СОДЕРЖАНИЕ

[Введение 4](#_Toc152244777)

[1 Аналитическая часть 6](#_Toc152244778)

[1.1 Анализ предметной области 6](#_Toc152244779)

[1.2 Описание исходных данных для анализа IT-инфраструктуры 12](#_Toc152244780)

[1.3 Описание логической топологии сети 13](#_Toc152244781)

[1.4 Описание взаимодействия серверов компьютерной сети 15](#_Toc152244782)

[1.5 Анализ и обоснование выбора программного обеспечения серверов и хостов сети 21](#_Toc152244783)

[1.6 Описание удаленного администрирования 25](#_Toc152244784)

[2 Проектная часть 28](#_Toc152244785)

[2.1 Установка операционной системы и дистрибутивов 28](#_Toc152244786)

[2.2 Установка сетевых протоколов и служб серверов 32](#_Toc152244787)

[2.3 Настройка сетевых служб хостов 34](#_Toc152244788)

[2.4 Организация администрирования компьютерной сети 38](#_Toc152244789)

[2.5 Организация взаимодействия между головным офисом и филиалами 41](#_Toc152244790)

[2.6 Настройка удаленного администрирования 45](#_Toc152244791)

[Заключение 47](#_Toc152244792)

[Список используемых источников 48](#_Toc152244793)

[Приложение А 51](#_Toc152244794)

[Приложение Б 52](#_Toc152244795)

Введение

Веб-студии расширяются для увеличения прибыли, расширения услуг, укрепления позиций на рынке, улучшения качества работы, завоевания новых рынков, развития и обучения сотрудников, а также снижения рисков.

Целью курсового проекта является администрирование компьютерной сети веб-студии. Для любой организации для ее успешного функционирования необходима локальная сеть, удовлетворяющая потребностям производства конкретных товаров и услуг. Поэтому при ее построении нужно учитывать множество факторов, начиная стоимостью создаваемой сети до ее размеров.

Объект исследования: работоспособная сегментированная компьютерная сеть с корректно настроенными групповыми политиками, с совместными программным и аппаратным обеспечением, с программами фильтрации трафика и методами защиты персональных данный пользователей.

Предмет исследования: организация администрирования и методы обеспечения безопасности компьютерной сети.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Выполнить анализ предметной области.
2. Описать исходные данные для анализа IT-инфраструктуры.
3. Описать логическую топологию сети.
4. Описать взаимодействие серверов компьютерной сети.
5. Проанализировать и обосновать выбор программного обеспечения для серверов и хостов сети.
6. Описать организацию удаленное администрирование.
7. Установить операционные системы и дистрибутивов.
8. Установить сетевые протоколы и службы.
9. Настроить сетевые службы.
10. Организовать администрирование компьютерной сети.
11. Организовать взаимодействие между головным офисом и филиалами.
12. Настроить удаленное администрирование.

В результате курсового проектирования должен быть создан прототип компьютерной сети, состоящей из трех локальных сетей (Веб-студия и филиалы).

1 Аналитическая часть

1.1 Анализ предметной области

Веб-студия – это специализированная компания, предоставляющая услуги по созданию и продвижению [сайтов](https://semantica.in/blog/chto-takoe-veb-sajt.html).

Головной офис занимается разработкой и продвижением сайтов, а также предоставляет услуги по созданию и поддержке интернет-проектов по всей России.

Для выполнения поставленной задачи необходимо объединить компьютерные сети веб-студии и филиалов.

Для объединения компьютерных сетей были выбраны два филиала:

1. Первый филиал располагается в Санкт-Петербурге, ориентирован на создание и продвижение сайтов с акцентом на предприятия из Северо-Западного федерального округа и стран Балтии.
2. Второй филиал располагается в городе Казань. Он специализируется на разработке и продвижении сайтов для компаний, работающих в Поволжье и на Урале.

Объединение компьютерных сетей происходит по нескольким причинам:

* Экономия на масштабе: Объединение нескольких студий может помочь сократить расходы на аренду офисов, оборудование, IT-инфраструктуру и другие общие затраты.
* Улучшение качества услуг: более крупная организация может предложить более качественные услуги благодаря большему опыту и знаниям в различных областях разработки веб-сайтов и приложений.
* Расширение клиентской базы: Большая организация может привлечь больше клиентов, так как она представляет большую надежность и стабильность.
* Снижение конкуренции.

На рисунке 1 показана логическая схема взаимодействия персонала веб-студии.



Рисунок 1 – Логическая схема взаимодействия персонала веб-студии

Системный администратор занимается администрированием для управления и контроля компьютерной сетью.

Администрирование ­­– это процесс управления и контроля за компьютерными системами, сетями и приложениями. Он включает в себя установку, настройку, обновление, мониторинг, обеспечение безопасности и резервное копирование данных.

Сетевое администрирование необходимо для обеспечения надежности и безопасности сети, эффективного использования сетевых ресурсов, обеспечения доступности и скорости работы сети, а также для решения проблем, возникающих в процессе работы сети.

Виды администрирования:

* Техническое администрирование сайтов (поддержка бесперебойной работы сайта, устранение и предотвращение возникновения пользовательских проблем, и актуальная отчетность о работе ресурса);
* Информационное администрирование сайтов (работа с наполнением сайта: он должен содержать самую актуальную информацию по теме, постоянное обновление новостей и карточек товаров, а также все возможные изменения в информации об организации).
* Администрирование сетей (процесс управления и контроля за работой компьютерных сетей, включающий в себя настройку и обслуживание сетевого оборудования, управление доступом к ресурсам, обеспечение безопасности данных и решение возникающих проблем).

Целью администрирования компьютерной сети является предоставление доступа к её ресурсам. В качестве ресурсов могут рассматриваться данные (файлы и папки), устройства (принтеры, сканеры, модемы) и вычислительные возможности, обеспечиваемые процессорами.

Для достижения этой цели администраторам сети приходится решать множество задач, которые могут быть разделены на следующие основные группы:

* задачи планирования;
* задачи установки и настройки программного и аппаратного обеспечения (при наличии большого числа компьютеров в сети требуется решать такие задачи централизованно и с максимальной степенью автоматизации);
* задачи управления безопасностью (в современных сетях, в большинстве своем подключенных к Интернету, проблема обеспечения безопасности является крайне острой и требует комплексного решения);
* задачи управления производительностью (решение этого типа задач следует осуществлять мониторинг процессов, происходящих в сети, и оперативно реагировать на выявившиеся проблемы с производительностью).

Рассмотрим основные функции администрирования сети:

* Установка и настройка серверов и сетевого оборудования.
* Мониторинг и управление сетевым трафиком, а также обеспечение безопасности сети.
* Управление пользователями, правами доступа и группами в сети.
* Резервное копирование данных и восстановление системы в случае сбоев.
* Обновление программного обеспечения и операционных систем.
* Устранение неполадок и поддержка пользователей.
* Организация и поддержка удаленного доступа к сети и приложениям.
* Планирование и управление емкостью сети, чтобы обеспечить ее эффективность и масштабируемость.
* Соблюдение законодательства и политик безопасности компании в отношении хранения и использования данных.
* Поддержка бесперебойной работы системы и предотвращение возможных проблем.

Сеть может подвергаться внешнем атакам с целью хищения важной информации, поэтому необходимо предпринимать меры по ее защите, проводить администрирование средств безопасности.

Администрирование средств безопасности – процесс управления и контроля за системами и инфраструктурой, которые обеспечивают безопасность информации и защиту от угроз и атак.

Администрирование средств безопасности включает в себя ряд задач, направленных на обеспечение безопасности информационных систем и данных. Перечислим основные задачи администрирования средств безопасности:

1. Идентификация и аутентификация пользователей.

Администраторы должны установить механизмы и процедуры для идентификации и аутентификации пользователей. Это включает в себя создание учетных записей пользователей, установку паролей, использование многофакторной аутентификации и других методов проверки личности пользователей.

1. Управление доступом.

Администраторы должны определить и управлять правами доступа пользователей к информационным ресурсам. Это включает в себя установку политик доступа, назначение ролей и привилегий, контроль доступа к файлам и папкам, а также мониторинг и аудит доступа.

1. Защита от внешних угроз.

Администраторы должны принимать меры для защиты информационных систем от внешних угроз, таких как вирусы, взломы, фишинг и другие виды кибератак. Это включает в себя установку и обновление антивирусного программного обеспечения, настройку брандмауэров и систем обнаружения вторжений, а также мониторинг сетевой активности.

1. Защита от внутренних угроз.

Администраторы должны также принимать меры для защиты информационных систем от внутренних угроз, таких как несанкционированный доступ со стороны сотрудников или утечка данных. Это включает в себя установку систем контроля доступа, мониторинг активности пользователей, шифрование данных и обучение сотрудников правилам безопасности.

1. Резервное копирование и восстановление данных.

Администраторы должны регулярно создавать резервные копии данных и разрабатывать планы восстановления в случае сбоя или потери данных. Это включает в себя выбор и настройку систем резервного копирования, тестирование процедур восстановления и обучение персонала по восстановлению данных.

1. Мониторинг и анализ безопасности.

Администраторы сети должны постоянно мониторить и анализировать безопасность информационных систем, чтобы обнаружить и предотвратить потенциальные угрозы. Это включает в себя использование систем мониторинга безопасности, анализ журналов событий, проведение аудитов безопасности и принятие мер по устранению обнаруженных уязвимостей.

Компьютерную сеть необходимо защищать от стороннего вредоносного Программного обеспечения (ПО).

Для безопасного и эффективного администрирования средств безопасности существует защита от вредоносного ПО.

Защита от вредоносного ПО – это важный аспект информационной безопасности, который направлен на защиту компьютерных систем от различных видов вирусов, троянов, червей и других вредоносных программ. Для обеспечения защиты от вредоносного ПО могут использоваться различные методы, например, антивирусные программы, брандмауэры, системы обнаружения вторжений и т.д.

Уменьшить вероятность заражения компьютерной системы можно, если использовать специальное антиспаммерское программное обеспечение, предназначенное для фильтрации спама, который очень часто используется для распространения вредоносных программ по каналам электронной почты.

Определенную защиту может дать использование операционных систем менее популярных по сравнению с Windows, например, Linux – такие системы более редко подвергаются хакерским атакам именно вследствие меньшей своей распространенности.

Таким образом, необходимо, чтобы на компьютере было установлено следующее программное обеспечение:

* антивирусное программное обеспечение;
* межсетевой экран;
* антитроянское программное обеспечение;
* антишпионское программное обеспечение;
* программное обеспечение для защиты от сетевых атак;
* программное обеспечение для фильтрации спама;
* программное обеспечение для контроля запущенных процессов;
* программное обеспечение для контроля файловой системы;
* программное обеспечение для контроля реестра;
* программное обеспечение для контроля уязвимости компьютера (открытые порты, открытые ресурсы и т. п.).

Необходимо описать исходные данные для анализа IT-инфраструктуры.

1.2 Описание исходных данных для анализа IT-инфраструктуры

Для анализа IT-инфраструктуры при создании единой компьютерной сети потребуются исходные данные компьютерных сетей организации и филиалов.

Исходными данными для анализа IT-инфраструктуры веб–студии являются:

1. Общая площадь этажа – 252 м2, количество помещений – 12.
2. Количество и места размещения рабочих станций – 18 компьютеров, расположенных в отделах; 3 коммутатора; 1 точка доступа; 2 камеры; 14 компьютеров; 1 роутер; 1 VoIP-шлюз; 8 принтеров; 14 телефонов; количество ip-телефонов – 14 шт.; количество принтеров – 7 шт.
3. Общее количество серверов – 2.
4. IP–адрес и маска компьютерной сети: Внутренний локальный   
   адрес – 172.16.14.0/24.

Рассмотрим отделы первого филиала:

1. Отдел охраны (1 человек).
2. Отдел программистов. (3 человека).
3. Отдел дизайна. (2 человека).

Общее количество помещений первого филиала веб-студии – 4. В отделах размещены: 1 коммутатор; 6 компьютеров; 3 камеры; 1 точка доступа для камер; 1 роутер; 1 принтер; 1 маршрутизатор и 1 беспроводной роутер; 1 сервер.

Рассмотрим отделы второго филиала:

1. Отдел охраны (1 человек).
2. Отдел программистов (3 человека).
3. Отдел дизайна. (2 человека).

Общее количество помещений второго филиала веб-студии – 4. В отделах размещены: 1 коммутатор; 6 компьютеров; 3 камеры; 1 точка доступа для камер; 1 роутер; 1 принтер; 1 маршрутизатор и 1 беспроводной роутер; 1 сервер.

Далее перейдем к описанию логической топологии сети.

1.3 Описание логической топологии сети

Топология сети – это способ соединения компьютеров, серверов и других устройств в сети. Топология определяет, как устройства соединяются друг с другом, какие устройства соединены, а также каким образом данные передаются от одного устройства к другому.

Топологии делится на 2 большие категории:

1. Физическая топология сети (физическая схема сети показывает, как эта сеть выглядит в реальном мире: где, как и какие кабели уложены, где, как и какое оборудование установлено, как оно запитано, какая длина у какого кабельного пролета, какой кабель в какой порт включен, как разварена оптика, как расшита кросс-панель и так далее).
2. Логическая топология сети (Логическая топология показывает, как по сети передаются определенные единицы информации, и определяет метод доступа к сетевой среде передачи данных).

На рисунках 2-4 изображены физическая и логическая топология сети организации.

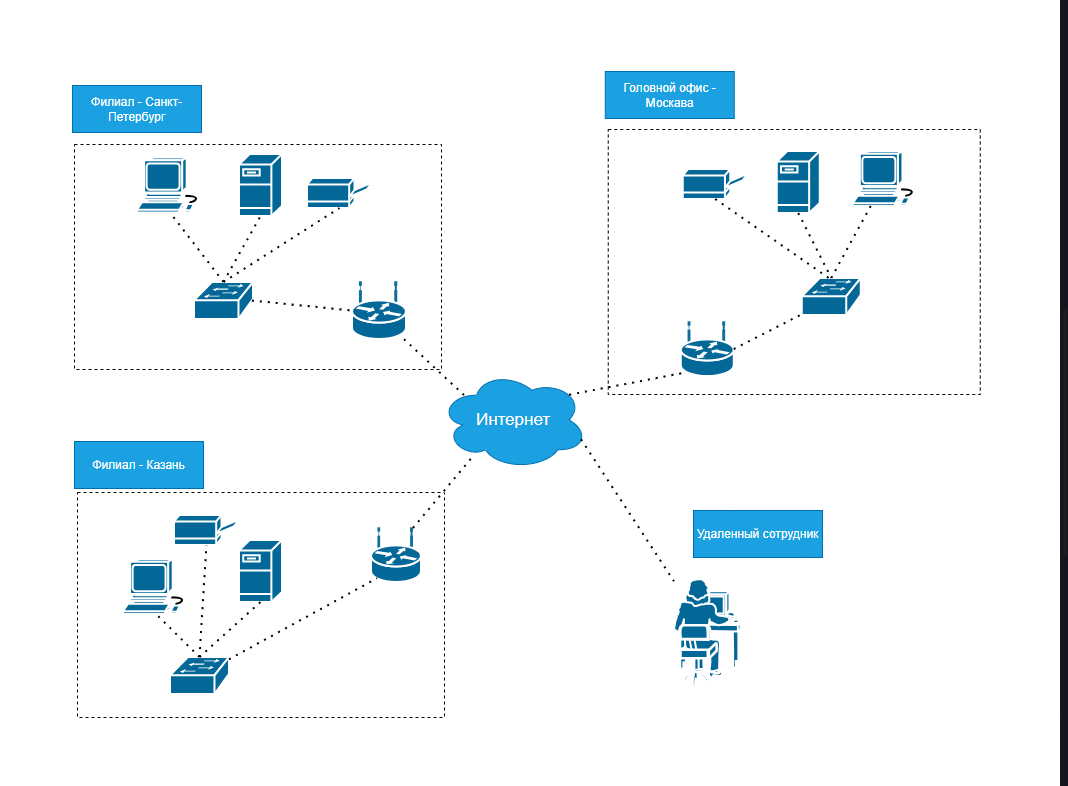


Рисунок 2 – Физическая топология сети организации

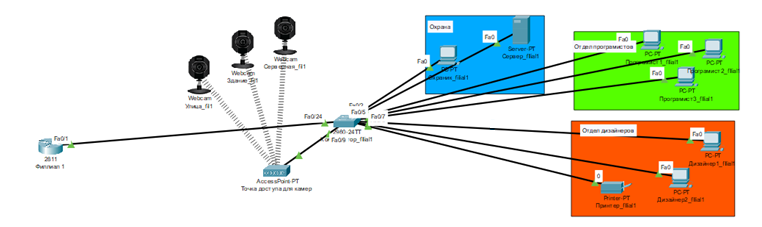


Рисунок 3 – Логическая схема сети филиала 1

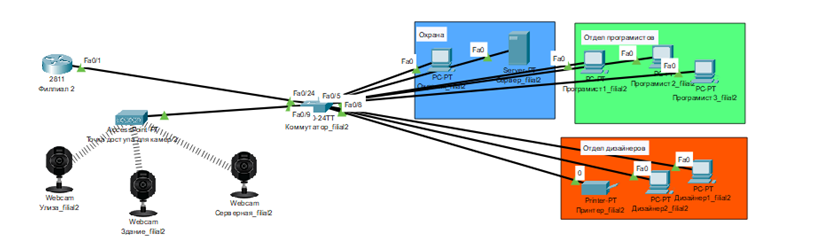


Рисунок 4 – Логическая схема сети филиала 2

Для управления организацией необходимо централизованное управление компьютерной сетью. Система компьютерной сети на правах отдела управляется централизованно и контролирует доступ сотрудников к ресурсам и информации через головной офис. Для этого потребуется Active Directory, что позволяет централизовано администрировать все ресурсы, любые произвольные объекты и сервисы: файлы, периферийные устройства, базы данных, подключения к Web, учетные записи и др. Рассмотрим назначение Active Directory:

1. Централизованное хранение информации.
2. Аутентификация и авторизация.
3. Управление групповыми политиками.
4. Репликация данных.
5. Управление сертификатами.
6. Интеграция с другими сервисами и приложениями.
7. Аудит и мониторинг.

Для предприятия с большим количеством узлов необходимы служба DHCP и DNS. Они есть в Active Directory, которая нужно для дальнейшей настройки прав доступа и групповых политик.

В целом, Active Directory является мощным инструментом для управления и организации информации в сети, обеспечивая безопасность, доступность и удобство использования для пользователей и администраторов.

Перейдем к логической структуре Active Directory.

Логическая структура Active Directory – модель службы каталога, которая определяет каждого участника безопасности на предприятии, а также организацию этих участников.

На рисунке 5 представлена логическая схема веб-студии.



Рисунок 5 – Логическая структура веб-студии

1.4 Описание взаимодействия серверов компьютерной сети

Сервера должны быть разделены: каждый сервер – отдельный сегмент сети. Между серверами должно быть соединение. Пользователи из различных подсетей не должны/должны иметь доступ друг к другу (пример: сегмент бухгалтерии, сегмент кассиров/операторов, сегмент склада и т.д.).

Опишем несколько способов соединения локальных сетей офисов и удаленных филиалов:

1. Использование VPN (Virtual Private Network – виртуальная приватная сеть). Этот способ позволяет создать безопасное соединение между офисами и обеспечить конфиденциальность передаваемой информации.
2. Применение беспроводных технологий для передачи данных, таких как Wi-Fi или 4G. Это позволяет передавать данные на большие расстояния без необходимости прокладки кабеля.
3. Использование облачных сервисов. Облачные сервисы позволяют хранить и обмениваться файлами между офисами без необходимости физического перемещения данных.
4. Организация удаленного доступа к корпоративным ресурсам через Интернет. Этот способ позволяет сотрудникам работать с корпоративными ресурсами из любой точки мира, где есть доступ к Интернету.
5. Применение специализированных программных средств для управления сетевым трафиком и оптимизации работы сети. Такие программы позволяют контролировать использование сетевых ресурсов и оптимизировать работу сети, что может повысить ее производительность.

Для соединения локальных сетей офисов и удаленных филиалов был выбран VPN, поскольку он обеспечивает безопасное и конфиденциальное соединение между ними. VPN создает зашифрованный туннель между офисами, что позволяет передавать данные без риска их перехвата или подмены. Кроме того, VPN может использоваться для доступа к корпоративным ресурсам из удаленных мест, что может быть полезно для сотрудников, работающих вне офиса.

Метод объединения двух сетей с применением технологии VPN в англоязычной литературе называется «Peer-to-Peer VPN» или «site-to-site VPN». Между двумя сетями устанавливается режим «прозрачного шифрования». Для шифрования и передачи трафика в IP-сетях наиболее часто используют протокол IPSec.

Для организации VPN-соединенией (VPN-туннелей) между центральным офисом и филиалами небольших компаний рекомендуют использовать аппаратные интернет-шлюзы (firewall) со встроенной поддержкой VPN. Примером таких шлюзов могут быть [ZyXEL ZyWALL](http://www.murava.ru/catalog/hard/index.php?SECTION_ID=218), Netgear Firewall, Check Point Safe@Office, и т.п. Данный класс продуктов рассчитан на применение в небольших компаниях со средней численностью персонала от 5 до 100 человек. Эти устройства просты в настройке, обладают высокой надежностью и достаточной производительностью.

В головном офисе организации часто устанавливают программные интегрированные решения по защите сети, такие как «Microsoft Internet Security and Acceleration Server 2016» (Microsoft ISA 2016), CheckPoint Express, CheckPoint VPN-1 Edge и другие. Для управления этими средствами защиты необходимо наличие высококвалифицированного персонала, который, как правило, или имеется в головном офисе или заимствуется у компании-аутсорсера.

Существуют специализированные аппаратные крипто-шлюзы, разработанные для решения узкоспециализированных задач. Примерами могут служить Cisco VPN Concentrator, «Континент-К» и др. Их область применения - сети средних и крупных компаний, где необходимо обеспечить высокую производительность при шифровании сетевого трафика, а также специальные возможности. Например, обеспечить шифрование данных по ГОСТ   
(«Континент-К»).

Выбирая оборудование для организации виртуальной частной сети (VPN), необходимо обратить внимание на следующие свойства:

* количество одновременно-поддерживаемых VPN-туннелей;
* производительность;
* возможность фильтрации сетевого трафика внутри VPN-туннеля (эта функция реализована далеко не во всех интернет-шлюзах);
* поддержка управления качеством QoS (очень полезна при передаче голосового трафика между сетями);
* совместимость с имеющимся оборудованием и применяемыми технологиями, например интеграция с LDAP, Microsoft Active Directory для сквозной авторизации пользователей и т.п.

Аппаратные решения:

Преимущества решений, построенных на недорогих аппаратных   
интернет-шлюзах:

1. Низкая стоимость.
2. Высокая надежность (нет необходимости в резервном копировании, при отключении питания ничего не выходит из строя).
3. Простота администрирования.
4. Малое энергопотребление.
5. Занимает мало места, можно установить, где угодно.

В зависимости от выбранной платформы для построения VPN, имеется возможность для установки на vpn-шлюз дополнительных сервисов: антивирусная проверка интернет-трафика, обнаружение атак и вторжений, и др, что существенно увеличивает общий уровень защищенности сети и уменьшает общую стоимость решения по комплексной защите сети.

Недостатки:

* Решение не масштабируется, увеличение производительности достигается полной заменой оборудования.
* Менее гибко в настройках.
* Интеграция с Microsoft Active Directory (или LDAP), как правило, не поддерживается.

Программные решения, которые имеют свои преимущества и недостатки:

Преимущества программных решений:

* Гибкость.
* Масштабируемость, т.е. возможность увеличить производительность по мере необходимости.
* Тесная интеграция с Microsoft Active Directory (Microsoft ISA 2006, решения CheckPoint).

Недостатки:

* Высокая цена.
* Сложность администрирования.

Прежде чем приступить к выбору оборудования и программного обеспечения для реализации проекта по объединению локальных сетей офисов в единую сеть через VPN, необходимо располагать следующими сведениями:

1. Определить топологию:
   * Meshed (полносвязные) – каждый сайт может автоматически организовать шифрованное соединение с любым другим сайтом.
   * Star (звезда) - филиалы могут организовать защищенные соединения с центральным сайтом.
   * Hub and Spoke (связь через концентратор) – филиалы могут соединяться между собой через концентратор центрального сайта.
   * Remote Access (удаленный доступ) - пользователи и группы могут организовать безопасные соединения с одним или несколькими сайтами.
   * Комбинации перечисленных выше методов (например, топология Star with Meshed Center - звезда с полносвязным центром, – в которой удаленные филиалы могут обмениваться информацией со всеми членами центральной VPN, имеющей полносвязную топологию).
2. Количество филиалов (какое количество одновременных VPN-соединений должно поддерживать оборудование головного офиса).
3. Количество пользователей в центральном офисе и в каждом филиале.
4. Какое оборудование и/или ПО используется в каждом филиале (данные необходимы для учета возможностей по использованию существующего оборудования и/или ПО).
5. Данные по подключению филиалов к Интернет: назначение IP адреса – динамическое или статическое, скорость канала связи.
6. Какой подход к управлению информационной безопасностью (защита периметра сети, антивирусная безопасность) будет применен: централизованное управление головным офисом и филиалами одним администратором безопасности (системным администратором), или в каждом филиале свой системный администратор.

Чтобы минимизировать угрозы проникновения в сеть центрального офиса, необходимо уделить должное внимание защите сетей филиалов организации. Использование VPN не гарантирует надежную защиту от проникновения, если сети филиалов также не будут надежно защищены. Если злоумышленник сможет получить несанкционированный доступ к сети филиала, то он также сможет получить доступ и к информационной системе головного офиса, поскольку сети головного офиса и филиала объединены в единую сеть через VPN.

Для взаимосвязи сетей используются сервисы сервера:

1. DNS (Domain Name System) – служба, которая преобразует доменные имена в IP-адреса и наоборот.
2. DHCP (Dynamic Host Configuration Protocol) – протокол, который автоматически назначает IP-адреса, маски подсети и другие параметры сетевым устройствам.
3. FTP (File Transfer Protocol) – сервис для передачи файлов между компьютерами в сети.
4. SSH (Secure Shell) – безопасный протокол для удаленного доступа к серверу и выполнения команд на нем.
5. SMTP (Simple Mail Transfer Protocol) – почтовый протокол для отправки и получения электронной почты.
6. POP3 (Post Office Protocol version 3) – почтовый протокол для получения электронной почты с сервера.
7. IMAP (Internet Message Access Protocol) – почтовый протокол для работы с электронной почтой на сервере.
8. Syslog – система регистрации событий, происходящих в операционной системе, приложениях или сетевых устройствах. Она позволяет собирать и анализировать информацию о работе.

Для серверов и хостов необходимо выбрать программное обеспечение. производи

1.5 Анализ и обоснование выбора программного обеспечения серверов и хостов сети

Существует множество дистрибутивов с различными преимуществами и недостатками, разберем несколько из них:

1. RedOS (Российская операционная система, основанная на Linux и предназначенная для бизнеса и государственных организаций. Она разрабатывается компанией Ред Софт с 2005 года и имеет сертификаты соответствия требованиям информационной безопасности. Она может использоваться как тонкий клиент для бездисковых систем и виртуальных машин, а также имеет интуитивно понятную графическую оболочку и набор системных утилит. РЕД ОС поддерживает работу с документами, графическими редакторами, почтовыми клиентами, мультимедийными плеерами, аудио и видео редакторами, а также имеет браузер с поддержкой ГОСТ-криптографии и отечественных ГИС).
2. Astra linux (Операционная система на базе ядра Linux, которая внедряется в России в качестве альтернативы Microsoft Windows в государственных организациях. Обеспечивает степень защиты обрабатываемой информации до уровня государственной тайны «особой важности» включительно. Astra Linux выглядит как неплохая замена офисной версии Windows в рамках программы перехода на свободное программное обеспечение госорганов, а для домашнего использования она может показаться несколько консервативной).
3. Ubuntu – это операционная система, основанная на ядре Linux. Она имеет открытый исходный код и распространяется бесплатно. Ubuntu предназначена для использования на компьютерах различных типов, включая настольные компьютеры, ноутбуки, серверы и другие устройства. Ubuntu имеет простой и понятный интерфейс, который легко освоить даже новичкам. В Ubuntu есть множество приложений, которые можно установить из магазина приложений Ubuntu. Ubuntu также имеет поддержку многих аппаратных устройств, что делает ее подходящей для использования на различных компьютерах.

Проанализируем их преимущества и недостатки, выберем самый подходящий.

В таблице 1 указаны преимущества и недостатки дистрибутивов.

Таблица 1 – Сравнение дистрибутивов Linux

|  |  |  |
| --- | --- | --- |
| Дистрибутив | Преимущества | Недостатки |
| RedOS | – Высокая степень защиты от вредоносных программ и вирусов благодаря использованию отечественных разработок в области информационной безопасности. – Поддержка российских криптографических алгоритмов, что делает систему более защищенной от атак на криптографические ключи. | – Ограниченное количество программного обеспечения, которое можно установить на систему, так как многие программы не имеют поддержки российских криптографических алгоритмов. – Недостаточное количество документации по настройке и использованию системы, что затрудняет работу с ней для неопытных пользователей. |
| Ubuntu | – Открытый исходный код: Ubuntu является одним из самых популярных дистрибутивов Linux, так как его исходный код является открытым и доступным для всех. – Бесплатное программное обеспечение: Ubuntu включает в себя множество бесплатных программ, которые могут быть использованы для выполнения различных задач. | – Ограниченное количество приложений: хотя Ubuntu имеет множество бесплатных приложений, некоторые профессиональные приложения могут быть недоступны. – Зависимость от обновлений: Ubuntu требует регулярных обновлений, чтобы поддерживать систему в актуальном состоянии. Если обновления не выполняются регулярно, система может стать уязвимой для атак. |

Продолжение таблицы 1

|  |  |  |
| --- | --- | --- |
| Astra linux | – Astra Linux имеет открытый исходный код, что означает, что любой желающий может просмотреть и изменить код операционной системы.  – Система имеет высокую степень защиты от вирусов и других вредоносных программ благодаря использованию антивирусного ПО ClamAV и системы обновления.  – Astra Linux поддерживает большое количество аппаратного обеспечения, что позволяет использовать ее на различных типах компьютеров.  – Операционная система имеет простой и интуитивно понятный интерфейс. | – Некоторые программы и приложения, которые используются в других операционных системах, могут не работать в Astra Linux. – Процесс обновления системы может быть сложным для некоторых пользователей, особенно для тех, кто не знаком с Linux. В целом, Astra Linux является надежной и безопасной операционной системой, которая подходит для использования в различных организациях. |

Для сервера был выбран дистрибутив RedOS, потому что эта система обладает высокой степенью защиты от вредоносного ПО и вирусов, поддерживает российские криптографические алгоритмы, а также имеет открытый исходный код. Кроме того, RedOS легко устанавливается и настраивается, что делает ее удобной для использования на сервере.

Для хоста был выбран дистрибутив Ubuntu, так как он имеет открытый исходный код и большое количество доступных приложений. Кроме того, Ubuntu прост в использовании и настройке, что делает его подходящим для начинающих пользователей.

Для мониторинга сети существуют специальные программы.

Программы для мониторинга сети позволяют оперативно реагировать на аномальную деятельность в пределах локальной сети, быть в курсе всех сетевых процессов и, таким образом, автоматизировать часть рутинной деятельности администратора: прежде всего той, что связана с обеспечением сетевой безопасности. Давайте рассмотрим несколько из них:

* Nagios (один из наиболее популярных инструментов для мониторинга сети благодаря своей гибкости, обширным возможностям и открытому исходному коду. Он поддерживает мониторинг различных параметров, включая доступность серверов, загрузку процессора, использование памяти, состояние сервисов и многое другое).
* Zabbix (популярный инструмент для мониторинга сети, который предлагает широкий спектр функций, таких как мониторинг производительности, обнаружение проблем, оповещение о событиях и интеграция с другими системами. Он имеет открытый исходный код и предлагает масштабируемость для больших сетей).
* Icinga (альтернативное решение для мониторинга Nagios, которое предлагает схожую функциональность. Он использует легкие агенты для мониторинга удаленных систем и централизованную консоль для управления и оповещения).
* Cacti (система мониторинга сети с открытым исходным кодом, которая фокусируется на мониторинге и отображении использования ресурсов, таких как пропускная способность сети, использование дискового пространства и загрузка процессора. Он предлагает визуализацию данных с помощью графиков и диаграмм).
* Zenoss (система мониторинга сети, которая обеспечивает мониторинг, оповещение и анализ в реальном времени).

В таблице 2 указаны преимущества и недостатки программ мониторинга.

Таблица 2 Сравнение программ мониторинга сети

|  |  |  |
| --- | --- | --- |
| Название | Преимущества | Недостатки |
| Nagios | Гибкость, обширные возможности, открытый исходный код | Требует знаний для настройки и управления |
| Zabbix | Широкий спектр функций, открытый исходный код, масштабируемость | Может быть сложным для настройки и управления для новичков |
| Icinga | Альтернатива Nagios, легкие агенты, централизованная консоль | Меньше функций по сравнению с Nagios и Zabbix |
| Cacti | Мониторинг и визуализация использования ресурсов, открытый исходный код | Ограниченный функционал по сравнению с другими решениями |
| Zenoss | Мониторинг, оповещение и анализ в реальном времени, визуализация данных | Высокая стоимость лицензий |

Для мониторинга объединённой компьютерной сети был выбран Zabbix, потому что это один из самых популярных и функциональных инструментов для мониторинга. Он обладает широким функционалом, открытым исходным кодом, гибкостью и масштабируемостью. Кроме того, Zabbix предлагает бесплатную версию и активно поддерживается сообществом.

Перейдем к описанию удаленного администрирования.

1.6 Описание удаленного администрирования

Удаленное администрирование – это процесс управления и поддержки компьютерных систем и сетей на расстоянии, обычно из центрального офиса или места, отличного от того, где находятся эти системы. Это позволяет организациям предоставлять своим сотрудникам, партнерам или клиентам доступ к ресурсам и приложениям, а также контролировать и управлять ими. Удаленное администрирование может включать в себя широкий спектр задач, таких как установка и настройка программного обеспечения, устранение неполадок, обновление систем, резервное копирование данных и многое другое.

Способы удаленного администрирования:

1. Удаленный Рабочий Стол – этот метод позволяет управлять компьютером на расстоянии, будто вы находитесь прямо перед ним. Для использования этого метода необходимо установить специальное программное обеспечение на оба компьютера.
2. Облачные Приложения – это приложения, доступные через интернет. Они могут использоваться для управления серверами и базами данных на расстоянии.
3. Мобильные Приложения – эти приложения позволяют управлять устройствами на расстоянии с помощью смартфона или планшета. Они обычно имеют ограниченный функционал по сравнению с другими методами удаленного администрирования.

В таблице 3 указаны преимущества и недостатки этих способов.

Таблица 3 ­ Сравнение приложений удаленного администрирования

|  |  |  |
| --- | --- | --- |
| Приложения удаленного администрирования | Преимущества | Недостатки |
| Удаленный рабочий стол | Высокая степень контроля | Требует значительных ресурсов |
| Веб-приложения | Доступ через интернет | Ограниченный функционал |
| Мобильные приложения | Удобство использования | Ограниченный функционал |

Опишем скрипты для реализации удаленного администрирования.

Скрипт – это программа или набор инструкций, которые выполняются на компьютере. Скрипты могут быть написаны на различных языках программирования, таких как Python, JavaScript, Powershell. Они используются для автоматизации рутинных задач, упрощения разработки приложений и улучшения производительности.

Сделав анализ предметной области, описав исходные данные, логическую топологию, взаимодействие серверов, удаленное администрирование и обосновав выбор программного обеспечения можно приступать к выполнению проектной части.

2 Проектная часть

2.1 Установка операционной системы и дистрибутивов

При разработке проектной части был создан прототип объединённой сети в программе для создания виртуальных машин в одной системе VMware Workstation Pro 17. Структура сети из ВМ показана на рисунке 6.

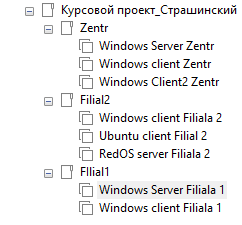


Рисунок 6 – Структура сети VMware Workstation

Было смоделировано три сети:

1. Cеть zentr, в эту сеть входят следующие ВМ: Server zentr (Windows Server 2016/2019), Windows client zentr (Windows 10 Pro), Udalen client (удаленный сотрудник подсоединяется к серверу по VPN). 192.168.14.0./24.
2. Cеть Filiala 1: Server Filiala 1 (Windows Server 2016/2019), Windows client Filiala 1 (Windows 10 Pro). 192.168.34.0./24.
3. Cеть Filiala 2: RedOS server Filiala 2, Ubuntu client Filiala 2, Windows client Filiala 2 (Windows 10 Pro). 192.168.114.0./24.

Связь между компьютерными сетями указанная на рисунке 7.

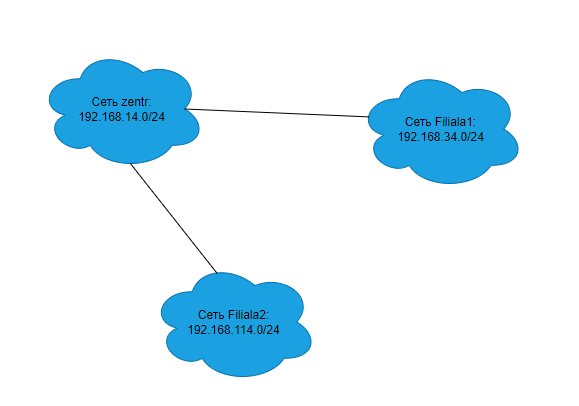


Рисунок 7 – Связь между компьютерными сетями

На виртуальных машинах в головной офис и филиал 1 была произведена установка операционных систем Windows Server 2019 и Windows 10 Pro, а на филиал 2 были установлены дистрибутивы RedOS server и Ubuntu client.

Установка Windows server 2019 была произведена следующим образом:

1. Выбран дистрибутив (язык системы вшит в образ).
2. При установке выбираем windows server stadart core.
3. Принимаем условия лицензирования.
4. Выбираем выборочную установку и диск на который будет установлна операционная система.
5. Начинается установка, после которой необходимо задать пароль для учетной записи.
6. Входим под администратором и начинаем настраивать необходимые службы.

Результат установки Windows Server 2019 показан на рисунке 8.

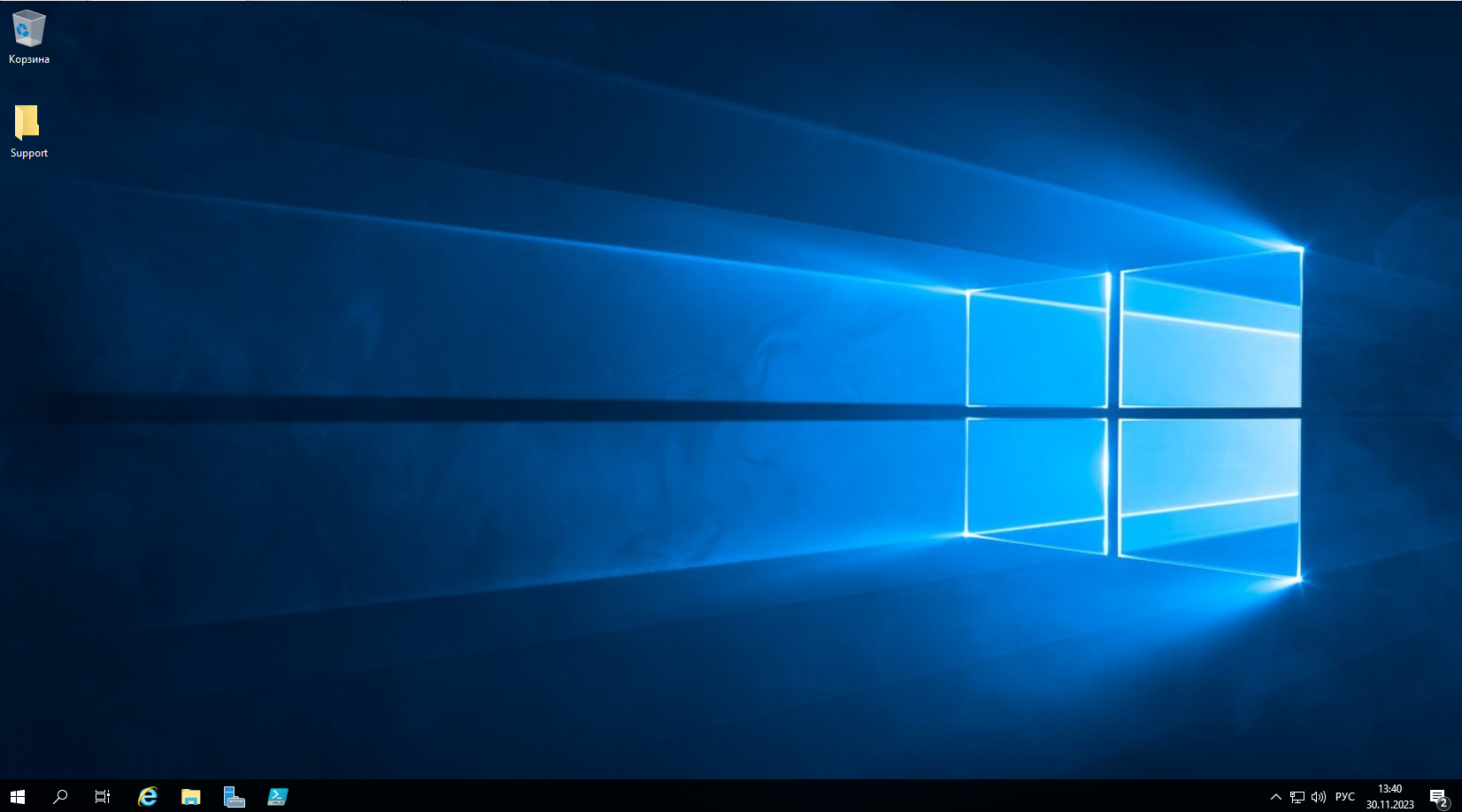


Рисунок 8 – Установленый Windows Server 2019

Аналогично с Windows Server 2019 был установлен Windows 10 Pro.

Результат установки Windows 10 Pro показан на рисунке 9.

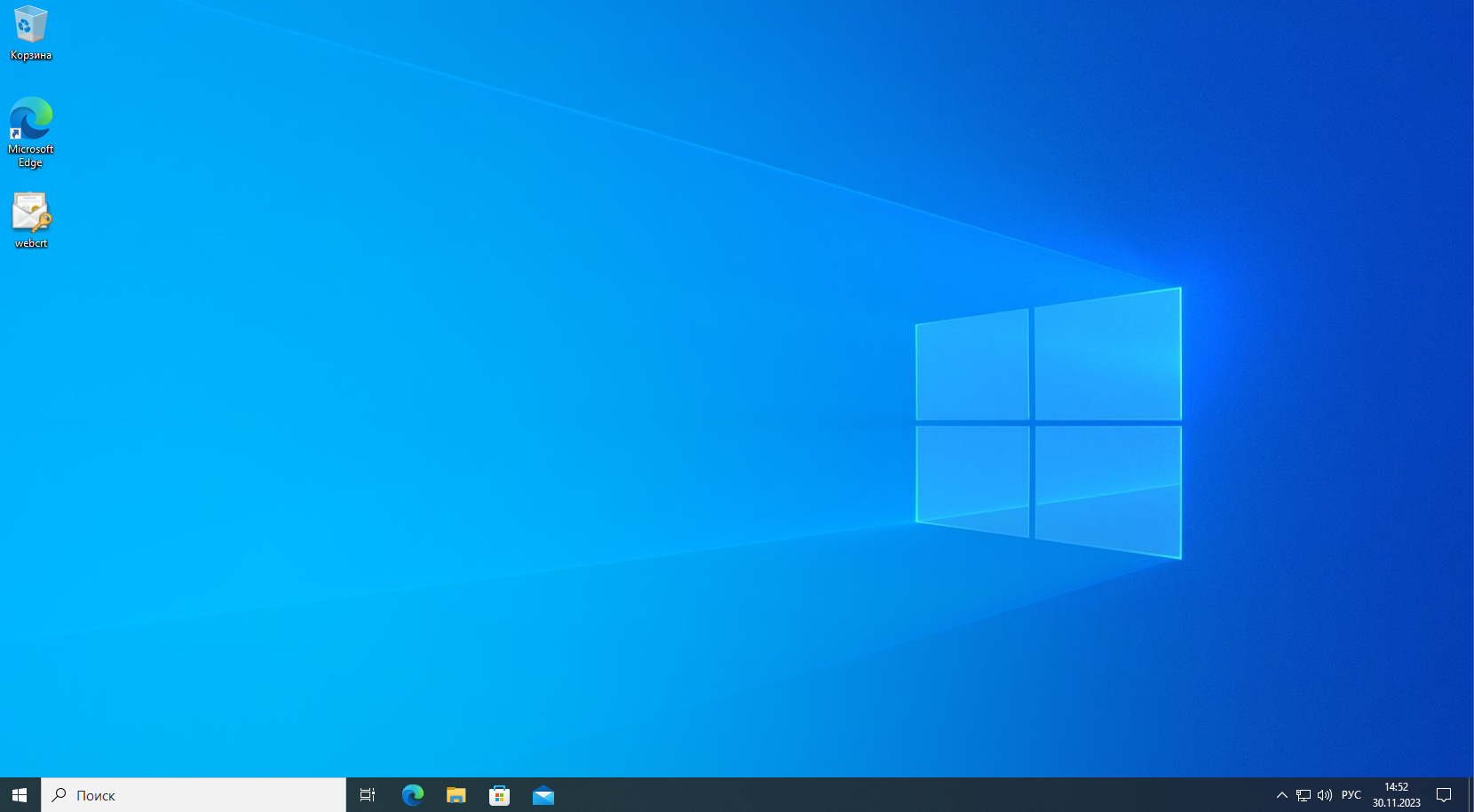


Рисунок 9 – Установленый Windows 10 Pro

Установка RedOS была произведена следующим образом:

1. Выбран дистрибутив.
2. Выбираем язык системы, временную зону, устанавливаем пароль root, создаем пользователя по умолчанию.
3. Ждем установки системы.
4. Принимаем условия лицензирования.
5. Входим под пользователем и настраиваем необходимые службы.

Результат установки RedOS показан на рисунке 10.



Рисунок 10 – Установленый RedOS

Установка Ubuntu была произведена следующим образом:

1. Выбран дистрибутив.
2. Выбираем язык системы, задаем пароль root, создаем пользователя по умолчанию, принимаем условия лицензирования.
3. Ждем установку системы.
4. Входим под пользователем и начинаем установку необходимых служб

Результат установки Ubuntu показан на рисунке 11.

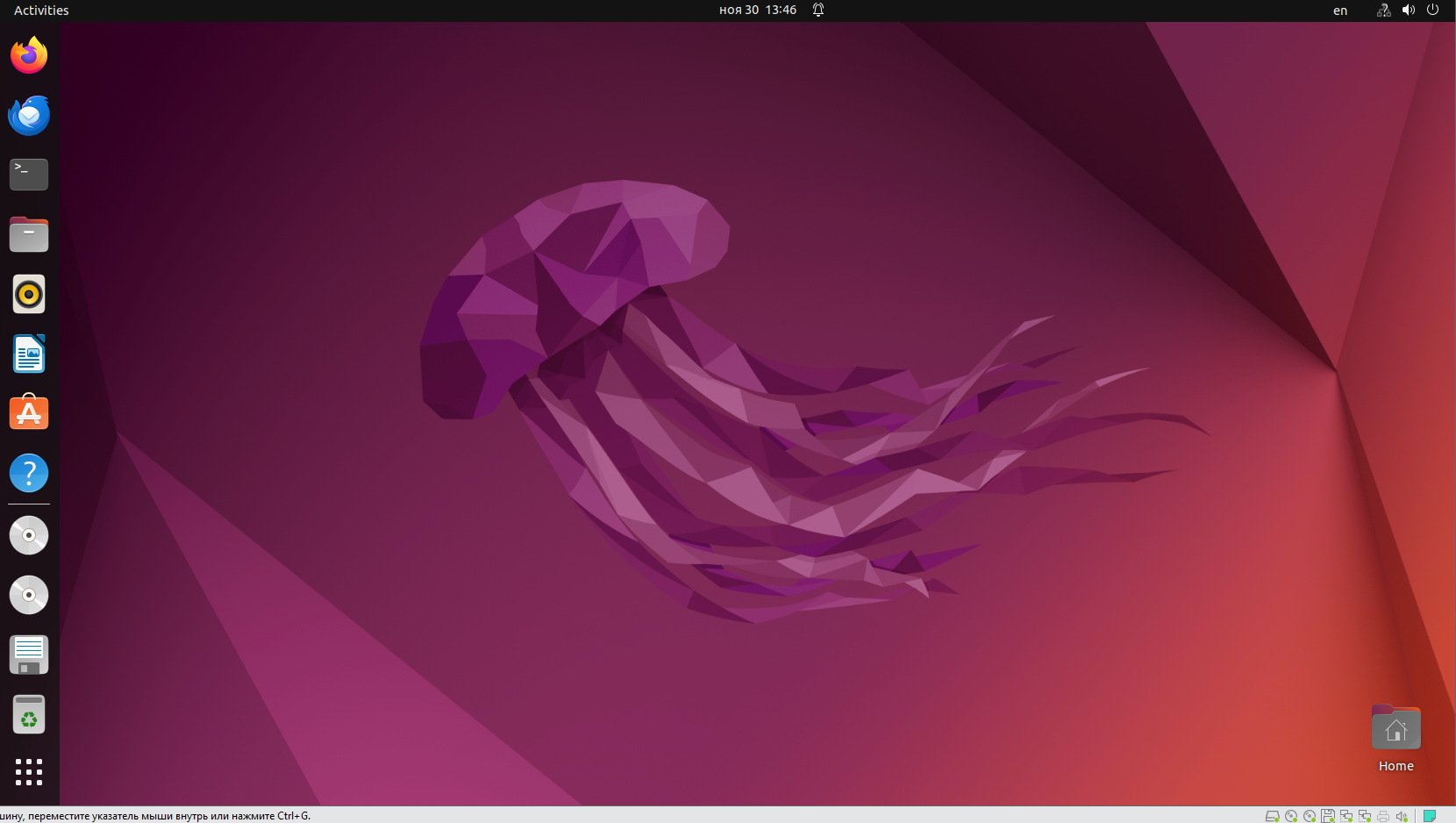


Рисунок 11 – Установленый Ubuntu

2.2 Установка сетевых протоколов и служб серверов

На виртуальной машине филиала 1 с установленной Windows Server 2019 были настроены службы DHCP, DNS, Web-server, Система архивации, файловый сервер, Домен, NTP, Сертификация, VPN.

Результаты настройки служб представлены на рисунках 12-17:

1. Для разворачивания Active Directory (AD) был задан статический адрес виртуальной машины, установлены доменные службы, создан новый лес, задан пароль администратора, указано имя NetBIOS, указаны пути до базы данных AD DS и файлов журналов и папки SYSVOL. Результат показан на рисунке 12.

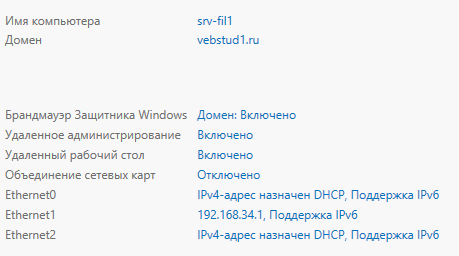


Рисунок 12 – Доменные службы AD

1. Для присваивания имен в сети была установлена служба DNS, показана на рисунке 13.

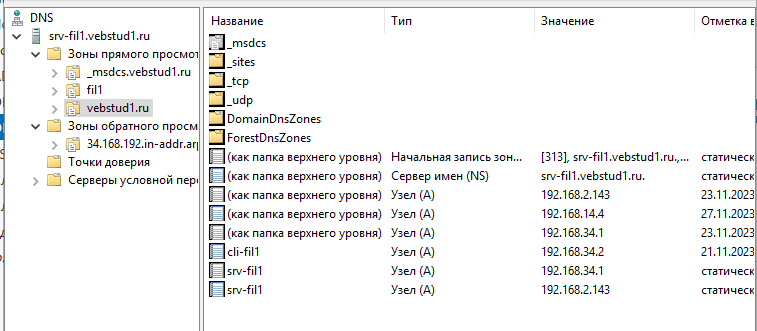


Рисунок 13 – Служба DNS

1. Для динамической раздачи адресов была установлена служба DHCP, показана на рисунке 14.

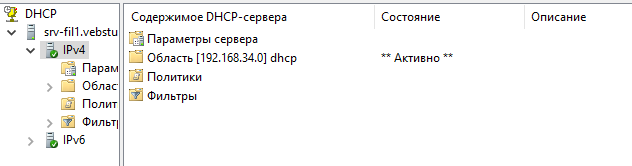


Рисунок 14 – Служба DHCP

1. Чтобы организация могла привлекать покупателей был настроен сайт, показан на рисунке 15.

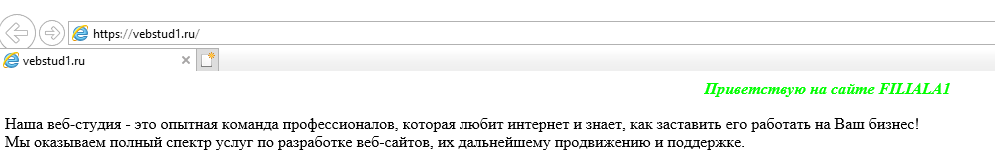


Рисунок 15 – Работа веб-сервера

1. Чтобы сайт пользовался доверием у покупателей был настроен центр сертификации, показан на рисунке 16.

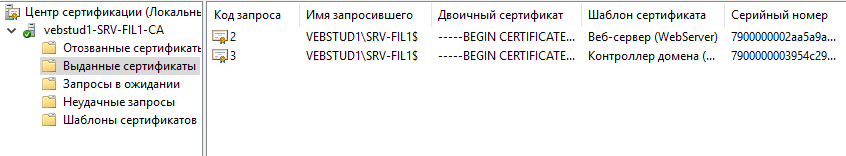


Рисунок 16 – Служба сертификатов

1. Для хранения файлов данных и предоставления к ним общего доступа настроена файловая служба, показана на рисунке 17.

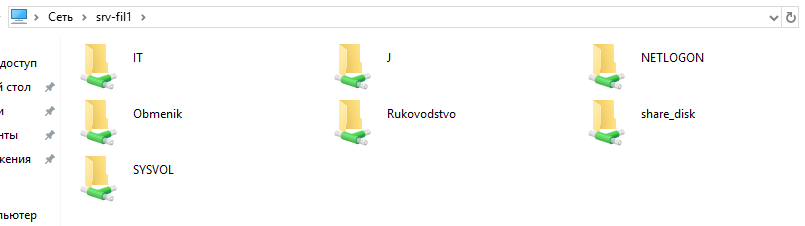


Рисунок 17 – Работа файловой службы

2.3 Настройка сетевых служб хостов

На виртуальную машину клиента головного офиса с Windows 10 Pro были установлены службы. На клиенте с Windows 10 Pro были настроены   
службы, показанные на рисунках 18-23:

1. Успешная проверка динамической раздачи адресов на клиенте, показана на рисунке 18.

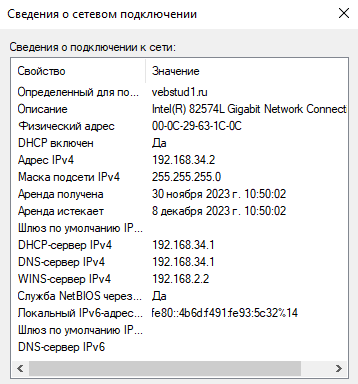


Рисунок 18 – Получение динамического адреса клиентом

1. Успешное присваивание доменных имен показано на клиенте, показано на рисунке 19.

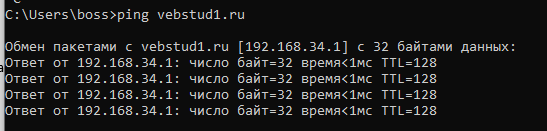


Рисунок 19 – Проверка работы DNS

1. Клиент имеет доступ к файловому серверу, показан на рисунке 20.

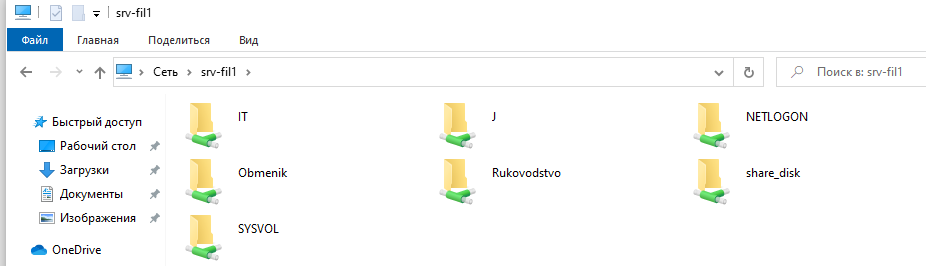


Рисунок 20 – Настройка файлового сервера

1. Сайт успешно открывается на клиенте, показан на рисунке 21.

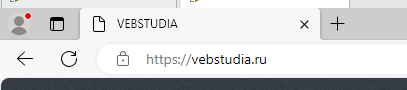


Рисунок 21 – Использование веб-сервера

1. Настроенный VPN успешно используется клиентом, показан на   
   рисунке 22.

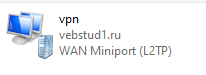


Рисунок 22 – Использование VPN

1. Клиент успешно синхронизировался с сервером NTP, показан на рисунке 23.

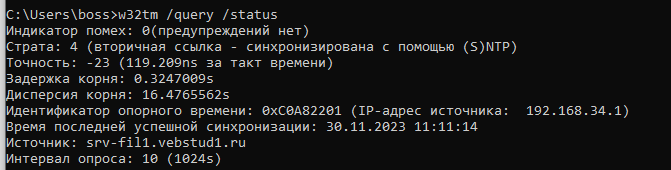


Рисунок 23 – Использование NTP

На виртуальную машину клиента филиала 2 с дистрибутивом RedOS были установлены следующие службы. Службы представлены на рисунках 24-28:

1. Развернутый домен показан на рисунке 24.

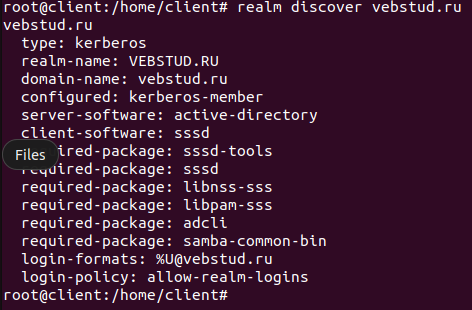


Рисунок 24 – Использование VPN

1. Результат синхронизации времени на машине клиента, показан на рисунке 25.

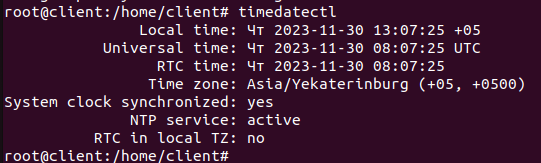


Рисунок 25 – Синхронизация времени

1. Работа настроенной DNS показана на рисунке 26.

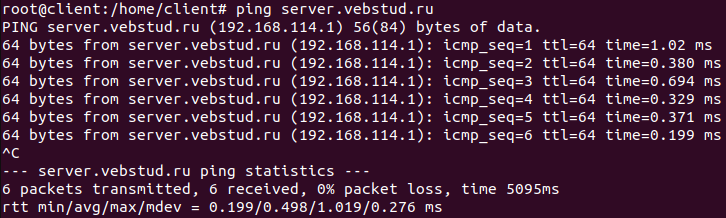


Рисунок 26 – Работа DNS

1. Открытие сайта по https показано на рисунке 27.

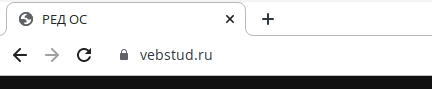


Рисунок 27 – Сайт организации

1. Доступ к файловому серверу для определенных пользователей показан на рисунке 28.

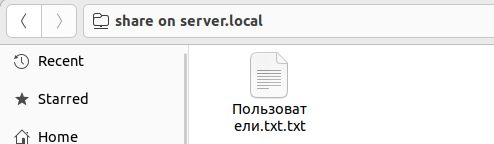


Рисунок 28 – Доступ к общей папке

2.4 Организация администрирования компьютерной сети

На сервер веб-студии с Windows Server 2019 были установлены и настроены службы. Результаты работы установленных служб показаны на рисунках 28-36:

1. Доменные службы AD предопределяют компьютер доменным контроллером, что позволяет управлять сетью и хранить на нем все имеющиеся данные. Результат показан на рисунке 29.

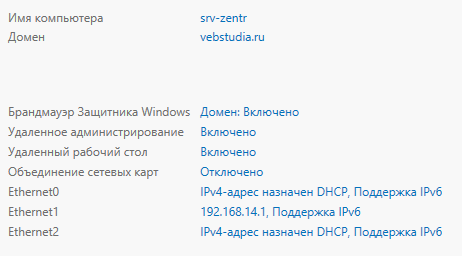


Рисунок 29 – Доменные службы AD

1. Для взаимодействия компьютерных сетей были присвоены имена через настроенную службу DNS, показаны на рисунке 30.

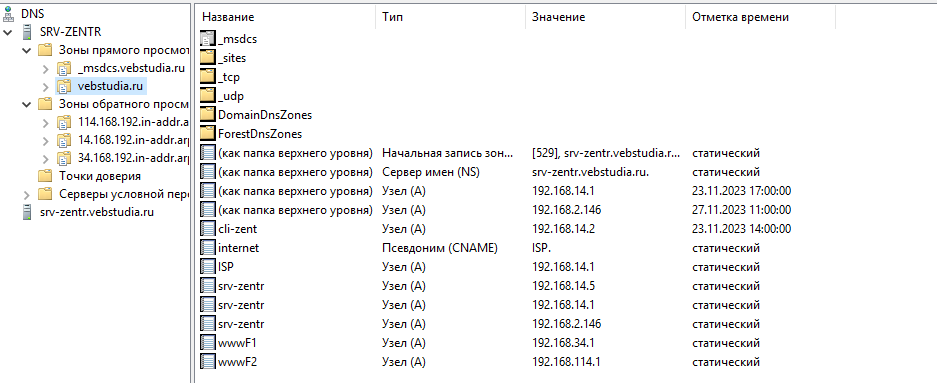


Рисунок 30 – Служба DNS

1. Для динамической раздачи адресов была установлена и настроена служба DHCP, настройка показана на рисунке 31.

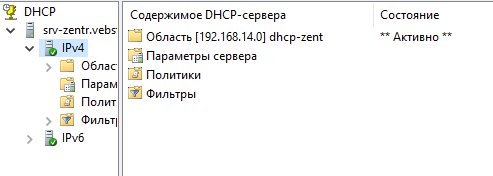


Рисунок 31 – Служба DHCP

1. Был настроен сертификат для открытия сайта по протоколу https, показан на рисунке 32.

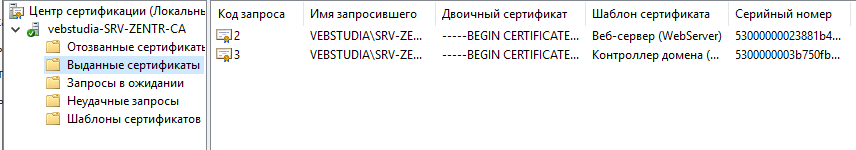


Рисунок 32 – Служба сертификатов

1. Для привлечения покупателей создан сайт организации, показан на рисунке 33.

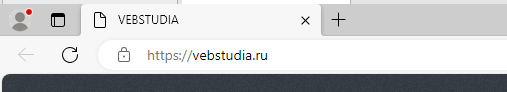


Рисунок 33 – Работа веб-сервера

1. Для хранения данных настроен общий ресурс, показано на рисунке 34.

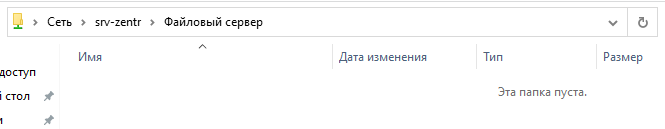


Рисунок 34 – Работа файловой службы

1. Чтобы не потерять важные данные настроена служба архивации Windows, показана на рисунке 35.

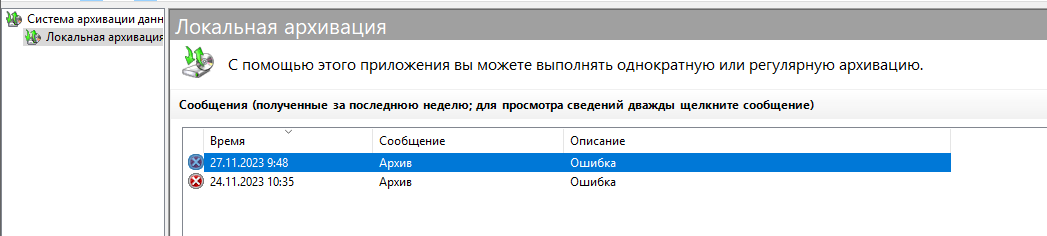


Рисунок 35 – Работа службы архивации Windows

1. Для удаленной настройки сервера настроен VPN, показан на рисунке 36.

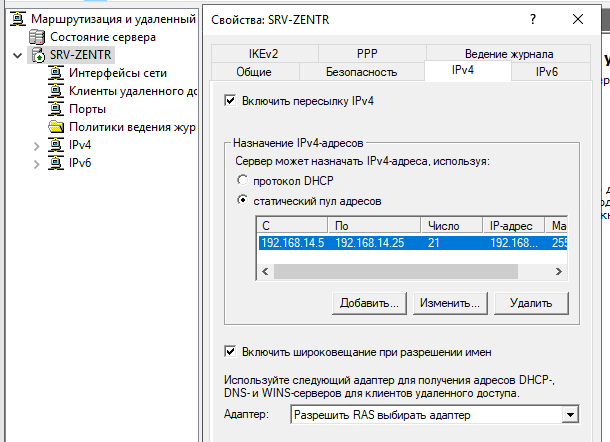


Рисунок 36 – Использование VPN

2.5 Организация взаимодействия между головным офисом и филиалами

Для этого настроим связность между подсетями филиал 1 – головной офис, филиал – головной офис и туннель между филиалами.

Для начала настроим логическую сеть в Cisco Packet Tracer: соединили кабелями маршрутизаторы, настроили статические адреса, настроили списки доступа, определили политику ISAKMP и указали что будем использовать предварительный ключ, настроили фазу 1 и 2 туннеля IPSec, связываем фазы вместе, определив крипто карту, активируем IPSec на исходящем интерфейсе, применяя крипто карту к интерфейсу, проверяем что туннель запущен, и настройка завершена.

Настроенный туннель между компьютерными сетями показан на   
рисунках 37-39.

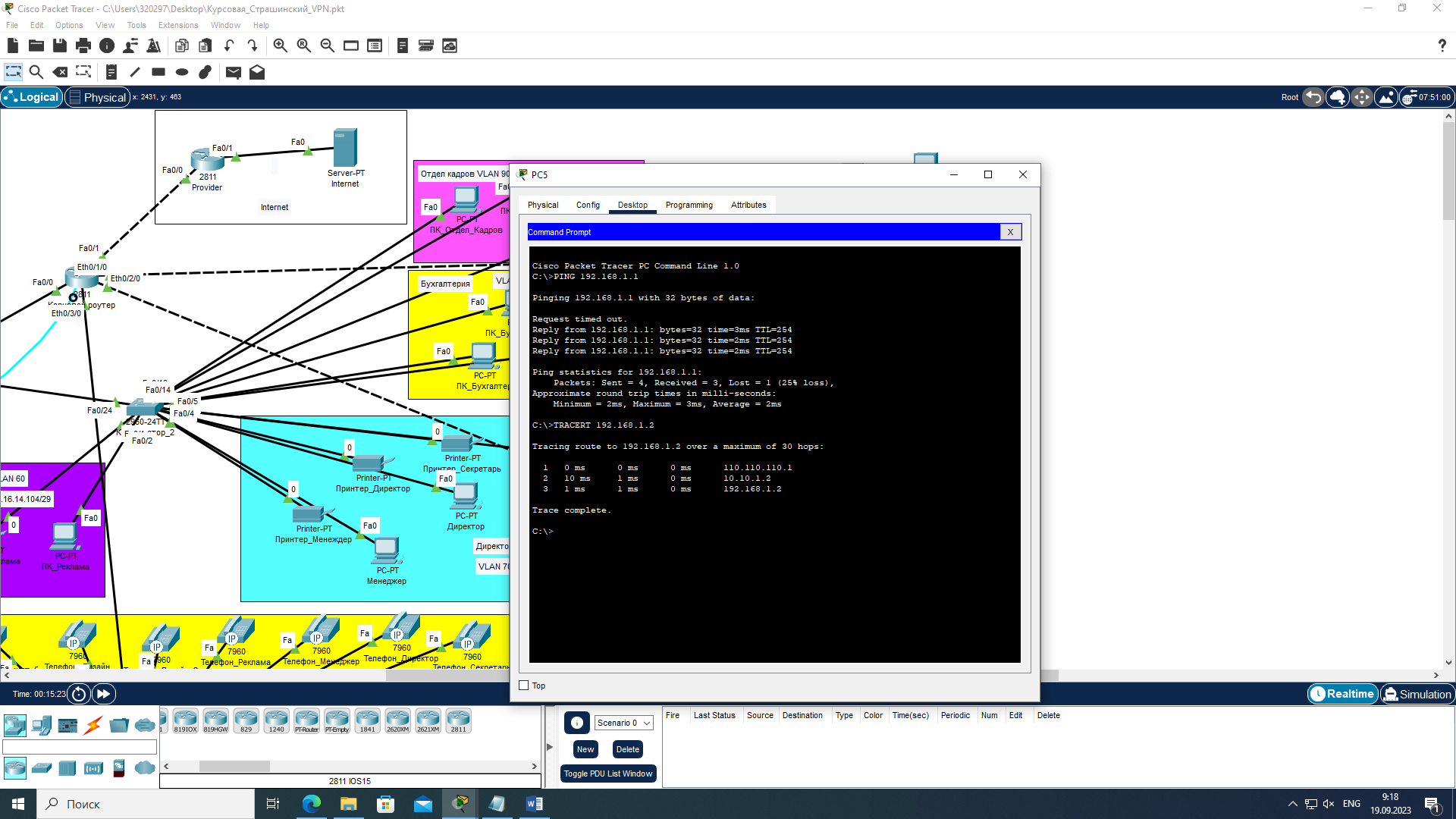


Рисунок 37 – Результат команды tracert

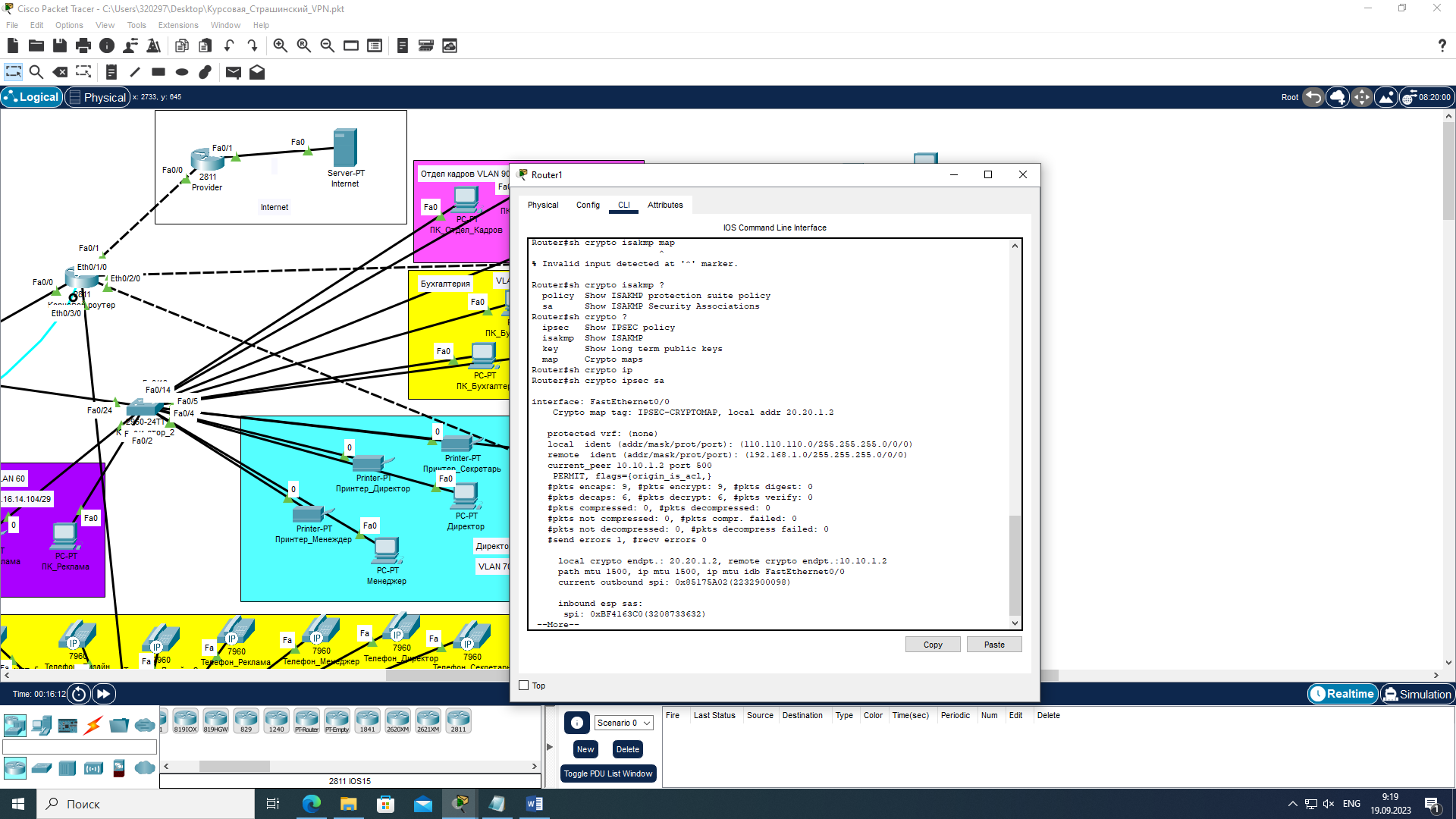


Рисунок 38 – Крипто карта

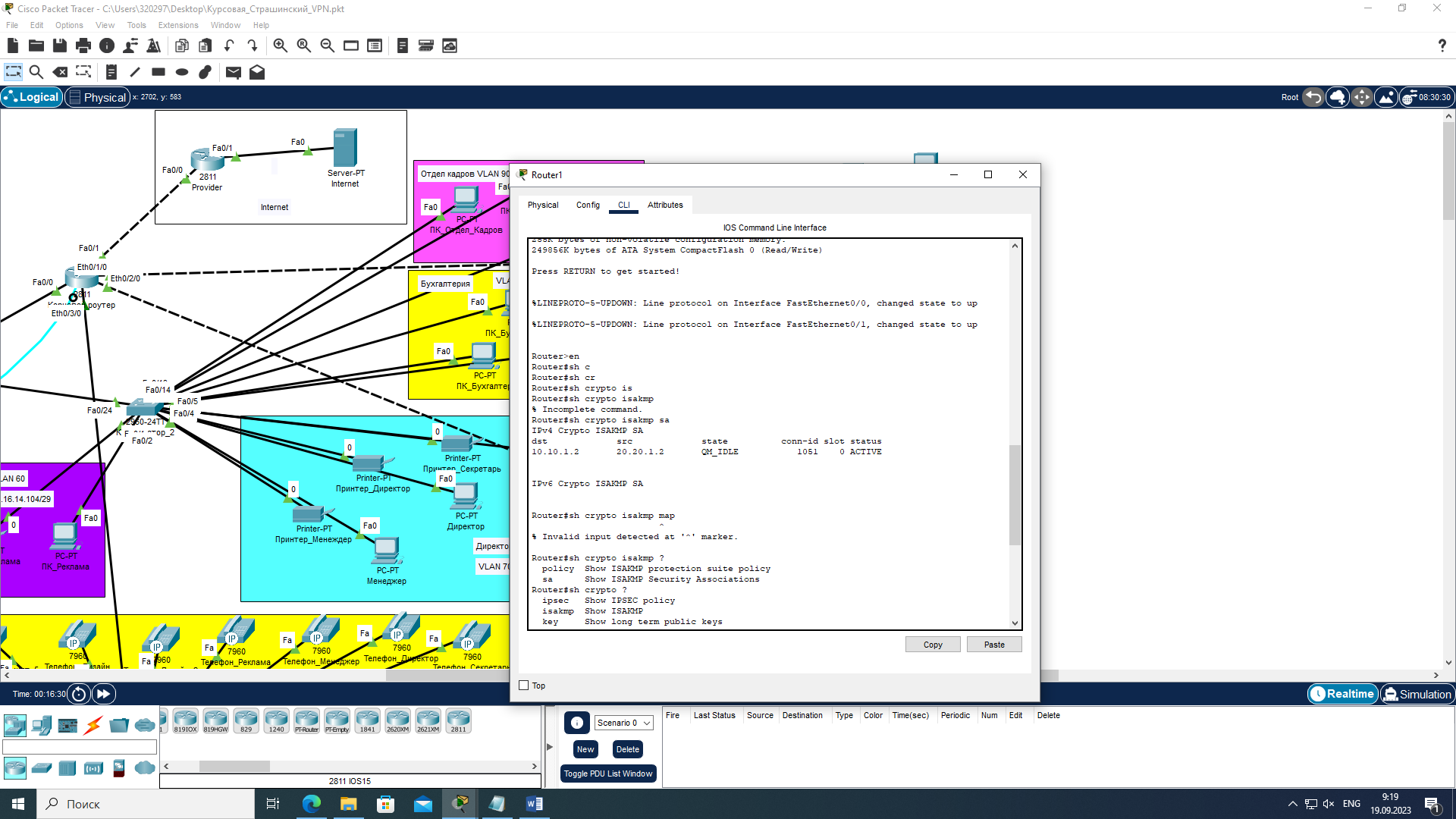


Рисунок 39 – Результат команды сrypto isakmp sa

На рисунке 40 показан путь до роутера организации.

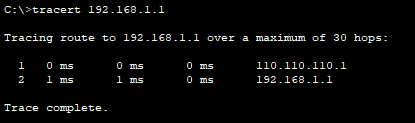


Рисунок 40 – Путь до роутера организации

Настроена связность между роутерами головного офиса и филиалов.

В приложении А представлена структура объединенной сети организации и ее филиалов.

На рисунке 41 показана установленная служба удаленного доступа.

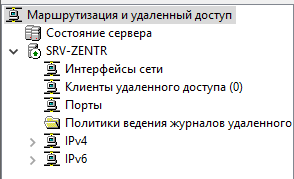


Рисунок 41 – Установленная служба удаленного доступа

На рисунках 42 и 43 показана настройка безопасности удаленного доступа.

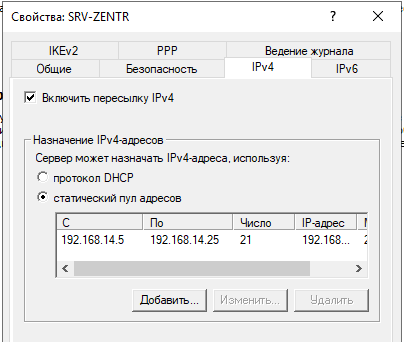


Рисунок 42 – Настройка статического пула адресов

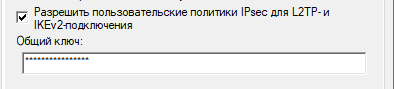


Рисунок 43 – Общий ключ

На рисунке 44 показана настройка пользователя, который будет заходить по удаленному доступу.

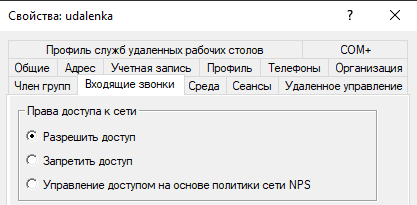


Рисунок 44 – Настройка пользователя

На рисунках 45–46 показано подключение по VPN c клиента.

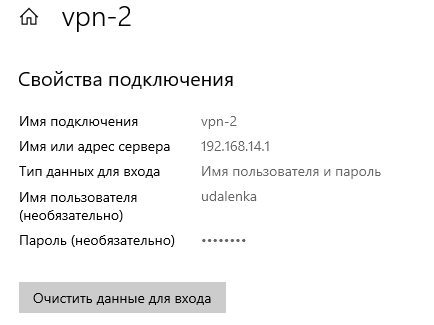


Рисунок 45 – Данные для подключения

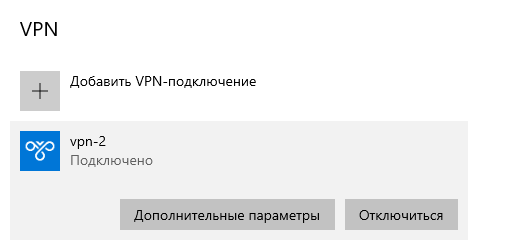


Рисунок 46 – Установленное VPN соединение

2.6 Настройка удаленного администрирования

Для автоматизации работы администраторов были созданы скрипты.

Выполнения скрипта для поиска неактивных пользователей показан на рисунке 47.

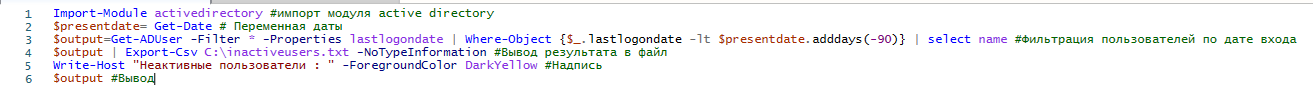


Рисунок 47 – Скрипт

Результат выполнения скрипта показан на рисунке 48.

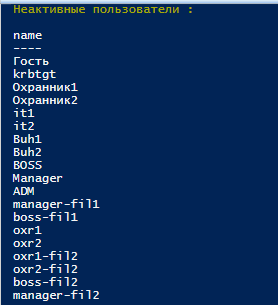


Рисунок 48 – Выполнение скрипта

Второй скрипт представлен в приложении Б.

Во втором разделе курсового проекта на сервер головного офиса и филиала 1 была установлена операционная система Windows server 2019, а на сервер филиала 2 установлен дистрибутив RedOS server, было настроено удаленное администрирование, настроены сетевые протоколы и службы   
серверов, организовано администрирование компьютерной сети и взаимодействия между серверами.

Заключение

В результате курсового проектирования проведено объединение локальных сетей веб-студии и удаленных филиалов веб-студии.

Цель курсового проекта администрирование компьютерной сети веб-студии.

Объект исследования: работоспособная сегментированная компьютерная сеть с корректно настроенными групповыми политиками, с совместными программным и аппаратным обеспечением, с программами фильтрации трафика и методами защиты персональных данный пользователей.

Предмет исследования: организация администрирования и методы обеспечения безопасности компьютерной сети.

Для достижения поставленной цели были выполнены следующие задачи:

1. Выполнен анализ предметной области.
2. Описаны исходные данные для анализа IT-инфраструктуры.
3. Описана логическая топология сети.
4. Описано взаимодействие серверов компьютерной сети.
5. Проанализирован и обоснован выбор программного обеспечения для серверов и хостов сети.
6. Описана организация удаленного администрирования.
7. Установлены операционные системы и дистрибутивов.
8. Установлены сетевые протоколы и службы.
9. Настроены сетевые службы.
10. Организовано администрирование компьютерной сети.
11. Организовано взаимодействие между головным офисом и филиалами.
12. Настроено удаленное администрирование.

Данный прототип сети можно использовать для практического применения в организации подобного типа.

Таким образом, в ходе проделанной работы цель была достигнута и все задачи выполнены.

Результатом курсового проекта является объединение сегментов корпоративной сети веб-студии и удаленных филиалов.

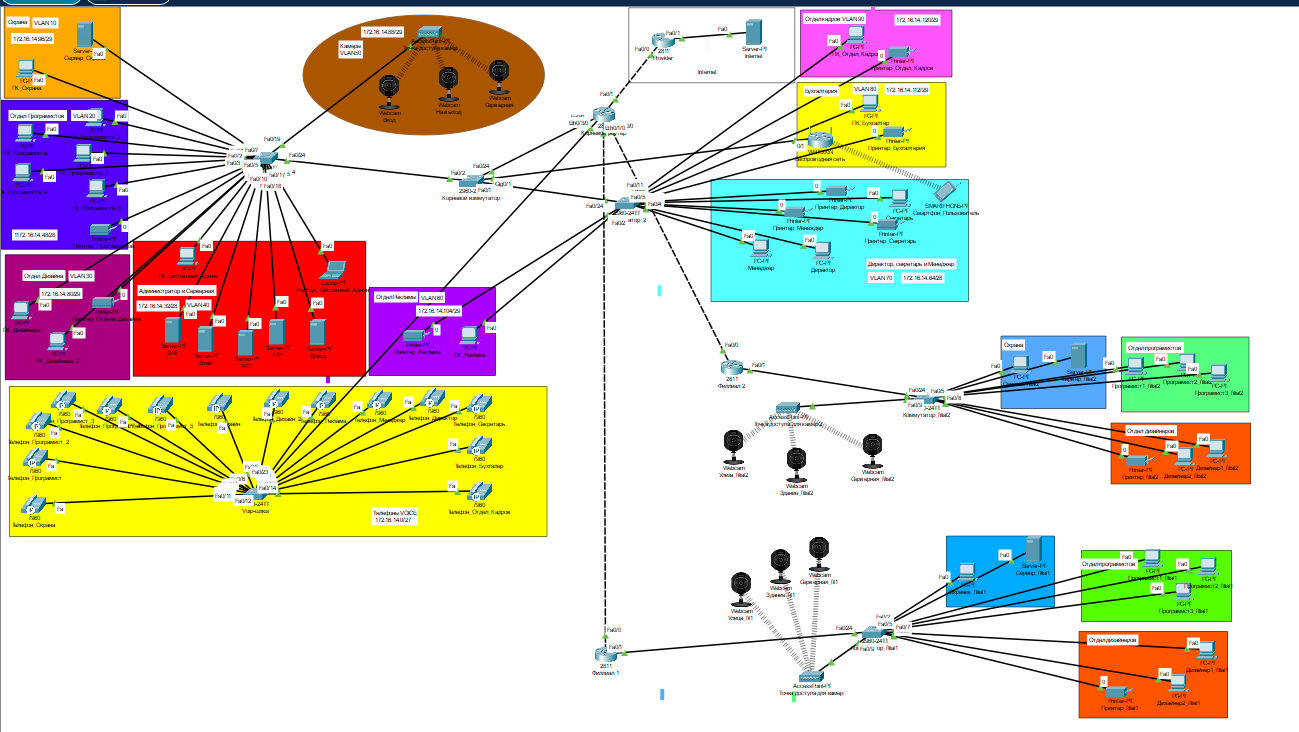
# Список используемых источников

1. ГОСТ 7.0.5-2008. Система стандартов по информации, библиотечному и издательскому делу. Библиографическое описание. Общие требования и правила составления. – Введ. 2008-04-28. – М.: ИПК Изд-во стандартов, 2008. – 22 с.
2. ГОСТ 2.105-95. Общие требования к текстовым документам. – Введ. 1996–01–07. –М. : Изд-во стандартов, 1996. – (Единая система конструкторской документации).
3. ГОСТ 7.1-2003. Библиографическая запись. Библиографическое описание. Общие требования и правила составления. – Введ. 2004-01-07. М. : Изд-во стандартов, 2004. (Система стандартов по информации, библиотечному и издательскому делу).
4. ГОСТ 7.80 – 2000. Библиографическая запись. Заголовок. Общие требования и правила составления. – Введ. 2000–01–07. – М. : Изд-во стандартов, 2000. – (Система стандартов по информации, библиотечному и издательскому делу).
5. ГОСТ 2.114-95. Единая система конструкторской документации. Технические условия. – Введ. 1995–04–26. – М. : Изд-во стандартов, 1995.
6. ГОСТ 19.201-78. Единая система программной документации. Техническое задание. Требования к содержанию и оформлению– Введ. 1980–01–01. – М. : Изд-во стандартов, 1980.
7. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы– Введ. 1900–01–01. – М. : Изд-во стандартов, 1990.
8. ГОСТ 7.70-96. Описание баз данных и машиночитаемых информационных массивов состав и обозначение характеристик. – Введ. 1997–01–07. – М. : Изд-во стандартов, 1997. ­ (Система стандартов по информации, библиотечному и издательскому делу).
9. Постановление Правительства РФ от 10 июля 2013 г. №582. [Электронный ресурс] - http://pravo.gov.ru/proxy/ips/?docbody=&nd=102166682
10. Распоряжения Правительства Российской Федерации от 25 апреля 2011 г. № 729-р г. Москва; [Электронный ресурс] – https://digital.gov.ru/ru/documents/3462/
11. Трудовой кодекс Российской Федерации [Электронный ресурс]   
    – http://tkodeksrf.ru/
12. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция) [Электронный ресурс] – http://www.consultant.ru/document/cons\_doc\_LAW\_61801/
13. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] – https://base.garant.ru/12148555
14. Федеральный закон от 27.07.2010г. №210-ФЗ «Об организации предоставления государственных и муниципальных услуг»; [Электронный ресурс] – https://www.zakonrf.info/doc-31965484/
15. Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»; [Электронный ресурс] – http://xn--273--84d1f.xn--p1ai/zakonodatelstvo/federalnyy-zakon-ot-29-dekabrya-2012-g-no-273-fz-ob-obrazovanii-v-rf
16. Архитектура ЭВМ и вычислительных систем: учебник / Н.В. Максимов, Т.Л. Партыка, И.И. Попов. – 5-е изд., перераб. и доп. – М. : ФОРУМ : ИНФРА-М, 2022. – 511 с. – доступ из ЭБС "Знаниум" <http://znanium.com/catalog/product/944312>
17. Баранчиков, А.И. Организация сетевого администрирования: учебник для студ. учрежд. СПО/ А.И. Баранчиков, П.А. Баранчиков, А.Ю. Громов. - М.: КУРС: ИНФРА-М, 2021. – 384 с.
18. Бродская, Ю. А. Денисов, Ю.А. Практика сетевого администрирования / Ю. А Бродская, Ю. А. Денисов / –SelfPub, 2018. – 87 с.
19. Исаченко, О.В. Программное обеспечение компьютерных сетей: учеб. пособие / О.В. Исаченко. – М. : ИНФРА-М, 2021. – 117 с. Режим доступа: http://znanium.com/catalog/product/989894
20. [Кенин,](http://avidreaders.ru/author/kenin-aleksandr-mihaylovich/) А. М., Д.Н. Колисниченко, Д.Н. Самоучитель системного администратора. / А. М. [Кенин,](http://avidreaders.ru/author/kenin-aleksandr-mihaylovich/) Д.Н. Колисниченко: Серия: Системный администратор. - БХВ-Петербург, 2021. – 528 с.
21. Компьютерные сети: Учебное пособие / Кузин А.В., Кузин Д.А. - 4-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2022. - 192 с. – доступ из ЭБС "Знаниум" <http://znanium.com/catalog/product/536468>
22. Костров, Б.В., Кистрин, А.В., Ефимов, А.И., Устюков; Д.И. Технологии физического уровня передачи данных. [Электронный ресурс]. – М.: Форум: НИЦ ИНФРА-М, 2022.- 240с.- доступ из ЭБС "Знаниум"
23. Куроуз, Джеймс, Росс, Кит Компьютерные сети: нисходящий подход. Джеймс Куроуз, Кит Росс. 6-е изд. – Москва : Издательство «Э», 2022 . – 912с.
24. Назаров, А.В. Эксплуатация объектов сетевой инфраструктуры / А.В. Назаров: Серия: Профессиональное образование. – М. : Академия, 2022. – 460 с.
25. Самоучитель системного администратора. / А. М. [Кенин,](http://avidreaders.ru/author/kenin-aleksandr-mihaylovich/) Д.Н. Колисниченко: Серия: Системный администратор. - БХВ-Петербург,   
    2022. – 528 с.

# Приложение А

(обязательное)

**Логическая схема объединённой сети**



# Приложение Б

(обязательное)

Скрипт

