МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра «Экономики и управления на предприятии природопользования»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(бакалаврская работа)
по направлению подготовки 09.03.03 Прикладная информатика
(квалификация – бакалавр)

На тему «Проектирование локальной вычислительной сети с учётом специфики деятельности предприятия»

Исполнитель Часткин Сергей Михайлович

Руководитель к.т.н., Тарасов Елизар Саввич

«К защите допускаю»

Руководитель кафедры _____

кандидат экономических наук

Майборода Евгений Викторович

«14» 01 2026 г.

Филиал Российского государственного гидрометеорологического университета в г. Туапсе
НОРМОКОНТРОЛЬ ПРОЙДЕН
«13» 01 2026 г.
Мартынова Т.В.
подпись расшифровка подписи

Туапсе
2026

ОГЛАВЛЕНИЕ

Введение

Современная гостиница представляет собой не только номера для проживания и административную инфраструктуру, но и сложный сервисный комплекс, в котором одновременно функционируют службы размещения, бухгалтерия, отдел кадров, служба материально-технического обеспечения, IT-подразделение, служба безопасности и администрация. Для координации их работы и обеспечения качественного сервиса требуется надёжная и масштабируемая локальная вычислительная сеть (ЛВС), позволяющая интегрировать и автоматизировать основные операции и обеспечить безопасный доступ к информационным ресурсам.

Основные отечественные и международные стандарты в области структурированных кабельных систем ориентированы на офисную и аналогичную ей недвижимость. Но и для гостиниц среднего класса могут быть востребованы совершенно разные решения в области автоматизации. В каждом случае при проектировании и реализации возникают свои проблемы и трудности. Несмотря на это, бесспорным является общее требование: гость не должен ощущать какого-либо неудобства, а предоставляемые сервисы должны соответствовать его ожиданиям.

Как правило, владельцы небольших гостиниц в своём понимании технологий, предъявляют простейшие требования и рассчитывают на минимальные затраты. Ожидают от решения слишком многого в автоматизации и надёжности. В тоже время в штате отсутствуют ИТ-специалисты. В лучшем случае предусматривают в бюджете найм приходящего специалиста.

Гостиница «Марьяж», состоящая из двух трёхэтажных корпусов, морально устаревшей IT-инфраструктурой, которая нуждается в модернизации с учётом современных требований, включая обновление инженерных систем и создание новой ЛВС. Заказчик планирует возможное расширение гостиничного комплекса, но не ранее чем через три года, и в настоящий момент отдаёт приоритет минимизации первоначальных затрат при сохранении возможности

дальнейшей модернизации.

Особенностью гостиницы «Марьяж» является круглосуточный режим работы и наличие как административных, так и гостевых зон. В первом корпусе размещаются руководство, служба размещения, отдел кадров и бухгалтерия, IT-отдел, служба безопасности и вспомогательный персонал. Во втором корпусе сосредоточены жилые номера для гостей. Для сотрудников и гостей требуется организовать проводную и беспроводную сеть с разделением доступа, обеспечивающую безопасную и стабильную работу информационных сервисов.

Дополнительную значимость проекту придаёт необходимость соблюдения нормативных требований Российской Федерации в части идентификации пользователей и хранения информации при предоставлении доступа в сеть Интернет через публичные точки Wi-Fi. В частности, доступ гостей к сети должен осуществляться по индивидуальным идентификаторам в соответствии с Постановлением Правительства РФ № 758 от 31.07.2014 г., что требует внедрения специализированных решений по учёту и хранению данных пользователей.

Актуальность темы выпускной квалификационной работы обусловлена следующим:

– рост требований клиентов к качеству IT-сервисов в местах размещения, включая высокоскоростной доступ в Интернет и бесперебойную работу сетевой инфраструктуры;

– необходимость интеграции гостиничного комплекса с государственными информационными системами (налоговой службой, фондами, системами отчётности и т.п.)[22];

– потребность в централизованной системе учёта, бронирования и аналитики, позволяющей оперативно оценивать загрузку номерного фонда и другие, в том числе финансовые показатели;

– требования к обеспечению информационной безопасности и защите персональных данных гостей и сотрудников.

Таким образом, объектом исследования является информационная инфраструктура гостиницы «Марьяж», включающая административный корпус, корпуса размещения гостей, территорию с существующей и планируемой инженерной инфраструктурой, а также систему предоставления доступа к сети Интернет.

Предмет исследования - процессы проектирования и реализации локальной вычислительной сети, учитывающей специфику деятельности гостиничного предприятия, требования по надёжности, безопасности, дальнейшей масштабируемости и экономической эффективности.

Целью выпускной квалификационной работы является разработка проекта локальной вычислительной сети гостиницы «Марьяж» с учётом специфики её функционирования с точки зрения IT-инфраструктуры, действующих нормативных требований и перспектив tt дальнейшего развития.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Провести анализ предметной области и обосновать необходимость проектирования новой ЛВС для гостиницы.
2. Исследовать потребности и ограничения предприятия, сформировать требования к сети и составить техническое задание на проектирование.
3. Разработать проектные решения по структуре ЛВС, выбору топологии, активного и пассивного оборудования, а также по организации проводной и беспроводной сети гостиницы.
4. Описать план практической реализации проекта на площадке заказчика, включая этапы монтажных и пусконаладочных работ, а также меры по обеспечению надёжности и информационной безопасности.
5. Разработать план тестирования и опытной эксплуатации сети.
6. Провести оценку экономической эффективности внедрения проектируемой ЛВС.

Структурно работа состоит из введения, четырёх разделов, заключения, списка использованных источников и приложений. Во введении обосновывается актуальность темы, формулируются цель и задачи исследования. В первой главе рассматриваются аналитические аспекты и необходимость проектирования сети. Во второй – формируются требования к проекту сети на основе анализа потребностей предприятия. Третья глава посвящена разработке проектных решений и описанию практической реализации. В четвёртой главе выполняется обоснование экономической эффективности предлагаемого проекта.

1 Аналитическая часть

Теоретической и методологической основой работы являются отечественные и международные стандарты по проектированию структурированных кабельных систем и локальных вычислительных сетей, нормативные документы в области безопасности труда и пожарной безопасности, а также действующие ГОСТ по проектной документации и эксплуатации информационных систем.

Практическая значимость работы заключается в том, что разработанный проект ЛВС может быть использован как основа для реальной модернизации сетевой инфраструктуры гостиницы «Марьяж» либо аналогичных объектов малого и среднего гостиничного бизнеса, а также может служить примером выполнения проектной части выпускной квалификационной работы по направлению 09.03.03 «Прикладная информатика».

1.1 Анализ исходного состояния и особенностей объекта

Исходным объектом для проектирования является гостиница «Марьяж», расположенная в Туапсинском районе. На территории размещены два трёхэтажных корпуса, предназначенных для административной деятельности и проживания гостей. Общая численность штата – 29 человек. В структуру подразделений входят служба размещения, IT-отдел, служба материально-технического обеспечения, отдел кадров, бухгалтерия, руководство, служба безопасности и секретариат.

Существующая инфраструктура гостиницы характеризуется следующими особенностями:

– наличие ЛВС и подключения к сети Интернет, однако кабельная система морально устарела и не соответствует современным требованиям к скорости и надёжности;

– здания находятся в стадии капитального ремонта, что создаёт

уникальную возможность для прокладки новой структурированной кабельной системы с учётом перспективного развития;

– размещение административных служб и серверного оборудования планируется в корпусе А, в специально выделенных помещениях (руководство, служба размещения, отдел кадров и бухгалтерия, IT-отдел, служба безопасности, серверная);

– корпус Б ориентирован на размещение отдыхающих и требует в первую очередь качественного покрытия Wi-Fi и обеспечения доступа к гостиничным сервисам;

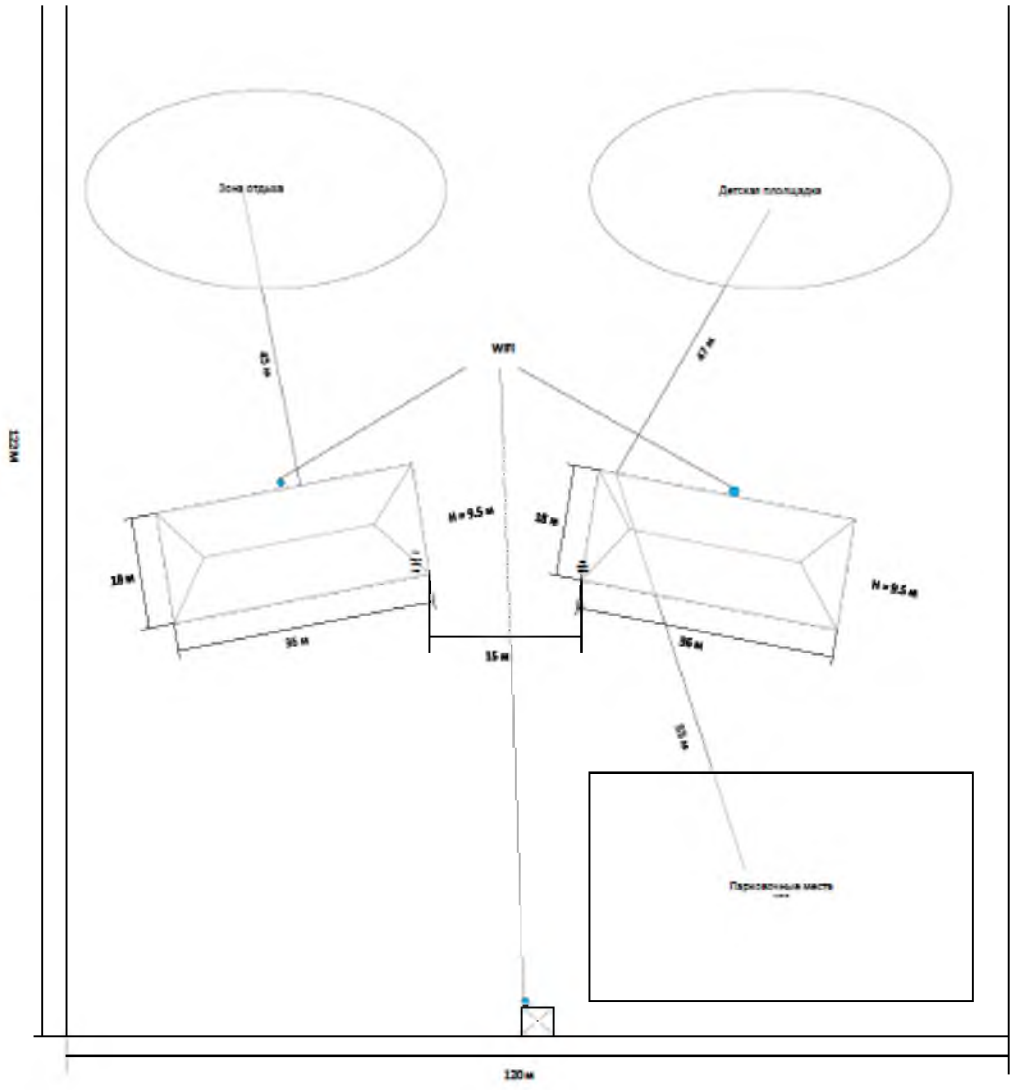

Рисунок 1.1 – Общий план территории объекта

– на каждом этаже обоих корпусов предусмотрено по две точки Wi-Fi, а также по одной внешней точке доступа на корпус и дополнительная внешняя точка в зоне охраны при въезде на территорию.

Важной особенностью является круглосуточный режим работы гостиницы. Это означает, что любые простои сетевой инфраструктуры непосредственно влияют на качество обслуживания гостей и могут приводить к финансовым потерям, негативным отзывам и снижению конкурентоспособности. Соответственно, к ЛВС предъявляются повышенные требования по отказоустойчивости и возможностям резервирования.

Таблица 1.1 – Характеристика корпусов гостиницы «Марьяж» и рабочих мест

Корпус	Назначение	Эт.	Основные помещения	Кол-во рабочих мест	Внутренние точки Wi-Fi	Внешние точки Wi-Fi
А	Административно-офисный	3	Руководство, бюро размещения, отдел кадров и бухгалтерия, IT, служба безопасности, серверная	6	6 (по 2 на этаж)	1
Б	Корпус размещения гостей	3	Номера, коридоры, небольшие служебные помещения персонала	2 (служебные)	6 (по 2 на этаж)	1
Территория	Въезд и зона охраны	–	Пост охраны, шлагбаум, КПП	1	–	1

С точки зрения перспектив развития собственник рассматривает возможность расширения комплекса за счёт строительства дополнительных объектов, однако не ранее чем через три года. Это накладывает требование к масштабируемости сети, т.е. необходимо заложить возможность подключения новых помещений и рабочих мест без полной модернизации уже построенной инфраструктуры.

1.2 Проблемы существующей инфраструктуры и риски её эксплуатации

Гостиница функционирует в круглосуточном режиме, что предъявляет повышенные требования к отказоустойчивости ЛВС: любые простои напрямую влияют на качество обслуживания и финансовый результат. В ЛВС должны поддерживаться следующие группы сервисов: автоматизация службы размещения (учёт и бронирование номеров, заселение и выселение, формирование отчётности); учёт и аналитика хозяйственной деятельности (бухгалтерия, финансово-экономический отдел, отдел кадров); административный доступ руководства к управленческой отчётности; – внутренняя IP-телефония и, при необходимости, интеграция с городскими линиями; система видеонаблюдения и контроля доступа (особенно для входных групп, коридоров, критичных внутренних помещений); гостевой доступ к сети Интернет через Wi-Fi, с идентификацией пользователей и хранением учётных данных; доступ к внешним информационным системам (налоговая, фонды, отчётность).

Сетевые сервисы разделяются на служебный и гостевой контуры, что требует логической сегментации сети (VLAN, отдельные SSID), а также применения межсетевого экрана/маршрутизатора с функциями DPI и контроля доступа.

С точки зрения беспроводной сети, требуется обеспечение устойчивого покрытия Wi-Fi во всех административных помещениях корпуса А, полноценное покрытие номеров и общих зон корпуса Б, покрытие прилегающей территории (зона отдыха, детская площадка, парковка, пост охраны) с использованием внешних точек доступа и работа гостевого Wi-Fi-портала с выдачей индивидуальных кодов доступа и учётом логинов/MAC-адресов согласно требованиям законодательства.

Анализ исходного состояния позволяет выделить ряд проблем, характерных для объектов с устаревшейIT-инфраструктурой, а именно:

1. Отсутствие единой структурированной кабельной системы. Как правило, в подобных объектах прокладка кабелей выполнялась поэтапно, без единого проекта, что приводит к фрагментированности сети, сложности в обслуживании и невозможности эффективной модернизации.

2. Ограниченная пропускная способность и низкая скорость передачи данных, когда использование устаревших стандартов сетевого оборудования и кабеля приводит к ограничению скорости доступа к внутренним сервисам и сети Интернет, что особенно критично при одновременной работе нескольких служб и значительного числа постояльцев.

3. Недостаточная надёжность и резервирование, при отсутствии продуманной схемы резервирования отказ одного коммутатора или маршрутизатора может приводить к остановке работы целого корпуса или критически важного сервиса (системы бронирования, видеонаблюдения и т.п.).

4. Повышенные риски в области информационной безопасности. Неоднородная и слабо управляемая сеть затрудняет реализацию политик безопасности, сегментацию трафика, контроль доступа и журналирование действий пользователей, что особенно важно при обработке персональных данных гостей и сотрудников.

5. Несоответствие современным нормативным требованиям. В частности, при предоставлении доступа в Интернет через беспроводную сеть необходимо обеспечивать идентификацию пользователей и хранение информации о фактах оказания услуг связи в соответствии с действующим законодательством РФ.

1.3 Обоснование необходимости проектирования новой ЛВС

Учитывая выявленные проблемы, создание новой локальной вычислительной сети на базе современных технологий является необходимым условием успешного функционирования гостиницы «Марьяж».

Необходимость разработки проекта ЛВС определяется следующими факторами:

– потребность в комплексной автоматизации хозяйственной деятельности гостиницы (учёт и бронирование номеров, управление тарифами, учёт дополнительных услуг, формирование отчётности);

– требование к обеспечению непрерывной работы служб размещения, бухгалтерии, отдела кадров и службы безопасности, тесно зависящих от доступа к информационным системам;

– необходимость создания единой информационной среды, обеспечивающей обмен данными между корпусами, зонами отдыха, парковкой и постом охраны;

– рост объёмов передаваемых данных, связанных с использованием систем видеонаблюдения, IP-телефонии, систем контроля доступа и обслуживающего персонала;

– потребность в организации высокоскоростного и безопасного доступа гостей к сети Интернет через Wi-Fi с возможностью учёта и идентификации пользователей.

Проектирование ЛВС на основе формализованных требований и действующих стандартов позволяет оптимизировать затраты на закупку оборудования и монтаж, исключив избыточные решения, обеспечить требуемый уровень качества для приоритетных задач, предоставить возможность дальнейшего наращивания инфраструктуры без полной её замены, а также упростить сопровождение и обслуживание сети за счёт стандартизации используемых компонентов.

В первом корпусе («корпус А») размещаются административные и сервисные помещения: кабинет руководства (1 помещение, 1 рабочее место), бюро размещения (1 рабочее место), совмещённый кабинет отдела кадров и бухгалтерии (1 помещение, 2 рабочих места), кабинет IT-специалиста (1 помещение, 1 рабочее место), служба безопасности (1 помещение, 1 рабочее место). В этом же корпусе размещается серверная и коммутационный шкаф. На

каждом из трёх этажей корпуса А предусмотрено по 2 точки доступа Wi-Fi (всего 6 внутренних точек).

Второй корпус («корпус Б») предназначен для размещения отдыхающих и ориентирован, прежде всего, на обеспечение качественного беспроводного доступа к сети Интернет и гостиничным сервисам. На каждом этаже корпуса Б также предусмотрено по 2 точки доступа Wi-Fi (всего 6 внутренних точек). Коммутационный шкаф.Кроме того, на каждом корпусе планируется по одной внешней точке доступа Wi-Fi для покрытия прилегающей территории, а у поста охраны на въезде на территорию – ещё одна внешняя точка доступа.

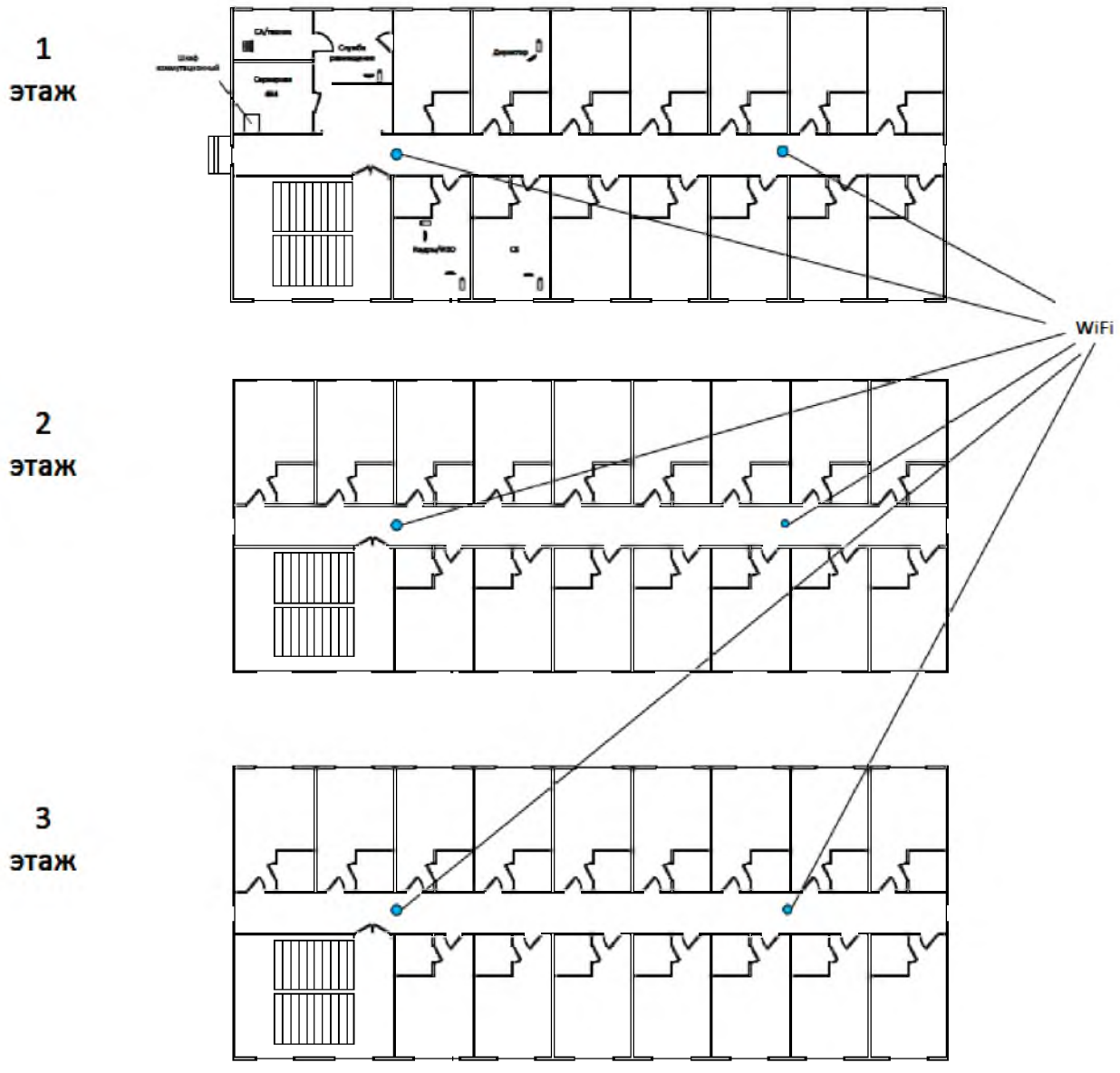

Рисунок 1.2 – Расположение точек доступа в корпусе А

Таким образом, разработка проекта ЛВС для гостиницы «Марьяж» является обоснованной и актуальной задачей, решение которой позволит сформировать надёжную основу для цифровой трансформации предприятия и повышения качества предоставляемых услуг.

2 Разработка требований к проекту сети

2.1 Анализ потребностей и ограничений предприятия на примере гостиницы

При формировании требований к ЛВС необходимо учесть, как функциональные требования заказчика, так и существующие ограничения, связанные с особенностями объекта, бюджетом и нормативной базой.

Ключевые потребности заказчика можно сгруппировать следующим образом.

1. Автоматизация основной деятельности гостиницы

– Ведение базы данных клиентов, истории их проживаний и оказываемых услуг.

– Автоматизированный учёт номерного фонда, статусов номеров (свободен, занят, забронирован, на уборке и т.п.).

– Интеграция с системами онлайн-бронирования и каналами продаж (сайт гостиницы, агрегаторы бронирования при необходимости).

– Формирование управленческой и финансовой отчётности по видам услуг, периодам, категориям клиентов.

2. Поддержка административно-управленческих процессов

– Работа отдела кадров с электронными личными делами сотрудников и системами учёта рабочего времени.

– Ведение бухгалтерского учёта и налоговой отчётности с использованием специализированного программного обеспечения.

– Обеспечение доступа руководства к аналитическим отчётам в режиме реального времени.

3. Обеспечение сервиса для гостей

– Высокоскоростной доступ в Интернет через Wi-Fi в номерах и общественных зонах.

– Возможность разграничения гостевого трафика и трафика служебных систем.

– Выдача индивидуальных учётных данных (кодов доступа) гостям с учётом требований законодательства РФ по идентификации пользователей.

4. Информационная безопасность и контроль

– Сегментация сети на служебный и гостевой контуры.

– Ограничение доступа персонала к критичным системам в соответствии с их должностными обязанностями.

– Ведение журналов доступа и мониторинг сетевой активности.

– Обеспечение защищённого обмена данными с внешними системами (налоговая служба, фонды, системы отчётности).

5. Надёжность и масштабируемость

– Круглосуточная работа ЛВС с минимальными простоями.

– Возможность резервирования ключевых элементов (маршрутизаторов, коммутаторов ядра, линий связи).

– Планирование резерва по портам, пропускной способности и кабельным трассам для подключения дополнительных рабочих мест и возможных новых зданий.

Основные ограничения проекта заключаются в минимизации капитальных затрат на начальном этапе при сохранении возможности последующей модернизации (то есть возможность поэтапного наращивания), а также необходимость учитывать требования по электробезопасности и пожарной безопасности для общественных зданий и требования к размещению оборудования обработки информации. Также следует учесть приоритет использования отечественного или поставляемого из дружественных стран оборудования в условиях санкционных ограничений. Свою роль играют и архитектурные особенности зданий (размеры корпусов, расположение помещений, высота этажей, необходимость аккуратного размещения кабельных каналов и шкафов).

С учётом перечисленных потребностей и ограничений формируется техническое задание на проектирование ЛВС.

2.2 Составление технического задания проекта сети

Техническое задание (ТЗ) на проектирование ЛВС гостиницы «Марьяж» составляется в соответствии с требованиями государственных стандартов к проектной документации и включает основные разделы: общие сведения, требования к системе, требования к надёжности и безопасности, состав и содержание работ, порядок приёмки и источники разработки.

Таблица 2.1 – Требования заказчика и основные ограничения

Содержание	Влияние на проектные решения
Автоматизация бронирования и учёта	Выбор клиент–серверной архитектуры, выделение серверного сегмента
Качественный гостевой Wi-Fi	Планирование зон покрытия, достаточное число точек, поддержка 802.11ac
Информационная безопасность	Сегментация VLAN, межсетевой экран, политика доступа
Интеграция с внешними системами	Наличие маршрутизатора с поддержкой VPN и фильтрацией трафика
Масштабируемость в горизонте 3+ лет	Магистральная оптика с запасом волокон, запас портов на коммутаторах
Ограниченный бюджет на стартовом этапе	Выбор оборудования среднего ценового сегмента (ELTEX)
Санкционные и логистические риски	Ориентация на оборудование российских/дружественных поставщиков
Архитектура зданий	Использование настенных шкафов, прокладка в существующих конструкциях

Ниже приводится структурированное содержание ТЗ с учётом уже подготовленного варианта и дополнительных уточнений.

1. Общие сведения

Полное наименование системы: локальная вычислительная сеть гостиницы «Марьяж» (ЛВС гостиницы «Марьяж»).

Основание для выполнения работ: реконструкция гостиничного комплекса, необходимость приведения инженерной и информационной инфраструктуры к современным стандартам предоставления гостиничных услуг, обеспечение интеграции с государственными информационными системами.

Сроки выполнения работ: декабрь 2025 – февраль 2026 года (проектирование, монтаж, пусконаладка).

Источники и порядок финансирования: определяются заказчиком и регламентируются действующими нормативными правовыми актами Российской Федерации и договором подряда.

2. Назначение и цели создания сети

Назначение ЛВС – обеспечение высоконадежной и безопасной передачи данных между подразделениями гостиницы, предоставление доступа в Интернет сотрудникам и гостям, поддержка функционирования информационных систем бронирования, учёта, видеонаблюдения, контроля доступа и других сервисов.

Основные цели:

– автоматизация хозяйственной деятельности гостиницы;

– обеспечение эффективного взаимодействия всех подразделений;

– создание инфраструктуры для предоставления современных цифровых сервисов гостям;

– выполнение требований нормативных документов в области связи, защиты информации и пожарной безопасности.

3. Состав и структура ЛВС

В состав ЛВС входят:

– автоматизированные рабочие места сотрудников (АРМ) в административных помещениях;

– серверная инфраструктура (серверы приложений, базы данных, хранения видеозаписей);

– активное сетевое оборудование (маршрутизаторы, коммутаторы, точки доступа Wi-Fi, оптические медиаконвертеры PON);

– пассивная инфраструктура (оптические и медные кабели, патч-панели, оптические кроссы, кабельные лотки и каналы, настенные и напольные коммутационные шкафы);

– системы бесперебойного питания (ИБП) для серверного и коммутационного оборудования;

– аппаратура подключения к сети провайдера.

Топология сети – иерархическая звезда с центральным узлом в серверной комнате корпуса А и распределительными шкафами в корпусе Б и на территории (для внешних точек доступа и систем видеонаблюдения). Между корпусами используется оптоволоконный магистральный канал с применением PON-медиаконвертеров.

Для гостиницы малого/среднего размера на две трёхэтажные секции с расстоянием между корпусами около 120 м оптимальной является именно иерархическая звезда с одним ядром в корпусе А и распределительным узлом в корпусе Б, поскольку упрощается управление (центральная точка администрирования), минимизируются затраты (нет необходимости в дорогостоящих кольцевых магистралях и сложных протоколах отказоустойчивости на старте проекта) и – сохраняется возможность последующей модернизации (добавление резервного коммутатора ядра, вторых оптических линий и т.д.)

4. Требования к надёжности и режимам функционирования

– ЛВС должна функционировать в круглосуточном режиме (24/7) за исключением периодов регламентного технического обслуживания.

– Среднее время восстановления работоспособности при отказе отдельного элемента сети не должно превышать значений, установленных внутренними регламентами предприятия (как правило, не более 4 часов для критичных узлов).

– Критически важное оборудование (маршрутизатор, коммутаторы ядра, ИБП) должно иметь возможности резервирования и поддерживать хранение конфигурации в энергонезависимой памяти.

– Диагностика состояния ИБП должна включать сигнализацию основных аварийных состояний (разряд батареи, отсутствие внешнего питания, перегрузка).

5. Требования к модернизации и масштабируемости

– При проектировании необходимо предусмотреть запас портов не менее 30 % от текущей потребности по каждому ключевому коммутатору для

подключения дополнительных рабочих мест и оборудования.

– Магистральные линии связи между корпусами должны обеспечивать возможность увеличения пропускной способности без полной их замены (например, за счёт использования оптического кабеля).

– В архитектуре сети должны быть предусмотрены возможности расширения периметра Wi-Fi-покрытия, подключения дополнительных точек доступа и сегментов видеонаблюдения.

6. Требования к диагностике и управлению

– Сетевая инфраструктура должна поддерживать централизованное управление и мониторинг (встроенные веб-интерфейсы, SNMP, журналы событий).

– Должны быть реализованы средства проверки доступности шлюза и ключевых сетевых ресурсов с рабочих мест пользователей (ping, traceroute, средства мониторинга).

– Настройка и администрирование оборудования должно выполняться авторизованным IT-персоналом с использованием защищённых протоколов (SSH, HTTPS).

7. Требования к техническому обслуживанию и ремонту

– Количество профилактических работ, требующих остановки ЛВС, должно быть минимальным; регламентное обслуживание с отключением питания допускается не более одного раза в год.

– Восстановительный ремонт активного оборудования осуществляется на заводе-изготовителе или в сертифицированных сервисных центрах.

– При перебоях электропитания должна обеспечиваться сохранность конфигураций и корректное завершение работы оборудования.

8. Требования к безопасности

В ТЗ включаются требования:

– по электробезопасности и защитному заземлению в соответствии с ГОСТ 12.2.003-91, ГОСТ 12.2.007.0-75, ГОСТ 12.1.030-81 и действующими главами ПУЭ;

– по пожарной безопасности в соответствии с Федеральным законом № 123-ФЗ, СП 5.13130.2009, СП 9.13130.2009 и Правилами противопожарного режима в РФ;

– по безопасности средств вычислительной техники (ГОСТ 21552 и др.);

– по обеспечению информационной безопасности и защите персональных данных (сегментация, идентификация и аутентификация пользователей, регистрация событий, ограничение доступа).

9. Требования к стандартизации и документации

– Проект и рабочая документация должны соответствовать требованиям ЕСКД, ЕСПД и ГОСТ Р 21.101-2020, а также стандартам по проектированию структурированных кабельных систем (ГОСТ Р 53245-2008, ГОСТ Р 53246-2008, ISO/IEC 11801 и др.).

– По завершении работ заказчику должны быть переданы комплект исполнительной документации, схемы ЛВС, спецификации оборудования, инструкции по эксплуатации и обслуживанию.

10. Состав и содержание работ

В ТЗ закрепляются этапы:

– разработка технического задания;

– разработка эскизного проекта (общие схемы, топология, основные решения по оборудованию и трассам);

– разработка рабочего проекта (детальные схемы, планы прокладки кабелей, спецификации, расчёты);

– монтажные работы;

– пусконаладочные работы и опытная эксплуатация;

– приёмка ЛВС в промышленную эксплуатацию.

Приёмка работ осуществляется комиссией с участием представителей заказчика и исполнителя, по результатам оформляется акт приёмочной комиссии.

Итак, по результатам составления ТЗ сформулируем основные требования к ЛВС гостиницы.

Таблица 2.2 – «Основные требования к ЛВС гостиницы «Марьяж»

Группа требований	Конкретные требования
Функциональные	Работа офисных систем, видеонаблюдения, IP-телефонии, гостевого доступа в Интернет
Эксплуатационные	Круглосуточный режим работы, время восстановления критичных узлов – не более 4 часов
По надёжности	Использование ИБП, управляемых коммутаторов, резерв по портам не менее 25–30 %
По безопасности	VLAN-сегментация, межсетевой экран, учёт пользователей Wi-Fi, шифрование
По модернизации	Возможность подключения новых корпусов по оптике, добавление коммутаторов и точек доступа
По стандартизации и документированию	Соответствие ГОСТ, СП, ПУЭ, актуальным методическим рекомендациям

3 Разработка проектных решений

Раздел посвящён обоснованию архитектуры локальной вычислительной сети гостиницы «Марьяж», выбору топологии, активного и пассивного оборудования, а также описанию логической структуры сети и организации беспроводного доступа. Отдельно рассматриваются вопросы практической реализации проекта на площадке заказчика и технические аспекты его эффективности.

3.1 Составление эскизного проекта сети, выбор и обоснование используемых средств и оборудования

3.1.1 Обоснование выбранной архитектуры и топологии

Основой проектируемой ЛВС гостиницы «Марьяж» является иерархическая топология типа «звезда», в которой роль центрального узла (ядра сети) выполняет коммутационный шкаф, расположенный в корпусе А. В центральном узле устанавливается граничный маршрутизатор, коммутатор ядра, оптический кросс и патч-панель горизонтальной подсистемы. От центрального узла отходят:

- магистральные оптические линии связи к корпусу Б;
- кабельные линии к внешним точкам доступа Wi-Fi, расположенным на фасадае корпусов;
- кабельная линия к посту охраны на въезде, где располагается отдельная внешняя точка доступа.

Такой подход позволяет централизовать управление сетью и обеспечить удобное дальнейшее расширение за счёт подключения дополнительных оптических линий и коммутаторов доступа.

В качестве альтернативных вариантов рассматривались:

- классическая топология звезда, в которой все конечные устройства (рабочие места и точки доступа) подключаются к единственному большому

коммутатору;

– кольцевая топология между корпусами, обеспечивающая резервирование магистрального канала;

– многоуровневое «дерево» с выделением отдельного уровня агрегации.

Классическая звезда даёт минимальные капитальные затраты, но плохо масштабируется и не позволяет гибко реализовать сегментацию сети. Кольцевая топология повышает отказоустойчивость, но существенно усложняет конфигурацию и удорожает проект. Многоуровневое дерево оправдано при большем масштабе объекта, когда количество корпусов или этажей значительно больше. Сравнение вариантов сведено в таблицу 3.1. По совокупности критериев для гостиницы малого/среднего размера оптимальной признана иерархическая звезда как компромисс между функциональностью и затратами.

Таблица 3.1 – Сравнительный анализ вариантов топологии ЛВС

Вариант топологии	Преимущества	Недостатки	Стоимость реализации	Вывод
Классическая звезда	Простая конфигурация, минимум оборудования	Слабая масштабируемость, сложнее обеспечить отказоустойчивость	Низкая	Не рекомендуется
Иерархическая звезда	Масштабируемость, удобное администрирование, разделение уровней	Одно ядро – потенциальная точка отказа (уменьшается резервированием)	Средняя	Выбранный вариант
Кольцо между корпусами	Высокая отказоустойчивость магистрали	Более сложная настройка, удорожание за счёт лишнего оборудования	Высокая	Возможен на этапе модернизации

Выбор иерархической топологии также увязан с требованием заказчика учитывать возможность расширения гостиничного комплекса, но не ранее чем через три года. Магистральная оптика и центральный узел в корпусе Апозволяют подключать новые корпуса, не перестраивая уже размещённую инфраструктуру[13].

3.1.2 Структура ЛВС корпуса А

Корпус А является административным центром гостиницы. В нём реализуются все ключевые служебные сервисы, поэтому именно здесь размещается коммутационный шкаф, выполняющий функции ядра ЛВС.

К основным помещениям корпуса А относятся:

- кабинет руководителя (1 рабочее место);
- бюро размещения (1 рабочее место);
- совмещённый кабинет отдела кадров и бухгалтерии (2 рабочих места);
- кабинет IT-специалиста (1 рабочее место);
- кабинет службы безопасности (1 рабочее место);
- серверная / помещение с коммутационным шкафом.

Всего в корпусе А требуется организовать 6 проводных рабочих мест. В соответствии с планами размещения на каждом этаже корпуса предусмотрено по две внутренние точки доступа Wi-Fi, обеспечивающие покрытие административных помещений и общих зон (ресепшн, холлы, коридоры). Дополнительно на фасаде здания размещается одна внешняя точка доступа для покрытия прилегающей территории.

Коммутационный шкаф корпуса А включает в себя:

- настенный 19″ шкаф высотой 10U;
- маршрутизатор ELTEX ESR-15R;
- коммутатор ELTEX MES2324, выполняющий функции ядра сети;
- коммутатор ELTEX MES2324 агрегирующий магистрали в корпусе А;
- оптический кросс для оконцовки магистральных и внешних оптических линий;
- меднуюпатч-панель на 24 порта для подключения рабочих мест и точек доступа;
- кабельные органайзеры и полки;

– источник бесперебойного питания (ИБП) для маршрутизатора и коммутатора[20].

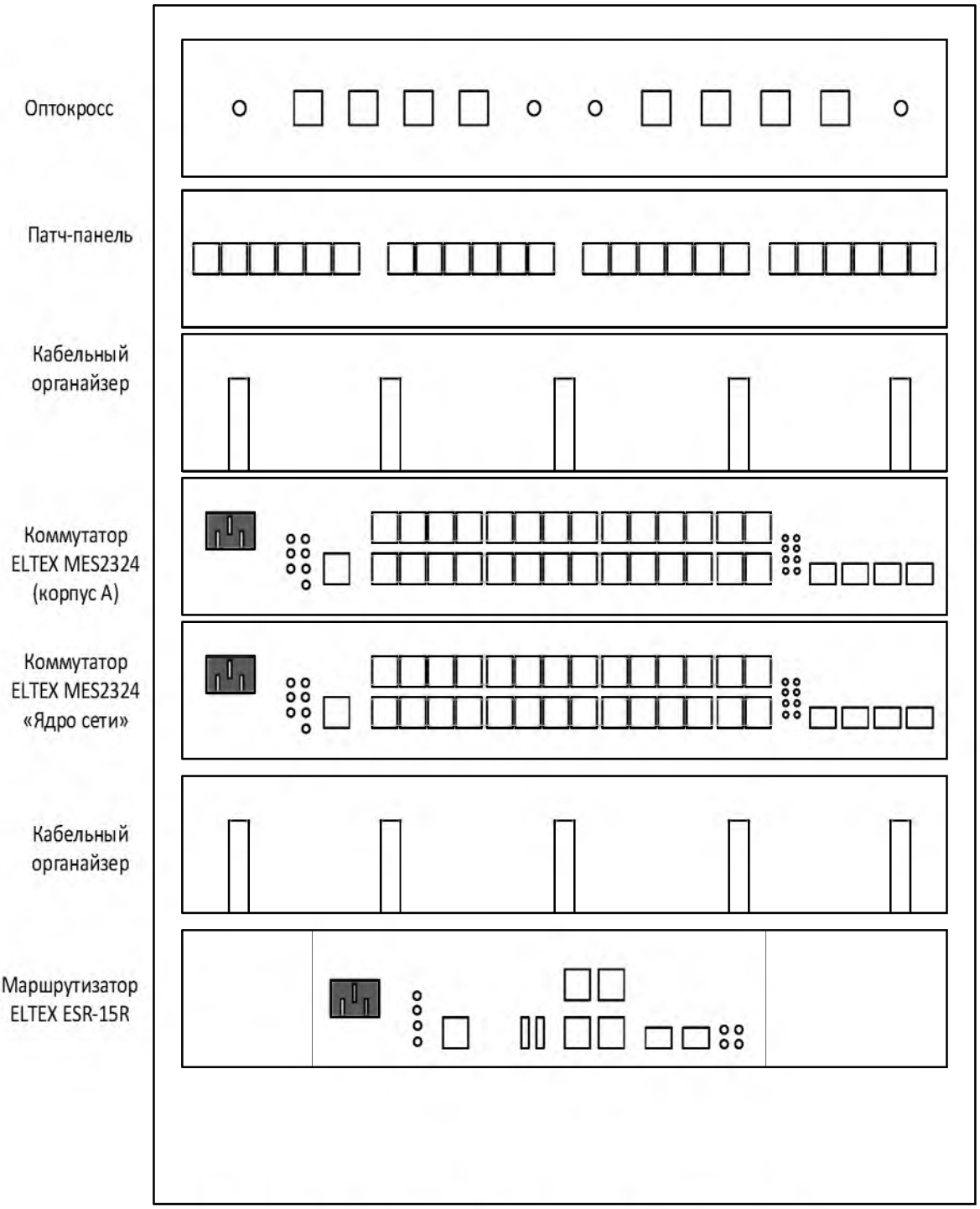

Рисунок 3.1 – Шкаф коммутации в корпусе А

Состав шкафа приведён в таблице 3.3. Эта структура обеспечивает удобный доступ к оборудованию, аккуратную разводку кабелей и возможность наращивания числа портов за счёт установки дополнительного коммутатора.

Таблица 3.2 – Сравнение вариантов активного оборудования

Производ. / класс	Стоимость (отн.)	Функциональность (VLAN, QoS, PoE и др.)	Доступность и поддержка в РФ	Сложность администр.	Итоговая оценка для проекта
ELTEX (ESR, MES, WEP/WOP)	Средняя	Полный набор необходимых функций, PoE-модели	Высокая	Средняя	Оптимален (выбран)
Cisco / HPE Aruba	Высокая	Широкий функционал, расширенные возможности	Средняя / ограниченная	Выше средней	Избыточен по цене
MikroTik / TP-Link SMB	Низкая	Достаточен для базовых задач, PoE-модели	Высокая	Средняя	Возможен, но не идеален по надёжности и поддержке

Таблица 3.3 – Состав элементов коммутационного шкафа

№ п/п	Элемент шкафа	Кол-во, шт.	Назначение
1	Настенный шкаф 19" 10U	1	Размещение активного и пассивного оборудования
2	Маршрутизатор ELTEX ESR-15R	1	Подключение к провайдеру, маршрутизация, firewall
3	Коммутатор ELTEX MES2324	2	Ядро ЛВС. Агрегация корпуса А
4	Оптический кросс 12 портов	1	Оконцовкаоптический линий
5	Патч-панель UTP Cat.5e/Cat.6, 24 порта	1	Коммутация медных линий к АРМ и точкам доступа
6	Кабельные органайзеры	2–3	Укладка и организация патч-кордов
7	Источник бесперебойного питания (ИБП)	1	Резервное питание активного оборудования
8	Патч-корды (оптические и медные)	комплект	Соединение кросса, патч-панели и активного оборудования

3.1.3 Структура ЛВС корпуса Б

Корпус Б предназначен для размещения отдыхающих и ориентирован на обеспечение беспроводного доступа в Интернет и к внутренним гостиничным сервисам. Здесь планируется:

- коммутационный шкаф, установленный в служебном помещении;
- коммутатор доступа (ELTEX MES2324);
- патч-панель для медных линий к точкам доступа Wi-Fi (рисунок 3.2).

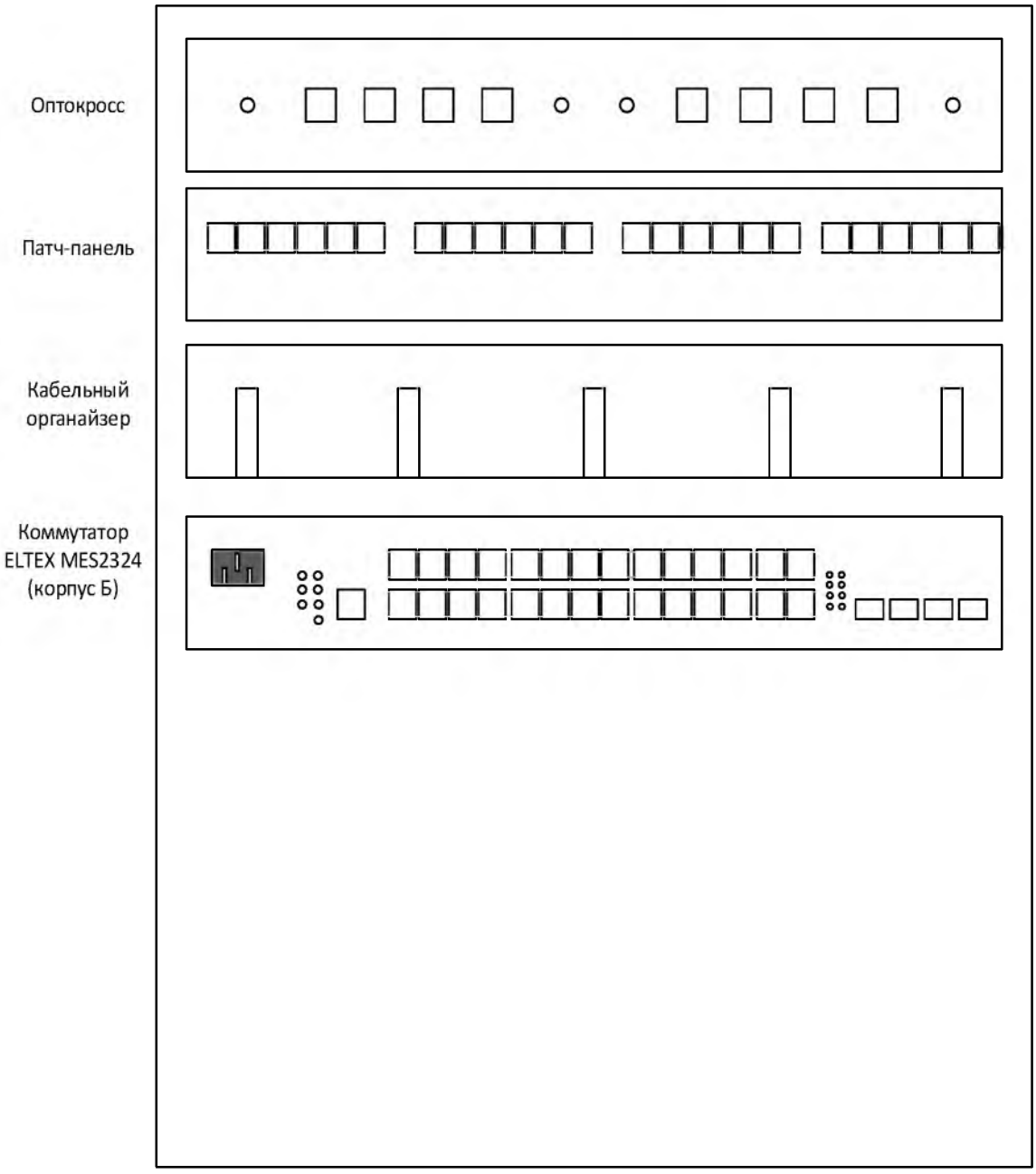

Рисунок 3.2 – Шкаф коммутации в корпусе Б

На каждом из трёх этажей корпуса Б устанавливаются по две внутренние точки доступа Wi-Fi – всего 6 внутренних точек. Они размещаются в коридорах на противоположных концах, что позволяет обеспечить равномерное покрытие всех номеров и общих зон[27]. На фасаде корпуса также устанавливается одна внешняя точка доступа, обеспечивающая покрытие прилегающей территории и части двора[18]. Расположение точек доступа по корпусам и территории сведено в таблицу 3.4.

Таблица 3.4 – Параметры и назначение точек доступа Wi-Fi

ID точки	Корпус / зона	Тип (внутр./внеш.)	Этаж/расположение	Сегмент (SSID)	Примечание
AP-A-1	Корпус А	Внутренняя	1 этаж, коридор	Staff, Guest	Офисная зона
AP-A-2	Корпус А	Внутренняя	1 этаж, холл/ресепшн	Staff, Guest	Покрытие зоны приёма
AP-A-3	Корпус А	Внутренняя	2 этаж, коридор	Staff	Офисные помещения
AP-A-4	Корпус А	Внутренняя	2 этаж, конференц-зона (если есть)	Staff, Guest	Резерв под мероприятия
AP-A-5	Корпус А	Внутренняя	3 этаж, коридор	Staff	Административные помещения
AP-A-6	Корпус А	Внутренняя	3 этаж, ближе к серверной	Staff	Надёжный сигнал для IT
AP-A-OUT	Корпус А	Внешняя	Фасад, ближе к входу	Guest	Территория у корпуса А
AP-B-1	Корпус Б	Внутренняя	1 этаж, коридор	Guest	Номера 1 этажа
AP-B-2	Корпус Б	Внутренняя	1 этаж, зона ресепшн/холл	Guest	Зона ожидания
AP-B-3	Корпус Б	Внутренняя	2 этаж, коридор	Guest	Номера 2 этажа
AP-B-4	Корпус Б	Внутренняя	2 этаж, противоположный конец коридора	Guest	Равномерное покрытие
AP-B-5	Корпус Б	Внутренняя	3 этаж, коридор	Guest	Номера 3 этажа
AP-B-6	Корпус В	Внутренняя	3 этаж, противоположный конец коридора	Guest	Равномерное покрытие
AP-B-OUT	Корпус Б	Внешняя	Фасад, в сторону двора	Guest	Территория у корпуса Б
AP-GATE	Территория	Внешняя	Пост охраны, въезд	Guest (при необходимости), Tech	Покрытие парковки и КПП

3.1.4 Организация Wi-Fi-покрытия

Wi-Fi-сеть гостиницы решает две ключевые задачи: предоставление гостевого доступа в Интернет для постояльцев и обеспечение служебного доступа сотрудников к внутренним системам с мобильных устройств (ноутбуки, планшеты, смартфоны).

Для этого на точках доступа настраивается минимум два SSID:

– MARRIAGE-GUEST – гостевая сеть, работающая через портал авторизации, выдающий индивидуальные коды доступа гостям; [28]

– MARRIAGE-STAFF – служебная сеть, доступная только сотрудникам по WPA2/WPA3-Enterprise с аутентификацией по учётным данным.

Карта точек доступа и их назначение описаны в таблице 3.4. На её основе выполняется предварительное радиопланирование: выбираются каналы, мощность передатчика, оценивается перекрытие зон покрытия. В случае 2,4 ГГц каналы подбираются так, чтобы соседние точки не создавали существенную взаимную интерференцию; в диапазоне 5 ГГц используется больше свободных каналов, что упрощает настройку[26].

3.1.5 Выбор активного оборудования и сравнительный анализ

На этапе эскизного проектирования был проведён сравнительный анализ нескольких вариантов активного оборудования:

– решения ELTEX (ESR-серия и MES-серия коммутаторов, точки доступа WEP/WOP);

– решения Cisco / HPE Aruba;

– решения MikroTik и TP-Link SMB-класса.

– Для каждого варианта оценивались:

– функциональные возможности (поддержка VLAN, QoS, PoE, средств безопасности);

– стоимость оборудования и лицензий;

– доступность на рынке, наличие сервисной поддержки;

– удобство администрирования и документации;

– перспективы масштабирования.

Результаты анализа отражены в таблице 3.2. Для текущих условий проекта, когда заказчик ориентирован на минимизацию затрат и при этом требует промышленного уровня надёжности, оптимальным был признан выбор оборудования ELTEX, т.к. стоимость ниже, чем у решений корпоративного уровня глобальных вендоров, достаточный набор функций для сегментации сети, реализации приоритезации трафика (QoS) и обеспечения безопасности, наличие PoE-моделей, что позволяет питать точки доступа или IP-камеры по тому же кабелю, по которому передаются данные, а также поддержка русскоязычной документации и технической поддержки.

Выбор отечественного или дружественного поставщика дополнительно снижает риски, связанные с санкциями и ограничениями поставок.

Таким образом, в ЛВС принимаются:

– маршрутизатор ELTEX ESR-15R в качестве граничного устройства и межсетевого экрана;

– коммутаторы ELTEX MES2324 – в качестве ядра в корпусе А и коммутаторов доступа в корпусе А иБ;

– внутренние и внешние точки доступа стандарта 802.11ac, обеспечивающие работу нескольких SSID и поддержку современных механизмов безопасности.

3.1.6 Пассивная инфраструктура и кабельная система

Пассивная инфраструктура строится на основе принципов структурированной кабельной системы (СКС) и включает:

– магистральную оптическую линию между корпусами с запасом минимум до 4 волокон (два рабочих и два резервных);

- горизонтальные медные линии категории не ниже Cat.5e или Cat.6, соединяющие коммутационный шкаф с рабочими местами и внутренними точками доступа;
- внешние оптические или экранированные медные кабели к точкам доступа на фасадах и посту охраны;
- настенные и напольные каналы, кабельные лотки, гофротрубы в тех местах, где прокладка выполняется скрытым способом.

Все линии подлежат маркировке в соответствии с принятой системой обозначений. Это упрощает дальнейшую эксплуатацию и диагностику неисправностей. Структура шкафа и состав элементов пассивной части были приведены в таблице 3.3.

3.1.7 Логическая структура сети: VLAN, IP-адресация и маршрутизация

Логическую структуру ЛВС формируют несколько изолированных сегментов, реализованных на базе VLAN:

- VLAN 10 – административные рабочие места (директор, бухгалтерия, кадры);
- VLAN 20 – служба размещения (ресепшн, бюро бронирования);
- VLAN 30 – служба безопасности и система видеонаблюдения;
- VLAN 40 – IT-служба и серверная инфраструктура;
- VLAN 50 – гостевой Wi-Fi;
- VLAN 60 – технические сервисы (системы контроля доступа, «умный номер», IoT-устройства).

План IP-адресации по подсетям приведён в таблице 3.5. Для каждого VLAN выделена отдельная подсеть класса C (маска /24), что обеспечивает необходимый запас адресов и упрощает администрирование. В качестве шлюзов по умолчанию выступает маршрутизатор ESR-15R, на котором также настраиваются правила межсетевого экранирования [16]:

– полный запрет прямого доступа из гостевого VLAN 50 ко всем служебным подсетям;

– разрешение инициировать исходящие подключения из служебных сегментов в Интернет;

– ограничение межсегментного взаимодействия только необходимыми сервисами (например, доступ службы размещения к серверу базы данных в VLAN 40).

Применение VLAN позволяет физически использовать общую кабельную инфраструктуру и коммутаторы, но логически разделить трафик разных служб, усиливая безопасность и управляемость [14].

Таблица 3.5 – План IP-адресации и VLAN-сегментации

VLAN	Назначение сегмента	Диапазон IP-адресов	Маска	Пример адреса шлюза	Тип пользователей / устройств
10	Административные АРМ	192.168.10.0 – 192.168.10.255	/24	192.168.10.1	Директор, бухгалтерия, отдел кадров
20	Служба размещения	192.168.20.0 – 192.168.20.255	/24	192.168.20.1	Бюро размещения, стойка ресепшн
30	Безопасность и видеонаблюдение	192.168.30.0 – 192.168.30.255	/24	192.168.30.1	Видеокамеры, рабочее место службы безопасности
40	IT и серверы	192.168.40.0 – 192.168.40.255	/24	192.168.40.1	Серверы, АРМ IT
50	Гостевой Wi-Fi	192.168.50.0 – 192.168.50.255	/24	192.168.50.1	Устройства гостей
60	Технические сервисы и IoT	192.168.60.0 – 192.168.60.255	/24	192.168.60.1	Системы «умного» номера, контроль доступа и т.п.

3.2 Описание планируемой практической реализации проекта на площадке заказчика, обоснование технической эффективности

В данном подразделе описывается последовательность практических действий по реализации ЛВС в гостинице «Марьяж», а также раскрываются технические преимущества выбранных решений.

3.2.1 Последовательность внедрения

Внедрение проекта ЛВС рекомендуется выполнять поэтапно.

Этап 1. Подготовительные работы

- анализ и уточнение строительных чертежей корпусов А и Б, определение трасс кабельных лотков и мест установки шкафов;
- выбор и согласование мест размещения точек доступа Wi-Fi (внутренних и внешних);
- уточнение перечня активного и пассивного оборудования на основе спецификации;
- разработка рабочей документации (кабельные планы, схемы коммутации, планы размещения оборудования).

Этап 2. Прокладка пассивной инфраструктуры

- монтаж настенных и потолочных кабельных каналов, лотков;
- прокладка магистрального оптического кабеля между корпусами;
- прокладка медных линий от коммутационных шкафов до рабочих мест и точек доступа;
- монтаж и маркировка розеток, патч-панелей, оптического кросса;
- проверка целостности линий простыми средствами (прозвонка, визуальные тесты).

Этап 3. Установка активного оборудования

- монтаж коммутационных шкафов в корпусах А и Б;
- установка маршрутизатора ESR-15R, коммутаторов MES2324, медиаконвертеров, ИБП;
- подключение внешних линий провайдера к маршрутизатору;
- подключение кросса и патч-панелей к активному оборудованию через патч-корды.

Этап 4. Первичная настройка и тестирование

- базовая настройка маршрутизатора (IP-адресация, VLAN-интерфейсы, правила NAT и firewall);

– настройка коммутаторов (VLAN, trunk-порты к маршрутизатору, access-порты к конечным устройствам);

– настройка точек доступа Wi-Fi (SSID, параметры безопасности, гостевой портал);

– проверка связи между сегментами, доступности Интернет, работы служебных приложений.

Этап 5. Интеграция с информационными системами

– подключение серверов бронирования, учёта, видеонаблюдения;

– настройка доступов для пользователей согласно их ролям;

– включение журналирования событий (syslog, SNMP-ловушки) на маршрутизаторе и коммутаторах;

– при необходимости – организация VPN-каналов к внешним системам и облачным сервисам.

Этап 6. Опытная эксплуатация

– запуск сети в эксплуатацию на ограниченный период (1–3 месяца) в режиме особого контроля;

– сбор статистики по инцидентам и производительности;

– анализ отзывов персонала и гостей;

– корректировка конфигураций (приоритизация трафика, изменения в политике доступа, оптимизация Wi-Fi-покрытия).

План испытаний и критерии приёмки сформирован в таблице 3.6, которая может быть использована как основа для приёмочной документации.

Таблица 3.6 – План испытаний и критерии приёмки ЛВС

Вид испытания	Описание проверки	Ожидаемый результат	Критерий успешности	Ответственный
Тест пассивной кабельной системы	Проверка медных линий тестером, измерение оптики	Все линии соответствуют категории, потери в норме	Не более 5 % линий с замечаниями	Подрядчик СКС

Продолжение таблицы 3.6

Проверка VLAN и маршрутизации	Пинг между сегментами, трассировка, доступ к шлюзам	Сегменты изолированы, доступ по правилам firewall	Нет несанкционированного доступа	IT-специалист
Тест гостевого Wi-Fi и портала	Подключение с разных устройств, авторизация, логирование	Успешная авторизация, запись данных сессий	100 % тестовых сеансов в журнале	IT-специалист
Нагрузочное тестирование	Одновременная работа N пользователей	Стабильная работа, задержки в допустимых пределах	Не более 5 % потери пакетов, ping< 50 мс	IT + подрядчик
Тест отказоустойчивости	Отключение/включение отдельных устройств и питания	Восстановление сети согласно регламенту	Время восстановления критичных узлов ≤ 4 ч	IT-специалист
Опытная эксплуатация	Работа сети в реальных условиях 1–3 месяца	Отсутствие критичных инцидентов	Не более X критичных инцидентов за период	Комиссия

3.2.2 Техническая эффективность выбранных решений

К основным показателям технической эффективности проектируемой ЛВС относятся:

- Пропускная способность. Использование гигабитных соединений в магистрали и на портах коммутаторов ядра обеспечивает достаточный запас по скорости для передачи трафика, видеонаблюдения и гостевого Wi-Fi. Горизонтальная подсистема на кабеле категории не ниже Cat.5e поддерживает скорость до 1 Гбит/сдля рабочих мест и точек доступа.

- Надёжность и отказоустойчивость. Наличие ИБП позволяет компенсировать кратковременные перебои электроснабжения. Магистральная оптика имеет запас по каналам, что даёт возможность реализовать резервные

каналы на этапе модернизации. Управляемые коммутаторы позволяют оперативно выявлять проблемные порты и перераспределять нагрузку.

- Масштабируемость. Заказчик заранее обозначил возможное расширение гостиничного комплекса через три и более года. Заложенный резерв портов коммутаторов и волокон в оптическом кабеле позволит подключать новые корпуса и дополнительные точки доступа без радикальной перестройки существующей инфраструктуры.
- Управляемость и контролируемость. Все ключевые элементы сети – маршрутизатор, коммутаторы, точки доступа – поддерживают удалённое управление и мониторинг по защищённым протоколам. Это позволяет IT-службе оперативно реагировать на инциденты, контролировать загрузку каналов и состояние оборудования.
- Безопасность. Логическая сегментация (VLAN) и межсетевой экран на маршрутизаторе обеспечивают разделение служебного и гостевого трафика, минимизируя риски несанкционированного доступа к критичным данным. Портал авторизации пользователей Wi-Fi реализует требования законодательства по учёту фактов оказания услуг связи.

3.2.3 Распределение трафика по сегментам

Для наглядной оценки структуры нагрузки ЛВС сформирована диаграмма распределения трафика по основным сегментам (рисунок 3.1). При расчёте учитывались следующие компоненты:

- гостевойWi-Fi – порядка 55 % общего трафика;
- система видеонаблюдения – около 20 %;
- административные системы – около 15 %;
- служба размещения – 5 %;
- прочие сервисы (IT, технические системы, IP-телефония) – 5 %.

Такое распределение показывает, что наибольшую нагрузку создаёт гостевой трафик, поэтому на этапе эксплуатации важно контролировать

потребление полосы пропускания гостевым сегментом, чтобы не допустить деградации качества для критичных служебных сервисов.

Рисунок 3.1 – Планируемое распределение трафика по сегментам сети

3.3 План тестирования и опытной эксплуатации сети

План испытаний детализирует процедуру проверки работоспособности сети до ввода её в промышленную эксплуатацию и во время опытного периода.

Проверка включает:

1. Испытания пассивной кабельной системы, каждая линия тестируется прибором категории не ниже той, для которой она проектировалась. Для оптического кабеля измеряются потери и отражения. Результаты оформляются в виде протоколов испытаний.

2. Функциональные испытания активного оборудования, выполняется проверка работы VLAN, маршрутизации, правил межсетевого экрана и NAT. Подтверждается, что гостевой сегмент не имеет доступа к служебным подсетям, а служебный трафик не испытывает необоснованных ограничений.

3. Испытания использования Wi-Fi. В контрольных точках на каждом

этаже измеряется уровень сигнала и реальная скорость передачи данных. Проводятся тестовые подключения к гостевой сети, проверяется работа портала авторизации и корректность регистрации сессий.

4. Нагрузочные испытания.

5. Моделируется одновременная работа типового числа пользователей (сотрудников и гостей), проверяется устойчивость сети под нагрузкой. Оценивается задержка, потери пакетов, реакция приложений.

6. Испытания отказоустойчивости. Отрабатываются сценарии отключения отдельных элементов (коммутатора, точки доступа, ИБП), проверяется, насколько быстро и корректно восстанавливается нормальный режим.

7. Опытная эксплуатация. В течение 1–3 месяцев сеть работает в обычном режиме, но под тщательным наблюдением IT-службы. Ведётся учёт всех инцидентов, на основе чего формируется статистика (по ней впоследствии строится диаграмма инцидентов – рисунок 3.2).

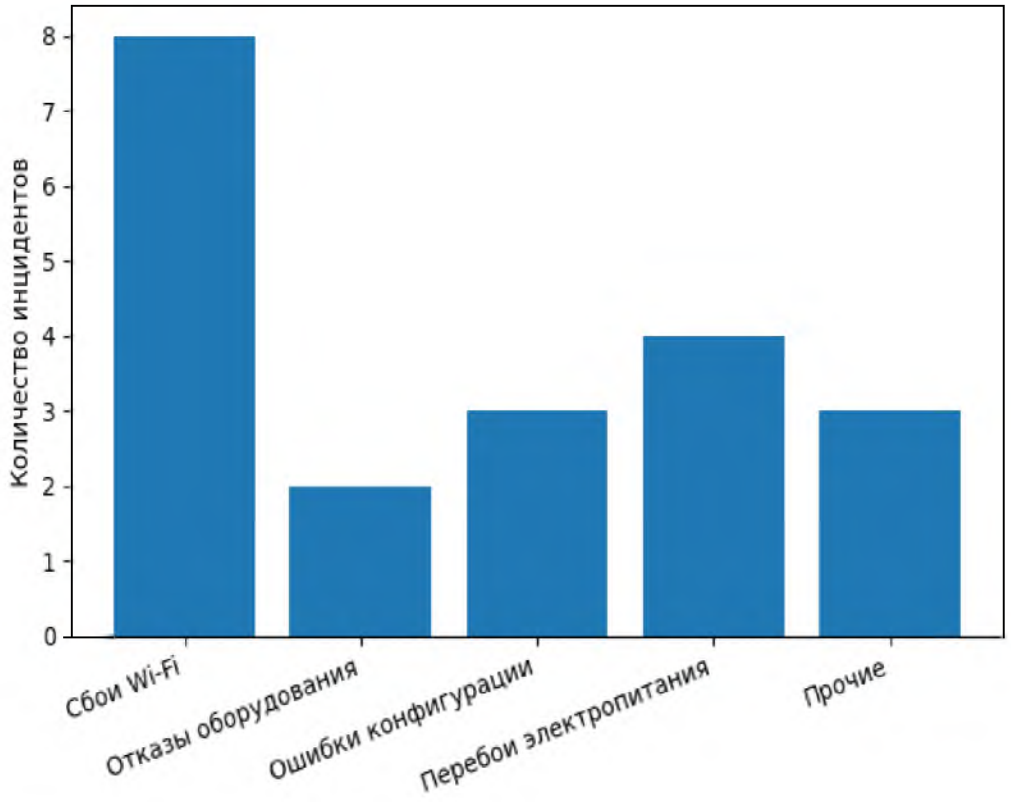

Рисунок 3.2 – Распределение инцидентов за период опытной эксплуатации

По завершении опытной эксплуатации комиссия делает вывод о готовности сети к реальной эксплуатации, при необходимости формирует перечень доработок.

Итоговая схема сети приведена на рисунке 3.3.

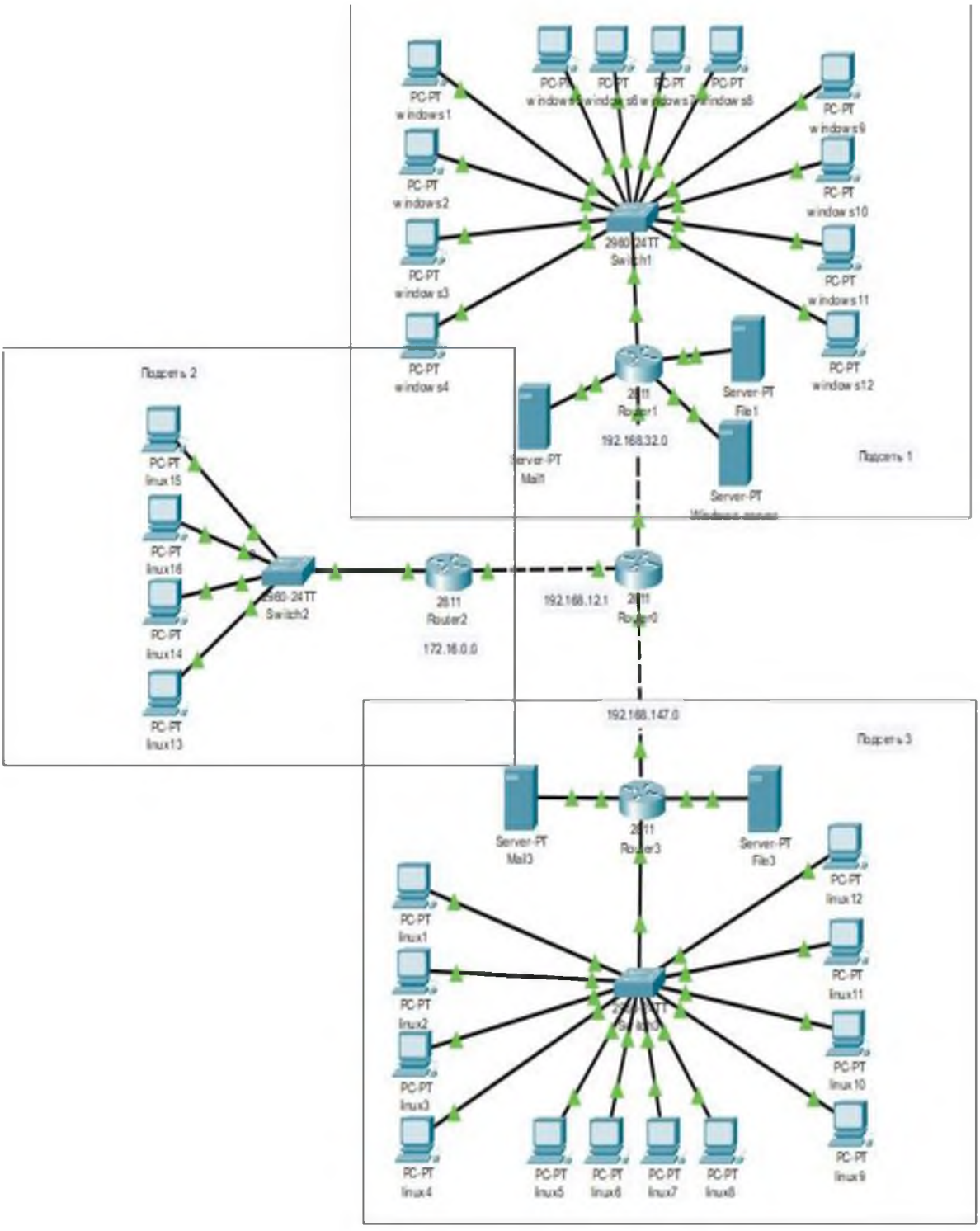

Рисунок 3.3 – Спроектированная схема сети

3.4 Обеспечение информационной безопасности и защиты персональных данных в ЛВС гостиницы

3.4.1 Нормативные требования к защите информации и персональных данных

Гостиница в рамках своей деятельности обрабатывает значительные объемы персональных данных (ПДн) клиентов и сотрудников: Ф.И.О., паспортные данные, адрес проживания, контактные телефоны и e-mail, сведения о бронировании, платежной активности и т.д. В соответствии с Федеральным законом № 152-ФЗ «О персональных данных» гостиница выступает оператором персональных данных и обязана обеспечивать их защиту при обработке в информационных системах персональных данных (ИСПДн)[1].

Общие требования к защите информации и к применению информационных технологий определяются Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации», задающим базовые принципы обеспечения конфиденциальности, целостности и доступности информации[2].

С точки зрения телекоммуникационной инфраструктуры проектируемая ЛВС и организуемые через нее услуги доступа в сеть Интернет должны соответствовать требованиям Федерального закона № 126-ФЗ «О связи», регулирующего отношения между пользователями, оператором связи и оператором информационной системы[3].

Для обработки ПДн в информационных системах оператора действуют специальные подзаконные акты:

- Постановление Правительства РФ № 1119 от 01.11.2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» – определяет уровни защищенности ПДн и общие требования к системе защиты персональных данных.

- Приказ ФСТЭК России № 21 от 18.02.2013 г. – устанавливает состав и

содержание организационных и технических мер по обеспечению безопасности ПДн для каждого уровня защищенности ИСПДн[6].

- Методики определения актуальных угроз безопасности ПДн ФСТЭК России от 2021 г.

Кроме того, для построения структурированной кабельной системы (СКС) и стационарной части ЛВС должны учитываться требования ГОСТ Р 53246-2008 (информационные технологии, структурированные кабельные системы) и стандартов на проектирование СКС, регламентирующих структуру подсистем и требования к кабелям, розеткам и кроссовому оборудованию[10].

Отдельный блок требований касается организации публичногоWi-Fi-доступа. Идентификация пользователей публичных Wi-Fi-сетей возложена на оператора связи, предоставляющего услуги доступа в Интернет: соответствующие требования формировались Постановлением Правительства РФ № 758 от 31.07.2014 (впоследствии утратившим силу, но его положения были учтены в обновленных правилах оказания услуг связи). Это означает, что при проектировании гостевого Wi-Fi гостиница должна либо использовать решения оператора связи с уже реализованной функцией идентификации (SMS-портал, авторизация через портал Госуслуг и т.п.), либо обеспечить интеграцию собственной системы аутентификации с платформой оператора.

С учетом указанных документов гостиница должна:

- определить состав ИСПДн (системы бронирования, бухгалтерский учет, HR, видеонаблюдение, системы контроля доступа и др.);

- отнести каждую ИСПДн к соответствующему уровню защищенности в соответствии с ПП РФ № 1119[5];

- разработать и реализовать систему защиты ПДн, включающую организационные и технические меры по Приказу ФСТЭК России № 21;

- при организации гостевого Wi-Fi обеспечить выполнение требований законодательства в части идентификации пользователей и хранения логов доступа.

3.4.2 Классификация и потоки персональных данных в ЛВС гостиницы

В ЛВС гостиницы обрабатываются ПДн нескольких основных категорий субъектов:

- клиенты (гости гостиницы);
- сотрудники гостиницы;
- контрагенты (юридические лица и ИП, представители туроператоров и т.д.).

Основные виды ПДн и их размещение в ЛВС можно представить в виде таблицы.

Таблица 3.4.1 – Категории персональных данных и их обработка в ЛВС гостиницы

Категория субъекта	Примеры обрабатываемых данных	Основные системы / узлы ЛВС	Уровень критичности
Гости	Ф.И.О., паспортные данные, гражданство, контактные данные, сведения о брони, информация о проживании, данные о платежах	PMS/система управления гостиницей, учетные базы 1С, база бронирования, рабочие места службы размещения и бухгалтерии	Высокий (ПДн, в т.ч. специальные категории при наличии)
Сотрудники	Ф.И.О., паспортные данные, ИНН, СНИЛС, трудовые договоры, данные о зарплате и премиях	Система кадрового учета, 1С:Зарплата и управление персоналом, рабочие места HR и бухгалтерии	Высокий
Контрагенты	Ф.И.О. контактных лиц, служебные координаты, реквизиты договоров	CRM, система документооборота, бухгалтерские системы	Средний
Посетители Wi-Fi	Номер телефона, IP-адрес, MAC-адрес, учетные записи для авторизации	Гостевой Wi-Fi-портал, лог-сервер, оборудование оператора связи	Средний

На основе таблицы видно, что критически важными зонами ЛВС в контексте ПДн являются серверный сегмент, рабочие места администратора гостиницы, бухгалтерии, отдела кадров и службы безопасности, а также зоны, через которые проходит трафик гостевого Wi-Fi (для хранения логов, идентификаторов и событий доступа)[8].

Для каждой из ИСПДн проводится детализация:

- перечень обрабатываемыхПДн;

- способы их обработки (сбор, запись, систематизация, хранение, передача);

- перечень пользователей и их ролей;

- каналы взаимодействия (локальные подключения, удаленный доступ, гостевой Wi-Fi).

Результаты анализа используются далее при построении модели угроз и выборе уровня защищенности в соответствии с ПП РФ № 1119 и Приказом ФСТЭК № 21.

3.4.3 Модель угроз и уровни защищенности ИСПДн гостиницы

В соответствии с Методикой ФСТЭК по определению актуальных угроз и требованиями ПП РФ № 1119 оператор ПДн обязан:

1. Определить круг актуальных угроз безопасности ПДн для каждой ИСПДн.
2. Определить уровень защищенности ПДн (УЗ-1…УЗ-4).
3. Выбрать набор организационных и технических мер по Приказу ФСТЭК № 21, соответствующий выбранному уровню[5].

Для ЛВС гостиницы можно выделить следующие группы угроз:

- несанкционированный доступ к информационным ресурсам (подбор паролей, использование учетных записей уволенных сотрудников, подмена прав доступа);

- утечка ПДн через незащищенные каналы связи (гостевой Wi-Fi, удаленный доступ, переносные носители);

- вредоносное ПО и атаки из сети Интернет (компрометация рабочих мест через фишинг, заражение серверов, кража базы клиентов);

- ошибки персонала (неправильная отправка документов, публикация ПДн, отключение антивируса и т.п.);

- физический доступ к оборудованию (кража ноутбука с базой ПДн, подключение постороннего устройства к порту ЛВС, доступ в серверную и к шкафам коммутации)[7].

Для целей дипломного проекта допускается обоснованно принять, что ИСПДн гостиницы относится к третьему или четвертому уровню защищенности ПДн (в зависимости от состава ПДн и числа субъектов), что соответствует типовой негосударственной ИСПДн, обрабатывающей «обычные» персональные данные без биометрии и без сведений, отнесенных к государственной тайне. Окончательное отнесение уровня защищенности в реальном проекте выполняется заказчиком на основании требований ПП РФ № 1119 [5].

3.4.4 Организационные меры по обеспечению безопасности ПДн

Организационные меры определяют «правила игры» для персонала и пользователей, а технические средства только обеспечивают их выполнение. На основе Приказа ФСТЭК № 21 и методических рекомендаций по защите ПДн для гостиницы целесообразно реализовать следующий комплекс организационных мер:

- утверждение Политики оператора в отношении обработки ПДн и положения о защите ПДн в гостинице;

- назначение ответственного за организацию обработки и защиту ПДн;

- утверждение перечня ИСПДн, перечня обрабатываемых ПДн и требований к их защите;

- разработка и введение внутренних регламентов:

- по разграничению доступа к ИСПДн;

- по учету, хранению и уничтожению носителей информации;

- по резервному копированию и восстановлению данных;

- по использованию гостевого Wi-Fi и корпоративного доступа в Интернет;

- заключение с сотрудниками соглашений о конфиденциальности, включающих ответственность за разглашение ПДн;

- организация обучения и инструктажа персонала по защите ПДн и безопасной работе в ЛВС;

- ведение журналов учета носителей, журналов доступа в серверные помещения и помещения с сетевым оборудованием;

- регламентация порядка подключения собственных устройств сотрудников (BYOD) к корпоративной сети (при необходимости – полный запрет либо использование отдельного сегмента).

Эти меры должны быть увязаны с техническими решениями, заложенными в проектируемую ЛВС: разделением сетей, контролем доступа, регистрацией событий безопасности и др.

3.4.5 Технические меры защиты в проектируемой ЛВС

На основе требований Приказа ФСТЭК № 21 и анализа угроз для ЛВС гостиницы формируется набор технических мер, отражающий архитектуру, предложенную в проекте.

1. Сегментация сети.

Выделение отдельных VLAN/подсетей для:

- административных рабочих мест (руководство, бухгалтерия, отдел кадров);

- технических служб (ИТ, служба безопасности);

- гостевого Wi-Fi;

- систем видеонаблюдения и контроля доступа;

- серверов и ИСПДн (PMS, бухгалтерские системы, файловые серверы).

Сегментация позволяет существенно снизить риск распространения атак и утечек из гостевого сегмента в корпоративную часть.

2. Межсетевое экранирование и фильтрация трафика.

Установка межсетевого экрана между:

- ЛВС гостиницы и сетью Интернет;

- гостевым Wi-Fi и корпоративной ЛВС;

- административными сегментами и серверным сегментом. На межсетевых экранах задаются правила фильтрации по принципу «запрещено все, что явно не разрешено», а также включается контроль прикладного трафика (в том числе HTTPS) с использованием современных средств защиты.

3. Идентификация и аутентификация пользователей.

Введение персонифицированных учетных записей пользователей (запрет общих «учёток»).

Использование централизованной службы каталогов (например, AD) для управления правами.

Ограничение привилегий (принцип наименьших прав).

4. Защита каналов передачи данных.

- Использование шифрования трафика (HTTPS, VPN) при удаленном доступе к ИСПДн (например, из дома администратора);

- Шифрование каналов соединения между корпусами гостиницы (по возможности – через IPSec-туннели или L2 VPN поверх магистральных каналов оператора).

5. Антивирусная защита и защита от вредоносного ПО.

Установка антивирусного ПОна рабочих станциях и серверах, использование централизованного управления политиками защиты;

Контроль запуска приложений, фильтрация вложений в электронной почте, блокировка вредоносных URL.

6. Контроль внешних устройств и носителей.

Ограничение подключения USB-носителей и внешних дисков к рабочим местам, на которых обрабатываются ПДн;

При необходимости – использование специализированного ПО для контроля подключаемых устройств.

7. Резервное копирование и восстановление.

Регулярное резервное копирование баз ПДн и критичных сервисов на выделенный сервер или сетевое хранилище;

Хранение резервных копий в отдельной защищенной зоне, периодическая проверка восстановления.

8. Регистрация событий безопасности и аудит.

Настройка журналирования:

- входов в учетные записи;
- доступа к базам ПДн;
- администраторских действий;
- конфигурационных изменений на сетевом оборудовании.

Центральный сбор логов (syslog/СЗИ мониторинга) с возможностью анализа инцидентов.

3.4.6 Обеспечение безопасности гостевого Wi-Fi и публичного доступа

Особое внимание следует уделить сегменту гостевогоWi-Fi, так как он является одновременно:

- ключевым сервисом для клиентов гостиницы;
- потенциальным источником угроз как для ЛВС, так и для юридической ответственности оператора.

С учетом действующих правил оказания услуг связи и требований к идентификации пользователей публичных Wi-Fi-сетей гостинице рекомендуется:

- организовать гостевой Wi-Fi на базе оборудования оператора связи или совместно с ним, чтобы идентификация пользователей (по SMS, по учетной записи на портале) и хранение логов осуществлялись на оборудовании оператора в соответствии с требованиями законодательства;
- физически и логически изолировать гостевой сегмент Wi-Fi от корпоративной ЛВС (отдельный VLAN, отдельный пул адресов, жесткая фильтрация на межсетевом экране);

- ограничить доступ из гостевой сети только к ресурсам Интернет, запретив доступ к внутренним IP-адресам гостиницы;

- ввести портальный доступ с отображением пользователю политики безопасности и согласия на обработку ПДн при подключении.

3.4.7 Сводная матрица угроз и реализуемых мер

Для наглядного обоснования эффективности предложенных мер целесообразно привести укрупненную матрицу соответствия угроз и реализуемых организационно-технических мер[4].

Таблица 3.4.2 – Соответствие основных угроз и реализуемых мер защиты

№	Угроза	Основные организационные меры	Основные технические меры
1	Несанкционированный доступ к ПДн	Регламенты разграничения доступа, учет прав, соглашения о КИ	Сегментация сети, МЭ, аутентификация, контроль привилегий
2	Утечка ПДн через гостевойWi-Fi	Политика использования гостевого доступа, договор с оператором	Изоляция Wi-Fi, фильтрация, идентификация, логирование
3	Вредоносное ПО и сетевые атаки	Инструктаж персонала, регламент обновлений ПО	Антивирус, МЭ, IDS/IPS, обновление ПО
4	Ошибки и нарушения сотрудниками	Обучение, регламенты обработки ПДн, ответственность	Ограничение функционала, контроль действий администраторов
5	Физический доступ к оборудованию	Пропускной режим, журналы посещений, инструкции по доступу	Замки, видеонаблюдение, контроль доступа к шкафам и серверной
6	Утрата данных вследствие сбоев/ошибок	Регламент резервного копирования, ответственные лица	Резервное копирование, отказоустойчивая инфраструктура

Такая таблица позволяет показать взаимосвязь архитектурных решений ЛВС и требований по ИБ и ПДн, а также продемонстрировать, что предложенный проект обеспечивает комплексную защиту информации с учетом специфики гостиницы.

4 Обоснование экономической эффективности проекта

Раздел содержит технико-экономическое обоснование разработки и внедрения ЛВС в гостинице «Марьяж». В нём рассматривается структура затрат, ожидаемый экономический эффект, рассчитываются базовые показатели эффективности и окупаемости проекта.

4.1 Методические подходы к оценке эффективности

Для оценки экономической эффективности используется классическая схема технико-экономического анализа, включающая определение единовременных капитальных затрат на создание ЛВС, оценку ежегодных эксплуатационных расходов, связанных с обслуживанием сети; определение ежегодного экономического эффекта, включающего:

- снижение трудозатрат персонала;
- уменьшение потерь от простоев и инцидентов;
- сокращение расходов на бумажный документооборот и связь;
- потенциальный рост выручки за счёт повышения привлекательности гостиницы;

В итоге можно провести расчёт срока окупаемости на заданном сроке планирования.

При расчёте дохода используется норматив приведения разновременных затрат, который в учебных методиках часто принимается на уровне 10–11 % годовых.

4.2 Структура единовременных затрат проекта ЛВС

Единовременные затраты состоят из стоимости оборудования, работ по монтажу и пусконаладке, а также резерва на непредвиденные расходы. Структура этих затрат представлена в таблице 4.1.

Таблица 4.1 – Структура единовременных затрат проекта ЛВС

Статья затрат	Кол-во	Ориентир.стоимость за единицу, тыс. руб.	Сумма, тыс. руб.
Маршрутизатор ELTEX ESR-15R	1	80	80
Коммутаторы ELTEX MES2324 (ядро+доступ)	3	40	120
Точки доступа Wi-Fi внутренние	12	8	96
Точки доступа Wi-Fi внешние	3	15	45
ИБП для серверной и шкафа корпуса Б	2	35	70
Коммутационные шкафы (корпус А и Б)	2	20	40
Кабели, патч-панели, кроссы, расходники	комплект	–	120
Сервер / шлюз авторизации пользователей	1	90	90
Проектные работы	–	–	80
Монтажные и пусконаладочные работы	–	–	120
Обучение персонала	–	–	20
Резерв (10 % от суммы выше)	–	–	81
Итого единовременные затраты	–	–	962

Активное оборудование включает маршрутизатор ESR-15R, три коммутатора MES2324 (один – ядро, два – в качестве коммутаторов доступа и/или резерва), 12 внутренних и 3 внешние точки доступа Wi-Fi, а также два ИБП для корпуса А и корпуса Б.

Пассивная инфраструктура это коммутационные шкафы, оптические и медные кабели, патч-панели, оптические кроссы, розетки, монтажные материалы. Эта статья во многом зависит от конкретных цен и объёмов работ, поэтому в расчётах используется агрегированная оценка.

Программное обеспечение включает сервер или специализированный шлюз авторизации пользователей Wi-Fi, лицензии на необходимые

программные продукты (если они закупаются в составе проекта).

Проектные и монтажные работы включают разработку рабочей документации, прокладку кабельных линий, установку оборудования, тестирование и наладку.

Резерв обычно принимается в пределах 5–10 % от суммы остальных затрат и предназначен для покрытия непредвиденных расходов (изменения цен, необходимость докупить расходные материалы и т.п.).

Для наглядности структура капитальных затрат представлена на диаграмме 4.1, где видно долевое участие каждой статьи расходов в общей стоимости проекта.

Рисунок 4.1 – Структура затрат проекта

4.3 Годовой экономический эффект от внедрения ЛВС

Экономический эффект формируется за счёт

1. Сокращения трудозатрат персонала. Автоматизация процессов бронирования, учёта и документооборота позволяет сократить время обработки каждой операции. При условной экономии, например, 0,2 человеко-часа на одну операцию и среднем числе операций в день, можно оценить годовую экономию фонда рабочего времени, пересчитанную в денежном выражении.
2. Снижения потерь от простоев. Старая инфраструктура приводила к

периодическим сбоям, в результате чего часть операций задерживалась или срывалась. Новая ЛВС с управляемым оборудованием и ИБП снижает частоту и длительность таких ситуаций. В денежном выражении это выражается в сохранённых доходах и отсутствии штрафов/неустоек.

3. Сокращения расходов на бумажный документооборот и связь. Переход на электронные документы уменьшает потребление бумаги, расходных материалов и снижает затраты на хранение документов. Внедрение IP-телефонии сокращает расходы на междугороднюю и мобильную связь.

4. Рост выручки за счёт повышения привлекательности гостиницы. Наличие надёжногоWi-Fi является важным фактором при выборе гостиницы. При прочих равных условиях гостиница с современной телекоммуникационной инфраструктурой может рассчитывать на более высокую загрузку номерного фонда и повышение лояльности клиентов.

Сводный годовой экономический эффект по основным статьям приведён в таблице 4.2.

Таблица 4.2 – Годовой экономический эффект и показатели эффективности

Статья эффекта / показателя	Значение	Обоснование
Экономия трудозатрат персонала, тыс. руб./год	180	Сокращение времени операций, повышение производительности
Снижение потерь от простоев, тыс. руб./год	80	Меньше отмен/сбоев при заселении, работе систем
Экономия на бумажном документообороте, тыс. руб./год	20	Переход на электронные документы
Снижение затрат на связь (IP-телефония), тыс. руб./год	30	Перевод части звонков во внутреннюю сеть
Рост выручки из-за повышенной привлекательности, тыс. руб./год	120	Дополнительная загрузка номерного фонда
Суммарный годовой эффект, тыс. руб./год	430	Э = сумма строк выше
Доп. эксплуатационные расходы (обслуживание ЛВС), тыс. руб./год	80	Сервис, электроэнергия, лицензии
Чистый годовой экономический эффект, тыс. руб./год	350	Эч = 430 – 80
Единовременные затраты $З_0$, тыс. руб.	962	Из таблицы 4.1
Простой срок окупаемости, лет	≈ 2,7	Ток = $З_0$ / Эч ≈ 962 / 350

На основе данных таблицы рассчитывается суммарный годовой экономический эффект (до вычета эксплуатационных расходов),

дополнительные ежегодные расходы на обслуживание ЛВС и чистый годовой экономический эффект (разность между эффектом и расходами). В нашем проекте чистый эффект составляет порядка 350 тыс. руб. в год.

4.4 Расчёт основных показателей эффективности

На основе оцененных единовременных затрат и годового экономического эффекта рассчитываются базовые показатели эффективности.

Простой срок окупаемости определяется как:

$$T_{ок} = \frac{З_0}{Э_ч},$$

Где $З_0$– единовременные затраты на проект,

$Э_ч$– чистый годовой экономический эффект.

Подставляя ориентировочные значения $З_0 \approx 962$тыс. руб. и$Э_ч \approx 350$тыс. руб./год, получаем:

$$T_{ок} \approx \frac{962}{350} \approx 2{,}7 \text{ года}$$

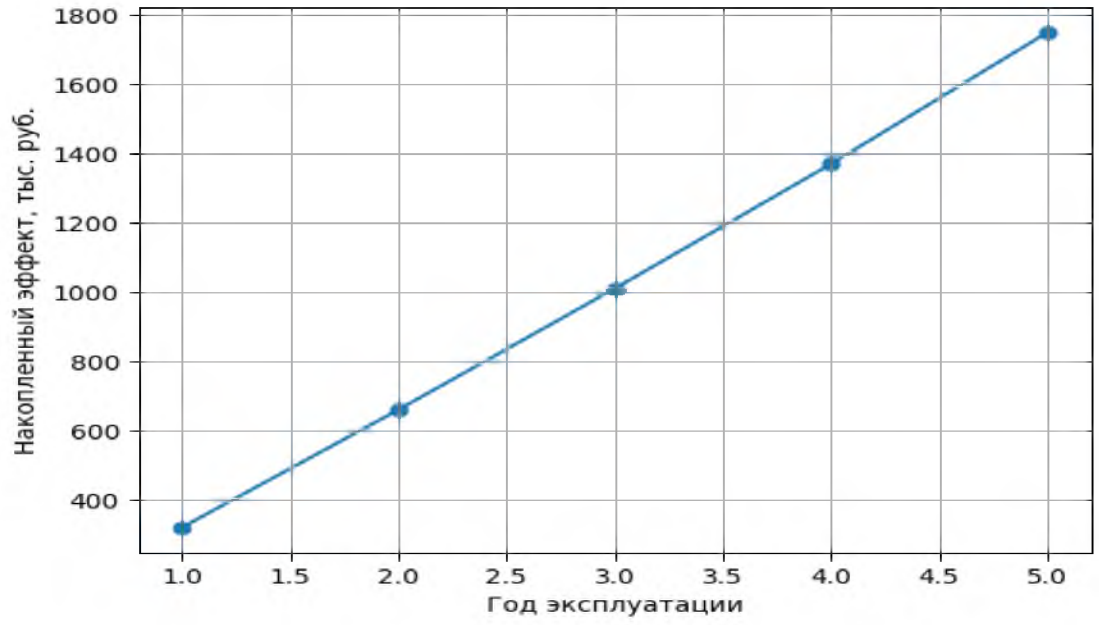

Рисунок 4.2 – Динамика накопленного экономического эффекта

Таким образом, проект окупается между 2-м и 3-м годами эксплуатации. На горизонте 5 лет накопленный экономический эффект превышает первоначальные затраты более чем в 1,8 раза (рисунок 4.2).

Помимо формализуемых финансовых показателей, внедрение ЛВС приносит ряд качественных преимуществ, таких как повышение прозрачности хозяйственных процессов и управляемости гостиницы, улучшение качества обслуживания клиентов за счёт ускорения процессов заселения, расчёта и предоставления дополнительных услуг, повышение информационной безопасности и соответствия требованиям законодательства и создание технологического задела для внедрения новых сервисов (онлайн-регистрация, мобильные ключи, «умные» номера и т.п.).

Эти эффекты сложно точно выразить в денежной форме, однако они прямо влияют на репутацию гостиницы и создают конкурентные преимущества в долгосрочной перспективе.

Заключение

Выпускная квалификационная работа посвящена проектированию локальной вычислительной сети (ЛВС) гостиничного предприятия «Марьяж» с учётом специфики его деятельности, приоритета минимизации текущих затрат и перспективы возможного расширения не ранее чем через три года.

Объект исследования – информационно-телекоммуникационная инфраструктура гостиничного предприятия, основанная на локальной вычислительной сети и обеспечивающая взаимодействие административных, сервисных и гостевых информационных систем.

Предмет исследования – методы, архитектурные решения и технические средства проектирования локальной вычислительной сети гостиницы, включая организацию структурированной кабельной системы, проводного и беспроводного доступа, логической сегментации и сетевой безопасности с учётом нормативных требований и будущего масштабирования.

В процессе выполнения работы решён комплекс задач, определённых во введении.

В аналитической части были рассмотрены особенности деятельности гостиницы как объекта информатизации: наличие административных служб (руководство, бухгалтерия, отдел кадров, IT-служба, служба безопасности), службы размещения, а также корпуса для проживания гостей. На основе анализа бизнес-процессов, потоков данных и требований к качеству обслуживания сформированы основные функциональные и эксплуатационные требования к ЛВС, включая необходимость одновременной поддержки служебного и гостевого трафика, круглосуточной доступности ключевых сервисов и соблюдения требований российского законодательства в области связи и обработки персональных данных.

Во второй главе были разработаны и формализованы требования к проекту сети. С учётом планировочных решений корпусов А и Б определены зоны, где необходимо организовать проводное подключение рабочих мест, а

также размещение внутренних и внешних точек доступа Wi-Fi. Особое внимание уделено юридическим ограничениям при предоставлении гостевого доступа в Интернет (идентификация пользователей, разделение гостевого и служебного трафика), а также нормативным документам по оформлению проектной документации и структурированных кабельных систем. На основании требований заказчика учтена перспектива расширения гостиничного комплекса через три года, что повлияло на выбор магистральной топологии и закладку резервов по портам и оптическим линиям.

В третьей главе разработаны конкретные проектные решения. Обоснован выбор иерархической топологии типа «звезда» с размещением ядра ЛВС в корпусе А и оптической магистралью к корпусу Б. Спроектирована структурированная кабельная система с разделением на магистральную и горизонтальную подсистемы в соответствии с действующими ГОСТами на СКС. Выполнен сравнительный анализ нескольких вариантов активного оборудования разных производителей; с учётом стоимости, функциональности, наличия русскоязычной поддержки и возможности масштабирования выбран вариант на базе управляемых коммутаторов и маршрутизатора уровня малого/среднего бизнеса.

Разработана логическая структура сети с разделением на виртуальные локальные сети (VLAN) для административных служб, службы размещения, систем видеонаблюдения и безопасности, IT-службы, гостевого доступа и технических сервисов. Такое решение позволяет обеспечить изоляцию критичных подсистем от гостевого сегмента, ограничить круг доступных ресурсов и реализовать политики межсетевого экранирования и контроля трафика. Отдельно спроектирована система беспроводного доступа с выделением служебного SSID и гостевого SSID, применением современных методов шифрования и механизмов авторизации пользователей Wi-Fi.

В рамках описания практической реализации сформирован поэтапный план внедрения: от обследования объекта и прокладки кабельной инфраструктуры до настройки активного оборудования, интеграции с

информационными системами гостиницы и проведения опытной эксплуатации. Разработаны предложения по тестированию ЛВС, включающие проверку пассивной подсистемы, функциональные, нагрузочные и отказоустойчивые испытания, а также сбор статистики по инцидентам и качеству сервиса в период опытной эксплуатации.

В четвёртой главе выполнено технико-экономическое обоснование проекта. На основании структуры спецификации оборудования и работ определены единовременные капитальные затраты на создание ЛВС. Оценён годовой экономический эффект от внедрения сети за счёт снижения трудозатрат персонала, уменьшения простоев, сокращения бумажного документооборота и повышения привлекательности гостиницы за счёт качественного Wi-Fi-сервиса. Расчёт простого срока окупаемости показал, что проект окупается в пределах нормативного срока службы оборудования, а накопленный эффект на горизонте пяти лет существенно превышает первоначальные вложения. Это свидетельствует об экономической целесообразности реализации предложенного проекта.

Практическая значимость выполненной работы заключается в том, что разработанные решения могут быть непосредственно использованы при модернизации информационно-телекоммуникационной инфраструктуры гостиницы «Марьяж» или аналогичных объектов малого и среднего гостиничного бизнеса. Представленные схемы, планы размещения оборудования, структура VLAN и методика тестирования могут служить основой для рабочей и эксплуатационной документации.

Теоретическая значимость работы состоит в систематизации подходов к проектированию ЛВС гостиничных предприятий с учётом одновременно трёх групп требований: технологических (пропускная способность, надёжность, масштабируемость), правовых (законодательство о связи, защите информации и персональных данных) и экономических (ограничения по бюджету, требования к сроку окупаемости). Полученные результаты могут быть использованы при дальнейшем исследовании вопросов оптимизации беспроводных сетей,

интеграции систем информационной безопасности, внедрения IP-телефонии и «умных» гостиничных сервисов.

В целом поставленная цель – разработка проекта локальной вычислительной сети гостиницы с учётом специфики её деятельности, приоритета минимизации текущих затрат и возможности масштабирования в среднесрочной перспективе – достигнута. Все основные задачи, обозначенные в работе, выполнены, а сформулированные выводы и рекомендации могут быть использованы как основа для практического внедрения и дальнейшего развития сети.

Список литературы

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Официальный интернет-портал правовой информации. URL: https://pravo.gov.ru (дата обращения: 19.12.2025).

2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Официальный интернет-портал правовой информации. URL: https://pravo.gov.ru (дата обращения: 19.12.2025).

3. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // Официальный интернет-портал правовой информации. URL: https://pravo.gov.ru (дата обращения: 19.12.2025).

4. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Официальный интернет-портал правовой информации. URL: https://pravo.gov.ru (дата обращения: 19.12.2025).

5. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Документы - Правительство России [Электронный ресурс]. URL: http://government.ru (дата обращения: 19.12.2025).

6. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // ФСТЭК России [Электронный ресурс]. URL: https://fstec.ru (дата обращения: 19.12.2025).

7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утв. ФСТЭК России 15.02.2008 // RPPA.PRO [Электронный ресурс]. URL: https://rppa.pro (дата обращения: 19.12.2025).

8. Методические рекомендации по обеспечению безопасности персональных данных при их обработке в ИСПДн // FSTEC21 [Электронный ресурс]. URL: https://fstec21.blogspot.com (дата обращения: 19.12.2025).

9. Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления:ГОСТ Р 7.0.5–2008. – Введ. 01.01.2009. – М.: Стандартинформ, 2008.

10. Информационная технология. Оборудование информационных технологий. Кабельные системы структурированные. Общие технические требования:ГОСТР 53246–2008. – М.: Стандартинформ, 2009.

11. Информация Минкомсвязи России от 08.08.2014 г. «Для получения доступа к Wi-Fi в публичных местах не обязательно предъявлять паспорт» // КонсультантПлюс [Электронный ресурс]. URL: https://www.consultant.ru(дата обращения: 19.12.2025).

12. Олифер, В.Г., Олифер, Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. – СПб.: Питер, 2016. – 992 с.

13. Таненбаум, Э., Уэзеролл, Д. Компьютерные сети. – СПб.: Питер, 2012. – 960 с.

14. Куроуз,Дж.Ф., Росс, К.У. Компьютерные сети. Нисходящий подход. – СПб.: Питер, 2016. – 765 с.

15. Столлингс, В. Компьютерные сети, протоколы и технологии Интернета. – СПб.: БХВ-Петербург, 2018. –832 с.

16. Чекмарев, Ю.В. Локальные вычислительные сети: учебное пособие. – М.: ДМК Пресс, 2023. – 201 с.

17. Семёнов, А.Б., Стрижаков, С.К., Сунчелей, И.Р. Структурированные кабельные системы: практическое руководство. – М.: ДМК Пресс, 2023. – 641 с.

18. Семёнов, А.Б. Администрирование структурированных кабельных систем. – М.: ДМК Пресс, 2023. – 193 с.

19. Гладких, А.А., Дементьев, В.Е. Базовые принципы

информационной безопасности вычислительных сетей: учебное пособие. – Ульяновск: УлГТУ, 2009. – 156 с.

20. Макаренко, С.И. Защита компьютерных сетей и телекоммуникаций: учебное пособие. – СПб.: Наукоёмкие технологии, 2024. – 311 с.

21. Варфоломеев, А.А. Основы информационной безопасности: учебное пособие. – М.: Бином. Лаборатория знаний, 2008. – 414 с.

22. Шумакова, Е.В. Информационные технологии в гостиничном бизнесе: учебное пособие. – М.: КноРус, 2025. – 183 с.

23. Альшаев, И.А., Лаврухин, В.А.О проектировании и оптимизации сетей Wi-Fi // Информационные технологии и телекоммуникации. – 2016. – Т. 4. – № 1. – С. 87–95.

24. Рудаков, Д.В., Комагоров, В.П., Фофанов, О.Б. К вопросу о проектировании беспроводных локальных сетей WLAN // Доклады ТУСУРа. – 2010. – № 2 (22), ч. 1. – С. 278–282.

25. Прусс, Б.Н. Проектирование беспроводных локальных сетей [Электронный ресурс]. – 2017. – Режим доступа: eLIBRARY.RU, URL: https://elibrary.ru/item.asp?id=30378566 (дата обращения: 19.12.2025).

26. Бражук, А. Построение беспроводных локальных сетей на основе ячеистой топологии // Беспроводные технологии. – 2006. – № 4. – С. 24–29.

27. Денисенко, В. Беспроводные локальные сети. Часть 2 // Справочник инженера. СТА [Электронный ресурс]. – 2009. – Режим доступа: https://www.cta.ru(дата обращения: 19.12.2025).

28. Полянский, Э. С., Тюхтяев, Д. А. Исследование беспроводной Wi-Fi сети корпуса КВолгоградского государственного университета // Проблемы передачи информации в инфокоммуникационных системах: сб. докл. VI Всерос. науч.-практ. конф. – Волгоград, 2015. – С. 128–132.

29. Беспроводная локальная сеть Wi-Fi [Электронный ресурс] // Википедия. Свободная энциклопедия. URL: https://ru.wikipedia.org/ wiki/Беспроводная _локальная_сеть (дата обращения: 19.12.2025).

30. Закон о доступе к публичным Wi-Fi сетям в РФ [Электронный ресурс] // GlobalHotspot. URL: https://global-hotspot.ru (дата обращения: 19.12.2025).

31. Милкова, О. И. Экономика и организация предприятия: учебник и практикум для вузов — Москва: Издательство Юрайт, 2025. — 473 с.