

Служба каталога Active Directory (AD)

Горячев Александр Вадимович
Доцент кафедры
Информационной безопасности
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

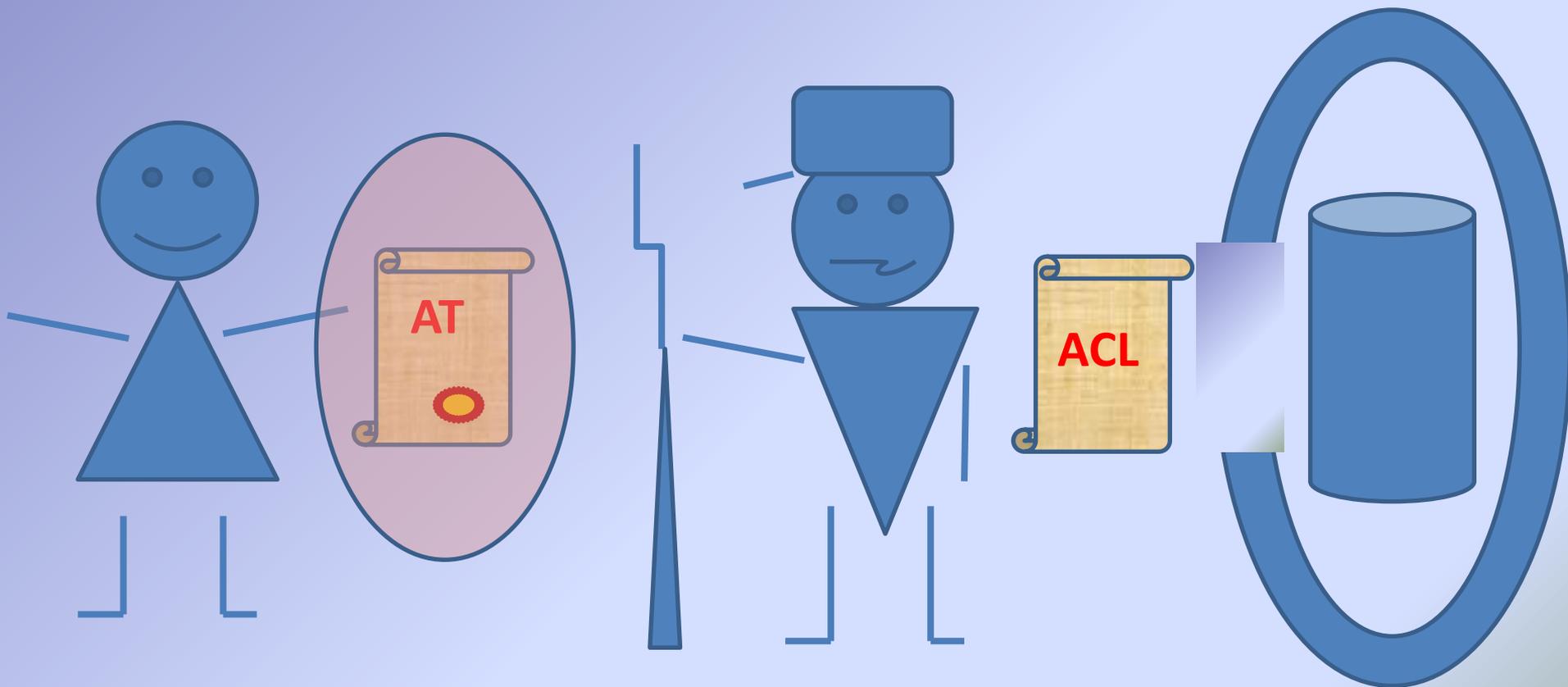
AD

Передача

Intranet Routing IPsec RMS NIDS-NIPS

Internet Firewall VPN NAP

Список контроля доступа



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

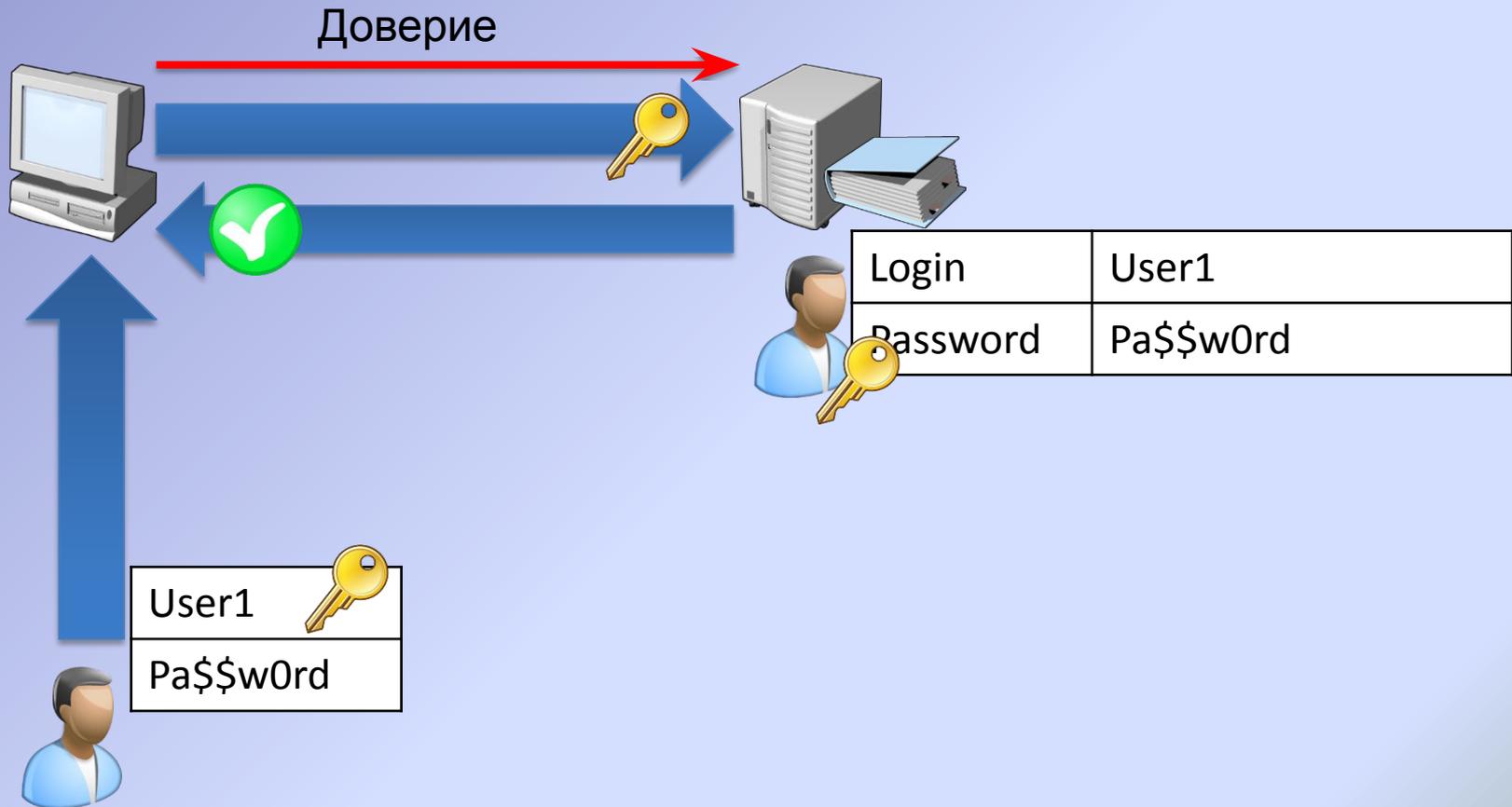
Учётные данные пользователя могут храниться
на локальном компьютере

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

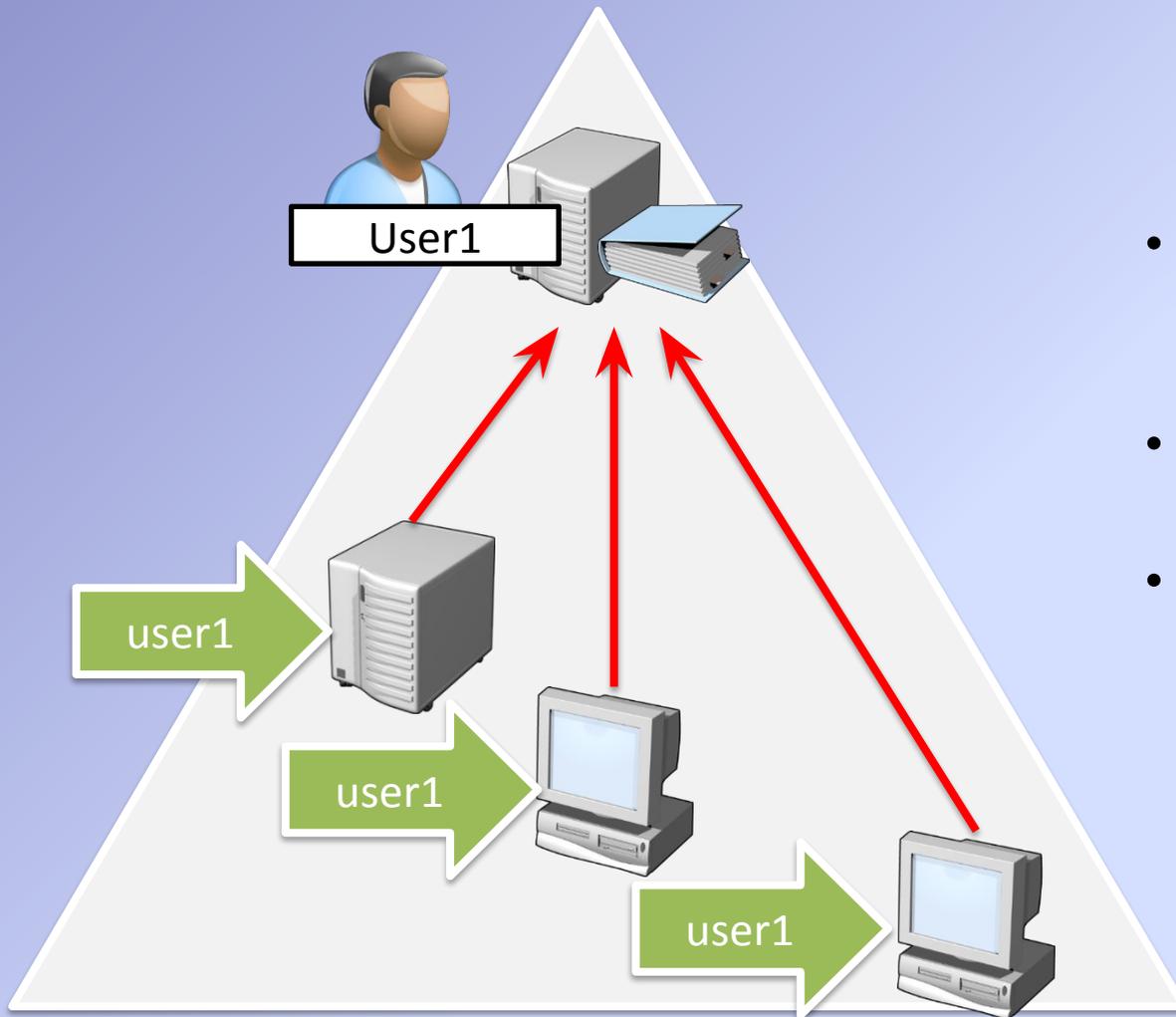
Решение: централизованное хранилище учётных данных

Служба каталогов Active Directory

Отношение доверия



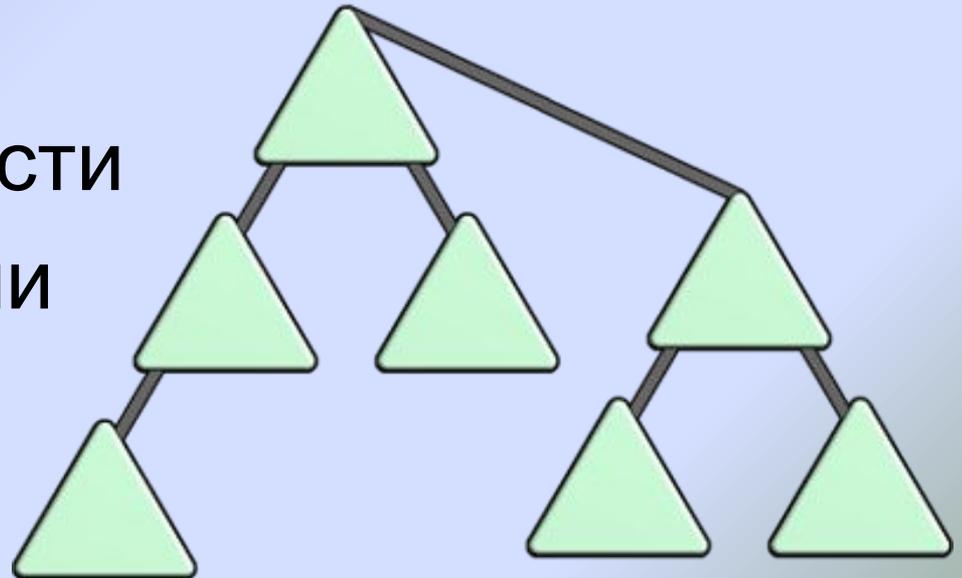
Домен Windows NT



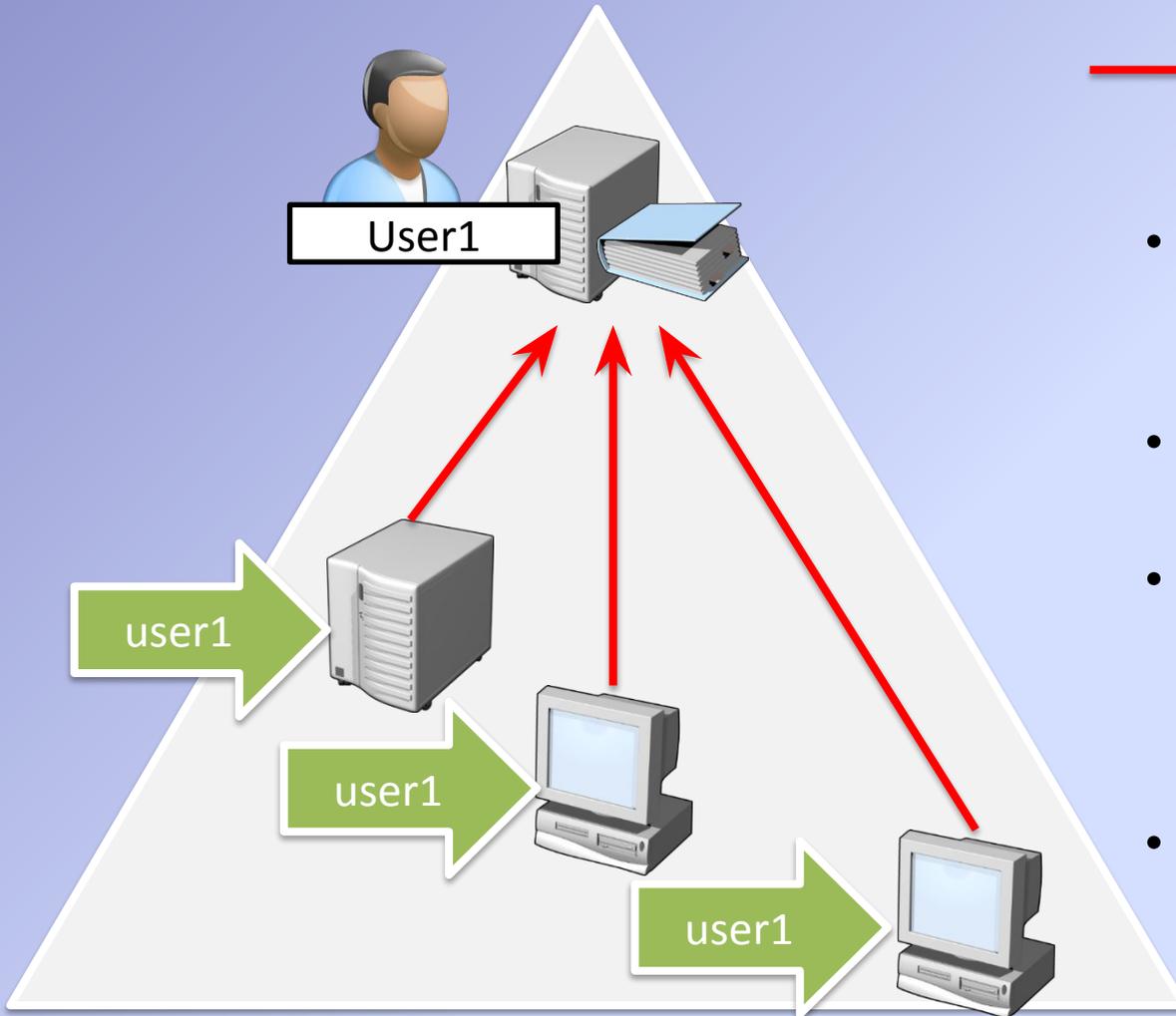
- Требует наличия как минимум одного контроллера домена (PDC)
- Граница репликации домена
- Доверенный источник учётных данных: любой доменный контроллер (PDC и BDC) может провести аутентификацию в домене

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

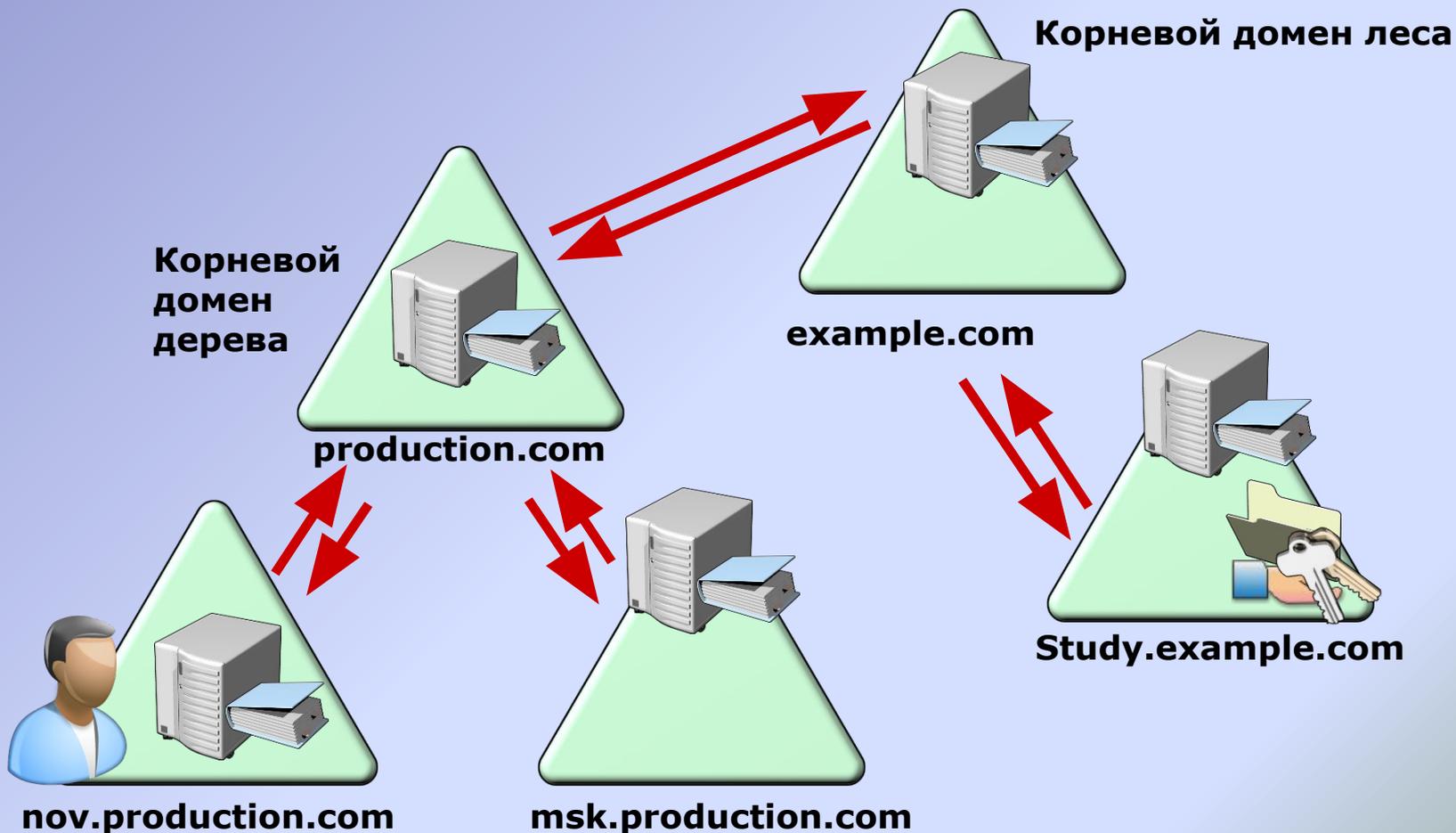
- Требует наличия как минимум одного контроллера домена
- Граница репликации доменного раздела
- Доверенный источник учётных данных: любой DC может провести аутентификацию в домене
- Граница применения политик

Подразделения

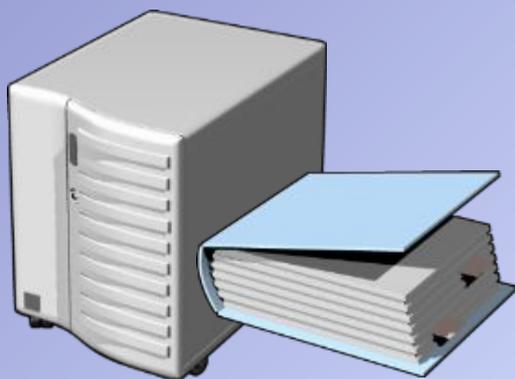
- Объекты
 - Пользователи
 - Компьютеры
- Подразделения
 - Контейнеры для группировки объектов в домене
 - Подразделения создаются:
 - Для делегирования разрешений
 - Для назначения групповых политик



Доверительные отношения в лесу Active Directory



Роль контроллера домена при аутентификации



Хранилище учётных данных

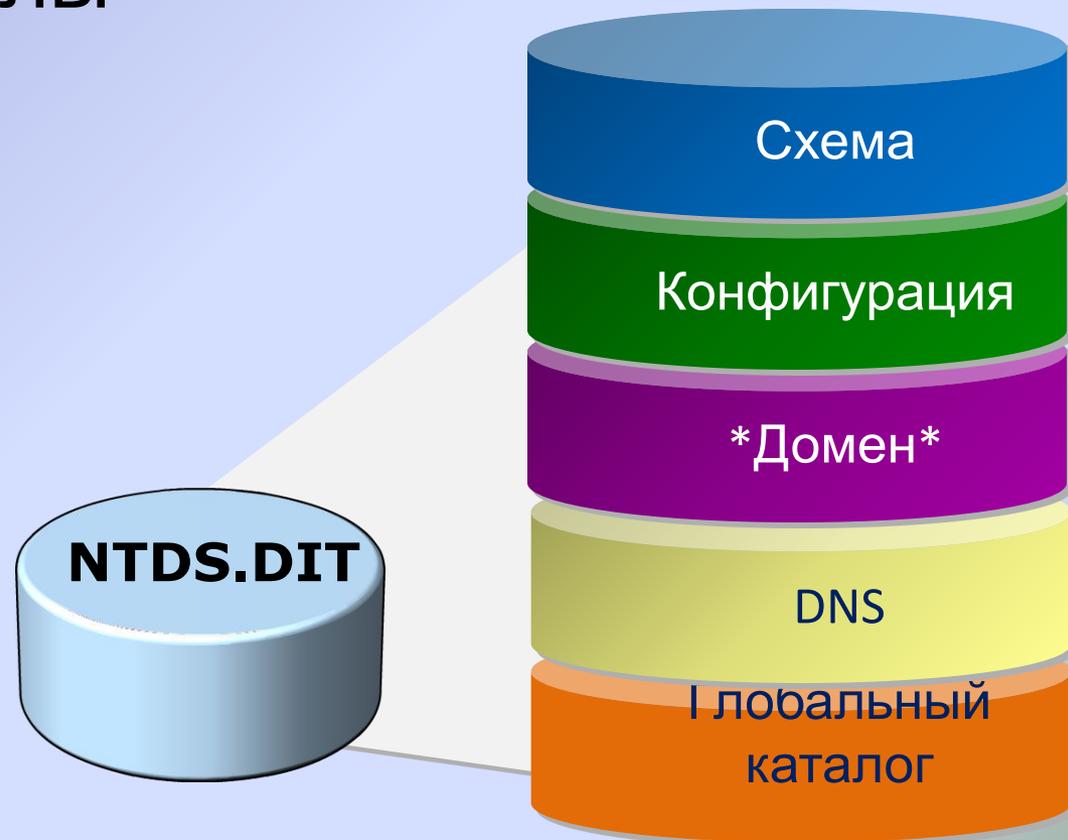
Login	User1	User2
Password	Pa\$\$w0rd	Pa\$\$word2



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 быстра

- Репликацией между сайтами можно управлять

- Локализация служб

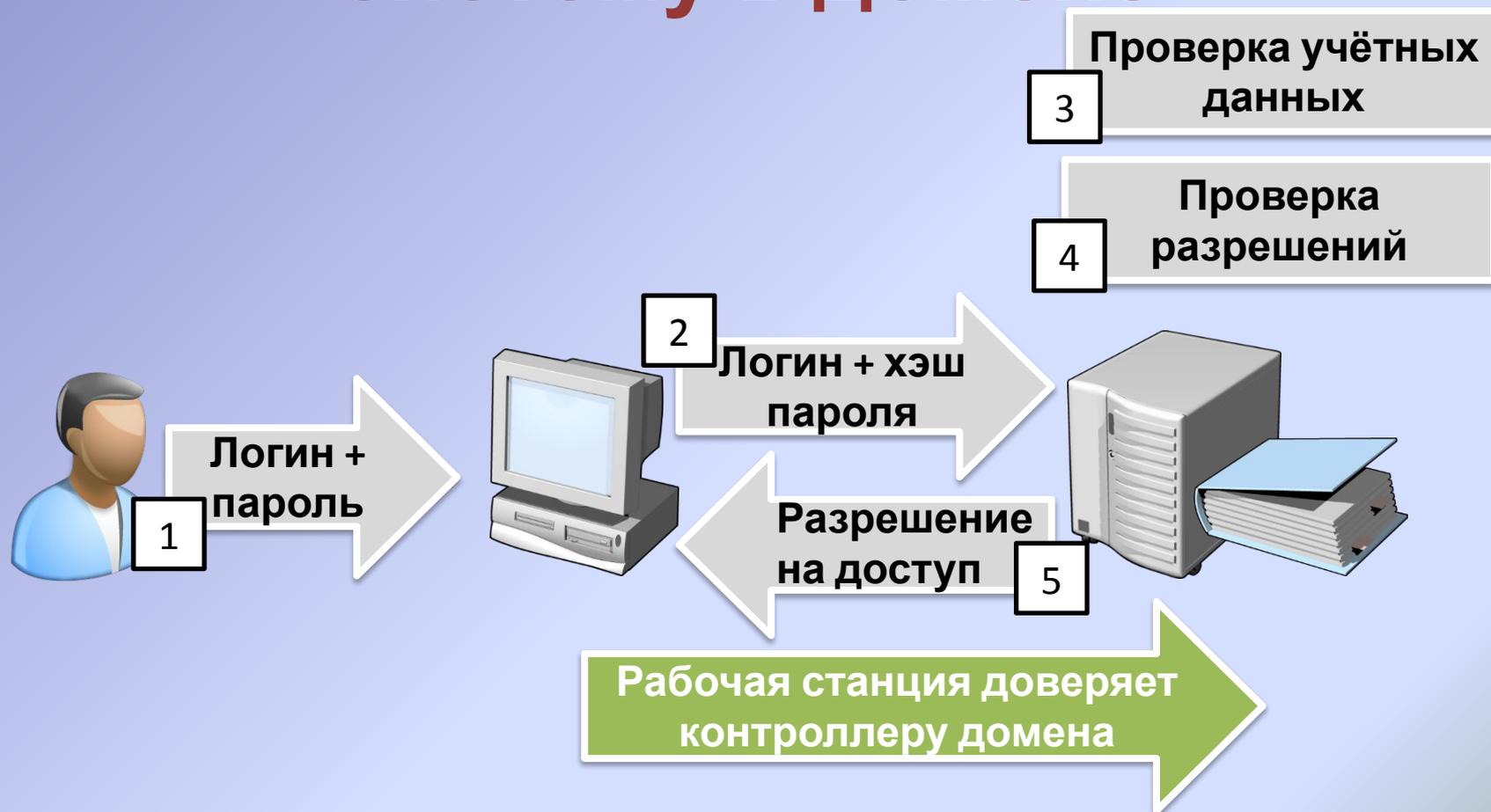
- Вход в систему на ближайшем контроллере



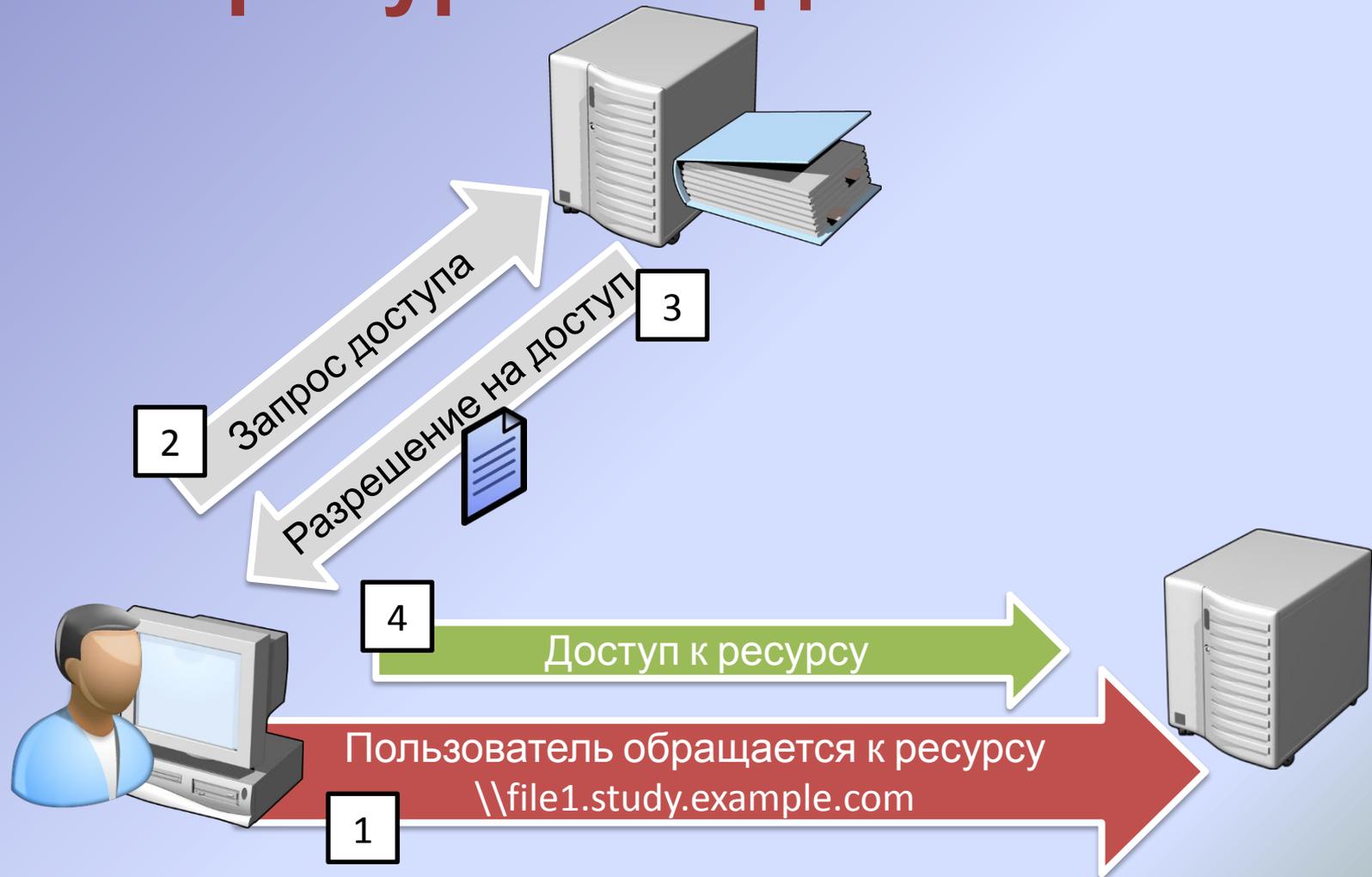
Учётные записи пользователей

- **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

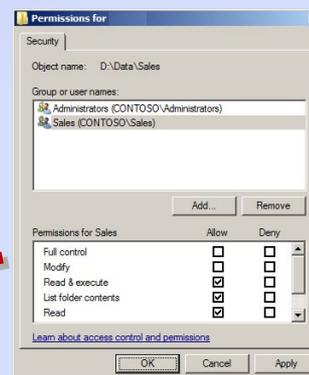
Пётр Петров

Василий Васильев

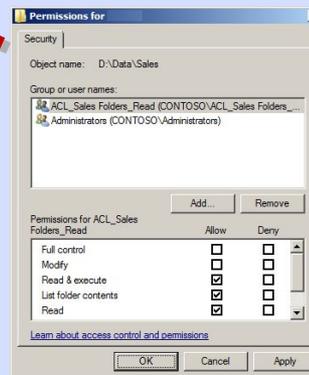
Sales

Auditors

ACL_Sales_read



SalesDocs



SalesShare

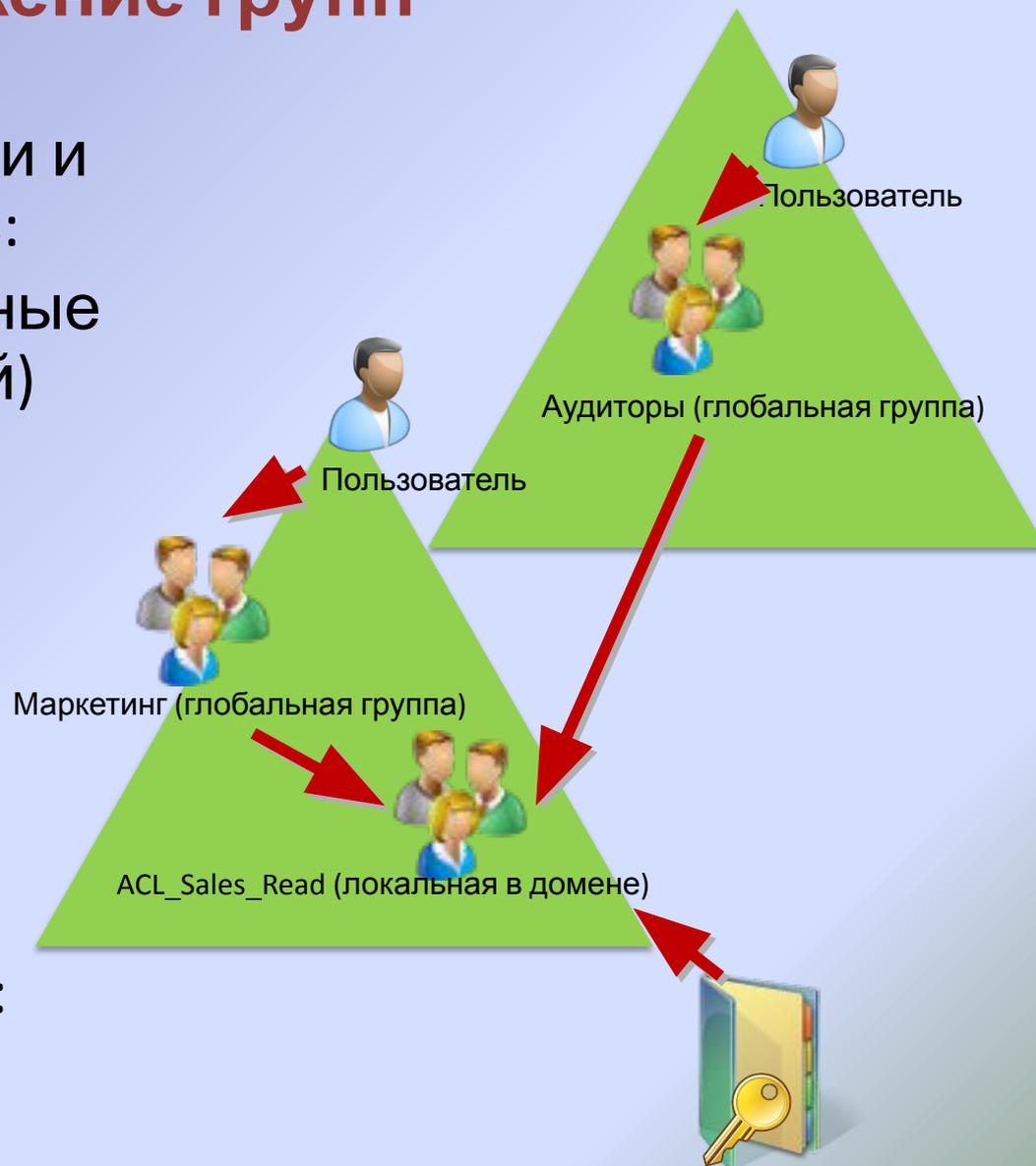
Диапазоны применения групп

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



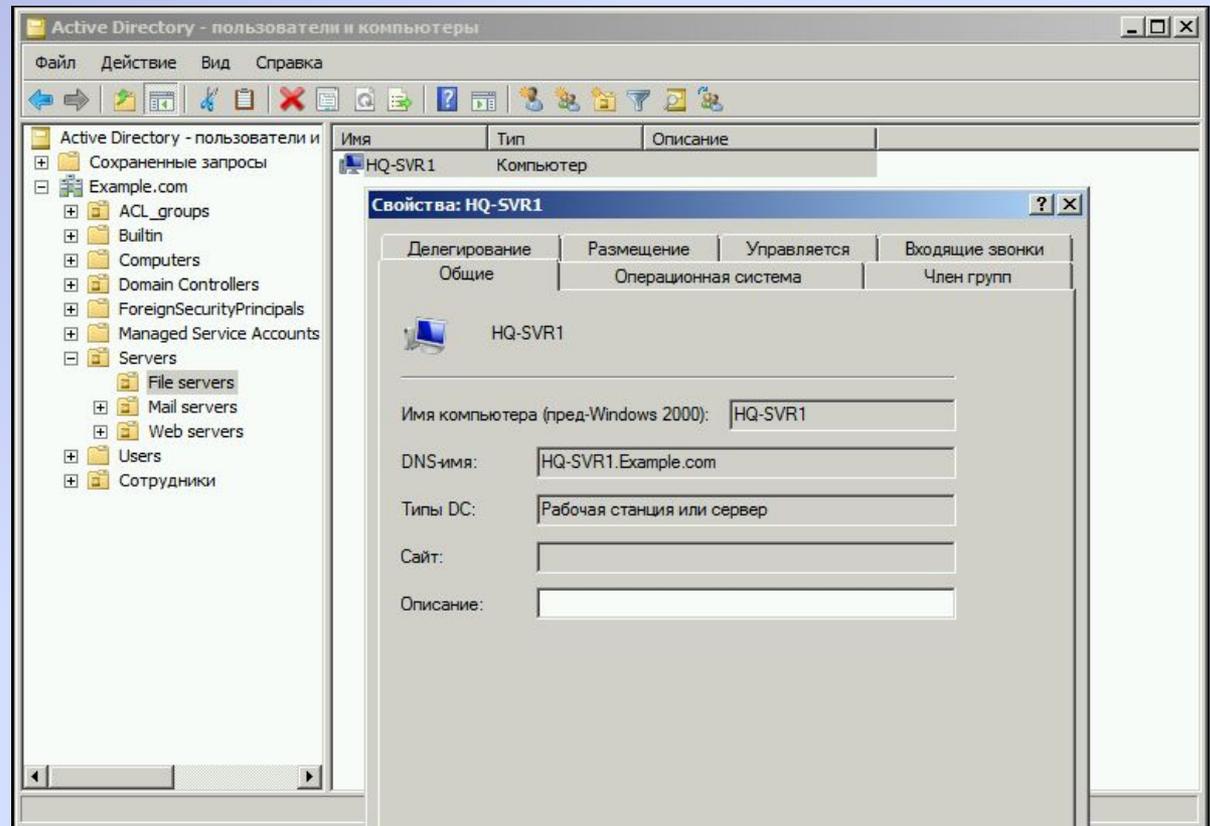
Группы безопасности

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

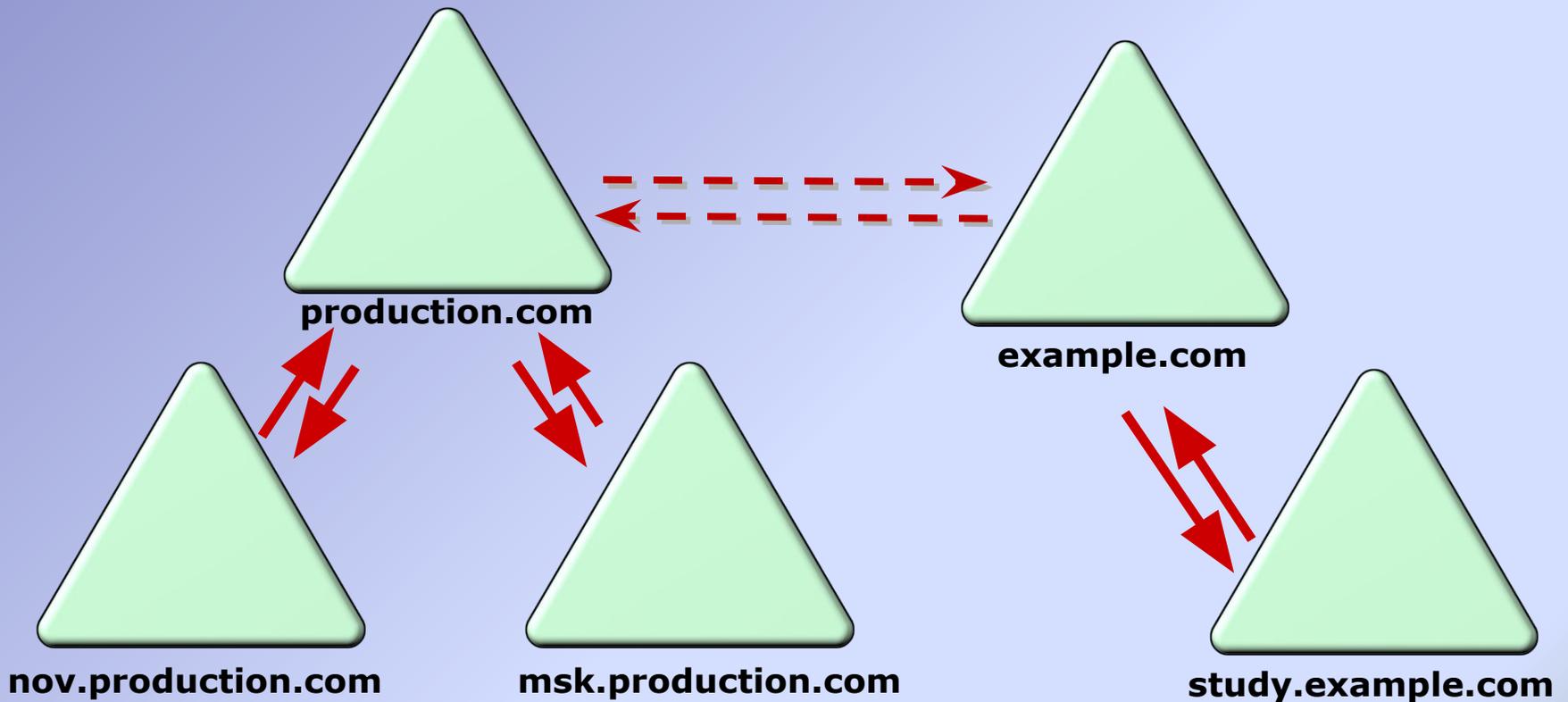


Учётные записи компьютеров

- 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 Autentication HIDS-HIPS

PKI

AD

Передача

Intranet Routing IPsec RMS NIDS-NIPS

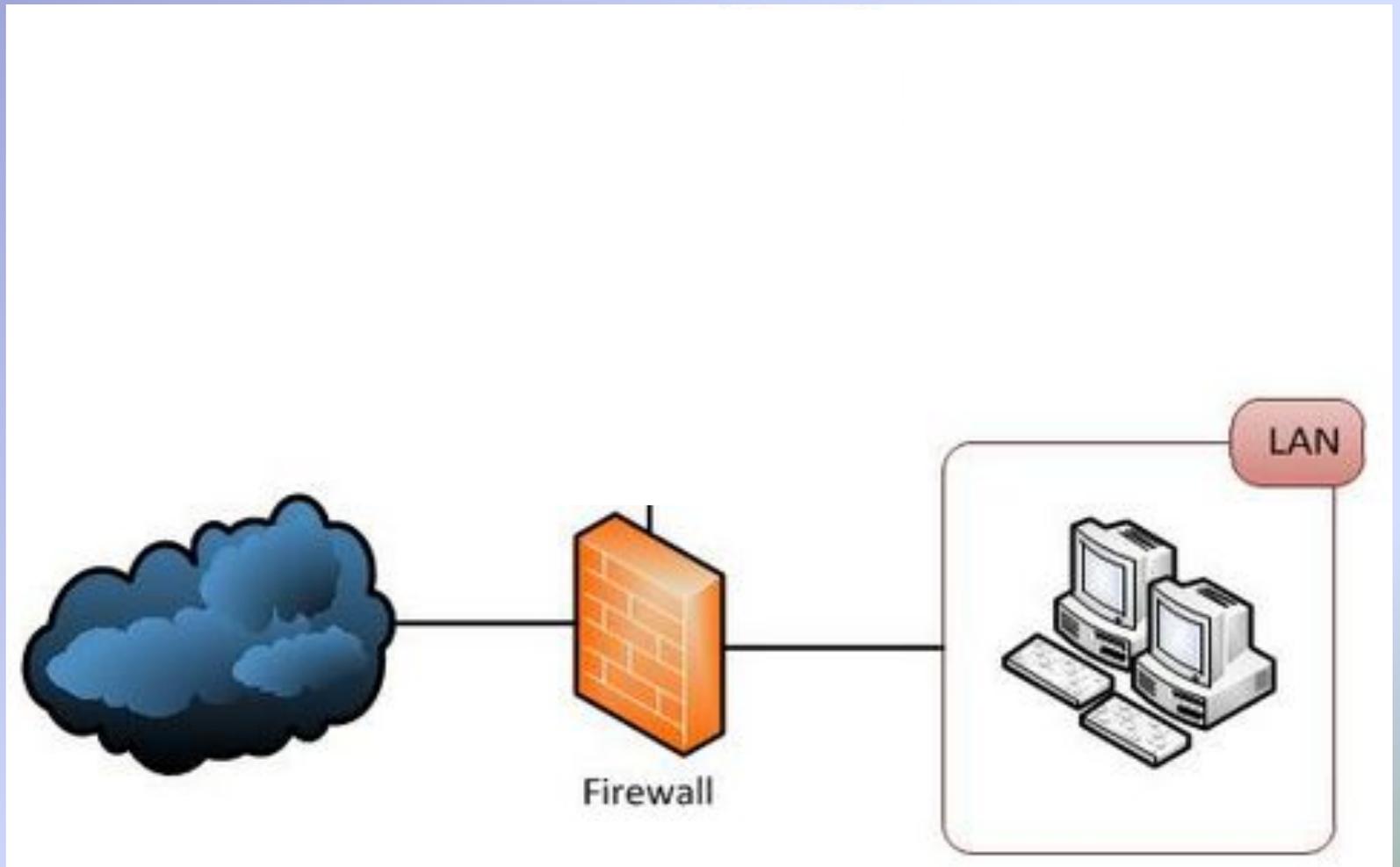
Internet **Firewall** VPN NAP

Набор технологий

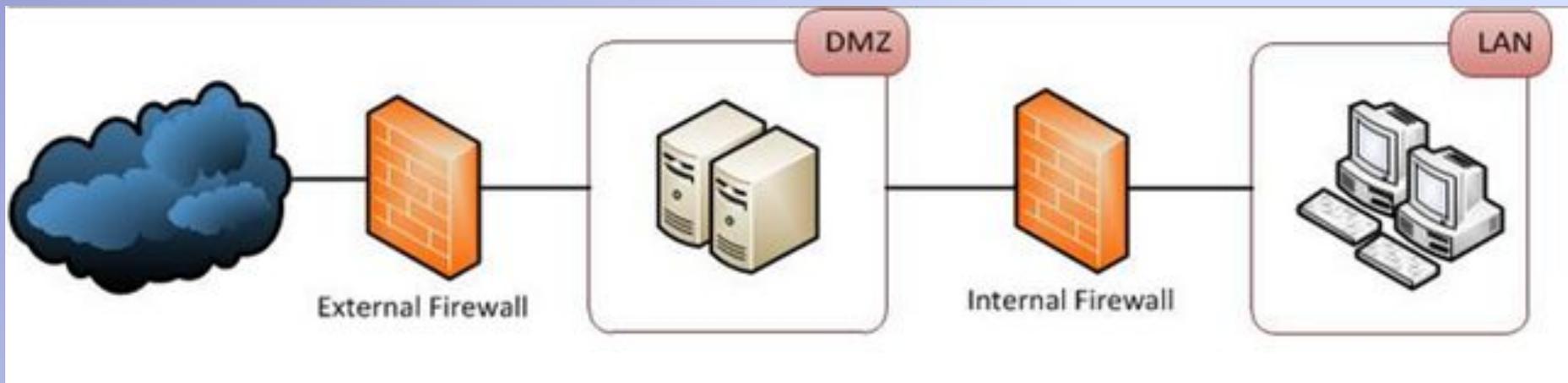
- Proxy 7
- VPN 6
- Контентная фильтрация 5
- Аутентификация 4
- Трансляция сетевых адресов 3
- Пакетные фильтры 2

1

Простые конфигурации



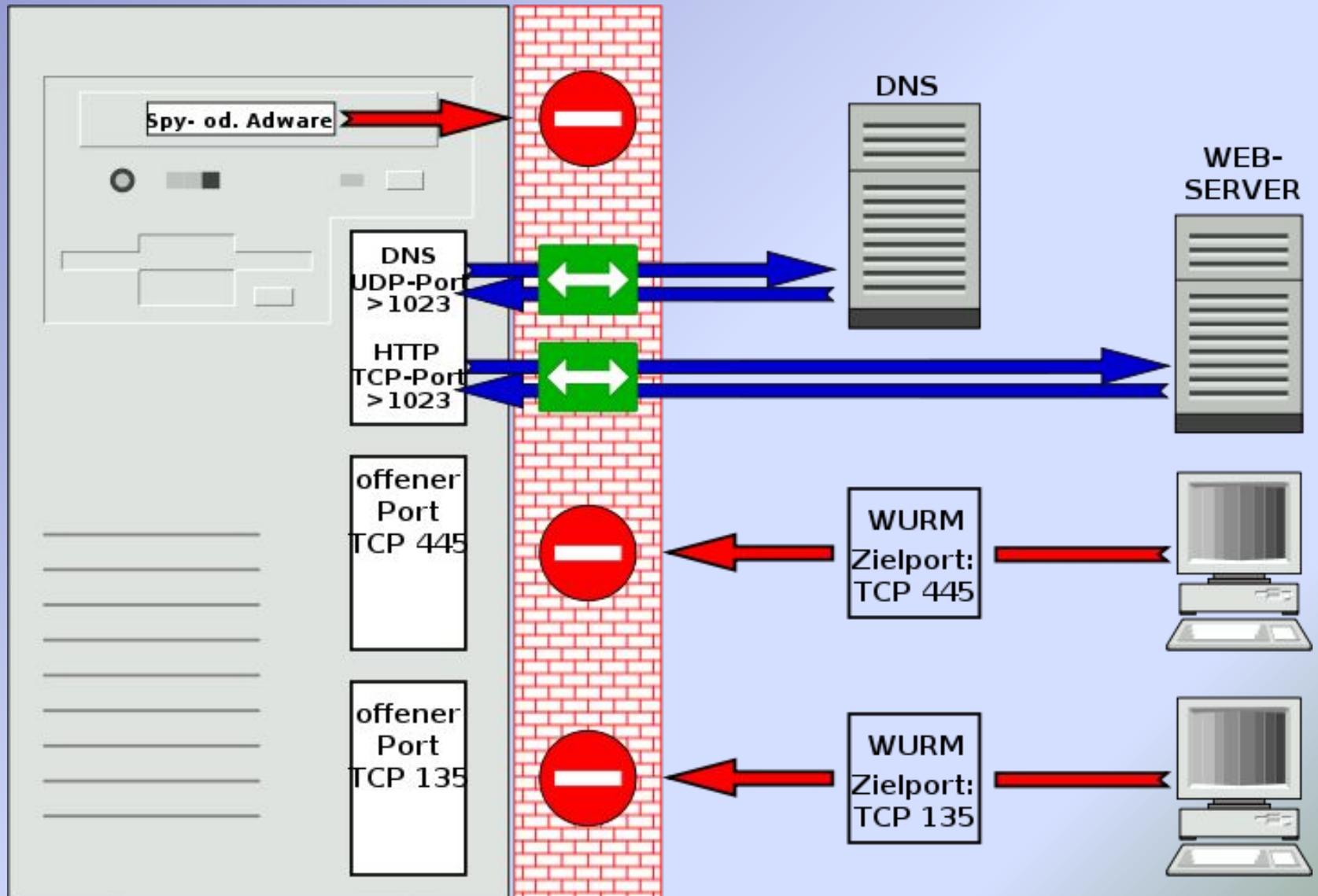
Демилитаризованная зона (сеть периметра)



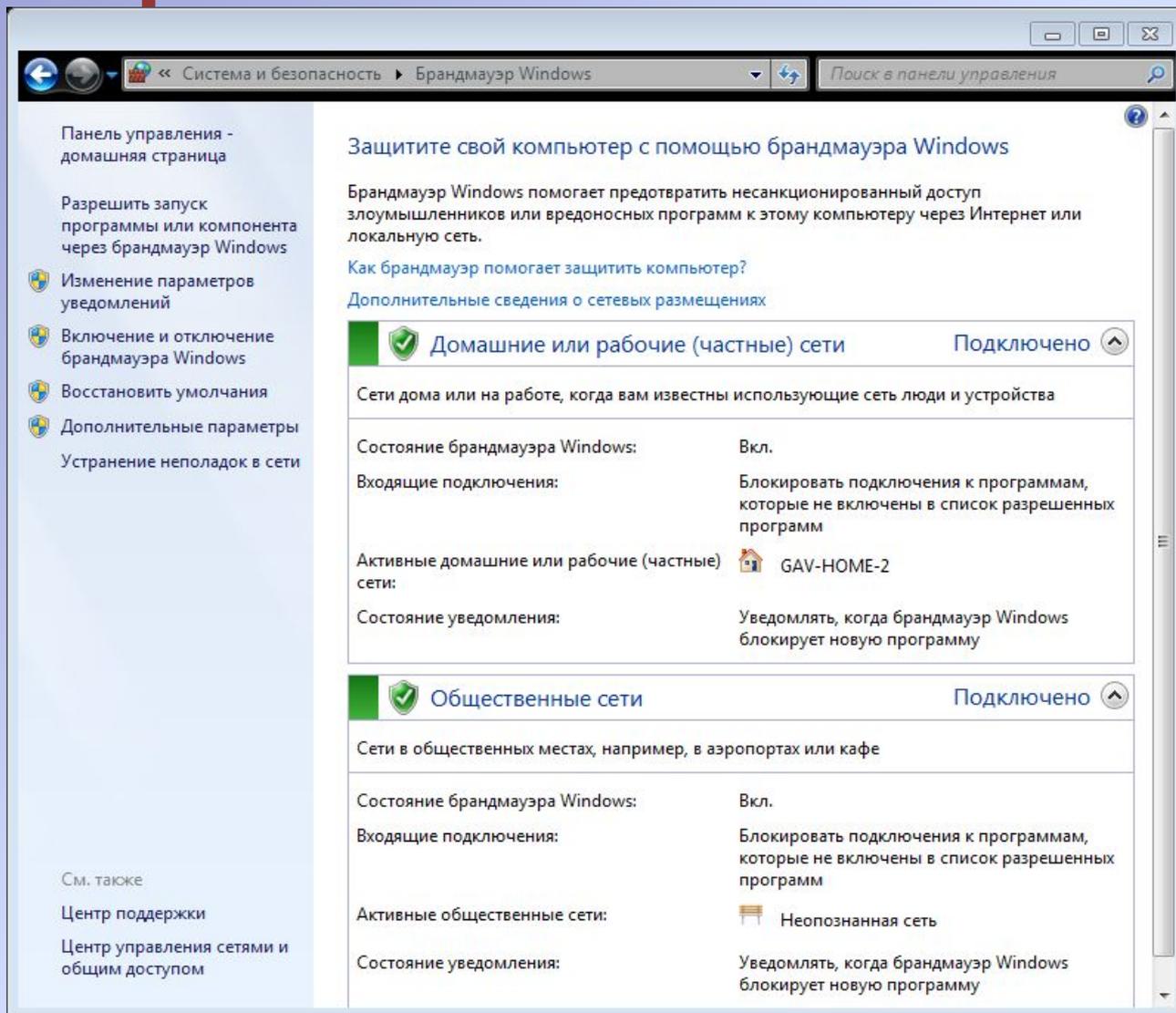
Windows Firewall?



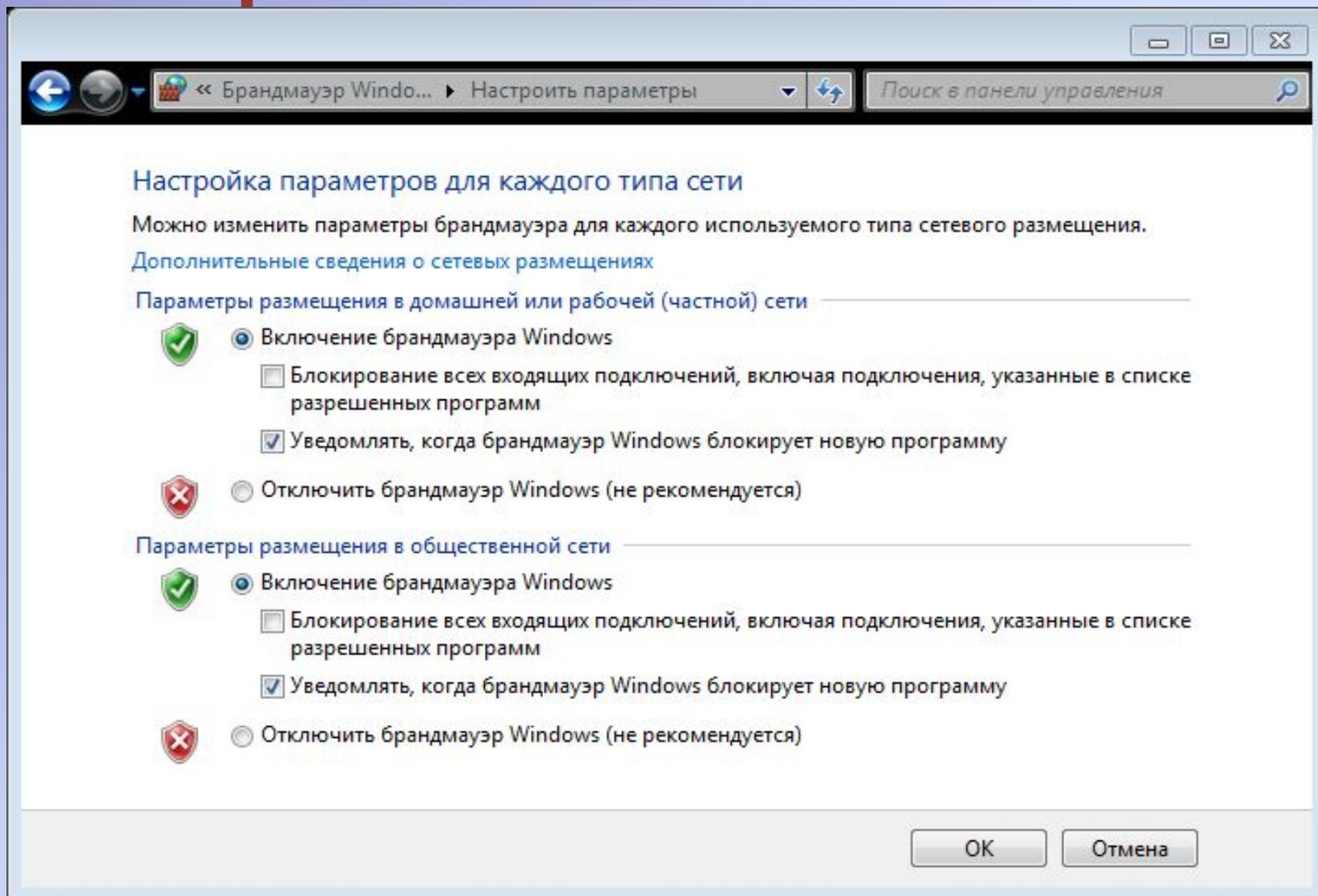
Персональный брандмауэр



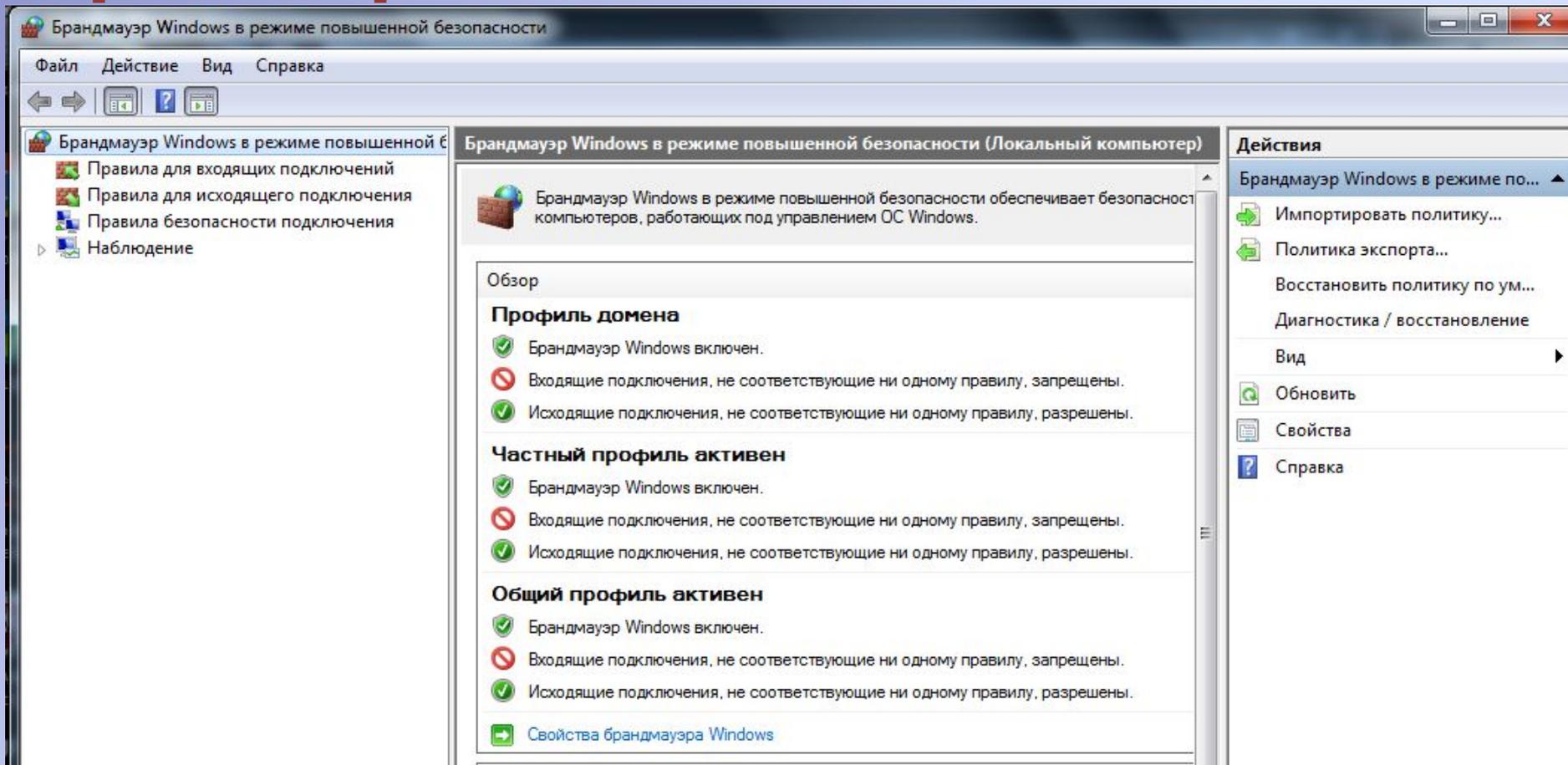
Windows Firewall с расширенными возможностями



Windows Firewall с расширенными возможностями



Windows Firewall с расширенными возможностями



Windows Firewall с расширенными возможностями

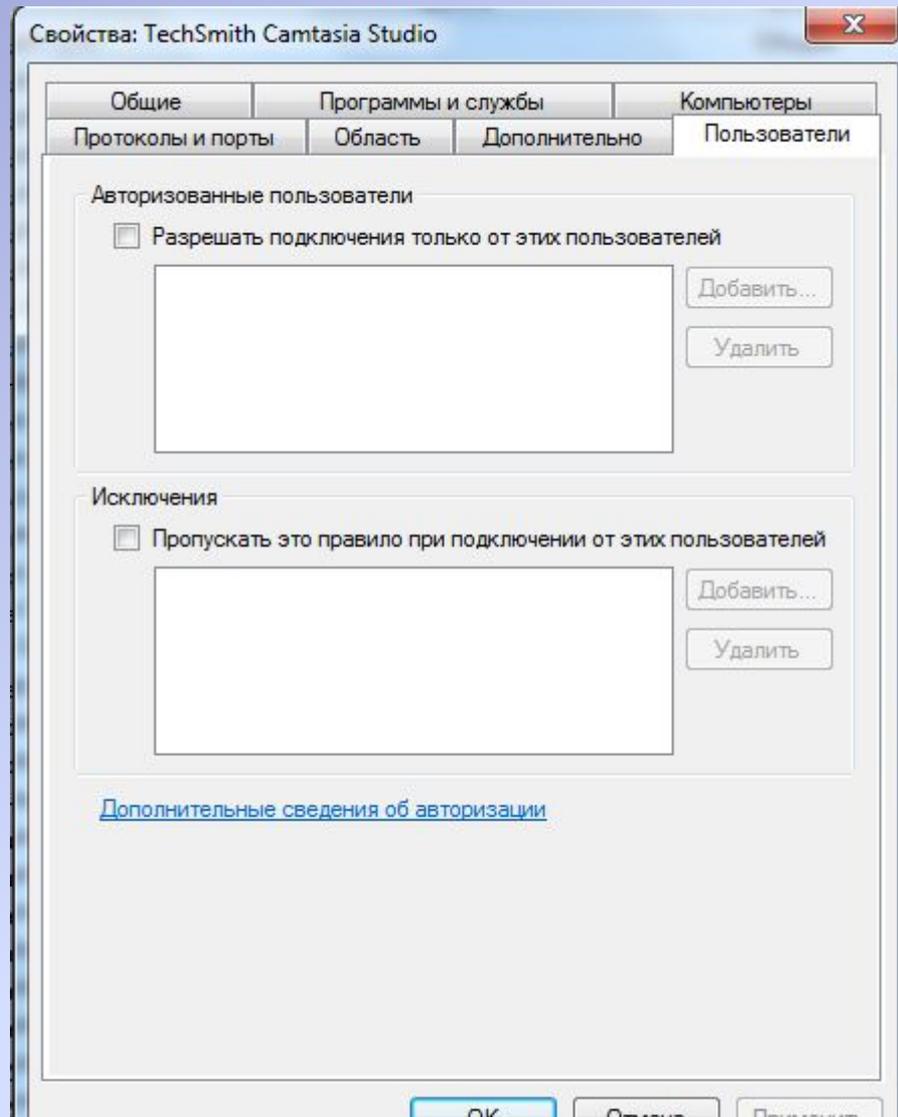
The screenshot displays the Windows Firewall Advanced Security console. The left sidebar shows the navigation pane with 'Правила для входящих подключений' (Inbound Rules) selected. The main area shows a list of rules with columns for Name, Group, and Profile. The right pane shows the 'Actions' (Действия) menu.

Имя	Группа	Профиль
Microsoft Lync		Общие
Microsoft Lync		Частный
Microsoft Lync		Частный
Microsoft Lync		Общие
Microsoft Lync Ucmapi		Частный
Microsoft Lync Ucmapi		Частный
Microsoft Lync Ucmapi		Общие
Microsoft Lync Ucmapi		Общие
Microsoft Office Outlook		Частный
TechSmith Camtasia Studio		Все
VMware Authd Service		Домен
VMware Authd Service (private)		Частный
Обнаружение кэширующих узлов BranchCache - обнаружен...	BranchCache - обнаружен...	Все
Получение содержимого BranchCache - получение ...	BranchCache - получение ...	Все
Сервер размещенного кэша BranchCache - сервер разм...	BranchCache - сервер разм...	Все
Google Chrome (mDNS-In)	Google Chrome	Все
Secure Socket Tunneling Protocol (SSTP-...	Secure Socket Tunneling Pr...	Все
Адаптер прослушивателя Windows Communication F...	Windows Communication F...	Все
Беспроводные переносные устройства...	Беспроводные переносны...	Все
Беспроводные переносные устройства...	Беспроводные переносны...	Все
Дистанционное управление рабочим с...	Дистанционное управлени...	Все

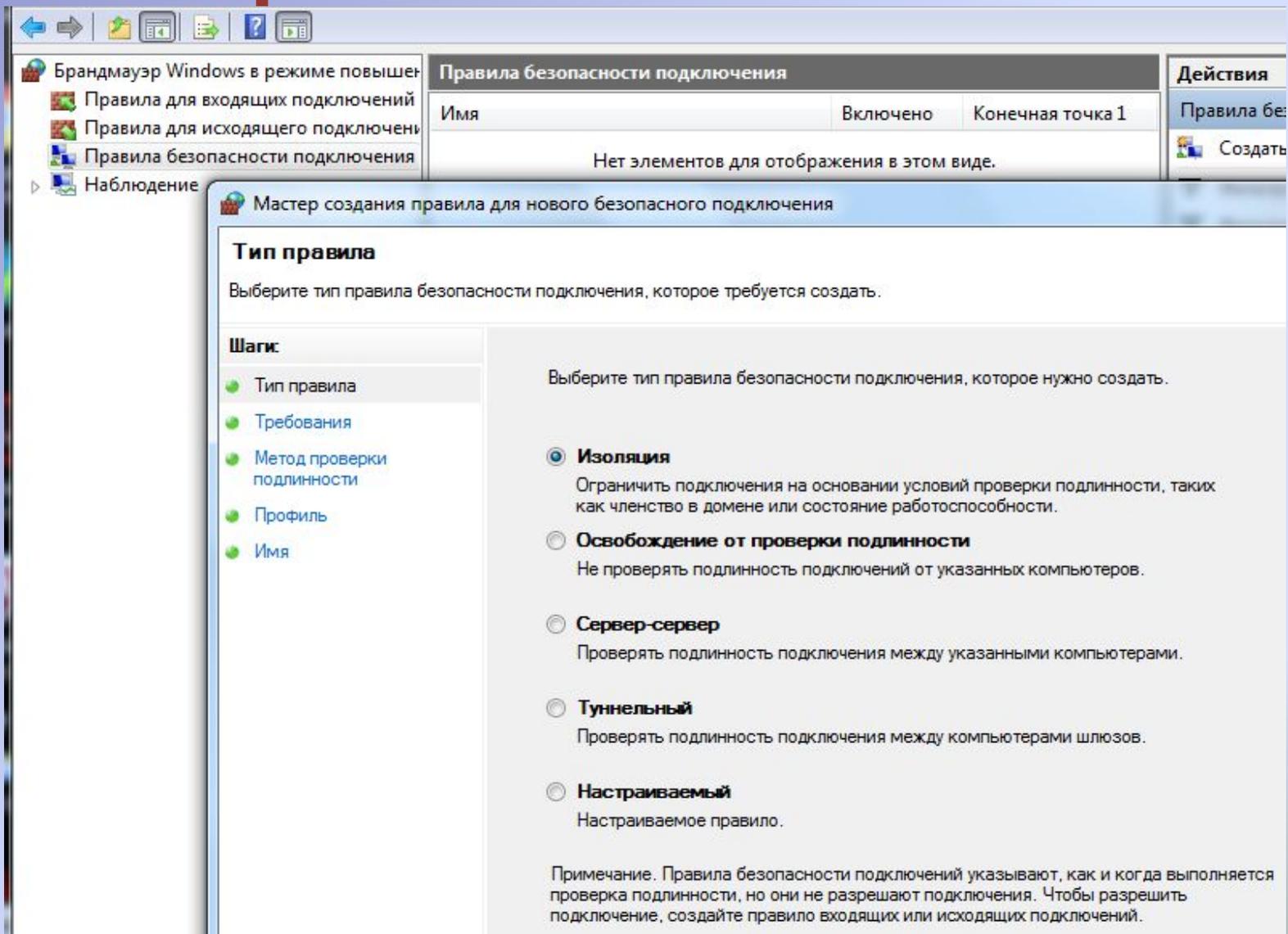
Действия

- Правила для входящих подключений
- Создать правило...
- Фильтровать по профилю
- Фильтровать по состоянию
- Фильтровать по группе
- Вид
- Обновить
- Экспортировать список...
- Справка

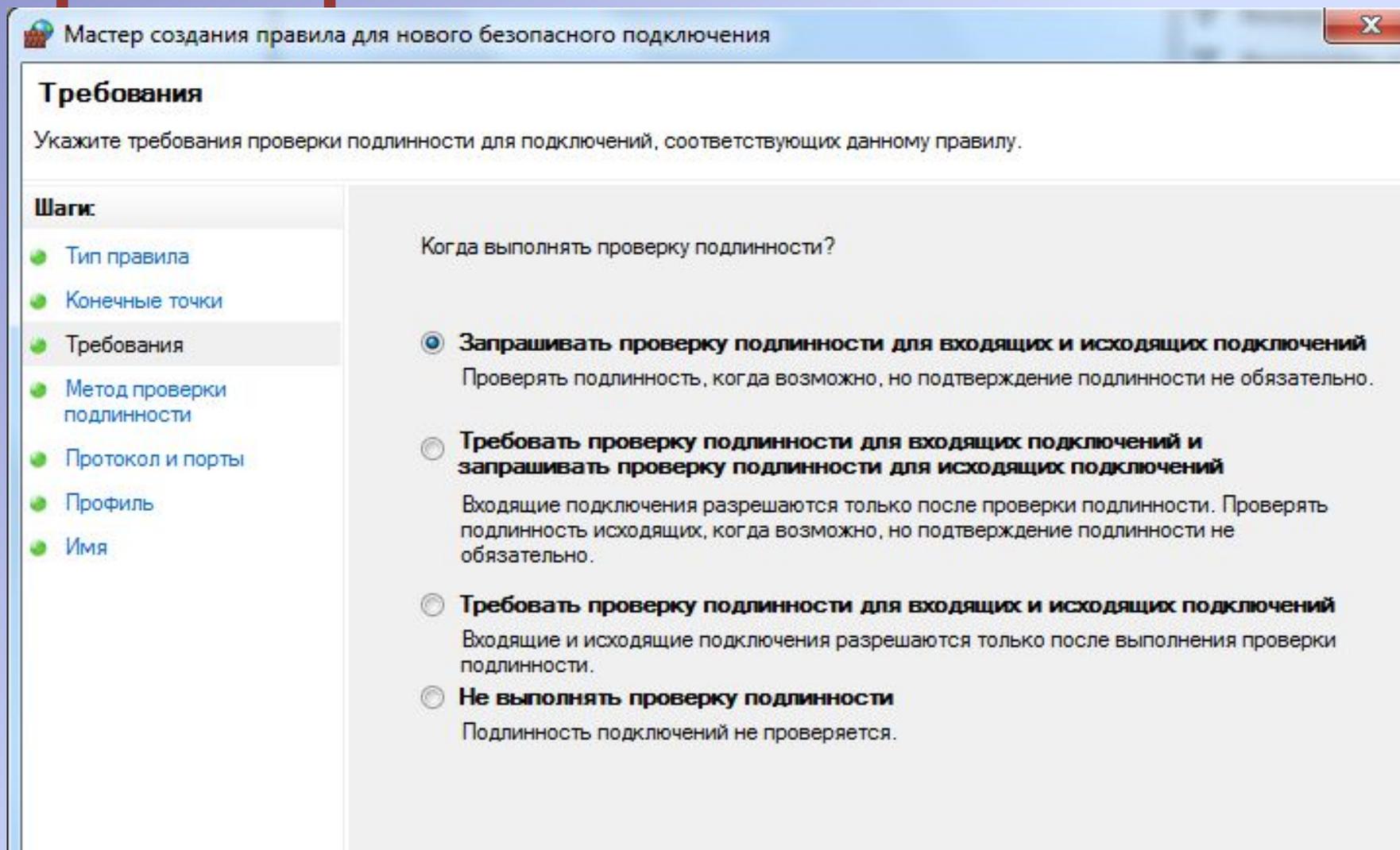
Windows Firewall с расширенными возможностями



Windows Firewall с расширенными возможностями



Windows Firewall с расширенными возможностями



Windows Firewall с расширенными возможностями

Мастер создания правила для нового безопасного подключения

Метод проверки подлинности

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

Шаги:

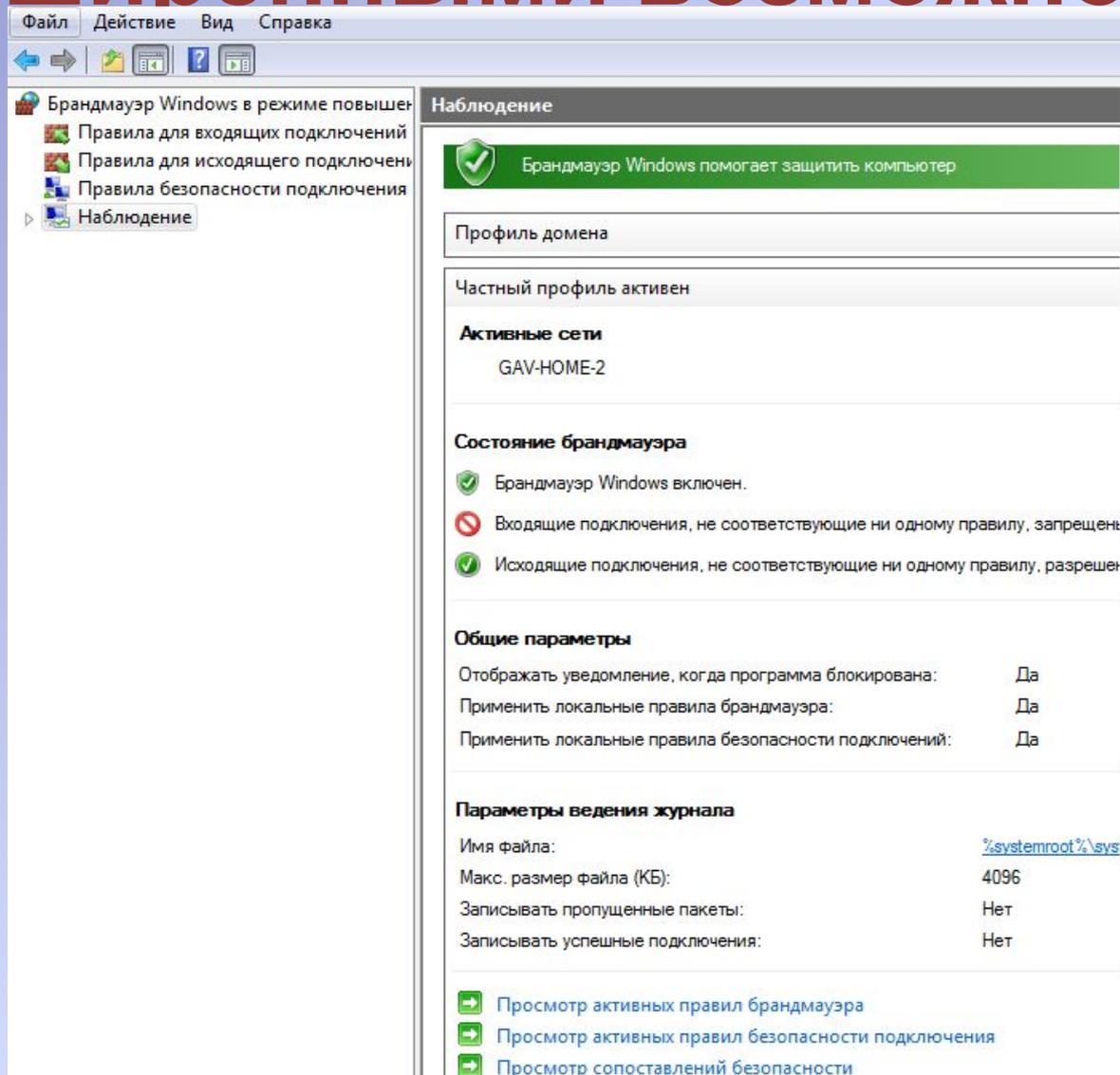
- Тип правила
- Конечные точки
- Требования
- Метод проверки подлинности
- Протокол и порты
- Профиль
- Имя

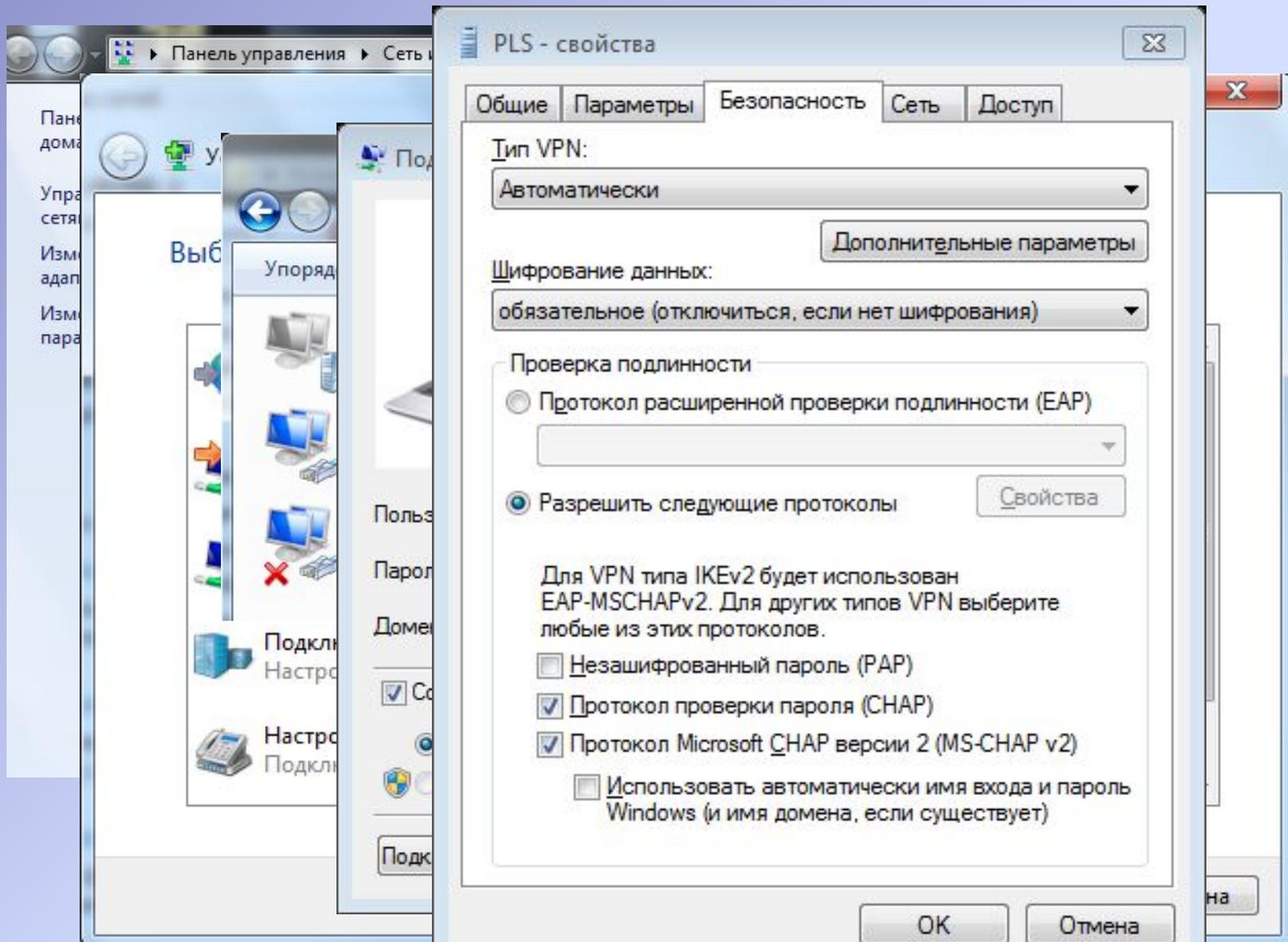
Выберите метод проверки подлинности.

- 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





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:

```

Имя компьютера . . . . . : Gav-WorkPlace
Основной DNS-суффикс . . . . . :
Тип узла. . . . . :
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. . . . . :
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
DNS-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

```

```

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

```

Адаптер беспроводной локальной сети Беспроводное сетевое соединение:

```

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
DNS-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

```

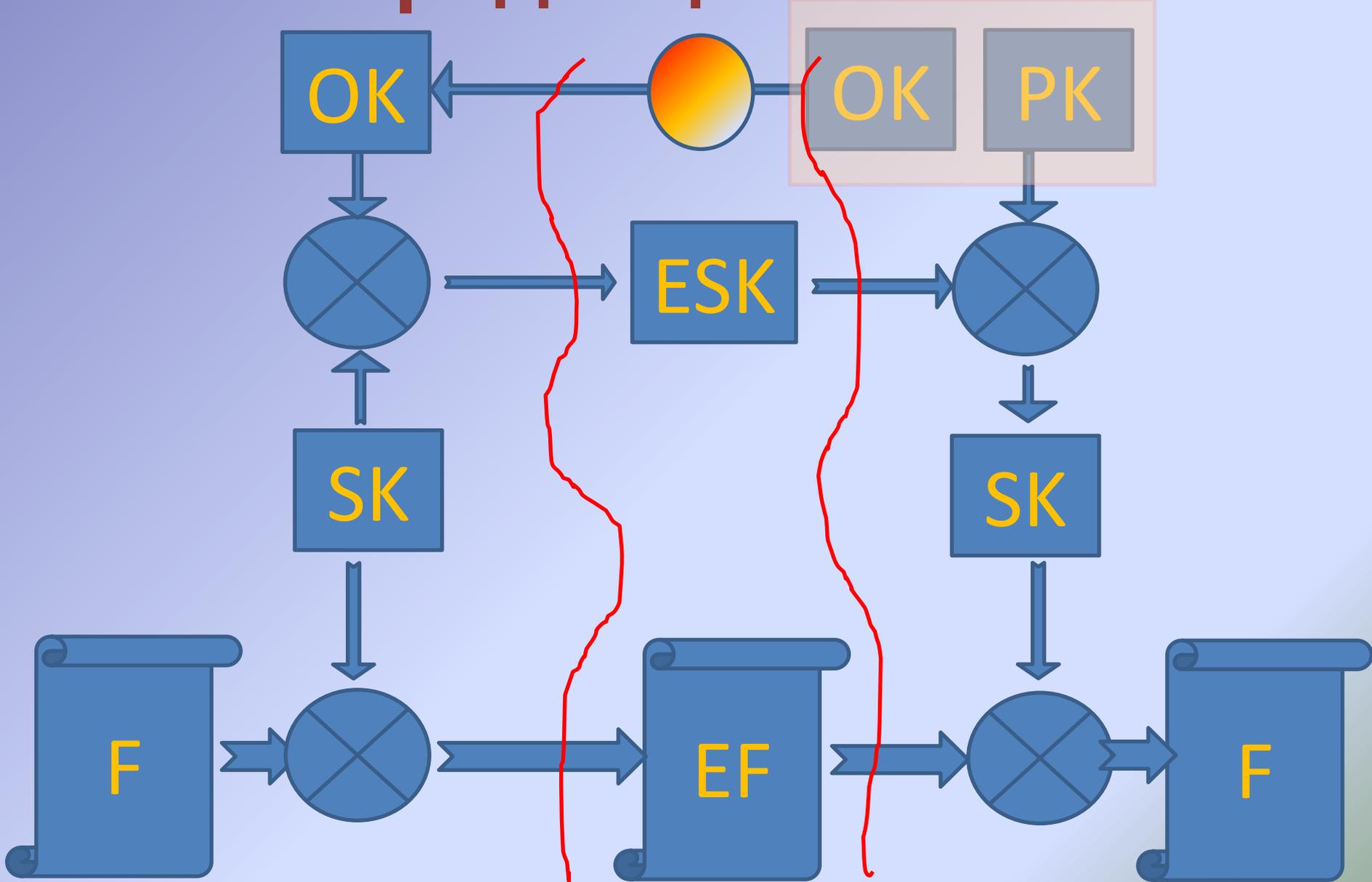
Ethernet adapter VMware Network Adapter VMnet1:

```

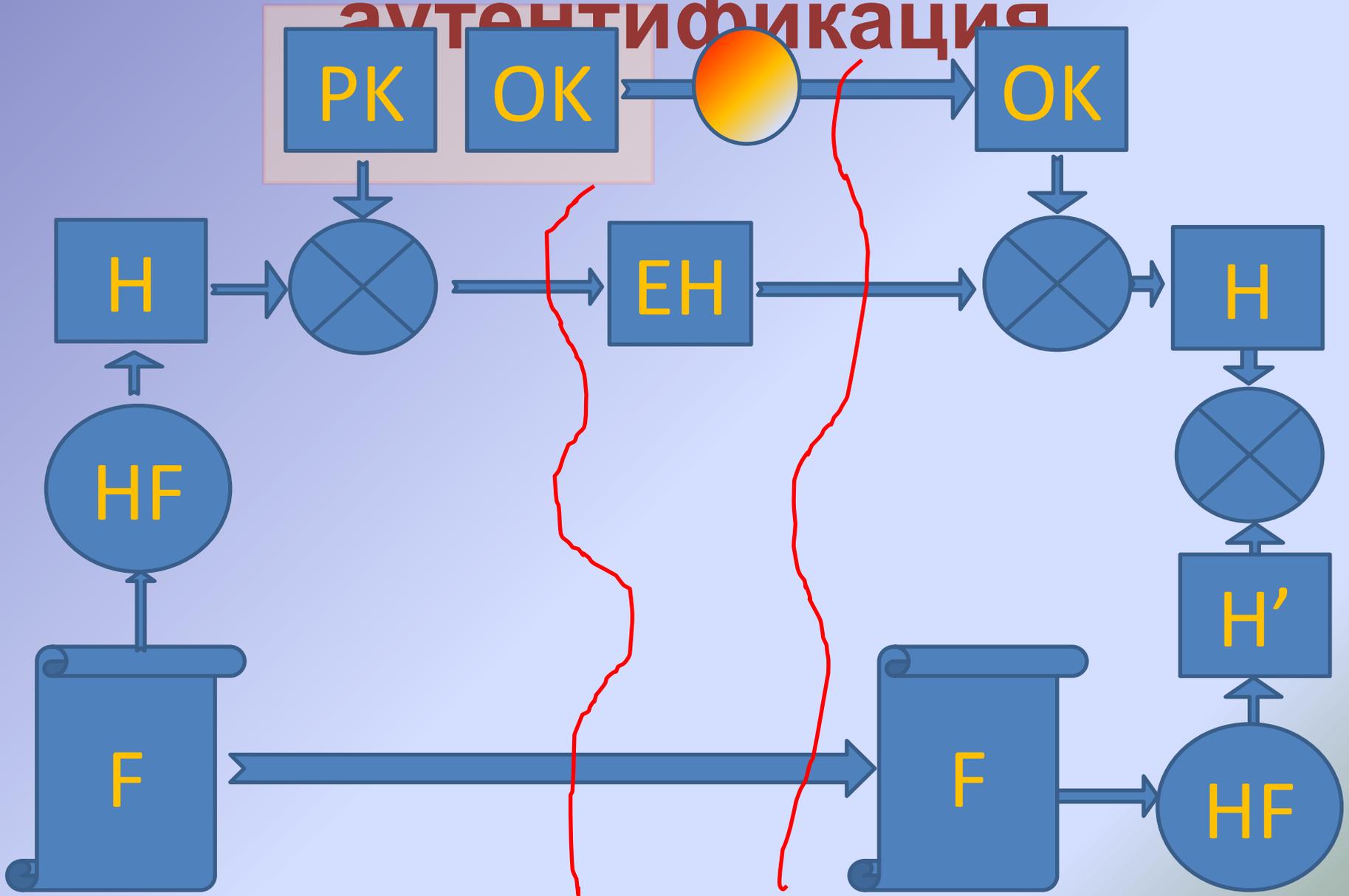
DNS-суффикс подключения . . . . . :
Описание. . . . . : VMware Virtual Ethernet Adapter for VMn

```

Конфиденциальность



Целостность и аутентификация



Списки управления доступом

Горячев Александр Вадимович
Доцент кафедры ИБ
avgoriachev@etu.ru

Модель эшелонированной обороны

Физический

Политики, процедуры, осведомленность

Хранение

e

ACL EFS Bitlocker

Backup Mirror RAID SC

Обработка

a

APPs

Antivirus Updates

OS/.NET

Antispyware Autentification HIDS-HIPS

PKI

Передача

a

Intranet

Routing

IPSec

RMS

NIDS-NIPS

AD

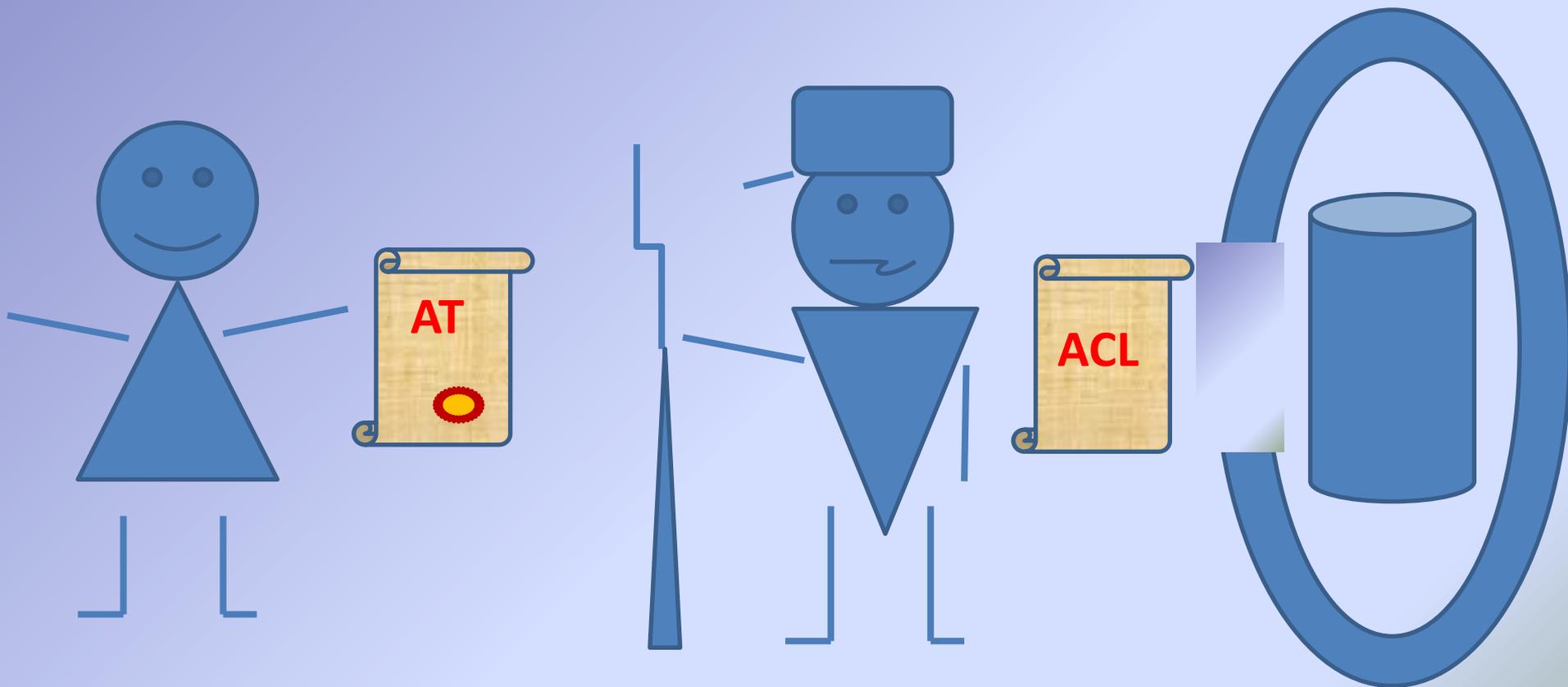
Internet

Firewall

VPN

NAP

Список контроля доступа



Список контроля доступа (ACL)

SID	Прав	A/D	I
SID 01	a R	A	
SID 02	RW	A	I
SID 03	RWM	D	

Маркер доступа (AT)

SID

SID группы

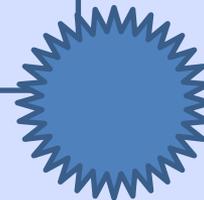
G1
SID группы

G2
SID группы

G3

Прав

а



Обеспечение доступности информации при хранении

Горячев Александр Вадимович
Доцент кафедры
Информационной безопасности
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 Autentication HIDS-HIPS

PKI

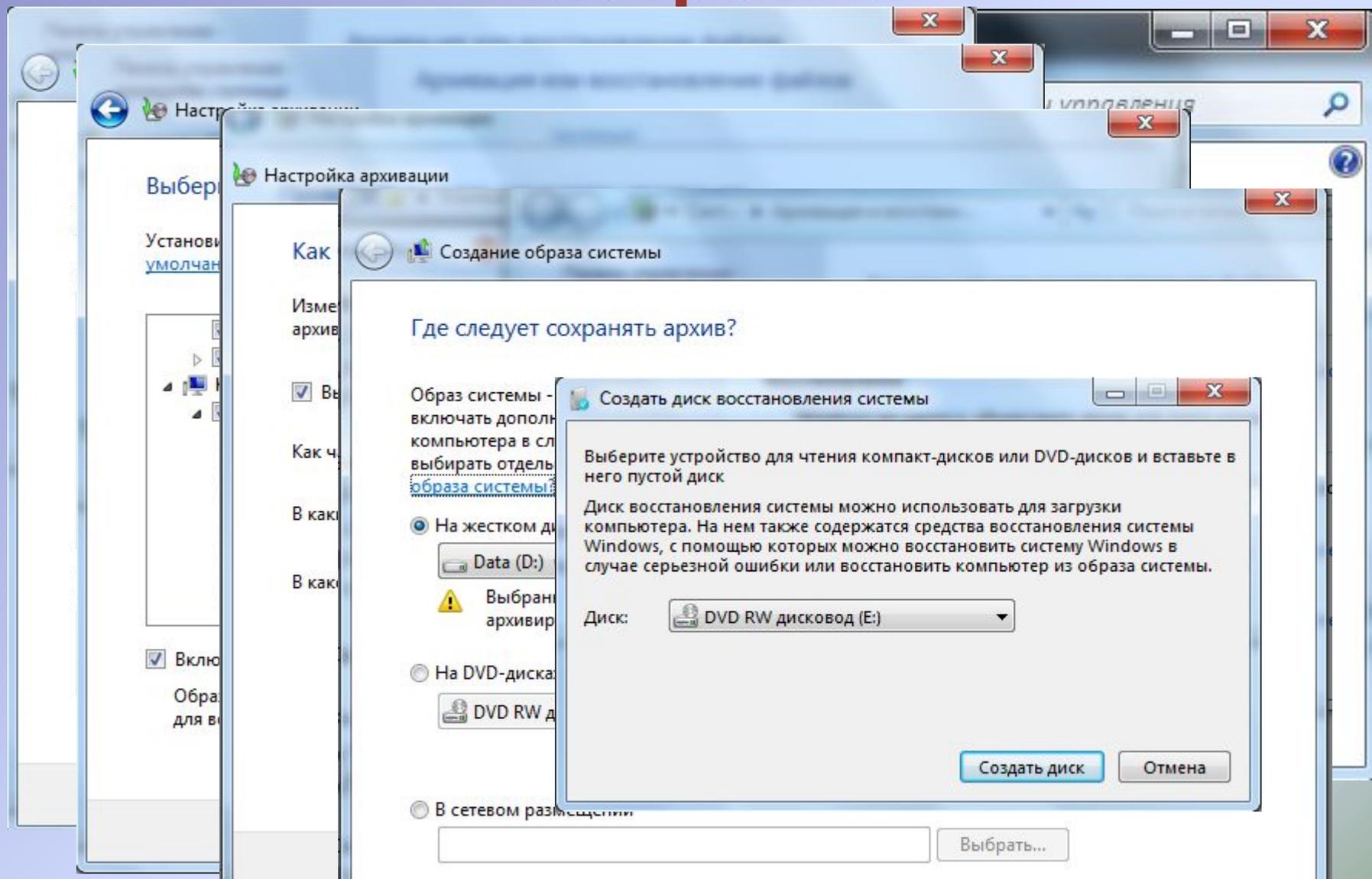
Передача

Intranet Routing IPsec RMS NIDS-NIPS

Internet Firewall VPN NAP

AD

Резервное копирование. Настройка



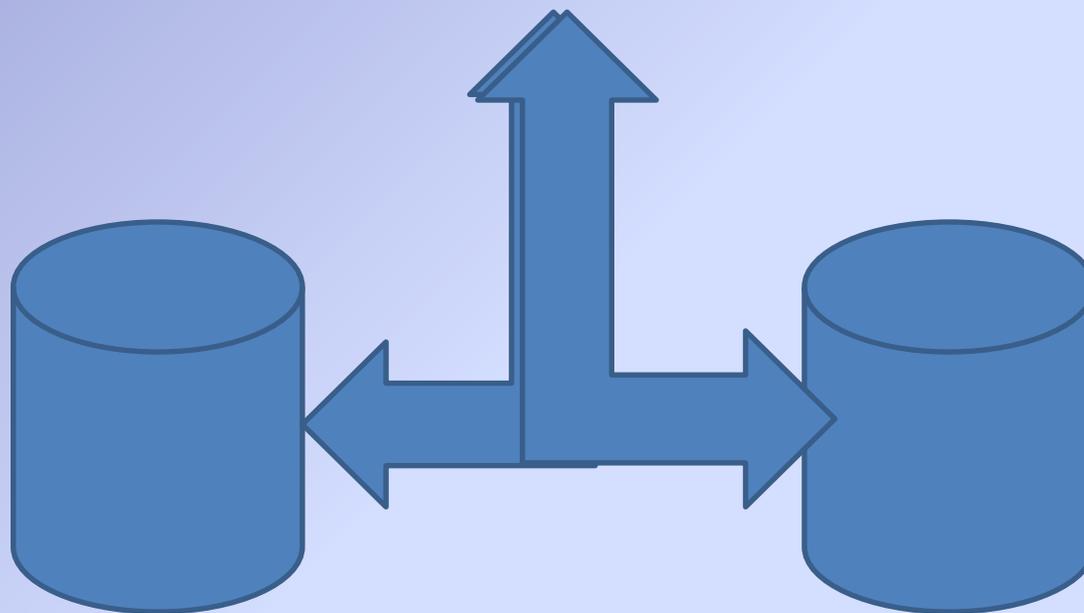
Резервное копирование. Схемы

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

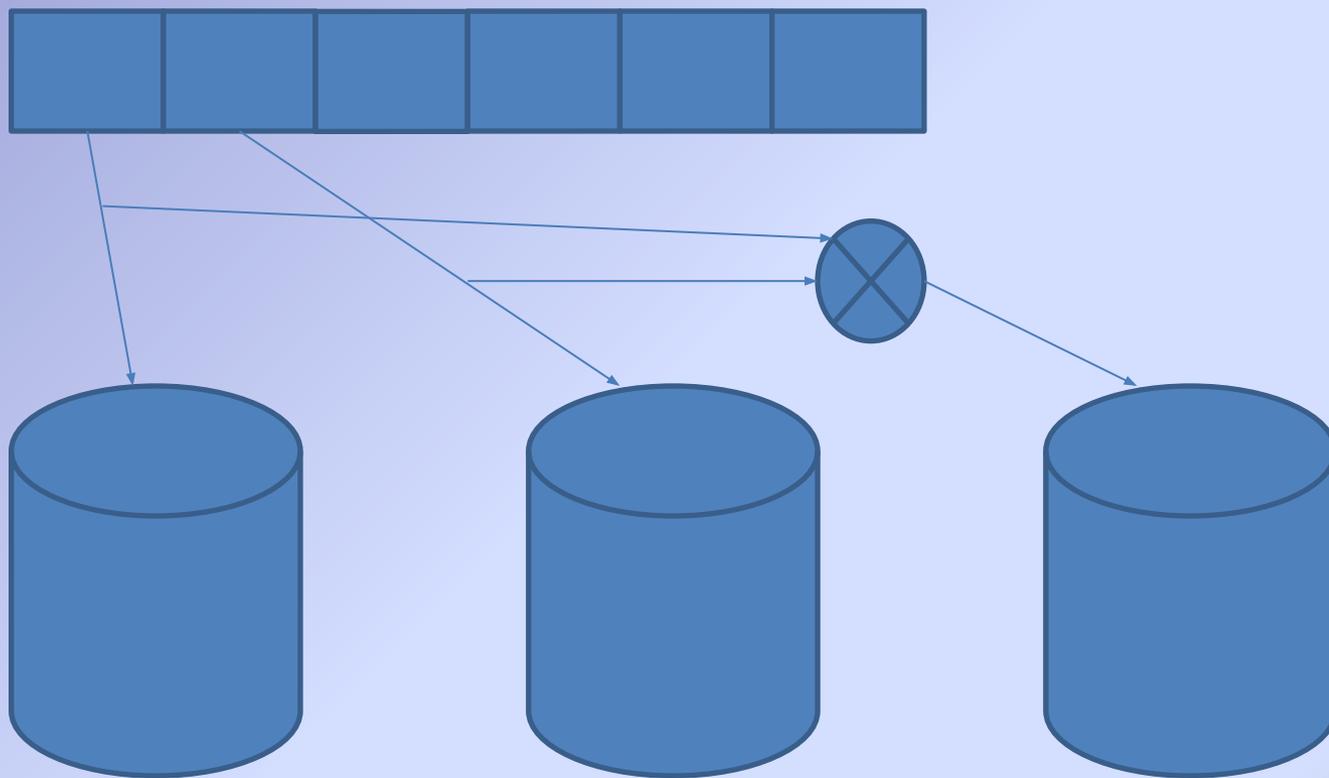
Резервное копирование. Правила

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

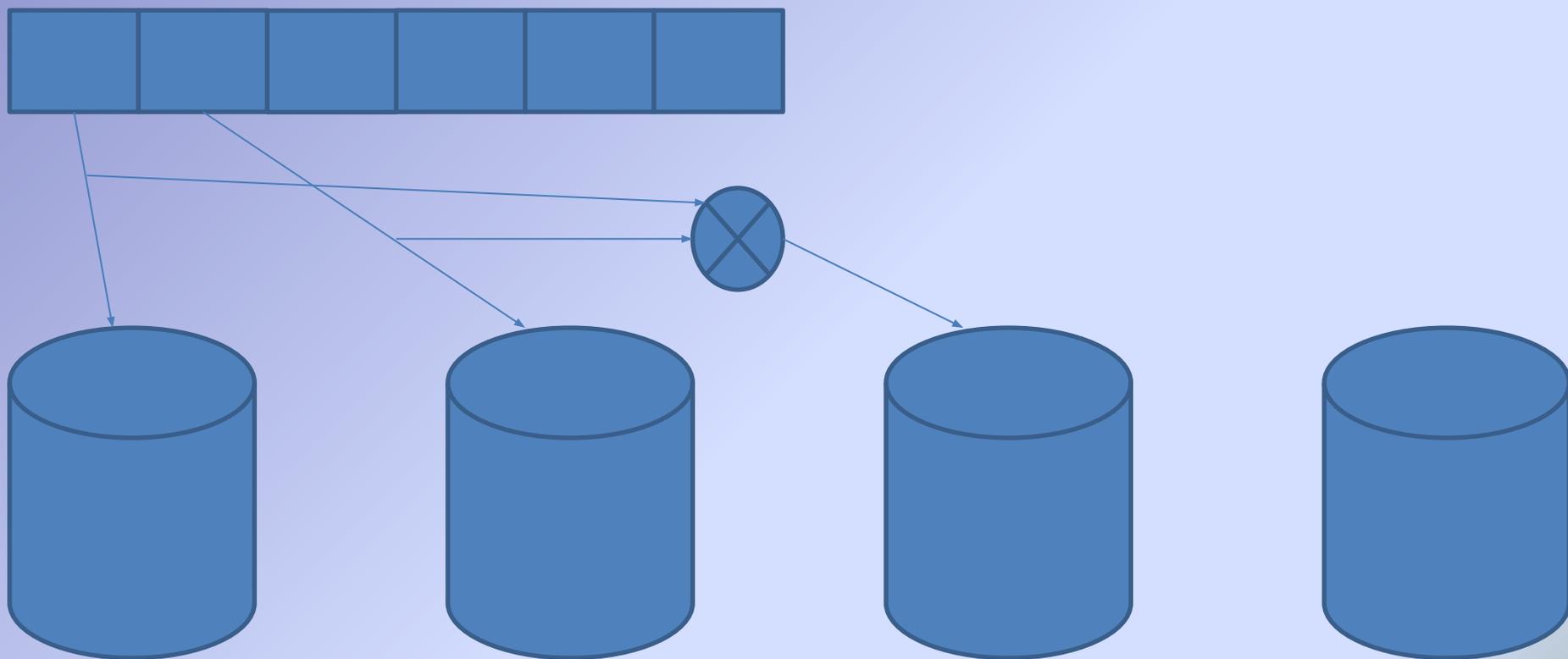
Дисковые массивы. Зеркало



Дисковые массивы. RAID 5



Дисковые массивы. Hot Spare



Shadow Copy

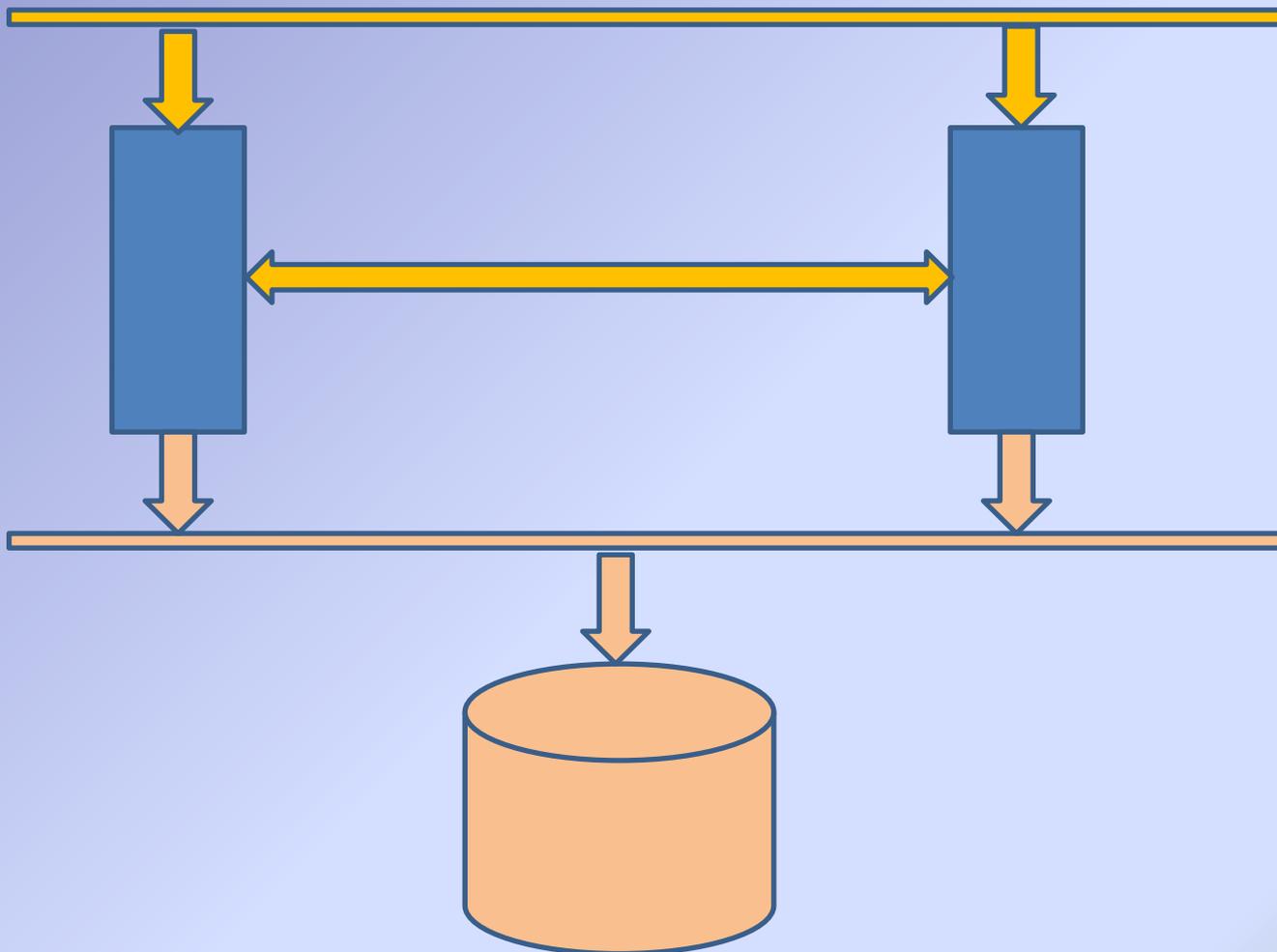
The image shows a Windows interface illustrating the Shadow Copy feature. It consists of several overlapping windows:

- Top Window:** "Свойства: Локальный диск (C:)" (Properties: Local Disk (C:)). The "Безопасность" (Security) tab is active, showing "Предыдущие версии" (Previous Versions) and "Квота" (Quota). A green arrow icon is visible.
- Middle Window:** "Свойства: Custom Production Presets 8.0" (Properties: Custom Production Presets 8.0). The "Безопасность" (Security) tab is active, showing "Предыдущие версии" (Previous Versions) and "Настройка" (Settings). It displays a list of file versions under "Версии папки:" (Folder Versions):

Имя	Дата изменения
На прошлой неделе (1)	
Custom Production Pr...	16.10.2015 3:00
- Bottom Window:** A file explorer window showing the contents of the "Custom Production Presets 8.0" folder. The files listed are:
 - 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)

Yellow arrows point from the "Предыдущие версии" tab in the top window to the "Предыдущие версии" tab in the middle window, and from the middle window to the file explorer window, indicating the flow of information from the system property to the file's version history and then to the actual files.

Кластер надежности



Групповые политики службы каталога Active Directory

Горячев Александр Вадимович
Доцент кафедры
Информационной безопасности
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 Autentication HIDS-HIPS

PKI

AD

Передача

Intranet Routing IPsec RMS NIDS-NIPS

Internet Firewall VPN NAP

Локальная политика безопасности

The screenshot displays the Windows Group Policy Editor interface. The left pane shows a tree view of the policy hierarchy, with 'Local Computer Policy' expanded to 'Security Settings' > 'Account Policies' > 'Password Policy'. The right pane shows a list of policies under the 'Policy' column and their corresponding 'Security Setting' values.

Policy	Security Setting
Enforce password history	24 passwords remember...
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

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 shows a list of policies with their corresponding computer settings. The 'Password must meet complexity requirements' policy is selected, and a dialog box is open to configure it.

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 Properties

Template Security Policy Setting Explain

Password must meet complexity requirements

Define this policy setting in the template

Enabled

Disabled

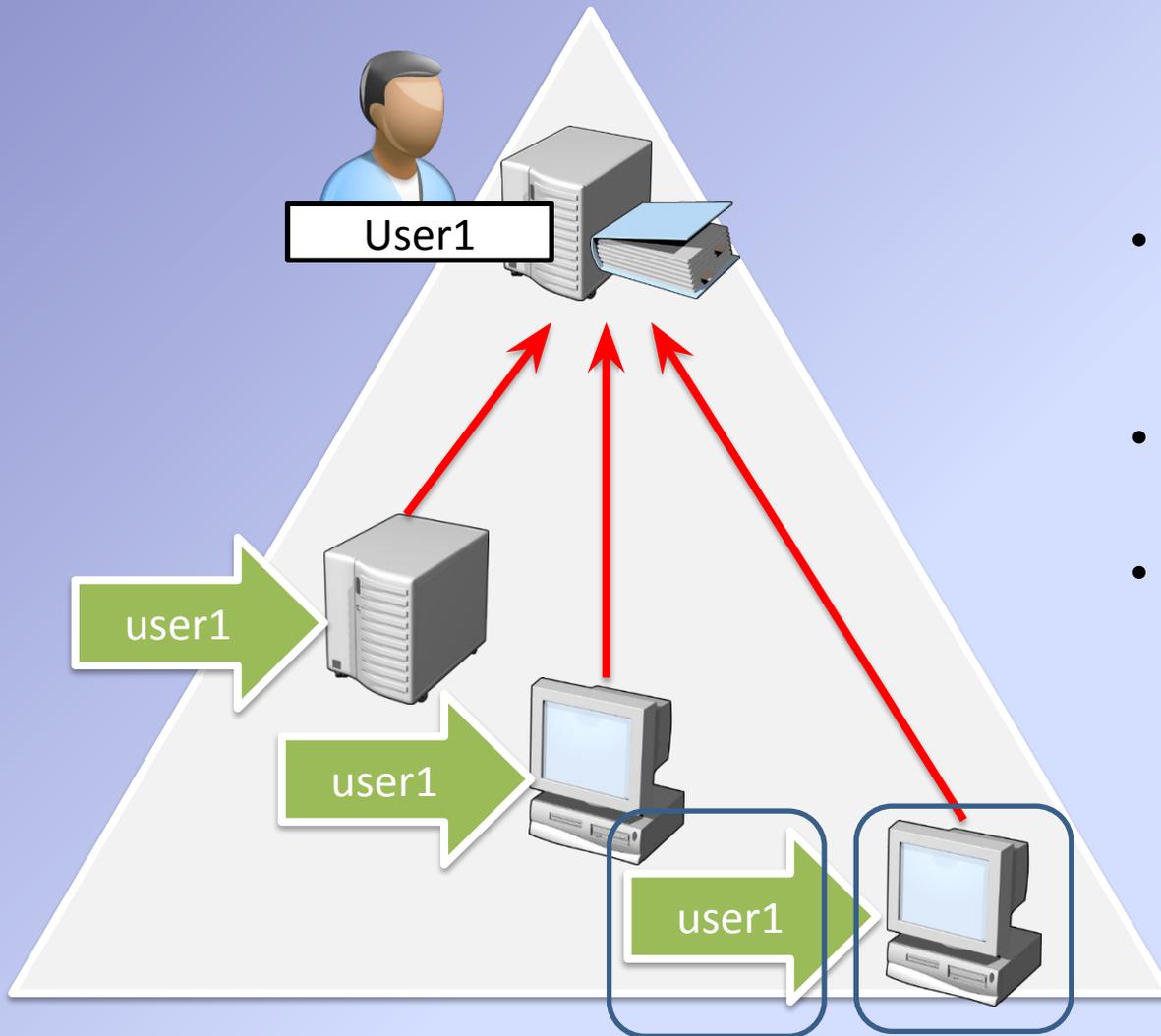
Анализ и конфигурация безопасности



The screenshot displays the Windows Security Configuration and Analysis console. The left pane shows the navigation tree with 'Password Policy' selected under 'Account Policies'. The right pane shows a table of policy settings.

Policy	Database Setting	Computer Setting
Enforce password history	Not Defined	24 passwords
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

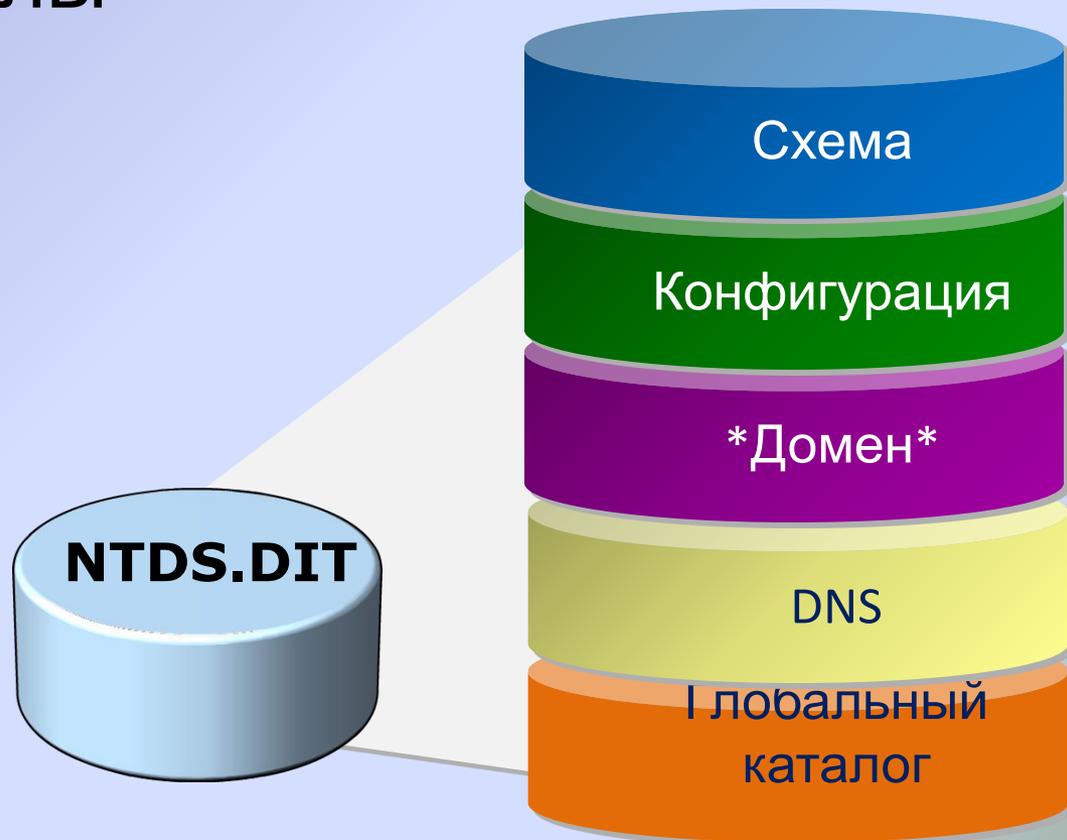


Хранилище данных Active Directory

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

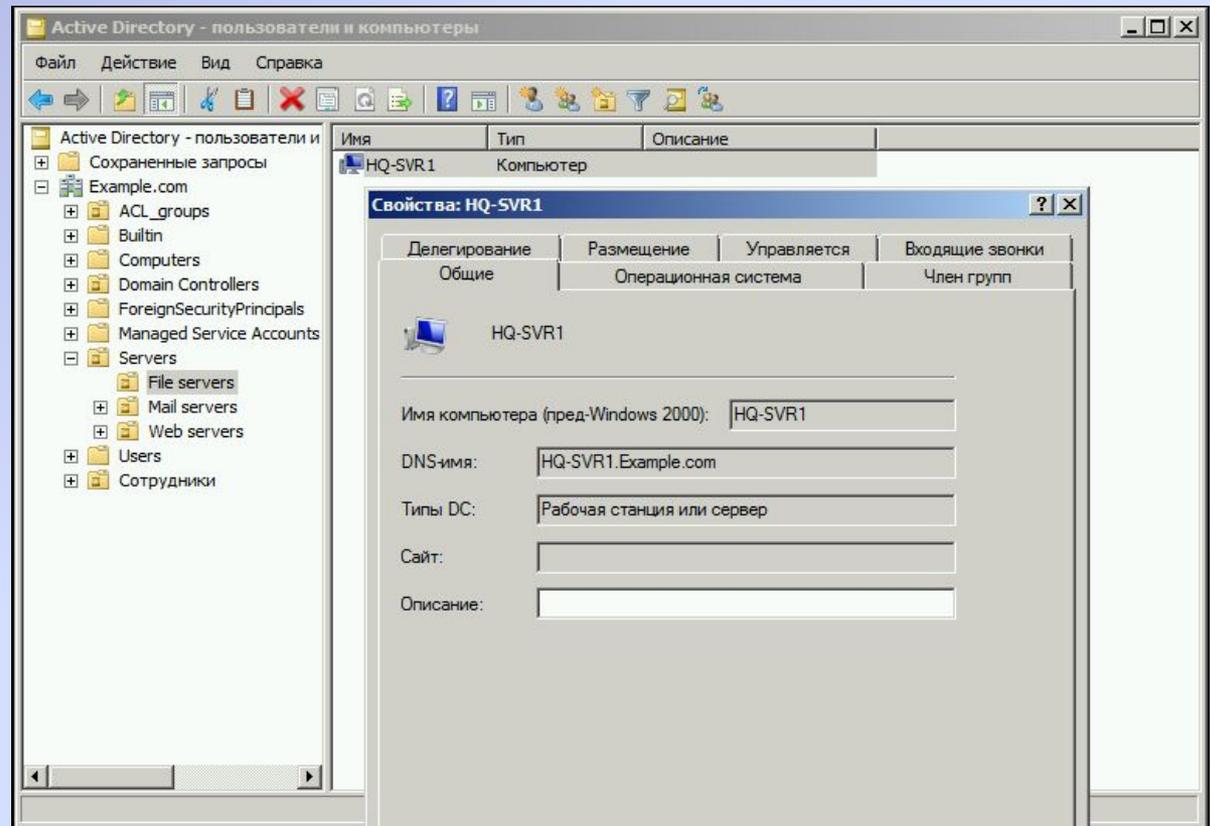
• SYSVOL

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



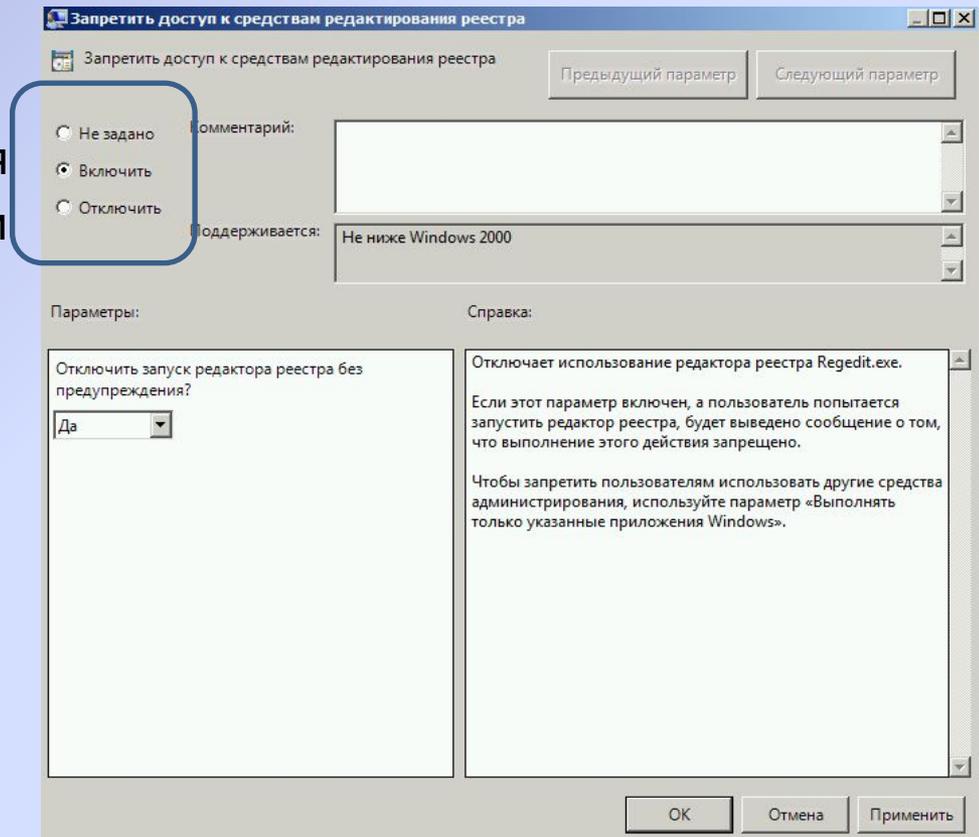
Учётные записи компьютеров

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



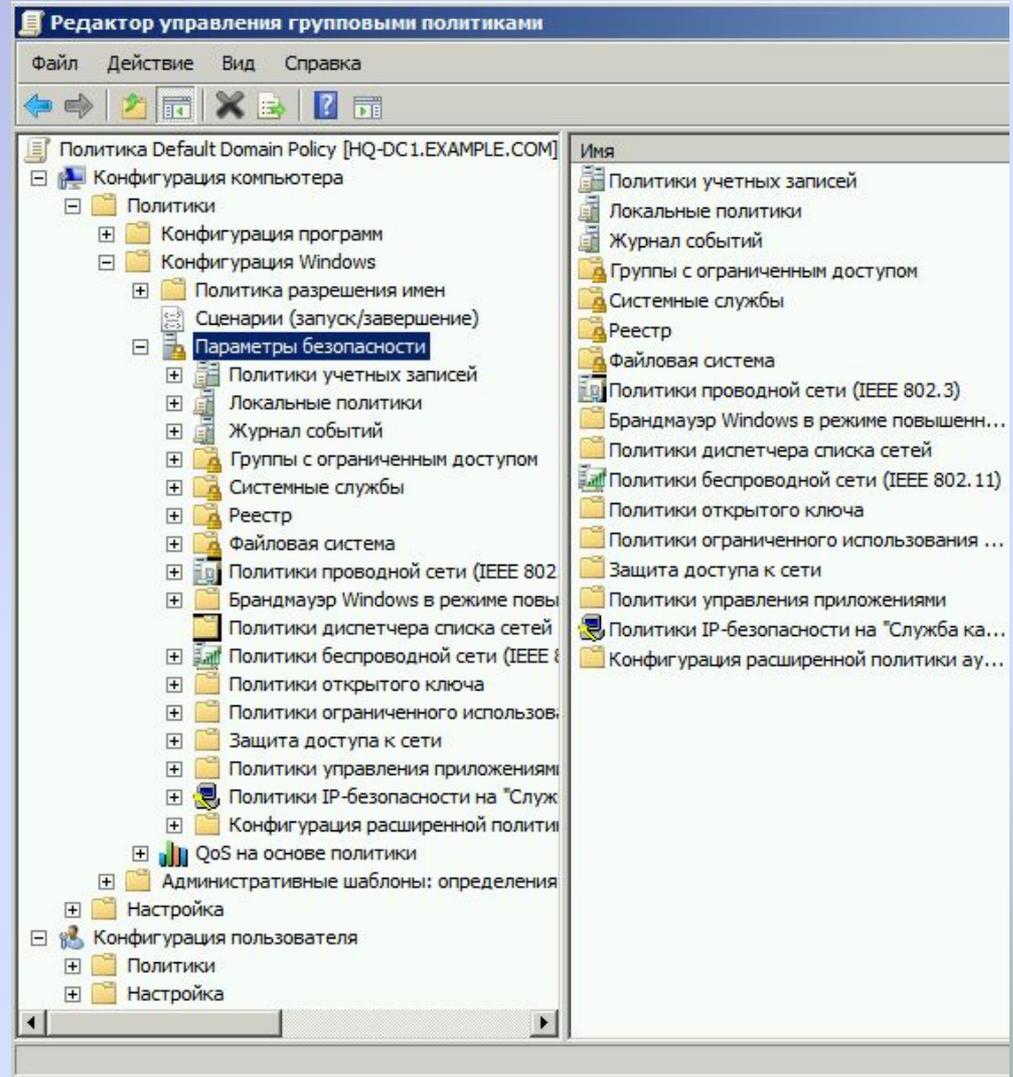
Параметры групповой политики

- 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)



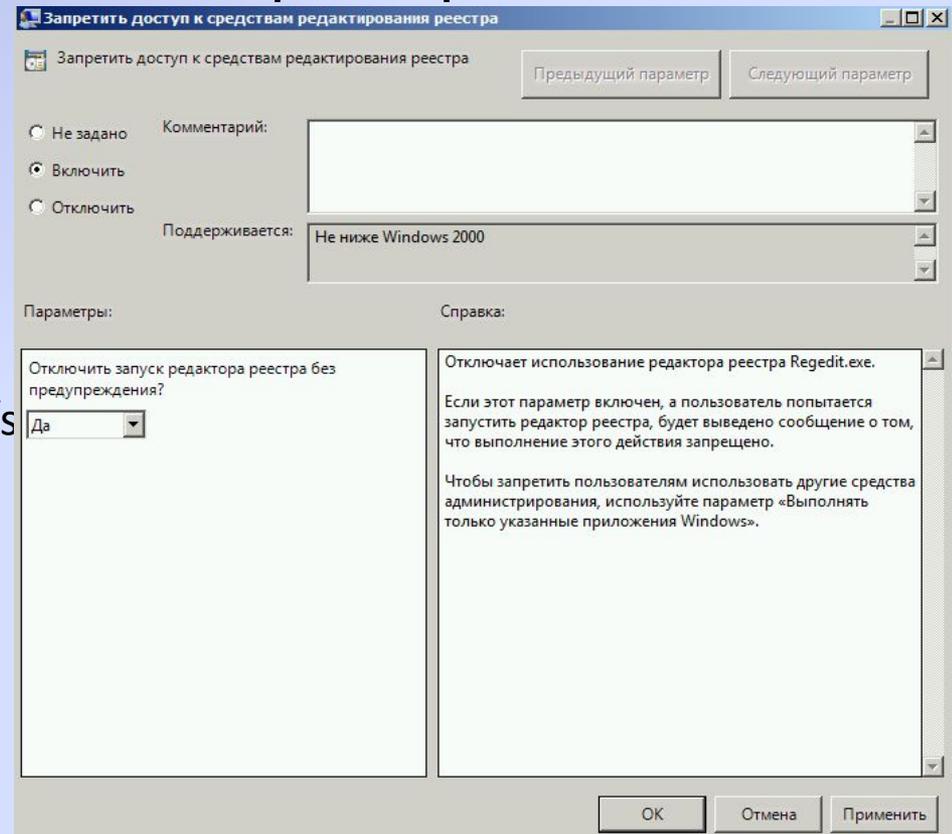
Объекты групповой политики

- 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

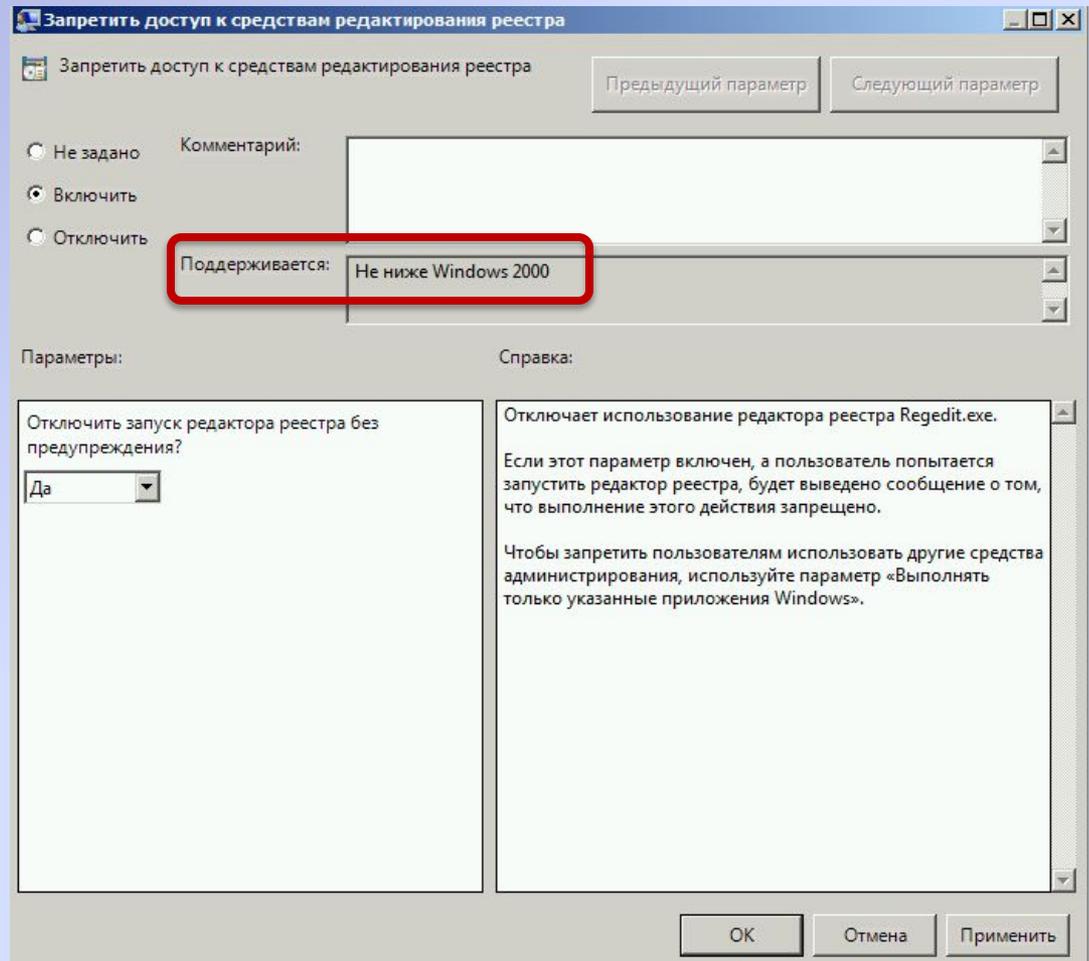


Клиент групповой политики и Client-side extensions

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

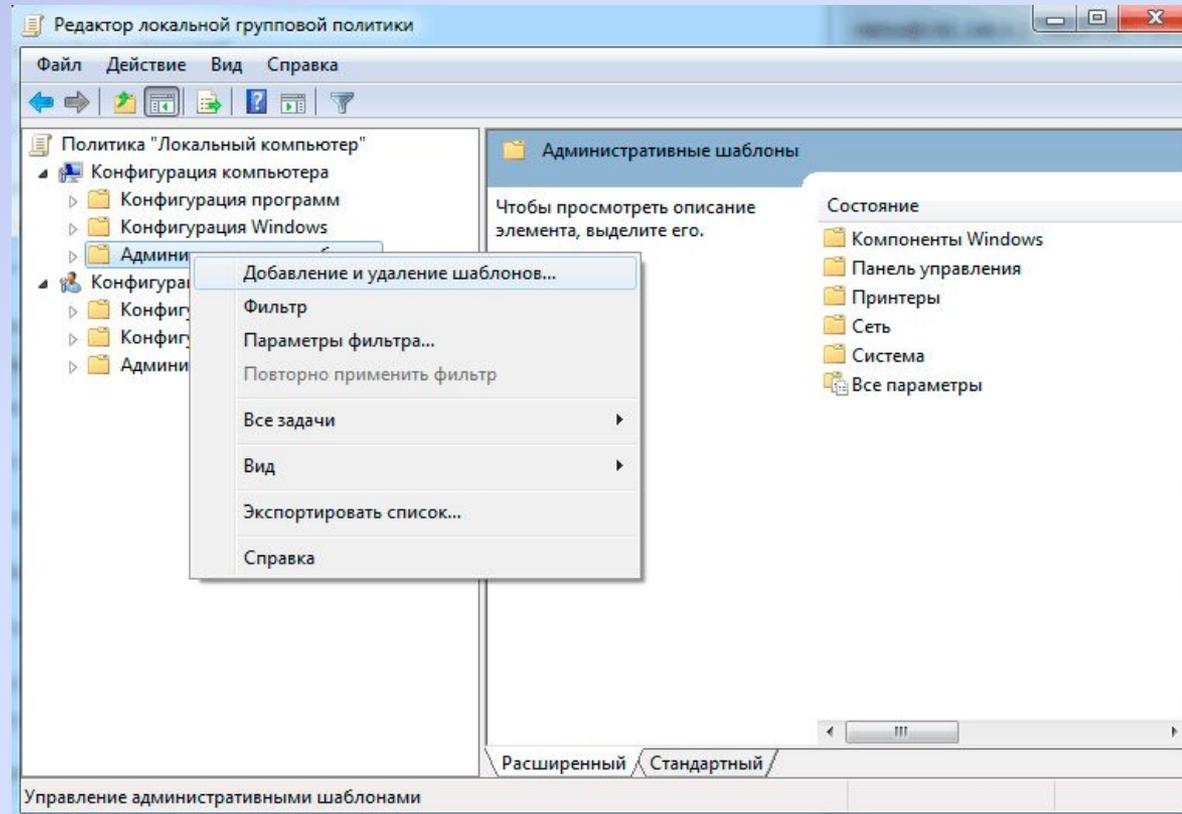
Применение политик разными операционными системами

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

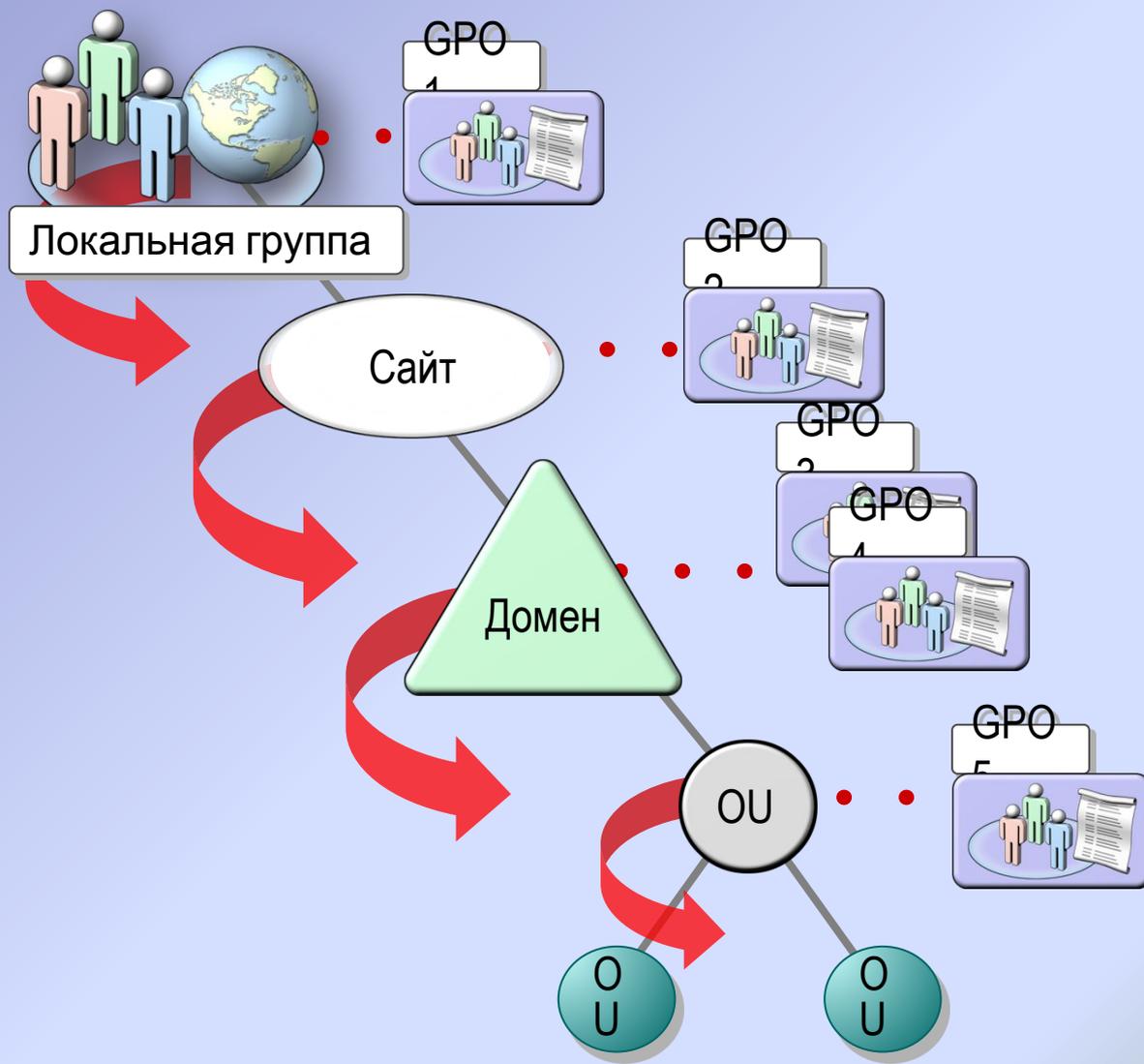


Расширение функционала с помощью административных шаблонов

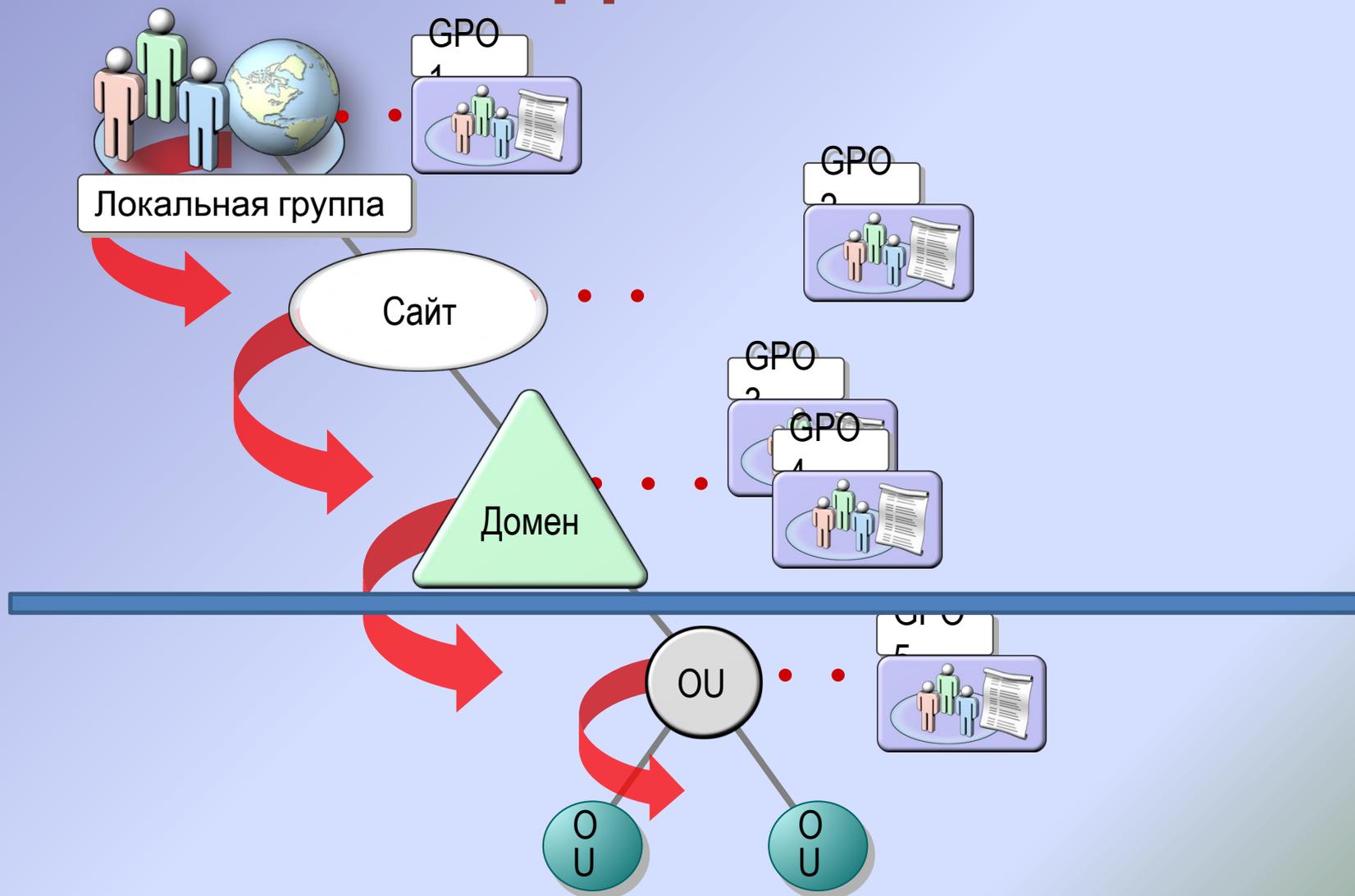
- Административные шаблоны позволяют централизованно управлять программным обеспечением:
 - Microsoft Office, Google Chrome, etc
- ADM
- ADMX/ADML



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:

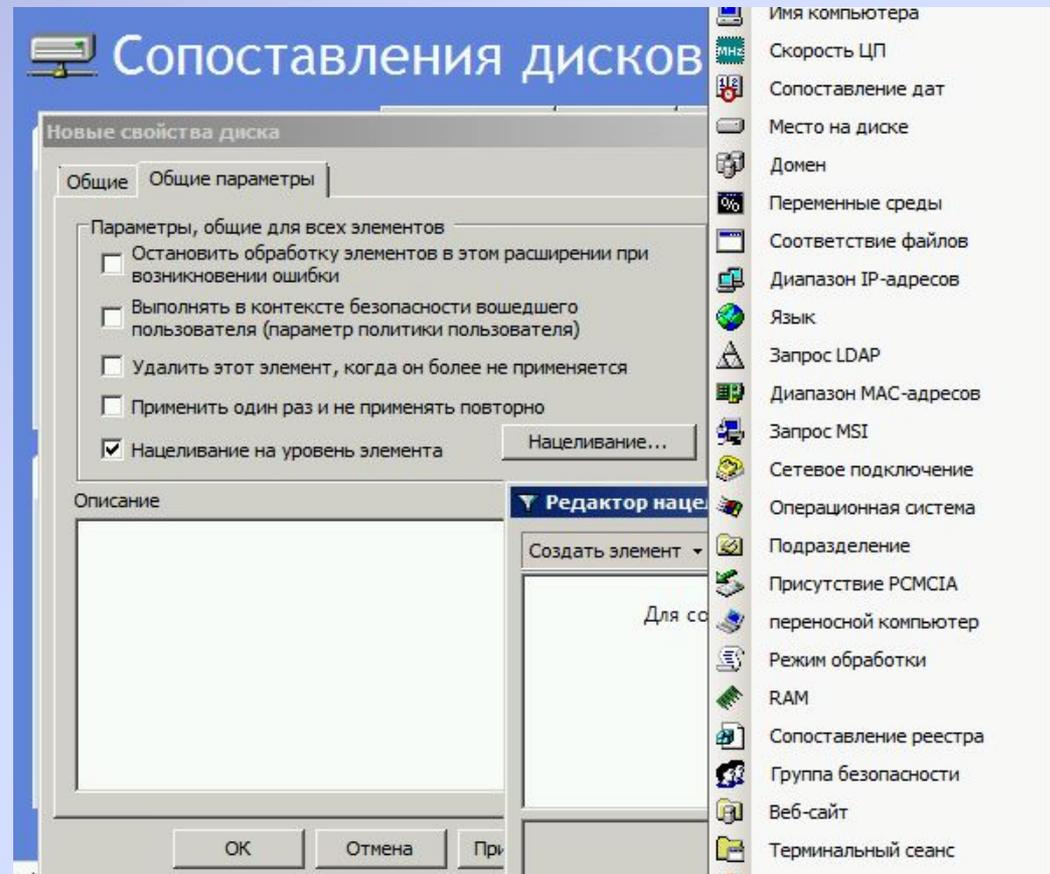
- Не блокируют настройки от изменения пользователем
- Позволяют настраивать параметры операционной системы и ПО
- иначе управляемые загрузочными скриптами (создавать ярлыки,
- подключать сетевые диски и т.д.

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

Модель эшелонированной обороны

Физический
доступ

Политики, процедуры,
осведомленность

Хранение

ACL EFS Bitlocker Backup Mirror RAID SC

Обработка

APPs Antivirus Updates

OS/.NET Antispyware Autentication HIDS-HIPS

PKI

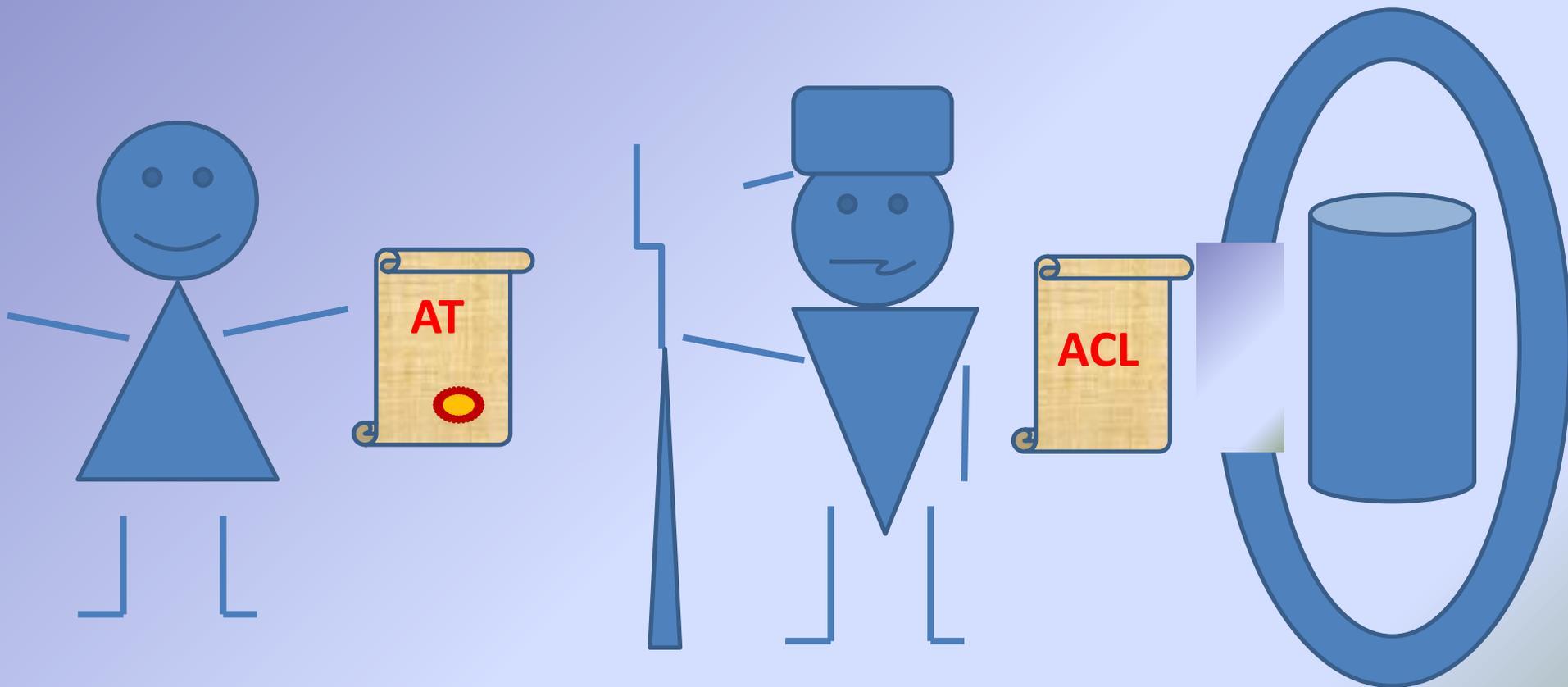
Передача

Intranet Routing IPsec RMS NIDS-NIPS

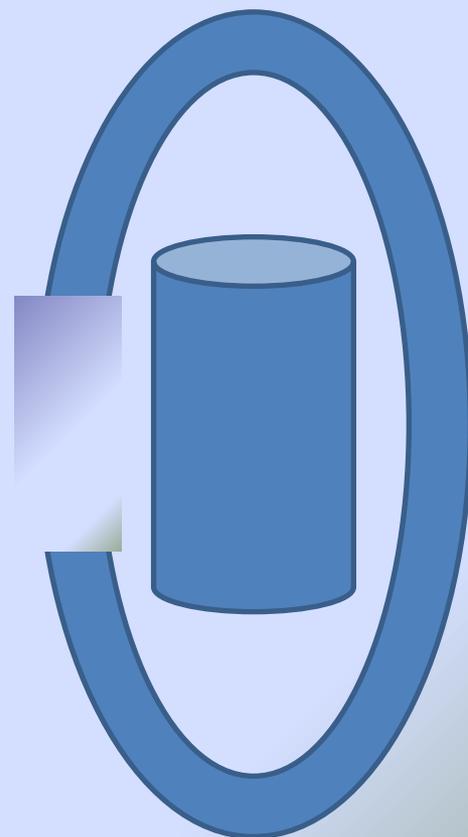
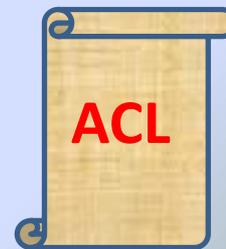
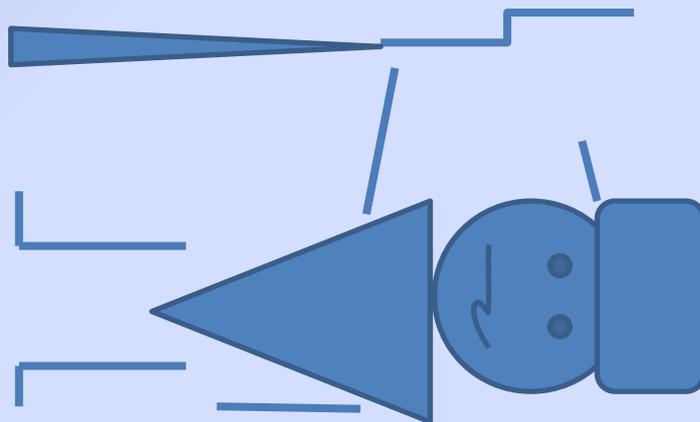
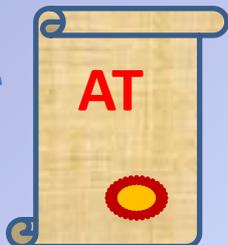
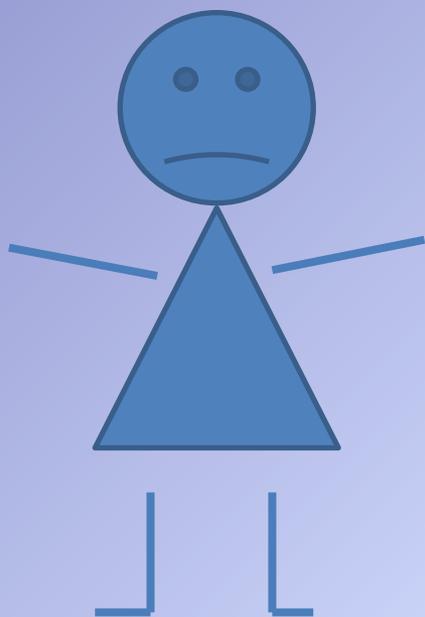
Internet Firewall VPN NAP

AD

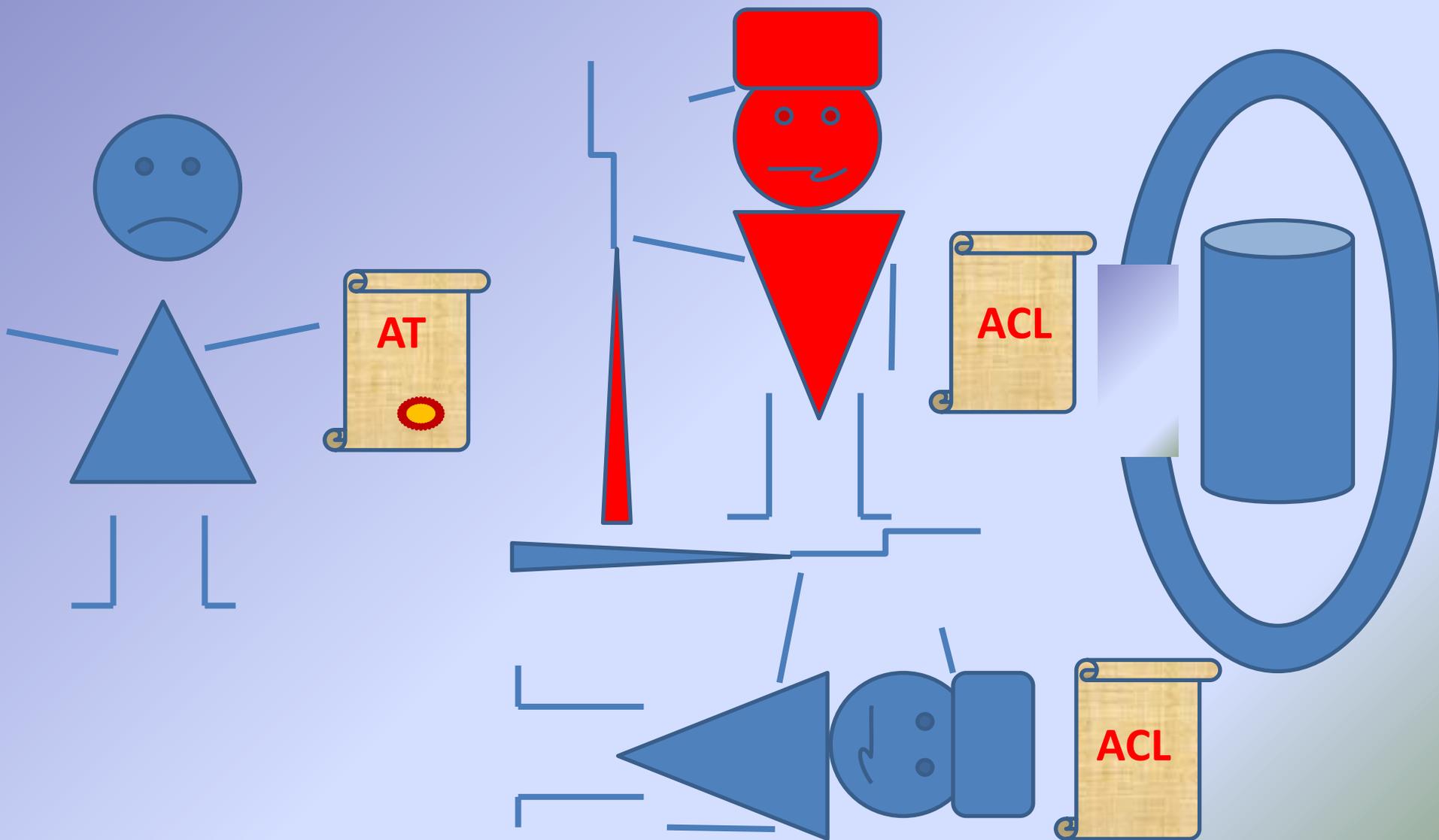
Список контроля доступа



Список контроля доступа



Список контроля доступа

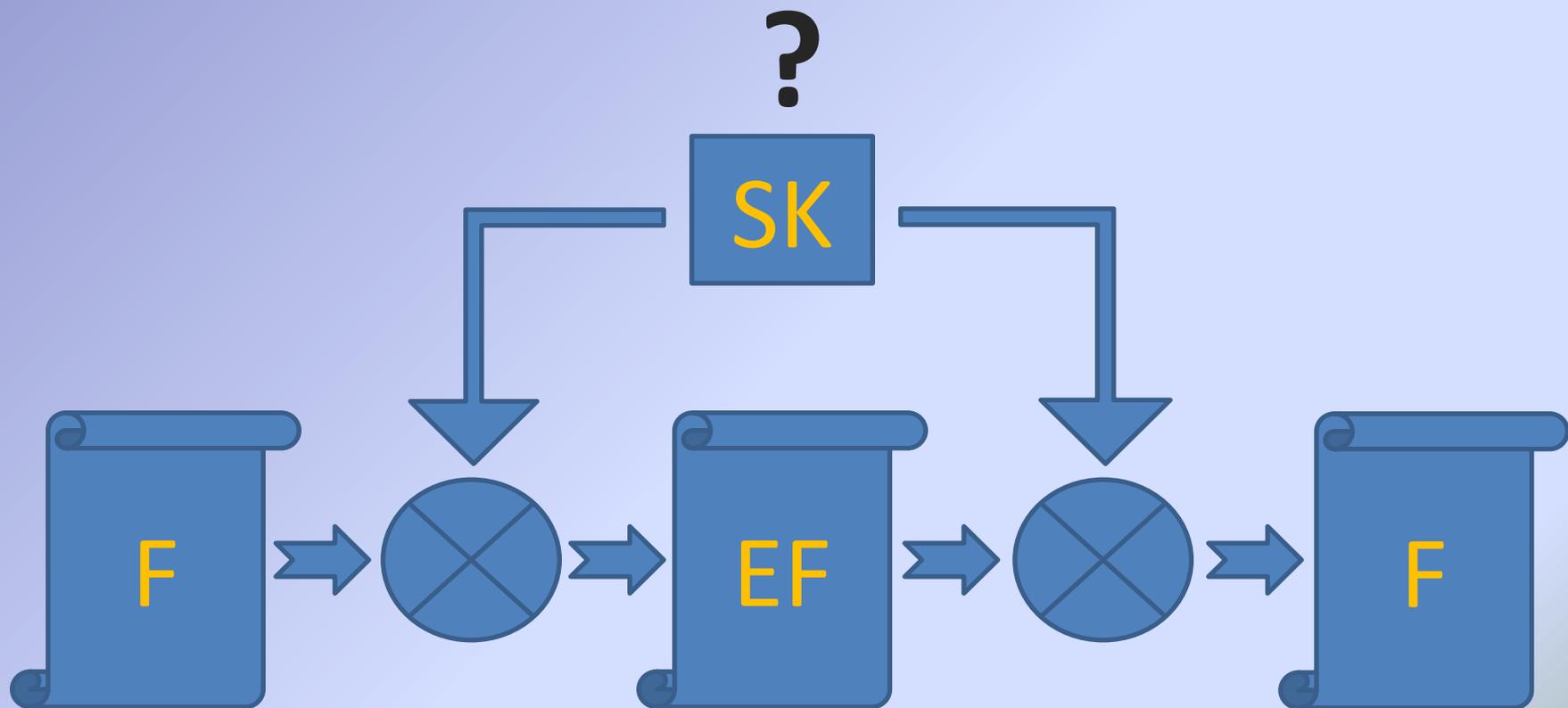


Шифрование с симметричным ключом

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

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

Простейший вариант



Шифрование с асимметричным ключом (открытым и закрытым ключами)

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

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

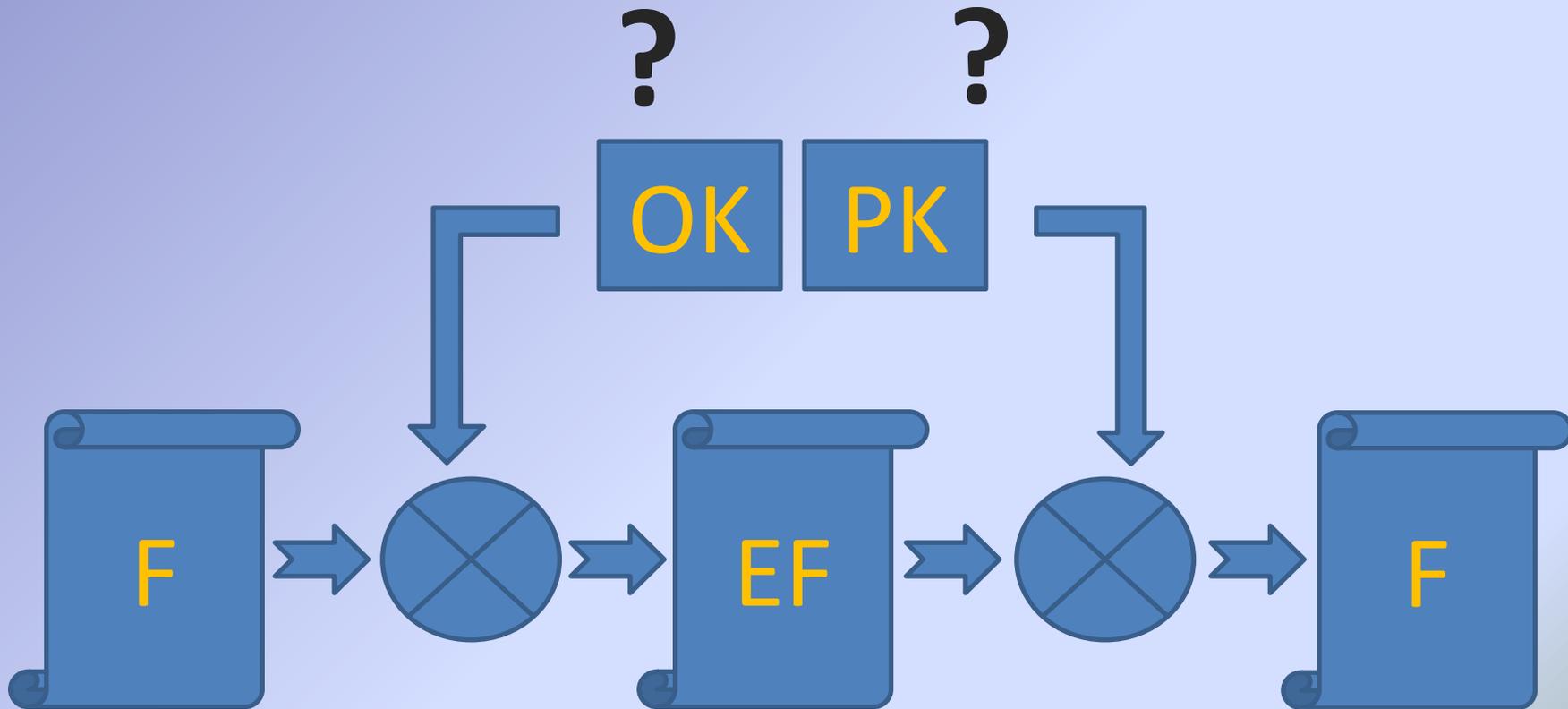
$$T^{-1}(e, p) = a$$

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

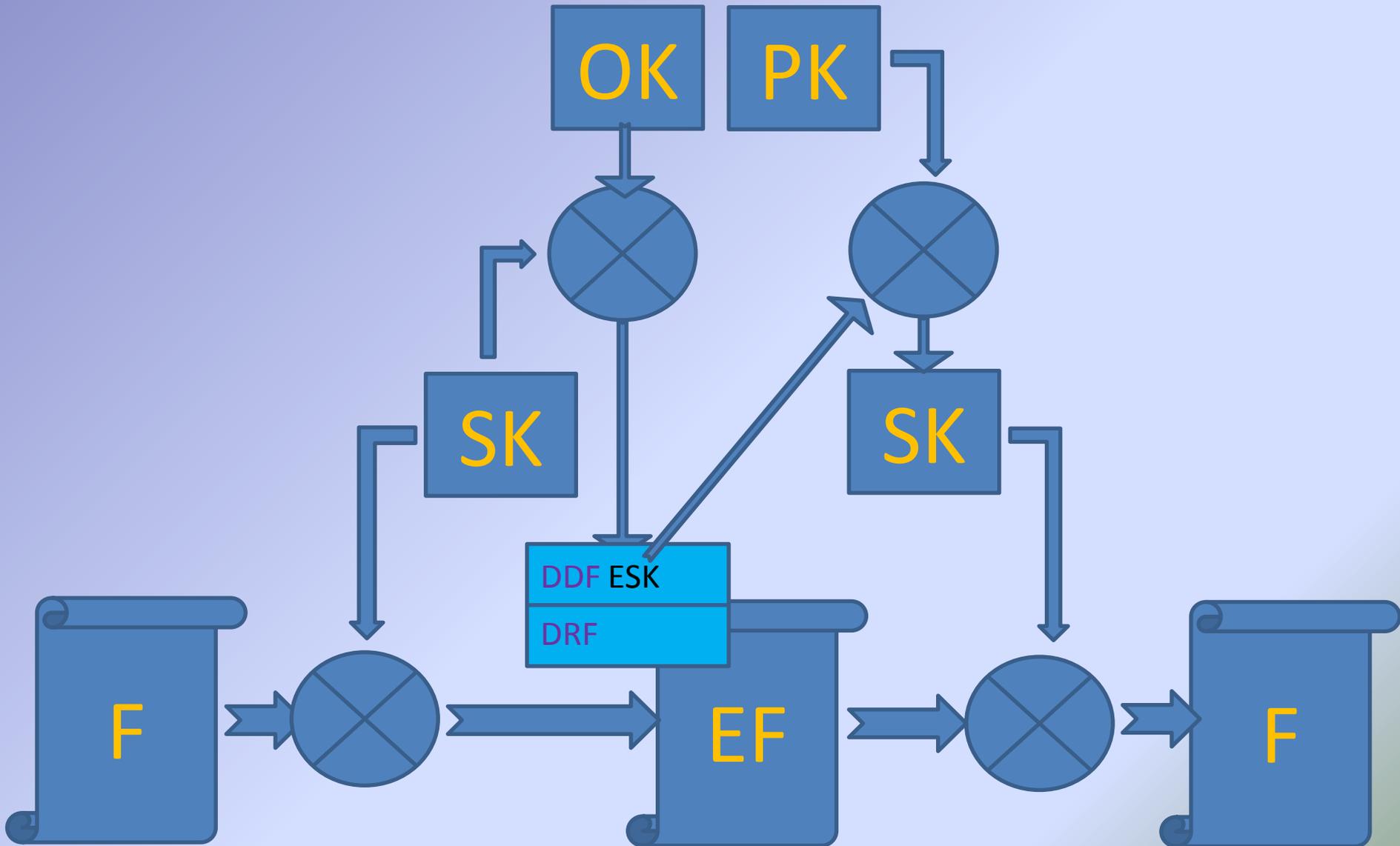
$$T(a, p) = e$$

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

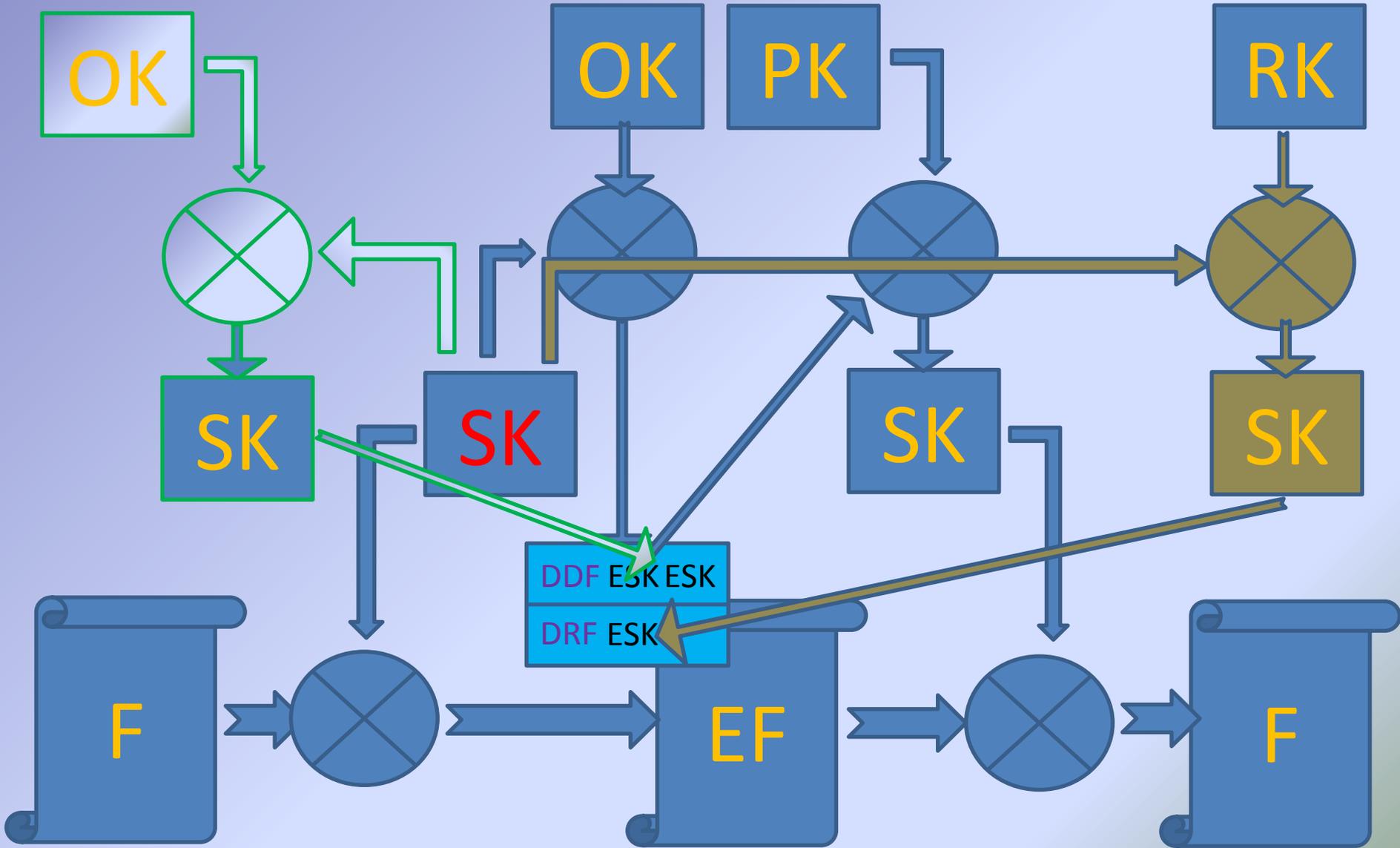
А можно так?



Уже правильнее



EFS



Формирование сертификата

Заявка на

сертификат

О
К

КТО?

Зачем
?

?

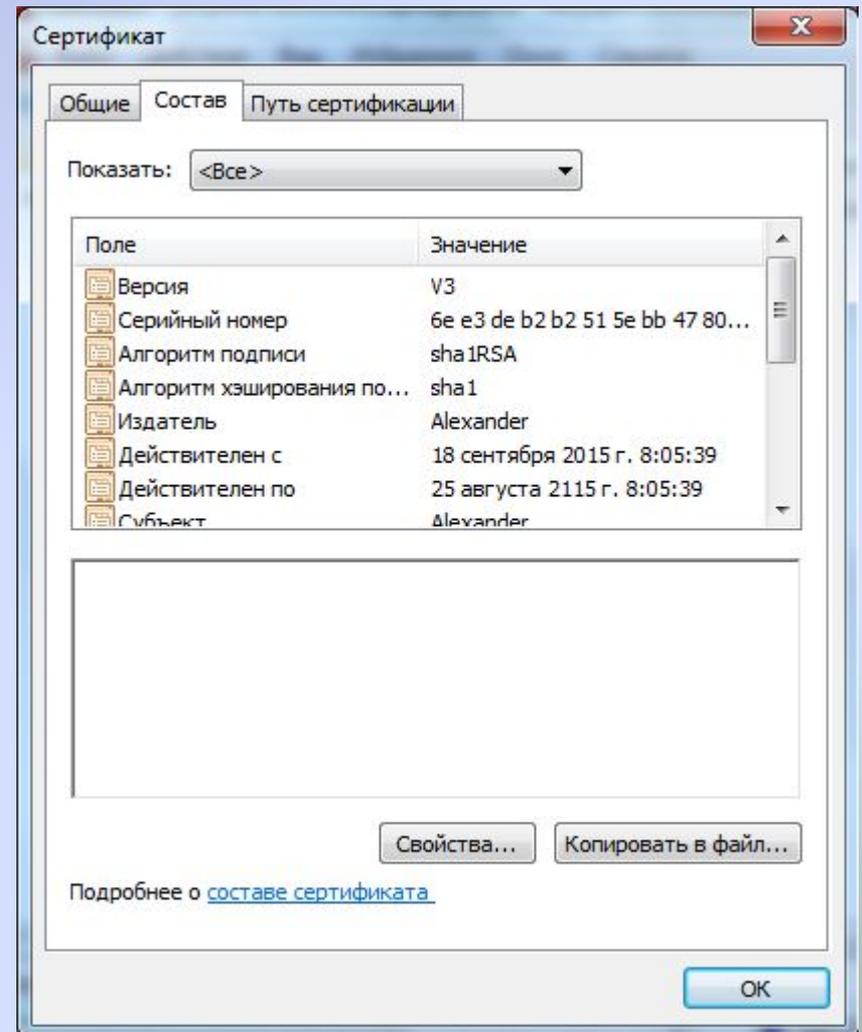
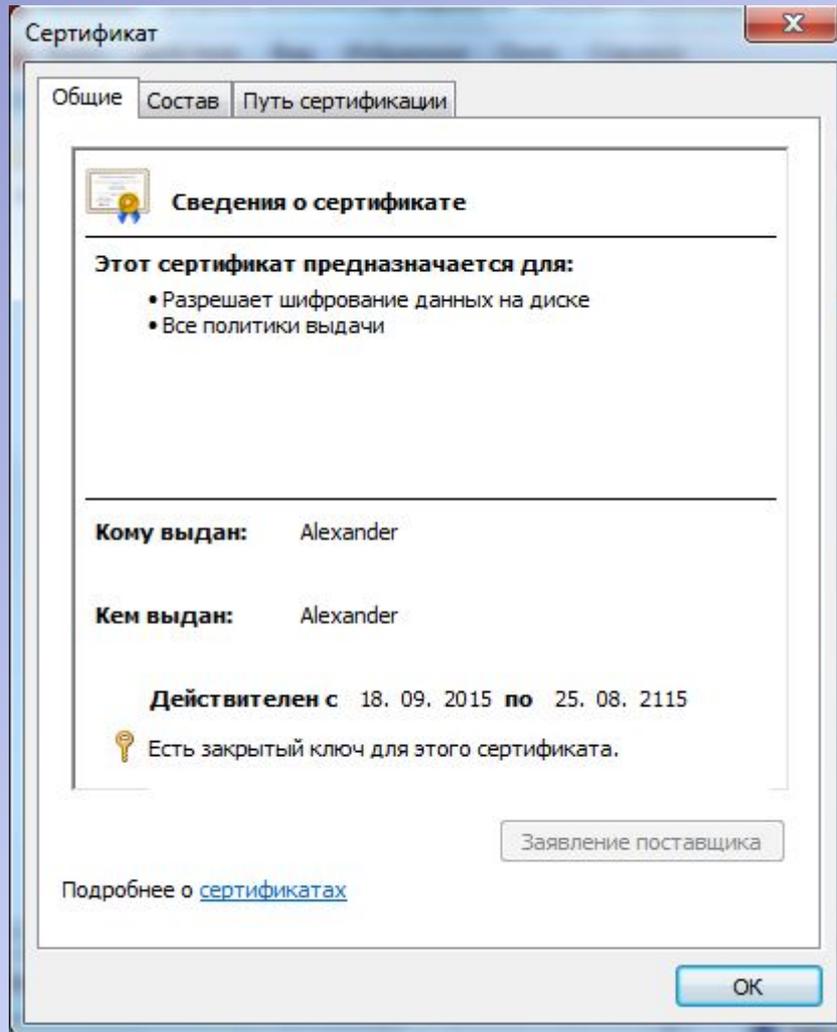
С
А

Инф
о

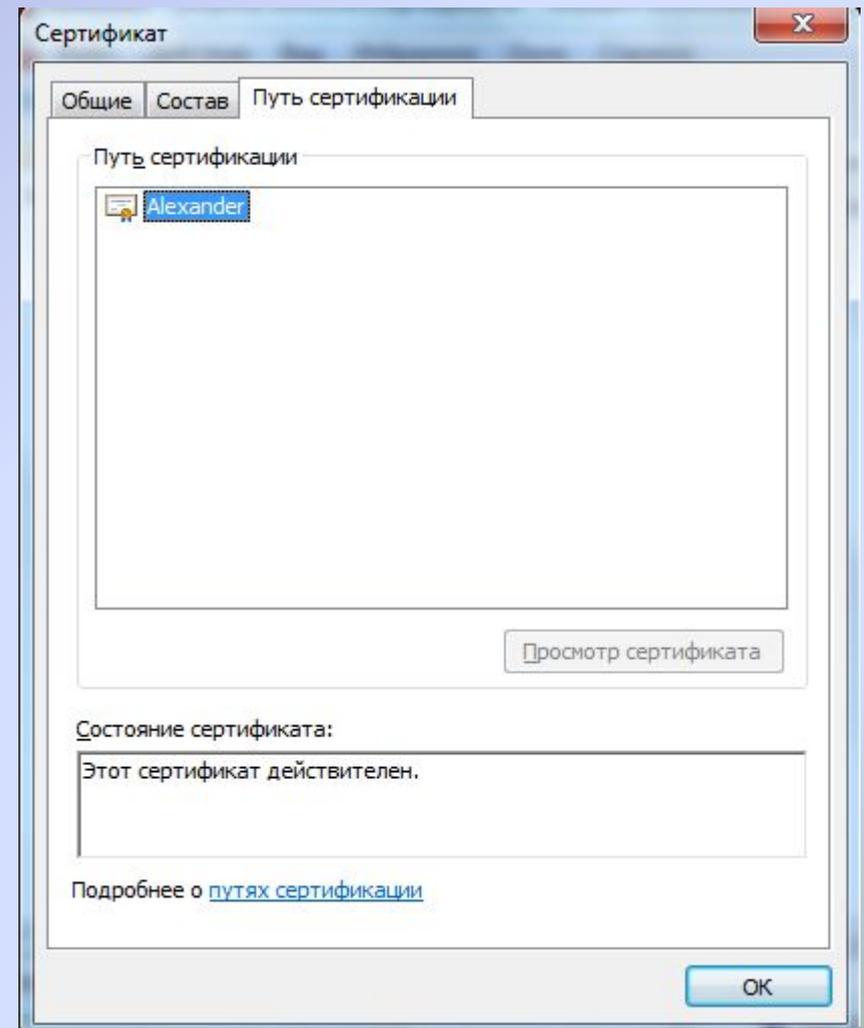
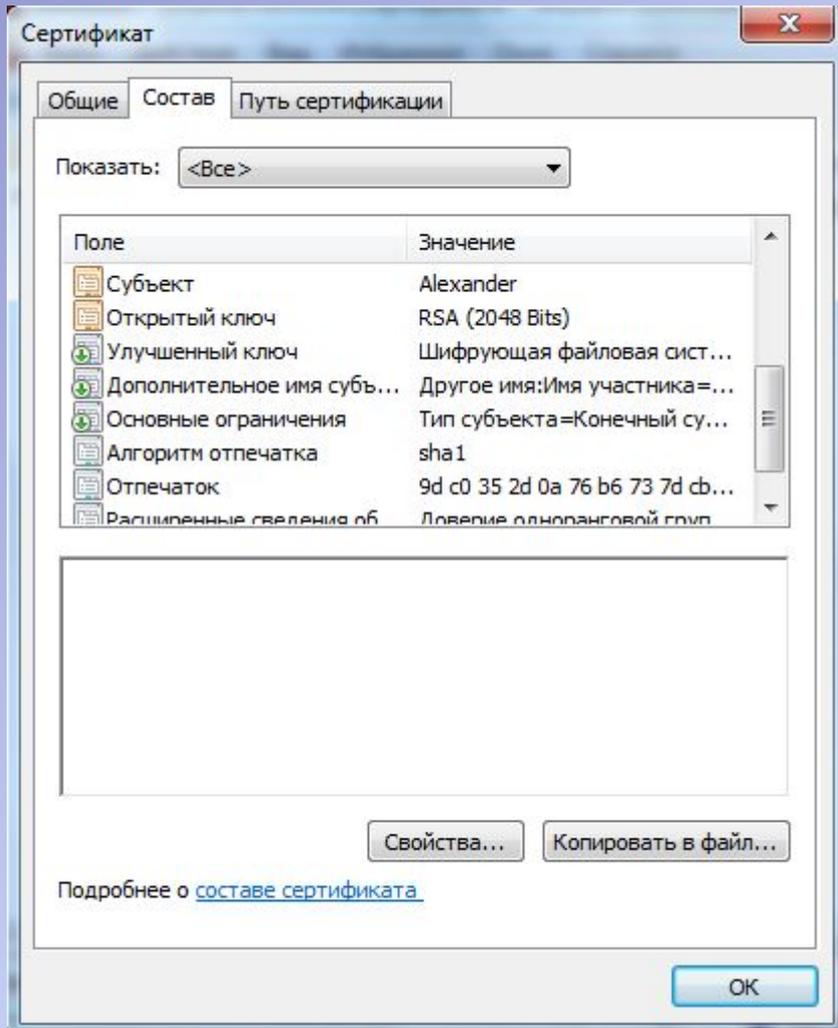
S

СА

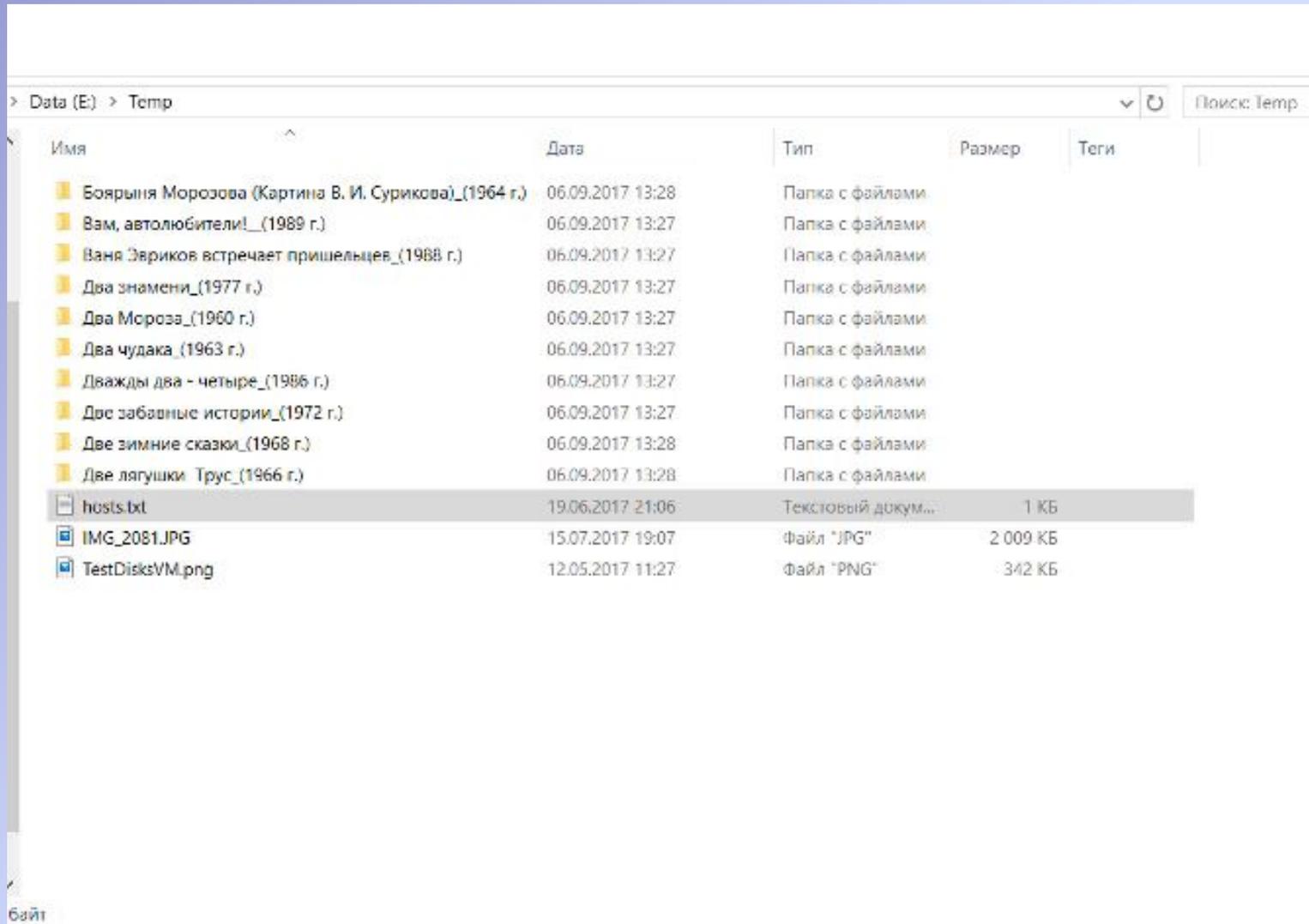
Сертификат



Сертификат



Интерфейс управления EFS



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

Модель эшелонированной обороны

Физический доступ

Политики, процедуры, осведомленность

Хранение

ACL EFS Bitlocker

Backup Mirror RAID SC

Обработка

APPs Antivirus Updates

OS/.NET Antispyware Autentication HIDS-HIPS

PKI

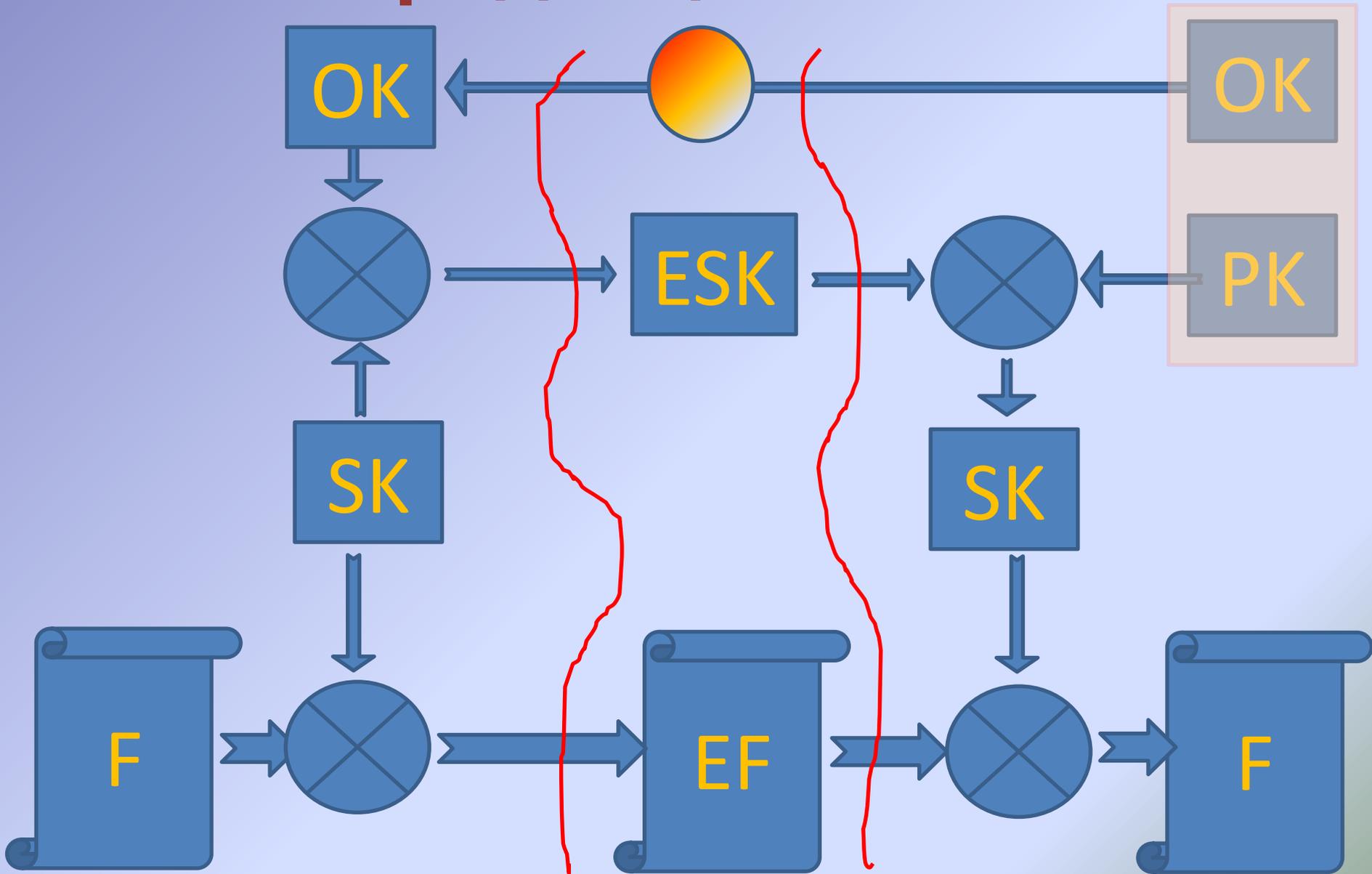
AD

Передача

Intranet Routing IPsec SSL RMS NIDS-NIPS

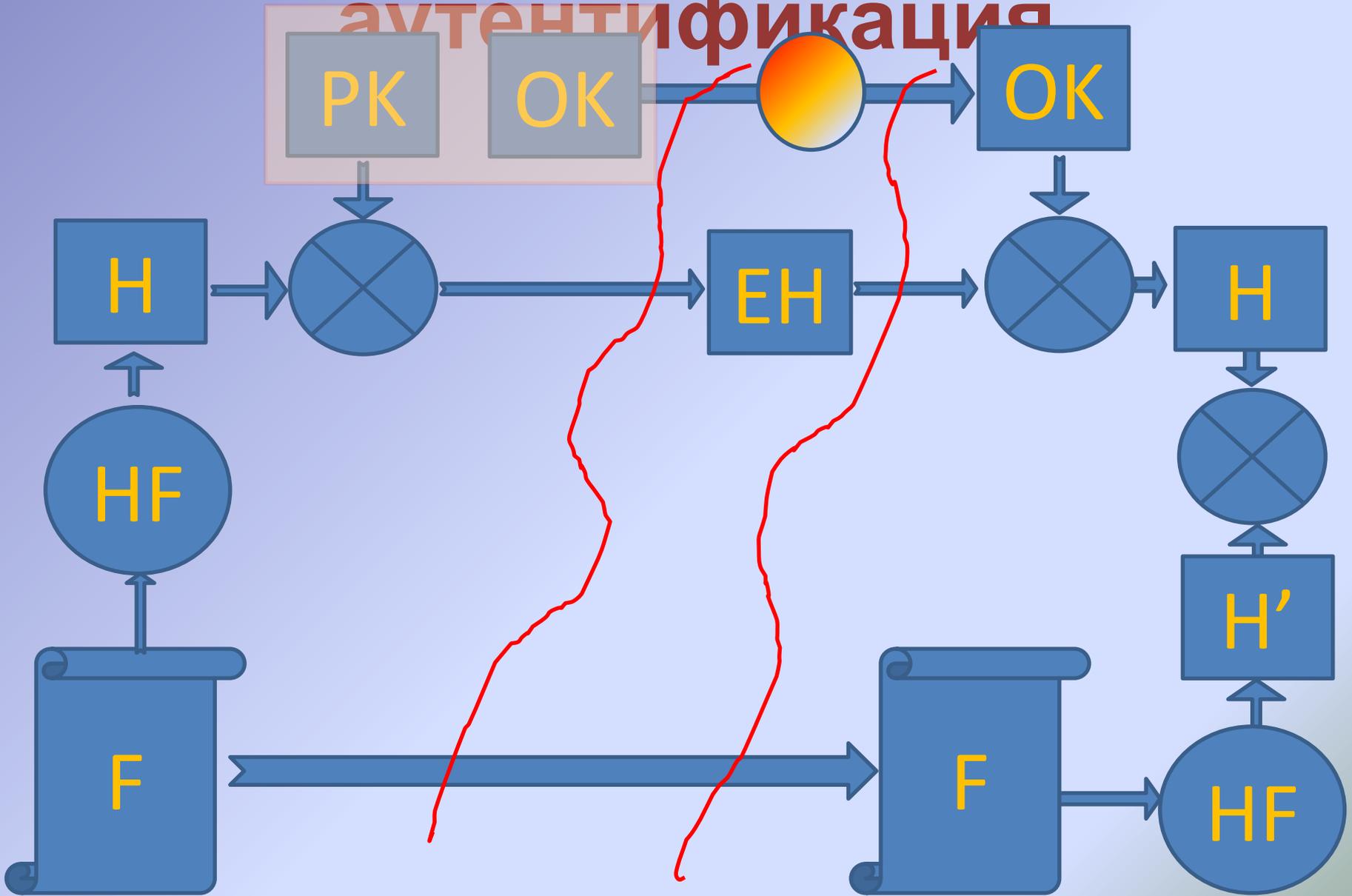
Internet Firewall VPN NAP

Конфиденциальность



Целостность и

аутентификация



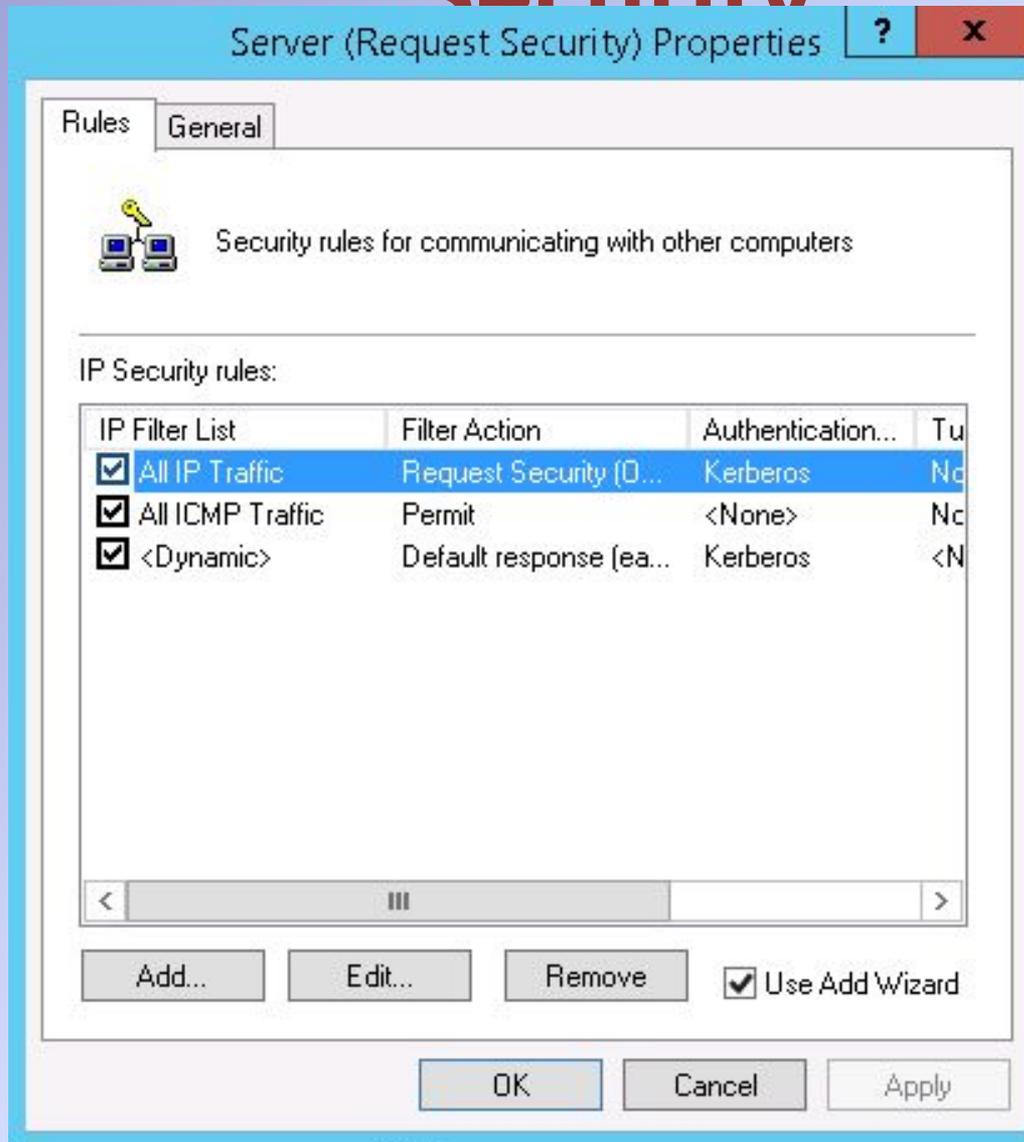
Настройка IP Security

Default Domain Policy [LON-DC1.ADATUM.COM] Policy

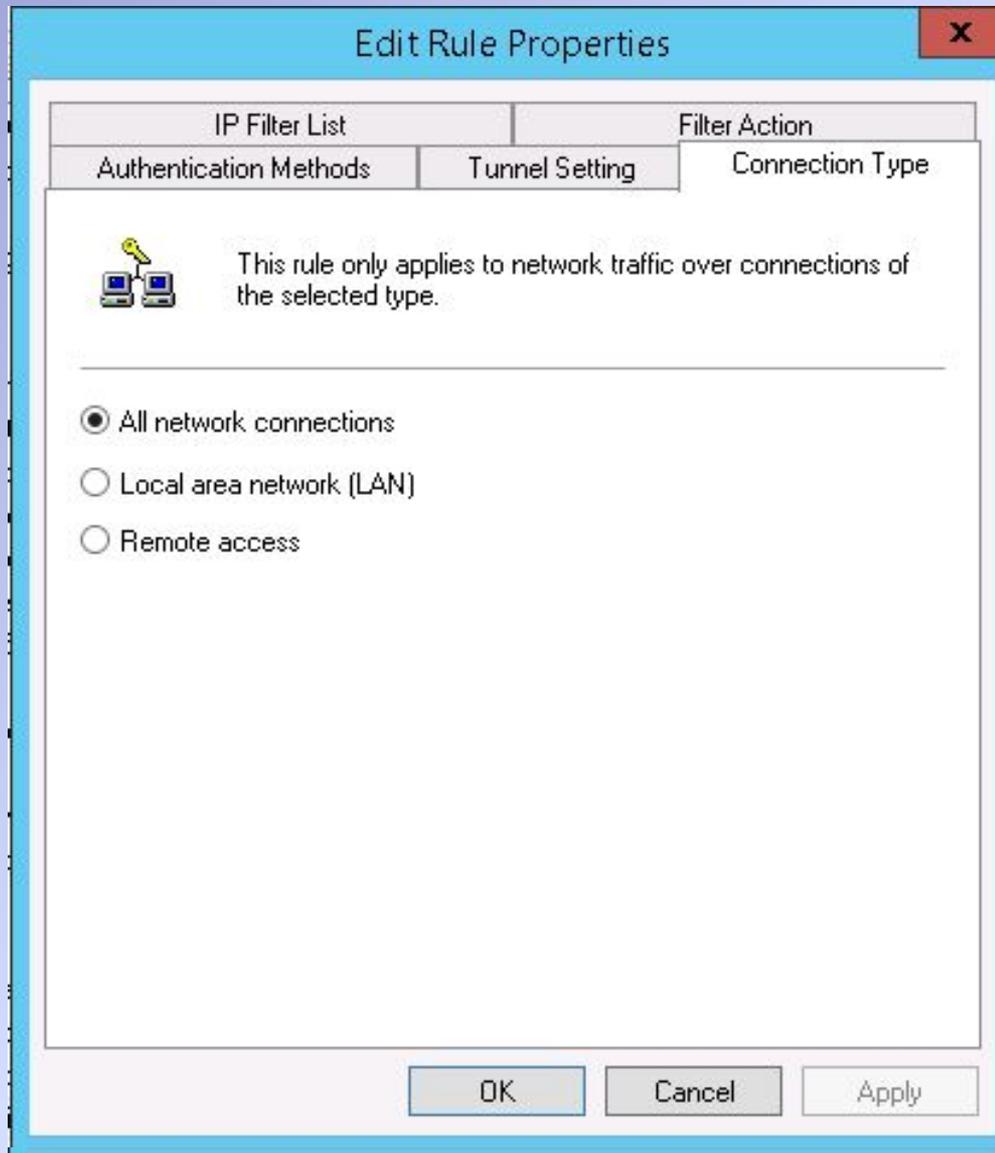
- Computer Configuration
 - Policies
 - Software Settings
 - Windows Settings
 - Name Resolution Policy
 - Scripts (Startup/Shutdown)
 - Security Settings
 - Account Policies
 - Local Policies
 - Event Log
 - Restricted Groups
 - System Services
 - Registry
 - File System
 - Wired Network (IEEE 802.3) Policies
 - Windows Firewall with Advanced Security
 - Network List Manager Policies
 - Wireless Network (IEEE 802.11) Policies
 - Public Key Policies
 - Software Restriction Policies
 - Network Access Protection
 - Application Control Policies

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



Настройка правил IP Security

Security Methods Authentication Methods

Offer these security methods when negotiating with another computer.

Security method preference order:

AH Integrity	ESP Confidential...	ESP Integrity
<None>	3DES	SHA1
<None>	3DES	MD5
<None>	DES	SHA1
<None>	DES	MD5
SHA1	<None>	<None>
MD5	<None>	<None>

Add...
Edit...
Remove
Move up
Move down

Use session key perfect forward secrecy (PFS)

Настройка аутентификации IP Security

The image shows two overlapping dialog boxes from the Windows Firewall configuration utility. The background dialog is 'Edit Rule Properties', which has tabs for 'IP Filter List' and 'Filter Action'. The 'Authentication Methods' tab is active, showing a list of authentication methods with 'Kerberos' selected. The foreground dialog is 'New Authentication Method Properties', which is used to configure the selected method. It has a tab for 'Authentication Method' and contains a description of authentication methods, a list of radio buttons for different protocols, and a text box for a preshared key.

Edit Rule Properties

IP Filter List | Filter Action

Authentication Methods | Tunnel Settings

Authentication methods specify how trust is established between computers. These are offered and accepted when negotiating an IPsec tunnel with another computer.

Authentication method preference order:

Method	Details
Kerberos	

New Authentication Method Properties

Authentication Method

The authentication method specifies how trust is established between the computers.

Active Directory default (Kerberos V5 protocol)

Use a certificate from this certification authority (CA):

Exclude the CA name from the certificate request

Enable certificate to account mapping

Use this string (preshared key):

123451234512345

OK

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

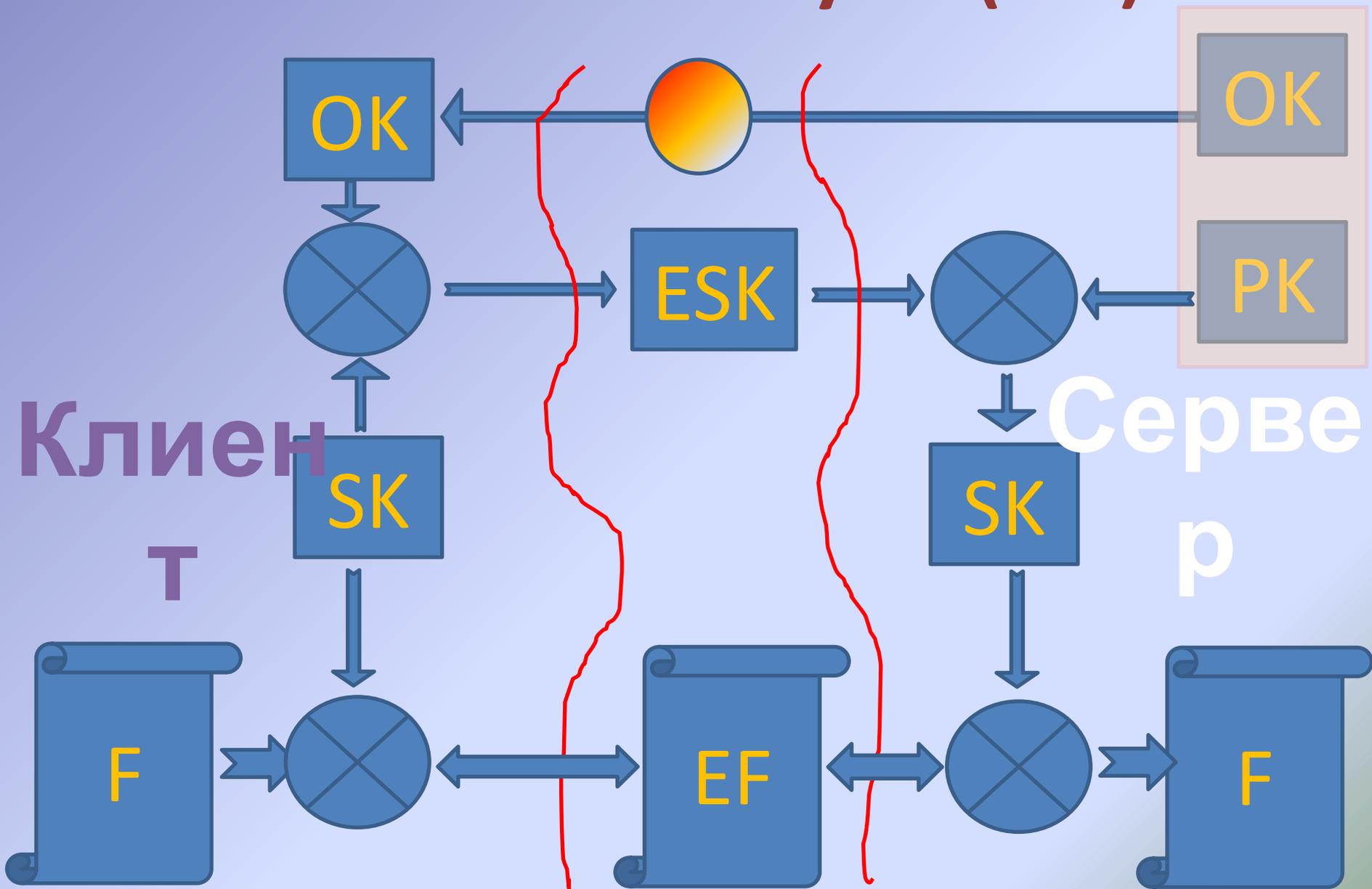
Параметры	Статистика
✗ Активных сопоставлений безопаснос...	0
✗ Разгруженные операции сопоставлен...	0
✗ Не законченные операции с ключами	0
✗ Дополнения по ключам	0
✗ Удалений ключей	0
✗ Повторное создание ключей	0
✗ Активных туннелей	0
✗ Сбойных пакетов SPI	0
✗ Незашифрованных пакетов	0
✗ Непроверенных 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

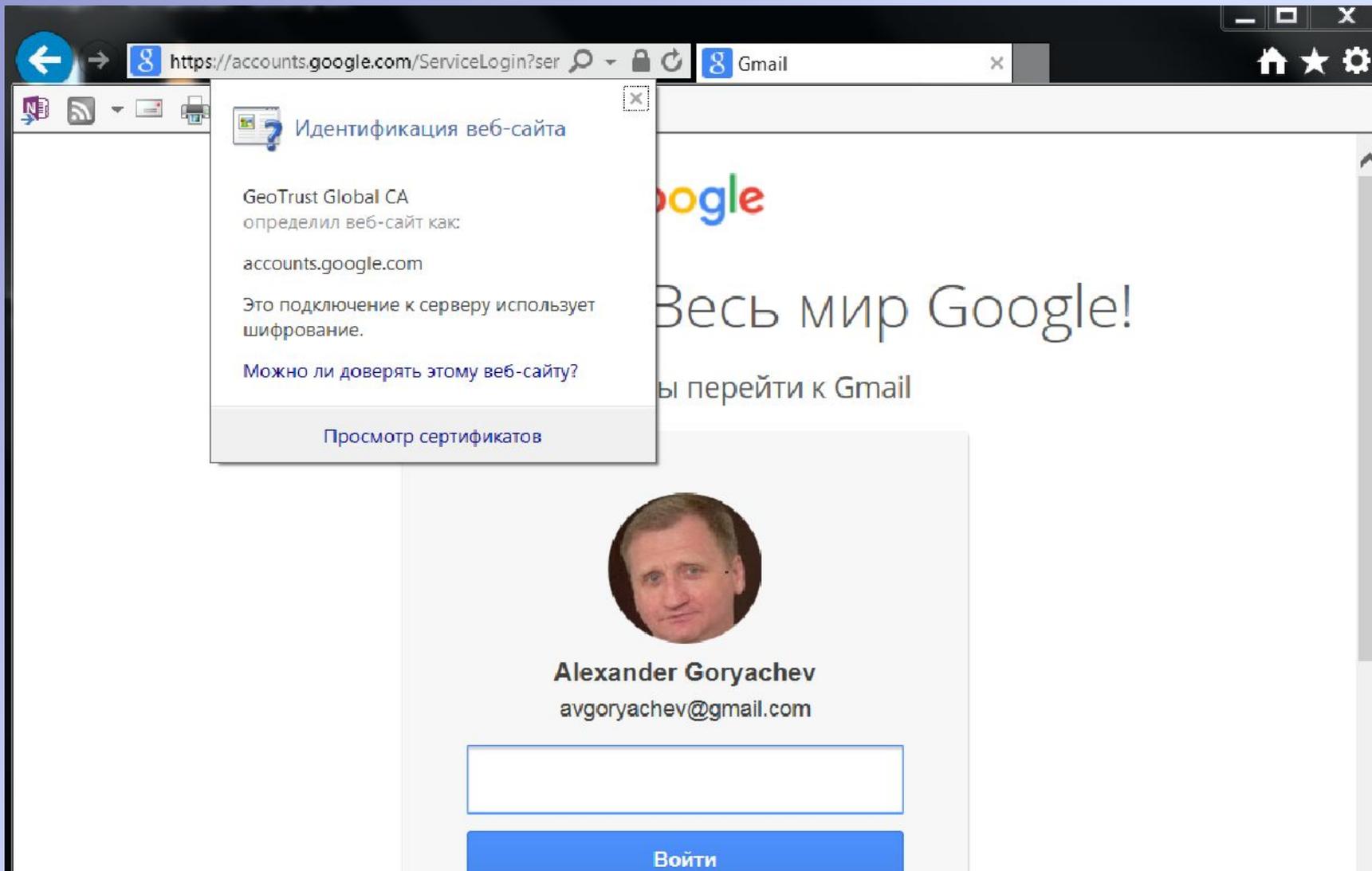
Статистика ▲

Дополнительные дей... ▶

Secure Socket Layers (SSL)



Установка соединения SSL



Сертификаты SSL

Консоль1 - [Корень консоли\Сертификаты - текущий пользователь\Доверенные корневые центры сертификации\Серти...

Файл Действие Вид Избранное Окно Справка

Основной режим

- Универсальные фильтры
- Специальные фильтры
- Политики IKE
- Статистика
- Сопоставления безопасн...

Быстрый режим:

- Универсальные фильтры
- Специальные фильтры
- Политики согласования
- Статистика
- Сопоставления безопасн...

Сертификаты - текущий пользова...

- Личное
- Доверенные корневые центр...
- Доверительные отношения в г...
- Промежуточные центры серти...
- Объект пользователя Active Di...
- Доверенные издатели
- Сертификаты, к которым нет д...
- Сторонние корневые центры с...
- Доверенные лица
- Другие пользователи
- Запросы заявок на сертификат
- Доверенные корневые сертиф...

Кому выдан

- Deutsche Telekom Root ...
- DigiCert Assured ID Root...
- DigiCert Global Root CA
- DigiCert High Assurance ...
- DST Root CA X3
- Entrust Root Certification...
- Entrust Root Certification...
- Entrust.net Certification ...
- Equifax Secure Certificat...
- GAV-HOME2-CA
- GAV-HOME2-CA
- GeoTrust Global CA
- GeoTrust Primary Certific...
- GeoTrust Primary Certific...
- GlobalSign
- GlobalSign
- GlobalSign Root CA
- Go Daddy Class 2 Certific...
- Go Daddy Root Certificat...
- GTE CyberTrust Global R...
- Microsoft Authenticode(t...
- Microsoft Root Authority
- Microsoft Root Certificat...

Сертификат

Общие Состав Путь сертификации

Сведения о сертификате

Этот сертификат предназначен для:

- Обеспечивает получение идентификации от удаленного компьютера
- Подтверждает удаленному компьютеру идентификацию вашего компьютера
- Защищает сообщения электронной почты
- Подтверждает, что программное обеспечение

Кому выдан: GeoTrust Global CA

Кем выдан: GeoTrust Global CA

Действителен с 21. 05. 2002 **по** 21. 05. 2022

Заявление поставщика

Подробнее о [сертификатах](#)

ОК

Хранилище Доверенные корневые центры сертификации содержит 49 с...

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

The image shows a Windows Certificate Manager window with the 'Advanced Key Usage' tab selected. The certificate details are as follows:

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 субь...	DNS-имя=login.live.com, DNS-...
Идентификатор ключа cv	7f ef 81 02 01 5b dd 9a 8d be

Below the table, the following key usage entries are listed:

- 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 Autentication HIDS-HIPS

PKI

AD

Передача

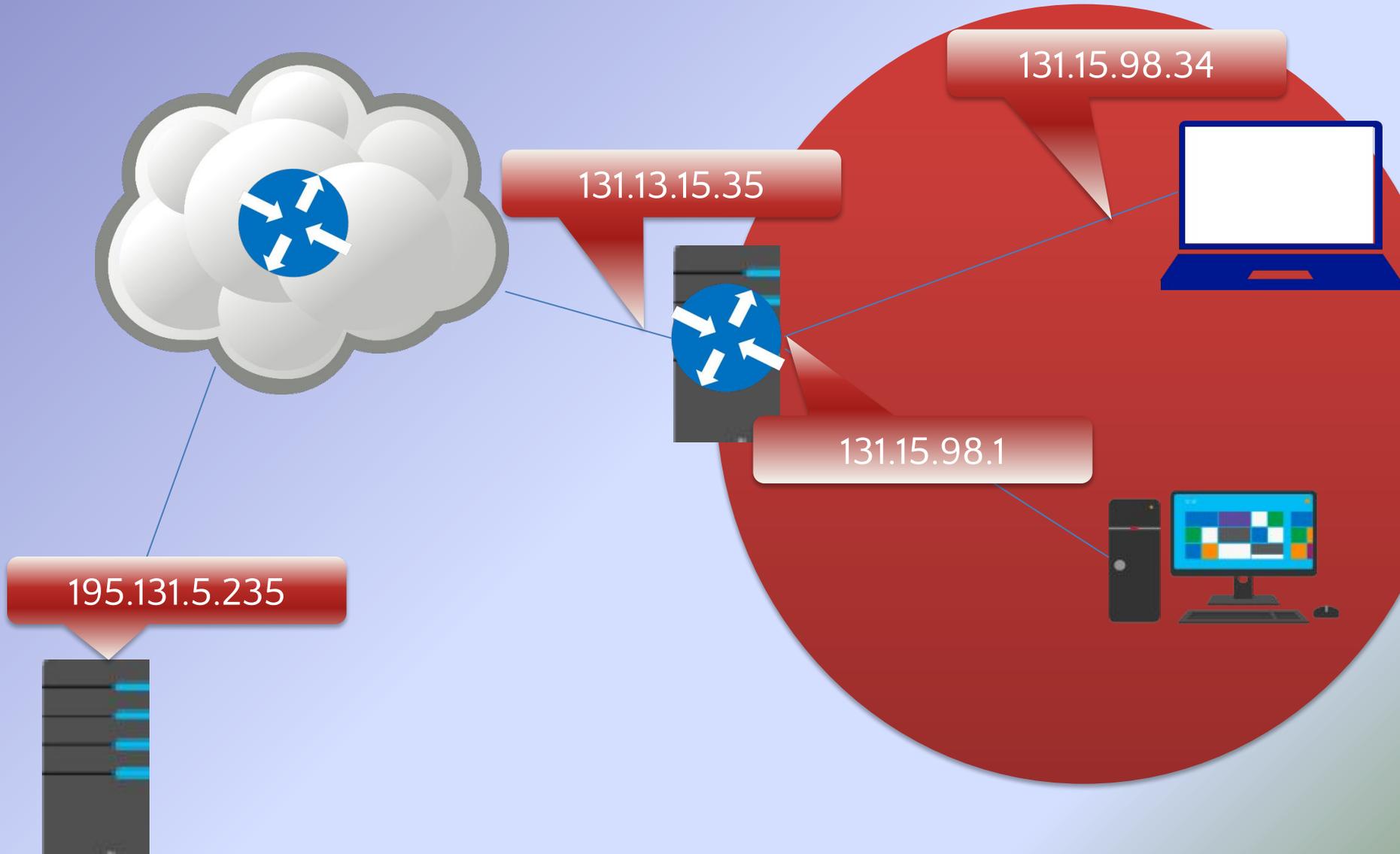
Intranet Routing IPsec SSL RMS NIDS-NIPS

Internet Firewall VPN NAP

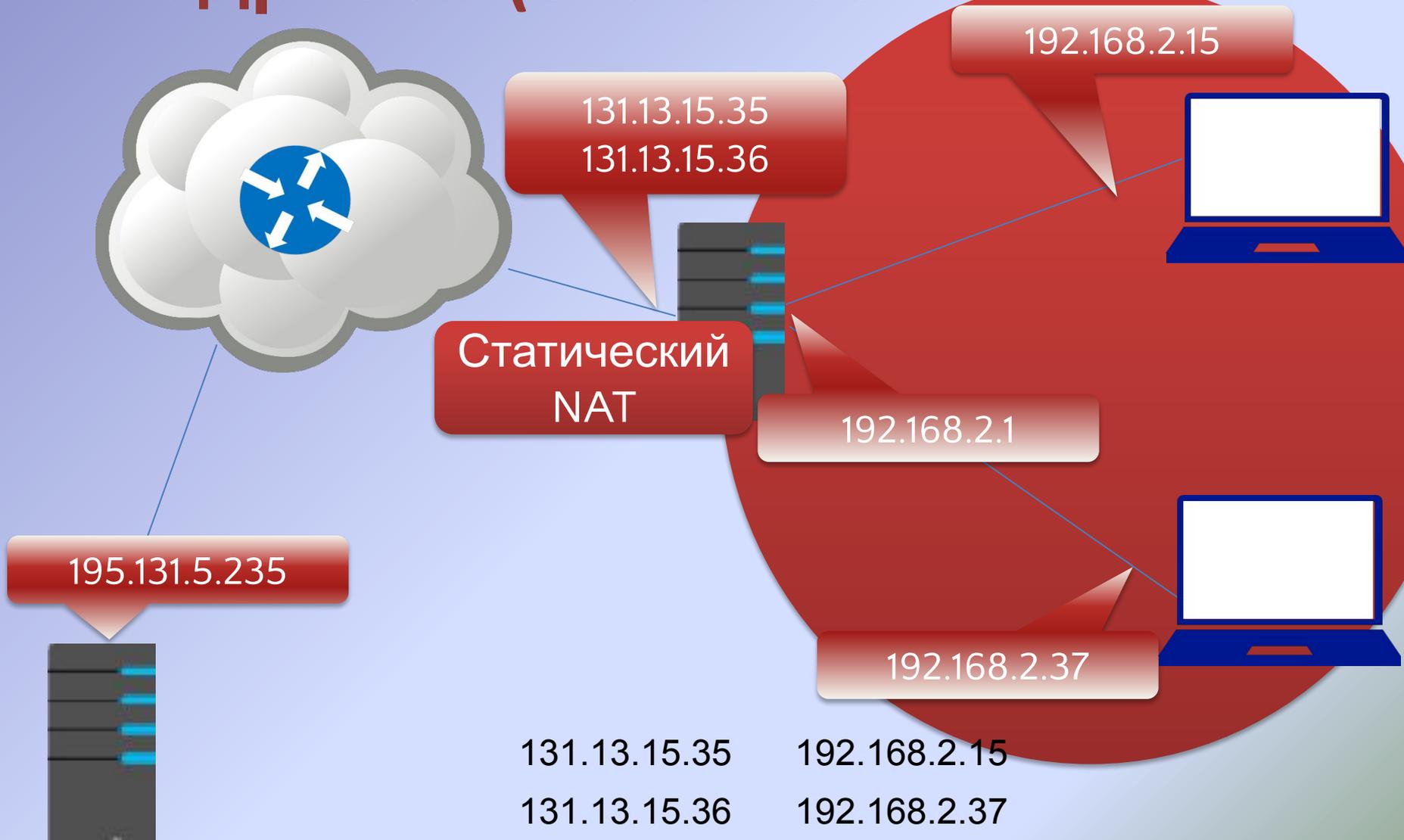
Технологии выхода в Интернет из корпоративной сети

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

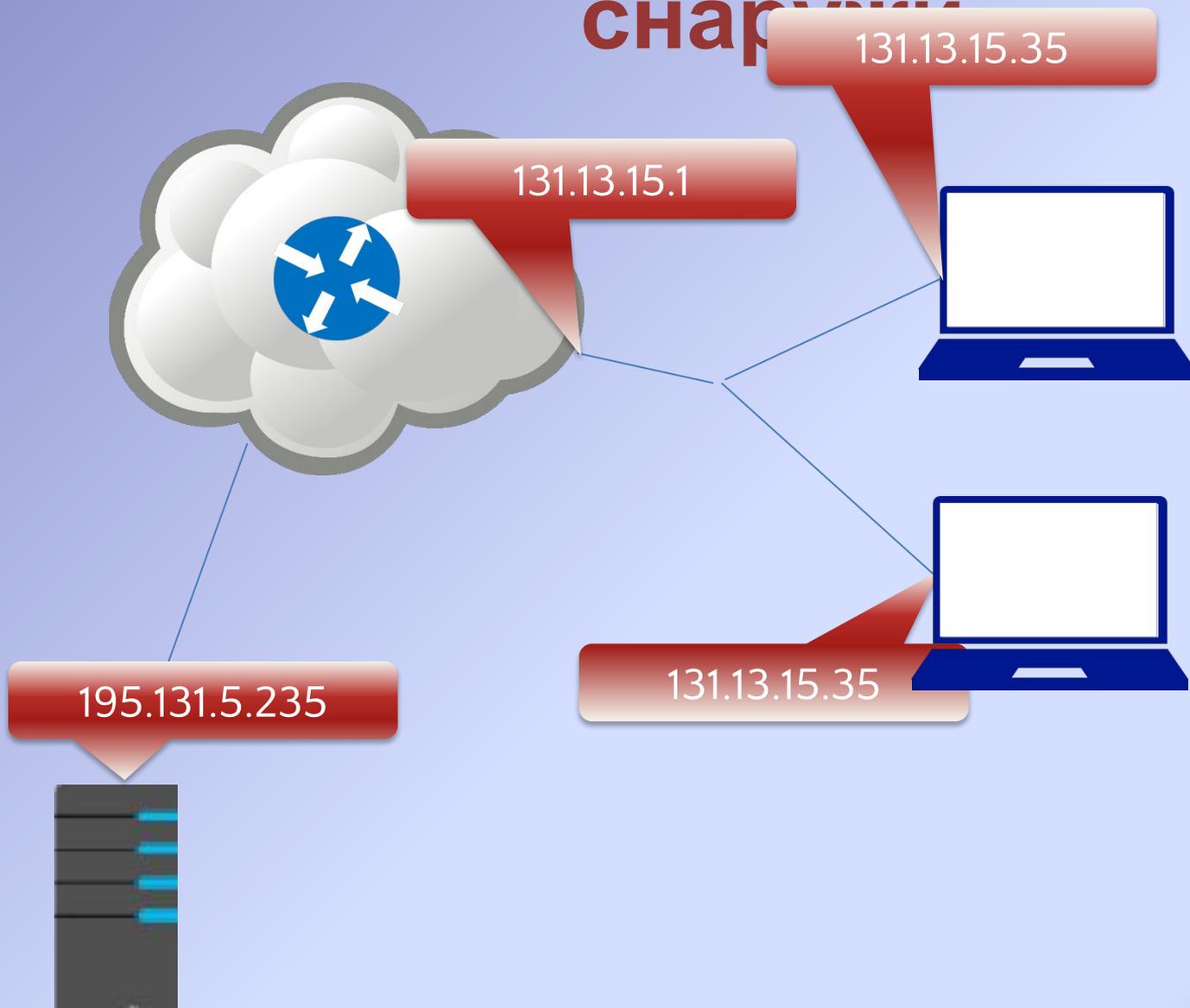
Маршрутизация



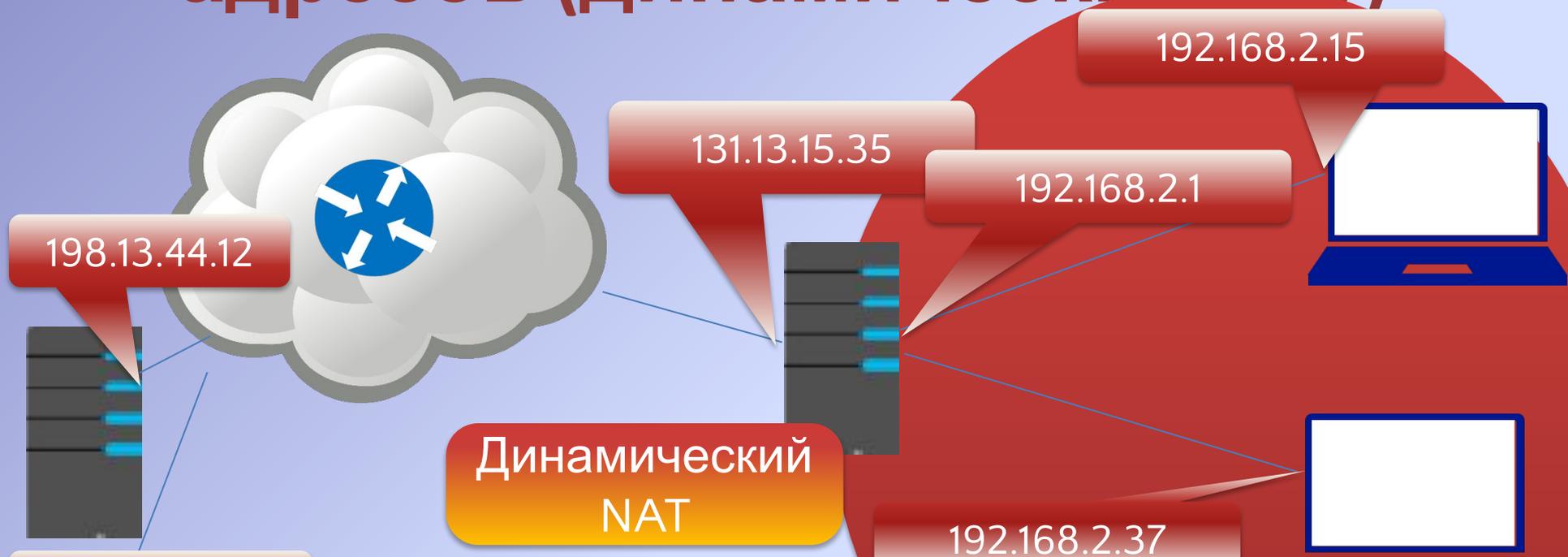
Статическая трансляция адресов (статический NAT)



Статический NAT – как выглядит снаружи



Динамическая трансляция адресов (динамический NAT)



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	

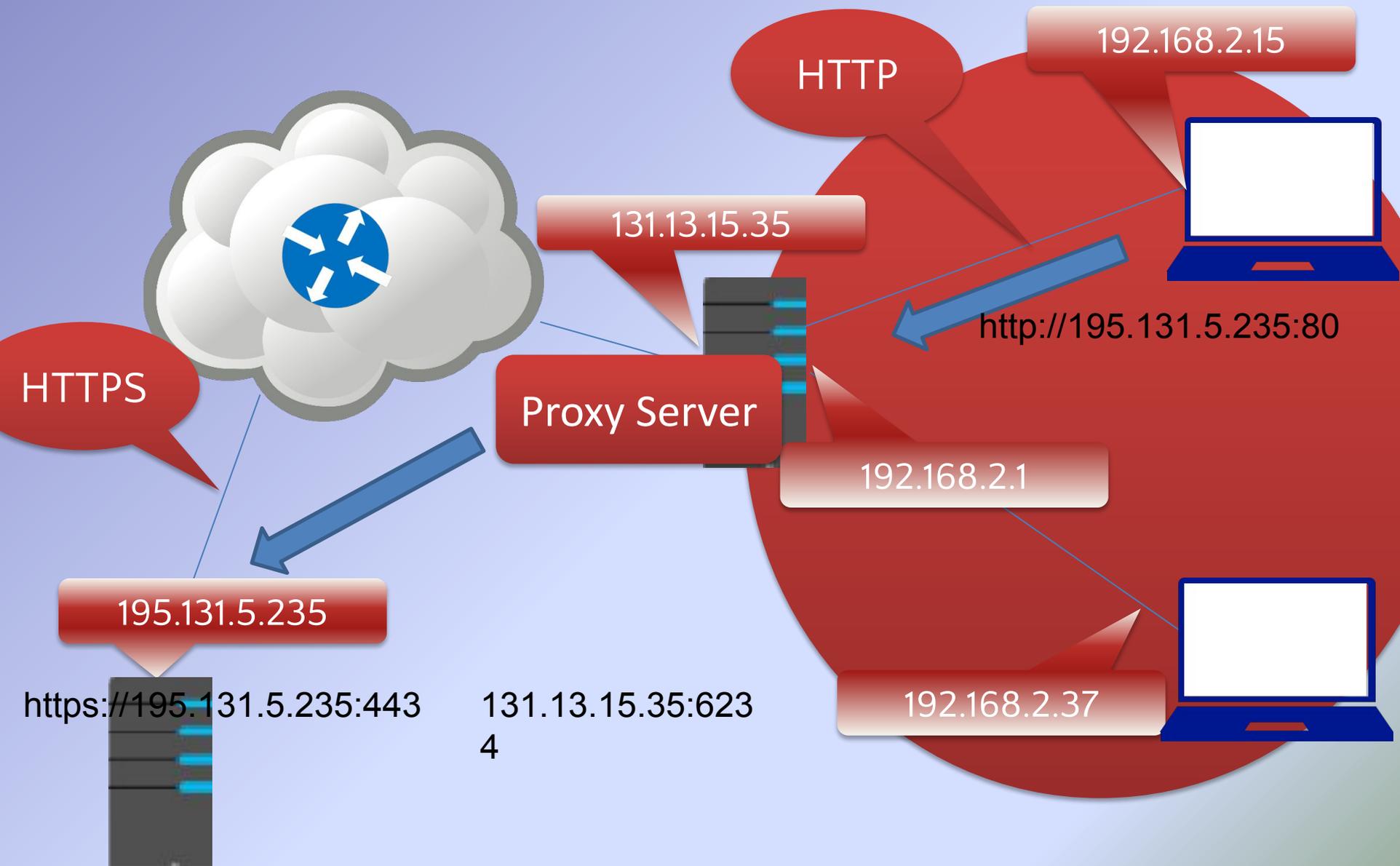
Пакет прямой:

Пакет ответный:

Отправитель: 198.13.44.12:80

Получатель: 131.13.15.35:34555

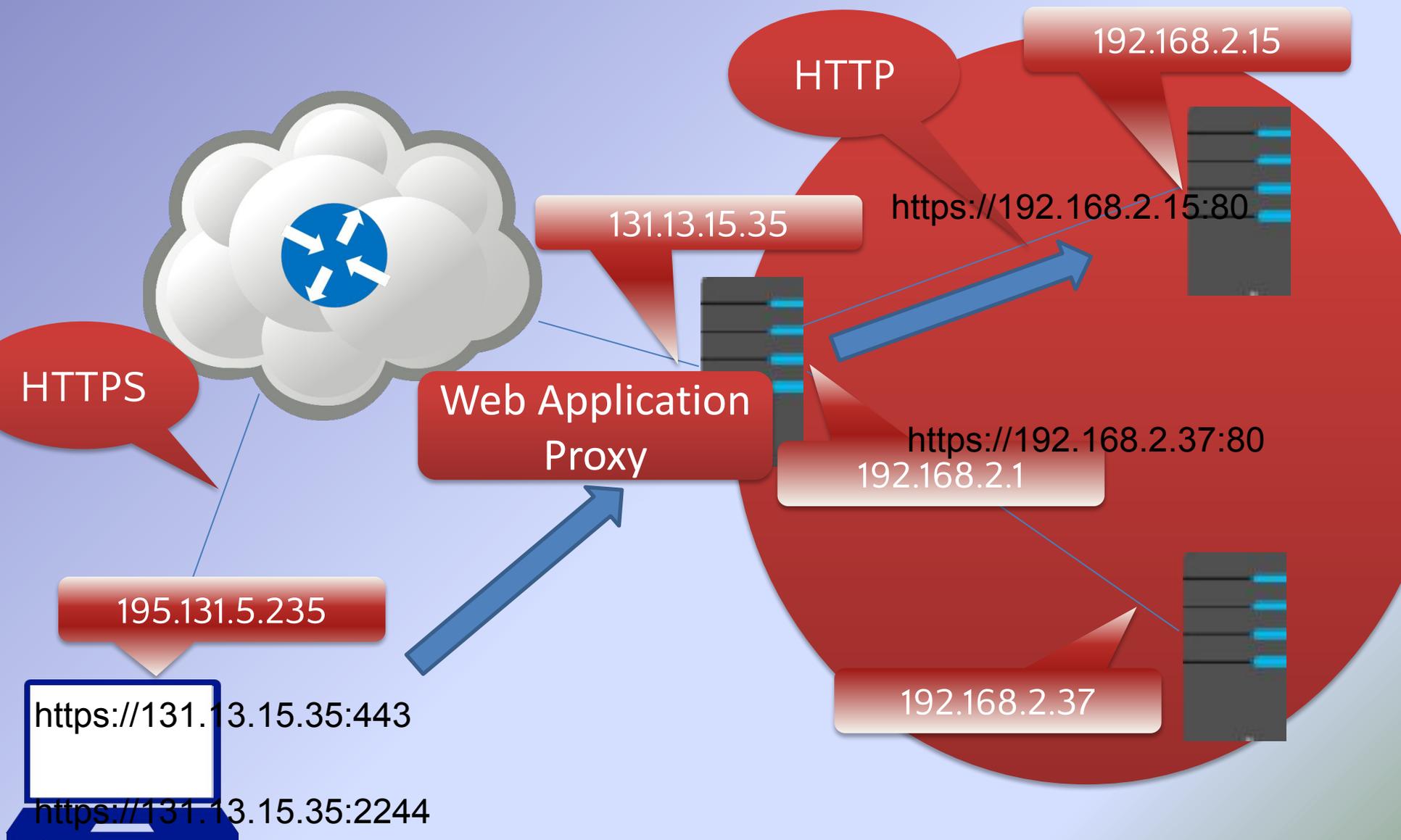
Прокси (Proxy)



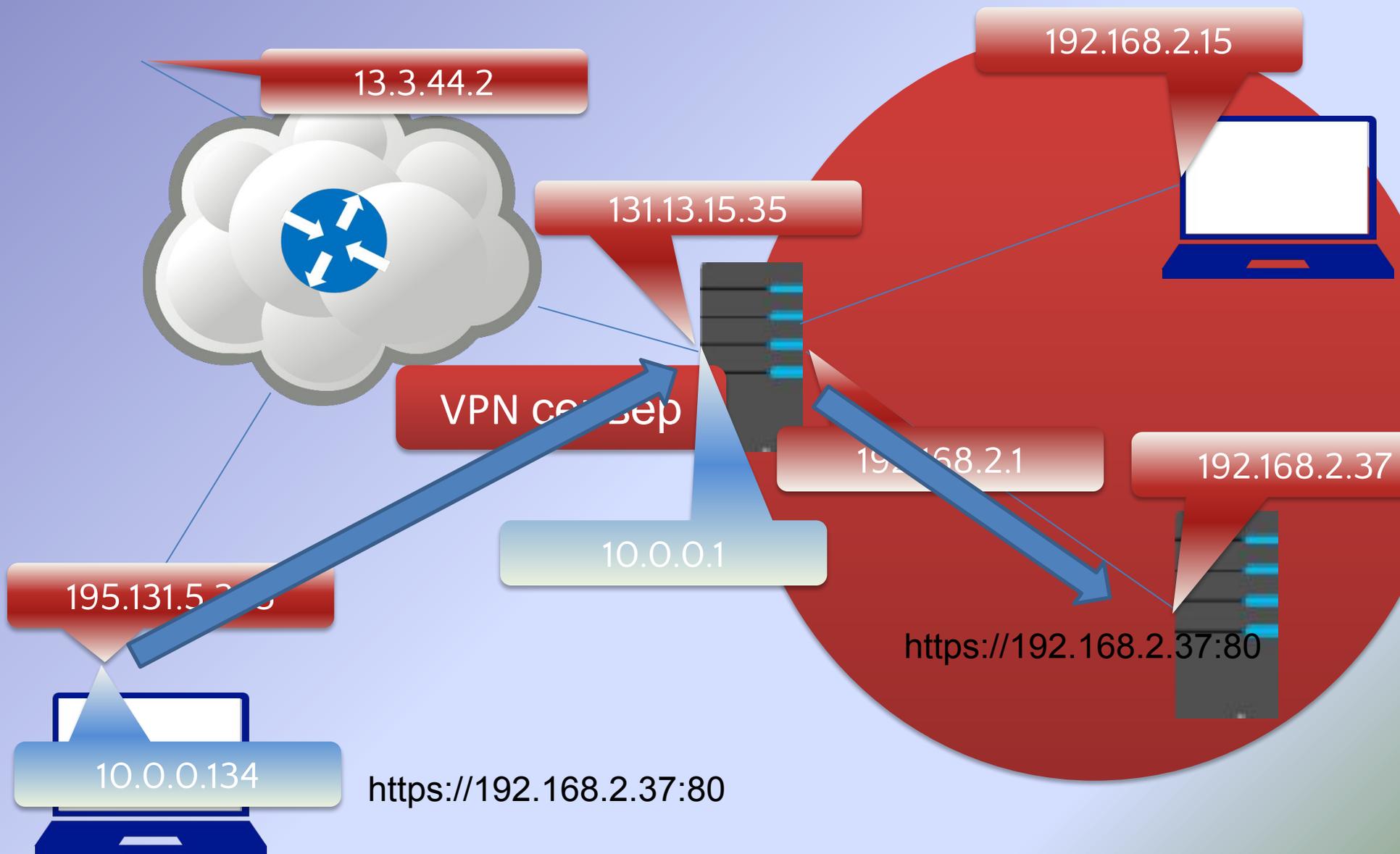
Технологии доступа из Интернет к ресурсам корпоративной сети

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

Web Application Proxy (Обратный прокси)

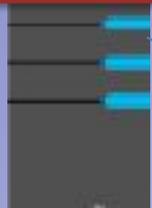


Виртуальные частные сети (VPN)



Виртуальные частные сети (VPN)

VPN сервер

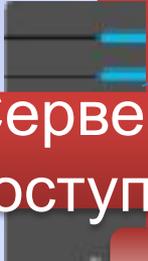


13.3.44.2



131.13.15.35

Сервер доступа



192.168.2.1

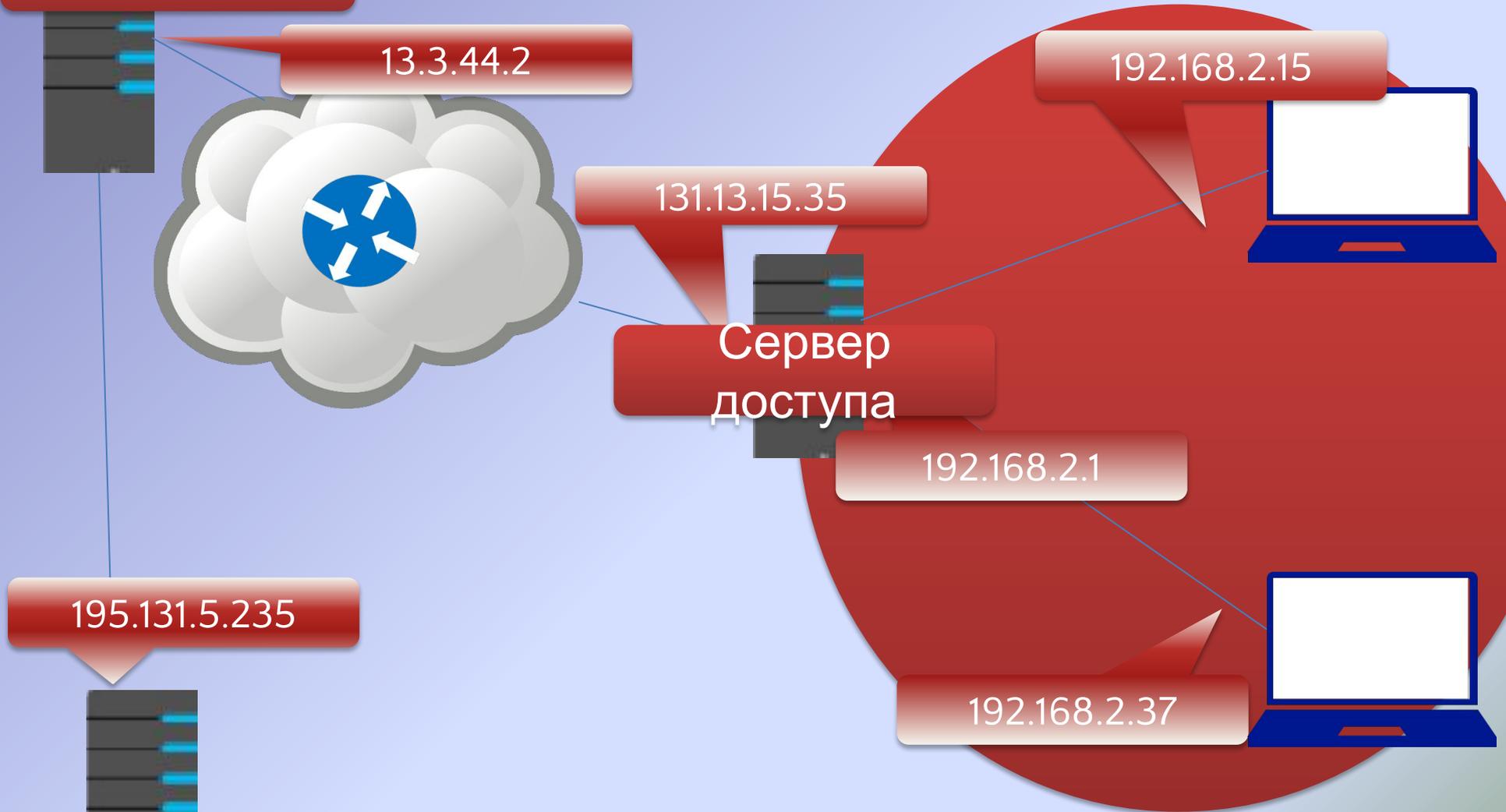
192.168.2.15



195.131.5.235



192.168.2.37



Настройка VPN в RRAS

Маршрутизация и удаленный доступ

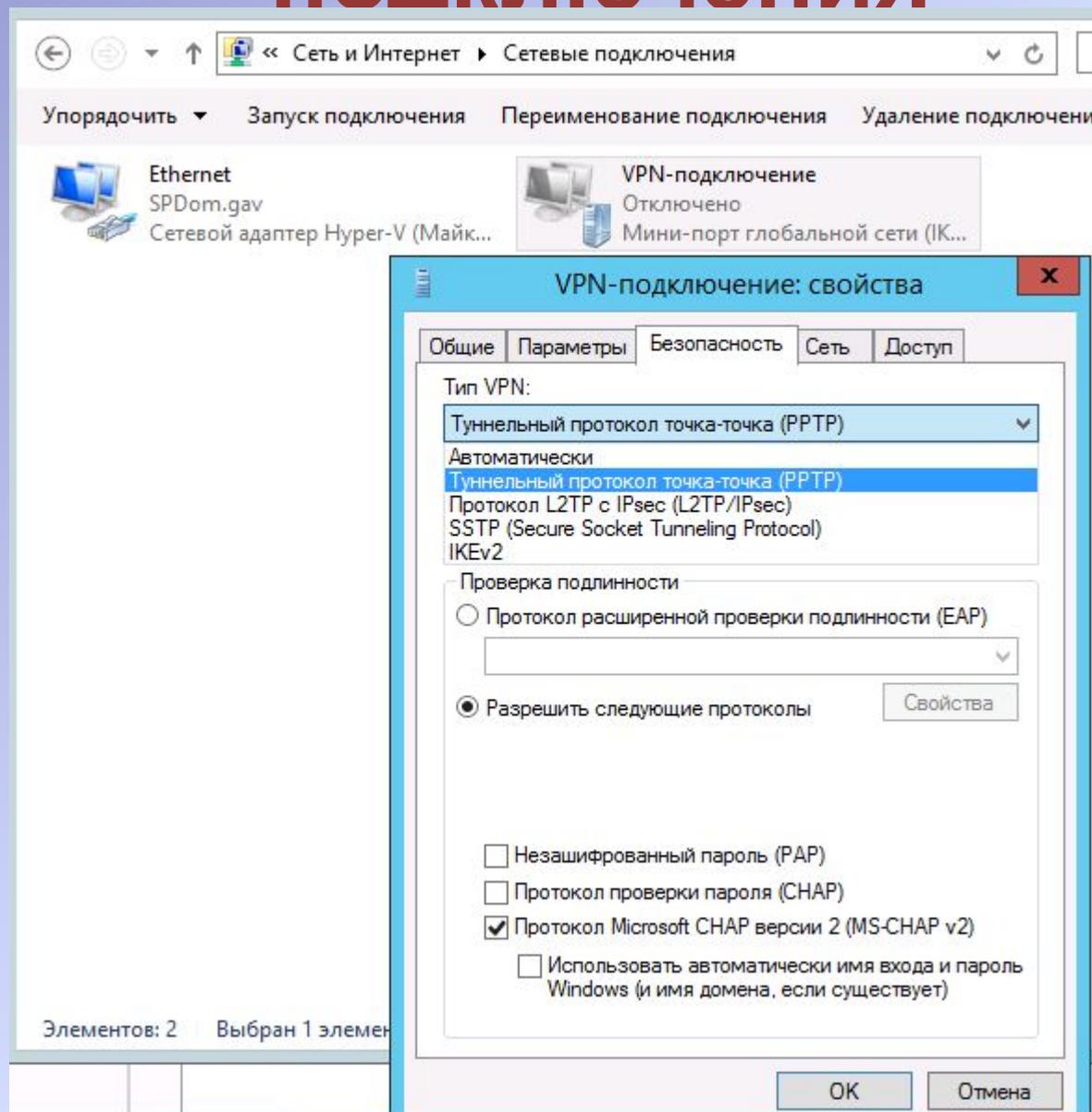
Файл Действие Вид Справка

Маршрутизация и удаленный доступ

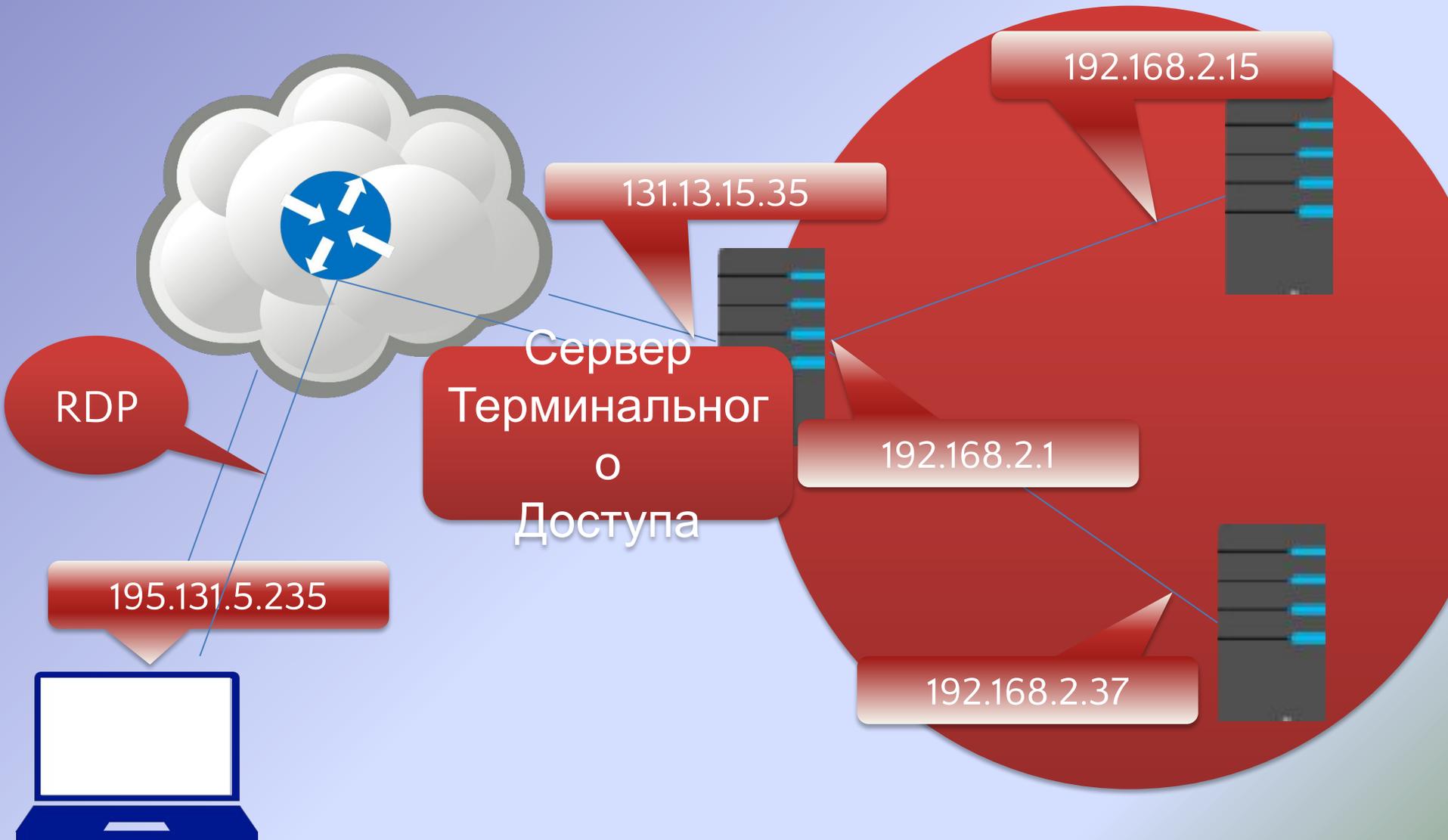
- Состояние сервера
- W2K12R2SQL (локально)
 - Интерфейсы сети
 - Порты
 - Клиенты удаленного доступа (0)
 - Политики ведения журналов удаленно
 - IPv4
 - IPv6
 - Общие
 - Статические маршруты

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

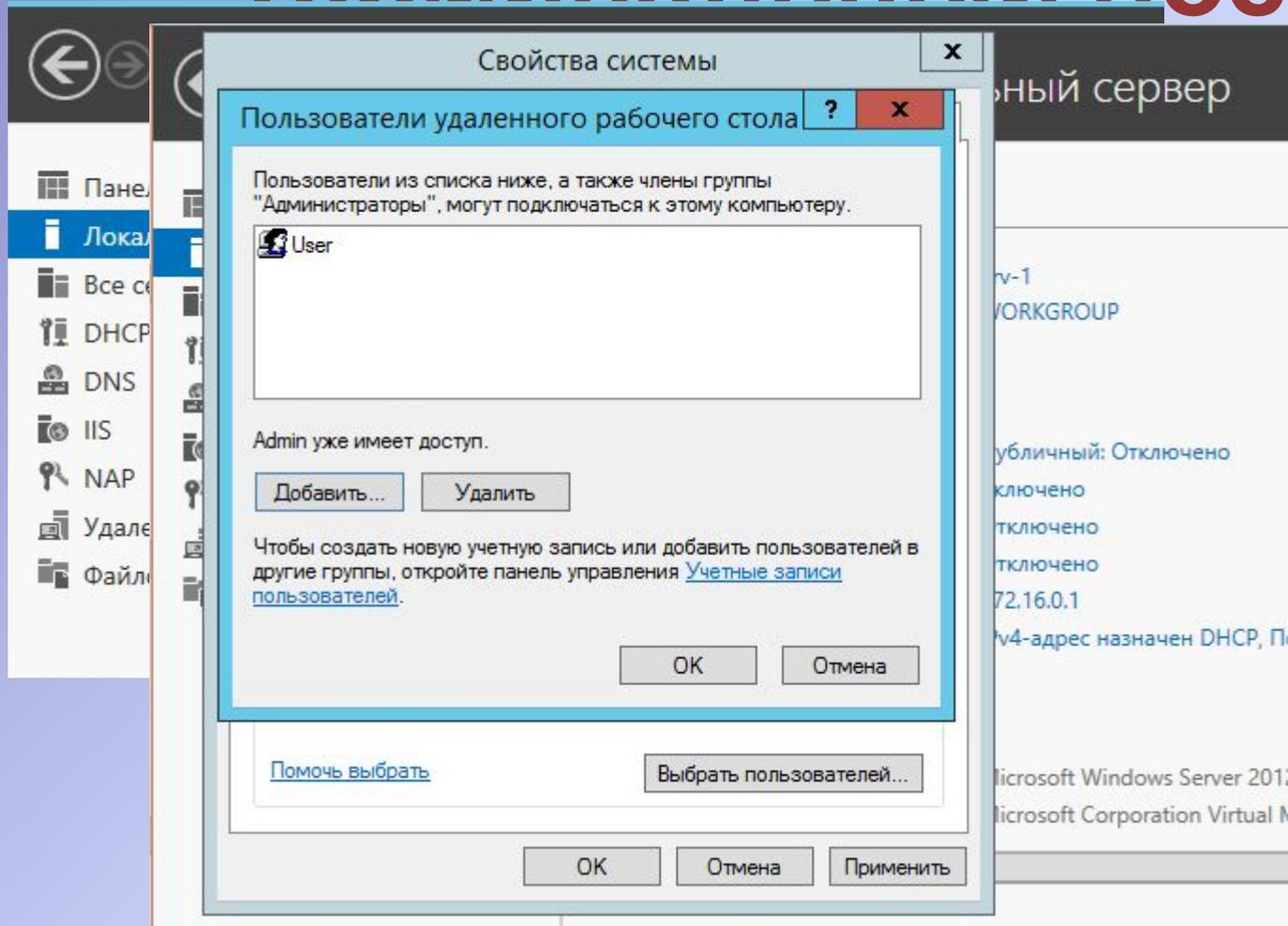
Настройка параметров подключения



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 Нурер-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 Нурер-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

```

Файл Главная Поделиться Вид

Сеть > 172.31.160.129 > Shara

Имя

- Избранное
- Загрузки
- Недавние места
- Рабочий стол
- Этот компьютер
- Сеть

FileOnShara

1 элемент



Корзина

```
Microsoft Windows [
(c) Корпорация Майкрософт
C:\Users\User>ipconfig /all

Настройка протокола IP для сети

Имя компьютера . . . . . : User-PC
Основной DNS-суффикс . . . . . :
Тип узла . . . . . : 1
IP-маршрутизация . . . . . : включено
WINS-прокси включено . . . . . :
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



User
Вход

Shara

Файл Главная Поделиться Вид

Сеть > 172.31.160.129 > Shara

Имя	Дата изменения	Тип
FileOnShara	12.04.2018 9:05	Текстовый документ

Диспетчер задач

Файл Параметры Вид

Процессы Производительность Пользователи Подробности Службы

Пользователь	Состояние	ЦП	Память
User (10)			
Диспетчер задач		0%	64,8 МБ
Диспетчер окон рабочег...		0%	5,8 МБ
Обработчик команд Win...		0%	15,6 МБ
Обработчик команд Win...		0%	0,3 МБ
Окно консоли узла		0%	0,3 МБ
Окно консоли узла		0%	0,8 МБ
Проводник		0%	0,9 МБ
Программа входа в систе...		0%	37,0 МБ
Процесс исполнения кли...		0%	0,8 МБ
Хост-процесс для задач ...		0%	1,0 МБ
		0%	2,1 МБ

1 элемент



Спасибо за внимание!

Сертификаты. Инфраструктура шифрования с открытым ключом (PKI)

Горячев Александр Вадимович
Доцент кафедры ИБ
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 Autentication HIDS-HIPS

PKI

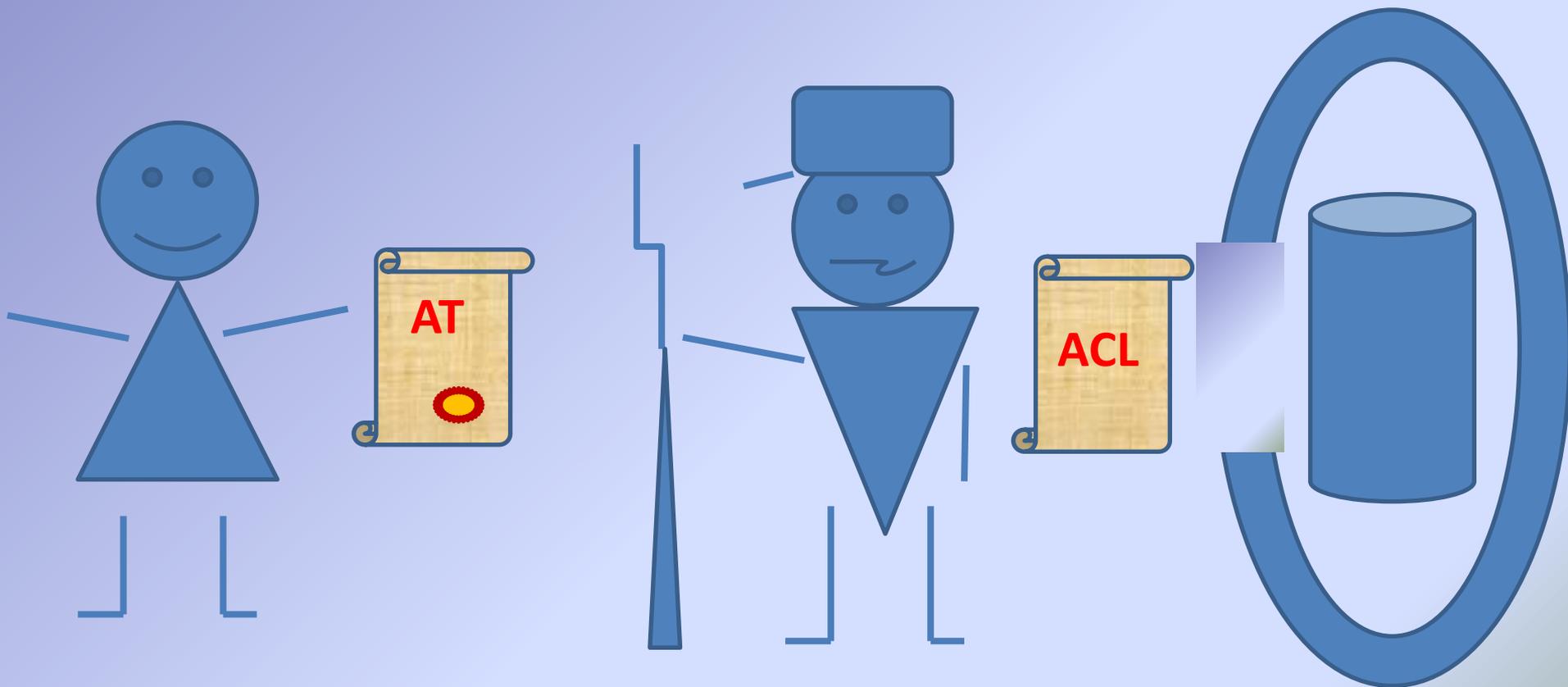
Передача

Intranet Routing IPsec RMS NIDS-NIPS

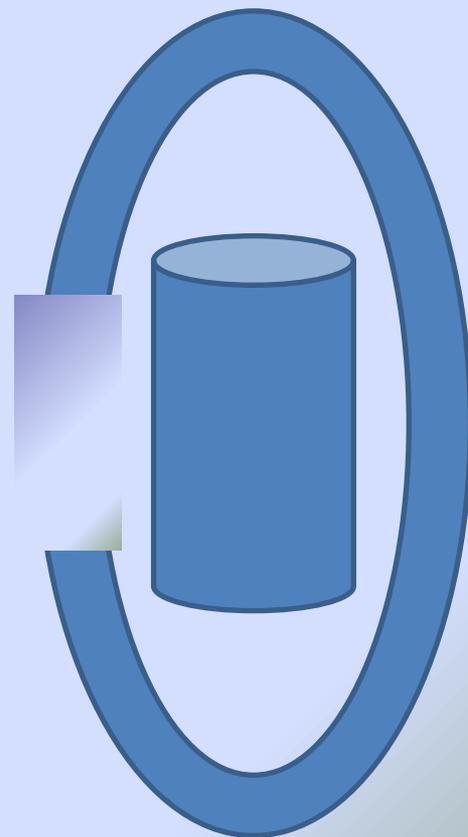
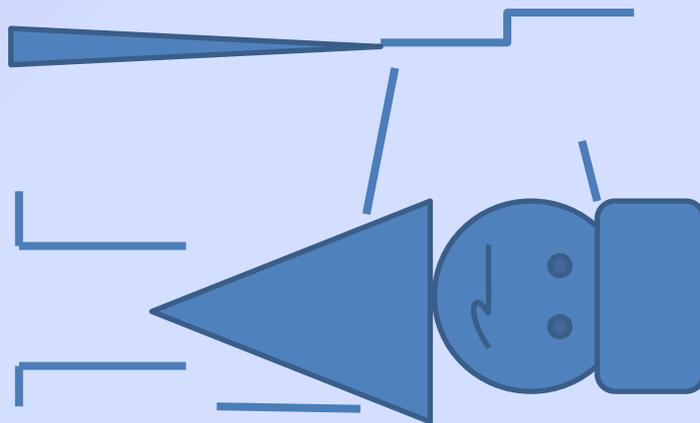
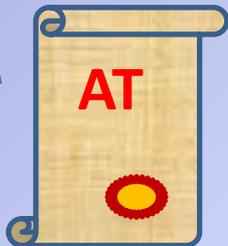
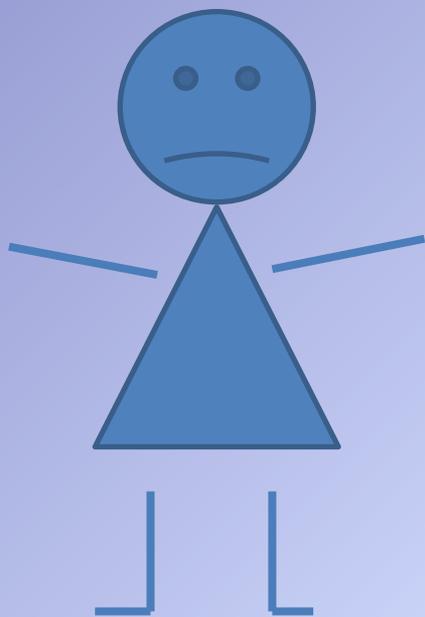
Internet Firewall VPN NAP

AD

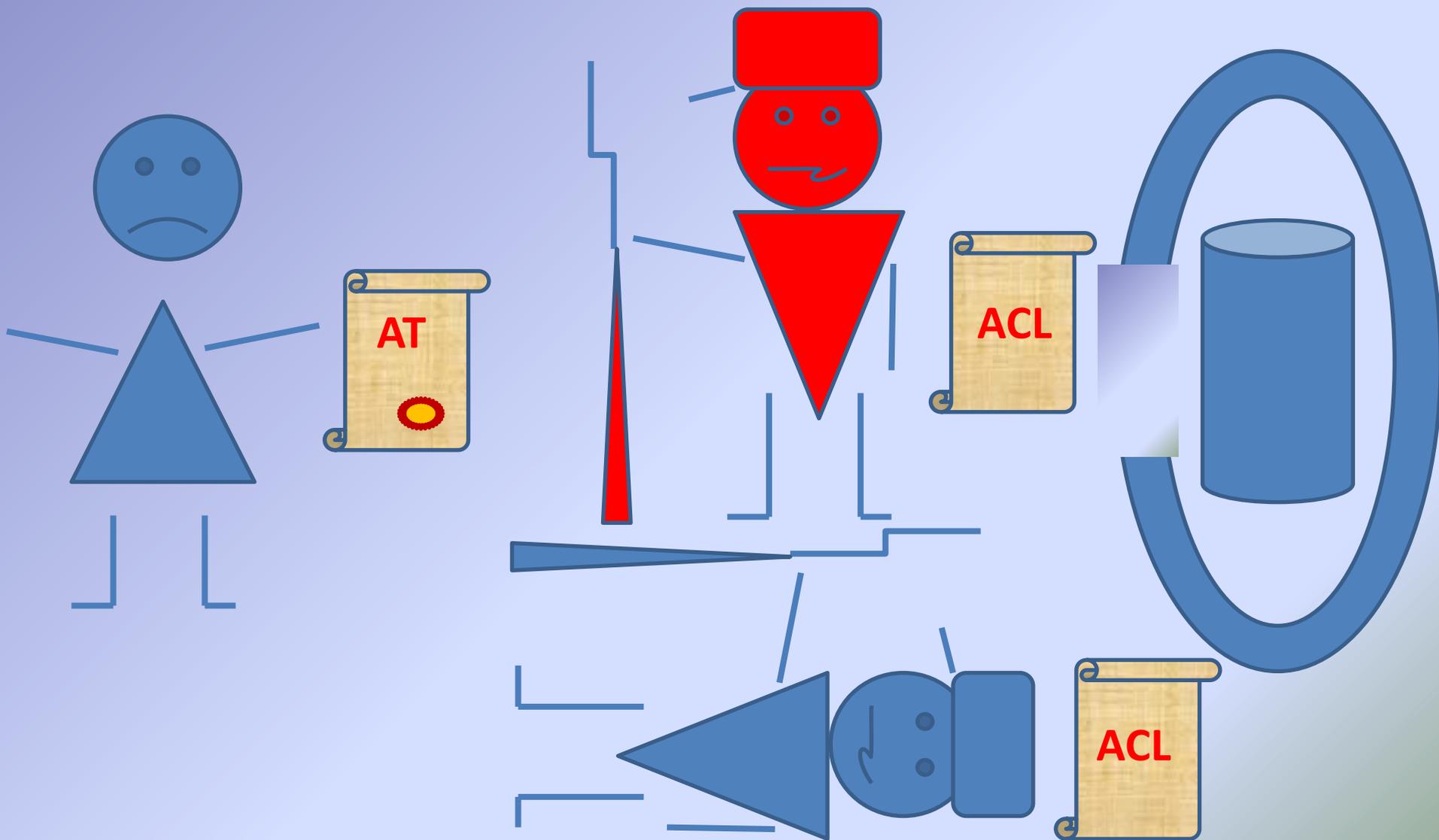
Список контроля доступа



Список контроля доступа



Список контроля доступа

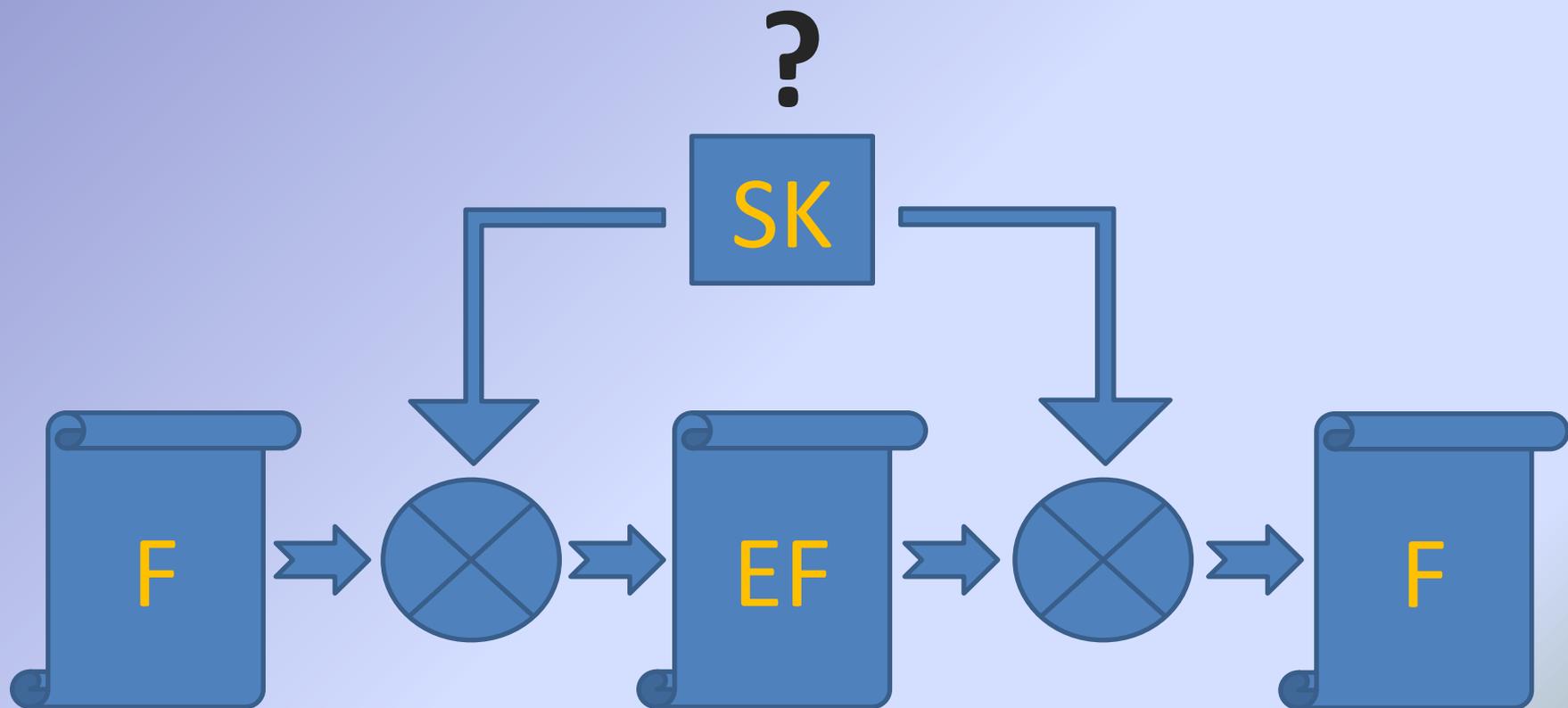


Шифрование с симметричным КЛЮЧОМ

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

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

Простейший вариант



Шифрование с асимметричным ключом (открытым и закрытым ключами)

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

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

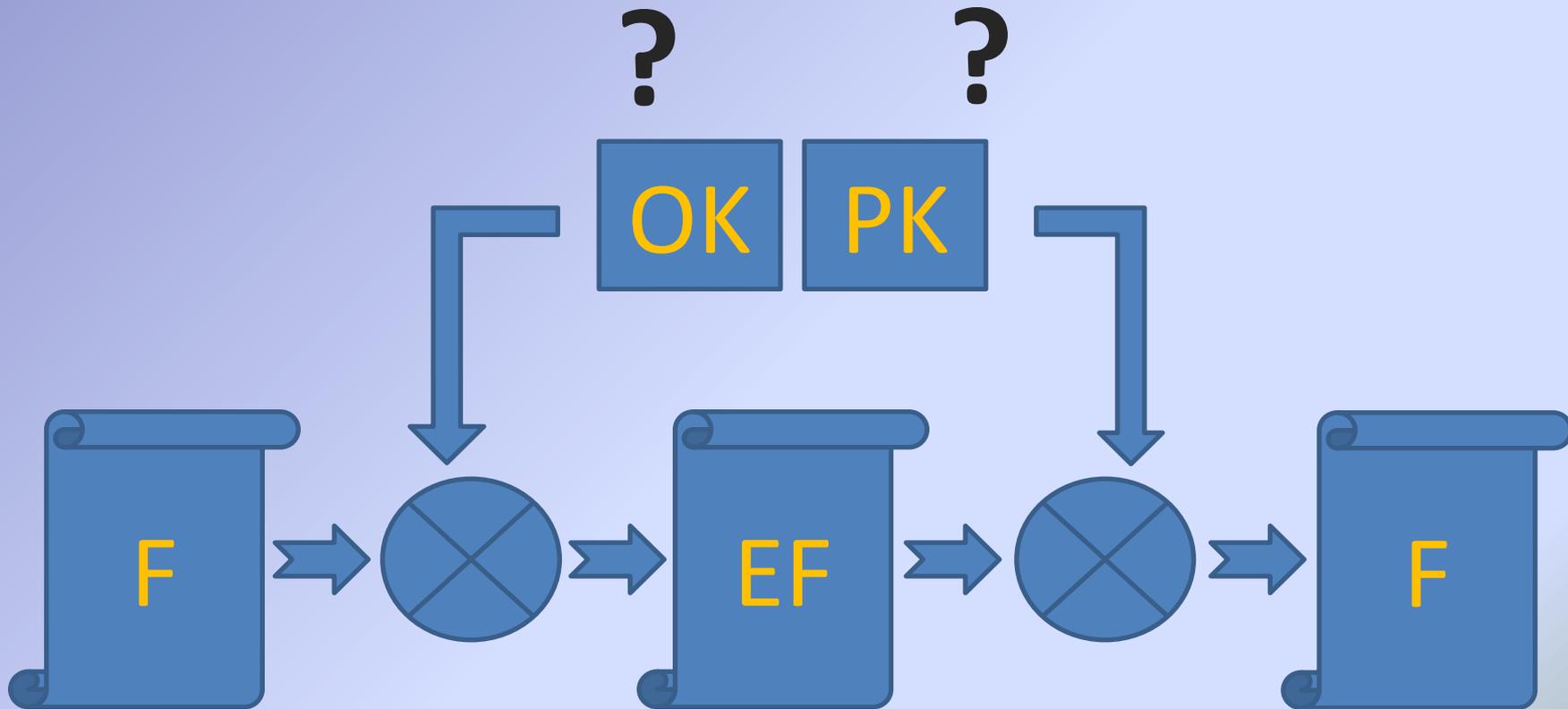
$$T^{-1}(e, p) = a$$

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

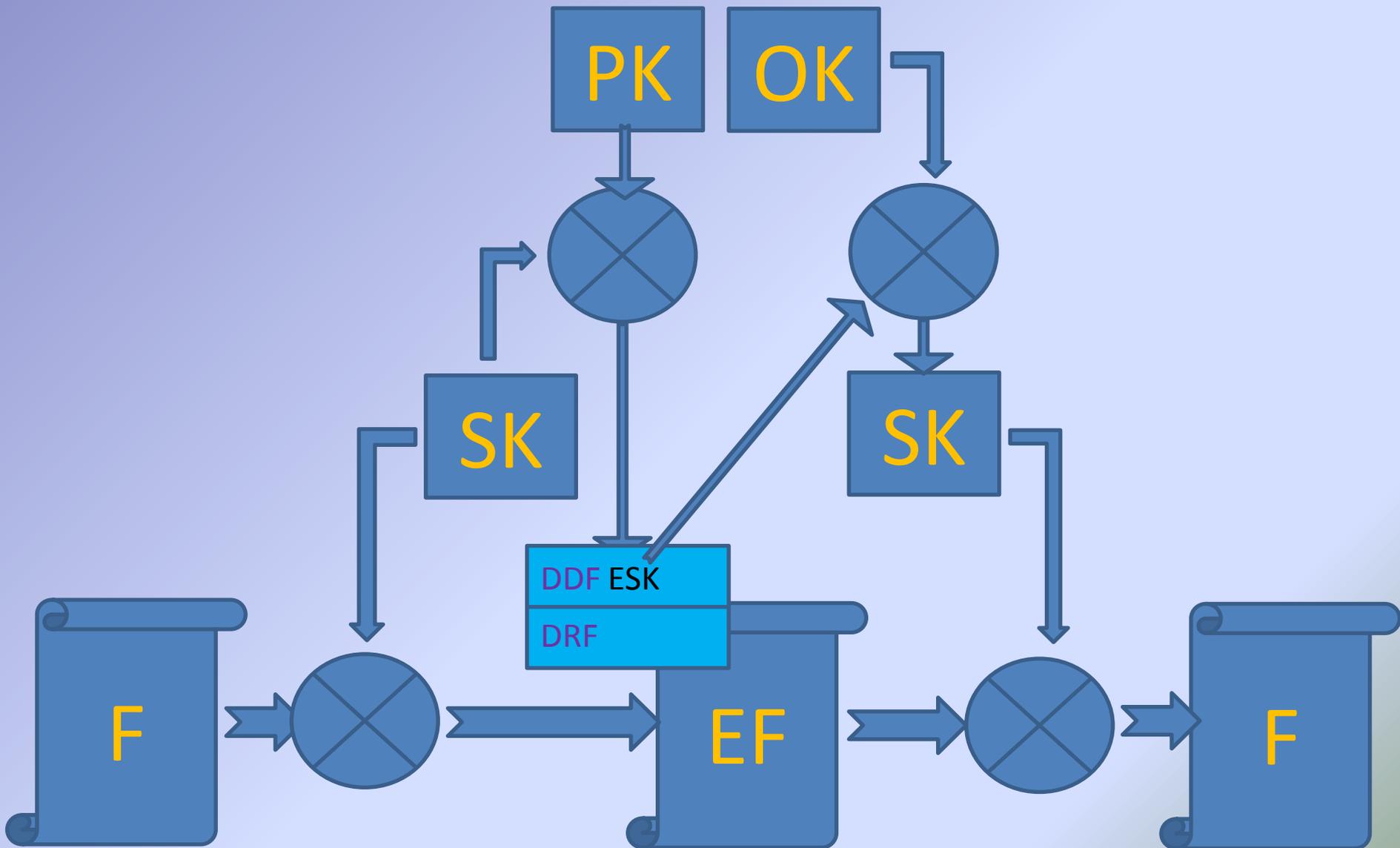
$$T(a, p) = e$$

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

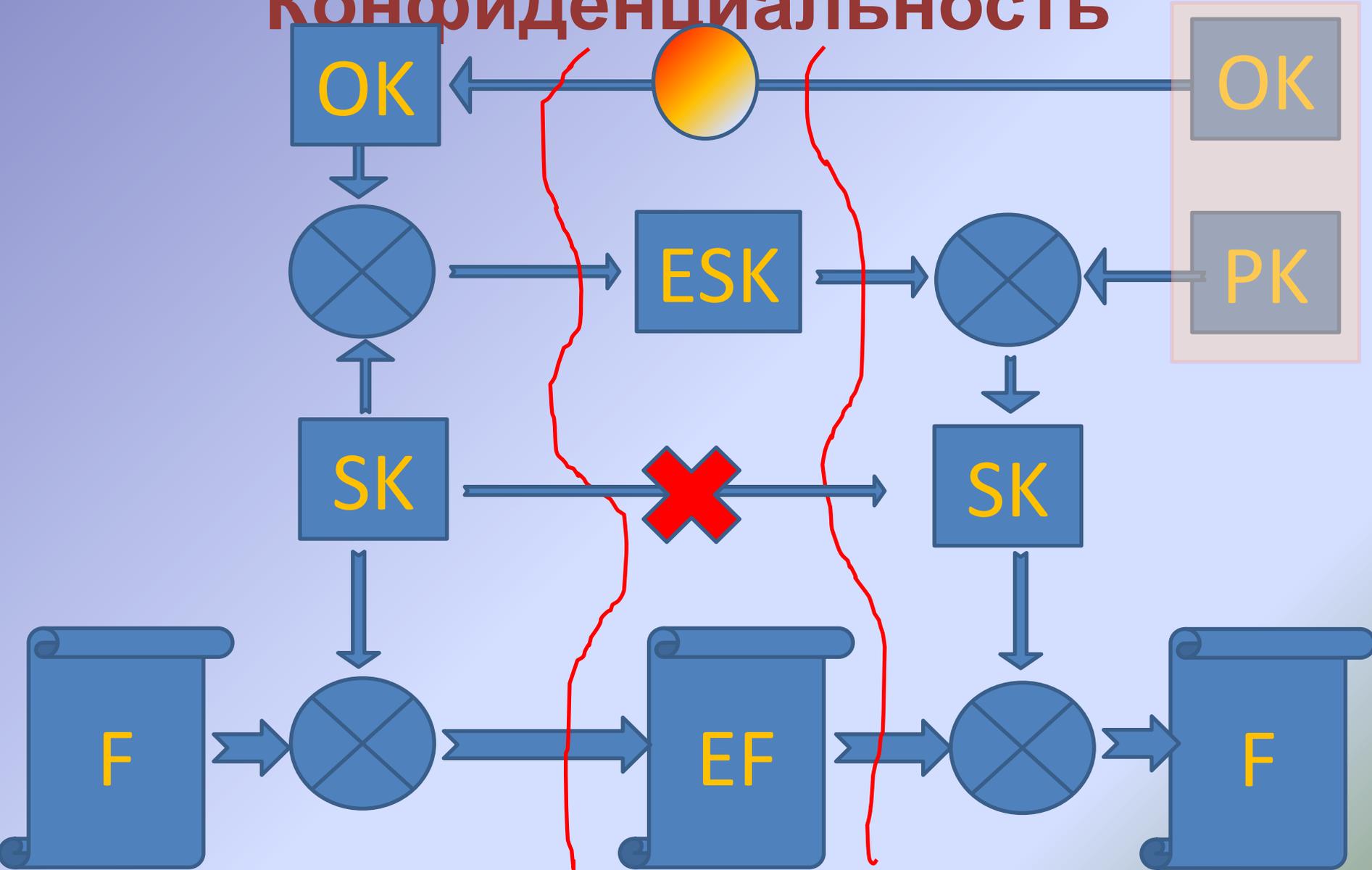
А можно так?



Уже правильнее

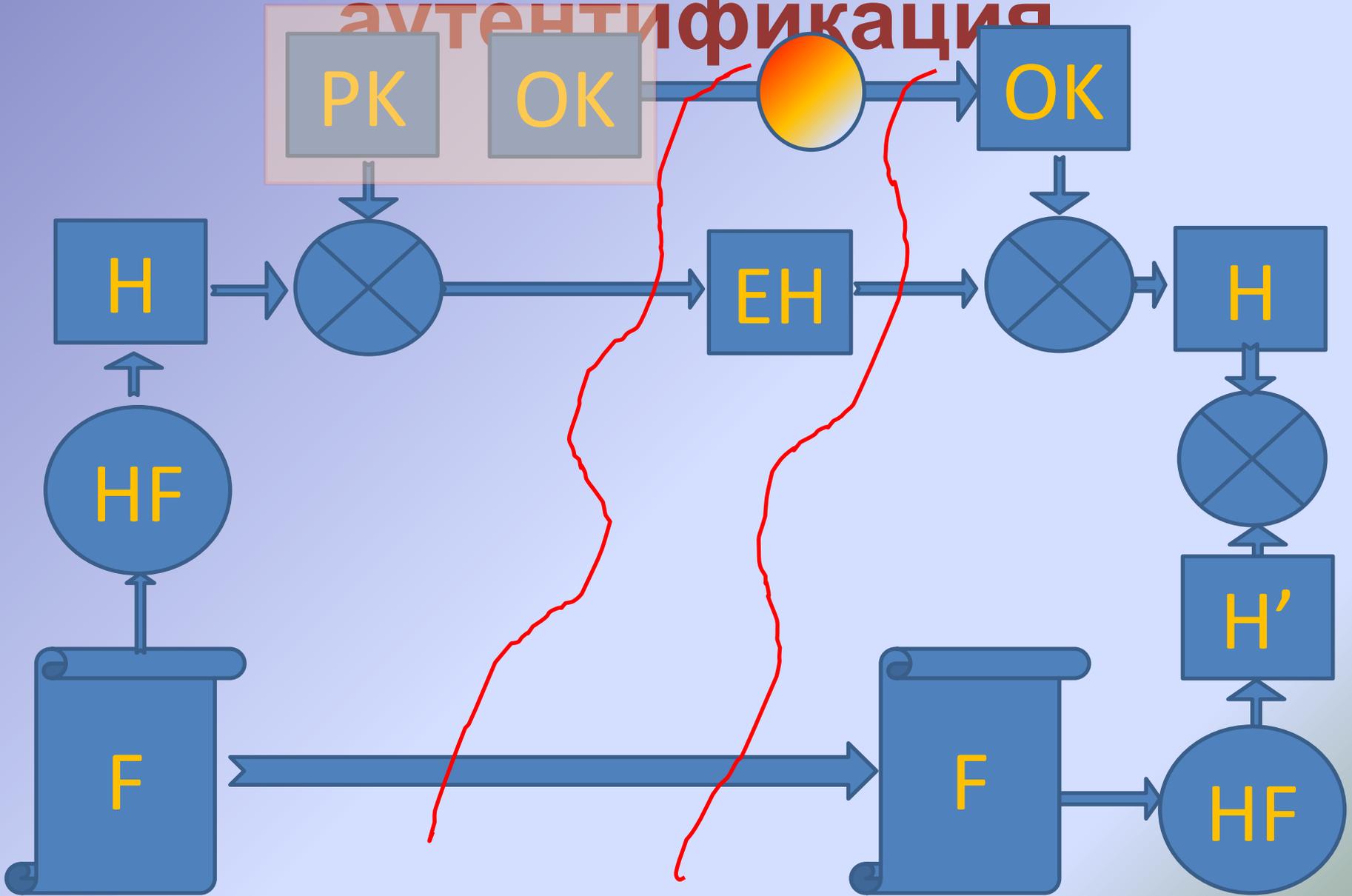


Передача - Конфиденциальность



Целостность и

аутентификация



Формирование сертификата

Заявка на

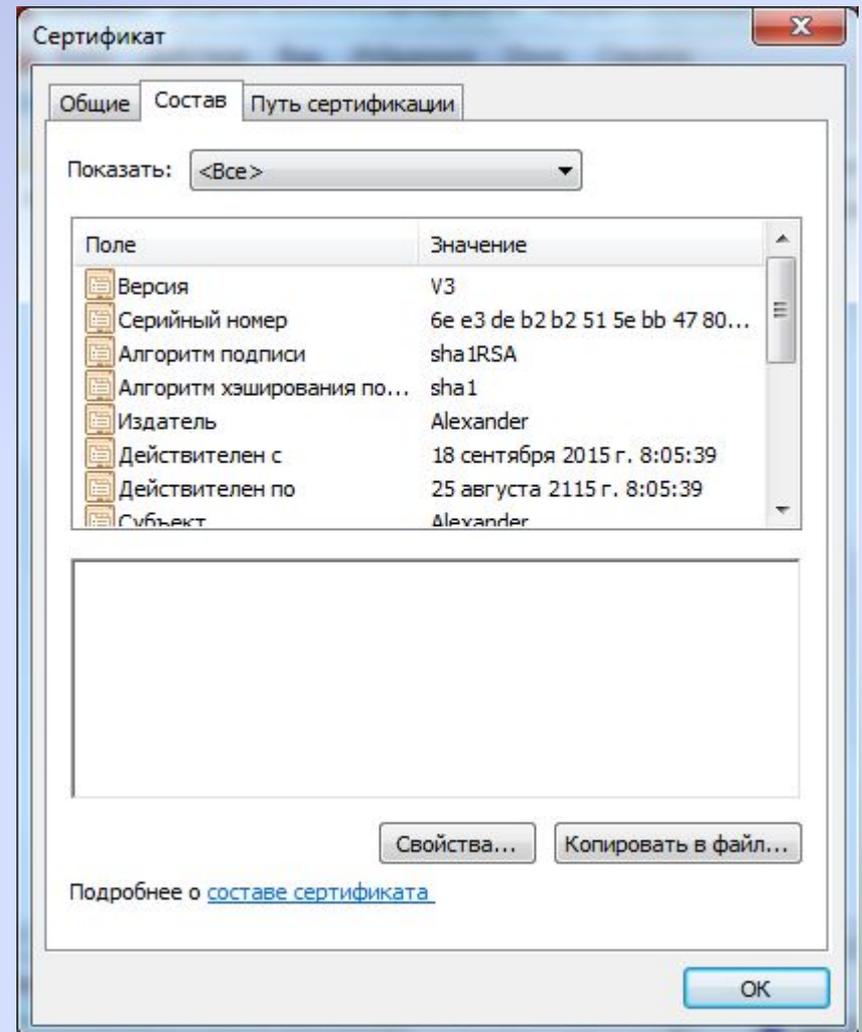
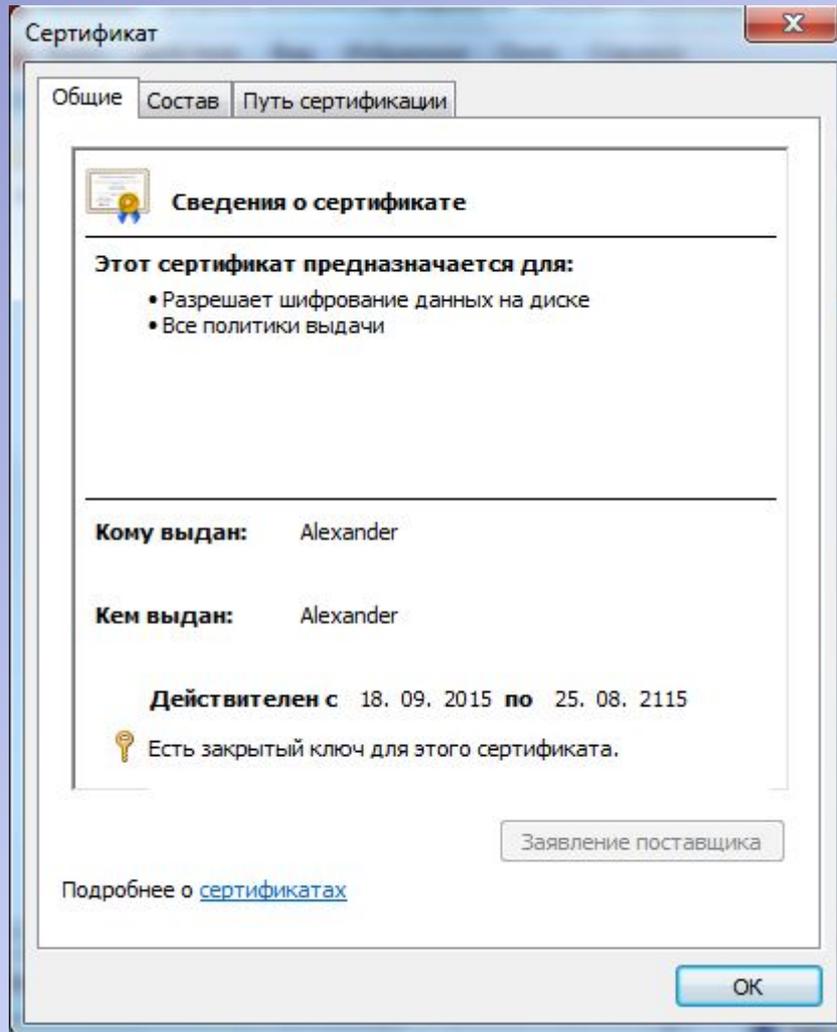
О	сертификат	Зачем		
К	PK	Кто?	?	?

С	Инф	
А	о	S

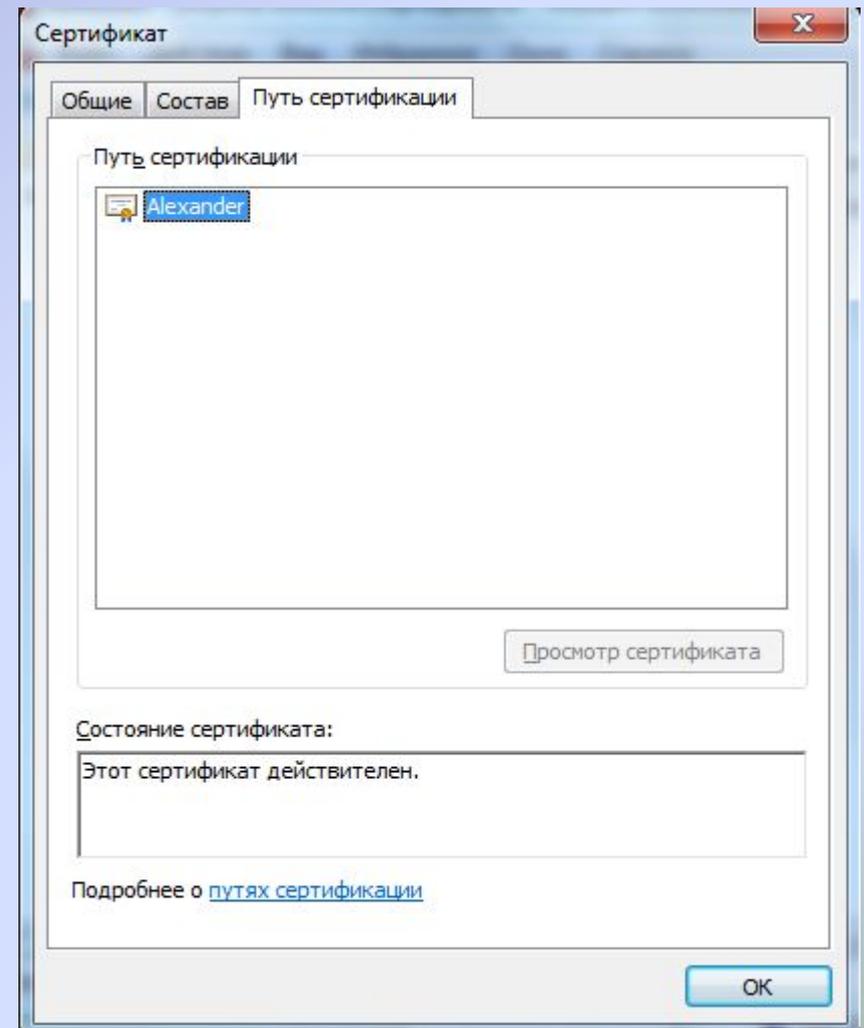
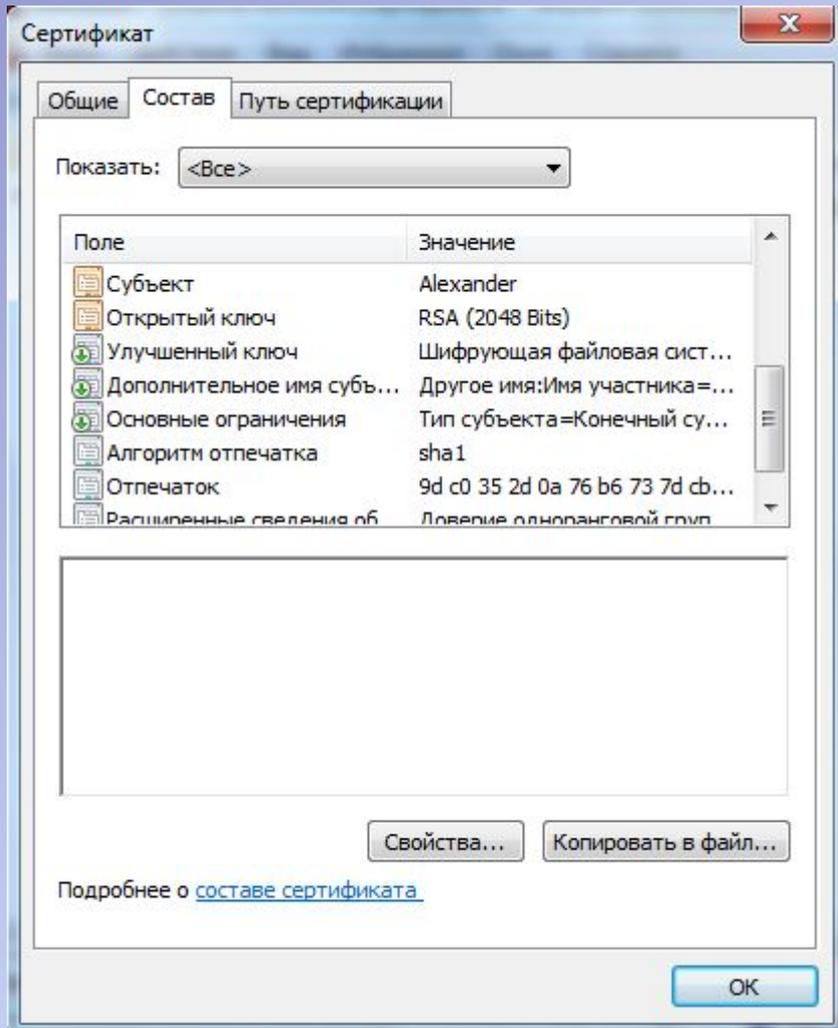


CA

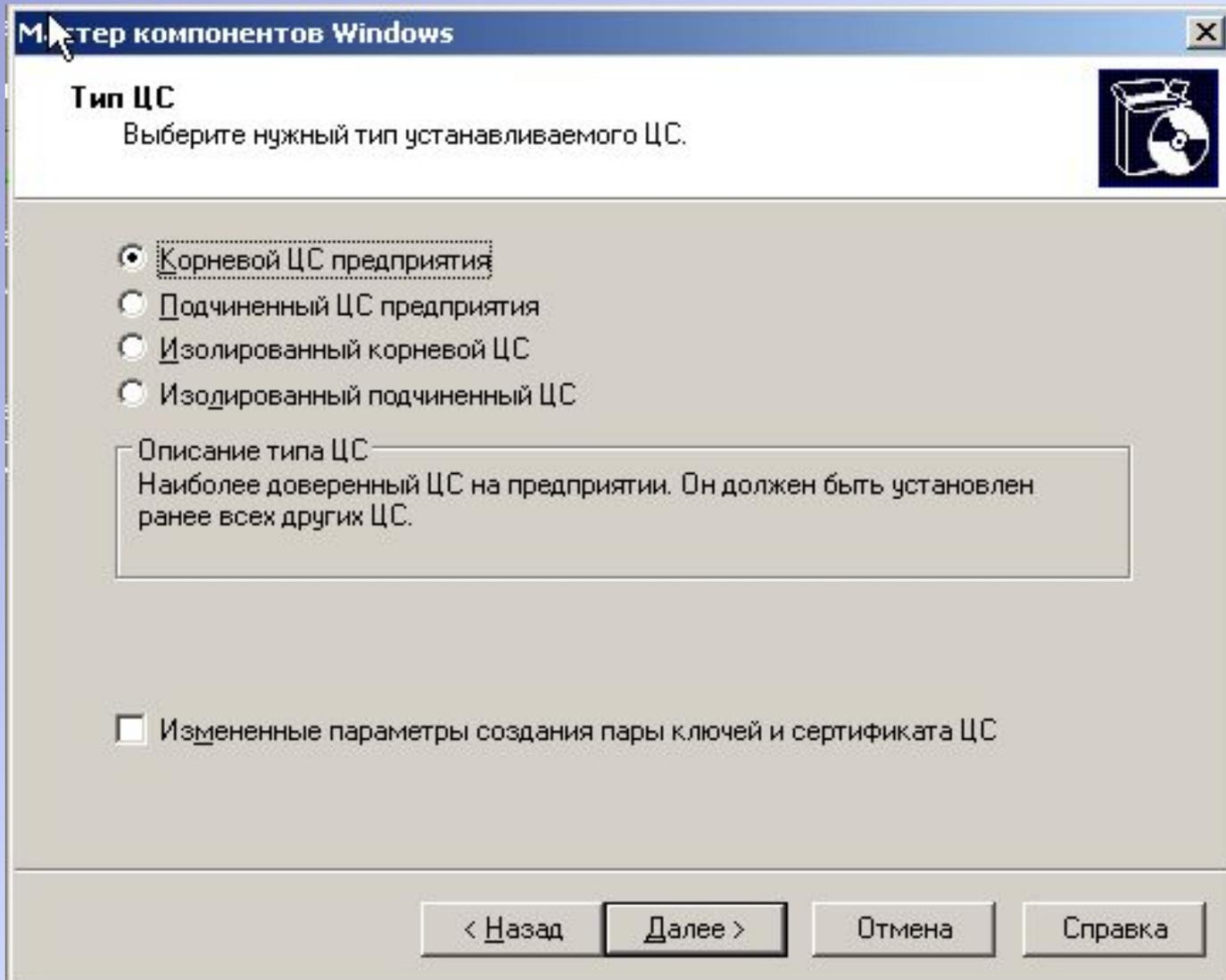
Сертификат



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

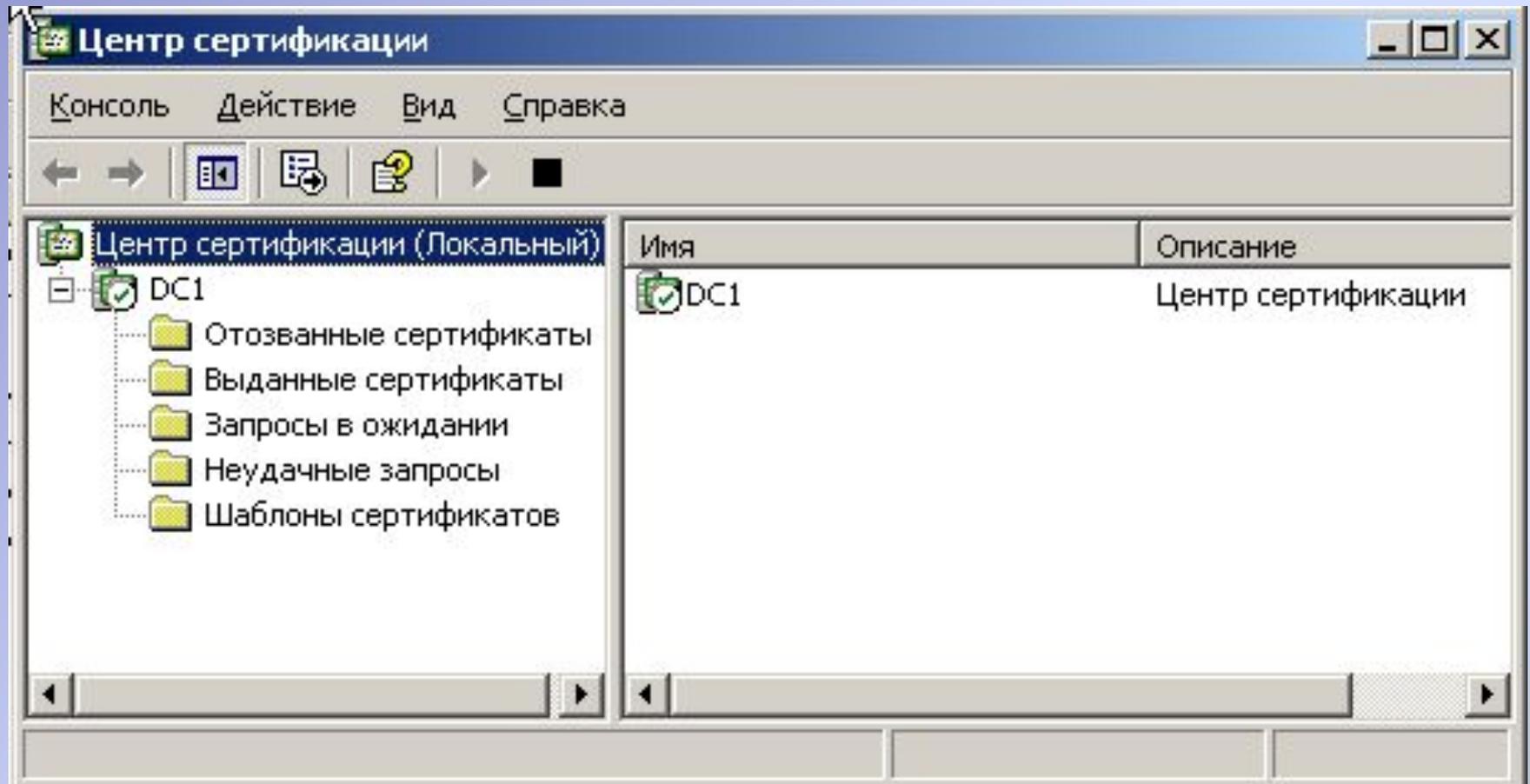
Просмотр различающегося имени:
CN=DC1,DC=sapr,DC=etu,DC=ru

Срок действия: 5 лет

Истекает: 25.09.2020 6:53

< Назад Далее > Отмена Справка

Консоль центра сертификатов

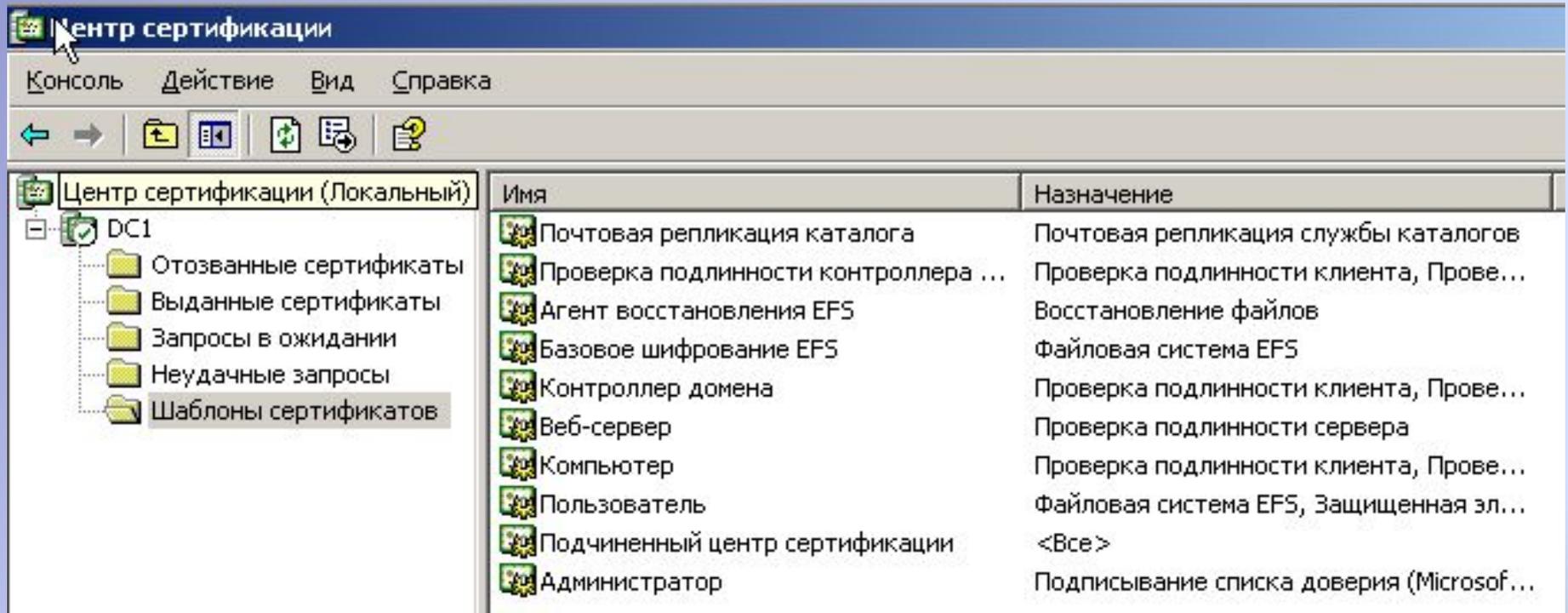


Выданные сертификаты

The screenshot shows the Windows Certificate Manager console window titled "Центр сертификации". The menu bar includes "Консоль", "Действие", "Вид", and "Справка". The left pane shows a tree view for "Центр сертификации (Локальный)" with a sub-tree for "DC1" containing folders for "Отозванные сертификаты", "Выданные сертификаты", "Запросы в ожидании", "Неудачные запросы", and "Шаблоны сертификатов". The right pane displays a table of issued certificates.

Код (ID) запроса	Имя запросившего	Двоичный сертификат	Шаблон сертификата	Серийный номер
2	SAPR\Администра...	-----BEGIN CERTIFICAT...	Базовое шифрование ...	61291e3...
3	SAPR\Администра...	-----BEGIN CERTIFICAT...	Агент восстановлени...	612acd3...
4	SAPR\DC1\$	-----BEGIN CERTIFICAT...	Контроллер домена (...)	612c078...

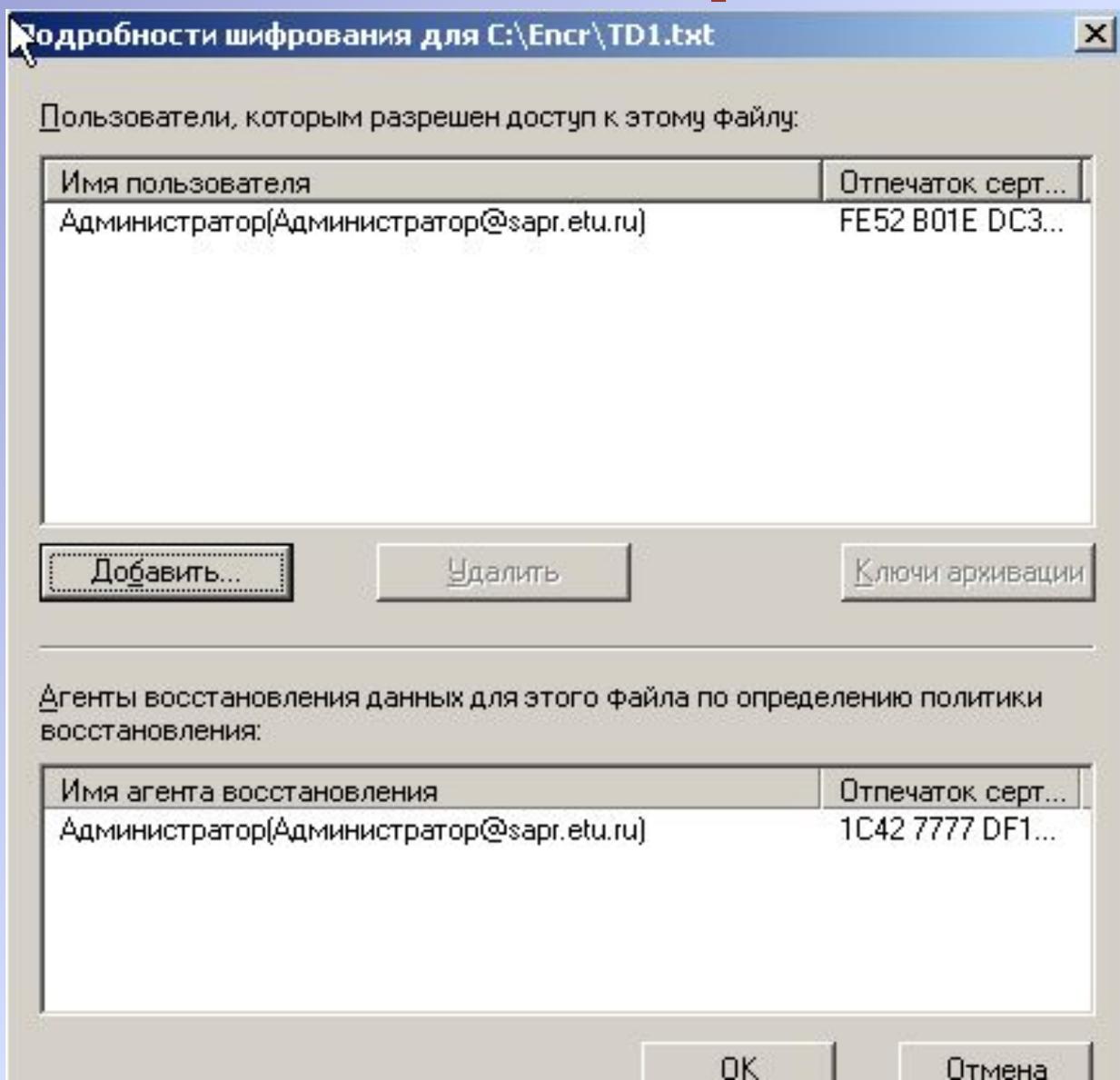
Шаблоны сертификатов



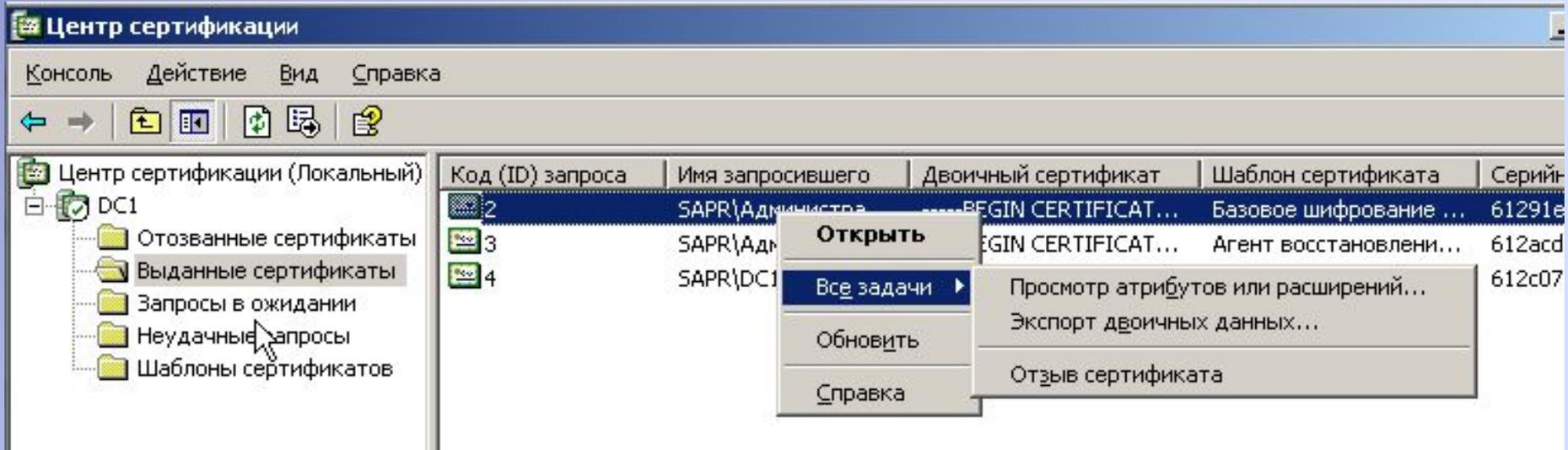
Скриншот интерфейса Центра сертификации (Локальный) в Windows. В левой панели отображены папки: Отозванные сертификаты, Выданные сертификаты, Запросы в ожидании, Неудачные запросы и Шаблоны сертификатов. В правой панели отображены следующие элементы:

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

The screenshot shows the Windows Certificate Center console. On the left, a tree view shows 'Центр сертификации (Локальный)' expanded to 'DC1', with 'Выданные сертификаты' selected. The main pane displays a table of certificates. A dialog box titled 'Отзыв сертификатов' is open, asking for confirmation to revoke selected certificates and offering a dropdown menu for the reason.

Код (ID) запроса	Имя запросившего	Двоичный сертификат	Шаблон сертификата	Серти...
2	SAPR\Администра...	-----BEGIN CERTIFICAT...	Базовое шифрование ...	6129
3	SAPR\Администра...	-----BEGIN CERTIFICAT...	Агент восстановлени...	612a
4	SAPR\DC1\$	-----BEGIN CERTIFICAT...	Контроллер домена (...	612c

Отзыв сертификатов

Вы действительно хотите отозвать выделенные сертификаты?

Можете также указать причину отзыва.

Код причины:

- Не определен
- Компрометация ключа
- Компрометация ЦС
- Изменение принадлежности
- Сертификат заменен
- Прекращение работы
- Приостановка действия

Нет

Отмена отзыва сертификата

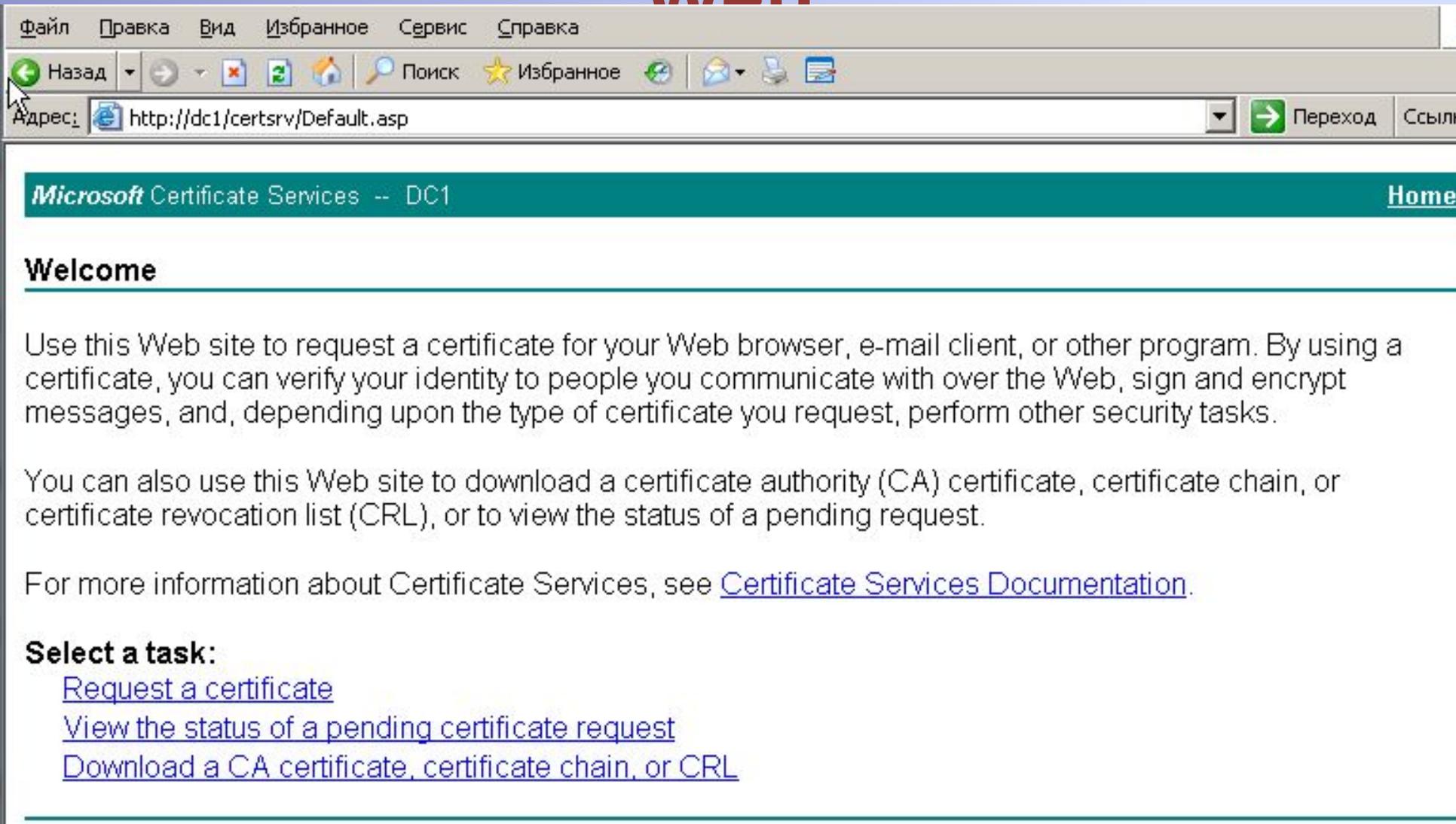
The screenshot shows the Windows Certificate Management console. The left pane displays the tree structure for the local Certificate Authority (CA), with 'DC1' expanded to show folders for 'Отозванные сертификаты', 'Выданные сертификаты', 'Запросы в ожидании', 'Неудачные запросы', and 'Шаблоны сертификатов'. The main pane shows a table of certificates with columns: 'Код (ID) запроса', 'Дата отзыва', 'Вступление в силу отзыва', 'Причина отзыва', and 'Имя запросившего'. A single certificate is listed with a red 'X' icon, indicating it is revoked. A context menu is open over this certificate, showing options: 'Открыть', 'Все задачи' (with a sub-menu), 'Обновить', and 'Справка'. The sub-menu for 'Все задачи' includes 'Просмотр атрибутов или расширений...', 'Экспорт двоичных данных...', and 'Отмена отзыва сертификата'.

Код (ID) запроса	Дата отзыва	Вступление в силу отзыва	Причина отзыва	Имя запросившего
2	25.09.2015 7...	25.	Приостановка д...	SAPR\Админи

Context menu options:

- Открыть
- Все задачи
 - Просмотр атрибутов или расширений...
 - Экспорт двоичных данных...
 - Отмена отзыва сертификата
- Обновить
- Справка

Запрос сертификата через Web



The screenshot shows a Microsoft Internet Explorer browser window. The address bar contains the URL <http://dc1/certsrv/Default.asp>. The page title is "Microsoft Certificate Services -- DC1". The main content area features a "Welcome" heading followed by a paragraph explaining the site's purpose: "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." Below this is another paragraph: "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." A link to "Certificate Services Documentation" is provided. At the bottom, a "Select a task:" section lists three options: "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

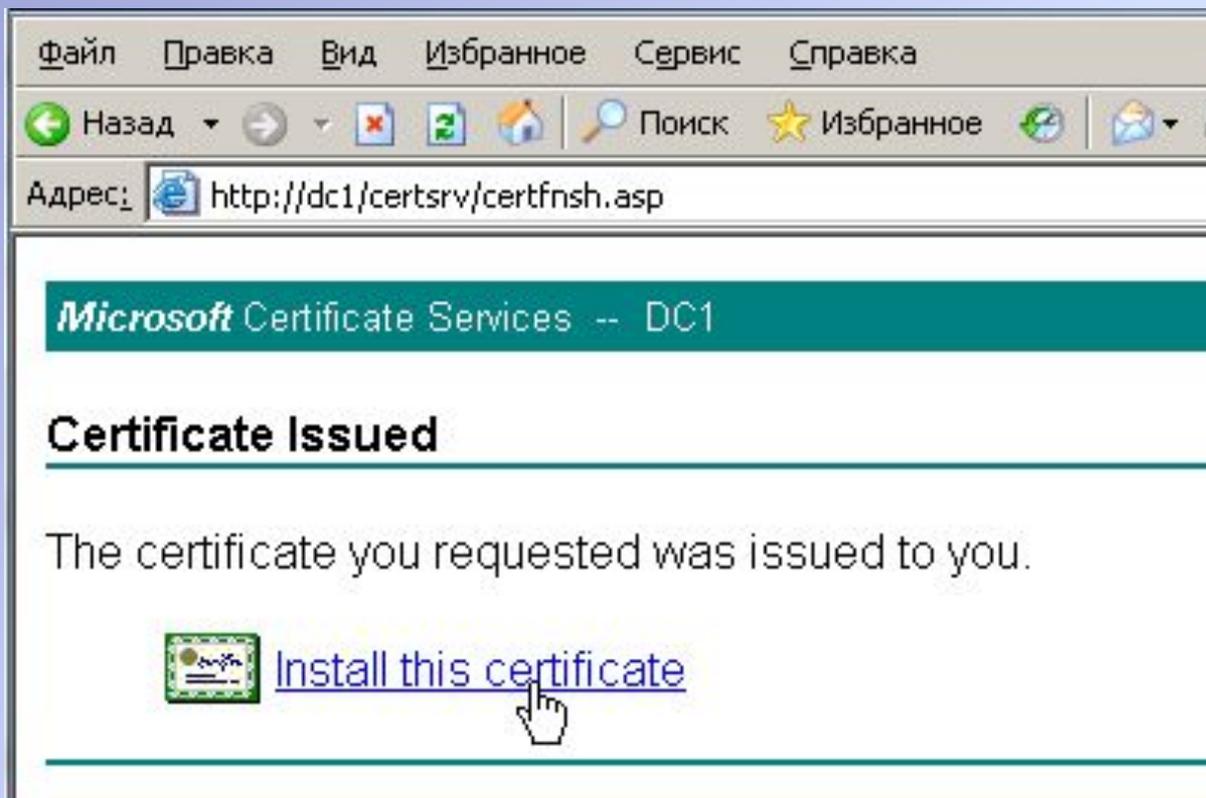
The image shows a web browser window displaying the Microsoft Certificate Services interface for DC1. The browser's address bar shows the URL `http://dc1/certsrv/certrqma.asp`. The page title is "Microsoft Certificate Services -- DC1".

The main content area is titled "Advanced Certificate" and contains a form for creating a certificate request. The form includes sections for "Certificate Template", "Key Options", and "Request".

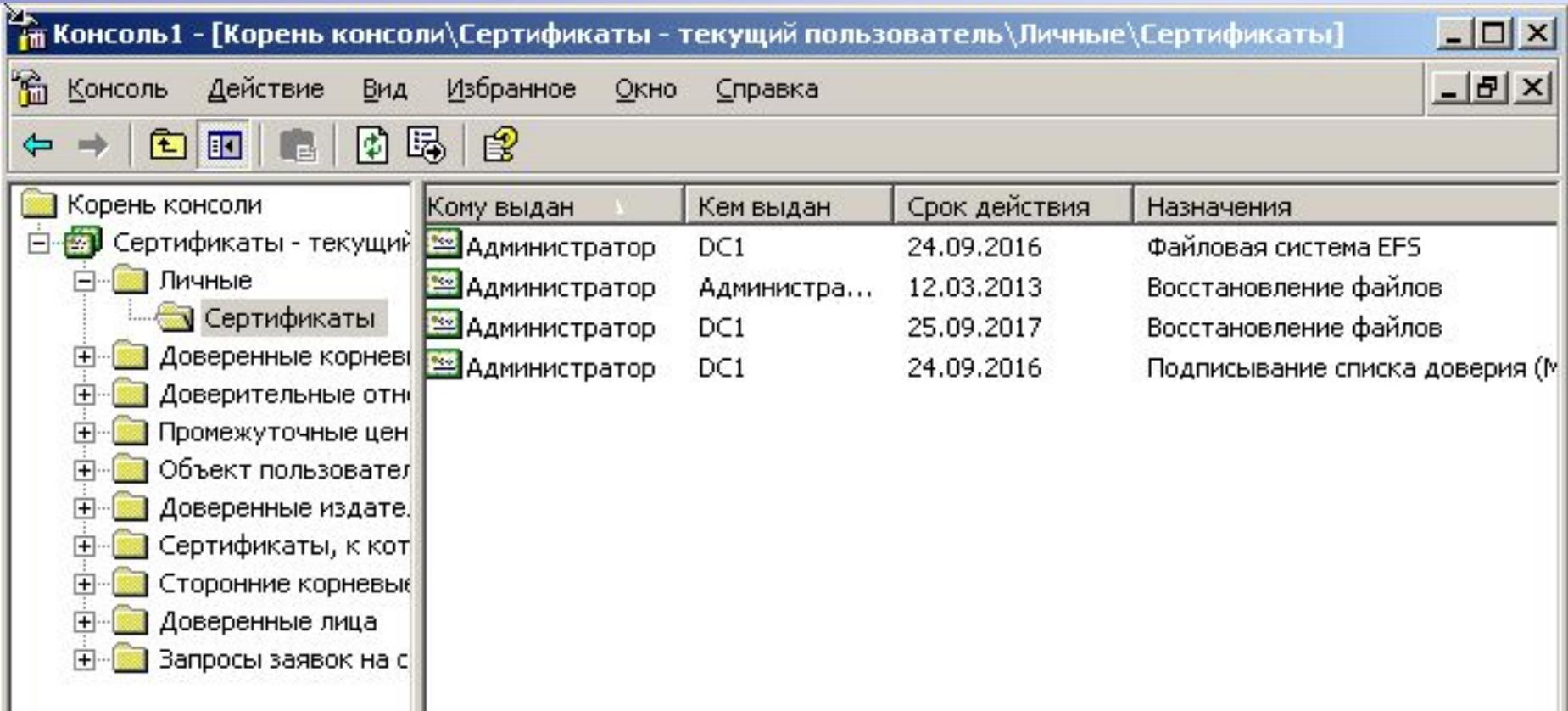
Overlaid on the bottom right is a Notepad window titled "req1 - Блокнот". It contains a certificate request in PEM format, enclosed in "-----BEGIN NEW CERTIFICATE REQUEST-----" and "-----END NEW CERTIFICATE REQUEST-----". The request body is a base64-encoded string starting with "MIIDaDCCATECAQAwADCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAZVctK/hH".

Visible elements in the browser window include the menu bar (Файл, Правка, Вид, Избранное, Сервис, Справка), the address bar, and the Microsoft Certificate Services logo. The Notepad window has its own menu bar (Файл, Правка, Формат, Вид, Справка).

Установка готового сертификата



Личные сертификаты



Консоль1 - [Корень консоли\Сертификаты - текущий пользователь\Личные\Сертификаты]

Консоль Действие Вид Избранное Окно Справка

Корень консоли

- Сертификаты - текущий пользователь
 - Личные
 - Сертификаты
 - Доверенные корневые центры сертификации
 - Доверительные отношения
 - Промежуточные центры сертификации
 - Объект пользователя
 - Доверенные издатели сертификатов
 - Сертификаты, к которым относятся доверительные отношения
 - Сторонние корневые центры сертификации
 - Доверенные лица
 - Запросы заявок на сертификаты

Кому выдан	Кем выдан	Срок действия	Назначения
Администратор	DC1	24.09.2016	Файловая система EFS
Администратор	Администра...	12.03.2013	Восстановление файлов
Администратор	DC1	25.09.2017	Восстановление файлов
Администратор	DC1	24.09.2016	Подписывание списка доверия (M...

Полученный сертификат

Сертификат

Общие Состав Путь сертификации

 **Сведения о сертификате**

Этот сертификат предназначен для:

- Разрешает шифрование данных

Кому выдан: Администратор

Кем выдан: DC1

Действителен с 25.09.2015 по 25.09.2020

 Есть закрытый ключ, соответствует сертификату

Сертификат

Общие Состав Путь сертификации

Путь сертификации

- DC1
 - Администратор

Сертификат

Общие Состав Путь сертификации

 **Сведения о сертификате**

Этот сертификат предназначен для:

- Все политики выдачи
- Все политики применения

Кому выдан: DC1

Кем выдан: DC1

Действителен с 25.09.2015 по 25.09.2020

Заявление поставщика

OK

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

Модель эшелонированной обороны

Физический
доступ

Политики, процедуры,
осведомленность

Хранилища

Хранилища

Обработка

Приложения Обновления Контроль
доступа
OS/.NET Обновления Аутентификация Антивирус
AD PKI

Передача

Intranet

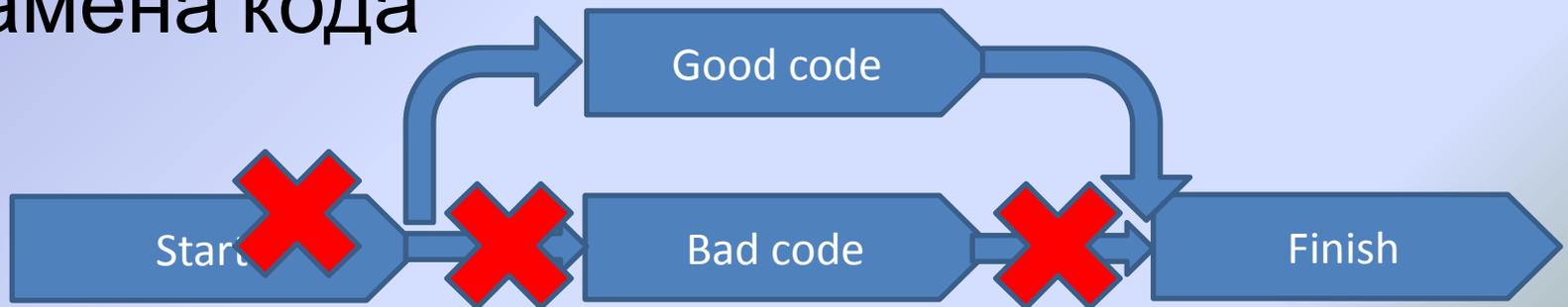
Internet

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



Программа-акцептор

- Файлы
- Система
- Загрузочная зона
- Макровирусы



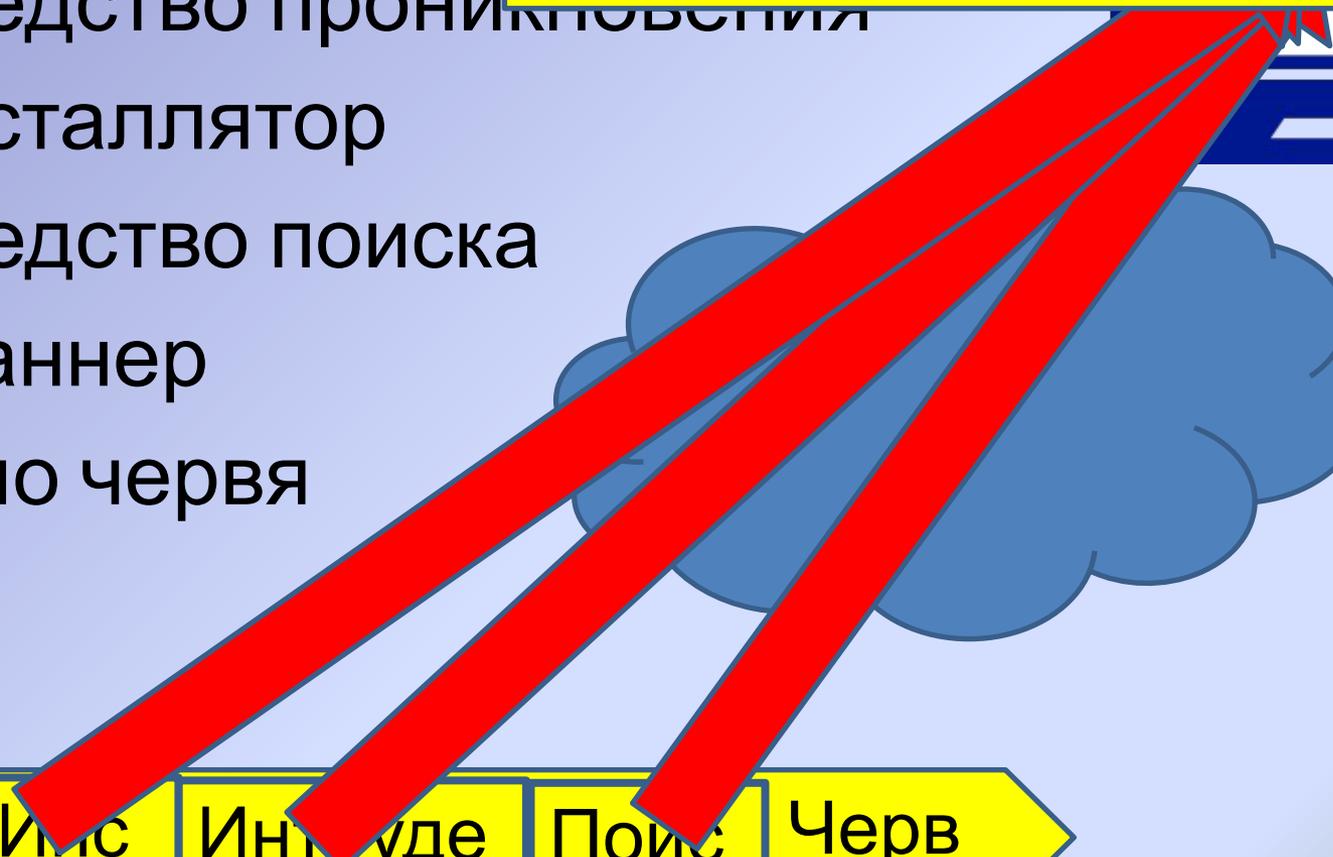
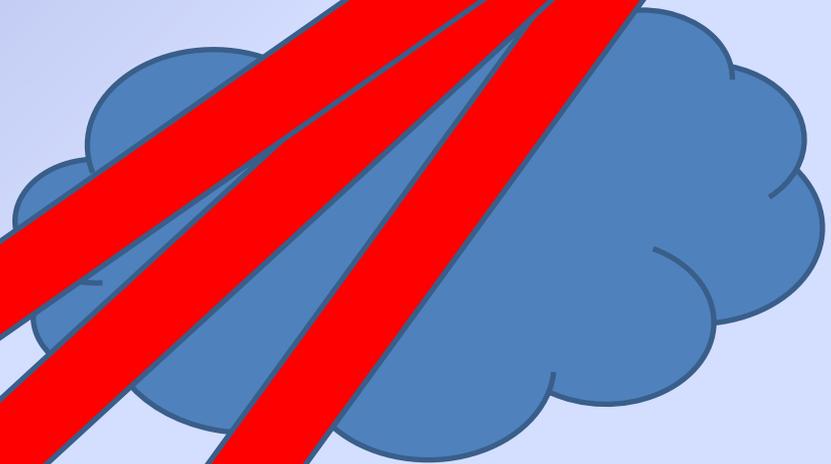
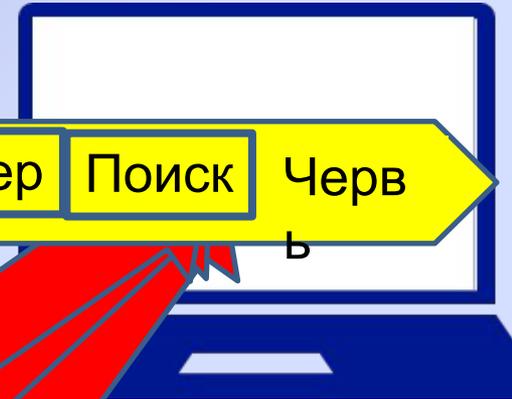
Тел Реп Мас Виру

О Л К С

Программа-донор

Черви

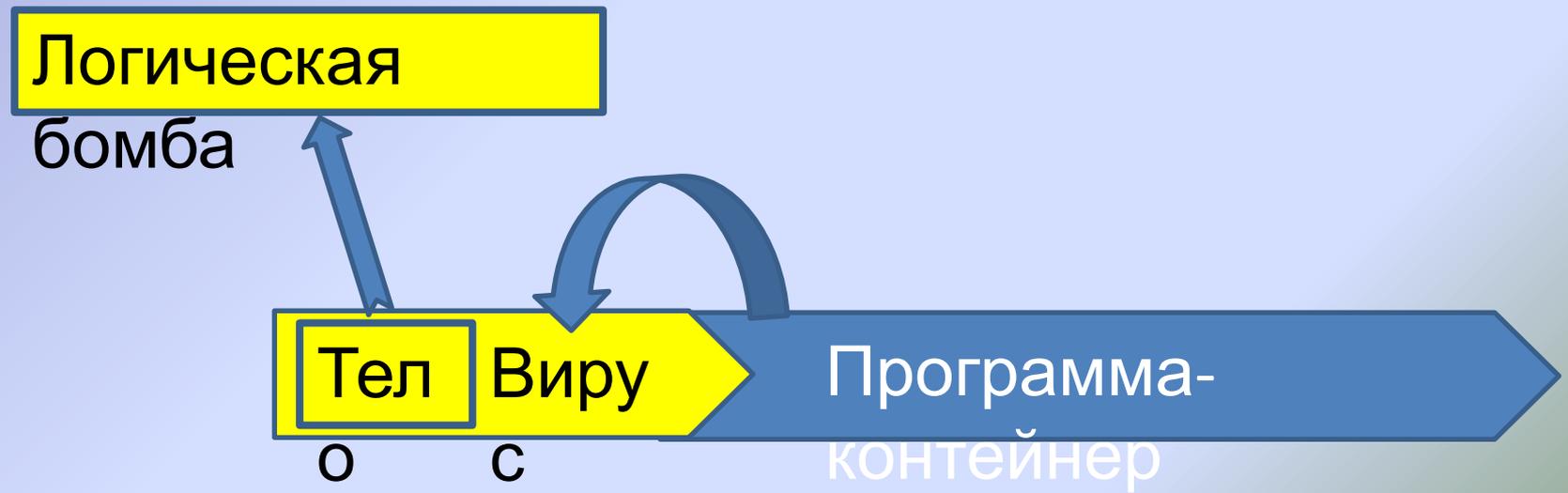
- Средство проникновения
- Инсталлятор
- Средство поиска
- Сканнер
- Тело червя



Т р к ь

Троян

- Контейнер – полезная программа
- Тело трояна



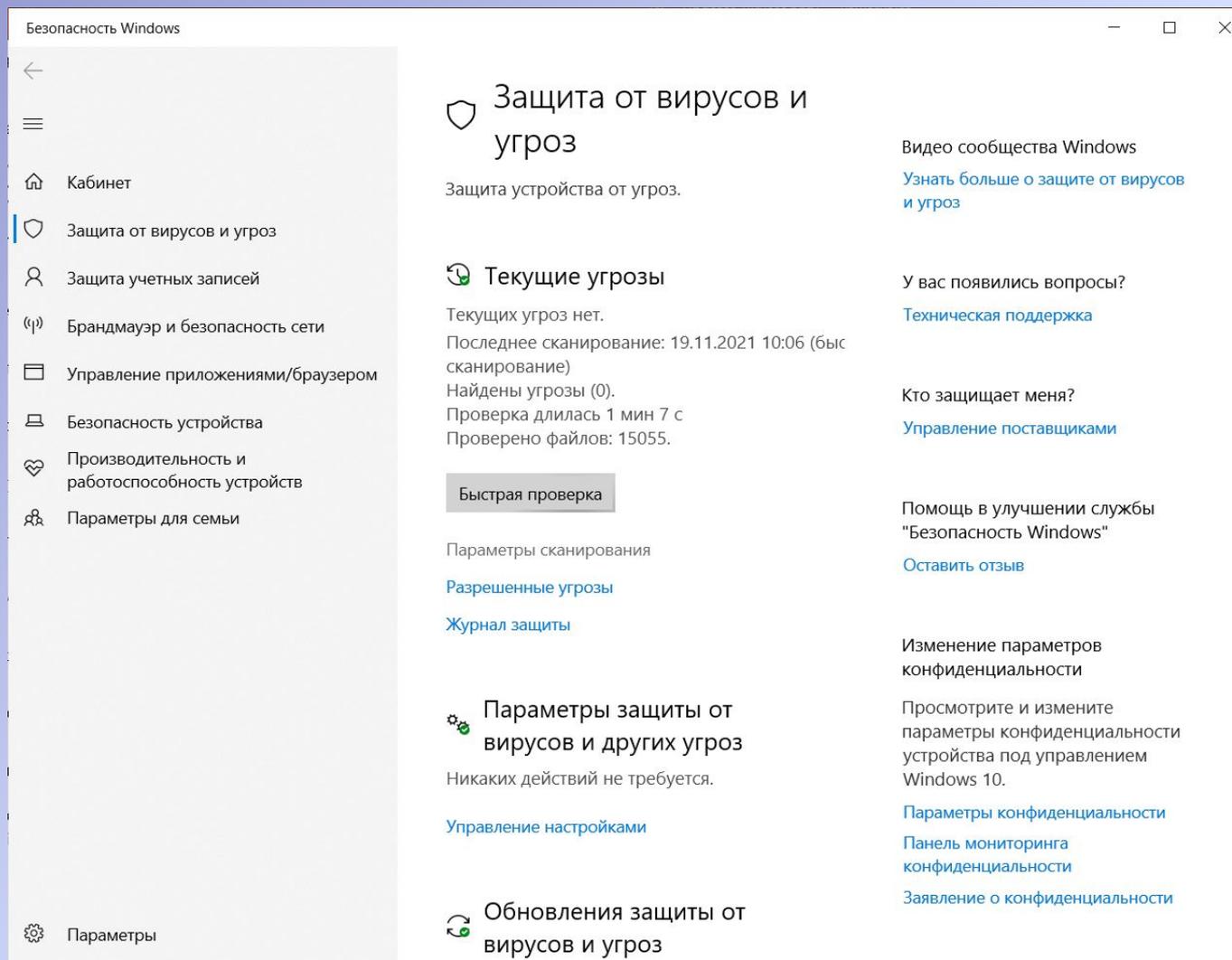
Root Kit

- 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)

12

13

14

15

Все Приложения Электронная_почта Интернет Другие ▾ Обратная связь ...

Параметры управления учетными записями пользователей

Настройка уведомления об изменении параметров компьютера

Контроль учетных записей помогает предотвратить изменения, вносимые в компьютер потенциально опасными программами.
[Подробнее о параметрах контроля учетных записей](#)

Всегда уведомлять

Никогда не уведомлять

Уведомлять только при попытках приложений внести изменения в компьютер (по умолчанию)

- Не уведомлять при изменении параметров Windows пользователем

i Рекомендуется при использовании знакомых приложений и посещении знакомых веб-сайтов.

OK Отмена

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

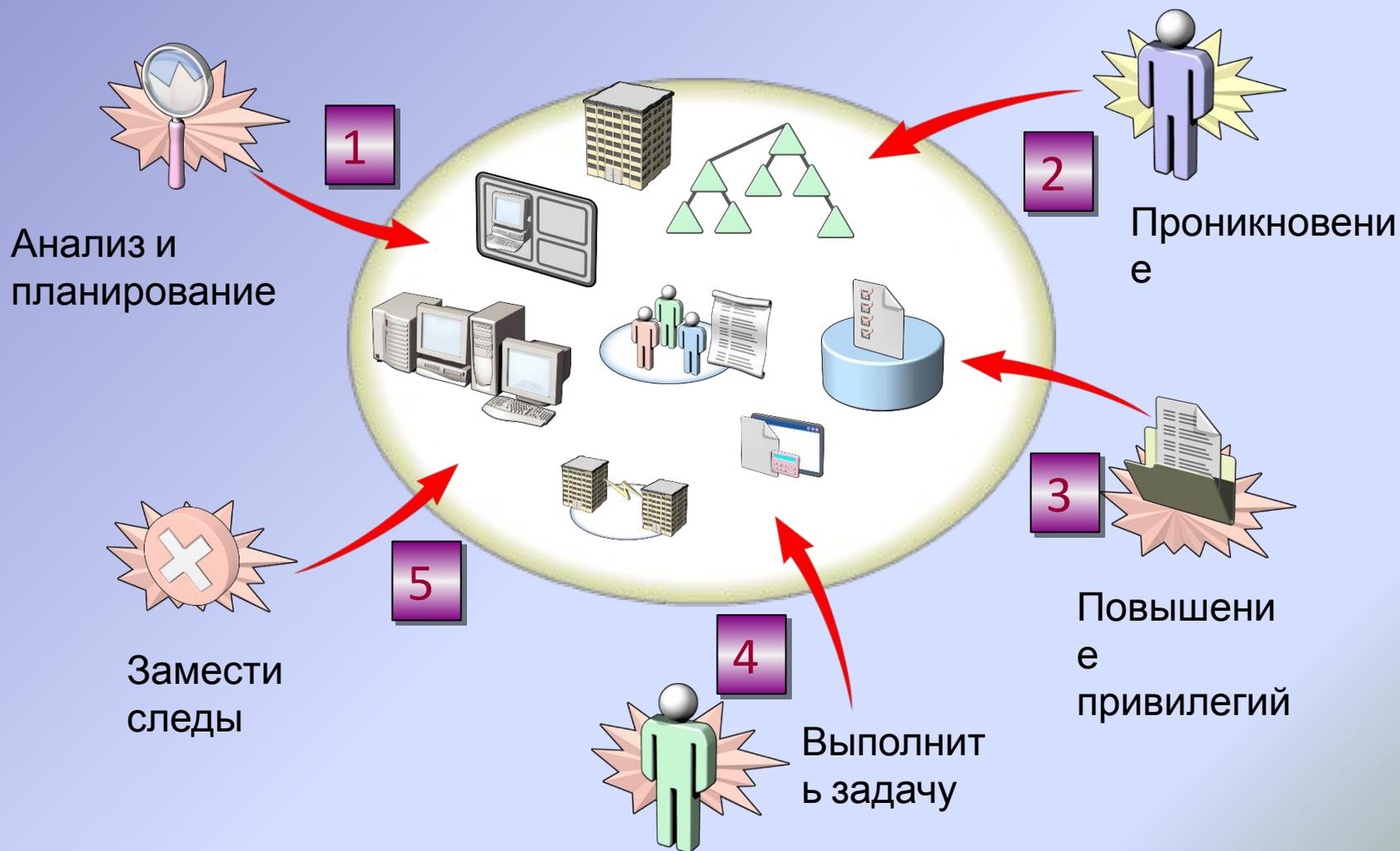
Denial of service

Приложение делается недоступным

Elevation of privilege

Получение полномочий привилегированного пользователя

Анатомия атаки



Борьба...

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

Модель эшелонированной обороны

Физический
доступ

Политики, процедуры,
осведомленность

Хранение

ACL EFS Bitlocker

Backup Mirror RAID SC

Обработка

APPs Antivirus Updates

OS/.NET Antispyware Autentication HIDS-HIPS

PKI

Передача

Intranet Routing IPsec RMS NIDS-NIPS

Internet Firewall VPN NAP

AD