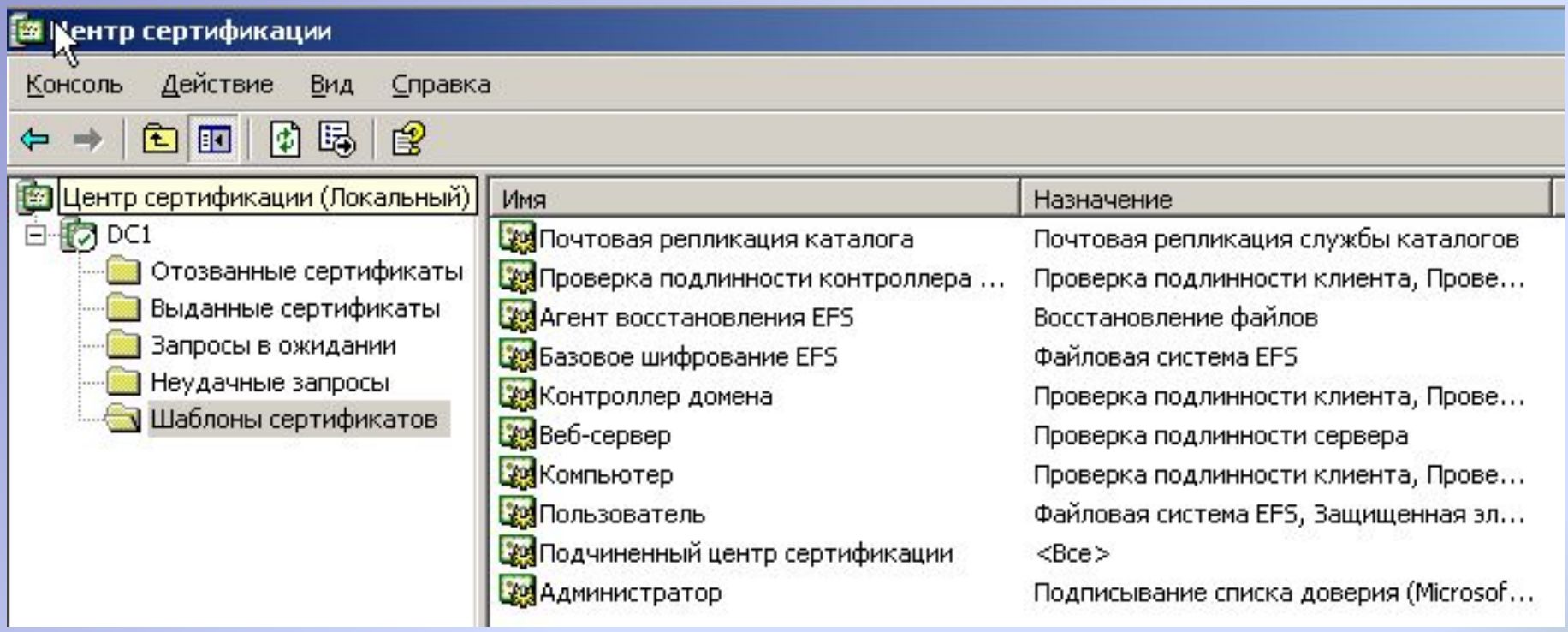
Консоль центра сертификатов



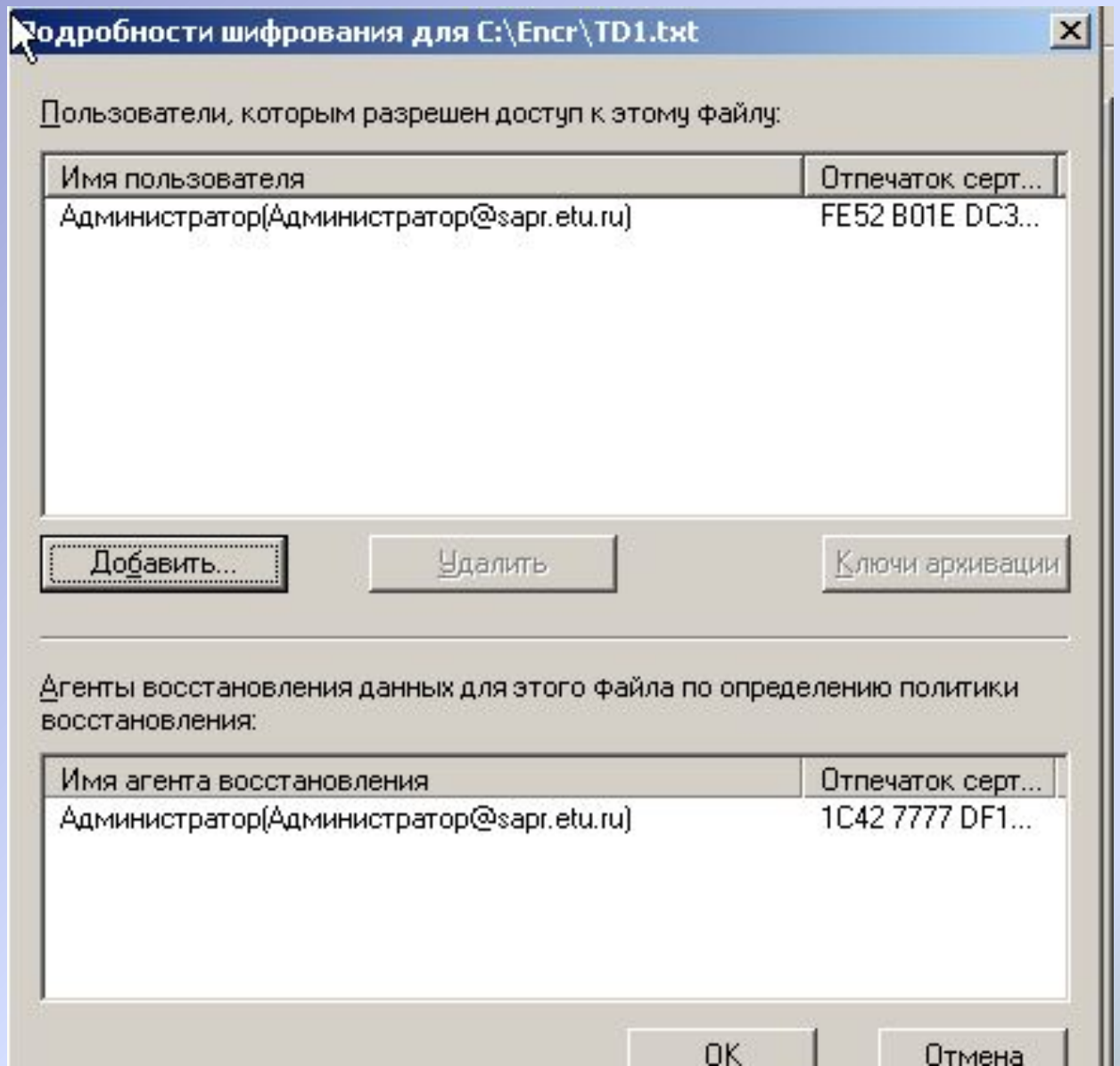
Выданные сертификаты



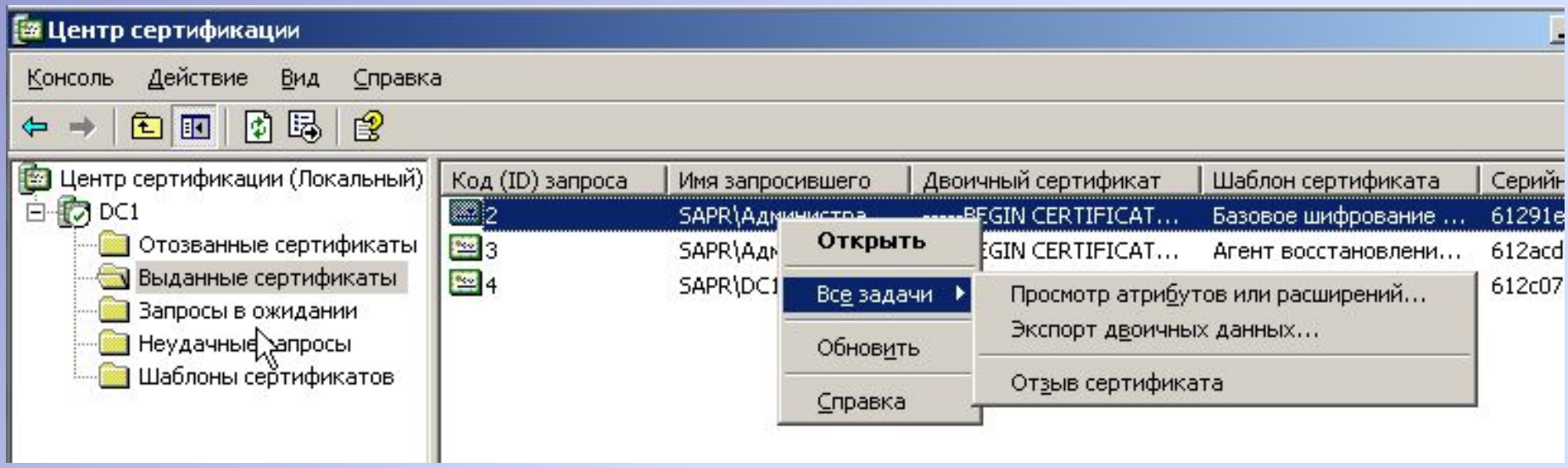
Шаблоны сертификатов



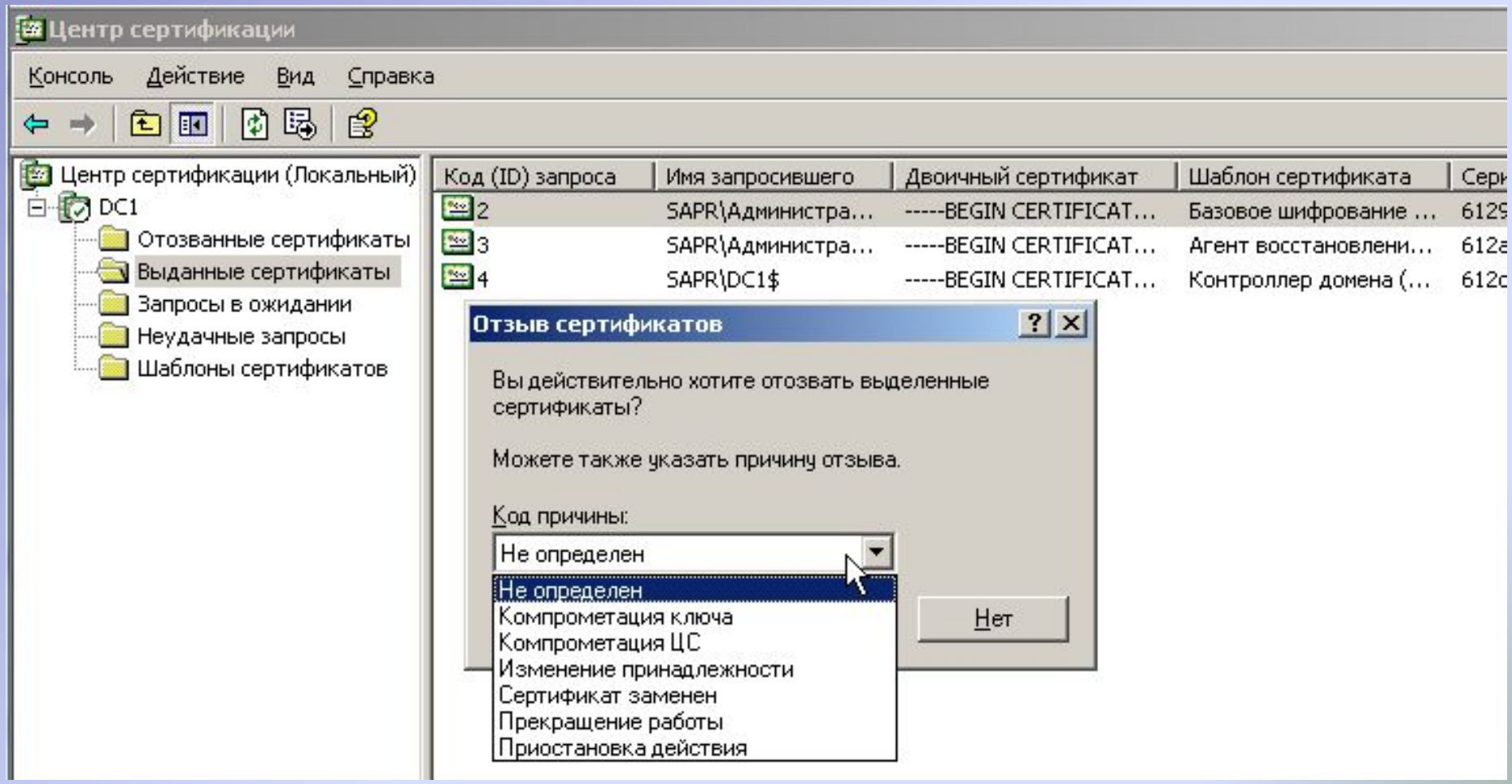
Заголовок файла



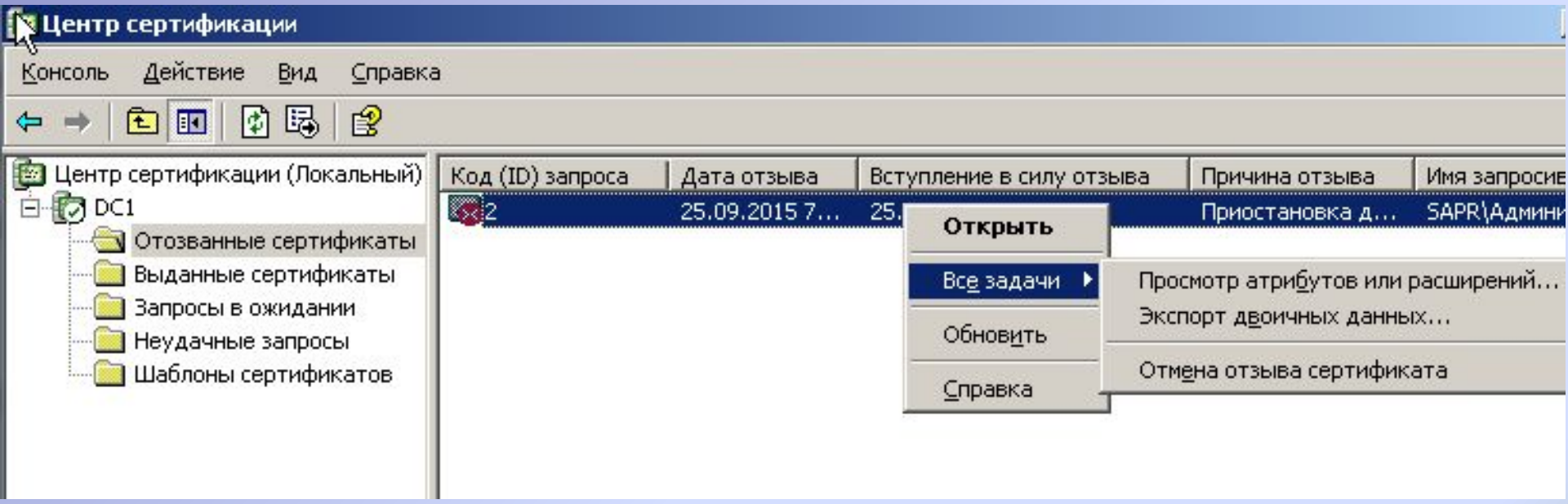
Отзыв сертификата



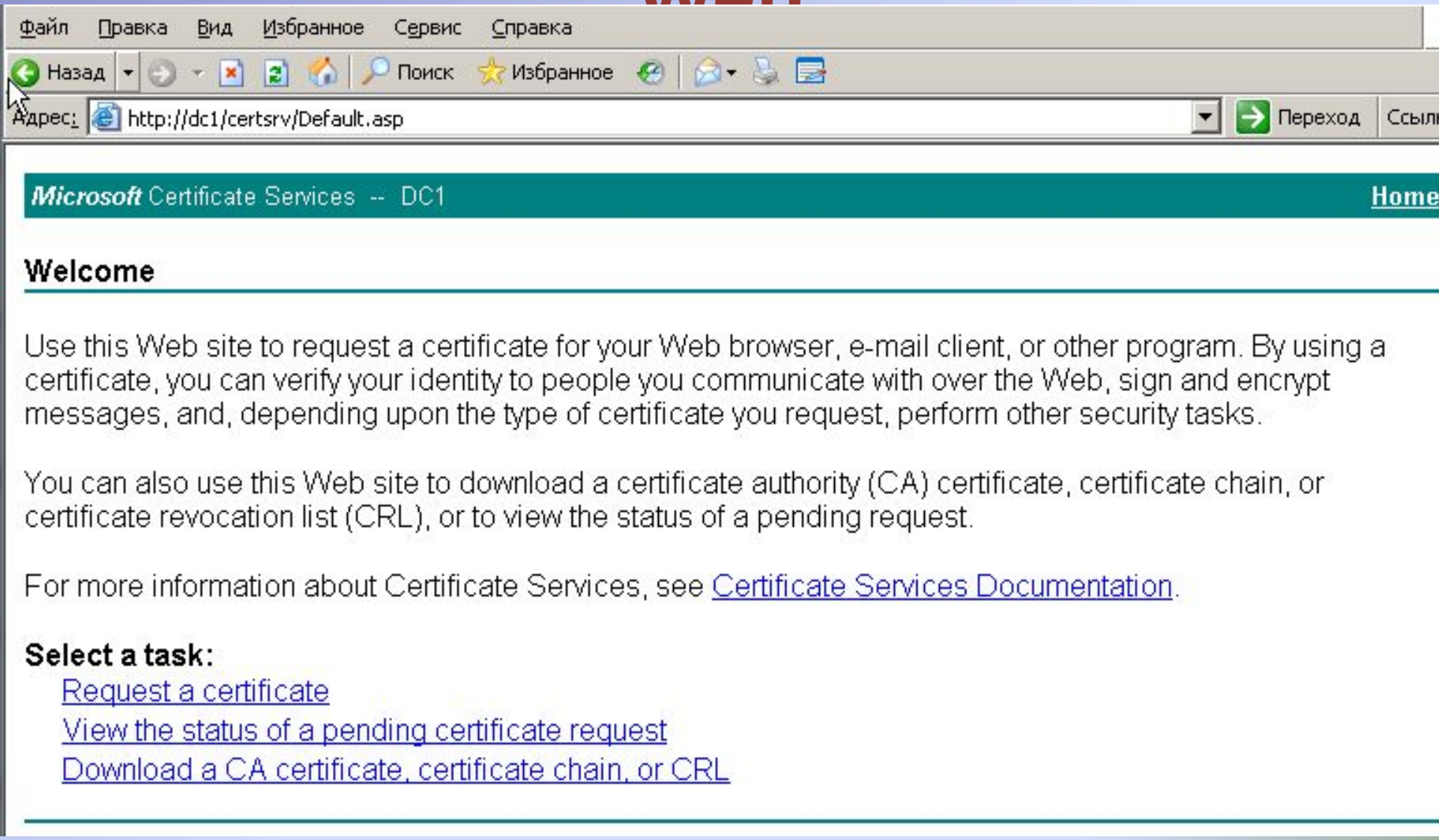
Отзыв сертификата - причина



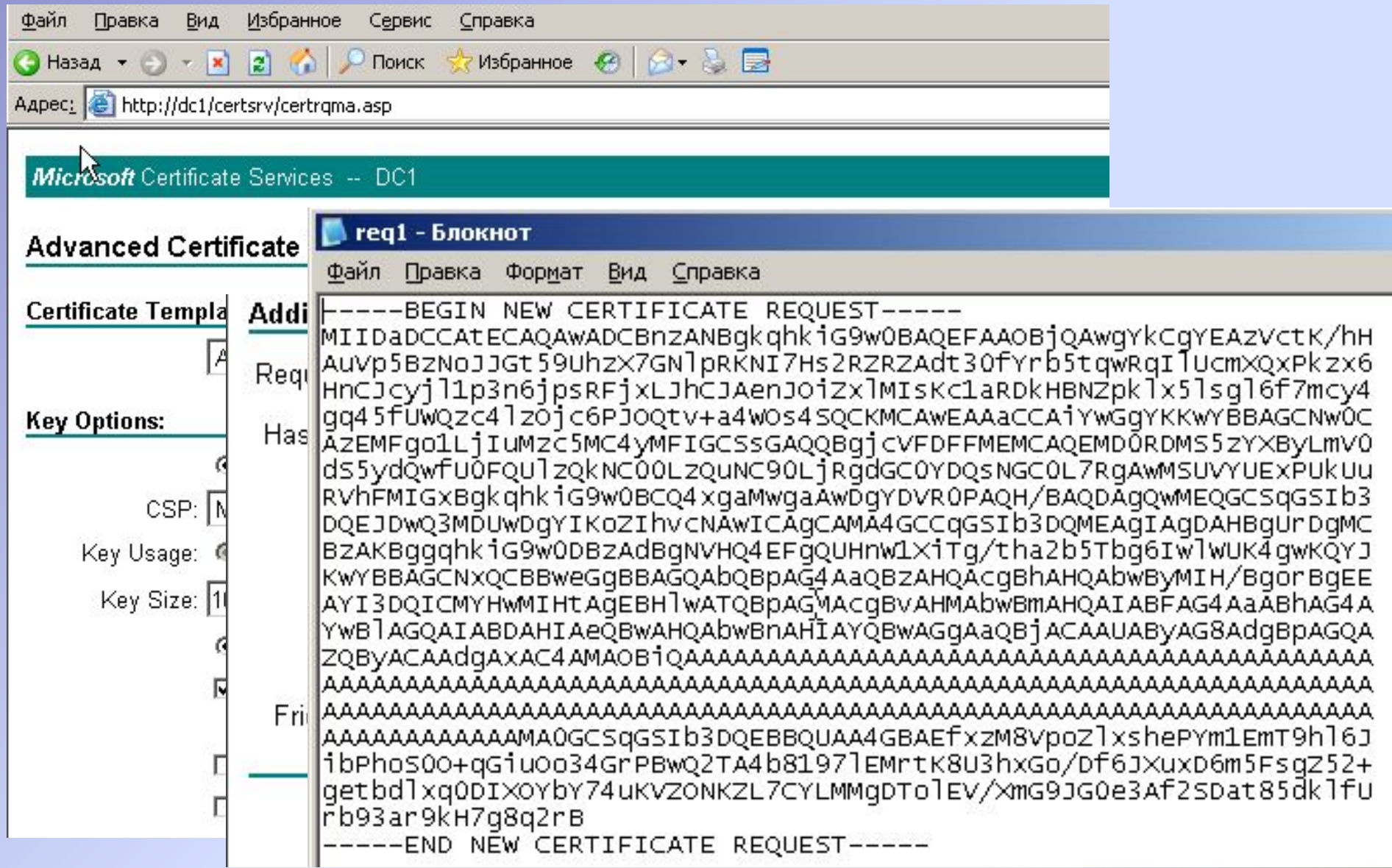
Отмена отзыва сертификата



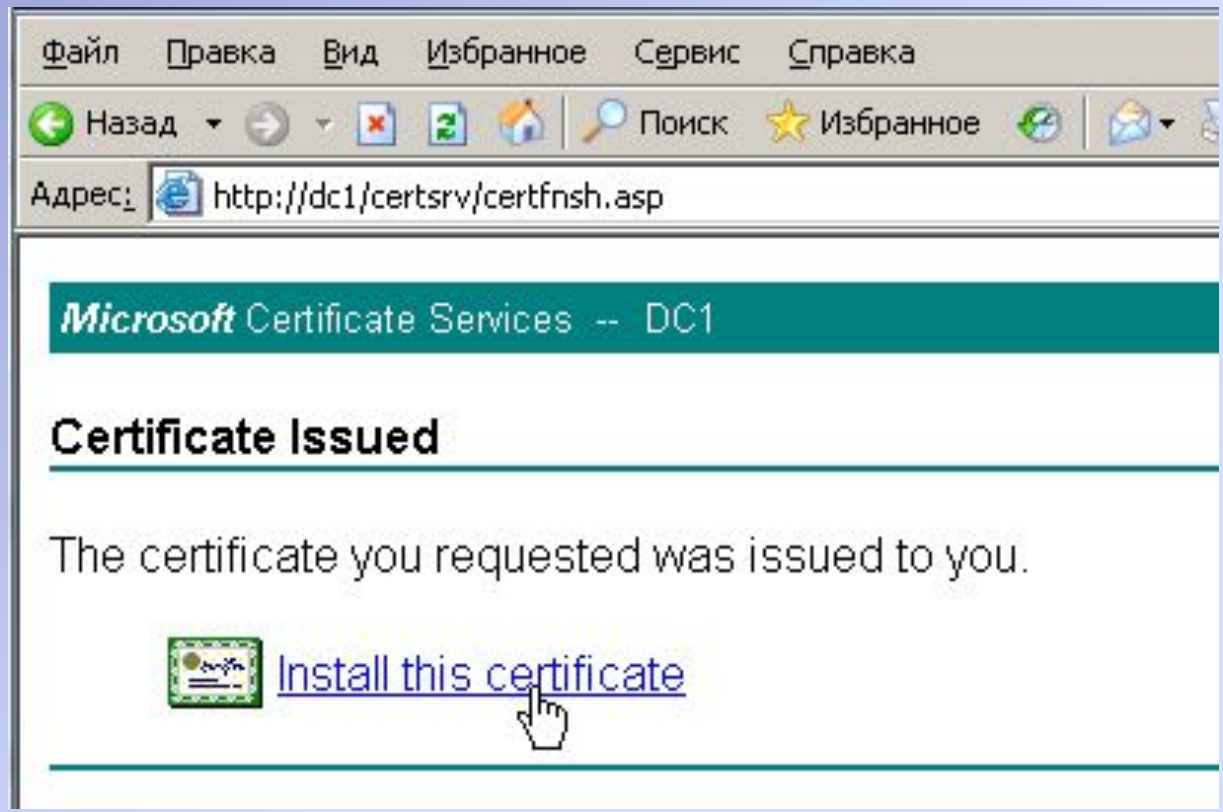
Запрос сертификата через Web



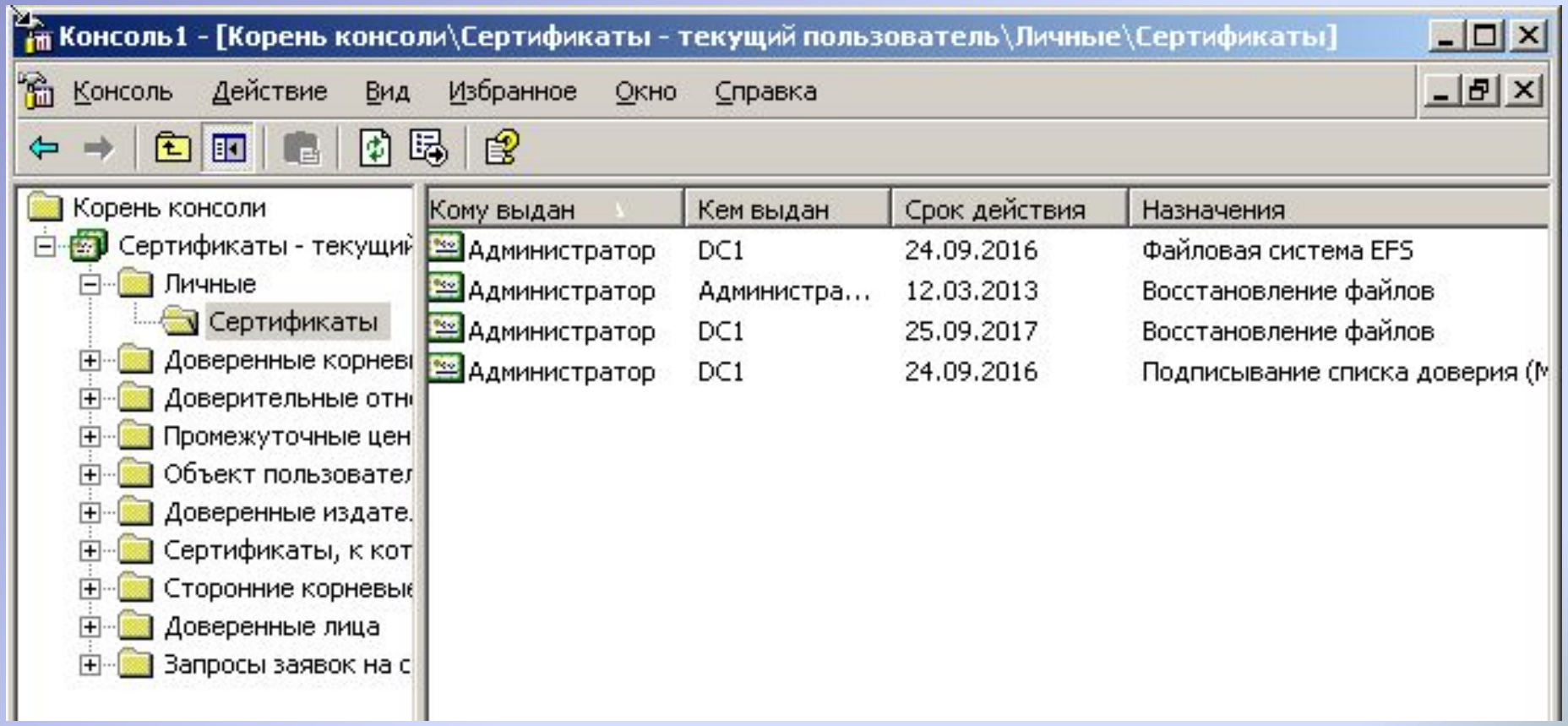
Детали запроса



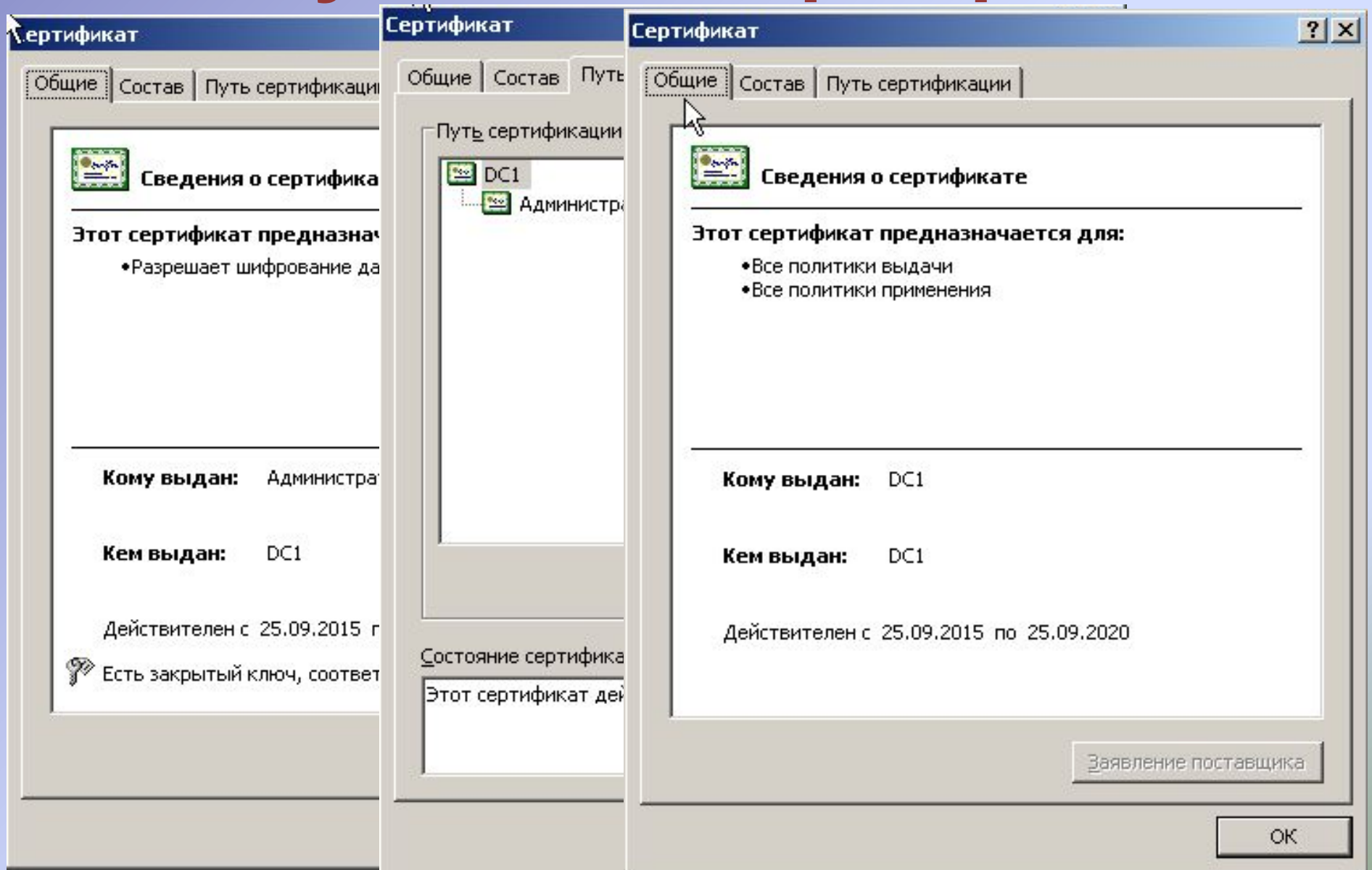
Установка готового сертификата



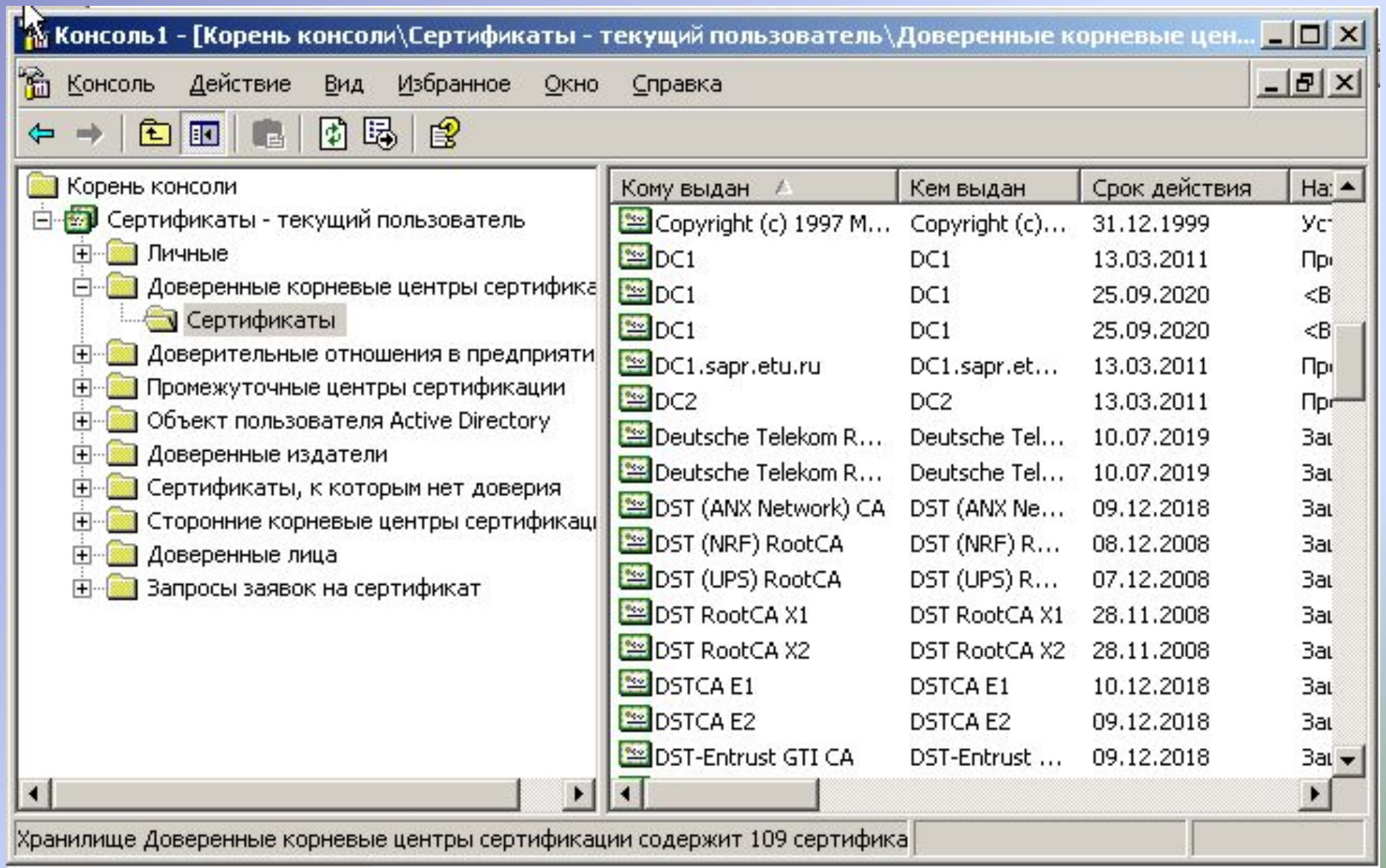
Личные сертификаты



Полученный сертификат



Доверенные сертификаты



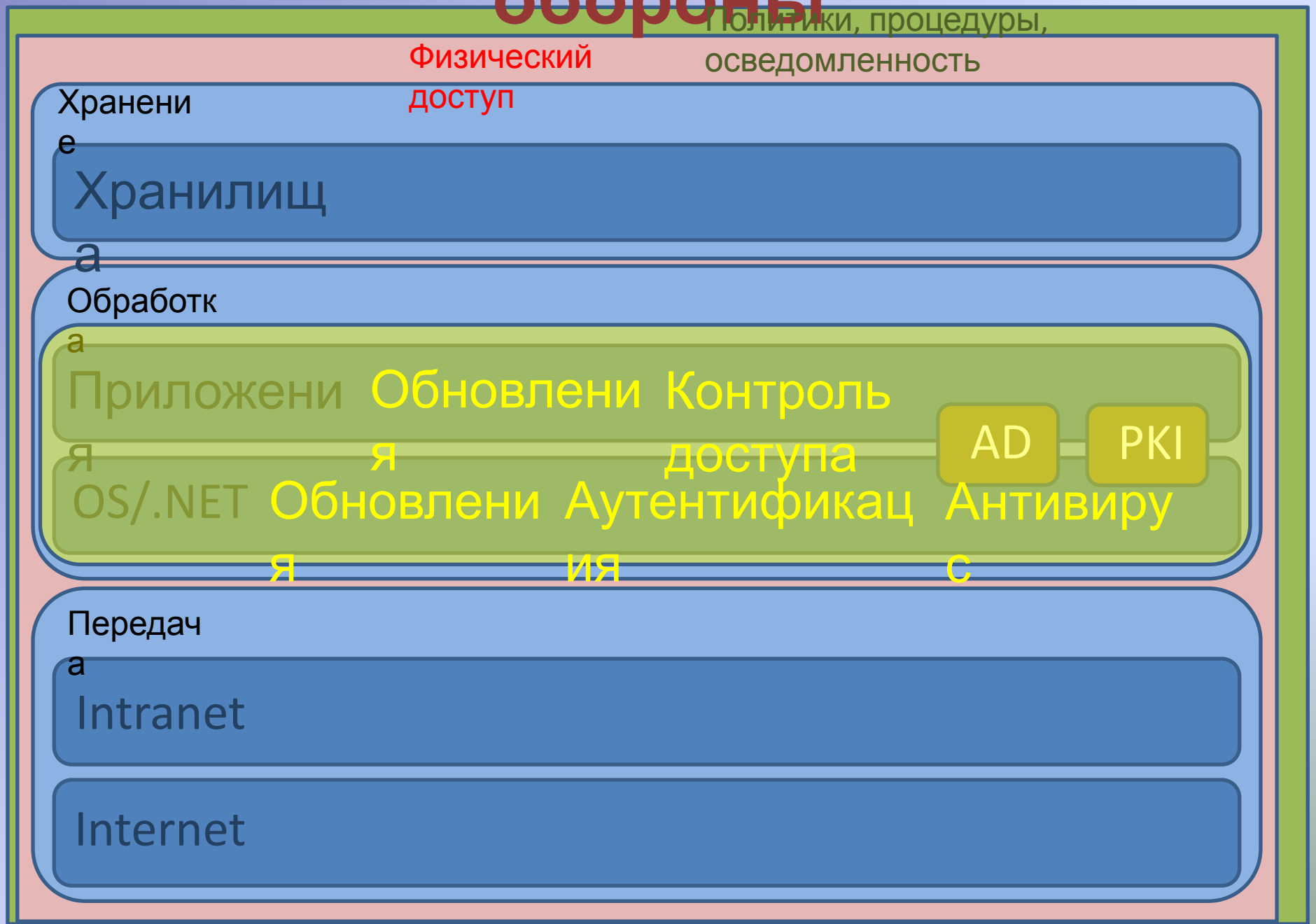
Защита компьютерной информации. Защита информации на уровне кода

Горячев Александр Вадимович

Доцент кафедры Информационной безопасности

Avgoriachev@etu.ru

Модель эшелонированной обороны



Обновления – какие проблемы?

- Ошибки изначального кода
- Уязвимости

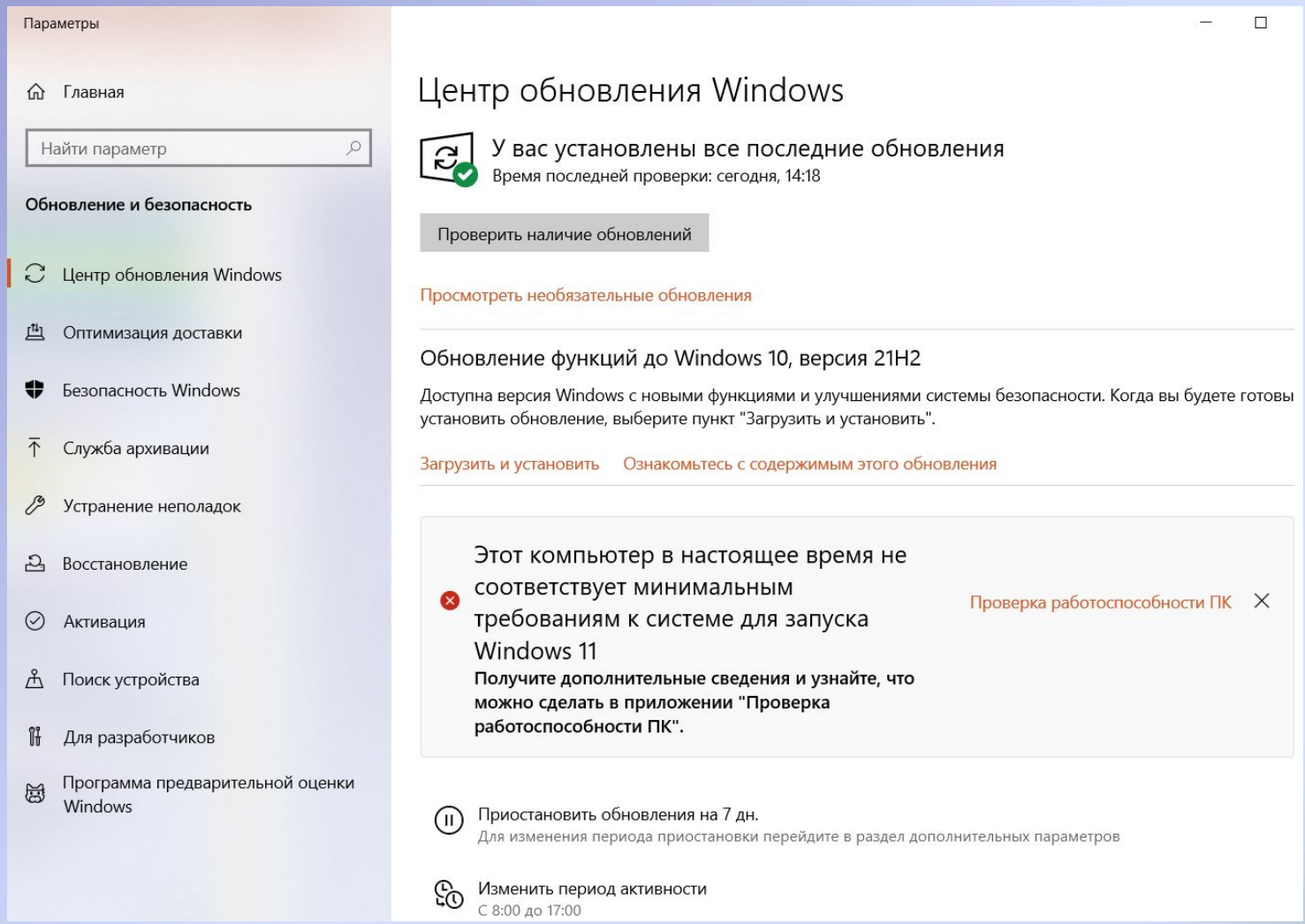
Как бороться?

- «Заплатки» (Patch)
- Замена кода

Все ли изменения нужны?

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

Центр обновлений Windows



Типы атак

Атака	Характеристики
Eavesdropping	• «Подсматривание» коммуникаций.
Data Modification	• Изменение пакетов данных.
Identity Spoofing	• Атака с чужого адреса или под чужой личиной.
Password Based	• Получение чужого пароля.
Denial of Service	• Прекращение нормальной работы объекта-цели.
Man in the Middle	• «Испорченый телефон».
Compromised Key	• Добыча чужого ключа.
Sniffer	• Мониторинг сети.
Application Layer	• Атака на приложение.

Phishing

Получение паролей, PIN-кодов и пр.

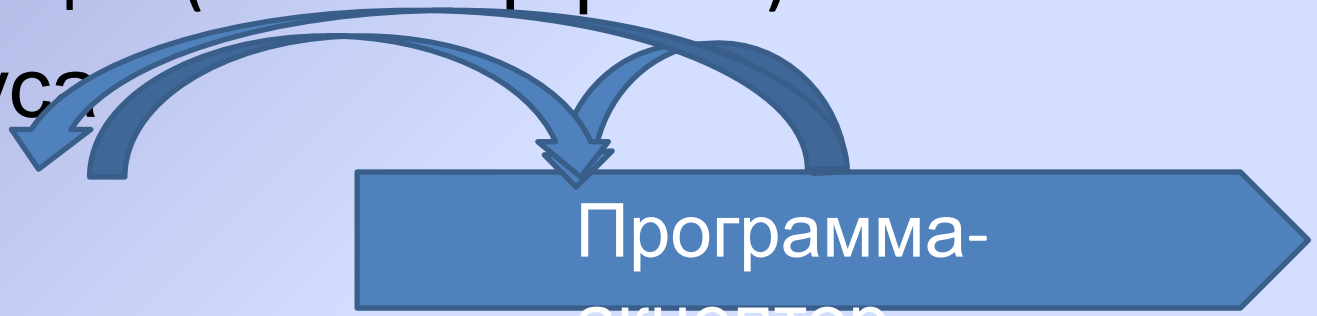
- Пассивное наблюдение
- Спровоцировать передачу неавторизованному участнику
- Проникновение с кражей

USB-флэш атака

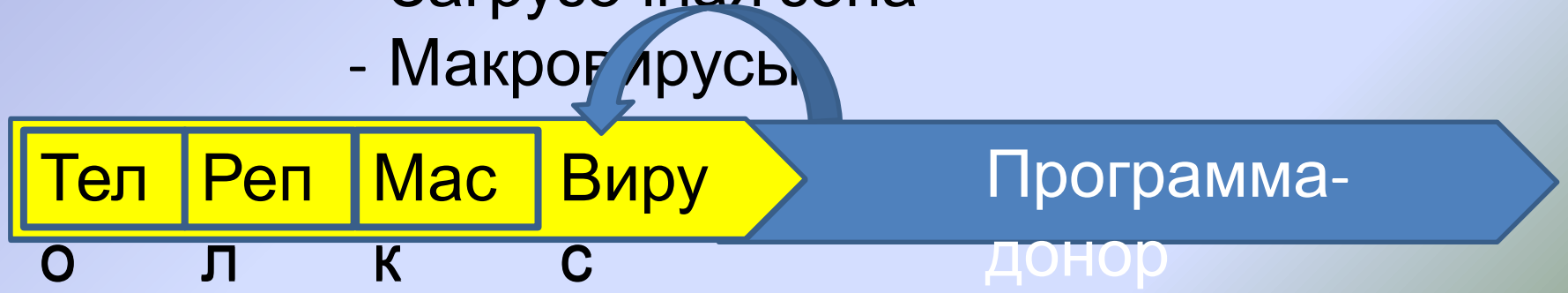
- Из 30 разбросанных по территории предприятия флэшек 20 «откликнулись» в течении часа

Вирус

- Репликатор
- Маскировщик (полиморфизм)
- Тело вируса:

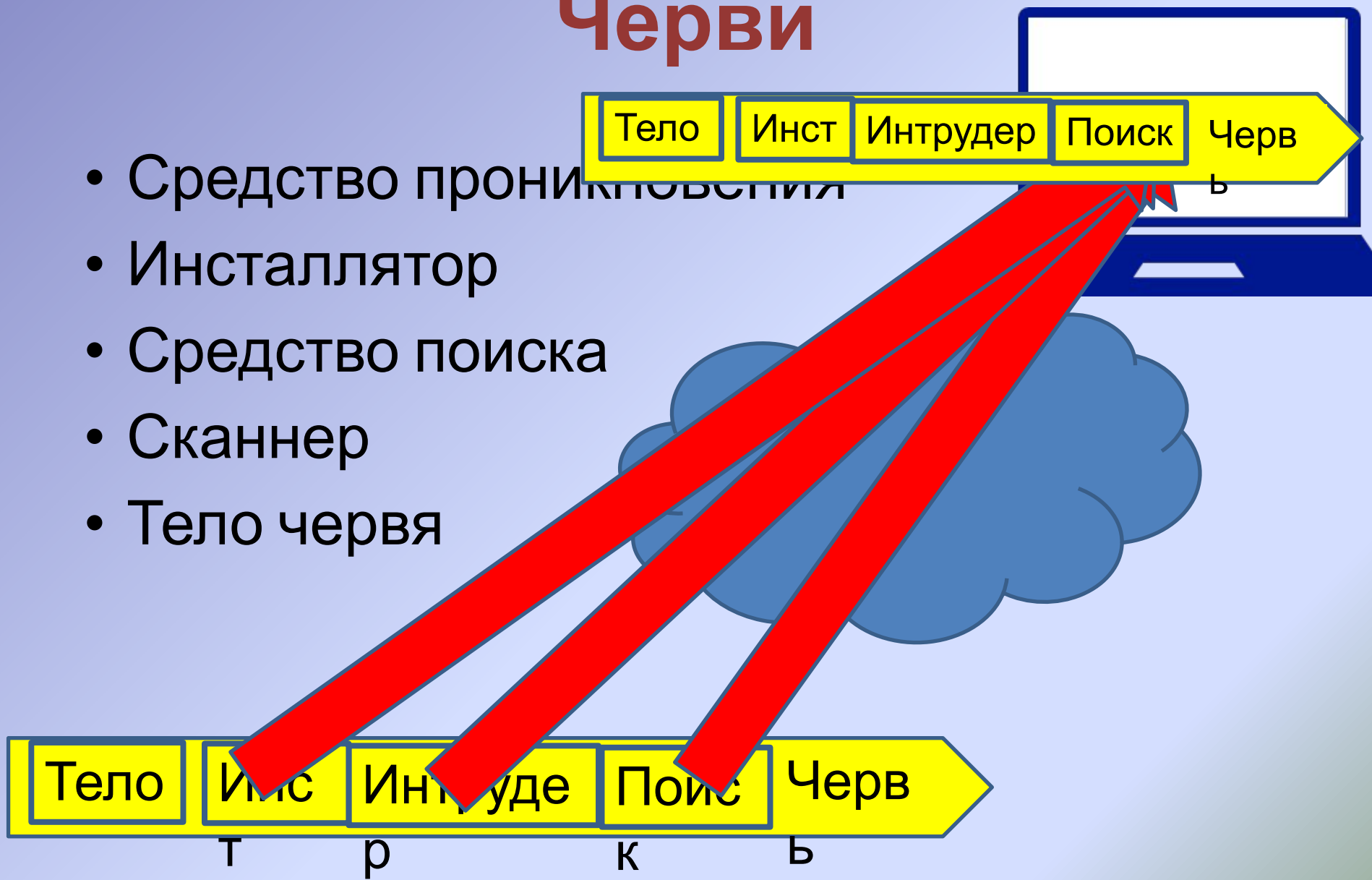


- Файлы
- Система
- Загрузочная зона
- Макровирусы



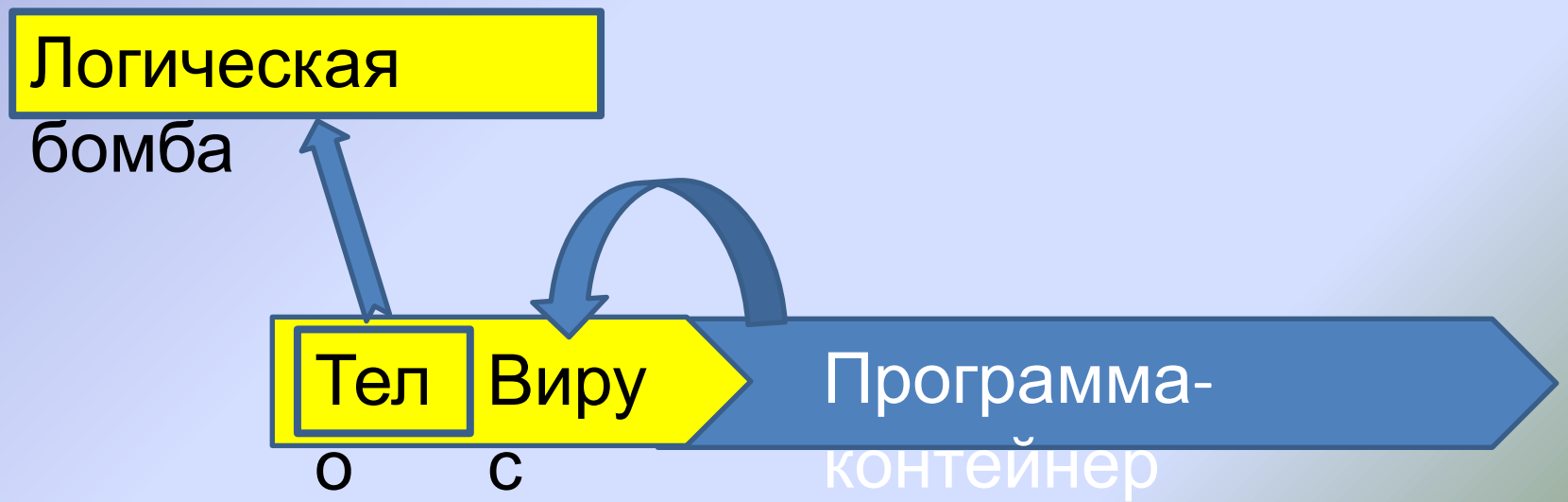
Черви

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



Троян

- Контейнер – полезная программа
- Тело трояна



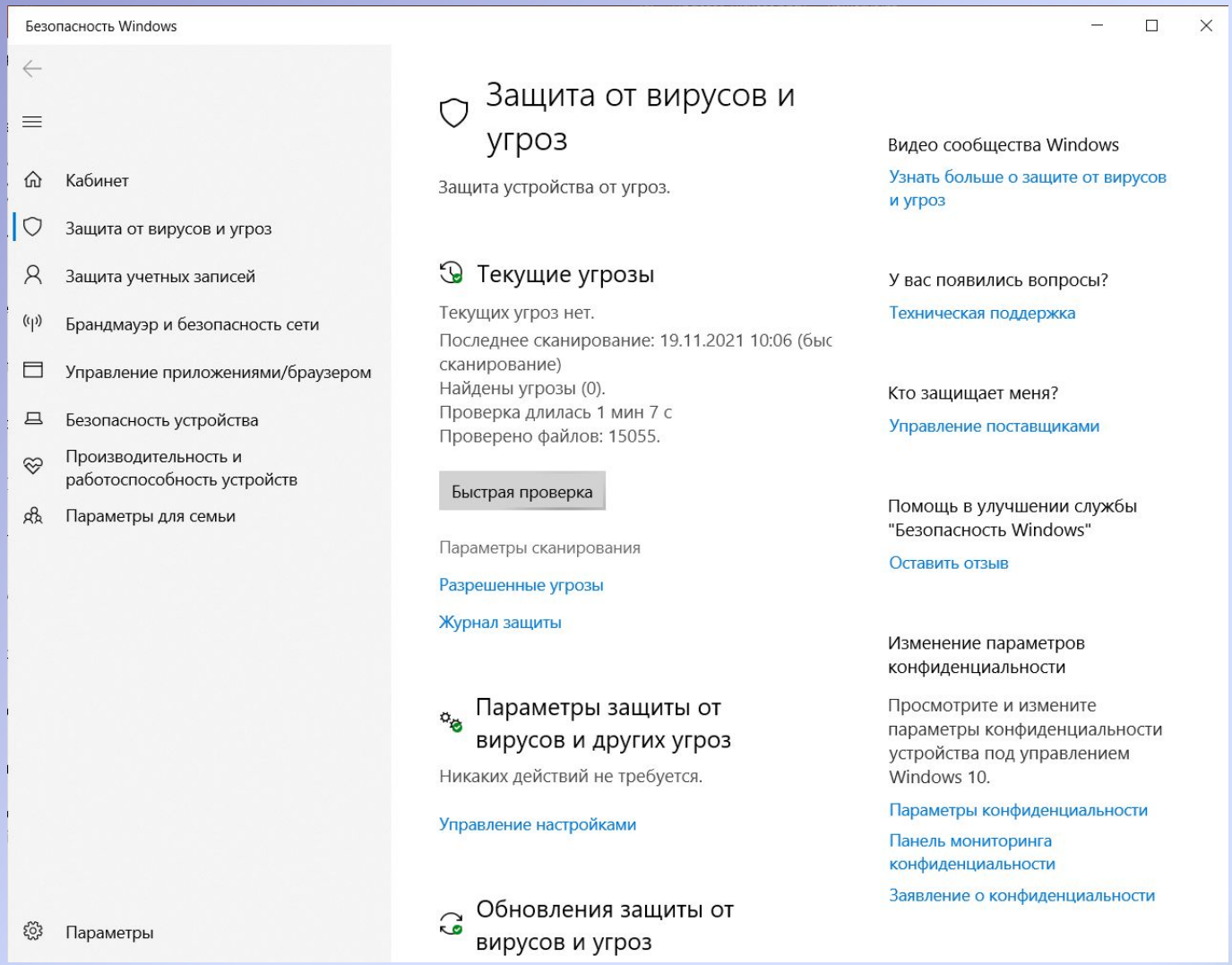
Root Kit

- Встраивается на уровне драйверов операционной системы
- Очень сложно обнаружить

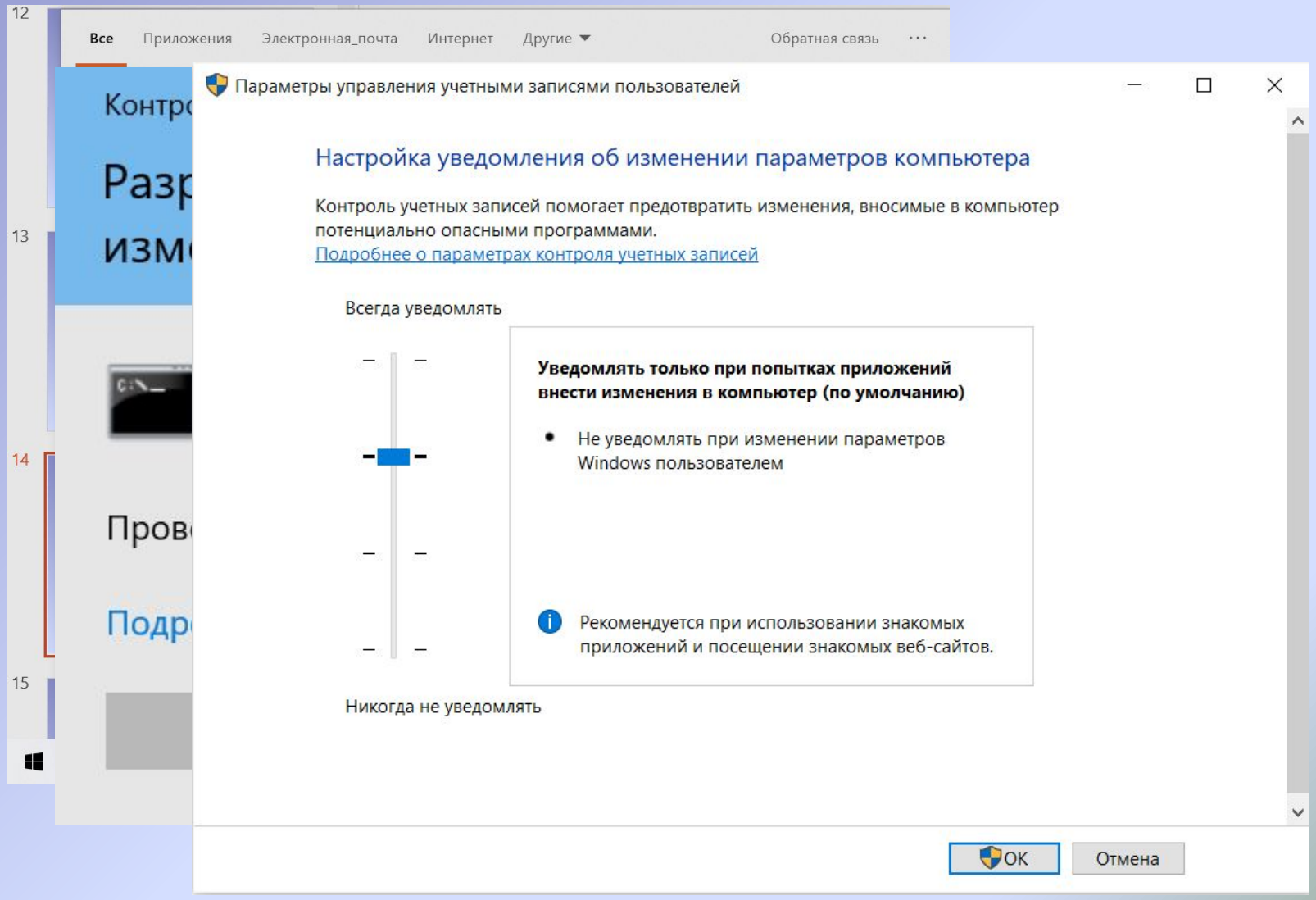
Методы обнаружения угроз ПО

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

Защита от вирусов и…



Контроль доступа (UAC)

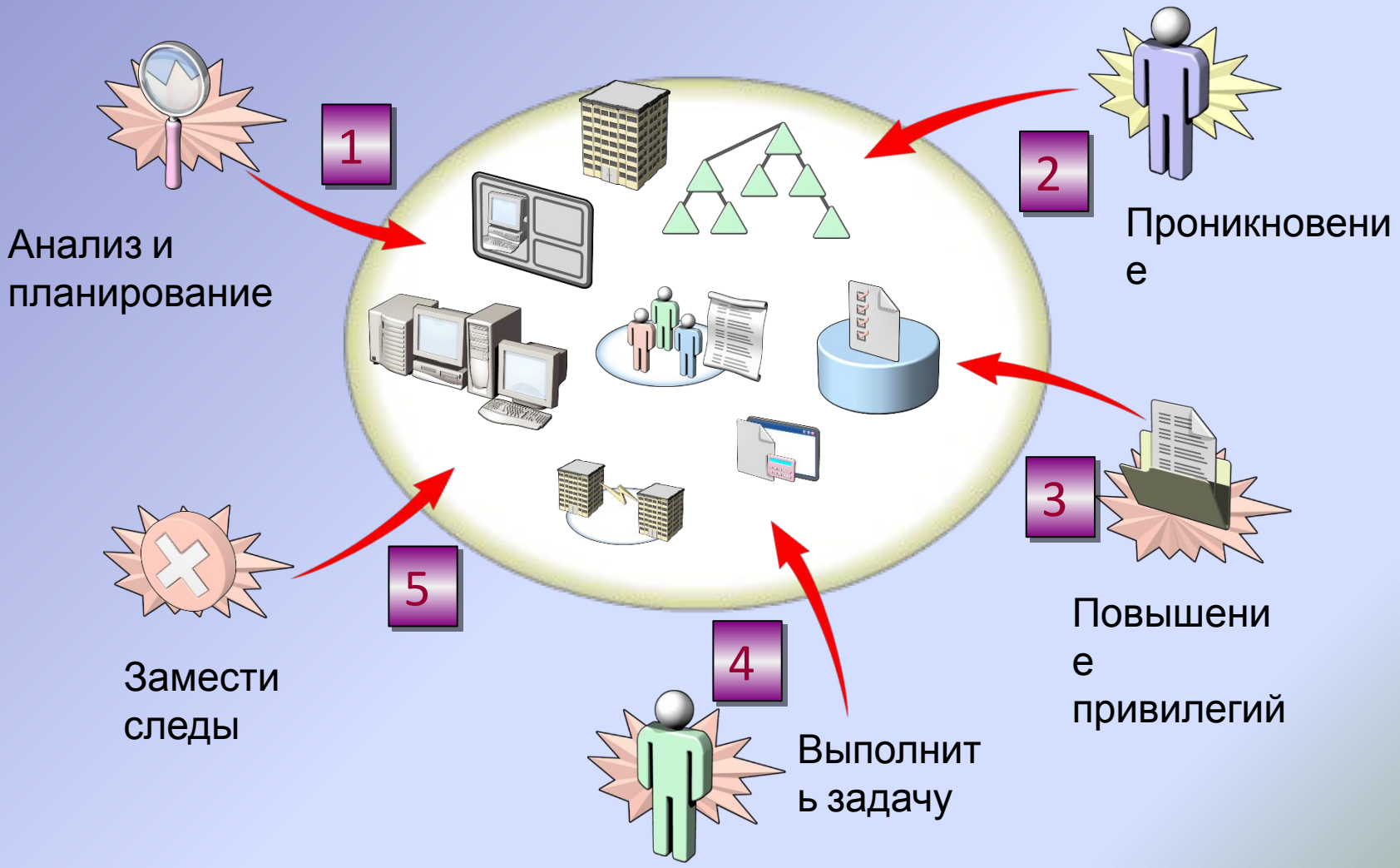


Обеспечение качества кода в ходе разработки

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
Spoofing	• Строгая аутентификация. • Не хранить секреты на виду. • Не передавать секреты открытым текстом.
Tampering	• Подписывать данные. • Использовать строгую аутентификацию • Использовать устойчивые протоколы.
Repudiation	• Аудит!!!. • Подписывать.
Information disclosure	• Использовать строгую аутентификацию. • Защищать коммуникации. • Не хранить секреты на виду.
Denial of service	• Использовать технологию контроля полосы трафика. • Контролировать входящий трафик.
Elevation of privilege	• Принцип минимальных привилегий.

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