

ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СТЕРЛИТАМАКСКИЙ МНОГОПРОФИЛЬНЫЙ ПРОФЕССИОНАЛЬНЫЙ КОЛЛЕДЖ
(ГАПОУ СМПК)

КУРСОВАЯ РАБОТА

«МОДЕЛИРОВАНИЕ ЭТАПОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБМЕНА ИНФОРМАЦИЕЙ
ПОЛЬЗОВАТЕЛЕЙ ЛОКАЛЬНОЙ СЕТИ»

Выполнил:
студент III курса группы ССА-39
специальности 09.02.06 Системное и
сетевое администрирование
Иванов Вячеслав Олегович.

Руководитель:
Шарафиев Ринат Расимович.

Стерлитамак, 2020

Цель проекта: обеспечение безопасности обмена информацией пользователей локальной сети организации.

Задачи проекта:

- 1. Рассмотреть учебно-техническую литературу по теме курсовой работы.
- 2. Описать способы организации и угрозы обмена информацией пользователей в локальной сети.
- 3. Описать методы обеспечения информацией пользователей в локальной сети.
- 4. Смоделировать объекты сетевой инфраструктуры локальной сети.
- 5. Описать этапы моделирования обеспечения безопасности обмена информацией пользователей локальной сети.
- Реализация предложенного проекта позволит рассмотреть более безопасный вариант обмена информации пользователей локальной сети

Теоретические основы

Локальные сети (от английского local – местный) – это сети, состоящие из близко расположенных компьютеров, чаще всего находящихся в одной комнате, в одном здании или в близко расположенных зданиях. Локальные сети, охватывающие некое предприятие или фирму и объединяющие разнородные вычислительные ресурсы в единой среде, называют корпоративными (от английского corporate – корпоративный, общий).

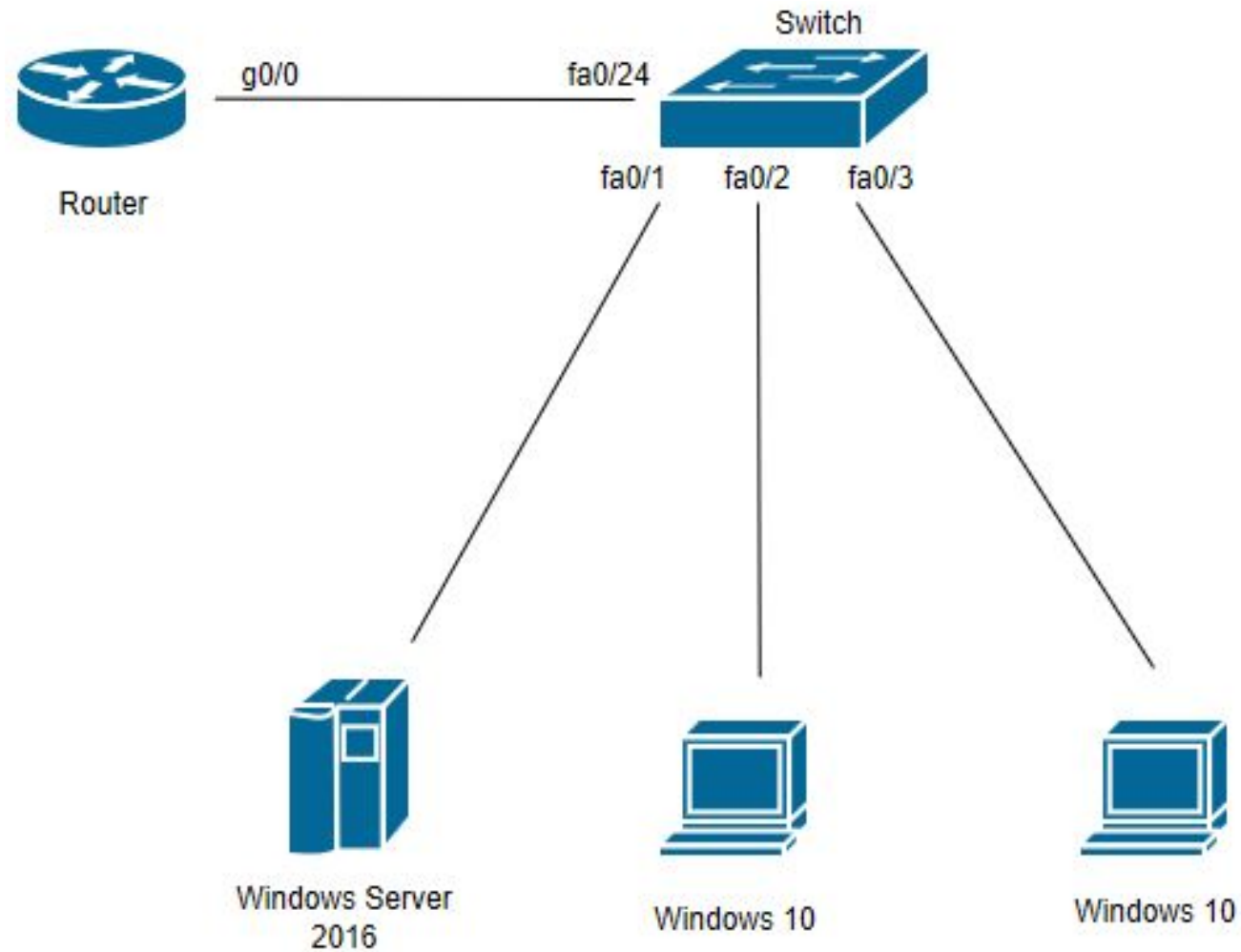


Обеспечения безопасного обмена информацией пользователей локальной сети

Обеспечение безопасности локальной сети является важным аспектом работы с сетями. Крайне важно понять, что безопасность — это не продукт, который можно купить в магазине и быть уверенным в собственной защищенности. Защита локальных сетей всегда является необходимой составляющей её профессиональной организации, причем, безопасность должна быть обеспечена на любом ее участке.

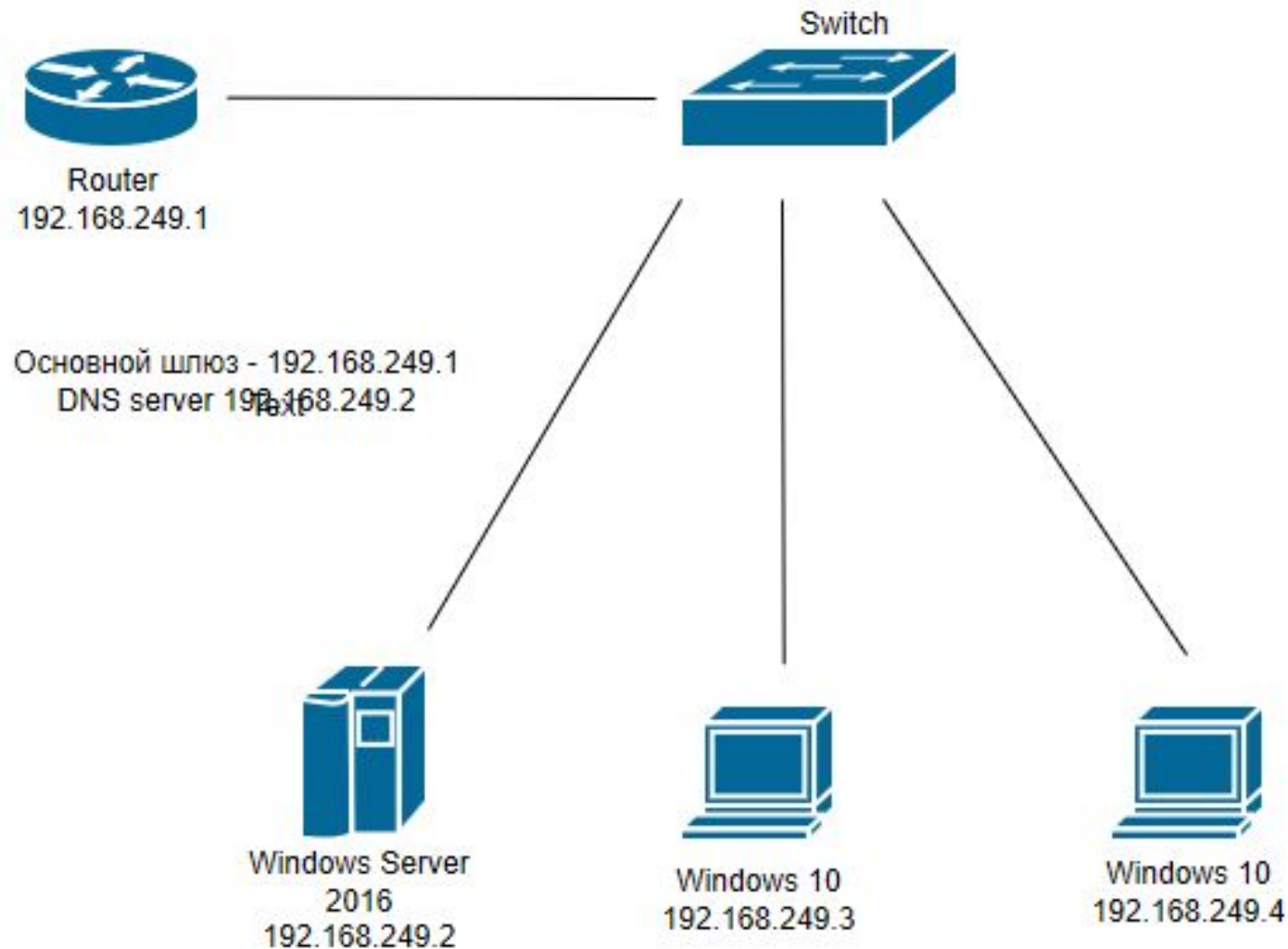
Моделирование локальной сети организации

Физическая топология организации

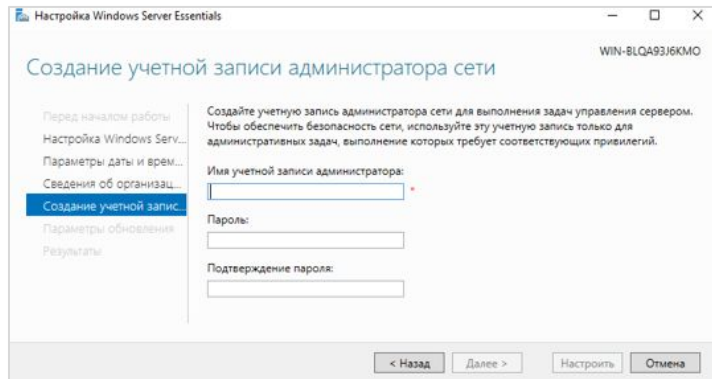


Моделирование локальной сети организации

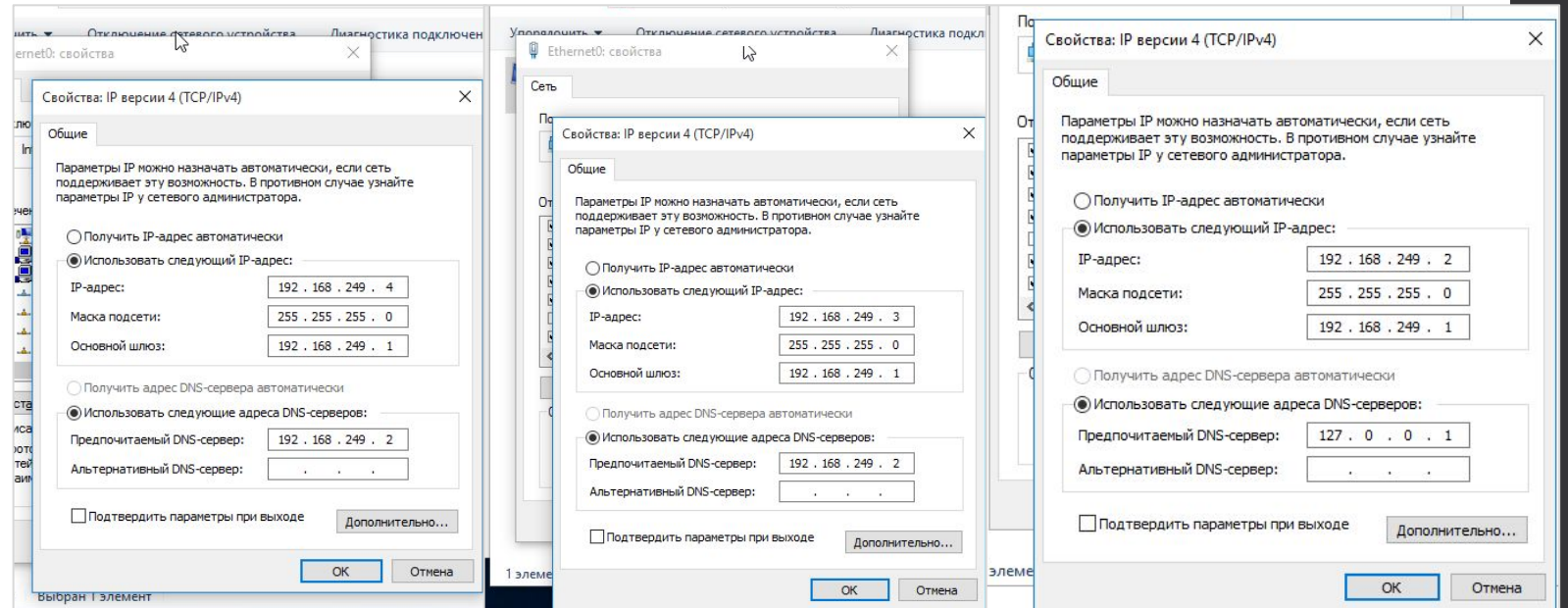
Логическая топология организации



Проведение базовой настройки оборудования

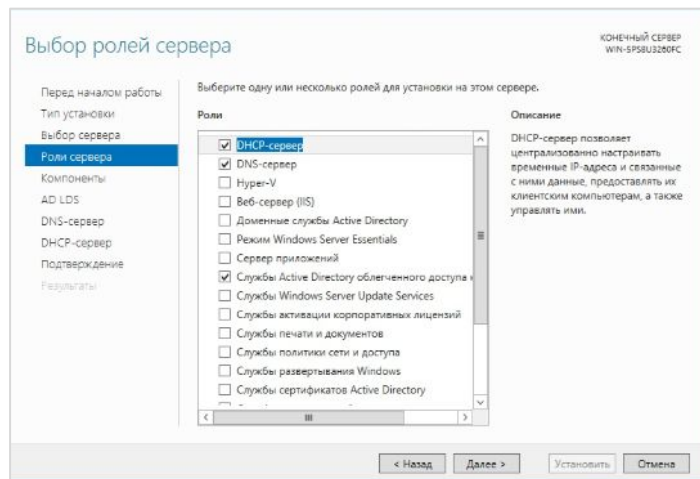


Создание учётной записи администратора



Настройка сетевого подключения

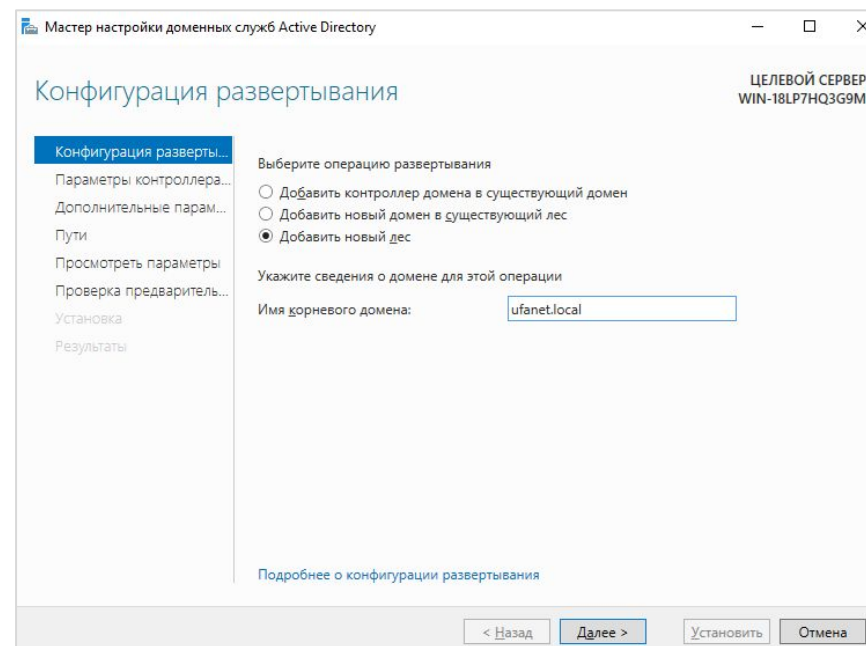
Установка и настройка доменной службы Active Directory и «DNS-сервер»



Через Диспетчер серверов нам следует поставить галочки на против «DNS-сервер» и «Доменные службы Active Directory» (Рисунок 8). После чего нужно повысить роль сервера до уровня контроллера домена.

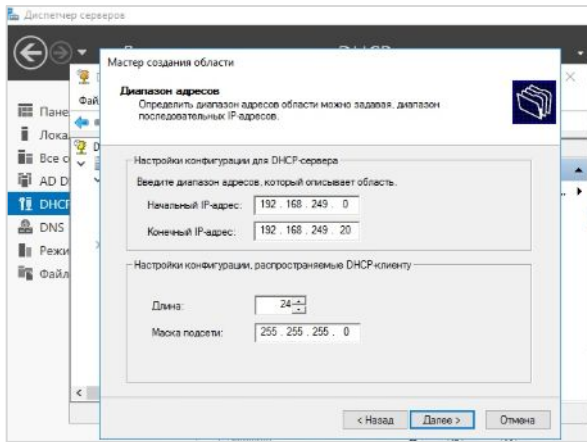
Установка доменной службы «Active Directory» и «DNS-сервер»

В появившемся окне добавить новый лес (ufanet.local) который будет являться нашим доменом



Повышение роли сервера до уровня контроллера домена

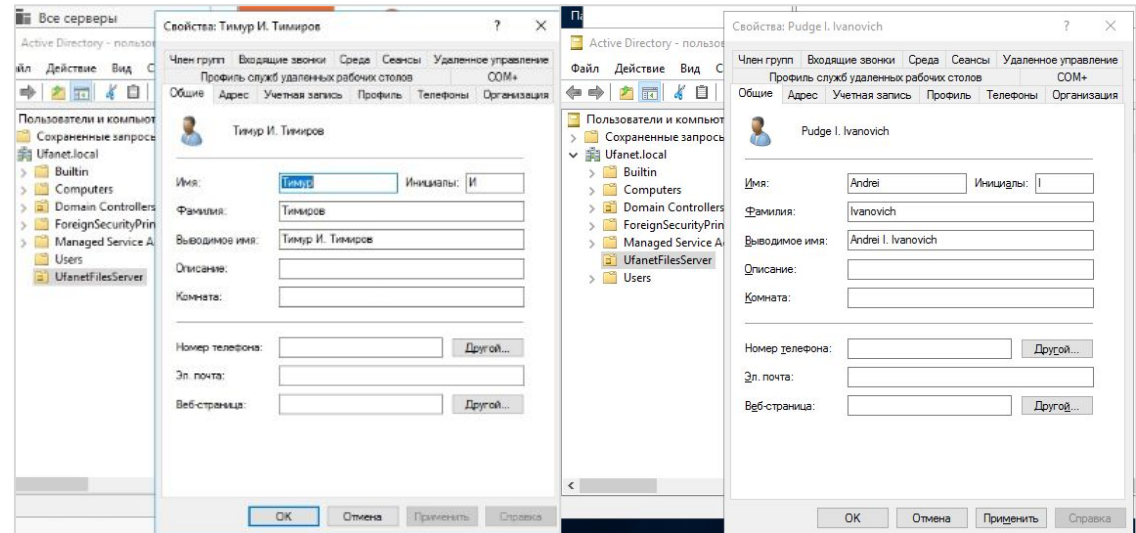
Фиксация DHCP и создание пользователей локальной сети «Уфанет»



Фиксируем DHCP сервер для автоматического получения IP-адреса из пула заданных адресов. Важно учесть, что IP-адрес сервера и IP-адрес основного шлюза нужно внести в исключения.

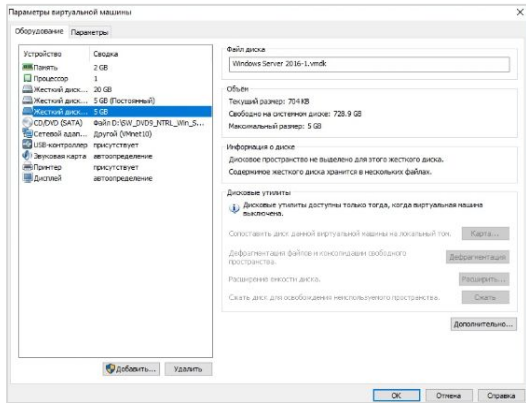
Установка и настройка DHCP сервера

Далее в разделе «Active Directory – пользователи и пароли» нужно создать пользователей локальной сети «Уфанет»



Создание пользователей локальной сети «Уфанет»

Создание жестких дисков для хранения данных и резервного копирования и установка компонента «Диспетчер ресурсов файлового сервера»

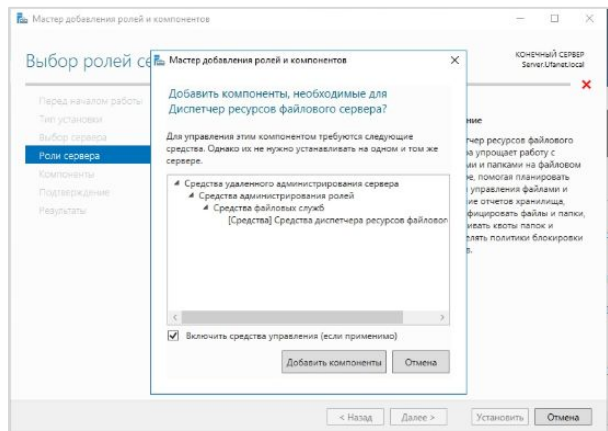


Так как для хранения данных будет использован файловый сервер, необходимо добавить локальный диск. Создаём два диска, первый – для хранения данных, второй – для хранения резервных копий документа

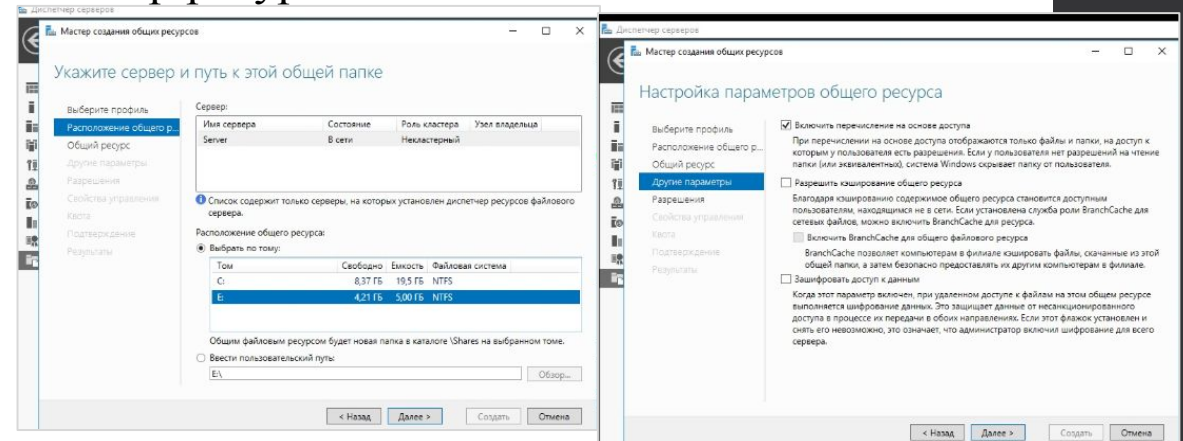
Создание жестких дисков для хранения данных и резервного копирования

Для работы с файловым сервером следует установить компонент «Диспетчер ресурсов файлового сервера»

Далее следует выполнить настройку в разделе «Мастер создания общих ресурсов»



Установка компонента «Диспетчер ресурсов файлового сервера»



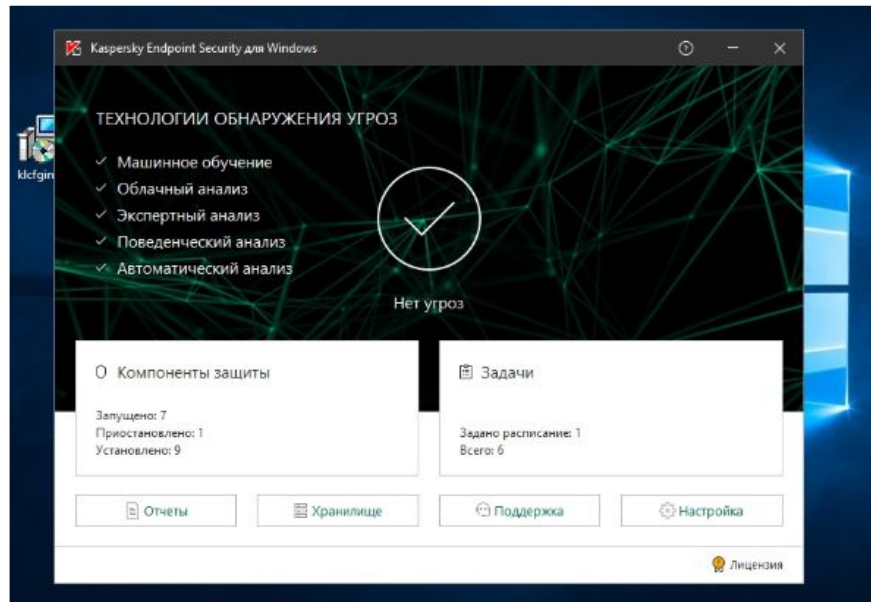
Настройка «Мастера создания общих ресурсов»

Обеспечение безопасности

Для обеспечения защиты информации необходимо установить специализированное программное обеспечение, таким является: Folder Protection версии 6.01, при помощи которой мы обеспечим сетевой диск паролем



Folder Protection версии 6.01

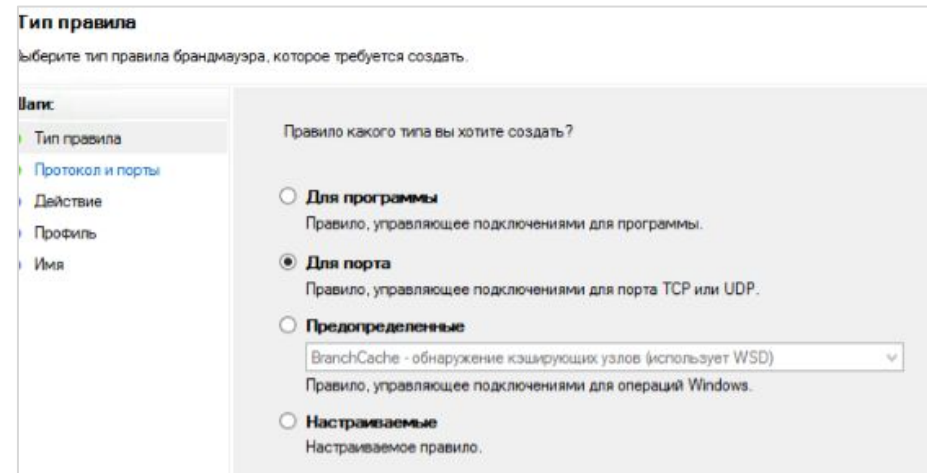


Kaspersky Endpoint Security

Так же, нам необходимо установить специализированное антивирусное ПО, чтобы обеспечить безопасный обмен информацией, и защиту данных от вирусов. Для этой роли существует Kaspersky Endpoint Security, который может обеспечить мониторинг статуса сети

Настройка брандмауэра

Так как наш файловый сервер постоянно подвергается атаке, следует настроить брандмауэр. Для этого переходим в «Диспетчер задач», открываем брандмауэр и настраиваем дополнительные параметры. Далее создаём правило для входящих подключений



Настройка брандмауэра

Таким образом, была реализована задача по моделированию обеспечения безопасности обмена информацией пользователей сети организации.

Заключение

Разработан оптимальный комплекс мер для обеспечения безопасности информацией в локальной сети.

Этот комплекс мер включает в себя:

- 1) настройка брандмауэра (firewall);
- 2) настройка групповых политик;
- 3) настройка паролей в локальной папке (файл сервера);
- 4) установка и настройка специализированного антивирусного ПО (Kaspersky Endpoint Security).

Таким образом, исходя из выше сказанного, цель курсовой работы достигнута.

ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СТЕРЛИТАМАКСКИЙ МНОГОПРОФИЛЬНЫЙ ПРОФЕССИОНАЛЬНЫЙ КОЛЛЕДЖ
(ГАПОУ СМПК)

КУРСОВАЯ РАБОТА

«МОДЕЛИРОВАНИЕ ЭТАПОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБМЕНА ИНФОРМАЦИЕЙ
ПОЛЬЗОВАТЕЛЕЙ ЛОКАЛЬНОЙ СЕТИ»

Выполнил:
студент III курса группы ССА-39
специальности 09.02.06 Системное и
сетевое администрирование
Иванов Вячеслав Олегович.

Руководитель:
Шарафиев Ринат Расимович.

Стерлитамак, 2020