

## **Курсовая работа**

ПМ.03 «Эксплуатация объектов сетевой инфраструктуры»

МДК.03.03 «Техническое обслуживание средств вычислительной техники и КС»

Специальность 09.02.02 «Компьютерные сети»

**Тема: «Обеспечение отказоустойчивой и бесперебойной работы сети предприятия.»**

**МПТ 09.02.02 ПЗ 04 КР**

### **Пояснительная записка**

Листа: 55

Руководитель

\_\_\_\_\_ / М.В. Володин /  
« \_\_\_\_\_ » \_\_\_\_\_ 2020 г.

Исполнитель

\_\_\_\_\_ / Э.Р. Кочарян /  
« \_\_\_\_\_ » \_\_\_\_\_ 2020 г.

2020г.

## СОДЕРЖАНИЕ

Введение .....	4
Основная часть .....	6
Раздел 1 «теоретическая часть» .....	6
Задача 1.1 Технические решения по обеспечению бесперебойной и отказоустойчивой работы сети предприятия.....	6
Задача 1.2 Обеспечение отказоустойчивой и бесперебойной работы сетевого оборудования.....	17
Задача 1.3 Репликация и резервирование.....	23
Задача 1.4 Мониторинг сети. Система мониторинга zabbix.....	24
Раздел 2 «Практическая часть».....	26
Задача 2.1 Проектирование топологии.....	26
Задача 2.2 Настройка сетевого оборудования.....	27
Задача 2.3 Настройка серверов: Windows server 2019, zabbix сервер...	35
Заключение.....	54
Список используемых источников.....	55

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР			
Разраб.		Кочарян Э. Р.			Обеспечение отказоустойчивой и бесперебойной работы сети предприятия.		Лит.	Лист
Провер.		Володин И. М.						
Реценз.							3	55
Н. Контр.							ФГБОУ ВО «РЭУ им. Г. В. Плеханова» МПТ	
Утверд.								

## 1. Введение.

Сейчас уже сложно представить какое либо предприятие без собственной компьютерной сети. Локальная компьютерная сеть позволяет предприятию реализовать свою работу намного эффективнее.

Локальная сеть объединяет в себе большое количество рабочих узлов-компьютеров, серверов и различных периферийных устройств, таких как принтеры и сканеры. Она значительно повышает эффективность и производительность работы предприятия в офисе или группе офисов.

Локальная сеть обеспечивает сотрудников постоянным одновременным доступом ко всем ресурсам сети, выходом в глобальную сеть Internet а также предоставляет в пользование все периферийные устройства. Она дает возможность комфортного и мгновенного обмена данными между сотрудниками.

Очень важно чтобы локальная сеть предприятия работала бесперебойно и имела повышенную отказоустойчивость, поскольку простой в работе предприятия зачастую несет для компании огромные финансовые потери. Для того чтобы обеспечить стабильную работу предприятия существует множество технологий. Этими технологиями могут быть как специально разработанные протоколы, так и рекомендации к организации локальной сети предприятия, а также различные технические решения.

Как правило, системные администраторы это те специалисты, которые обеспечивают сеть предприятия стабильной работой. В случае долгих простоев предприятия и не решенных проблем в сети именно на этого специалиста будет возложена ответственность, поскольку одна из главных функций системного администратора это обеспечение стабильной и бесперебойной работы сети предприятия.

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						4

Темой данной курсовой работы является: «Обеспечение отказоустойчивости и бесперебойной работы сети предприятия».

В данной курсовой работе будут рассмотрены следующие темы:

- Рекомендации по проектированию топологии отказоустойчивой сети предприятия.
- Обеспечение отказоустойчивости сети предприятия техническими средствами.
- Различные технологии и протоколы обеспечивающие отказоустойчивость сетевого оборудования.
- Репликация и резервирование в Windows Server 2019.
- Мониторинг серверов с помощью Zabbix сервера на базе Linux.

Данная курсовая работа определенно очень важна и рекомендуется к прочтению для специалистов в области системного администрирования.

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						5

## Раздел 1. Теоретическая часть.

### 1.1 Технические решения по обеспечению бесперебойной и отказоустойчивой работы сети предприятия

#### 1.1.1 Введение.

Перед тем как закупать оборудование и начинать его установку нужно, спроектировать топологию сети предприятия. Поскольку именно после проектирования начинается этап реализации. Проектирование топологии поможет определиться с количеством и типом нужных устройств и их связей в сети, а также с их физическим расположением в пространстве. Также проектирование топологии поможет понять примерную стоимость внедрения сети на предприятие.

Проектирование топологии — это важный этап в организации и создания локальной вычислительной сети, на нём определяется структура ЛВС исходя из назначения сети, количество используемой техники: компьютеров, принтеров, сканеров, ip телефонов и тд.[1]

#### 1.1.2 Топология. Виды топологий.

Топология - это схема соединения и расположения всех устройств участвующих в локальной вычислительной сети (ЛВС). [2]

Различают два основных типа топологий:

- 1) Логическая топология сети — Это схема, в которой указаны все соединения устройств в сети независимо от их реального расположения а также направленность потоков данных и способы передачи этих данных.[2]
- 2) Физическая топология сети — Это схема реального расположение всех устройств участвующих в ЛВС, а также их связей в пространстве.[2]

Топология сети имеет сильное влияния на отказоустойчивость ЛВС предприятия. Правильно выбранная топология это основа всех стабильно работающих компьютерных сетей.[3]

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						6

Основные виды топологий: звезда, шина, кольцо.[4]

В шинной топологии основным элементом является общий кабель к которому подключены компьютеры сети на его концах установлены терминаторы (заглушки).[5] В шинной топологии сигнал проходит от одного конца к другому концу каждое устройство в сети проверяет адрес сообщения и если адрес совпадает с адресом машины, то она принимает сообщение.

Если не совпадает, то сигнал уходит дальше по общему кабелю. К основным достоинствам данной топологии стоит отнести: легкость и гибкость в установке, а также поломка любого из устройств в топологии не влияет на работоспособность сети.[7] Основными недостатками являются: низкая производительность и то, что поломка или дефекты в общем кабеле приведут к неработоспособности ЛВС. На практике уже сложно найти место, где использовалась бы данная топология.

В топологии кольцо каждый компьютер соединен последовательно где последний компьютер соединен с первым, что образует круговое соединение от этого и название кольцо. Каждый компьютер в такой топологии выступает в роли повторителя, усиливая сигнал и отправляя его дальше по сети. Так как сигнал проходит через каждое устройство в сети то сбой одного компьютера приведет к поломке всей сети.[6]

Топология «Звезда» представляет собой соединение каждого компьютера к центральному устройству концентратору. Число устройств работающих в сети зависит от количества портов концентратора или коммутатора. Сети с такой топологией не дороги и легки в установке.[6]

Одним из главных преимуществ в сетях с топологией «Звезда» является то, что в них есть возможность мониторинга и централизованного управления сетью. При централизованном управлении сетью поиск дефектов в сети максимально упрощается. К недостаткам можно отнести только то, что для построения такой сети понадобится большое количество кабеля и то что поломка центрального устройства приведет к полной не работоспособности сети.[8]

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						7

Но в основном на практике используют сети с комбинированными топологиями. Они комбинируют в себе вышеперечисленные топологии. Стоит отметить что в случае использование небольшого кол-во конечных устройств и если нет в планах расширения офиса и соответственно сети, то возможно для данного варианта идеальным решением будет топология звезда.[10]

### 1.1.3 Трех уравнивая иерархическая модель сети.

Это модель, в которой описывается взаимодействие устройств участвующих в ЛВС и их распределение на логические уровни в зависимости от выполняемых функций в сети.[2]

Современные компьютерные сети очень сложны, поскольку в них используется множество протоколов, с конфигурациями и технологиями. С помощью иерархии можно организовать все компоненты в легко рассматриваемой модели. Притом, модель будет определять характеристики каждого иерархического уровня. Трех уровневая иерархическая модель помогает в проектирование, реализации и обслуживании масштабируемых, а также надежных и отказоустойчивых компьютерных сетей.

Основные плюсы иерархической модели и цели ее внедрения:

- Гибкость позволяет внедрять только те решения, которые необходимы для сети компании в данный момент. Масштабируемость сети в случае нужды благодаря модульности.[2]
- Простота внедрения в организацию, то есть быстрое развертывание.
- Простота в управлении сетевой инфраструктурой;[2]
- Избыточность, отказоустойчивость и безопасность. В случае выхода из строя основного устройства, сеть продолжает работать в штатном режиме. Также сеть работает стабильно во время атак.[2]
- Модульность. Обеспечивает гибкость в проектировании сети и облегчает простое внедрение и устранение неполадок.[2]

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						8

В данной модели определены следующие три уровня:

- Базовый уровень (уровень ядра) — Core Layer.
- Уровень распространения — Distribution layer .
- Уровень доступа — Access layer.

Для предприятия с количеством пользователей не более 10 имеет смысл внедрять только уровень доступа. Для организации, использующей несколько этажей или целое здание, будет правильным применение и уровня доступа и уровня распределения. Для сетей, соединяющих несколько зданий нужны все три уровня, а именно: уровень доступа, уровень распределения и уровень ядра.[7]

### **Уровень доступа.**

Данный уровень является точкой входа в сеть всех пользователей и сетевых устройства (таких как принтеры, сканеры, ip-телефоны и т. д.). Также здесь происходит управление пользователями и рабочими группами при обращении к общим ресурсам сети. Как правило, устройствами уровня доступа являются коммутаторы второго уровня (L2) модели OSI. Здесь происходит первичное сегментирование сети с использованием технологии VLAN. Так как именно через этот уровень происходит подключение всех устройств к сети важно предусмотреть защиту пользователей и ресурсов предприятия.[6]

Рекомендации по реализации данного уровня на предприятии.

Если планируется использование следующих сетевых устройств (ip-камеры, ip-телефоны, беспроводные точки доступа WI-FI) то будет правильно использовать коммутаторы с поддержкой технологии PoE. Это упростит, а также удешевит использование данных устройств, благодаря исключению необходимости питания от электросети.[9]

При выборе устройств стоит смотреть на те технологии, которые планируется использовать и сверять с возможностями рассматриваемого устройства, а также на стоимость за порт подключения.

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						9



## **Уровень распределения.**

Уровень распределения обслуживает множество важных сервисов сети. Основной задачей этого уровня является агрегация и объединение всех коммутаторов уровня доступа в единую сеть. Это позволяет существенно уменьшить количество соединений. Как правило, именно к коммутаторам распределения подключаются самые важные сервисы сети. Для создания данного уровня обычно используются коммутаторы третьего уровня (L3) модели OSI. Здесь происходит маршрутизация трафика между сегментами сети (VLAN), перенаправление маршрутов между маршрутизаторами сети. Также на этом уровне иногда используются статические маршруты для изменений в маршрутизации на основе динамических протоколов. На уровне распределения реализуется система безопасности в частности списки доступа (ACL). [10]

## **Базовый уровень (Core layer).**

Это самый верхний уровень, в иерархической модели который отвечает за быструю и надежную отправку больших объемов трафика. Его предназначение это скоростная коммутация трафика. Данный уровень формирует ядро ЛВС. Основной задачей является коммутация и объединение всех коммутаторов уровня распределения в единую сеть. На данном уровне используют коммутаторы третьего уровня (L3). Поскольку ошибка на базовом уровне приводит к не дееспособности сети то стоит обеспечить максимальную надежность на этом уровне. Здесь обрабатываются большие объемы трафика, поэтому не менее важно учитывать скорость и задержки. Не списки доступа, не маршрутизация между виртуальными локальными сетями VLAN, не фильтрация пакетов не должны замедлять трафик. На уровне ядра стоит выбирать протокол маршрутизации с максимально быстрой конвергенцией. На данный момент для устройств cisco хорошим выбором будет протокол динамической маршрутизации EIGRP, поскольку он имеет наиболее быструю конвергенцию.[8]

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						10

Также очень важно правильно реализовывать техническую сторону сетевой инфраструктуры. Правильное обустройство серверной комнаты, использование бесперебойных источников питания, а также грамотный монтаж СКС позволит работать сети организации с минимальным количеством технических и аппаратных ошибок в сети. Это естественно хорошо скажется на отказоустойчивости и бесперебойности работы сети предприятия. [4]

#### **1.1.4 Серверная комната.**

Сама по себе серверная комната больше нужна для обеспечения безопасности хранения данных, а также централизованного доступа к ним, нежели чем для обеспечения отказоустойчивости или бесперебойной работы сети предприятия. Но поскольку многие компании используют собственные серверные комнаты, то считаю важным поднять эту тему и раскрыть ее с точки зрения обеспечения отказоустойчивости оборудования в таких комнатах. [10]

##### **Охлаждение.**

Серверная комната — это такое помещение, в котором находиться очень большое количество сетевых устройств, самих серверов на которых хранятся данные компании, различных ИБП и персональных компьютеров, зачастую такая комната по правилам безопасности не имеет окон и находится в удаленном месте от входа на предприятие, для затруднения проникновения несанкционированных лиц. И конечно вся техника в серверной комнате имеет свойство нагреваться. Излишне говорить, что высокие температуры плохо сказываются на работоспособности оборудования. Желательная температура в помещении от 18 до 27°C. В идеале нужно два отдельных кондиционера, которые включаются посменно, поддерживая непрерывную работу серверного оборудования.[6]

##### **Кабель менеджмент.**

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						11

Хороший менеджмент кабелей сложно переоценить, так как почти каждый элемент в стойке связан с кабелями Ethernet. Поэтому правильно будет использовать разные цвета проводов для Ethernet LAN, IP видеокамер и других сетевых подключений. К основным решениям для создания хорошего кабель менеджмента можно отнести различные зажимы, стяжки и хомуты.

Все эти решения помогают правильно укладывать кабели. [10]

Очень важно также проводить маркировку оборудования, поскольку благодаря маркировки можно будет намного быстрее найти неисправный узел в сети. Самыми простыми способами сделать маркировку кабелей и сетевого оборудования это использование скотча, бумаги, фломастера или малярного скотча и фломастера. Также существуют специальные маркировочные принтеры. Маркирование принтером получается более качественное и красивое, но такой принтер стоит неплохих денег, поэтому если на предприятии нету огромного дата центра, то лучше использовать более простые варианты маркирования.

### **1.1.5 Бесперебойные блоки питания.**

Плохое электропитание – это одна из основных угроз выхода из строя конечных устройств участвующих в сети, а также сетевого оборудования.

Независимо из того, что помехи, возникающие в электросети, носят периодический характер, они оказывают плохое влияние на компоненты современных электронных устройств, подключаемых к розетке. Для защиты критически необходимого оборудования или сохранения данных при исчезновении питающего напряжения наиболее часто используются источники бесперебойного питания.[1]

Назначение ИБП (Источник бесперебойного питания) – обеспечение корректной работы нагрузки при резких «провалах» или «всплесках» напряжения, а также обеспечение кратковременной автономной работы подключенного оборудования при полном отключении электроэнергии.[3]

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						12

Современные ИБП делятся на три класса:

- Резервные или Offline;
- Линейно-интерактивные;
- С двойным преобразованием энергии.

### **ИБП резервного типа Offline.**

Основная сфера применения ИБП резервного типа – защита бытового компьютерного и мультимедийного оборудования. Схема работы данного типа ИБП предельно проста: в штатном режиме оборудование питается от сети, а при исчезновении в ней напряжения прибор переключается в режим работы от батареи. Время переключения между типами подачи энергии - ненулевое. ИБП резервного типа рекомендуется к использованию для домашнего ПК.[2]

### **ИБП Линейно-интерактивные.**

К преимуществам ИБП линейно-интерактивного типа можно отнести плавную стабилизацию сигнала, а также возможность работы в широком диапазоне входных напряжений. При существенной нестабильности сети (частых колебаниях напряжения в диапазоне от 15-20 В) резервный ИБП будет постоянно переключать нагрузку на автономное питание, что негативно скажется на сроках службы батарей. Линейные ИБП больше подходят для сетей с нестабильным напряжением для защиты: мониторов, системных блоков, узлов ЛВС, рабочих станций, компьютерной периферии и прочих устройств с импульсными блоками питания, что делает его отличным ИБП для офиса.[2]

### **ИБП с двойным преобразованием напряжения (Online).**

Наиболее совершенный в плане защиты оборудования – ИБП с двойным преобразованием напряжения. Для него характерно мгновенное переключение между режимами работы и независимость параметров сигнала на выходе от параметров на входе. Поэтому именно этот тип ИБП

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						13

предназначен для защиты: серверов, рабочих станций, узлов связи и медицинского оборудования, то есть для критически важных устройств.[2]

Можно сделать вывод, что для обычных рабочих станций стоит выбирать Линейно интерактивный ИБП, а для серверов и сетевого оборудования ИБП с двойным преобразованием напряжения.[8]

### **1.1.6 Монтаж СКС, основные принципы.**

При монтаже СКС стоит соблюдать следующие принципы:

#### **Первый принцип — надежность.**

Ненадежная сеть всегда выйдет дороже за счет стоимости ее обслуживания, убытков при простое и убытков от постороннего вмешательства.[4] Исходя из этого принципа, всегда стоит проектировать основную сеть только проводной, и при необходимости использовать дополнительную беспроводную сеть (гостевая сеть Wi-Fi). Беспроводная сеть менее надежная, так как у любой беспроводной сети есть ряд проблем с безопасностью, стабильностью и совместимостью. Беспроводная сеть слишком не надежно для серьезных компаний.[4]

Надежность определяет и структуру сети. Топология «Звезда», о которой уже говорили выше, это идеал к которому нужно стремиться. «Звезда» сокращает необходимое количество коммутаторов, количество уязвимых trunk линий, упрощает обслуживание. Намного проще искать проблему в одном коммутаторе, чем в нескольких разбросанных по кабинетам.[7]

Если не удастся поместить все коммутаторы в одно место, то смешанную топологию использовать будет правильнее, т.к. все trunk линии пойдут разными трассами, что сведет к минимуму вероятность одновременного повреждения нескольких магистралей. [10]

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						14

Коммутаторы соединенные trunk линиями обязаны иметь резервный канал, тогда в случае неисправности одной из линий связь между узлами останется и ни одно соединение не будет потеряно. Это позволит системному администратору спокойно перетянуть поврежденный кабель.[9]

### **Второй принцип — рациональность и практичность.**

Практично использовать по 2 розетки rj45 на место. Вторая линия может понадобиться, к примеру, для подключения аналогового (цифрового) телефона, или она может быть просто резервной [1]. Две розетки обычно используют в крупных компаниях. Для малого и среднего бизнеса рациональнее использовать по одной компьютерной розетке на рабочее место, поскольку IP телефоны в основном имеют два порта — входящий порт и второй для подключения через него компьютера. Для сетевых принтеров нужно проектировать отдельное рабочее место, и располагать по возможности удобно для всех использующих его сотрудников, например в коридорах. Решать что важнее — рациональность или практичность должен человек компетентный в IT сфере от руководства предприятия или компании. К принципу рациональности и практичности также относиться выбор оборудования и материалов. Всем известно высказывание «скупой платит дважды», поэтому не стоит экономить на материалах. Использовать омедненную витую пару вместо медной, значит гарантированно через пару лет получить проблему плохих соединений.[8]

Не стоит отказываться от патчпанелей, заводских патчкордов и органайзеров, так как в противном случае можно получить через какое-то время неразбериху в серверном шкафу, постоянно «отваливающиеся» линки и окисление коннекторов.[9]

Не стоит экономить и на серверном шкафу [8]. Большой размер не только позволит разместить в нем больше оборудования, но и облегчит его обслуживание.

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						15

Качественные заводские патчкорды должны быть как на рабочих местах, так и в серверном шкафу. Если посчитать время, затраченное на обжимание коннекторов и стоимость материалов, то купить заводской патчкорд окажется дешевле.

В обычных случаях для рабочей станции работать на скоростях 10G нет нужды, поэтому рациональнее использовать витую пару категории 5е, а не 6-й, поскольку она дешевле, тоньше, гибче и соответственно удобнее в монтаже.

### **Упорядоченность.**

Третий принцип — это упорядоченность. Чем больше сеть, тем более важно иметь порядок в сети.[4] Розетки и порты патчпанелей должны быть обязательно пронумерованы. Нумерация обычно начинается по рабочим местам слева направо от входа в помещение. Обязательно должен быть утвержденный план помещений с расположением и нумерацией розеток. Именно для упорядоченности, а не для физического разделения сетей используются патчпанели.

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						16

## **1.2 Обеспечение отказоустойчивой и бесперебойной работы сетевого оборудования.**

Помимо различных технических решений для обеспечения отказоустойчивости и бесперебойной работы сети предприятия также есть и программные. В данные решения можно включить различные сетевые протоколы, средства операционных систем, различные системы мониторинга и тд. — в общем, это все что обеспечивает или помогает обеспечивать стабильную и бесперебойную работу сети предприятия.

В данном пункте будут рассмотрены различные протоколы, применяемые на различных уровнях трехуровневой модели сети с целью обеспечения отказоустойчивой и бесперебойной работы сети предприятия.

### **1.2.1 Технология VLAN.**

Сегментирование сети это один из самых важных этапов в проектирование топологии. Оно позволяет разделить права доступа на тот или иной ресурс сети, что благополучно сказывается на безопасности сети. Сегментирование сети происходит благодаря использованию технологии VLAN [1].

VLAN (Virtual Local Area Network, виртуальная локальная сеть) – эта технология позволяет на одном физическом интерфейсе маршрутизатора или коммутатора создать несколько виртуальных локальных сетей.[1]

VLAN позволяет:

- 1) Гибко разделить устройства на сегменты (группы).
- 2) Уменьшить объем широковещательного трафика в сети.
- 3) Обеспечить безопасность и управляемость в сети.

Благодаря данной технологии порты коммутатора уровня доступа разделяются на сегменты.

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						17



### 1.2.2 Технология DHCP Snooping.

Чаще всего в локальной сети есть только один DHCP сервер. Как правило появление второго DHCP сервера генерирует конфликт ip адресов.

На практике иногда случается, что пользователи подключают свои неправильно сконфигурированные устройства к локальной сети и вызывают ошибку. Также существует угроза подключение к сети злоумышленника, который настраивает свой DHCP сервер и выполняет атаку на основной DHCP сервер с целью исчерпания его ресурсов (ip адресов).

После такой атаки пользователи получают ложные данные, такие как шлюз по умолчанию, в результате чего злоумышленник получает контроль над трафиком в локальной сети.

Чтобы защититься от подобной атаки можно воспользоваться технологией на коммутаторах cisco DHCP snooping. Суть этой технологии заключается в разделении портов коммутатора на доверенные (Trust) и не доверенные (Untrust).[2]

Доверенные — это порты, к которым подключаются корпоративные DHCP сервера или же коммутаторы, к которым уже подключен DHCP сервер.[2]

Не доверенные — это порты, которые будут подниматься при подключение другого DHCP сервера, но в тоже время будут блокировать его настройки.[2]

### 1.2.3 Технология HSRP.

HSRP (Hot Standby Router Protocol) - проприетарный протокол Cisco, главная задача, которого добиться максимальной отказоустойчивости маршрутизаторов выполняющих роль шлюза по умолчанию или коммутаторов L3.[8] Отказоустойчивость достигается объединением маршрутизаторов в standby группу и назначением общего IP-адреса, который будет использоваться как шлюз по умолчанию. В случае поломки основного маршрутизатора начинает работать резервный.

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						18

В терминологии HSRP существует несколько базовых понятий:

- 1) Активный маршрутизатор (Active Router) — маршрутизатор или коммутатор третьего уровня, выполняющий роль виртуального маршрутизатора и организовывающий отправку пакетов из одной подсети в другую.[6]
- 2) Резервный маршрутизатор (Standby Router) — маршрутизатор или коммутатор третьего уровня, выполняющий роль запасного виртуального маршрутизатора, ждущего отказа активного маршрутизатора в рамках одной HSRP группы.[6]
- 3) Группа резервирования (Standby Group) — группа маршрутизирующих устройств, которые являются членами одной HSRP - группы и обеспечивают работу и отказоустойчивость виртуального маршрутизатора.[6]

Протокол HSRP будет настраивать в практической части на уровне распределения, а именно на коммутаторах 3 (L3) уровня.

#### **1.2.4 Создание резервных копий конфигурации с помощью сервера и протокола TFTP .**

Стоит отметить, что в процессе работы сети могут случаться разные неполадки и в том числе поломка оборудования и чтобы не тратить время, на то чтобы заново настроить конфигурацию на новом оборудовании стоит озаботиться резервным копированием данных. Для этого можно воспользоваться TFTP (Trivial File Transfer Protocol — простой протокол передачи файлов) и сервером с его использованием.[7] Резервные копии стоит делать для всего оборудования.

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						19

### 1.2.5 Агрегирование каналов, технология LACP.

Агрегирование каналов — технология, позволяющая объединить несколько физических каналов (соединений) в один логический канал передачи данных. Такое объединение позволяет увеличивать пропускную способность и надежность канала, что в свою очередь улучшает отказоустойчивость сети. Агрегирование каналов может быть настроено между двумя коммутаторами, коммутатором и маршрутизатором, между коммутатором и хостом.[8]

Агрегирование каналов позволяет решить две задачи:

- повысить пропускную способность канала, то есть увеличивать предел возможной нагрузки на канал передачи данных.
- обеспечить резерв на случай потери одного из соединений

Хоть агрегирование каналов и позволяет увеличить пропускную способность канала, но не стоит рассчитывать на хорошую балансировку нагрузки между интерфейсами в агрегированном канале. Реальная загруженность конкретного интерфейса никак не учитывается. Поэтому один интерфейс может быть загружен больше, чем другие.[1]

Для агрегирования каналов в Cisco может быть использован один из трёх вариантов:

- LACP (Link Aggregation Control Protocol) стандартный протокол
- PAgP (Port Aggregation Protocol) проприетарный протокол Cisco
- Статическое агрегирование без использования протоколов

Так как LACP и PAgP решают одни и те же задачи (с небольшими отличиями по возможностям), то лучше использовать стандартный протокол.

Фактически остается выбор между LACP и статическим агрегированием.

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						20

Сравнение статического агрегирования и протокола LACP (Таблица №1).

Таблица №1.

Способ агрегирования	Преимущества	Недостатка
Статическое агрегирование	Не вносит дополнительную задержку при поднятии агрегированного канала или изменении его настроек. Вариант, который рекомендует использовать Cisco[1]	Нет согласования настроек с удаленной стороной. Ошибки в настройке могут привести к образованию петель
С помощью протокола LACP	Согласование настроек с удаленной стороной позволяет избежать ошибок и петель в сети. Поддержка standby-интерфейсов позволяет агрегировать до 16ти портов, 8 из которых будут активными, а остальные в режиме standby.[5]	Вносит дополнительную задержку при поднятии агрегированного канала или изменении его настроек.

Судя из (таблицы №1) для соединений коммутаторов (L2 - L2) можно использовать статическое агрегирование, но для соединений где, скорее всего, будет использоваться технология HSRP нужно использовать протокол LACP. И все-таки из-за возможных ошибок статического агрегирования лучше везде использовать LACP [2].

При настройке агрегирования каналов на оборудовании **Cisco** используется несколько терминов:

- **EtherChannel** — технология агрегирования каналов. Термин, который использует **Cisco** для агрегирования каналов.
- **port-channel** — логический интерфейс, который объединяет физические интерфейсы.
- **channel-group** — команда, которая указывает какому логическому интерфейсу, принадлежит физический интерфейс и какой режим используется для агрегирования.

### 1.2.6 Динамическая маршрутизация OSPF или EIGRP.

Как говорилось ранее, EIGRP является более предпочтительным протоколом динамической маршрутизации для уровня ядра, но если рассматриваем уровень распределения с количеством маршрутизирующих устройств более 15 штук, то тут лучше использовать OSPF.[3] Для того чтобы убедиться в данном тезисе произведем сравнение этих протоколов.

Алгоритм и производительность.

OSPF использует в маршрутизации алгоритм SPF (Shortest Path First). SPF зависит от пропускной способности для расчета метрики, то есть рассчитывает стоимость каждой конкретной линии связи и на основе полученных данных узнается наиболее короткий путь с наименьшей общей стоимостью. В OSPF храниться информация обо всех сетях в конкретной области. Каждый раз, когда происходит изменение в области, все маршрутизаторы повторно синхронизируют свои базы данных, а затем снова запускают SPF. Данный процесс занимает много ресурсов процессора.[3]

EIGRP использует протокол DUAL (Diffusive Update Algorithm). DUAL использует пропускную способность и задержку для вычисления метрики с использованием сложных формул. В отличие от OSPF, при изменений в сети

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						22

передается не вся таблица маршрутизации, а только изменения в таблице, это значительно уменьшает нагрузку на сеть. Также данный протокол занимает меньше ресурсов процессора. [3]

В практической части данной курсовой работы будет использоваться протокол EIGRP, поскольку в выбранной топологии будет только два L3 коммутатора на уровне распределения. Уровень ядра же не будет конфигурироваться в практической части данной курсовой работы. Уровень ядра заменит машина на базе Linux EvE ng, на которой будет располагаться сетевое оборудование. Данная машина будет выступать в роли маршрутизатора между сетевым оборудованием и серверами.

### **1.3 Репликация и резервирование.**

В данной курсовой работе в практической части будет рассматриваться настройка двух Windows server 2019 с точки зрения обеспечения отказоустойчивой работы данных серверов.

#### **1.3.1 Резервирование на RAID средствами Windows server 2019.**

Для возможности восстановления системы в случае сбоя будет использоваться служба архивирования Windows server. Также к одному из серверов будет подключены два диска одинакового объема для создания RAID 0 массива (Зеркальный том). На этот RAID будет производиться резервное копирование службами архивации Windows server. Такое решение позволит быть уверенным в том, что в случае поломки основного жесткого диска можно будет поменять диск и быстро восстановить систему с RAID.

Служба архивации Windows server использует интересный подход к созданию резервных копий. Во первых используется служба теневого копирования тома (VSS), которая позволяет работать в момент резервного копирования с открытыми файлами.[10] Во вторых для данной службы выделяется отдельный диск, на который происходит резервирование, причем

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						23

работает оно по принципу работы видеонаблюдения, то есть при не достатке места для создания резервной копии происходит перезапись самой старой резервной копии на диске. В третьих можно настроить автоматическое резервное копирование в определенное системным администратором время суток.[10] Все вышеперечисленное делает резервное копирование с помощью средств Windows server очень удобным в применении.

### **1.3.2 Дополнительный контроллер домена Active Directory.**

Как уже было выше сказано, в практической части данной курсовой работы будет использоваться два Windows server 2019. В большинстве случаев если на предприятии используют Windows server то обязательно используются и Active Directory [2]. Добавление в сеть дополнительно контроллера домена позволяет обеспечить отказоустойчивость данной службы, а также уменьшает нагрузку на основной сервер.[6]

Дополнительный котроллер домена реплицирует данные с основного сервера, тем самым имея идентичные данные служб каталогов и тд.

### **1.3.3 Файловый сервер TFTP.**

Для создания резервных копий конфигураций сетевого оборудования понадобится TFTP сервер, где будут храниться эти копии. В данной работе будет использоваться сторонняя программа tftpd64. Есть два варианта установки данного программного обеспечения: как службу (service edition) и как приложение (standard edition). Для задачи, решаемой в практической части данной курсовой работы будет лучше установить это ПО как службу.

### **1.4 Мониторинг сети. Система мониторинга zabbix.**

Каждый уважающий себя системный администратор должен иметь систему мониторинга сети. Почему же так важно иметь систему мониторинга?

Термином мониторинг сети называют работу системы, которая выполняет непрерывное наблюдение за компьютерной сетью в поисках медленных или неисправных узлов сети и которая при обнаружении сбоев сообщает о них

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						24

сетевому администратору с помощью почты, телефона или других средств оповещения.

Системы мониторинга, позволяют заранее понять, какой компонент сети имеет, какие либо проблемы. Системы мониторинга позволяют отслеживать все данные состояния устройств участвующих в сети предприятия, что позволяет в свою очередь выявить будущую проблему, к примеру, заканчивающееся место на диске на хосте.

Это позволяет запланировать системному администратору техническое обслуживание устройств до их полного выхода из строя.

Также системы мониторинга позволяют намного быстрее найти неисправный узел в сети, что в свою очередь намного увеличивает скорость исправления неисправности в сети.

В данной курсовой работе будет рассматриваться бесплатная система мониторинга zabbix. Так как темой данной курсовой работы не являются системы мониторинга, то подробных сравнений систем мониторинга тут не будет. Предпочтение к данной системе мониторинга было выбрано на основе того что она бесплатная и знакома автору данной курсовой работы.

Данный zabbix сервер будет развернут на отдельном сервере, на базе операционной системы Linux Debian 9.

На мониторинг будут поставлены для примера оба Windows сервера с помощью zabbix клиента установленного на эти сервера.

Хотя система мониторинга Zabbix и позволяют настраивать гибко то, что конкретно будет мониториться на определенной машине и создавать свои собственные оповещения, но рассматриваться данная тема не будет в этой курсовой работе. На мониторинг устройства будут поставлены по заготовленным шаблонам. Также на сервере будут настроены оповещения по email и создана карта сети.

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						25



## Раздел 2. Практическая часть.

### 2.1 Проектирование топологии.

В сети предприятия есть два коммутатора L2 и два L3 коммутатора, а также 2 типа PC находящиеся в разных подсетях и три сервера два из которых это Windows сервера и один Debian 9 Zabbix сервер. Коммутаторы L2 находятся в разных отделах офиса, а L3 и сервера в серверной комнате. К L2 коммутаторам подсоединены по два ПК, один из которых относится к подсети сотрудников, а другой к подсети администраторов.

Рассмотрим спроектированную топологию (Рис.1).

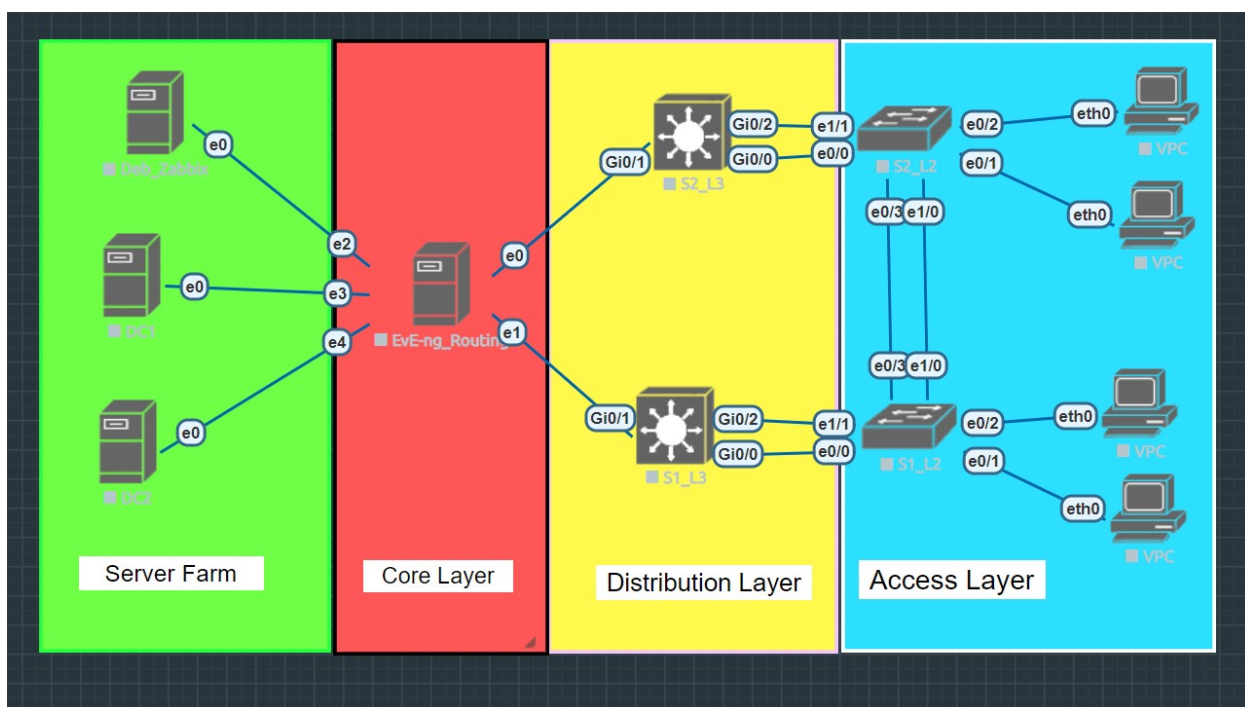


Рис.1 - Топология.

Уровень доступа (Access Layer).

На уровне доступа у нас есть два коммутатора L2 соединенные вместе двумя физическими каналами связи. Также они соединены с коммутаторами L3 двумя физическими каналами. Благодаря избыточности добивается повышенная отказоустойчивость. И дополнительно к коммутаторам L2 подключено четыре ПК.

Уровень распределения (Distribution Layer).

На уровне распределения, находятся два L3 коммутатора которые соединены с двумя L2 коммутаторами посредством двух физических каналов.

Уровень ядра (Core Layer).

В физическом плане на данном уровне находится EvE-ng машина на базе Linux которая выступает в роли гипервизора. На ней запущены виртуальные операционные системы сетевого оборудования. Данная машина выступает в роли маршрутизирующего устройства, маршрутизируя трафик от сетевого оборудования к виртуальным машинам серверов.

Серверная ферма (Server Farm).

На данном уровне находятся три виртуальные машины серверов, 2 из которых Windows server 2019 и один Zabbix сервер. Они подключены к EvE-ng виртуальной машине.

## 2.2 Настройка сетевого оборудования.

Произведем настройку сетевого оборудования. В начале, произведем базовую настройку устройств. Отключим поиск DNS имен и зададим имена хостам (Рис.2).

```
Switch(config)#no ip domain lookup
Switch(config)#hostname S1-L3
S1-L3(config)#
Switch(config)#no ip domain lookup
Switch(config)#hostname S2_L3
S2_L3(config)#
S2-L2(config)#no ip domain lookup
S2-L2(config)#hostname S2-L2
S2-L2(config)#
Switch(config)#no ip domain lookup
Switch(config)#hostname S1-L2
S1-L2(config)#
```

Рис.2 – Настройка.

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						27

### 2.2.1 Настройка коммутаторов L3.

На L3 коммутаторах настроим интерфейсы. Для начала переведем порты в режим L3 и зададим IP адреса на интерфейсы, после поднимем их (Рис.3).

```
S1-L3(config)#int g0/1
S1-L3(config-if)#no sw
S1-L3(config-if)#no switchport
S1-L3(config-if)#ip ad
*Dec 10 12:10:50.385: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed
e to up
*Dec 10 12:10:51.389: %LINEPROTO-5-UPDOWN: Line protocol on Interface Gigab
ernet0/1, changed state
S1-L3(config-if)#ip add 172.16.4.2 255.255.255.0
S1-L3(config-if)#no sh
S1-L3(config-if)#
S2_L3(config)#int g0/1
S2_L3(config-if)#no sw
S2_L3(config-if)#no switchport
S2_L3(config-if)#
*Dec 10 12:11:53.300: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed
e to up
*Dec 10 12:11:54.302: %LINEPROTO-5-UPDOWN: Line protocol on Interface Gigab
ernet0/1, changed state to up
S2_L3(config-if)#ip add 172.16.4.3 255.255.255.0
S2_L3(config-if)#
```

Рис.3 – Настройка сетевых интерфейсов.

Произведем настройку VLAN с номерами 10 и 20. И пробросим их через широковещательные интерфейсы, также не забываем перевести порты в магистральный trunk режим (Рис.4-5).

```
S1-L3(config-if)#int vlan 10
S1-L3(config-if)#ip add 192.168.10.1 255.255.255.0
S1-L3(config-if)#int vlan 20
S1-L3(config-if)#ip add 192.168.20.1 255.255.255.0
S1-L3(config-if)#int range g0/0,g0/2
S1-L3(config-if-range)#switchport trunk allowed vlan 10,20
S1-L3(config-if-range)#switchport trunk encapsulation dot1q
S1-L3(config-if-range)#switchport mode trunk
S1-L3(config-if-range)#
```

Рис.4 – Настройка S1-L3.

```
S2_L3(config-if)#int vlan 10
S2_L3(config-if)#ip add 192.168.10.2 255.255.255.0
S2_L3(config-if)#int vlan 20
S2_L3(config-if)#ip add 192.168.20.2 255.255.255.0
S2_L3(config-if)#int range g0/0,g0/2
S2_L3(config-if-range)#switchport trunk allowed vlan 10,20
S2_L3(config-if-range)#switchport trunk encapsulation dot1q
S2_L3(config-if-range)#switchport mode trunk
S2_L3(config-if-range)#
```

Рис.5 – Настройка S2-L3.

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						28

Настроим маршрутизацию. Для начала необходимо включить маршрутизацию командой (ip routing) , после прописываем маршрут по умолчанию до адреса сетевого интерфейса pnet5 виртуальной машины Eve-ng (ip route 0.0.0.0 0.0.0.0 172.16.4.1) после переходим к настройке протокола EIGRP (Рис.6 – Рис.7).

```
S1-L3(config)#ip routing
S1-L3(config)#ip route 0.0.0.0 0.0.0.0 172.16.4.1
S1-L3(config)#router eigrp 1
S1-L3(config-router)#network 192.168.10.0 0.0.0.255
S1-L3(config-router)#network 192.168.20.0 0.0.0.255
S1-L3(config-router)#
```

*Рис.6 – Настройка маршрутизации S1-L3.*

```
S2_L3(config)#ip routing
S2_L3(config)#ip route 0.0.0.0 0.0.0.0 172.16.4.1
S2_L3(config)#router eigrp 1
S2_L3(config-router)#network 192.168.10.0 0.0.0.255
S2_L3(config-router)#network 192.168.20.0 0.0.0.255
S2_L3(config-router)#
```

*Рис.7 – Настройка маршрутизации S2-L3.*

### 2.2.2 Настройка маршрутизации на виртуальной машине Eve-ng.

После необходимо настроить маршрутизацию на машине Eve-ng.

Подключимся к машине по ssh и для начала включим на ней маршрутизацию в нутрии себя для этого необходимо изменить значение 0 на 1 в следующем файле (Рис.8).

```
root@192.168.1.11:22 - Bitvise xterm - root@eve-ng: ~
GNU nano 2.5.3 File: /proc/sys/net/ipv4/ip_forward
1
```

*Рис.8 – Включаем маршрутизацию.*

Теперь необходимо задать IP адрес на интерфейс pnet5 к которому подключены интерфейсы L3 коммутаторов. Для этого воспользуемся командой ip address add 172.16.4.1 dev pnet5 (Рис.9).

```
root@eve-ng:~# ip address add 172.16.4.1/24 dev pnet5
root@eve-ng:~#
```

*Рис.9 – Задаем адрес на интерфейс.*

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						29

Посмотрим таблицу маршрутизации (Рис.10).

```
root@eve-ng:~# netstat -r
Kernel IP routing table
Destination        Gateway             Genmask             Flags        MSS Window  irtt Iface
default            csp1.zte.com.cn    0.0.0.0             UG           0 0        0 pnet0
172.16.4.0         *                  255.255.255.0       U            0 0        0 pnet5
192.168.1.0        *                  255.255.255.0       U            0 0        0 pnet0
root@eve-ng:~#
```

Рис.10 – Таблица маршрутизации.

Проверим доступность с одного L3 коммутатора до другого (Рис.11).

```
S2_L3(config-router)#do ping 172.16.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.4.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/5/11 ms
S2_L3(config-router)#do ping 172.16.4.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.4.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/9/14 ms
S2_L3(config-router)#
```

Рис.11 – Проверка маршрутизации.

Для того чтобы был доступ к удаленным серверам произведем настройку ip tables на eve-ng (Рис.12).

```
root@eve-ng:~# iptables -t nat -A POSTROUTING -o pnet0 -s 172.16.4.0/24 -j MASQUERADE
root@eve-ng:~# iptables -t nat -A POSTROUTING -o pnet5 -s 192.168.1.0/24 -j MASQUERADE
```

Рис.12 – Настройка IPtables.

Проверим доступность рабочего компьютера, на котором находятся виртуальные машины. Для этого выполним команду ping до него (Рис.13-14).

```
Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . : 
Описание. . . . . : Intel(R) Dual Band Wireless-AC 8260
Физический адрес. . . . . : A0-C5-89-95-C5-1D
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::a2c5:89ff:fe95:c51d%3(Основной)
IPv4-адрес. . . . . : 192.168.1.17(Основной)
```

Рис.13 – Адрес основной машины.

```
S2_L3(config-router)#do ping 192.168.1.17
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.17, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/8/14 ms
```

Рис.14 – Доступность основной машины.

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						30

Проверка доступность L3 коммутатора с основной машины (Рис.15).

```
c:\Users\colt5>ping 172.16.4.2
Обмен пакетами с 172.16.4.2 по с 32 байтами данных:
Ответ от 172.16.4.2: число байт=32 время=20мс TTL=254
Ответ от 172.16.4.2: число байт=32 время=8мс TTL=254
Ответ от 172.16.4.2: число байт=32 время=8мс TTL=254
```

Рис.15 – Доступность S1-L3.

### 2.2.3 Настройка HSRP на L3 коммутаторах.

Перейдем к настройке протокола HSRP. Для этого переходим во VLAN интерфейсы, задаем standby группу и общий адрес, меняем версию протокола на 2 (Рис.16).

```
interface Vlan10
 ip address 192.168.10.2 255.255.255.0
 standby version 2
 standby 0 priority 110
 standby 0 preempt
 standby 0 track 1 decrement 10
 standby 1 ip 192.168.10.254
 shutdown
!
interface Vlan20
 ip address 192.168.20.2 255.255.255.0
 standby version 2
 standby 0 priority 110
 standby 0 preempt
 standby 0 track 1 decrement 10
 standby 2 ip 192.168.20.254
 shutdown
```

Рис.16 – Настройка HSRP.


Перейдем к настройке LACP (Рис.17). Указываем протокол а после номер группы и тип.

```
S1-L3(config-if-range)#int range g0/0,g0/2
S1-L3(config-if-range)#channel-protocol lacp
S1-L3(config-if-range)#channel-group 1 mode active
```

Рис.17 – Настройка LACP.



Произведём настройку dhcp сервера на S1-L3 для будущей проверки dhcp snooping (Рис.18). Исключаем уже используемые адреса в сети и настраиваем два пула для VLAN сетей, шлюзом выбираем адрес standby группы.

 S1\_L3

```
!
!!
!
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.10.2
ip dhcp excluded-address 192.168.10.254
ip dhcp excluded-address 192.168.20.254
ip dhcp excluded-address 192.168.20.2
ip dhcp excluded-address 192.168.20.1
!
ip dhcp pool 1
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.254
!
ip dhcp pool 2
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.254
```

*Рис.18 – Настройка DHCP.*

Попробуем получить ip адрес с клиента (Рис.19).

```
VPCS> ip dhcp
DORA IP 192.168.10.3/24 GW 192.168.10.254

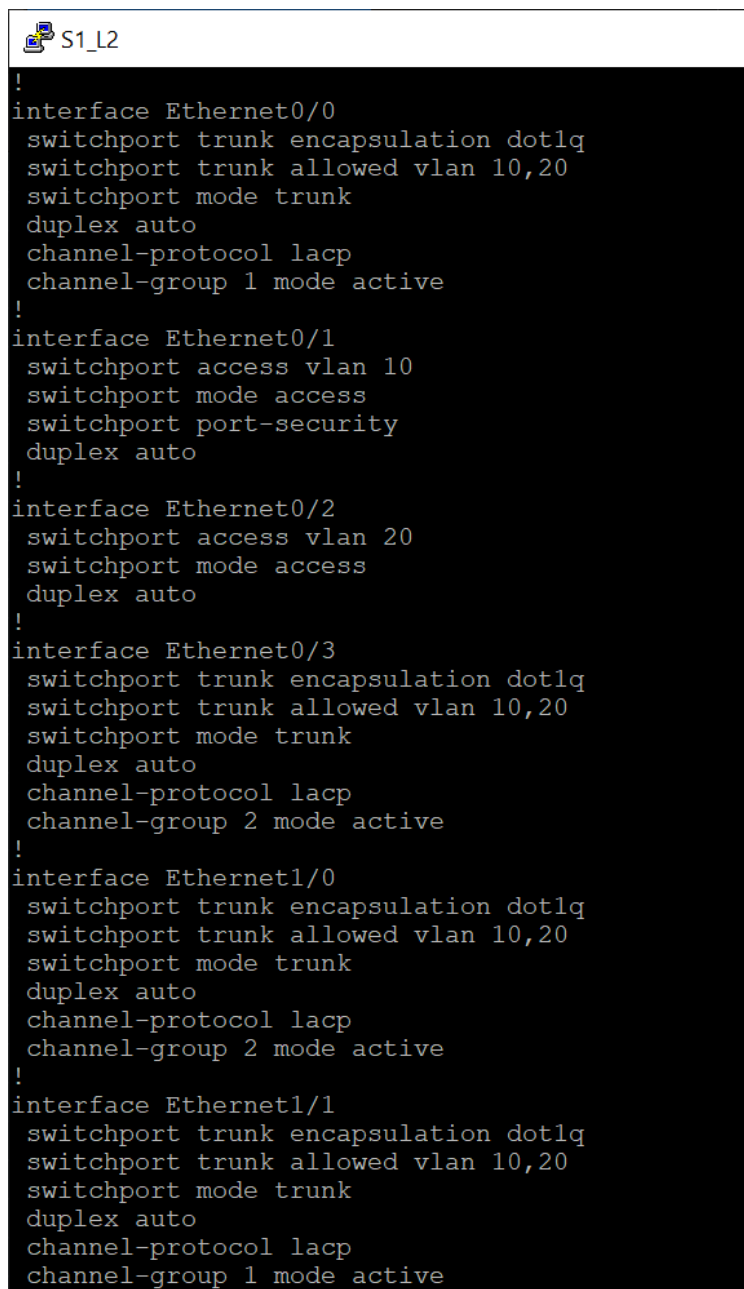
VPCS> █
```

*Рис.19 – Получение адреса.*

## 2.2.4 Настройка коммутаторов L2.

Настройка агрегирования и и VLAN.

Коммутатор S1-L2 (Рис.20). Прокидываем VLAN, а также настраиваем агрегирование LACP.



```
!
S1_L2
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 duplex auto
 channel-protocol lacp
 channel-group 1 mode active
!
interface Ethernet0/1
 switchport access vlan 10
 switchport mode access
 switchport port-security
 duplex auto
!
interface Ethernet0/2
 switchport access vlan 20
 switchport mode access
 duplex auto
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 duplex auto
 channel-protocol lacp
 channel-group 2 mode active
!
interface Ethernet1/0
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 duplex auto
 channel-protocol lacp
 channel-group 2 mode active
!
interface Ethernet1/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 duplex auto
 channel-protocol lacp
 channel-group 1 mode active
```

Рис.20 – Настройка интерфейсов.

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						33



Комутатор S2-L2 (Рис.21). Прокидываем VLAN, а также настраиваем агрегирование LACP.

```
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,20
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 1 mode active
!
interface Ethernet0/1
switchport access vlan 10
switchport mode access
duplex auto
!
interface Ethernet0/2
duplex auto
!
interface Ethernet0/3
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,20
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 2 mode active
!
interface Ethernet1/0
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,20
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 2 mode active
!
interface Ethernet1/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,20
switchport mode trunk
duplex auto
channel-protocol lacp
channel-group 1 mode active
!
```

*Рис.21 – Настройка интерфейсов.*

Настройка DHCP snooping. Вначале нужно включить DHCP snooping (Рис.22). Для в глобальной конфигурации пишем команду (ip dhcp snooping), а также включаем для нужных нам VLAN то есть 10 и 20.

```
S1-L2(config)#ip dhcp snooping
S1-L2(config)#ip dhcp snooping vlan 10,20
S1-L2(config)#
```

*Рис.22 – Включение DHCP snooping.*

Попробуем получить ip адрес теперь с PC. Поскольку все порты по умолчанию не являются доверенными то ПК не получает адрес (Рис.23).

```
VPCS> ip dhcp
DDD
Can't find dhcp server
```

*Рис.23 – Не удалось найти dhcp сервер.*

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						34

А теперь сделаем порты доверяемыми которые подключены к S1-L3 на котором настроен DHCP (Рис.24).

```
S1-L2(config)#int range e0/0,e1/1
S1-L2(config-if-range)#ip dhcp snooping trust
```

Рис.24 – Доверяемые порты.

Пробуем получить ip адрес (Рис.25).

```
VPCS> ip dhcp
DDD
Can't find dhcp server

VPCS> ip dhcp
DORA IP 192.168.20.3/24 GW 192.168.20.254
```

Рис.25 – Получение ip адреса.

Сохраняем конфигурацию и переходим к настройке серверов.

## 2.3 Настройка серверов: Windows server 2019, zabbix сервер.

### 2.3.1 Базовая настройка серверов Windows 2019.

Произведем базовую настройку. Для начала у обоих, виртуальных машин выбираем в сетевом адаптере сетевой мост (Рис.26).

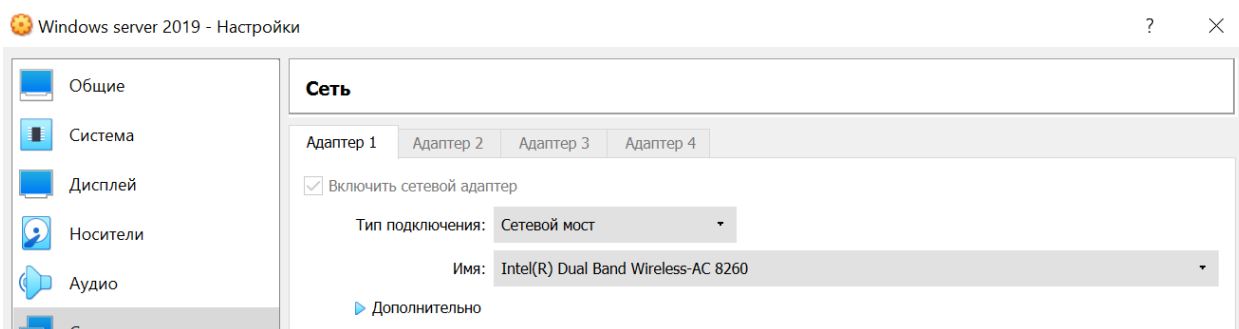


Рис.26 – Настройка типа подключения.

Дальше настраиваем сетевой адаптер. Задаем IP адрес и шлюзом указываем адрес виртуальной машины EvE-ng (Рис.27).

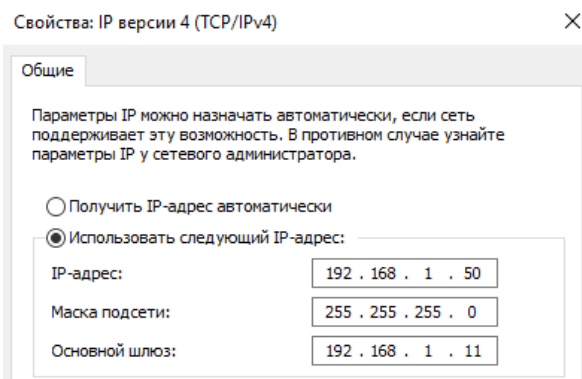


Рис.27 – Настройка интерфейса DC1.

Задаем имя серверу (Рис.28).

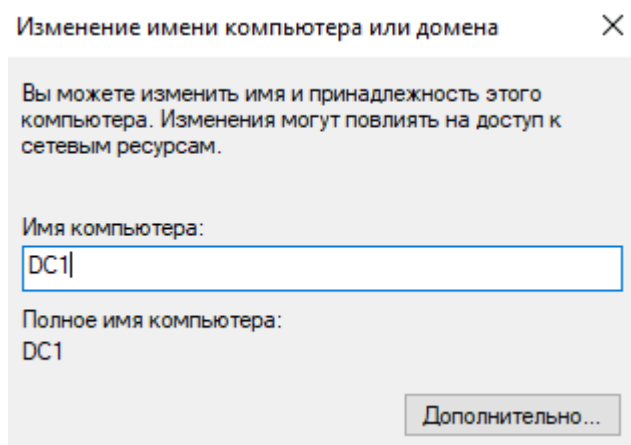


Рис.28 – Задаем имя сервера.

Также зададим имя второму серверу DC2 и настроим интерфейс (Рис.29).

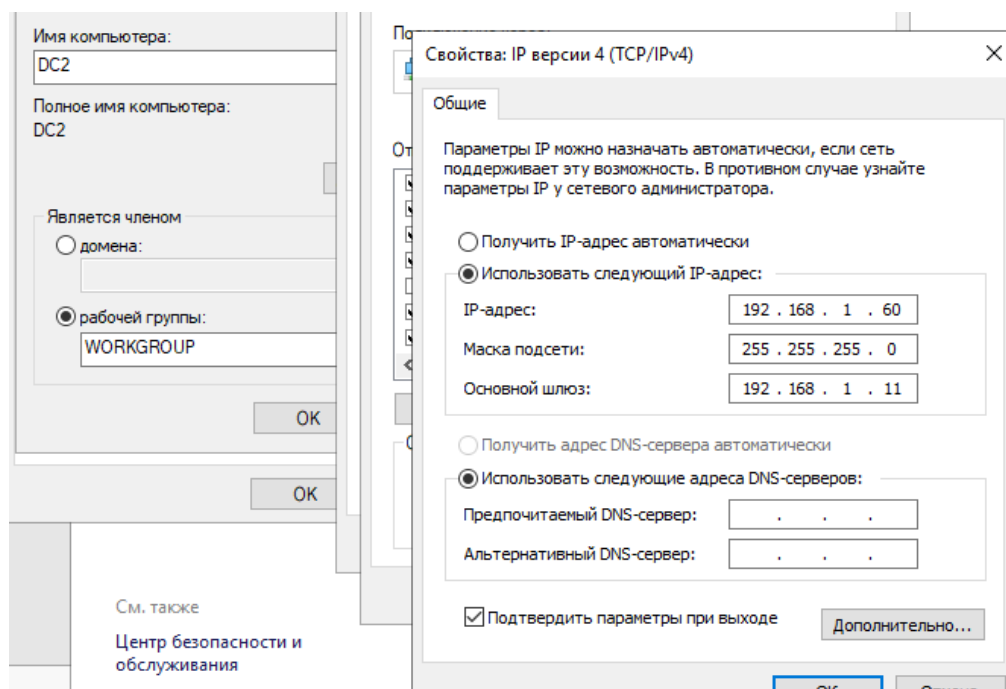


Рис.29 – Базовая настройка DC2.

### 2.3.2 Настройка tftp64.

Установим программу tftp64 на DC1.

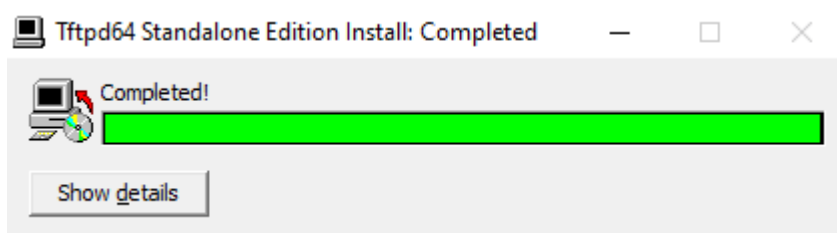


Рис.30 – Установка.

Производим настройку указываем адрес сервера и папку в которой будут храниться полученные данные (Рис.31).

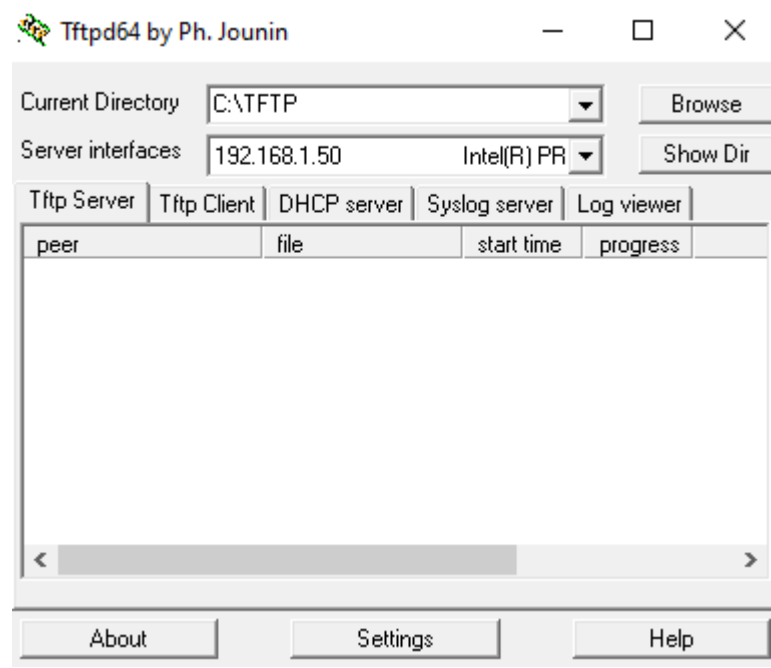


Рис.32 – Настройка TFTP.

После необходимо открыть 69 порт UDP, так как на нем работает протокол TFTP (Рис.33). Для этого нужно создать разрешающее правило для входящего трафика.

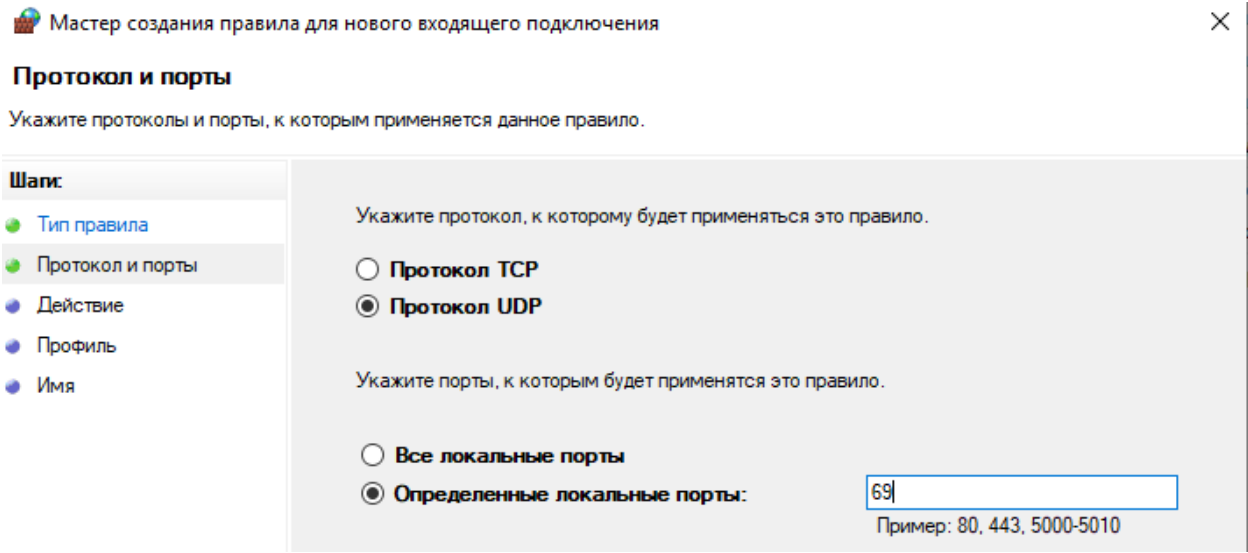


Рис.33 – Создание правила для протокола tftp.

Попробуем отправить работающие конфигурации L3 коммутаторов. Для этого воспользуемся командой сохранения рабочей конфигурации с добавлением протокола передачи данных tftp для отправки конфигурации на сервер (Рис.34).

```
S1-L3#copy running-config tftp:
Address or name of remote host []? 192.168.1.50
Destination filename [s1-l3-config]?
█
```

Рис.34 – Команда.

Полученные конфигурации (Рис.35).

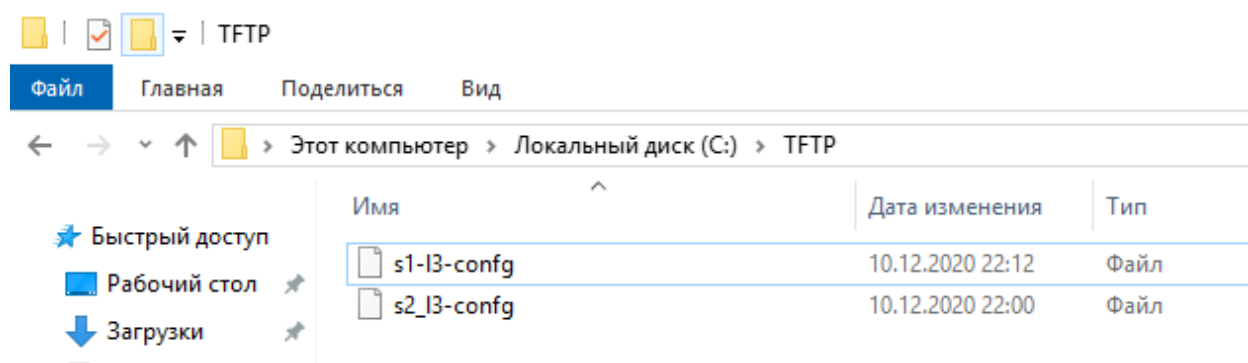


Рис.35 – Полученные файлы.

### 2.3.3 Active Directory дополнительный контроллер домена (репликация).

Сделаем сервер DC1 контролером домена нового леса ad.kocharuan.er.

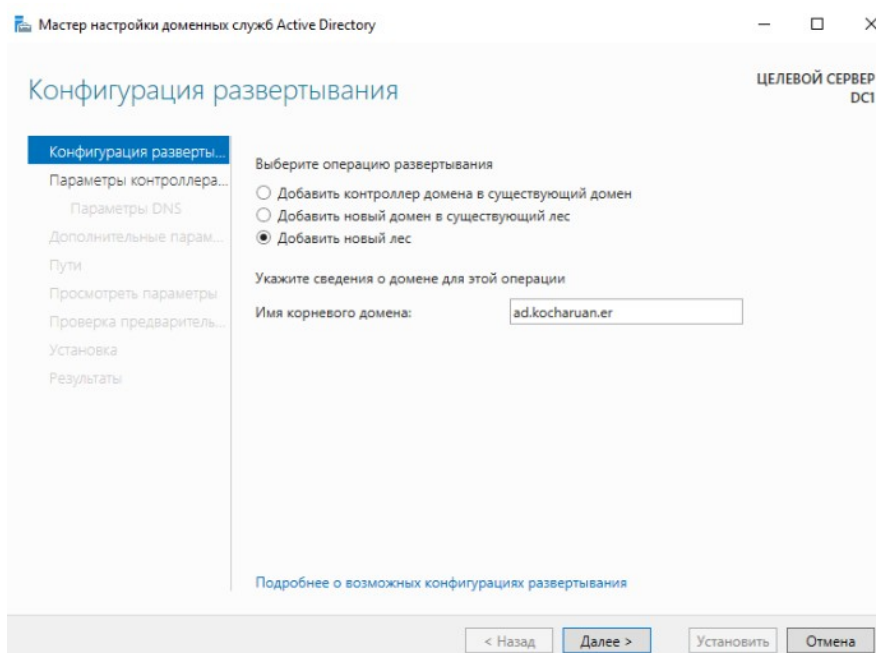


Рис.36 – Создание контроллера домена.

Добавим дополнительный контроллер домена DC2 в ранее созданный лес для этого в начале введем DC2 в домен(Рис.37).

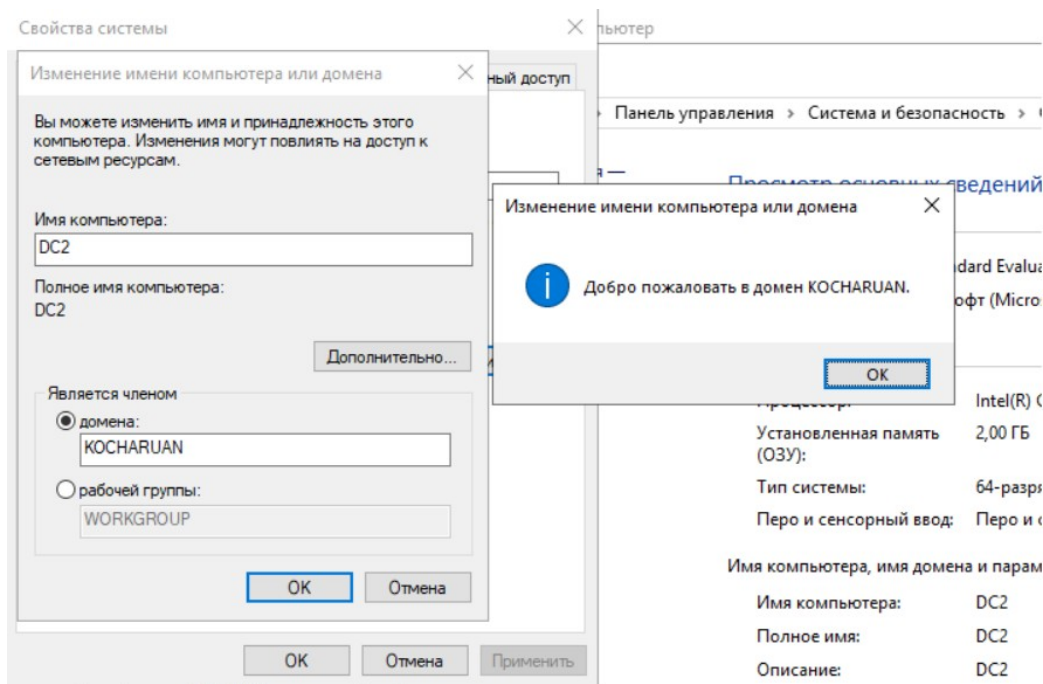


Рис.37 – Добавление сервера в домен.

После повышаем сервер DC2 до контроллера домена и добавляем его к существующему домену.

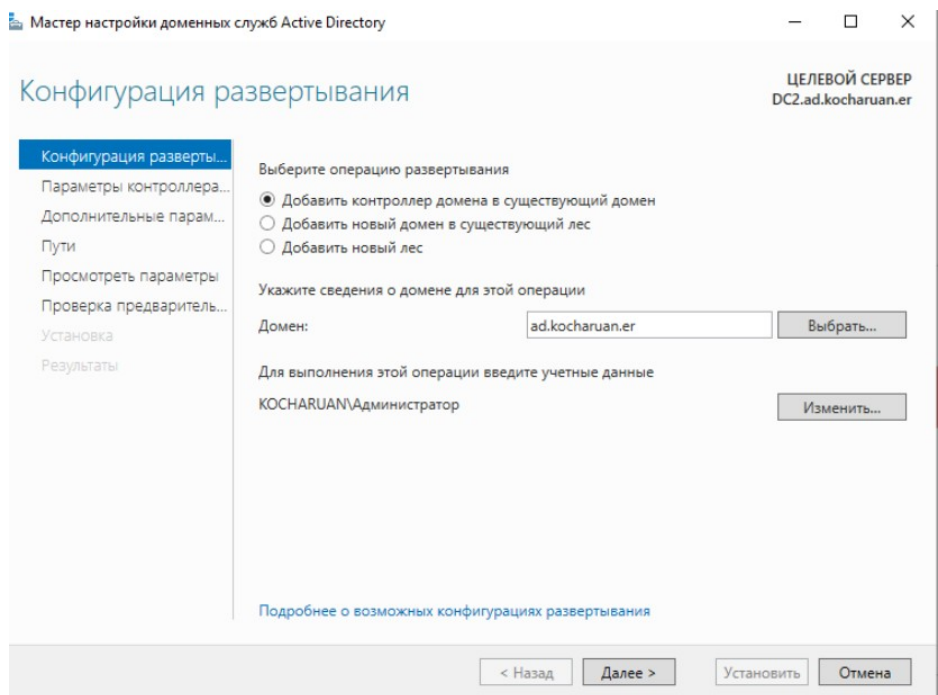


Рис.38 – Добавление второго контроллера домена.

Выбираем сервер DC1 который будет источником репликации (Рис.39).

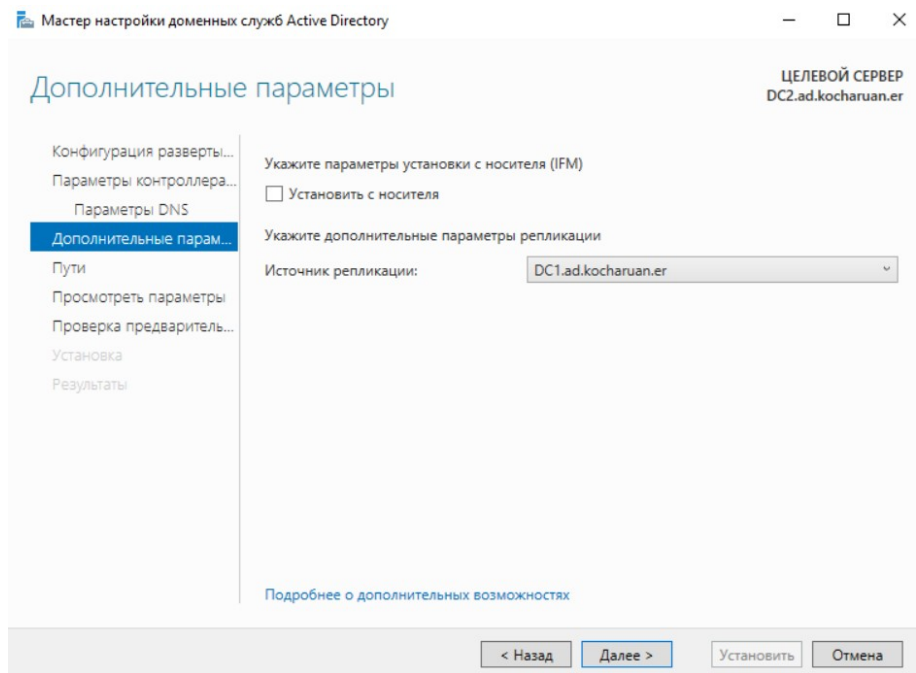


Рис.39 – Выбор источника репликации.

Для проверки репликации создаем пользователя ПРОВЕРКА на DC1 (Рис.40).

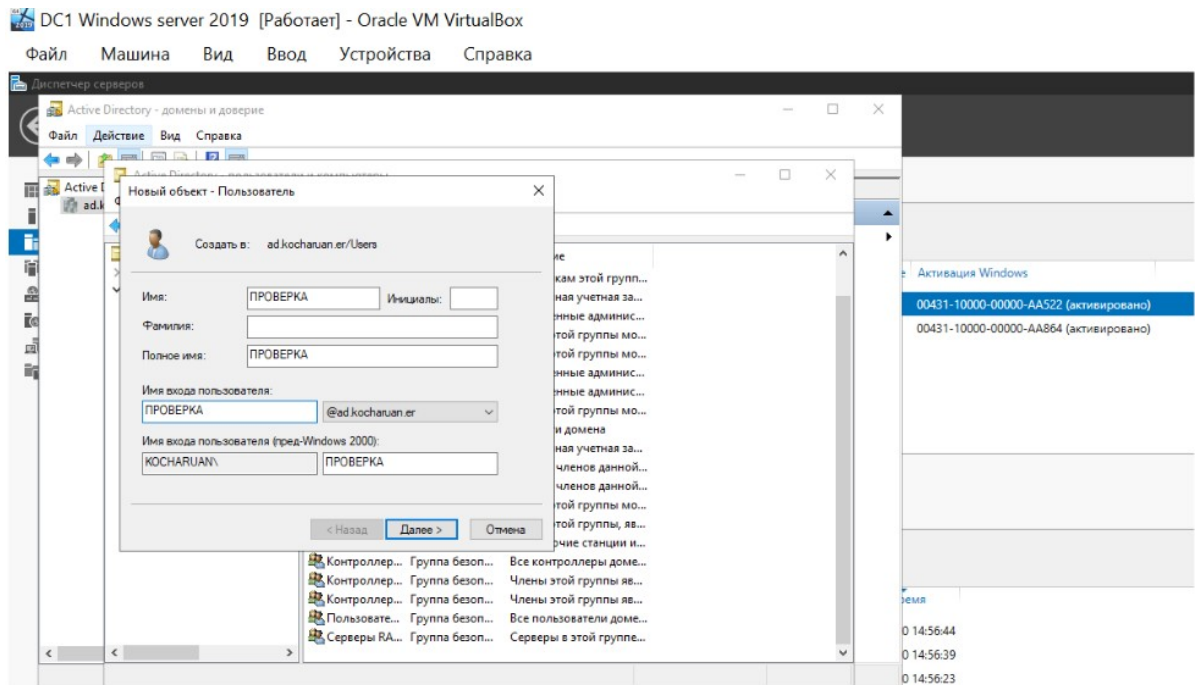


Рис.40 – Создание пользователя.



Проверяем репликацию данного пользователя на DC2 (Рис.41).

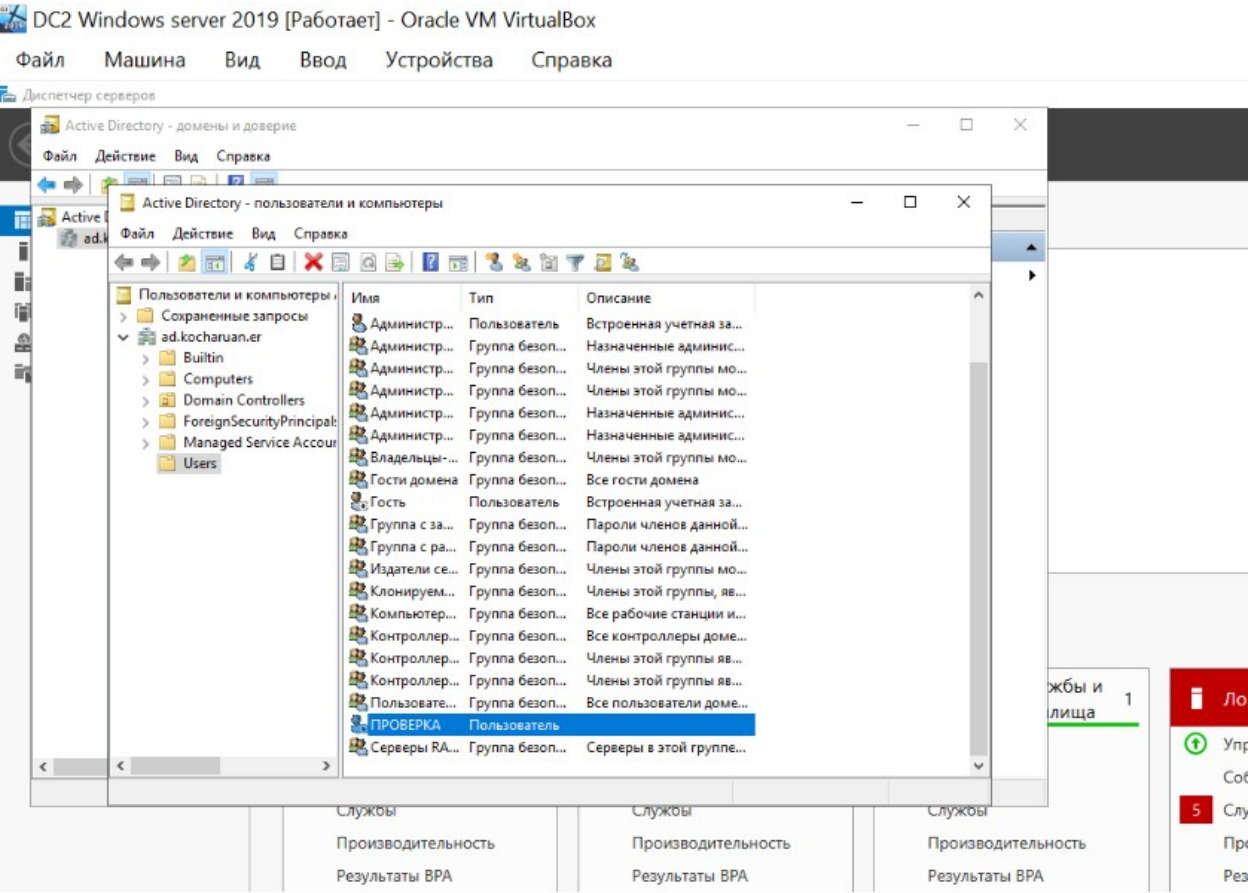


Рис.41 – Репликация.

2.3.4 Настройка автоматического резервирования на RAID.

В начале, стоит установить систему архивации данных Windows server DC1 (Рис.42).

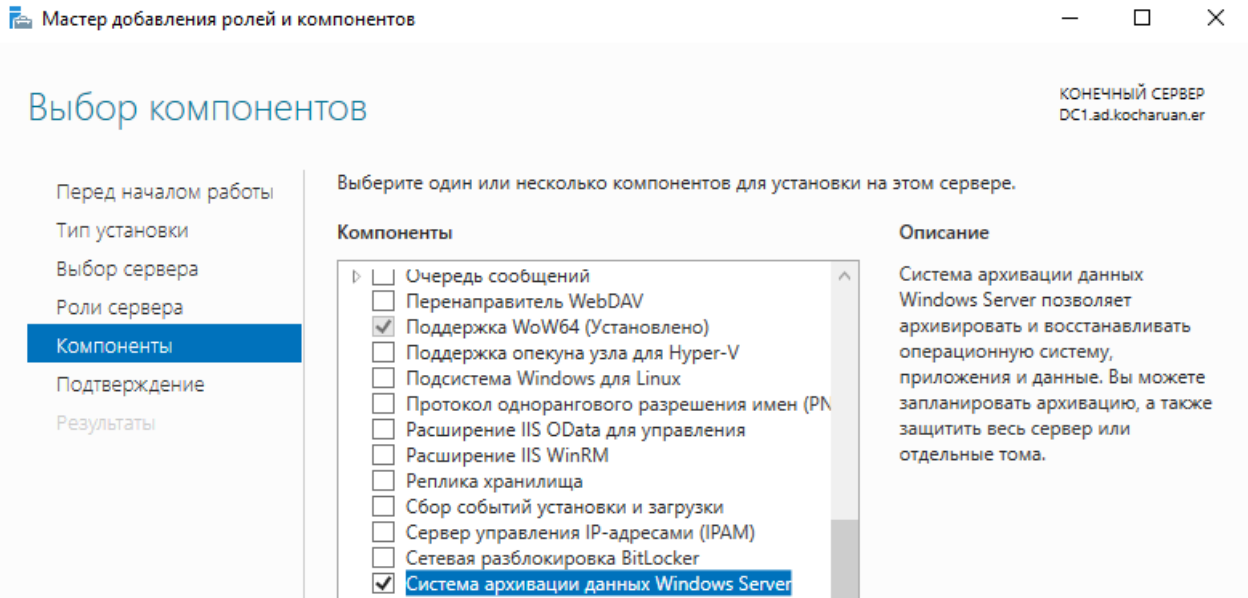


Рис.42 – Установка системы архивации.



После необходимо инициализировать два новых диска и сделать из них зеркальный том. Инициализация (Рис.43).

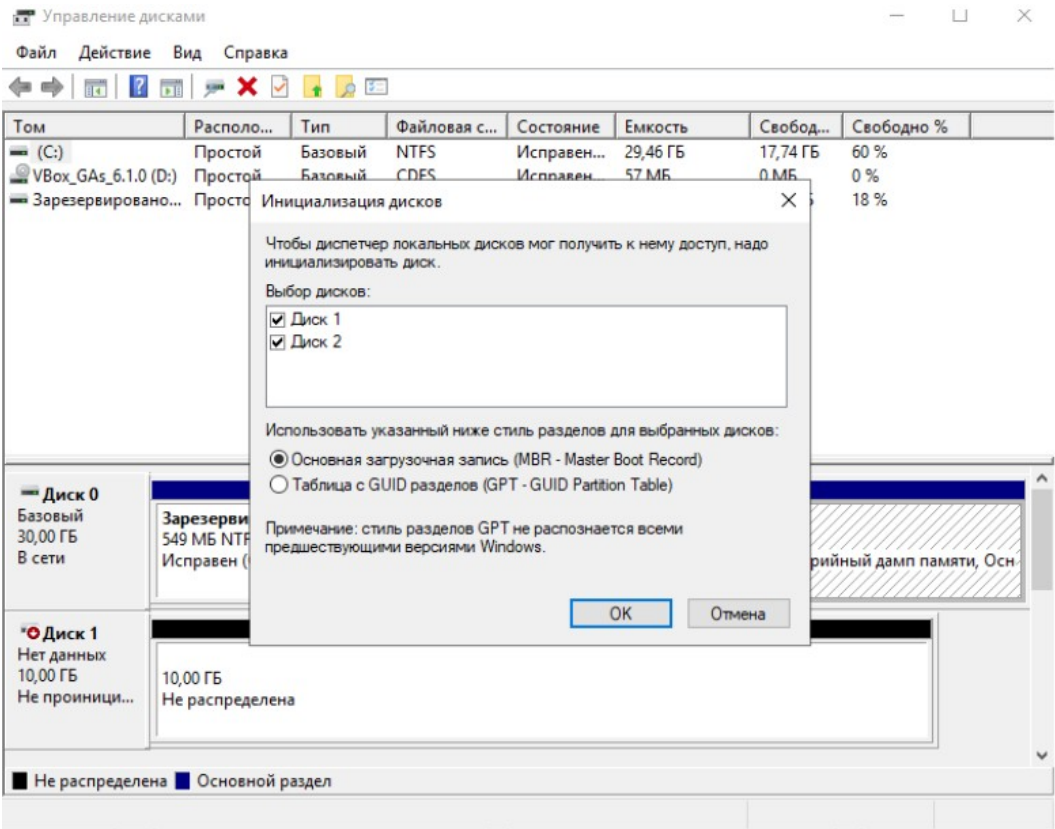


Рис.43 – Инициализация.

Создаем RAID 1 или зеркальный том (Рис.44).

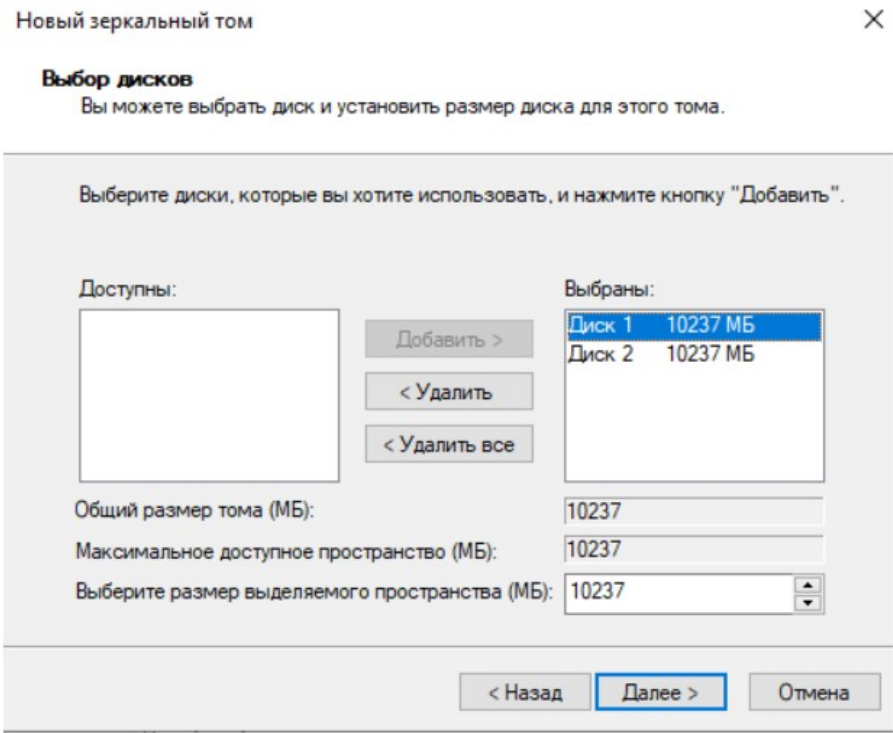


Рис.43 – Создание зеркального тома.

Выбираем файловую систему NTFS, размер кластера по умолчанию, меткой тома выбираем E: (Рис.44).

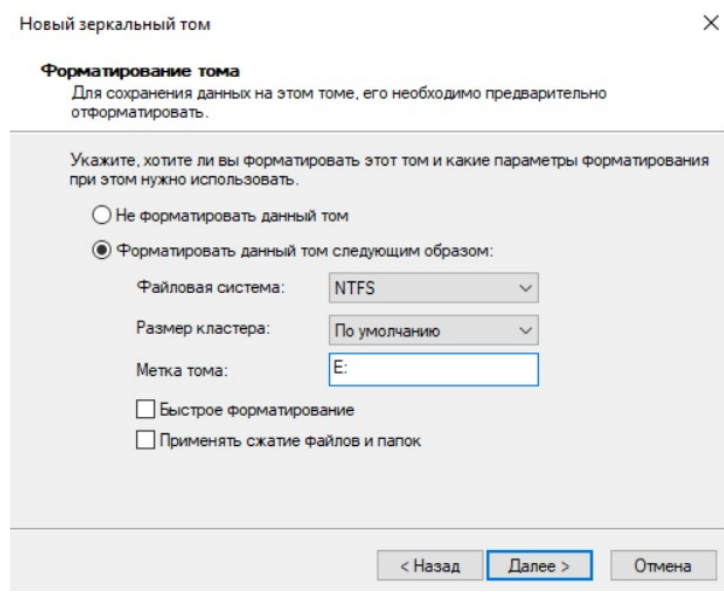


Рис.44 – Форматирование.

Процесс синхронизации и форматирования (Рис.45).

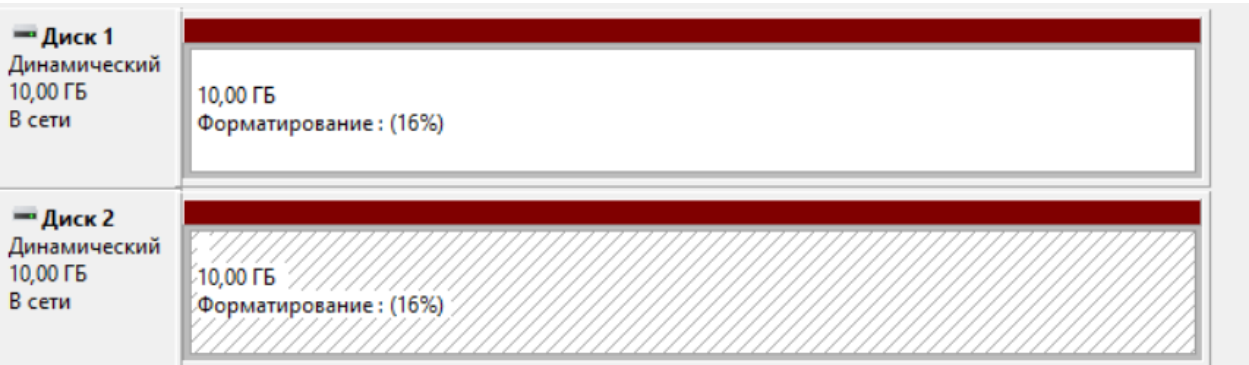
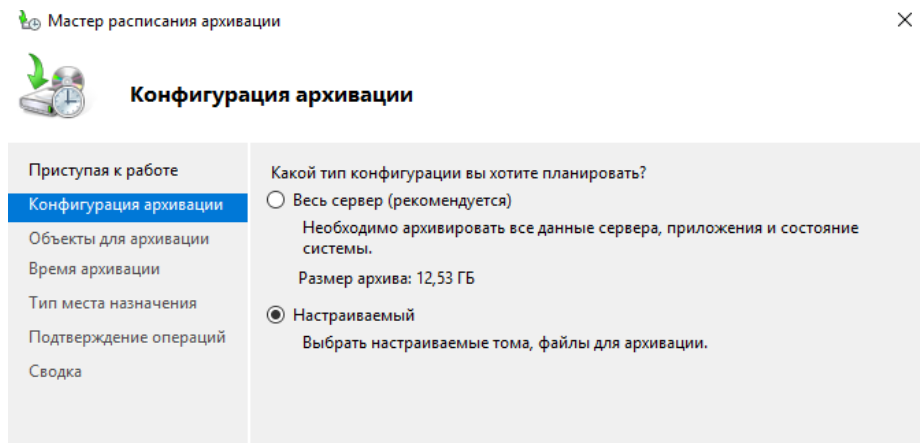


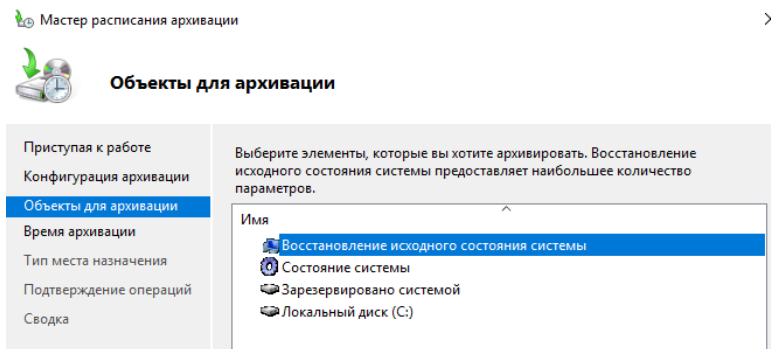
Рис.45 – Форматирование.

Теперь перейдем к настройке системы архивации Windows. В данном окне выбираем тип конфигурации настраиваемый (Рис.46).



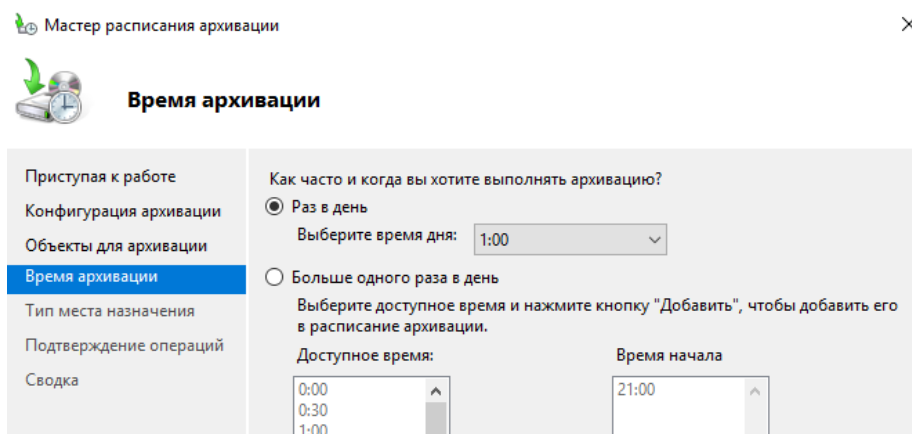
*Рис.46 – Конфигурация архивации.*

Выбираем объекты архивации (Рис.47). В данном случае выбираем Восстановление исходного состояния системы.



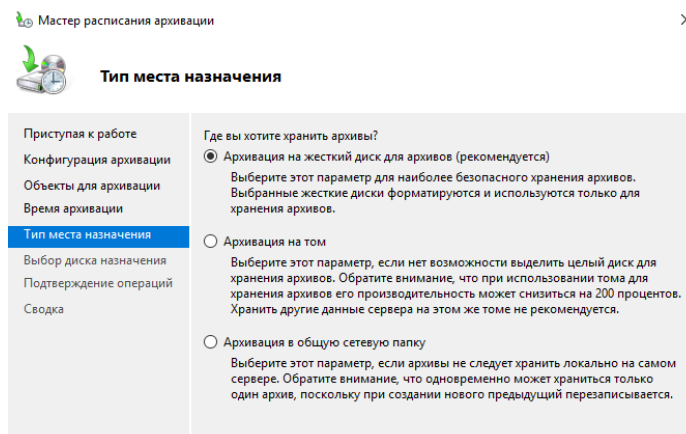
*Рис.47 – Объекты архивации.*

Выбираем время архивации. Лучше всего выбирать позднее время суток, когда возможная ошибка будет, не столь критична... (Рис.48).



*Рис.48 – Выбор времени архивации.*

Выбираем тип носителя, для хранения архивов для DC 2 выбираем Архивация на том. Для DC1 выбираем архивацию в общую сетевую папку (Рис.49).



*Рис.49 – Тип места назначения.*

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						44

Выбираем том для DC2 и выбираем сетевую папку для DC1 (Рис.50 – Рис.51).

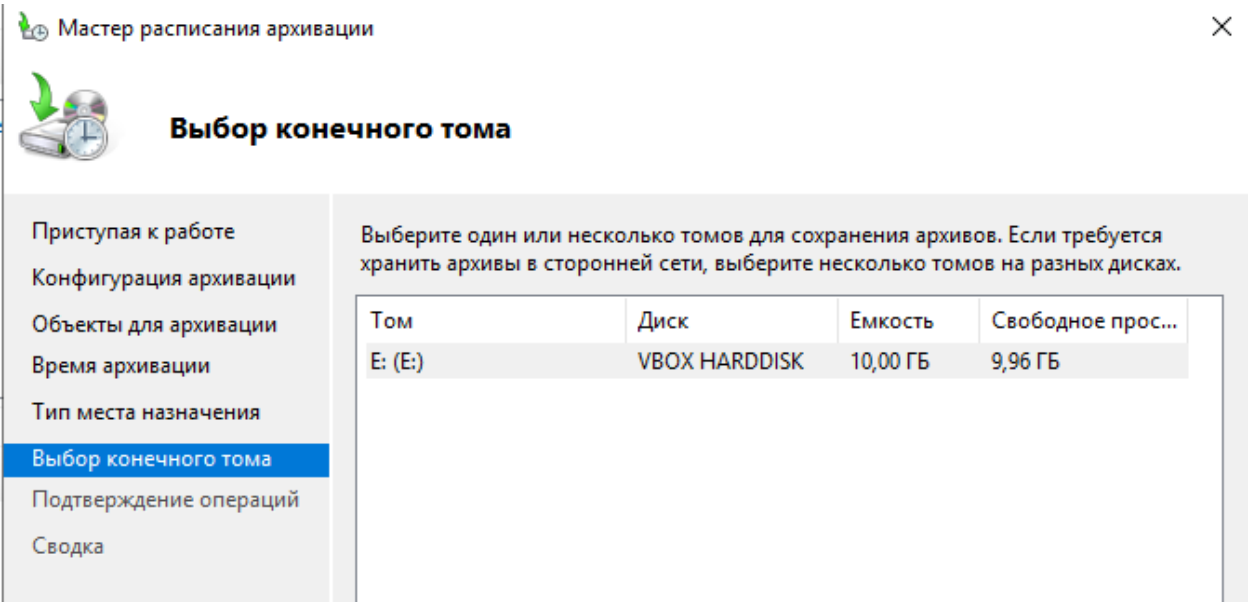


Рис.50 – Выбор тома.

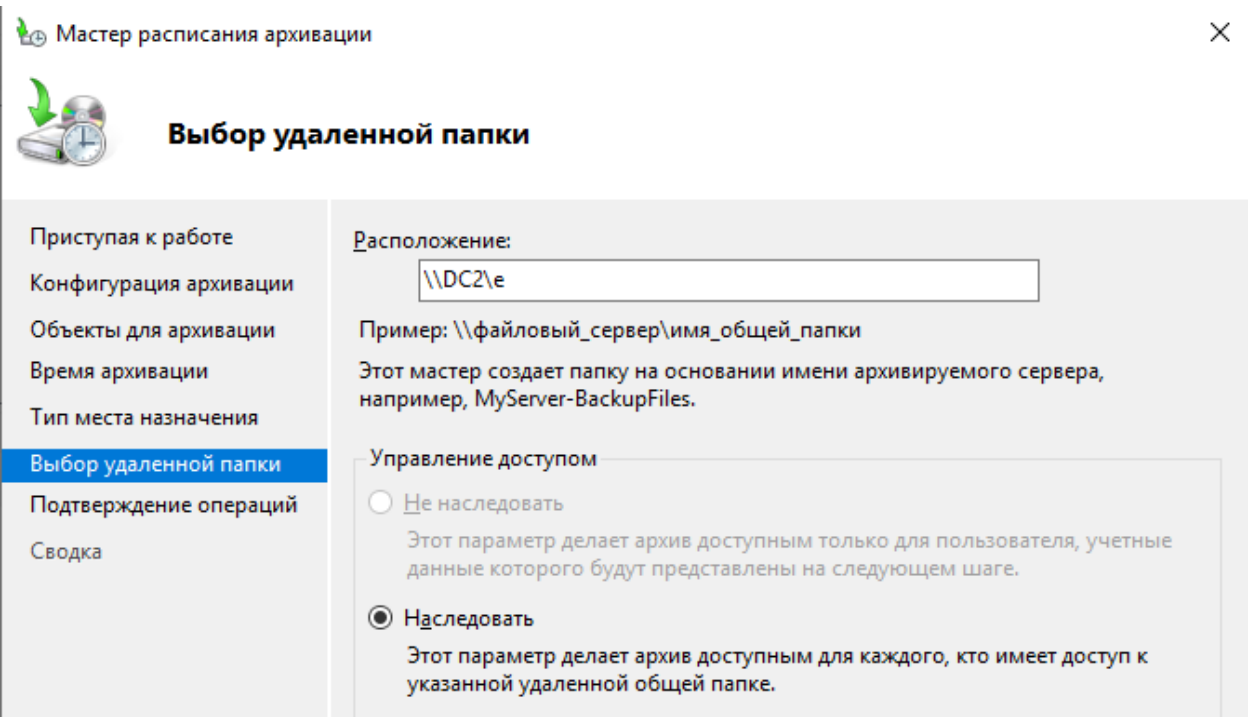


Рис.51 – Выбор сетевой папки.

После нажимаем готово. Теперь в случае необходимости всегда можно будет восстановить сервера.

### 2.3.5 Настройка мониторинга серверов с использованием Zabbix.

Развертывание системы мониторинга Zabbix в данной курсовой работе рассмотрено не будет, так как эта тема не является темой данной курсовой работы.

Для начала необходимо установить Zabbix агент на DC1 и DC2. Для этого перейдем на официальный сайт Zabbix в «шапке» нажимаем на пункт продукт, после ниже выбираем Zabbix агенты, далее выбирается дистрибутив ОС и версию ОС, платформу, версию Zabbix и формат пакета с выбором шифрования (Рис.52).

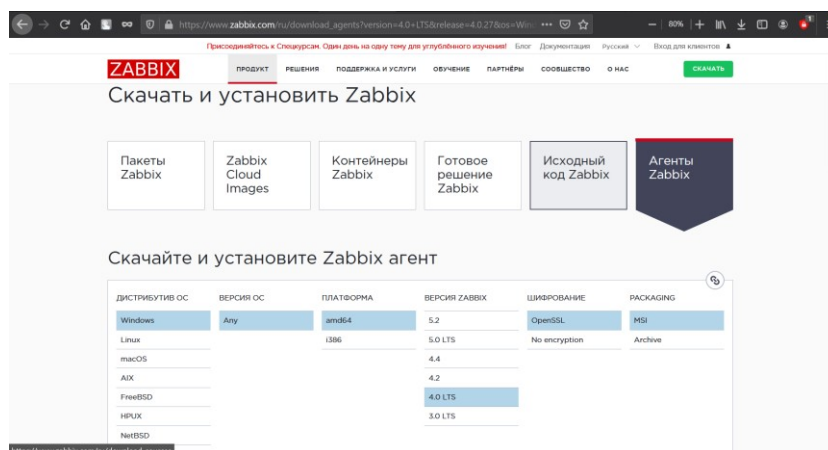


Рис.52 – Выбор агента zabbix.

Спускаемся ниже и нажимаем кнопку скачать. Далее необходимо перенести данный пакет на сервера DC1 и DC2, для этого можно воспользоваться функцией «drag on drop» в Virtual Box. После устанавливаем агенты, при установке указываем адрес Zabbix сервера (Рис.53). Адрес сервера можно узнать используя команду «ip -a» на нем, так как это Linux.

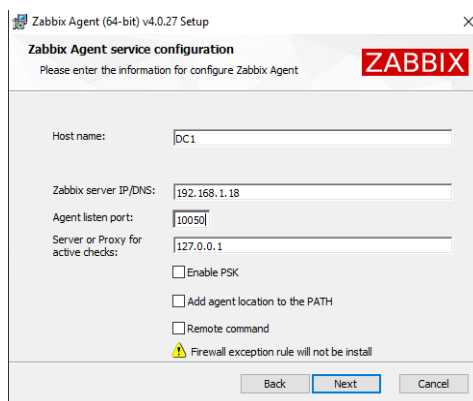


Рис.53 – Установка агента zabbix.

Поскольку Zabbix агент по умолчанию использует протокол TCP и порт 10050 то необходимо создать разрешающее правило для входящего трафика в брандмауэре Windows (Рис.54).

Рис.54 – Создание правила.

После проделывания идентичных действий на DC2 перейдем к Zabbix агенту для добавления на мониторинг этих серверов.

Переходим в браузере к Zabbix агенту. Жмем на настройки после на узлы сети, и добавит новый узел. Указываем имя узла сети, группу поиска, адрес удаленного узла тип протокола IP и порт подключения (Рис.55).

Рис.55 – Настройка узла сети.

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						47

Как говорилось, в теоретической части сервера будут поставлены на мониторинг по шаблону. Переходим к шаблонам и добавляем шаблон Windows (Рис.56).

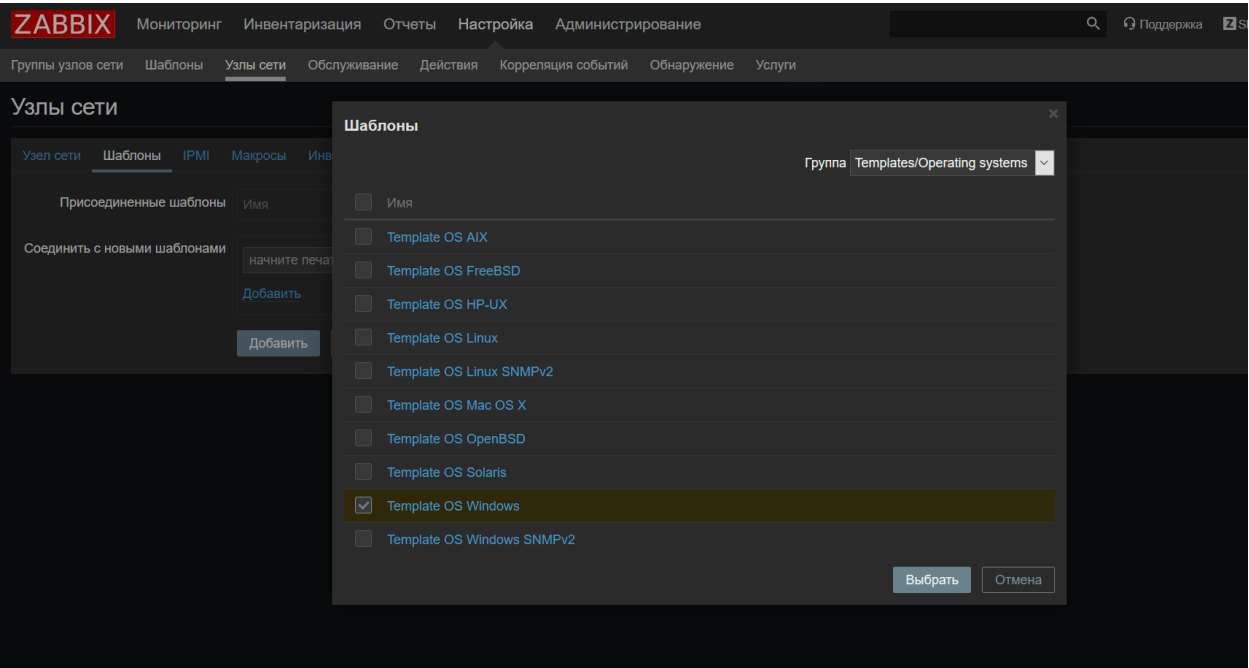


Рис.56 – Выбор шаблона.

После жмём кнопку добавить под шаблоном и потом кнопку добавить узел (Рис.57) как мы видим, индикатор доступности горит зеленым цветом, это значит, что узел доступен.

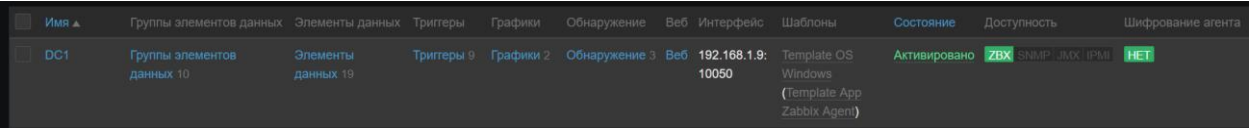


Рис.57 – Доступность узла.

Таким же образом добавляем DC2 (Рис.58).

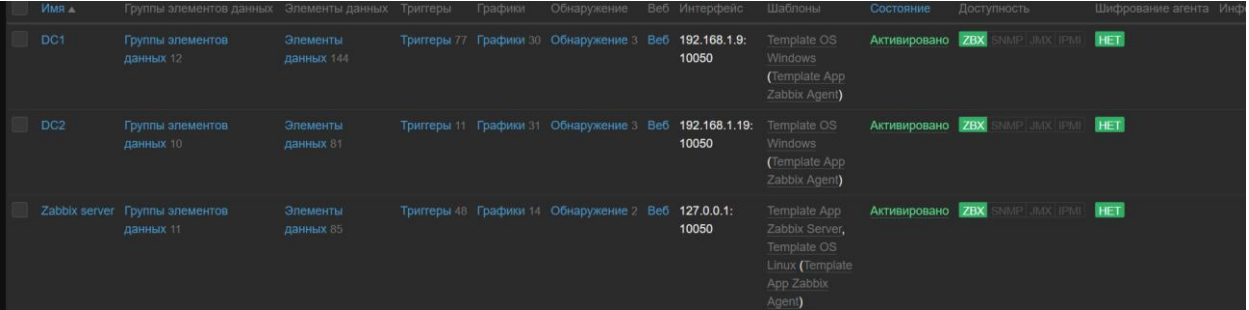


Рис.58 – Узлы сети.



На главной панели можно просматривать различные оповещения (Рис.59).

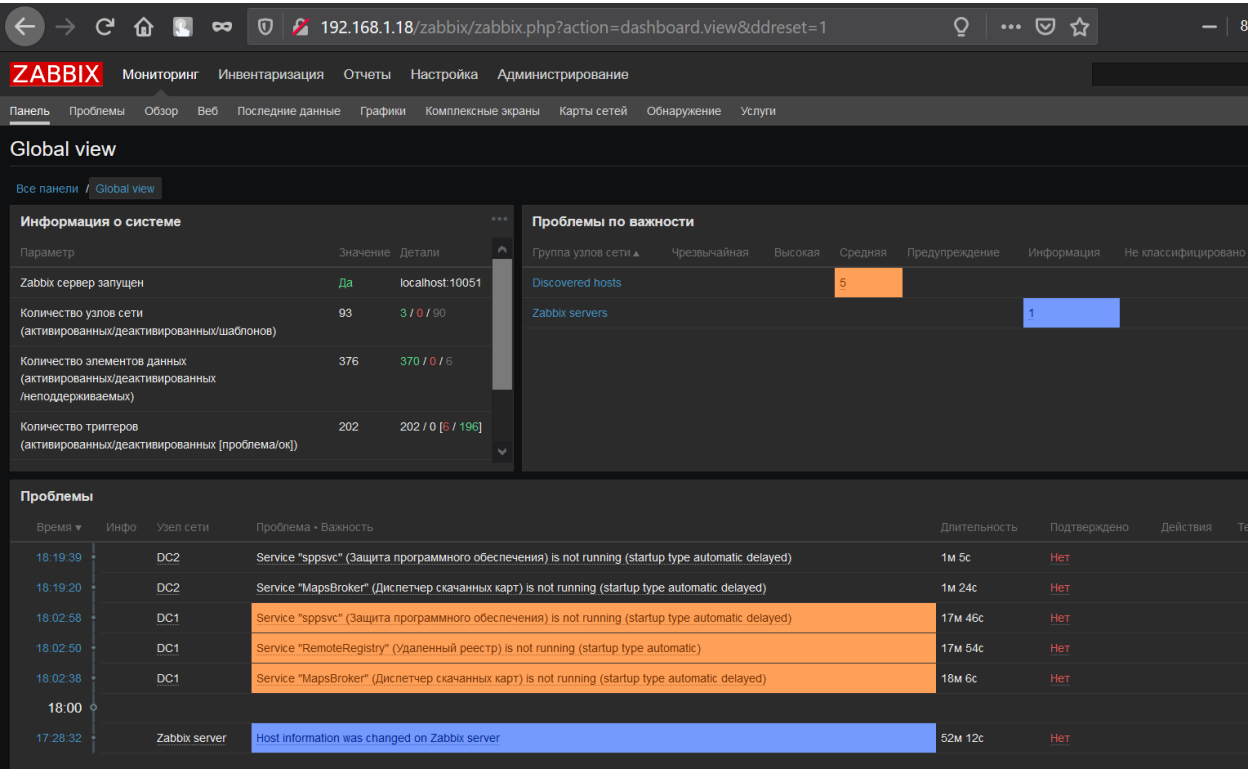


Рис.59 – Главная панель.

В разделе графики можно просматривать различную информацию о состоянии узла, к примеру, график загрузки процессора. Выбираем группу и имя узла в сети и интересующий нас график (Рис.60).

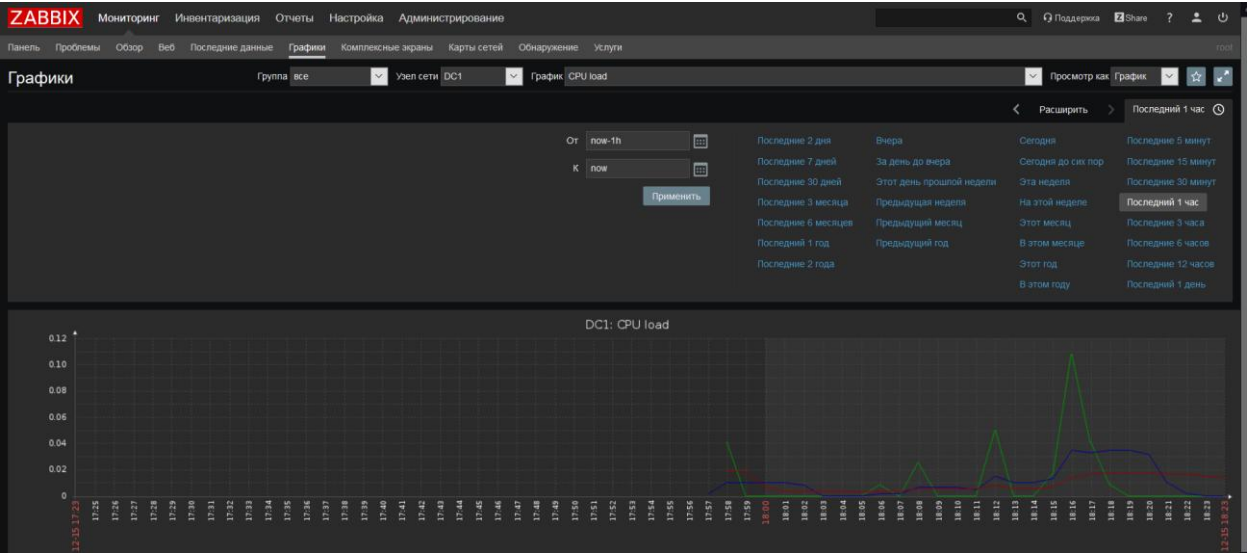


Рис.60 – Загруженность процессора DC1.



Для того чтобы всегда быть в курсе событий происходящих в сети необходимо настроить систему оповещений. Для этого необходимо перейти в способы оповещения и нажать добавить способ оповещения. В первом поле имя указываем имя способа оповещения Gmail, далее тип email, после указываем порт SMTP сервера. Дальше необходимо указать SMTP hello и адрес почты после выбираем протокол шифрования, дальше указываем данные аутентификации.

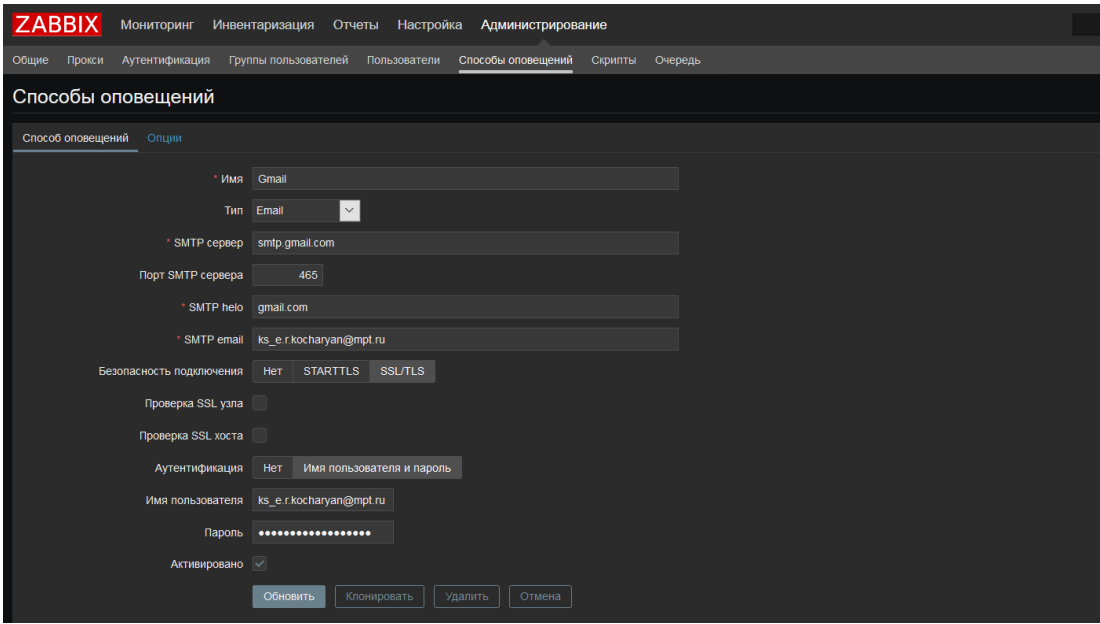


Рис.61 – Настройка способа оповещения.

После того как был настроен способ оповещения необходимо в настройках профиля добавить оповещения (Рис.62). Выбираем ранее созданный тип Gmail и указываем адрес, на который будем отправлять сообщения. Также указываем тип отправляемых сообщений.

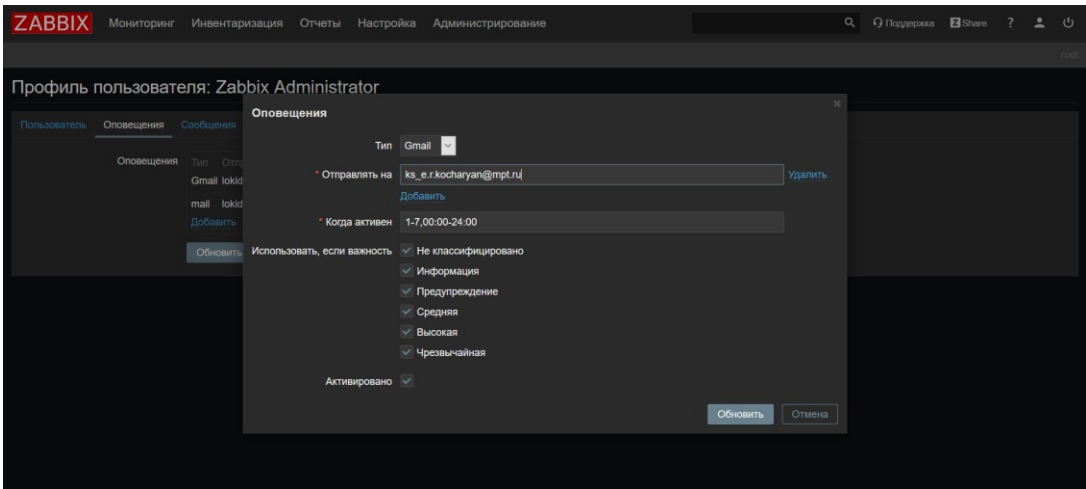


Рис.62 – Настройка оповещений.

Для проверки произведем перезагрузку сервера и проверим полученное уведомление. Поскольку Zabbix является сторонним приложение, Google заблокировал вход в данный акаунт (Рис.63).

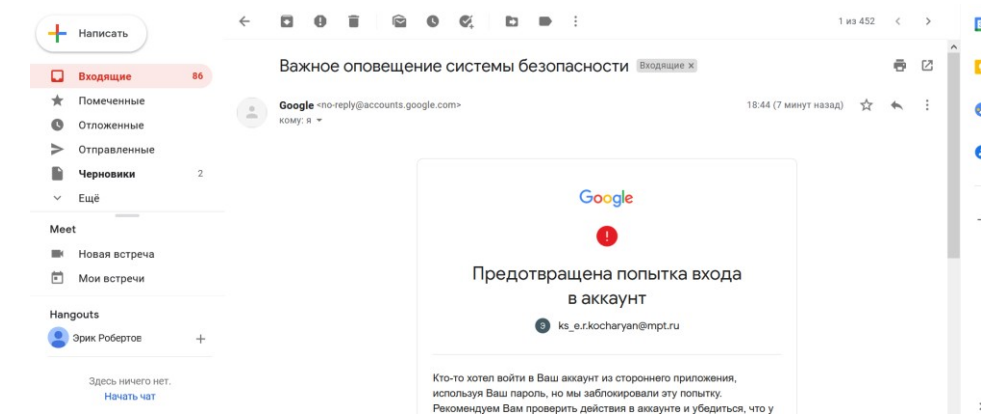


Рис.63 – Сообщение системы безопасности.

Для того чтобы все заработало, перейдем в настройки безопасности акаунта Google и разрешим доступ к неизвестным приложениям (Рис.64).



Рис.64 – Настройка доступа.

Выполним перезагрузку сервера DC1 и получим сообщение в Zabbix агенте (Рис.65).

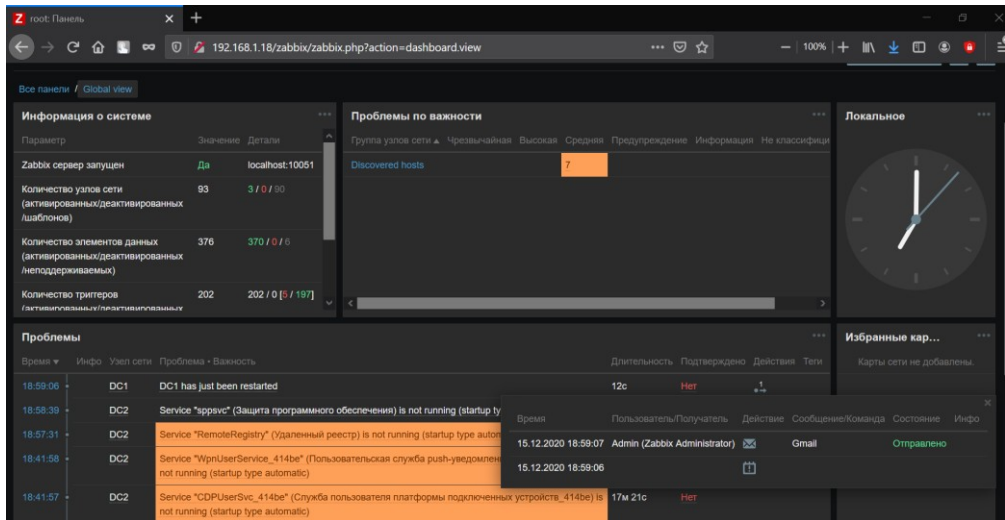


Рис.66 – Оповещения.

Проверим почту. Как видно из (Рис.67) сообщения пришли.

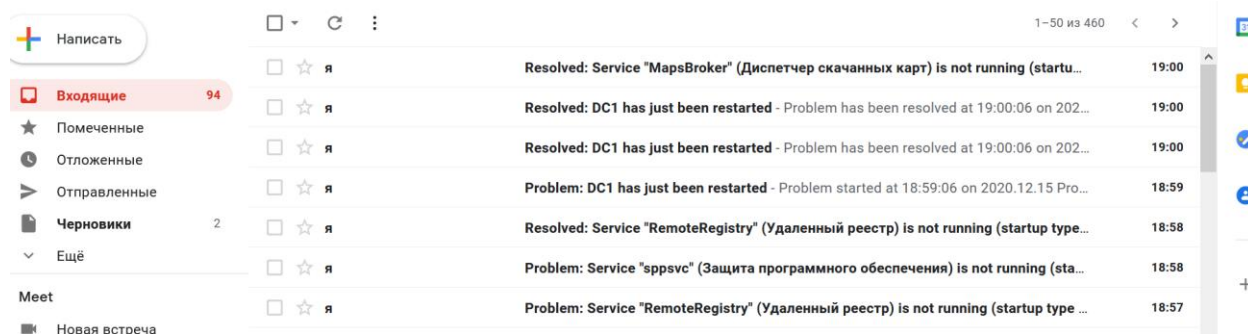


Рис.67 – Пришедшие сообщения.

Для того чтобы получать действительно важную информацию и не захламлять почту стоит изменить тип отправляемых оповещений (Рис.68). Оставляем только высокую и чрезвычайную информацию.

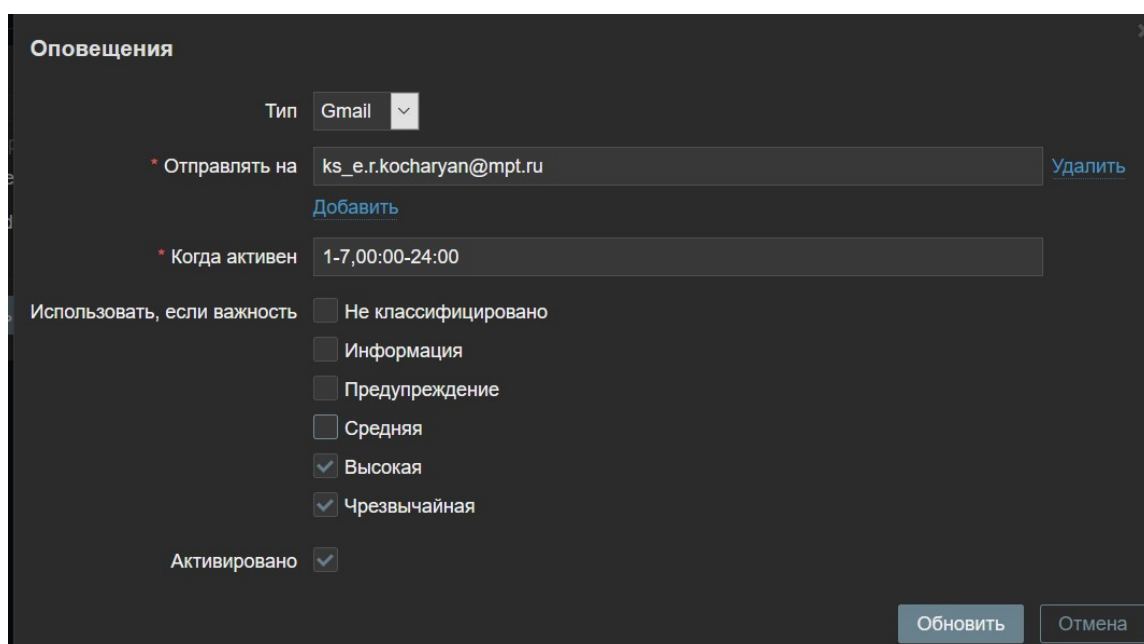


Рис.68 – Важность оповещений.

Теперь настроим карту сети в Zabbix (Рис.69). Переходим в Мониторинг, карты сетей и жмем изменить карту сети. Далее нажимаем добавить элемент карты сети. В открывшемся окне выбираем тип узел сети, далее подписываем элемент и выбираем конкретный узел в сети.

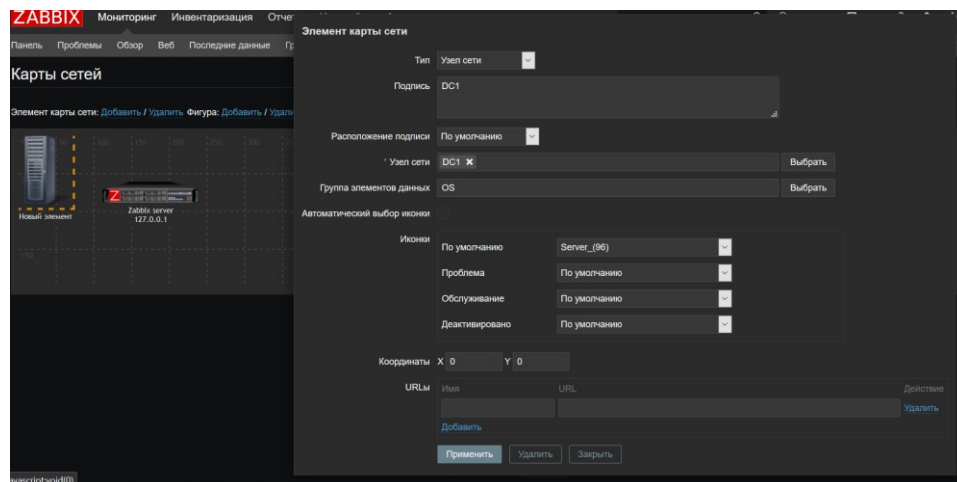


Рис.69 – Добавление DC1 в карту сети.

Таким же образом добавляем DC2. После настраиваем соединения между устройствами (Рис.70).

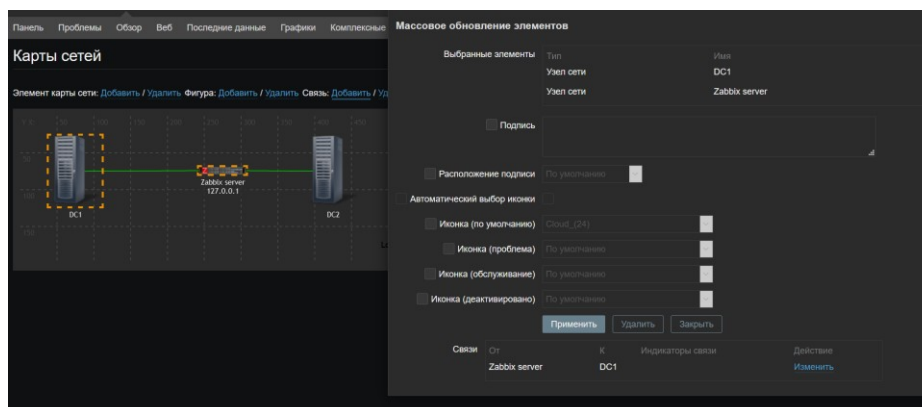


Рис.70 – Добавление связи.

Имеем следующую карту сети (Рис.71).

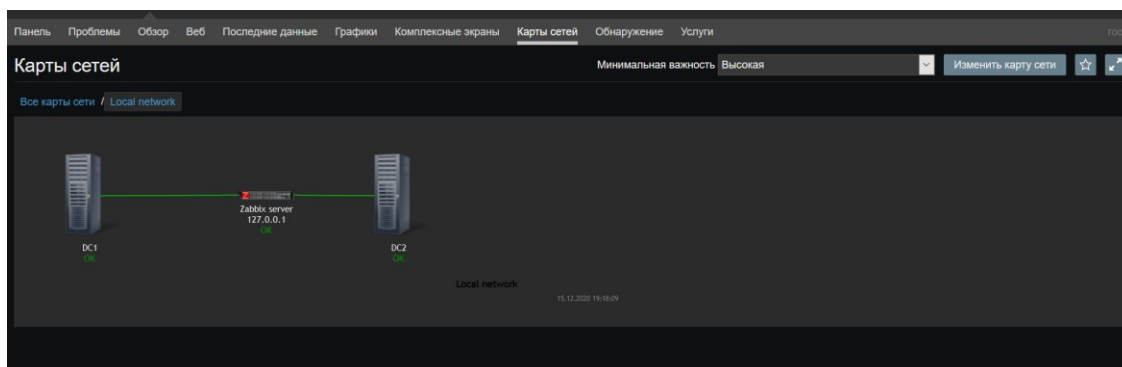


Рис.71 – Карта сети.

## Заключение.

В ходе данной курсовой работы была рассмотрена тема бесперебойной и отказоустойчивой работы сети предприятия. В вовремя изучения данной темы было выделено два крупных отличающихся направления это технические решения для обеспечения отказоустойчивой и бесперебойной работы сети, а также программные решения.

В направление технических решений были рассмотрены следующие темы: бесперебойные блоки питания, серверная комната температурные нормы, кабель менеджмент, а также была рассмотрена тема проектирования топологии с точки зрения трехуровневой модели сети и принципы проектирования сети.

В направление программных решений были рассмотрены следующие темы: Настройка сетевого оборудования (Протоколы: EIGRP, OSPF, LACP, TFTP, HSRP, VLAN, DHCP snooping.). Настройка серверов Windows 2019 (Службы: Active Directory 2 контроллера домена, архивирования данных Windows server на RAID, TFTP сервер.).

Также была затронута тема мониторинга компьютерных сетей с помощью сервера Zabbix. В процессе были поставлены два сервера на базе Windows 2019 на мониторинг. Также была произведена настройка Email оповещений на Gmail почту. И в заключение была произведена настройка карты сети в Zabbix.

Можно с уверенностью сказать, что поставленная задача данной курсовой работы была выполнена.

К сожалению, ограничение по размеру курсовой работы не позволяли рассмотреть и изучить тему курсовой работы глубже. Поэтому в будущем обязательно изучу эту тему еще лучше.

Подводя итог, хочется сказать что в современном мире с активно развивающимися сетевыми технологиями специалисты, разбирающиеся области компьютерных сетей всегда будут актуальны.

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						54

## Список используемых источников и литературы.

1. Авторы: Максимов Николай Вениаминович Попов Игорь Иванович  
Компьютерные сети (2017) — Текст : электронный — URL:  
<https://znanium.com/catalog/document?pid=792685>
2. Авторы: Кузин Александр Владимирович Кузин Дмитрий Александрович  
Компьютерные сети (2017) — Текст : электронный — URL:  
<https://znanium.com/catalog/document?pid=938938>
3. Компьютерные сети: расширенный начальный курс Авторы: А. А. Букатов, С. А. Гуда (2019) — Текст : электронный — URL:  
<https://www.litres.ru/aleksandr-pyhalov-un/komputernye-seti-rasshirennyu-nachalnyy-kurs-48613245/>
4. Олифер, Олифер: Компьютерные сети. Принципы, технологии, протоколы. Юбилейное издание (2020) — Текст : электронный — URL:  
<https://www.labirint.ru/books/737421/>
5. Олифер, Олифер: Компьютерные сети. Принципы, технологии, протоколы. (2019) — Текст : электронный — URL: <https://www.labirint.ru/books/511422/>
6. С. Грингард «Интернет вещей. «Будущее уже здесь» (2017) ) — Текст : электронный — URL: <https://www.alpinabook.ru/catalog/book-75330/>
7. Компьютерные сети: Принципы, технологии, протоколы (2018) ) — Текст : электронный — URL: [https://www.bsuir.by/m/12\\_100229\\_1\\_85460.pdf](https://www.bsuir.by/m/12_100229_1_85460.pdf)
8. Интернет изнутри. Экосистема глобальной сети. (2017) ) — Текст : электронный — URL: <https://www.ozon.ru/context/detail/id/33354294/>
9. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-105: маршрутизации коммутация ) — Текст : электронный — URL: <https://www.ozon.ru/context/detail/id/147417590/>
10. Компьютерные сети. Учебник (2018) ) — Текст : электронный — URL: <https://www.chitai-gorod.ru/catalog/book/1168613/>

Изм.	Лист	№ докум.	Подпись	Дата	МПТ 09.02.02 ПЗ 04 КР	Лист
						55