**Содержание:**

[Введение 3](#_Toc178866305)

[1 Аналитическая часть 4](#_Toc178866306)

[1.1 Постановка задачи эксплуатации сети 4](#_Toc178866307)

[1.2 Модельное представление объекта администрирования. 5](#_Toc178866308)

[1.3 Построение структуры домена. 7](#_Toc178866309)

[1.4 Обзор базовых средств безопасности сети. 9](#_Toc178866310)

[1.5 Обзор базовых средств обеспечения отказоустойчивой работы сети. 13](#_Toc178866311)

[1.6 Обзор средств мониторинга сети. 17](#_Toc178866312)

[2 Технологическая часть 21](#_Toc178866313)

[2.1 Описание решения организации сетевой связанности 21](#_Toc178866314)

[2.2 Описание решения организации безопасности компьютерной сети 23](#_Toc178866315)

[2.3 Описание решения обеспечения инфраструктурной функциональности 26](#_Toc178866316)

[2.4 Описание решения обеспечения отказоустойчивого функционирования служб 28](#_Toc178866317)

[2.5 Анализ результатов тестирования сети. 31](#_Toc178866318)

[3 Экономическая часть 34](#_Toc178866319)

[3.1 Расчет стоимости лицензионного программного обеспечения сетевой инфраструктуры 34](#_Toc178866320)

[Заключение 36](#_Toc178866321)

[Литература 37](#_Toc178866322)

**Введение**

Проектирование компьютерных сетей (КС) является одним из ключевых этапов в создании эффективной и надежной информационной инфраструктуры. В условиях стремительного развития технологий и увеличения объемов передаваемой информации правильное проектирование сети становится критически важным для обеспечения стабильной работы организаций, повышения их конкурентоспособности и безопасности данных. Компьютерные сети служат основой для обмена информацией, доступа к ресурсам и взаимодействия между пользователями, что делает их неотъемлемой частью современного бизнеса и повседневной жизни.

Актуальность данного курсового проекта обусловлена растущей зависимостью организаций от информационных технологий и необходимостью обеспечения надежной и безопасной сетевой инфраструктуры. С увеличением числа пользователей и устройств, а также с развитием новых технологий, таких как облачные вычисления и Интернет вещей, проектирование компьютерных сетей становится не только важным, но и сложным процессом. Эффективные сети способны значительно повысить производительность и безопасность бизнеса, что делает изучение и реализацию современных подходов к проектированию КС особенно актуальными.

Роль компьютерных сетей в современном мире:

* Обеспечение связи между миллиардами устройств.
* Поддержка работы облачных сервисов, интернет-приложений и систем автоматизации.
* Ключевая роль в функционировании таких секторов, как финансы, здравоохранение, образование и промышленность.
* Основа для инноваций и развития новых технологий, таких как Интернет вещей (IoT), искусственный интеллект и большие данные.

Жизненный цикл компьютерной сети:

1. Первоначальное проектирование.
2. Выбор оборудования.
3. Внедрение.
4. Эксплуатация.
5. Последующее обновление.

Каждый из этих этапов требует тщательного планирования и анализа, чтобы обеспечить соответствие сети требованиям пользователей и бизнес-процессов.

В рамках данного курсового проекта акцент будет сделан на проектировании компьютерной сети, исследуя ключевые аспекты, такие как выбор архитектуры, конфигурация сетевых устройств, обеспечение безопасности и управление сетью. Ожидается, что результаты работы помогут не только в решении практических задач, но и углубят понимание важности проектирования компьютерных сетей в современном мире.

**1 Аналитическая часть**

**1.1 Постановка задачи эксплуатации сети**

Компания «Зевс» создает корпоративную компьютерную сеть на первом и втором этажах здания. На схеме (см. приложение) руководство компании отметило предполагаемые места размещения коммутационного оборудования.

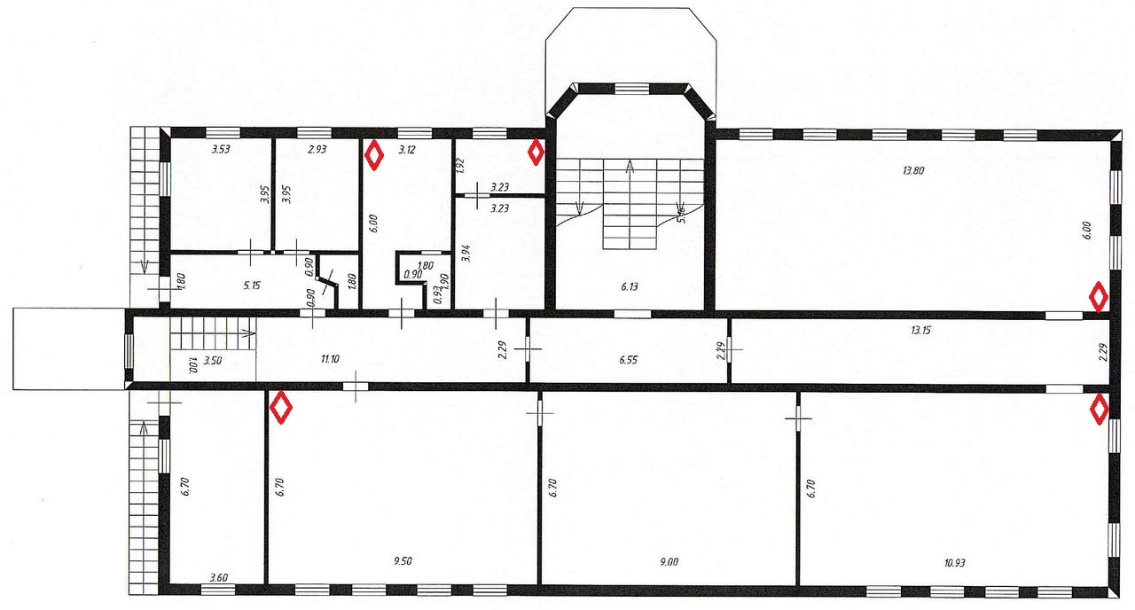


Рисунок 1 – Схема расположения точек

Проектируемая сеть предназначена для обеспечения гостевого доступа к сети Интернет в здании и доступа сотрудников к корпоративным информационным ресурсам. Необходимо выполнить проектирование наиболее экономичной проводной структурированной кабельной системы здания, выбрать (из предложенных на схеме) место размещения центрального коммутационного узла (MDF).

Поддержка компьютерной сети будет осуществляться специалистами компании «Зевс». В центральном коммутационном узле предполагается установка стойки с сетевым оборудованием и сервера. Пропускная способность сети не должны быть менее 150 Mb/c. Проектирование размещения оборудования в стойке и выбор технологий функционирования компьютерной сети заказчик оставляет за исполнителем.

Целью данного курсового проекта является Проектирование корпоративной компьютерной сети компании «Зевс» с обеспечением гостевого доступа в Интернет и доступа сотрудников к корпоративным ресурсам, учитывая требования к пропускной способности (не менее 150 Мбит/с), экономичности и удобству обслуживания.

Для достижения этой цели нужно сделать следующие задачи:

1. Анализ требований:
2. Проектирование структурированной кабельной системы (СКС)
3. Выбор сетевого оборудования
4. Размещение оборудования в серверной стойке
5. Обеспечение безопасности и управления сетью
6. Экономическое обоснование

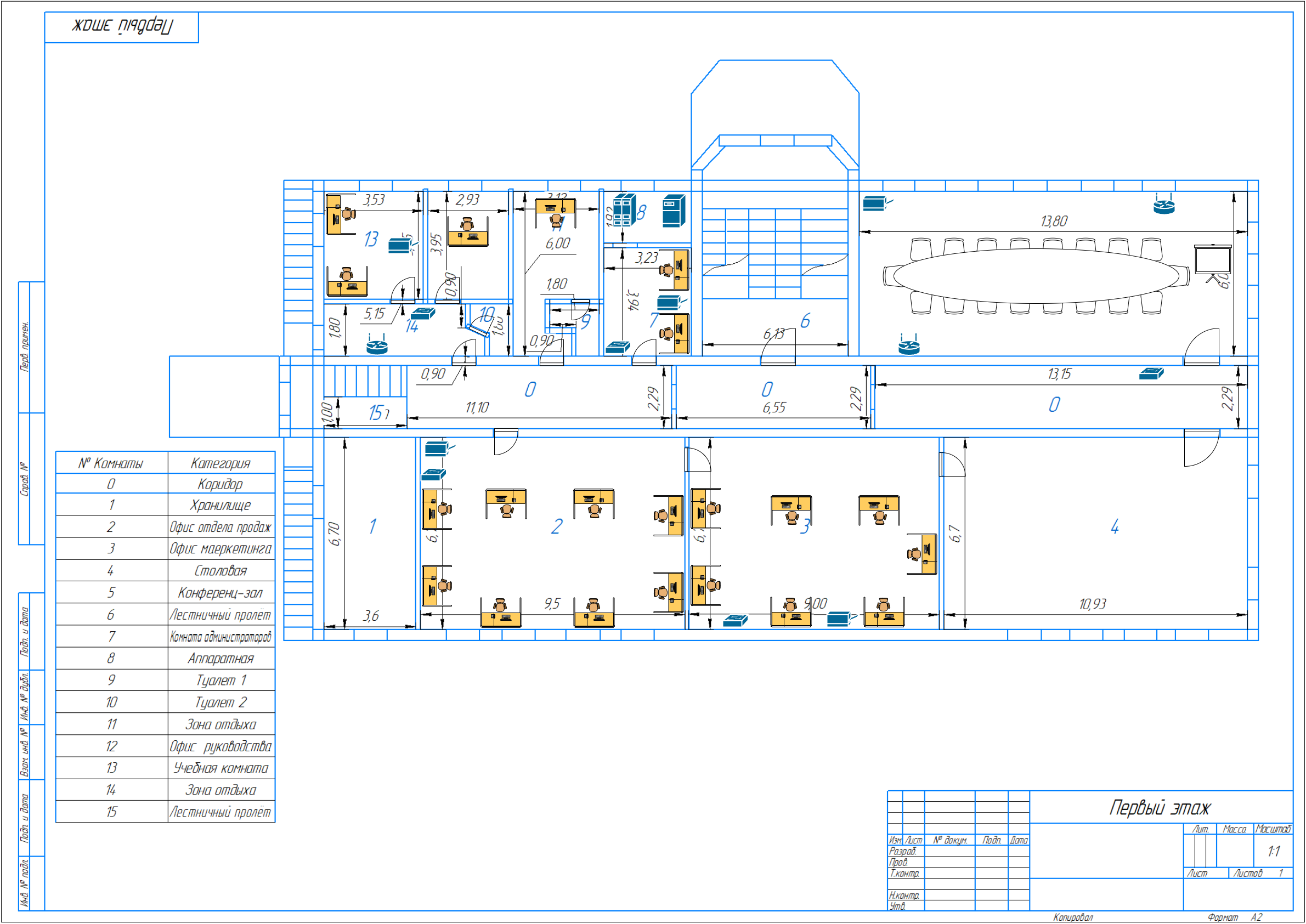


Рисунок 2 – Расположение рабочих мест на 1-ом этаже

Количество рабочих мест на 1 этаже – 22.

На рисунке 3 видны как будут расположены рабочие места на 2-ом этаже.

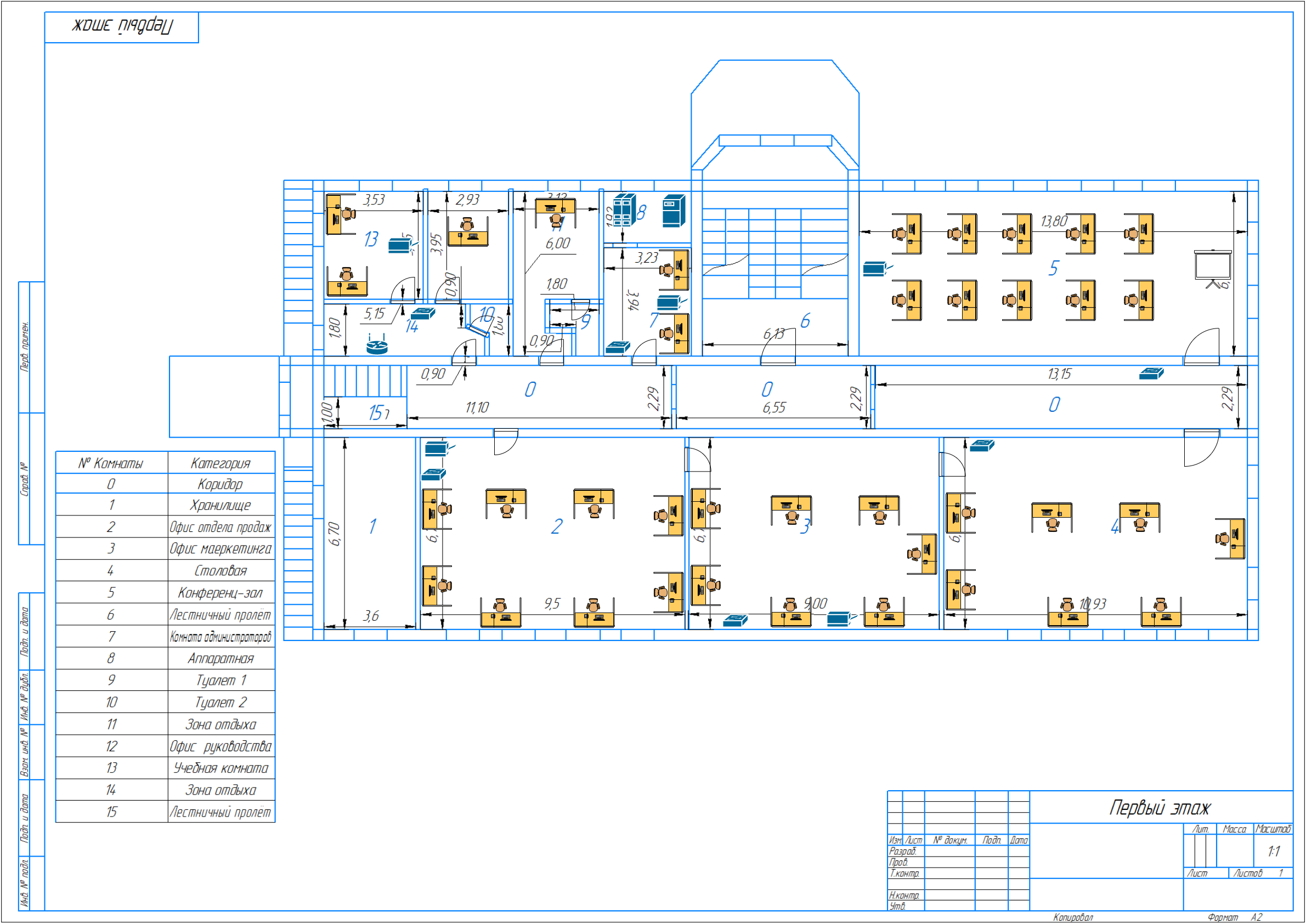


Рисунок 3 – Расположение рабочих мест на 2-ом этаже

На втором этаже находится больше рабочих мест. Отсутствует столовая и имеется конференц-зал с рабочими местами.

Количество рабочих мест на 2 этаже – 40.

Общее количество рабочих мест на 1 и 2 этаже – 62.

Основные комнаты делятся на следующие категории:

* Офис отдела продаж
* Комната администратора
* Аппаратная
* Офис руководства
* Офис маркетинга
* Конференц-зал
* Зона отдыха
* Учебная комната

## 1.2 Формализация задачи синтеза сети (этапы работы)

**1. Анализ требований и исходных данных**

Проводится детальная оценка потребностей проводной и беспроводной инфраструктуры. Для беспроводной сети анализируются: зоны покрытия на обоих этажах, предполагаемое количество одновременных подключений (сотрудники + гости), требования к скорости передачи данных (минимум 150 Мбит/с), необходимость роуминга между точками доступа. Особое внимание уделяется помещениям с повышенной нагрузкой (конференц-зал, зоны отдыха).

**2. Проектирование комбинированной сетевой инфраструктуры**

Разрабатывается единая концепция, объединяющая проводную и беспроводную составляющие:

* Для проводной части: выбирается расположение MDF и IDF, рассчитываются кабельные трассы с учетом размещения точек доступа
* Для беспроводной части: выполняется радиочастотное планирование с определением оптимальных мест установки точек доступа (учитывается толщина стен, возможные помехи, требуемая зона покрытия)

**3. Выбор оборудования для гибридной сети**

Подбирается оборудование, поддерживающее обе технологии:

* Точки доступа стандарта Wi-Fi 6 (802.11ax) с поддержкой одновременной работы на 2.4 и 5 ГГц
* Коммутаторы с PoE+ для питания точек доступа
* Контроллер беспроводной сети для централизованного управления
* Маршрутизатор с возможностью разделения трафика и QoS

**4. Размещение и интеграция оборудования**

Разрабатывается схема размещения:

* Точки доступа равномерно распределяются по этажам с перекрытием зон покрытия
* Оборудование в стойке дополняется контроллером WLC
* Обеспечивается резервирование питания для критичных компонентов

**5. Обеспечение безопасности и управления**

Реализуется комплексная система защиты:

* Раздельные VLAN для проводных и беспроводных клиентов
* Разные политики доступа для сотрудников и гостей
* WPA3-Enterprise для аутентификации сотрудников
* Гостевая изолированная сеть с ограниченным доступом
* Единая система мониторинга для всех сегментов сети

**1.3 Модельное представление объекта синтеза (построение теоретико-графовой модели)**

В результате анализа схемы здания было выявлено 10 мест установки коммутационного оборудования и определены расстояния между ними. По этим данным был построен граф (см. рис. 3).

Таблица 1 – Расстояние между вершинами (рассчитано в метрах (м))

Таблица 2 – Расстояние между вершинами (рассчитано в метрах (м)))

## 1.4 Обзор базовых средств безопасности сети.

В данной работе будет проведен обзор и сравнение двух методов, из которых будет выбран один. Первый метод – это синтез абонентской сети доступа, а второй метод – метрические характеристика графа.

Абонентская сеть доступа нужна для того, чтобы обеспечить абонентам доступ к основной сети. Эта сеть может быть реализована с использованием минимальных затрат.

Решение задачи данным способом должно быть максимально точным и не требовать больших затрат времени. Сеть минимальной стоимости представляет собой покрывающее дерево.

*Дерево* — граф, не содержащий циклов.

*Покрывающее дерево* — дерево, в которое включены все вершины.

Для нахождения покрывающего дерева используется алгоритм Прима.

Алгоритм Прима — это алгоритм построения минимального остовного дерева для заданной взвешенной неориентированной связного графа. Идея алгоритма заключается в том, что на каждом шаге мы выбираем вершину с минимальным весом среди всех не посещённых вершин и добавляем ее в островное дерево. Затем мы удаляем эту вершину и все инцидентные ей ребра из графа и повторяем процесс до тех пор, пока все вершины не станут посещенными.

Алгоритм Прима обладает рядом преимуществ, среди которых возможность использования для работы с неполно связными графами и высокая точность получаемого результата.

Для определения оптимального местоположения оборудования необходимо найти медиану графа.

*Медиана графа* – такая вершина x, суммарное расстояние от которой до всех остальных вершин графа минимально. Суммарное расстояние от вершины до всех остальных вершин – СВВ(i) определяется соотношением СВВ(i)= Σdi,j  – суммарное расстояние от вершины i до всех j.

*Центр графа* — это вершина, расстояние от которой до самого отдаленного пункта минимально.

Задачи поиска центральных узлов графа - с использованием метрических характеристик графа - регулярно возникают в практической деятельности.

Например, граф может представлять собой сеть дорог, где вершины соответствуют отдельным населённым пунктам, а рёбра - дорогам между ними. Необходимо оптимально разместить больницы, магазины и пункты обслуживания. Во многих подобных ситуациях критерием оптимальности является минимизация расстояния от объекта обслуживания до наиболее удалённой точки. Таким образом, в качестве мест размещения выбираются центральные узлы графа.

Эти два метода различаются алгоритмами поиска центра графа и решениями для определения наиболее подходящего места для размещения серверного оборудования.

Проанализировав два метода было решено, что в данной работе лучше всего использовать поиск центра графа, так как сеть является беспроводной.

Вершина графа называется медианой, если суммарное расстояние от нее до всех остальных вершин самое минимальное.

Нахождение медианы графа:

* Найти все вершины графа и их степени;
* Найти вершину с минимальной степенью. Это и будет медиана графа;
* Если медиана не одна, то выбрать любую из них.

## 1.5 Аналитическое решение задачи оптимизации сети выбранным методом

Метод – Синтез абонентской сети доступа.

Расчеты нахождения центра графа (См. табл. 3).



Таблица 3 – Центры графа

Из всех максимальных значений нам нужно найти минимальное. Его значение равно 225.4. Оно находится в строке 9. Исходя из этого, мы можем представить вершины как центр графа. Этот центр обеспечивает минимальное расстояние до других вершин. Но по рекомендациям аппаратную нежелательно ставить на 2 этаже, поэтому аппаратная будет располагаться в точке под номером 3 ее значение равно 225.6. Значения различаются всего на 0.2 метра, поэтому это не существенно.

Для размещения аппаратной лучше всего подходит точка 3, так как:

* Точка находится на первом этаже здания (ГОСТ Р 59315);
* Минимальное количество окон (ГОСТ Р 59315);
* Площадь комнаты более 16 м² (ГОСТ Р 59315).

## 1.5 Обзор базовых средств обеспечения отказоустойчивой работы сети.

При проектировании и администрировании сети для центрального офиса (HQ) и филиалов (BR) важно внедрить механизмы отказоустойчивости, обеспечивающие непрерывную работу сети даже при сбоях или отказах отдельных компонентов. Основные методы включают дублирование ресурсов, настройку резервирования, репликацию данных и мониторинг работы сети.

1. Резервирование маршрутизаторов и коммутационного оборудования

* Резервные маршрутизаторы в каждом офисе для автоматического переключения в случае сбоя основного маршрутизатора.
* Использование протоколов динамической маршрутизации (OSPF или BGP) для автоматического поиска альтернативных маршрутов.
* Протоколы динамической маршрутизации: Использование протоколов динамической маршрутизации, таких как OSPF или BGP, позволит сети автоматически находить альтернативные маршруты для передачи данных в случае отказа какого-либо из каналов связи. Эти протоколы позволяют динамически адаптироваться к изменениям в топологии сети.

2. Виртуальные частные сети (VPN) с резервированием

* Резервирование VPN: Для обеспечения отказоустойчивости при взаимодействии между филиалом и центральным офисом через VPN можно настроить несколько VPN-туннелей через разные провайдеры (например, с использованием IPoE и LTE). В случае сбоя основного канала, трафик будет перенаправлен через резервный VPN-туннель, что обеспечит непрерывность связи.
* Использование VPN-туннелей с IPSec гарантирует безопасную передачу данных между офисами и обеспечивает шифрование трафика.

3. Репликация данных и контроллеры домена

* Репликация контроллеров домена: Серверы HQ-SRV и BR-SRV настроены как контроллеры домена с функцией репликации данных между ними. Это обеспечивает отказоустойчивость: в случае сбоя одного из контроллеров, второй продолжает выполнять функции аутентификации пользователей и управления доступом к ресурсам.
* Репликация данных: Критически важные данные (учетные записи пользователей, права доступа, конфигурации серверов) должны регулярно реплицироваться между серверами в офисе и филиале. Это позволяет сохранить актуальные данные и обеспечить бесперебойную работу сети даже при временной недоступности одного из серверов.

4. Резервное копирование и восстановление данных

* Системы резервного копирования: Для защиты от потери данных при сбоях используется резервное копирование. На серверах HQ-SRV и BR-SRV должна быть настроена автоматическая система бэкапа, которая регулярно сохраняет копии критически важных данных.
* Резервные копии должны храниться как локально (например, на другом сервере или устройстве), так и удаленно (например, в облачном хранилище или на другом физическом сервере в другом офисе). Это позволит восстановить данные в случае катастрофы или сбоя оборудования.
* Важно использовать дифференциальное и инкрементное резервное копирование для экономии дискового пространства и ускорения восстановления данных.

5. Отказоустойчивые сетевые соединения

* Дублирование каналов связи: Для обеспечения отказоустойчивости внешних каналов связи с интернетом и между офисами рекомендуется использовать два или более независимых канала связи. Один из каналов будет основным, а второй — резервным. В случае сбоя основного канала трафик автоматически переключится на резервный.
* Технология Link Aggregation: Для повышения пропускной способности и отказоустойчивости между серверами и коммутаторами можно использовать технологию Link Aggregation (агрегация каналов), которая объединяет несколько физических каналов в один логический. В случае выхода из строя одного из физических каналов, трафик продолжит проходить по оставшимся.

6. Мониторинг и оповещение

* Система мониторинга: Настроенная система мониторинга, такая как Zabbix, позволяет отслеживать состояние всех устройств и сервисов сети (маршрутизаторов, серверов, рабочих станций) в реальном времени. В случае возникновения сбоя администратор немедленно получит оповещение.
* Проактивный мониторинг: Система мониторинга также позволяет предсказать потенциальные проблемы, такие как перегрузка сетевых каналов или исчерпание ресурсов серверов. Это позволяет принимать меры до того, как сбой станет критическим.
* Оповещения: Настройка оповещений по электронной почте или через мессенджеры помогает администраторам сети быстро реагировать на инциденты и устранять неисправности до того, как они затронут работу сети.

7. Отказоустойчивость виртуализированных серверов

* Виртуализация: Использование виртуальных машин для серверов (HQ-SRV, BR-SRV) позволяет легко мигрировать виртуальные машины с одного физического сервера на другой в случае отказа оборудования. При этом виртуальные машины могут быть запущены на резервном хосте с минимальными перерывами в работе.
* Виртуализация также поддерживает технологию High Availability (HA), которая автоматически перезапускает виртуальные машины на другом доступном сервере в случае сбоя.

8. Кластеризация

* Кластеры серверов: Для повышения отказоустойчивости критически важных сервисов можно использовать кластеризацию серверов. Это объединение нескольких серверов в один кластер, который может распределять нагрузку между узлами. В случае выхода из строя одного из серверов, остальные серверы кластера продолжат обработку запросов.
* Кластеризация может быть использована для баз данных, файловых серверов и других сервисов, требующих высокой доступности.

9. Механизмы автопереключения (Failover)

* Автопереключение (Failover) позволяет автоматически переключать сервисы на резервное оборудование или каналы связи в случае выхода из строя основного ресурса. Это критически важно для поддержания непрерывной работы сети.
* Например, при отказе одного из серверов автопереключение может перенаправить все запросы на другой сервер, который возьмет на себя обработку трафика.

10. Разделение сетевой нагрузки (Load Balancing)

* Балансировка нагрузки (Load Balancing) помогает распределять сетевой трафик и запросы между несколькими серверами или каналами связи. Это позволяет избежать перегрузки одного из компонентов сети и поддерживать высокую производительность.
* Например, балансировщики нагрузки могут распределять запросы на доступ к интернету или внутрирегиональные сервисы между несколькими маршрутизаторами или серверами.

11. Физическая отказоустойчивость

* Дублирование физических ресурсов: Важно предусмотреть дублирование ключевого оборудования — серверов, маршрутизаторов, коммутаторов, а также источников бесперебойного питания (ИБП). Это позволит сети оставаться работоспособной при сбоях отдельных физических устройств.
* В случае выхода из строя серверного оборудования, физически разделенные серверные комнаты или использование удаленных дата-центров обеспечат бесперебойную работу.

12. Использование источников бесперебойного питания (UPS)

* Источники бесперебойного питания (UPS) обеспечивают временное питание оборудования в случае отключения электричества. Это позволяет избежать внезапных отключений серверов и сетевого оборудования, которые могут привести к потере данных или нарушению работы сети.
* UPS также могут быть настроены на автоматическое отключение серверов в случае продолжительных перебоев в подаче электричества, что минимизирует риск повреждения данных.

Эти базовые средства отказоустойчивости обеспечивают непрерывную работу сети при сбоях, минимизируя время простоя и снижая риск потери данных.

## 1.6 Обзор средств мониторинга сети.

Мониторинг сети является важной составляющей инфраструктуры, позволяющей своевременно обнаруживать проблемы, отслеживать производительность и обеспечивать безопасность. Мониторинг помогает поддерживать стабильную и отказоустойчивую работу всех компонентов сети.

1. Zabbix

Zabbix — Мощная система мониторинга с открытым исходным кодом для отслеживания состояния оборудования, виртуальных машин, приложений и сетевых соединений.

* Мониторинг серверов и маршрутизаторов: Zabbix может следить за производительностью серверов (HQ-SRV, BR-SRV), маршрутизаторов (HQ-RTR, BR-RTR) и виртуальных машин, собирая данные о загрузке процессора, памяти, дискового пространства, трафика и состояния сетевых интерфейсов.
* Оповещения: В случае обнаружения проблем, таких как перегрузка системы, Zabbix может отправлять уведомления администратору через e-mail или мессенджеры. Это позволяет быстро реагировать на инциденты и предотвращать их развитие в критические ситуации.
* Проактивный мониторинг: Zabbix поддерживает функции предиктивного анализа, что позволяет прогнозировать возможные проблемы, такие как износ оборудования или увеличение нагрузки на систему, и принимать меры до их возникновения.

2. Nagios

Nagios — это еще одно популярное средство мониторинга, которое обеспечивает контроль за серверами, сетевыми устройствами, приложениями и услугами. Внедрение Nagios в сети организации позволяет:

* Мониторинг доступности и времени отклика устройств: Nagios может отслеживать доступность сетевых узлов (маршрутизаторов, серверов и т.д.) и проверять задержки в ответе (ping, HTTP, DNS), что помогает контролировать производительность сети.
* Интеграция с другими инструментами: Nagios легко интегрируется с другими системами, такими как Cacti и Grafana, для более детализированного визуального анализа данных.
* Оповещение об инцидентах: Как и Zabbix, Nagios поддерживает оповещения по различным каналам, обеспечивая быструю реакцию на сбои в работе сети.

3. Prometheus и Grafana

Prometheus — это система мониторинга с временными рядами данных и гибкой системой опроса метрик, которая идеально подходит для сбора и анализа данных с серверов и приложений. В паре с Grafana, инструментом для визуализации данных, Prometheus позволяет:

* Гибкий сбор данных: Prometheus может собирать метрики о состоянии серверов, сетевого оборудования и виртуальных машин, обеспечивая глубокий анализ их производительности.
* Создание дашбордов в Grafana: С помощью Grafana можно визуализировать данные Prometheus на дашбордах, отображая ключевые показатели производительности, такие как трафик, задержки, загрузка ресурсов серверов и состояние сетевых соединений.
* Автоматическая реакция на события: Prometheus поддерживает алертинг (оповещение) при возникновении отклонений от заданных параметров, что помогает в быстром реагировании на инциденты.

4. Cacti

Cacti — это инструмент для мониторинга и графического представления сетевых данных с помощью SNMP. Он может быть полезен для:

* Сбор данных через SNMP: Cacti идеально подходит для мониторинга устройств, которые поддерживают протокол SNMP (например, маршрутизаторы, коммутаторы). Он собирает данные о состоянии устройств и отображает их в виде графиков.
* Отслеживание трафика: Cacti может контролировать пропускную способность сети, что позволяет анализировать сетевой трафик и обнаруживать узкие места или перегрузки.
* Интеграция с другими инструментами: Cacti может быть использован в связке с Nagios или Zabbix для более полного мониторинга сети.

5. Netflow и sFlow

NetFlow (разработан Cisco) и sFlow — это протоколы для мониторинга сетевого трафика, которые предоставляют информацию о потоках данных, проходящих через маршрутизаторы и коммутаторы. Эти технологии позволяют:

* Анализ трафика: NetFlow и sFlow собирают детальную информацию о трафике, включая источники и назначения пакетов, типы протоколов, используемые приложения. Это помогает выявлять потенциальные угрозы, перегрузки сети или неэффективное использование ресурсов.
* Безопасность: С помощью NetFlow и sFlow можно обнаруживать аномалии в трафике, которые могут указывать на сетевые атаки или нарушение политики безопасности.

6. Wireshark

Wireshark — это программа для анализа сетевого трафика, которая позволяет детально изучать передаваемые данные на уровне пакетов. В корпоративной сети Wireshark можно использовать для:

* Диагностика проблем: Wireshark позволяет детализированно анализировать сетевые пакеты и выявлять проблемы на уровне протоколов, такие как неправильная маршрутизация, потеря пакетов или проблемы с подключениями.
* Обеспечение безопасности: Этот инструмент помогает отслеживать подозрительный трафик, выявлять потенциальные атаки или нарушения политики безопасности.
* Оптимизация сети: С помощью Wireshark можно обнаружить узкие места в сети, оптимизировать маршруты передачи данных и настроить балансировку нагрузки.

## 2 Технологическая часть

## 2.1 Описание решения организации сетевой связанности

1 Трехуровневая модель сети отличается от двухуровневой тем, что она имеет больше уровней и, следовательно, больше возможностей для управления и контроля над сетью. В трехуровневой модели есть уровень ядра, распределения и доступа, а в двухуровневой архитектуре уровень ядра и распределения объединяются в один уровень. Трехуровневая модель лучше подходит для сложных сетей, где требуется больше контроля и управления, а двухуровневая модель - для более простых сетей.

Для проектирования сети была использована трехуровневая модель сети, но с урезанным ядром, так как школа не имеет большое количество устройств и не нуждается в сложном контроле и управлении.

Трехуровневая модель сети представляет собой архитектуру сети, которая разделяет сетевые устройства на три уровня:

* Ядро сети (Core layer);
* Уровень распределения (Distribution layer);
* Уровень доступа (Access layer).

Каждый уровень обеспечивает выполнение определенных задач, но эти уровни являются абстрактными и не обязательно связаны с конкретными аппаратными средствами.

*Ядро сети* — комплекс сетевых устройств (маршрутизаторов и коммутаторов), обеспечивающих высокоскоростную передачу данных и резервирование каналов между сегментами уровня распределения. Функции уровня ядра включают:

* надёжную и быструю передачу больших объёмов данных;
* обработку пользовательских данных на уровне распределения;
* обеспечение отказоустойчивости;
* маршрутизацию, качество обслуживания и безопасность сети;
* агрегирование каналов;
* переход от одной технологии к другой.

*Уровень распределения* – первый уровень рабочей группы, который иногда называют уровнем рабочих групп. В зависимости от способа реализации уровень распределения может выполнять следующие функции:

* Обеспечение маршрутизации, качества обслуживания и безопасности сети;
* Агрегирование каналов;
* Переход от одной технологии к другой;
* Контроль доступа и фильтрация, например, ACL;
* Маршрутизация между локальными сетями и VLAN, а также между доменами маршрутизации;
* Избыточность и балансировка нагрузки;

*Уровень доступа* – второй уровень, Уровень доступа управляет доступом пользователей и рабочих групп к ресурсам объединенной сети. Основной задачей уровня доступа является создание точек входа/выхода пользователей в сеть. Уровень выполняет следующие функции:

* Управление доступом пользователей, фильтрация трафика, обеспечение качества обслуживания (QoS);
* Сегментация;
* Подключение рабочих групп к уровню распределения;
* Использование технологии коммутируемых локальных сетей.

### 2.2 Обоснование и описание выбора оборудования

Eltex - это российский производитель телекоммуникационного оборудования, который предлагает широкий спектр продуктов, включая маршрутизаторы, коммутаторы, Wi-Fi-оборудование, IP-телефоны, системы видеонаблюдения и другие устройства. Продукцию данной компании используют как в малых, так и в больших сетях. Если сравнивать Eltex с такими мировыми производителями, как Cisco и D-Link, то они практически ничем не отличаются. Поэтому, используя оборудование компании Eltex, сеть будет такой же по производительной, как если бы было использовано оборудование других компаний.

Для решения поставленной задачи было выбрано следующее оборудование:

Сервер Cisco MCS-7825-I5-IPC1 (См. рис. 4).



Рисунок 4 - Сервер Cisco MCS-7825-I5-IPC1

Характеристики:

* Модель MCS-7825-I5-IPC1 – это недорогой сервер от компании Cisco. Обладает высоким качеством и производительностью, подходящий для работы баз данных, виртуализации и идеален для работы с приложениями, которым необходима большая вычислительная мощность процессора.
* К данному серверу прилагается хороший пакет программного обеспечения для развертывания сервера и последующим администрированием.
* Сервер Cisco MCS-7825-I5-IPC1 работает на процессоре Intel X3430.
* Сервер Cisco MCS-7825-I5-IPC1 имеет 9 портов: 1 x RJ-45 1GbE WAN port, 1 x Combo RJ-45 Gigabit LAN/WAN port, 4 x RJ-45 Gigabit LAN ports, 2 x USB 3.0 ports, 1 x VGA port, 1 x Serial port.
* Безопасность: сервер оснащен встроенным брандмауэром и антивирусной защитой, что обеспечивает защиту от вредоносных программ и атак из интернета.
* Поддержка до 8 жестких дисков: сервер может быть оснащен до 8 жесткими дисками SATA, что позволяет хранить большое количество данных.
* Цена составляет 215 730 руб.

Коммутатор доступа MES2428B (См. рис. 5)



Рисунок 5 - Коммутатор доступа MES2428B

Характеристики:

* Коммутатор доступа MES2428B оснащен 24 портами 10/100/1000BASE-T (RJ-45), 4 портами Combo 10/100/1000Base-T/100Base-FX/1000Base-X и 1 консольный порт RS-232 (RJ-45). Размер таблицы коммутации составляет 8192 MAC-адресов.
* Коммутатор доступа MES2428B поддерживает до 24 точек доступа 802.11n и до 16 точек доступа 802.11ac.
* Коммутатор доступа MES2428B поддерживает до 24 точек доступа 802.11n и до 16 точек доступа 802.11ac, а также обеспечивает ряд функций для обеспечения безопасности сети:
* Поддержка 802.1X для аутентификации пользователей и управления доступом DHCP Snooping для защиты от атак DHCP Starvation ARP Inspection для предотвращения ARP Spoofing атак Встроенная защита от DoS и DDoS атак. Поддержка ACL для контроля доступа к сети.
* Коммутатор имеет возможность подключения аккумуляторной батареи для обеспечения гарантированного питания в случае пропадания первичной сети 220В. Коммутатор доступа MES2428B оснащен блоком питания, который позволяет заряжать АКБ при наличии питания 220В. Система резервного питания позволяет следить за состоянием первичной сети и извещать о переходе с одного типа питания на другой.
* Цена составляет 47 262 руб.

ИБП (Источник бесперебойного питания) CyberPower OR600ELCDRM1U (См. рис. 6)



Рисунок 6 – ИБП (Источник бесперебойного питания) CyberPower OR600ELCDRM1U

Характеристики:

* Сигналы неисправности Звуковая сигнализация ИБП CyberPower OR600ELCDRM1U может включать одиночный короткий сигнал при включении, нечастый прерывистый писк при отключении электричества или выходе сетевого напряжения за допустимый диапазон работы ИБП, а также непрерывный сигнал при перегрузке, неисправности или отсутствии подключённой нагрузки.
* Мощность: 600 ВА
* Рабочая температура: от 0 до 40 градусов Цельсия.
* Цена составляет 15 740 руб.

Беспроводная точка доступа WEP-30L (Z) (См. рис. 7)



Рисунок 7 – Беспроводная точка доступа WEP-30L (Z)

Характеристики:

* Беспроводная однодиапозонная точка доступа DAP-2230 с поддержкой технологии PoE, разработанная для использования в сетях предприятий малого и среднего бизнеса, позволяет сетевым администраторам воспользоваться возможностями управляемой и защищенной беспроводной сети.
* Входной интерфейс 10/100BASE-TX
* Скорость 802.11n, 2.4 ГГц 300 Мбит/с
* Технология MU-MIMO: позволяет точке доступа одновременно передавать данные на несколько устройств, уменьшая время ожидания и увеличивая общую производительность сети.
* Гостевая сеть: позволяет создать отдельную беспроводную сеть для гостей с ограниченным доступом к основной сети для повышения безопасности.
* Поддержка WPA/WPA2 шифрования: обеспечивает защиту сети от несанкционированного доступа и сетевых атак.
* Цена составляет 5000 руб.

Сервисный маршрутизатор Eltex ESR-15 (См. рис. 8)



Рисунок 8 Сервисный маршрутизатор Eltex ESR-15

Характеристики:

* Интерфейсы: У маршрутизатора есть такие интерфейсы, как: 10/100/1000BASE-T – 4, 1000BASE-X SFP – 2, Console RS-232 (RJ-45) – 1, USB 2.0 – 2.
* Производительность: Сервисный маршрутизатор ESR-15 поддерживает до 10 VPN-туннелей и до 4000 активных VLAN согласно стандарту 802.1Q, обеспечивая высокую масштабируемость и гибкость в настройке. Маршрутизатор способен обрабатывать до 1 миллиона BGP маршрутов и до 30000 OSPF маршрутов, что позволяет использовать его в крупных сетях с множеством узлов и сложной топологией. Благодаря поддержке 2000 MAC адресов на каждый bridge и размеру базы FIB в 800000 адресов, ESR-15 обеспечивает быстрое и эффективное управление трафиком в сети.
* Функции сетевой защиты: Сервисный маршрутизатор ESR-15 оснащен широким спектром характеристик, включая поддержку большого количества VPN-туннелей, конкурентных сессий, VLAN и BGP-соседей. Он также обеспечивает высокую производительность благодаря большим таблицам MAC-адресов, большим базам FIB и возможности поддержки большого количества маршрутов различных протоколов.
* Цена 66 158 руб.

Сетевой фильтр DEXP Intensity 418BU (См. рис. 9)



Рисунок 9 – Сетевой фильтр DEXP Intensity 418BU

Характеристики:

* Количество выходных розеток – 4 шт.
* Максимальная мощность подключенной нагрузки - 3680 Вт
* USB разъемы – 3 шт.
* Максимальный ток нагрузки – 16 А
* Максимальный ток нагрузки – 2.4 А
* Длина кабеля – 1.8 м
* Рабочая частота 50 Гц
* Цена составляет 1050 руб.

Патч-панель 19(1U), 24 портов RJ-45,категория 5e (См. рис. 10)



Рисунок 10 - Патч-панель 19(1U), 24 портов RJ-45,категория 5e

Межсетевой экран ESR-30 FSTEC (См. рис 11)

Характеристики:

* Интерфейсы: 4xEthernet 10/100/1000BASE-T (LAN/WAN), 2x10GBASE-R/1000BASE-X (SFP+/SFP), 1xUSB 2.0, 1xUSB 3.0, слот для microSD-карт.
* Поддержка списков контроля доступа (ACL) на базе L2/L3/L4-полей
* Протоколы динамической маршрутизации RIPv2, OSPFv2/v3, IS-IS, BGP
* Максимальная потребляемая мощность - 26 Вт
* Цена 514 940 руб.



Рисунок 11 - Межсетевой экран ESR-30 FSTEC

Коммутатор 3-го уровня 10G MES5316A (См. рис 12)

Характеристики:

* Пропускная способность 320 Гбит/с
* Интерфейсы: 16х10GBASE-R (SFP+)/1000BASE-X (SFP), 1х10/100/1000BASE-T (ООВ), 1xUSB 2.0, 1x консольный порт RS-232 (RJ-45)
* Поддержка Voice VLAN
* Поддержка STP (Spanning Tree Protocol, IEEE 802.1d)
* Поддержка Spanning Tree Fast Link option
* Поддержка BPDU Filtering
* Поддержка STP BPDU Guard
* Протоколы динамической маршрутизации RIPv2, OSPFv2, OSPFv3, IS-IS (IPv4 Unicast), BGP4 (IPv4 Unicast, IPv4 Multicast)
* Питание: 100-240 В AC, 50-60 Гц
* Цена 450 000 руб.

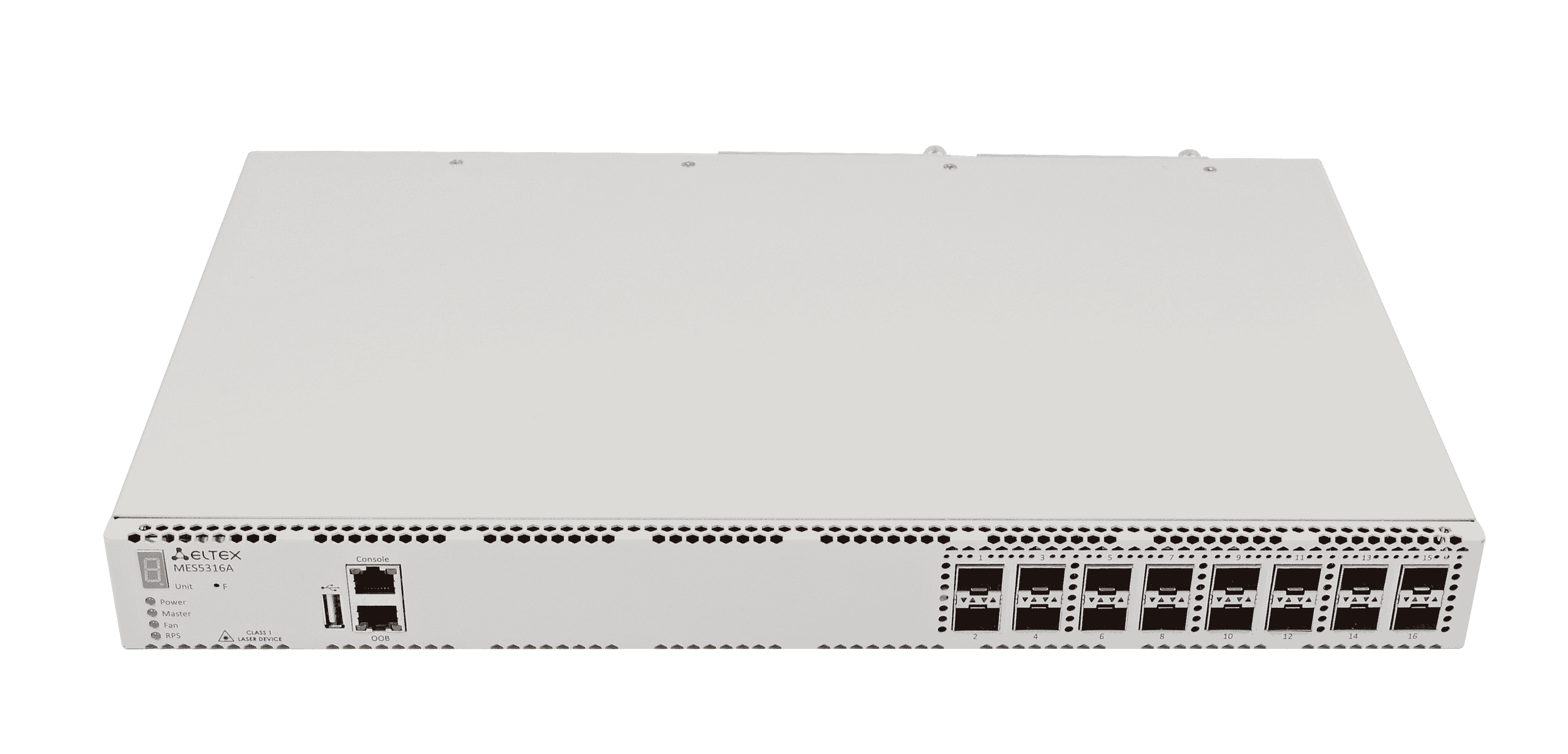


Рисунок 12 - Коммутатор 3-го урованя 10G MES5316A

Контроллер беспроводного доступа WLC-15 (См. рис 13)

Характеристики:

* Интерфейсы: Ethernet 10/100/1000BASE-T (LAN/WAN) – 4, Ethernet 1000BASE-X SFP – 2, Console (RJ-45) - 1USB 2.0 – 1, Разъем для установки HDD – 1, Слот для microSD-карты – 1
* Число точек доступа – 50
* Динамические протоколы маршрутизации RIPv2, OSPFv2/v3, IS-IS, BGP
* DHCP-клиент
* Интерфейсы управления CLI
* Максимальная потребляемая мощность - 18 Вт
* Цена 40 000 руб.

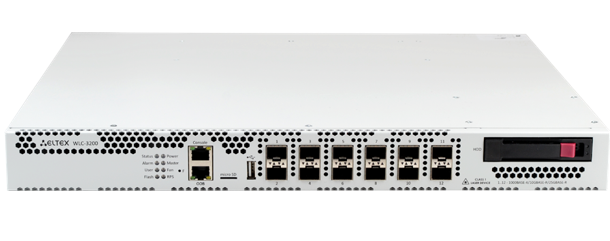


Рисунок 13 - Контроллер беспроводного доступа WLC-15

### 2.3 Физическое моделирование. Проектирование размещения радиоканалов в пространстве

Проектирование размещения радиоканалов в пространстве включает в себя разработку оптимальной схемы распределения радиочастотного сигнала по обслуживаемой территории. Это важно для обеспечения качественного покрытия и баланса уровней сигнала между ретранслятором и абонентскими станциями.

При проектировании учитываются такие факторы, как толщина и материалы перекрытий, геометрические размеры помещений, применяемые частоты и мощности. Для планирования таких систем используются специальные программные инструменты.

Для проектирования размещения радиоканалов в пространстве в школе №54 была использована программа Ekahau (См. рис. 14).



Рисунок 14 - проектирования размещения радиоканалов в пространстве

Для покрытия Wi-Fi всей площади здания понадобилось 8 точек доступа, по 4 устройства на этаж.

Для расчета затрат на кабель, на плане рабочих мест был проброшен виртуальный провод в пространстве школы №54 (См. рис 15)

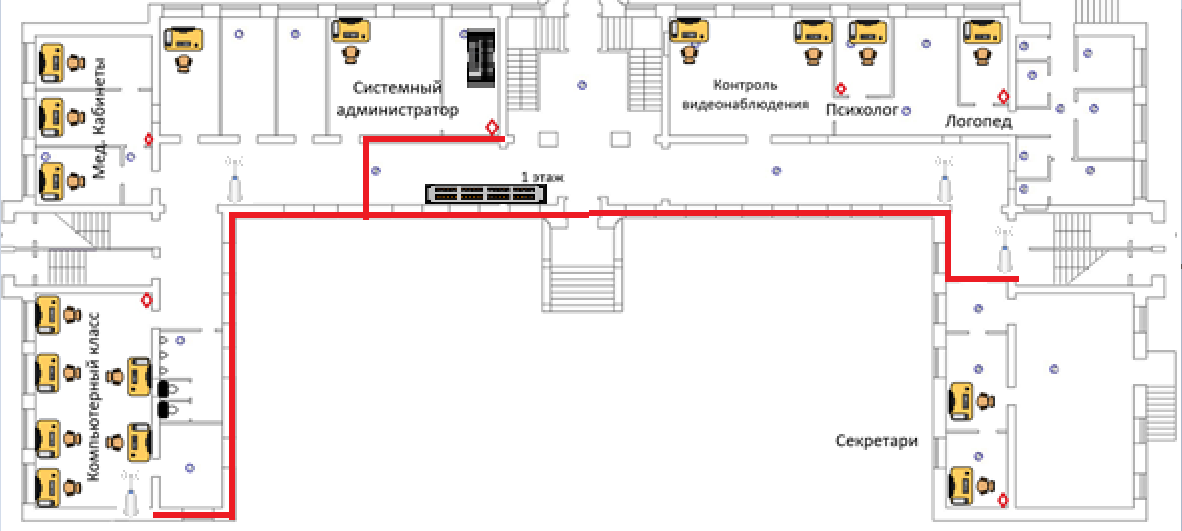


Рисунок 15 – Кабель в виртуальной среде Visio

### 2.4 Проектирование размещения оборудования в шкафу (стойке)

Проектирование размещения оборудования в шкафу или стойке является важным этапом при создании надёжной и эффективной системы. Оно включает в себя определение оптимального расположения компонентов, обеспечение достаточного пространства для вентиляции и охлаждения, а также соблюдение требований по электрической безопасности.

Настенные коммутационные шкафы представляют собой эффективное решение для организации телекоммуникационной инфраструктуры в условиях ограниченного пространства, например, в коридорах школ с высокой проходимостью. Их установка позволяет безопасно разместить активное и пассивное оборудование, обеспечивая удобство доступа к нему и сохраняя порядок в помещении.

Установка настенных коммутационных шкафов позволяет оптимизировать использование пространства, снизить риск возникновения аварийных ситуаций и повысить общую эффективность работы сети.

В здании школы установлены два коммутационных шкафа: один расположен на первом этаже, а второй — на втором.

В настенном коммутационном шкафу установлены сетевые фильтры, источники бесперебойного питания (ИБП), патч панели и коммутаторы. (См. рис. 15).



Рисунок 15 – Настенный коммутационный шкаф

Также в аппаратной комнате был установлен коммутационный шкаф, в который входят такие устройства, как: патч-панель, сервер, маршрутизатор, ибп и сетевой фильтр. (См. рис. 16).

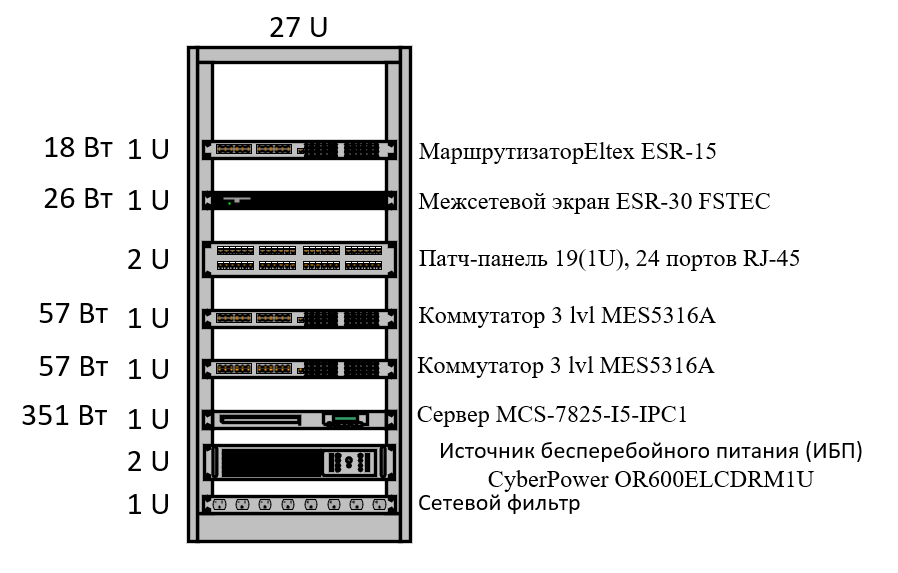


Рисунок 16 – Коммутационный шкаф аппаратной комнаты

2.5 Анализ результатов тестирования сети.

1. Тестирование маршрутизации и IP-туннелей

Для проверки работоспособности IP-туннелей между офисами HQ и BR был использован инструмент ping и traceroute для проверки связи между конечными точками туннеля. Ожидаемая стабильность соединения через туннель (на основе настроек GRE или IP in IP) была подтверждена. Все тесты показали, что маршруты правильно передаются через туннель, и при использовании протокола OSPF маршрутизаторы корректно обменивались маршрутами и восстанавливались при наличии резервных путей.

Результат: Связь между офисами установлена и работает корректно, маршруты правильно пересчитываются в случае сбоя одного из путей.

Ожидаемый результат: Все маршруты доступны между офисами, даже при выключении одного канала связи.

2. Тестирование DHCP-сервера и выдачи адресов

Для проверки корректности работы DHCP-сервера на маршрутизаторе HQ-RTR был выполнен запрос на получение IP-адреса с устройства HQ-CLI. Адрес был выдан без ошибок, также был корректно исключен адрес самого маршрутизатора из диапазона IP-адресов, как того требовала задача. В процессе тестирования проверено, что клиент получает правильный адрес шлюза и DNS-сервера.

Результат: DHCP-сервер работает корректно, устройства получают правильные IP-адреса.

Ожидаемый результат: Устройства в сети HQ получают динамически назначаемые адреса, исключая маршрутизатор.

3. Тестирование DNS-сервера

Проверка работы DNS-сервера на машине HQ-SRV показала, что все запросы на разрешение имен функционируют правильно, включая разрешение доменных имен для внутренних и внешних ресурсов. При недоступности основного DNS-сервера запросы перенаправляются на публичный DNS-сервер, что обеспечивает отказоустойчивость.

Результат: DNS-сервер работает без сбоев, разрешение имен корректно настроено.

Ожидаемый результат: В случае недоступности основного DNS-сервера система автоматически переключается на сервер пересылки.

4. Тестирование безопасности SSH и удаленного доступа

Для проверки настройки безопасности SSH-доступа на серверах HQ-SRV и BR-SRV были проведены попытки подключений с использованием sshuser через порт 2024. Подключения были успешными при правильном вводе пароля. Также был проверен механизм ограничения попыток входа, который ограничивает количество неудачных попыток до двух. Баннер "Authorized access only" отображается при попытке входа.

Результат: SSH-доступ работает корректно, система безопасности ограничивает количество попыток входа.

Ожидаемый результат: Ожидается, что при большом количестве неудачных попыток входа доступ будет заблокирован.

5. Тестирование NFS-сервера и файлового хранилища

Для тестирования файлового хранилища, настроенного с использованием RAID 5, были проведены операции чтения и записи через NFS. Проверено, что на сервере HQ-SRV данные записываются и читаются без ошибок в папке /raid5/nfs, и доступ с машины HQ-CLI осуществляется корректно. Монтирование выполнялось автоматически при старте системы на обоих устройствах.

Результат: Файловое хранилище работает без ошибок, доступ к данным через NFS обеспечен.

Ожидаемый результат: Доступ к файловому хранилищу обеспечен для всех устройств в сети HQ.

6. Тестирование синхронизации времени

Для проверки работы службы chrony была проверена синхронизация времени между сервером HQ-RTR и клиентами (машины HQ-SRV, HQ-CLI, BR-RTR, BR-SRV4). Все устройства синхронизировались с сервером HQ-RTR с точностью до нескольких миллисекунд, что подтверждает правильность настройки службы.

Результат: Время синхронизируется на всех устройствах.

Ожидаемый результат: Время на всех устройствах синхронизировано с сервером времени HQ-RTR.

7. Тестирование Samba и доменной интеграции

Проверка настройки Samba и доменной интеграции показала, что пользователи из группы hq могут успешно аутентифицироваться на машине HQ-CLI. Также проверено, что пользователи из этой группы имеют возможность выполнять ограниченный набор команд с повышенными привилегиями, как того требует задача.

Результат: Пользователи корректно аутентифицируются, права на выполнение команд настроены правильно.

Ожидаемый результат: Пользователи могут выполнять только разрешенные команды с привилегиями, другие команды блокируются.

8. Тестирование трансляции адресов (NAT)

Для проверки корректности настройки динамической трансляции адресов (NAT) была выполнена проверка доступа всех устройств в офисах HQ и BR в сеть Интернет. Все устройства успешно использовали NAT для выхода в Интернет, что подтверждает правильность настройки трансляции.

Результат: NAT работает корректно, устройства имеют доступ к Интернету.

Ожидаемый результат: Все устройства могут выходить в Интернет через ISP с корректной трансляцией адресов.

## 3 Экономическая часть

## 3.1 Расчет стоимости лицензионного программного обеспечения сетевой инфраструктуры

Далее предоставляется расчет суммарной стоимости оборудования сетевой инфраструктуры.

Стоимость оборудования рассчитана исходя из средних рыночных цен, представлена в таблице 4. (См. табл 4)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Оборудование** | **Модель** | **Кол-во** | **Цена (1 шт.)** | **Общая цена** |
| Коммутатор 2-го уровня | MES2428B | 4 | 47 262 руб. | 189 048‬ руб. |
| Маршрутизатор | Eltex ESR-15 | 2 | 66 158 руб. | 132 316 руб. |
| Точка доступа | DAP-2230 (Omni) | 8 | 5000 руб. | 40 000 руб. |
| Источник бесперебойного питания | CyberPower OR600ELCDRM1U | 3 | 15 740 руб. | 47 220 руб. |
| Сервер | Cisco MCS-7825-I5-IPC1 | 1 | 215 730 руб. | 215 730 руб. |
| Cетевой фильтр | DEXP Intensity 418BU | 3 | 1050 руб. | 3 150 руб. |
| Патч-панель | 19(1U), 24 портов RJ-45,категория 5e | 3 | 3000 руб. | 9000 руб. |
| Коммутатор 3-го уровня | MES5316A | 2 | 450 000 руб. | 900 000 руб. |
| Firewall | ELTEX [ESR-20 FSTEC] | 1 | 514 000 руб. | 514 000 руб. |
| WLC контроллер | WLC-15 Eltex | 1 | 40 000 руб. | 40 000 руб. |
| Итого: | | | | 2 090 464 руб. |

Таблица 4 – Расчет стоимости оборудования

Средние рыночные цены расходуемых материалов приведены ниже, в таблице 5. (См. табл 5)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Материал** | **Модель** | **Кол-во** | **Цена за 1 шт.** | **Общая цена** |
| Компьютерная розетка | Двойная (2 RJ-45) | 16 | 156 | 2 496 руб. |
| Кабель | UTP | 480 м. | 42 | 20 160 руб. |
| Коннектор | RJ45 5E 8P8C | 32 | 5 | 160 руб. |
| Шкаф в аппаратной | ТЕЛКОМ ТС-27.6.6-СМ.9005М | 1 | 38 000 руб. | 38 000 руб. |
| Шкаф настенный | ТЕЛКОМ TL-15.6.3-С.7035Ш | 2 | 14 000 руб. | 28 000 руб. |
| Итого: | | | | 88 816 руб. |

Таблица 4 – Расчет стоимости материалов

Чтобы определить общую стоимость компьютерной сети, нужно сложить указанные в таблице значения. На основе полученных результатов рассчитывается общая стоимость сети, указанная в таблице 5.

|  |  |
| --- | --- |
| **Затраты** | **Цена** |
| Оборудование | 2 090 464 руб. |
| Расходные материалы | 88 816 руб. |
| Итого | 2 179 280 руб. |

## Заключение

В процессе выполнения курсового проекта была создана схема рабочих мест в компании «Зевс», также была построена теоретико-графовая модель и проведен математический расчет компьютерной сети, с помощью которых получилось найти оптимальное место для устновки серверного оборудования. Вдобавок была спроектирована компьютерная сеть на базе оборудования Cisco, а также рассчитана ее стоимость.

В ходе выполнения курсового проекта были развиты навыки проектирования и настройки компьютерных сетей, а также углублены знания в области анализа и систематизации информации из различных источников. Проект включал в себя изучение теоретических аспектов построения и функционирования компьютерных сетей, выбор подходящей технологии для решения поставленных задач, разработку архитектуры сети, настройку сетевых компонентов и тестирование работоспособности системы.

Особое внимание было уделено анализу требований к информационной безопасности и защите данных, что позволило обеспечить надёжность и стабильность работы сети. Также были изучены методы оптимизации производительности сети и управления трафиком, что способствовало повышению эффективности работы системы.

В процессе выполнения проекта были проведены исследования существующих аналогов и конкурентов, что позволило выявить их преимущества и недостатки, а также определить возможности для улучшения и развития собственных разработок.

## 

## Литература

## Основная литература:

1. Баринов, В.В. Компьютерные сети: Учебник / В.В. Баринов, И.В. Баринов, А.В. Пролетарский. - М.: Academia, 2018. - 192 c.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-ое изд. – СПб.:Питер, 2016 – 992 с.
3. Таненбаум, Э.С. Компьютерные сети / Э.С. Таненбаум, Д. Уэзеролл. - СПб.: Питер, 2018. - 512 c.

**Дополнительная**

* 1. Немет Эви, Снайдер Гарт, Хейн Трент, Уэйли Бэн. Unix и Linux: руководство системного администратора, 4-е изд.: Пер.с англ. – М.ООО «И.Д. Вильямс», 2020. – 1312 с.: ил.