МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

филиал ФГБОУ ВО «РГГМУ» в г. Туапсе

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 и разработка системы мониторинга и анализа производительности серверов и сетевой инфраструктуры»

Исполнитель Старцев Александр Андреевич

Руководитель кандидат технических наук, доцент Попов Николай Николаевич

«К защите допускаю»

Руководитель кафедры _____

кандидат экономических наук

Майборода Евгений Викторович

«20» 01 2025 г.

Филиал Российского государственного гидрометеорологического университета в г. Туапсе
НОРМОКОНТРОЛЬ ПРОЙДЕН
«16» 01 2025 г.
Мартынова Е.В.
ПОДПИСЬ РАСШИФРОВКА ПОДПИСИ

Туапсе
2025

ОГЛАВЛЕНИЕ

Введение

Сетевой мониторинг выполняет критически важную функцию в поддержании безопасности и эффективности управления сетевой инфраструктурой. Этот процесс включает в себя непрерывное отслеживание активности в сети, целящееся на поддержание её безопасного и стабильного функционирования. Однако, несмотря на его значимость, множество небольших и средних предприятий стремятся игнорировать необходимость внедрения таких систем. Основная проблема для этих компаний заключается в отсутствии квалифицированных специалистов в области сетевого администрирования, которые могли бы адаптировать и максимально эффективно использовать существующие на рынке решения для мониторинга сетей. Это пренебрежение может привести к значительным финансовым потерям или даже к утрате важных данных в результате сбоев в сети.

В представленной выпускной квалификационной работе рассматривается разработка системы для мониторинга локальных вычислительных сетей, направленной на устранение определенных проблем за счет удобства в обращении и наличия всех необходимых для мониторинга функциональностей. Особенностью предложенной системы является ее доступность для использования даже пользователями без продвинутых навыков в области IT, благодаря интуитивно понятному интерфейсу и минимальным требованиям к предварительным знаниям, что является актуальным на сегодняшний день и делает систему идеально подходящей для применения в небольших и средних предприятиях, где может не быть специализированного персонала, занимающегося обслуживанием сетевой инфраструктуры.

Объектом исследования является – система мониторинга вычислительной сети.

Предмет исследования – организация процесса мониторинга локальной вычислительной сети.

Основная цель выпускной квалификационной работы заключается в

разработке и внедрении системы для наблюдения за локальной вычислительной сетью предприятия.

Для реализации поставленной цели требуется выполнить следующие задачи:

1) обозначить типы систем наблюдения за ИТ-инфраструктурой.

2) исследовать текущие проекты и аргументировать выбор технологии проектирования,

3) разработать сетевую систему наблюдения,

4) разработать концепцию локальной вычислительной сети предприятия,

5) разработать логическую модель системы контроля сетевой инфраструктуры,

6) разработать реалистичную физическую схему сетевой архитектуры предприятия,

7) внедрить систему наблюдения за инфраструктурой ИТ сети компании.

8) Вычислить критерии экономической результативности деятельности.

Практическая значимость выпускной квалификационной работы заключается в разработке и внедрении системы мониторинга, обеспечивающей контроль за производительностью и эффективностью корпоративной сети.

ВКР состоит из введения, трех глав и заключения. Во введении описана цель ВКР и обоснована необходимость автоматизированного решения.

Первая глава ВКР является аналитической, в ней приведен анализ существующих систем и инструментов мониторинга сети.

Вторая глава ВКР является проектной и содержит этапы проектирования проектных решений.

Третья глава – реализация предложенной системы и оценка экономической эффективности.

Выпускная квалификационная работа представляет собой созданное

программное решение для контроля за локальной сетью предприятия, способствующее автоматизации процессов мониторинга производительности и оптимальности сетевых операций, что ведёт к минимизации времени, необходимого для управления данными процессами.

1 Изучение доступных методов и программ для мониторинга сетей

1.1 Обзор моделей для мониторинга сетевых систем

Пионеры компьютерной технологии разработали машины, габариты которых сопоставимы с размерами целой комнаты, оснащенные отдельной вычислительной единицей, предназначенной для выполнения базовых арифметических операций. С того времени, как были созданы эти первоначальные устройства, компьютерная индустрия непрерывно развивалась. В современной эпохе наиболее значимым вызовом для данных технологий стало обеспечение их бесперебойного соединения с сетью.

Компьютерная сеть является комплексом взаимосвязанных автономных устройств, объединенных чрез использование стандартизированных протоколов передачи данных. Основу сетевой инфраструктуры составляют аппаратные устройства, такие как мосты, коммутаторы, маршрутизаторы, выполняющие функции по организации, распределению и управлению трафиком данных. Для физического соединения узлов сети используются различные среды передачи данных: проводные (включая оптоволоконные линии и коаксиальные кабели) и беспроводные технологии (WLAN сети, микроволновое и инфракрасное связи). Классификация компьютерных сетей осуществляется по их масштабу и охвату, выделяя персональные (PAN), локальные (LAN), городские (MAN), глобальные (WAN) сети, а также магистральные сети и Интернет, отличающиеся географическим охватом и объемом обрабатываемых данных.

Осуществление надзора за производственными показателями сетевых структур дает возможность пользователю осуществлять контроль и регулирование эффективности, анализируя полученные данные и обнаруживая неполадки в сетях, использующих интернет-протокол (IP). Инструменты для мониторинга производительности представляют собой критически важные ресурсы для системного администратора, обеспечивая ему способность к непрерывному обзору состояния сетевых операций на основе данных,

собранных в определенные интервалы времени. Стандартная конфигурация сети включает в себя широкий спектр оборудования, включая, но не ограничиваясь, мосты, ретрансляторы, коммутаторы, роутеры и т.д. Мониторинг сетей направлен на проверку эффективности работы указанного оборудования и гарантирование бесперебойности сетевой инфраструктуры.

Изучим некоторые распространенные подходы к мониторингу сетей. Сетевая мониторинговая система предназначена для трех ключевых задач: поддержания непрерывного и корректного функционирования сети, составления сводок о текущем состоянии сетевой инфраструктуры и генерации отчетов о зафиксированных событиях.

Моррис Сломан [23] разработал новаторскую концепцию в области мониторинга сетевых систем, представив модель, которая вносит изменения в управление событиями, усовершенствуя подходы, предложенные в предыдущих работах. Эта модель фокусируется на анализе и отслеживании событий, а также на состоянии устройств, интегрированных в сеть. Ее основная задача заключается в генерации детализированного отчета о мониторинге, который затем направляется сетевому администратору для последующего реагирования и оптимизации работы сети.

В изученной архитектуре разработаны журналы событий и статусов для обеспечения возможности администратора оценивать эффективность работы сетевой инфраструктуры и координацию между клиентскими машинами. рисунок 1 демонстрирует структуру анализируемой системы.

Рисунок 1 - Модель управления сетевыми ресурсами

Исследованной альтернативой является модель DiMAPI [25]. Этот Application Programming Interface (API) для сетевого мониторинга вносит модификации в стандартные подходы к наблюдению за сетями, развивая идеи традиционных пинг-методов. DiMAPI усовершенствует концепцию, предложенную ранее в модели MAPI, переходя от централизованного к децентрализованному многоточечному контролю за сетевым пространством.

DiMAPI, в отличии от MAPI, сосредотачивается на мониторинге сетевого трафика с помощью отправки пакетов ICMP для проверки доступности, обеспечивая обзор работы сетевых узлов. Этот подход позволяет использовать ping не только для проверки доступности ресурсов, но и для анализа качества соединения, в том числе измерения задержек, выявления потерь пакетов и оценки общего состояния сетевой инфраструктуры.

В исследовании [25] учёные описали ключевые возможности DiMAPI, включая анализ трафика и наблюдение за Peer-to-Peer (P2P) связями. Термин P2P обозначает тип распределённой сети, где участники напрямую обмениваются данными без посредника в виде центрального сервера. В рамках данной работы для отслеживания движения данных был применен метод ping. Этот метод, посылая и принимая данные между устройствами в сети, позволяет оценить активность и загруженность сети.

Также, в архитектуре сетевого мониторинга критическое значение имеет наличие заранее определённых возможностей для данных передач, что обеспечивает транспортировку специфических сведений.

В предлагаемой в данной ВКР модели рабочие станции также требуют наличия клиентской версии программного обеспечения для мониторинга сетевых операций. Однако, мониторинг сложных и динамичных сетей, подобных тем, что используются на промышленных объектах, может представлять собой сложную задачу при реализации вручную. По этой причине, в отличие от традиционного подхода к мониторингу, предложена модель, основанная на принципах интеллектуального мониторинга. Эта модель предусматривает регулярную отправку и возврат пакетов данных между

сервером и рабочими станциями в определенные промежутки времени, что позволяет поддерживать непрерывное соединение между ними. Экспериментальные испытания модели DiMAPI демонстрируют, что данная система интеллектуального мониторинга обеспечивает эффективный мониторинг сети в режиме реального времени и повышает ее безопасность.

Освещая механизмы удаленного доступа, можно заметить, что в контексте сетевого мониторинга, он предоставляет сетевому администратору легитимную возможность проведения ряда операций в устройствах, интегрированных в сеть, включая коммутационные устройства, маршрутизаторы, а также клиентские компьютеры.

Чтобы обеспечить дистанционное взаимодействие, данные, использующие протокол TCP для управления передачей, будут пересылаться через прокси-сервер на консольный интерфейс маршрутизатора и возвращаться обратно. В контексте осуществления такого доступа, любые устройства, ассоциированные с данным прокси-сервером, становятся доступными для управления на расстоянии посредством серверного администрирования. Серверный администратор осуществляет выбор и управление нужными операциями на каждом из подключенных устройств. Графическое представление описываемого процесса можно увидеть на рисунке 2.

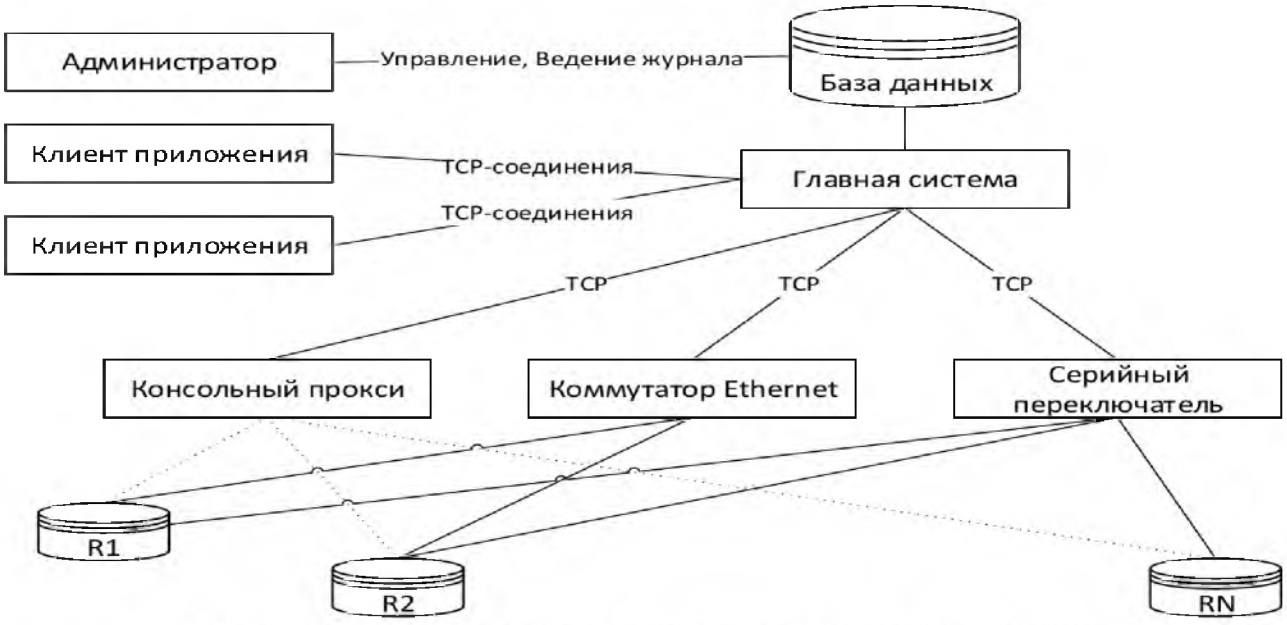


Рисунок 2 - Методология систем доступа на расстоянии

Сетевой инженер задействует настройку связи между парой роутеров, интегрированных в системный интерфейс для мониторинга сетей, и еще одним роутером, который обеспечивает подключение к рабочим станциям. Как упоминалось ранее, на каждом конечном пользовательском оборудовании должен быть установлен клиентский компонент мониторинговой системы. Это позволяет реализовать прямую связь сервера с клиентскими станциями для обеспечения выполнения запланированных операций и задач в сети.

Каждое устройство, подключенное к сети, будет иметь IP-адрес, регистрируемый на сервере, что позволяет серверу идентифицировать и выбирать конкретный клиент или рабочую станцию для осуществления операций на выбранном устройстве [17].

1.2 Исследование наработок в данной области и аргументация выбора метода проектирования

В этой части мы анализируем программы, схожие с предложенным сетевым мониторинговым приложением. Осветим достоинства и, при наличии, недостатки каждого программного решения.

Spiceworks является заметным инструментом в арсенале для сетевого мониторинга. Эта платформа обеспечивает мониторинг событий в сетевом окружении, дополнительно предоставляя функционал для анализа данных по пропускной способности и эффективности работы сетевых ресурсов. В качестве серверного приложения, Spiceworks дает возможность администрировать и конфигурировать сетевые параметры, обеспечивая централизованное управление. Помимо этого, администратор получает детализированную информацию о подключенных устройствах, доступ к аккаунтам и данным пользователей, а также способность оказывать поддержку пользователям станций при сетевых проблемах. Несмотря на удобство и эффективность в мониторинге, Spiceworks ограничен в использовании с операционными системами, отличными от Linux, и не предоставляет функционал для активного

управления сетью, лишь позволяя наблюдать за ее состоянием без возможности прямого вмешательства.

Wireshark занимает лидирующие позиции среди инструментов для диагностики сетевых проблем и проведения глубокого анализа сетевого трафика. Он обладает широким спектром возможностей, включая подробный анализ трафиковых пакетов, расширенный анализ VoIP коммуникаций, обширный мониторинг потоков данных и многое другое. Программа позволяет интерцептировать и изучать сетевые пакеты, предоставляя функционал для их сохранения и последующего анализа. Wireshark имеет ряд достоинств, но также сопровождается и определенными недостатками. Его бесплатная лицензия, открытый код и кроссплатформенность являются значительными плюсами. Однако, несмотря на мощные аналитические возможности, пользовательский интерфейс программы может оказаться сложным для освоения. Кроме того, для эффективного использования Wireshark необходим глубокий понимание стека протоколов TCP/IP, что также может выступать в роли барьера для неподготовленных пользователей. Наличие подобных препятствий указывает на некоторые ограничения в применении данного аналитического инструмента.

Tcpdump является известным инструментарием для анализа сетевых данных. В стандартном режиме сетевые интерфейсы пропускают только те пакеты, которые предназначены для данной сети. В отличие от этого, Tcpdump захватывает весь трафик, независимо от его назначения, активируя режим promiscuous на сетевом интерфейсе. Это дает возможность администраторам наблюдать за всеми передаваемыми пакетами, выявлять аномалии в сетевом трафике и определять характеристики трафика, анализируя информацию, содержащуюся в заголовках пакетов. Работая на основе командной строки и поддерживая UNIX-подобные системы, Tcpdump предлагает глубокий анализ сетевых пакетов.

Этот инструмент сопоставим с Wireshark, оба предоставляют функционал захвата и анализа сетевых пакетов на разных уровнях, облегчая задачи администрирования и безопасности сетей.

OpManager, выдающийся инструмент мониторинга сетей для корпоративных пользователей, представляет всю сетевую инфраструктуру в форме картографического изображения, интегрированного с Google Maps, включая перечень всех подсоединенных устройств. Это дает возможность администраторам сети визуализировать местоположение каждой рабочей станции в реальном времени.

Функционал визуализации выделяет OpManager среди конкурентов, давая возможность администраторам эффективно управлять сетью. Через эти инструменты можно создавать персонализированные сетевые карты, что позволяет подстроить представление сети под конкретные бизнес-потребности и географическое размещение рабочих мест. OpManager предоставляет не только базовые функции управления, но и способствует идентификации и конфигурации устройств, демонстрируя схожесть с функционалом, доступным в Spiceworks. Добавление управления MySQL усиливает его полезность для администраторов, обеспечивая детальный контроль за хранимой информацией. При всех своих преимуществах OpManager требует ручной настройки, что может быть времязатратным, а его интерфейс имеет высокий порог вхождения для новых пользователей. Это отражает некоторые из основных недостатков программы, которые необходимо учитывать при её выборе.

В таблице 1 представлено сравнение четырех доступных на рынке инструментов с предлагаемой системой мониторинга сетевого трафика.

Таблица 1 - Анализ предложенной системы в сравнении с альтернативными решениями

Функции	Wireshark	TCPdump	OpManager	SolarWinds	Предлагаемая система мониторинга
Чтение пакетов	+	+	+	+	+
Захват пакетов	+	+	+	+	+
Фильтры для отображения данных	+	-	-	-	-
Обнаружение вызовов VoIP	+	-	+	-	-

Продолжение таблицы 1

Графический интерфейс	+	-	+	+	+
На основе командной строки	-	+	-	-	-
Мониторинг оборудования	-	+	+	+	+
Среднеевремя отклика	+	+	+	-	+
Сетевая трассировка	+	+	+	+	+
Система чата	-	-	-	-	+
Клиент-серверная архитектура	-	-	+	+	+
Потеря пакетов	+	+	+	-	-
Сохранение журнала	+	+	+	+	+
Статистический отчет	+	-	-	+	+

В таблице 1 представлено сопоставление, основывающееся на функционале каждого инструмента. В данной выпускной квалификационной работе предложенная система будет обладать функциональными возможностями, схожими с текущими системами мониторинга сети.

Сравнительно с конкурирующими продуктами, значительным преимуществом нашей системы является встроенный модуль обмена сообщениями. Этот модуль, разработанный как дополнительная удобная опция, облегчает взаимодействие пользователей.

К тому же, система контроля сетевой активности будет оснащена удобным для пользователя интерфейсом.

2 Проектирование системы мониторинга сети

2.1 Концептуальное проектирование системы локальной вычислительной сети организации

На рисунке 3 демонстрируется схема, иллюстрирующая механизм управления внутренней вычислительной сетью.

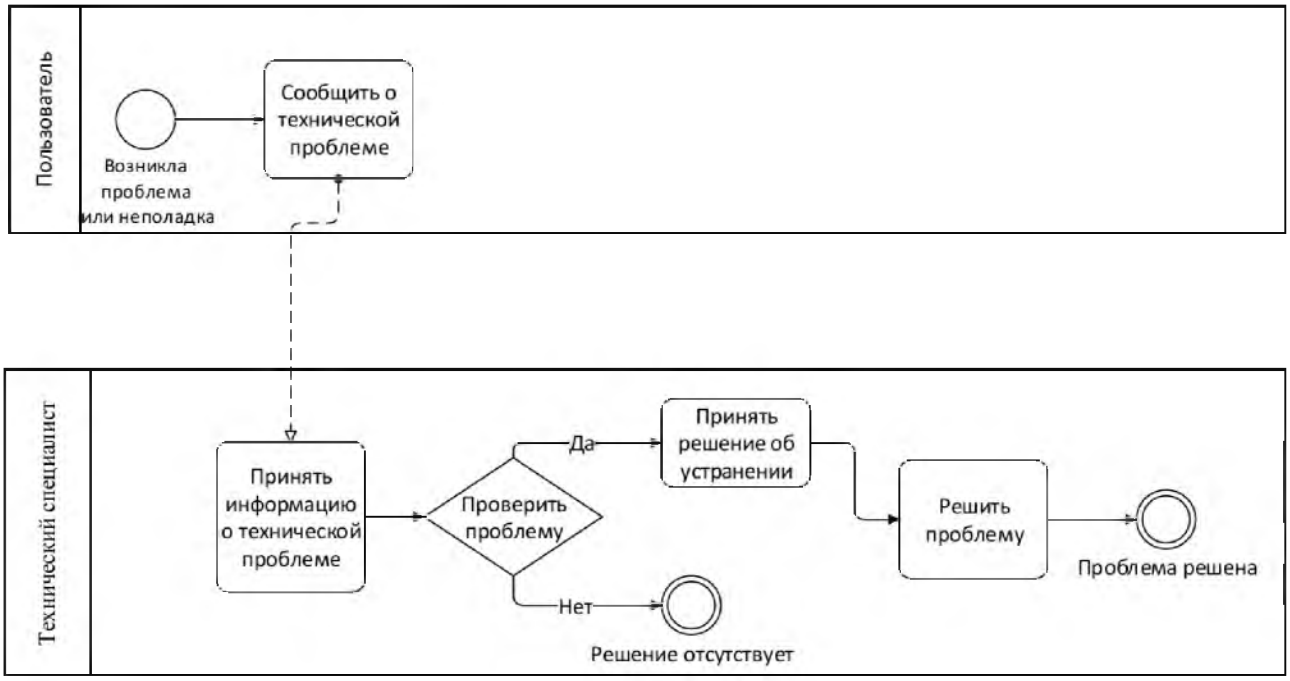


Рисунок 3 - Демонстрация BPMN-диаграммы процесса контроля и управления локальной компьютерной сетью.

Управление локальными вычислительными сетями (ЛВС) охватывает ряд аспектов [5]:

1) при появлении технического сбоя у клиента следует обратиться за помощью к специалисту по информационным технологиям.

2) Первичная диагностика осуществляется непосредственно на территории, а именно в офисе или здании, где зарегистрирована техническая неисправность, куда направляется IT-специалист

3) инженер технической поддержки анализирует неполадку и, если это возможно, предоставляет мгновенное решение, в ином случае исправление будет выполнено в установленный срок.

4) Все формы поддержки являются физическими и зависят от затрат времени.

5) При возникновении технического сбоя у пользователя требуется обратиться за помощью к техническому специалисту.

На рисунке 4 показана блок-схема, иллюстрирующая методику регулирования вычислительной сети.

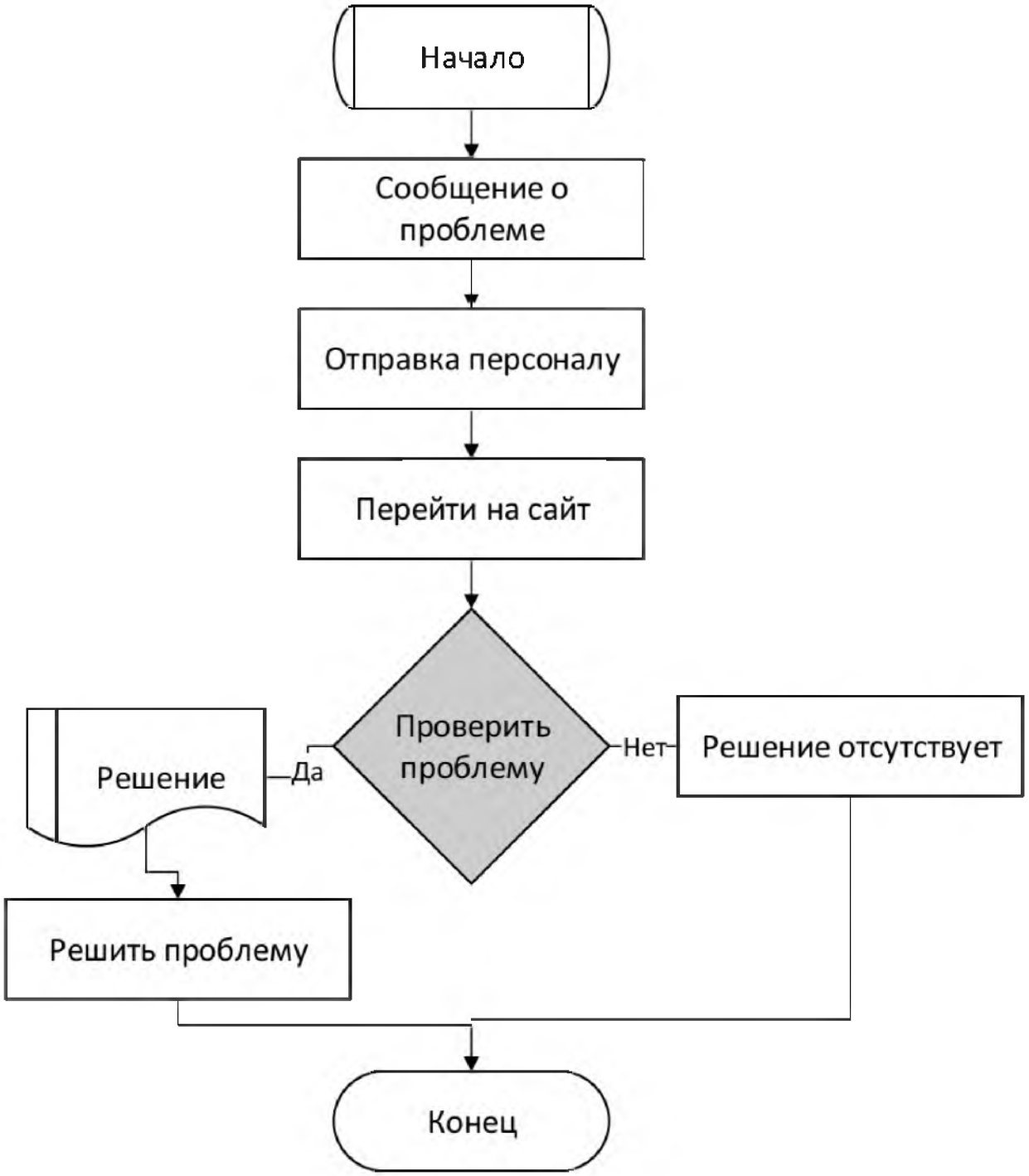


Рисунок 4 - Схематическое изображение процедуры контроля за компьютерной сетью

Исследуя механизмы управления внутрисетевыми процессами, можно идентифицировать ряд недостатков:

1) отсутствует ссылка на предшествующую проблематику,

2) несмотря на применение ручного управления, переход между зданиями для устранения сетевых неполадок требует значительного времени,

3) Задержки в реакции приводят к снижению производительности и эффективности ежедневных операций.

4) нет постоянно действующей службы поддержки для урегулирования ежедневных задач и обращений клиентов.

На рисунке 5 демонстрируется алгоритмическая модель предполагаемой системы наблюдения за локальной компьютерной сетью компании.

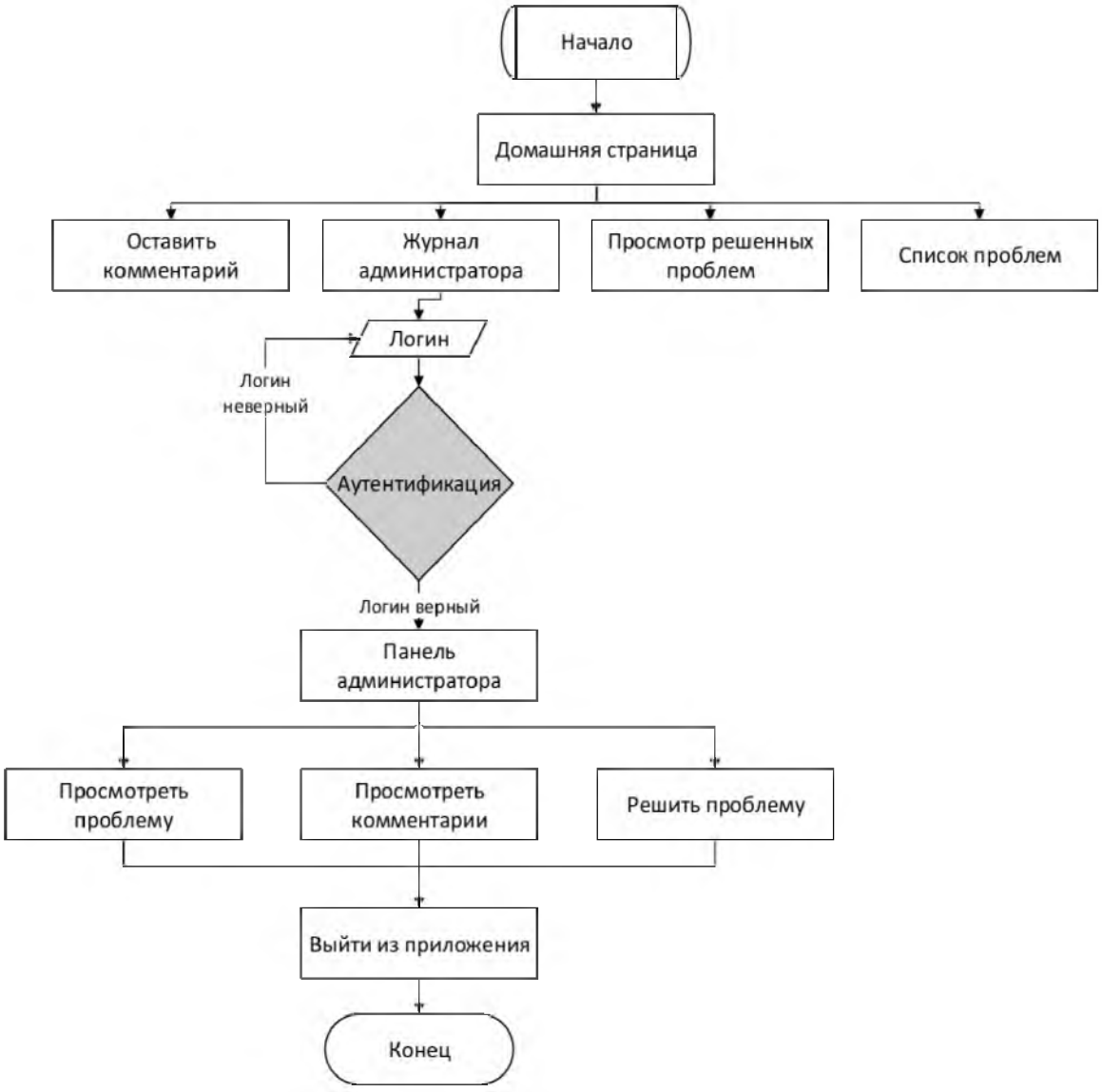


Рисунок 5 – Схематическое представление алгоритма предложенной системы

Следовательно, можно предложить меры по сокращению негативных реакций, связанных с имеющимся системным недостатком:

1) Платформа даст возможность клиенту размещать описание своих трудностей и потребностей, в то время как клиенты смогут обращаться за поддержкой через интернет,

2) Платформа предоставляет возможность пользователю самостоятельно находить решение возникшей проблемы в режиме онлайн, минуя необходимость обращения в службу поддержки.

3) Эта система обеспечивает эффективное управление временем и ресурсами, предоставляя возможность автоматического создания отчетов о запросах пользователей на еженедельной основе.

4) Данная система дает возможность системным администраторам и специалистам технической поддержки определять и мониторить возникшие проблемы на основе геолокации запросов.

На рисунке 6 демонстрируется схема, отражающая систему автоматизации для контроля за работой локальной компьютерной сети.

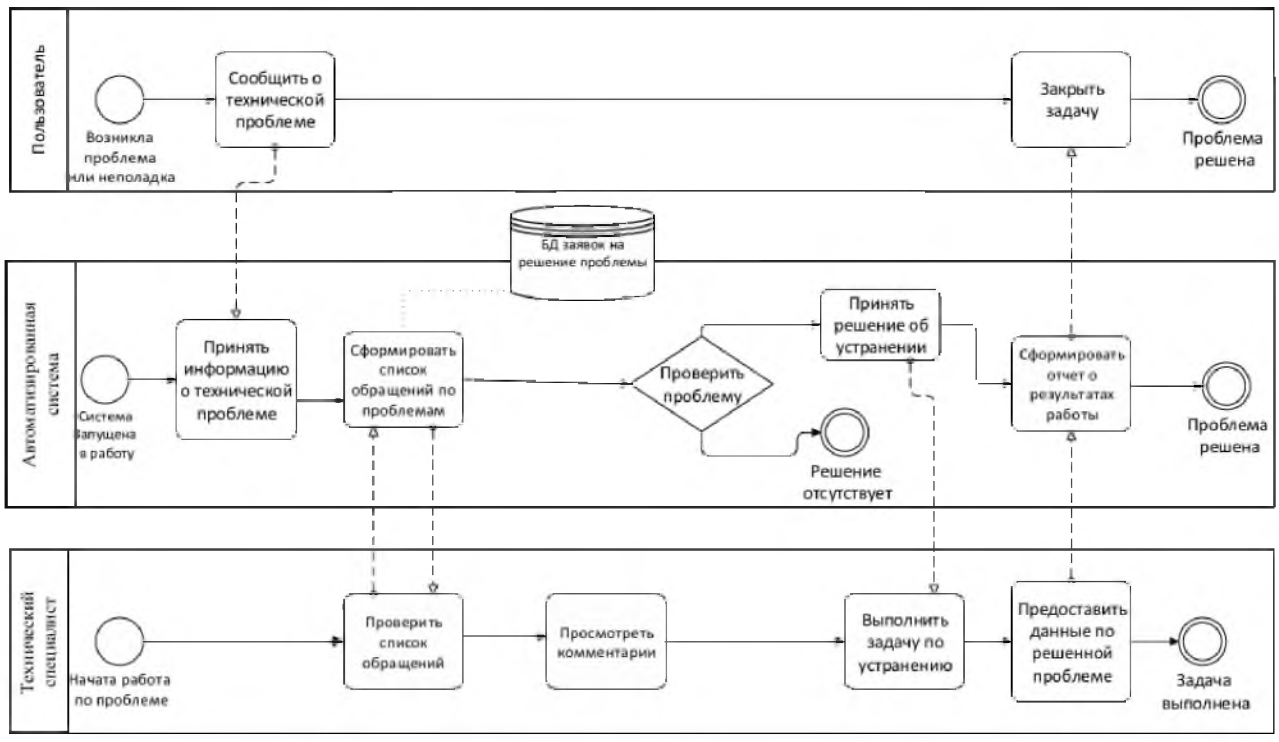


Рисунок 6 - диаграмма BPMN, описывающая процесс контроля за локальной вычислительной сетью

Систематизация отслеживания запросов через автоматизацию значительно оптимизирует управление инцидентами и обращениями клиентов. Это позволяет администраторам эффективно управлять обращениями онлайн, предоставляя возможность доступа и контроля в реальном времени из любой точки. Благодаря интеграции с базами данных, каждый запрос или проблема получает уникальный идентификатор, исключая риск дублирования и ускоряя процесс обработки и архивирования информации о инцидентах.

На рисунке 7 изображена схема процессов предложенной системы.

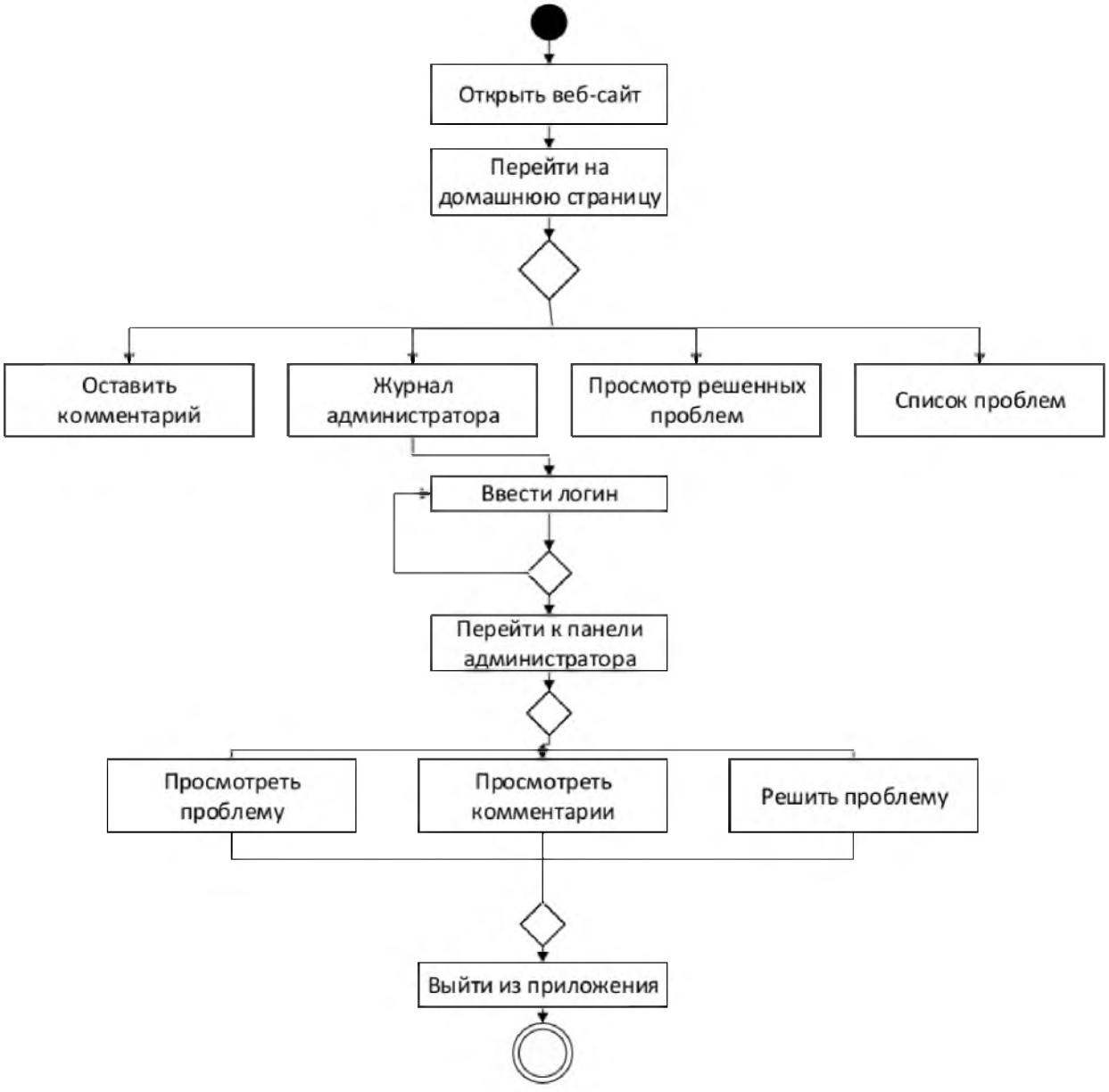


Рисунок 7 - Схема процессов рекомендуемой системы

Это приложение использует архитектуру клиент-сервер. Основа системы

предполагает установку приложения на клиентских и серверных устройствах. Сервер, имея сетевое подключение, позволяет клиентам соединяться с ним через определённый порт и IP-адрес.

В контексте удаленного доступа, после установления связи клиент-сервер, доступны определенные настройки для конфигурации администратором сервера.

В данном случае, результаты демонстрируются через анализ минимальной, максимальной и средней длительности процесса, дополнительно включая данные о потерях пакетов, а также количество отправленных и успешно доставленных пакетов.

За счет интеграции системы в сетевую инфраструктуру, администратор обладает возможностью просматривать журнал запросов из любой точки мира, условием является доступ в Интернет и наличие нужных данных для аутентификации [4].

Давайте рассмотрим иерархический подход к проектированию, который делит проект на модульные категории. Определим три основных уровня:

1) Права доступа: гарантируют возможность подключения группы работников или отдельного пользователя к локальной сети.

2) Распределенный уровень: интегрирует уровни привилегий и гарантирует соединение со службами.

3) Основной уровень: гарантирует связь между уровнями дистрибуции в крупных локальных сетях.

Таким образом, проектируемая система контроля формирует иерархию взаимодействующих элементов.

2.2 Разработка физических и логических моделей для системы контроля сетевых ресурсов и информационной инфраструктуры предприятия

В процессе разработки системы мониторинга сетевых процессов применён стандартный инструментарий - унифицированный язык

моделирования UML. Этот язык представляет собой универсальную нотацию для визуализации архитектуры, функций и поведения программных продуктов или системных решений в целом.

Обычно, UML состоит из пяти ключевых диаграмм и деталей, что обеспечивает базовое понимание предложенной системы в отношении каждой её функции[10].

В рамках начального этапа работы с UML, нашим действием будет создание диаграммы вариантов использования, отображающей ключевые функциональности проектируемой системы через визуальную схему.

В данной работе представленный сценарий демонстрирует взаимодействие двух участников: клиента и сервера, подчеркивая их доступность для коммуникации. На рисунке 8 демонстрируются ключевые функции разработанного программного продукта.

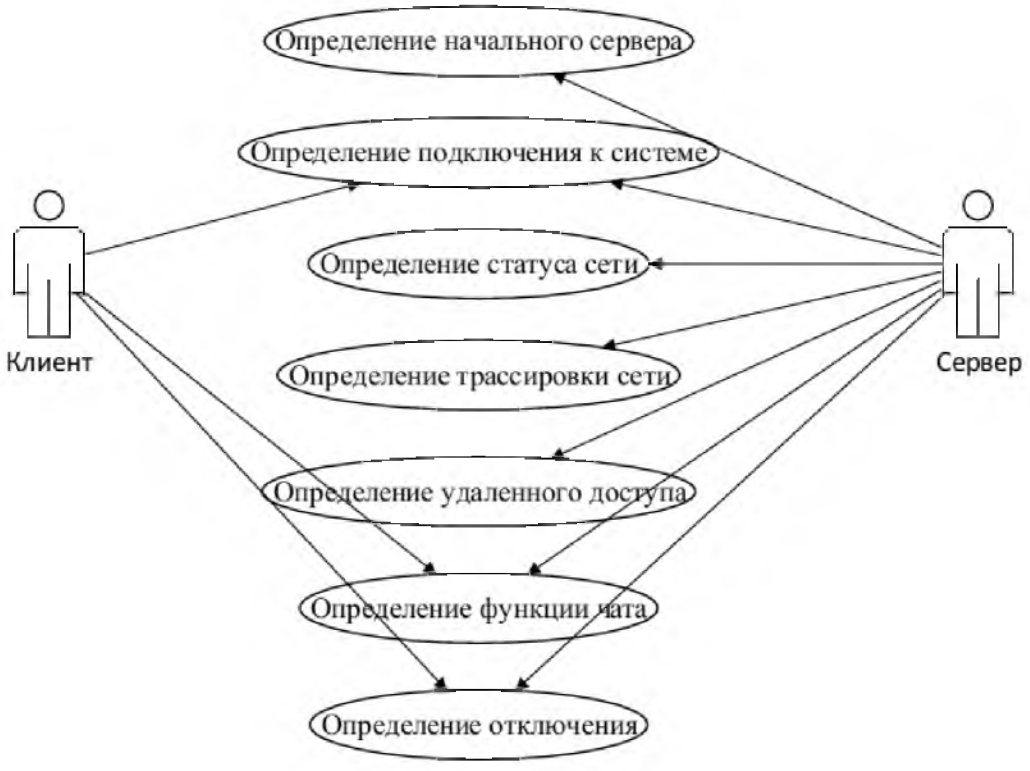


Рисунок 8 - Схема применения альтернативных вариантов

В таблицах с номерами 2-8 описывается спецификация сценариев применения, включая детализацию предоставляемых функций. Таблица 2 детализирует процедуру инициализации серверного приложения.

Таблица 2 - Выбор первичного сервера

Стартовый сервер	
Актеры	Доступ назначен Серверу
Описание	Администратор сервера может его запустить
Нормативные документы	У администратора есть разрешение на запуск сервера
Предпосылка	--
Результат	Администратор сервера должен запустить систему, чтобы клиент мог подключиться

Из содержания таблицы очевидно, что исключительный доступ разрешён только системному администратору. Начальная фаза процедуры наблюдения за активностью в сетевой инфраструктуре включает в себя активацию сервера со стороны администрирующего лица. Дополнительно, происходит обнуление прав в ранее упомянутой таблице, предоставляя администратору эксклюзивные полномочия на включение сервера. На данном этапе отсутствует необходимость в предварительном запросе на запуск, поскольку это действие является исходной точкой всего процесса подачи запроса. В результате, по завершению данной фазы, сервер оказывается в рабочем состоянии, позволяя клиенту осуществить подключение.

Далее следует этап подсоединения, как демонстрируется в таблице 3.

Таблица 3 - Описание процесса подключения к системе

Связь	
Актеры	Привилегии назначаются как Серверу, так и Клиенту.
Описание	Сервер и клиент способны устанавливать соединение с системой.
Нормативные документы	Серверный администратор налаживает коммуникацию, далее клиент получает возможность соединения с сервером.
Предпосылка	Сервер назначает порт, позволяя клиенту соединяться с сервером через конкретный порт и IP-адрес.
Результат	Коммуникация между клиентом и сервером будет успешно налажена

Эта таблица определяет процесс взаимодействия. Возможность подключения открыта как для клиента, так и для сервера, что обеспечивает двустороннюю связь между элементами приложения. Процесс начинается с

инициации соединения со стороны сервера, что позволяет клиенту последующее подключение. Важной частью процедуры является запрос от клиента с использованием уникальных сетевых идентификаторов: IP-адреса сервера и номера порта, предварительно назначенного сервером. Это позволяет точно адресовать запросы клиента к серверу, завершая процесс успешным установлением соединения и началом обмена данными между клиентом и сервером.

Стоит подчеркнуть, что в разрабатываемой системе порт имеет фиксированный номер, облегчая тем самым её эксплуатацию. Информацию о состоянии сети можно найти в таблице 4.

Таблица 4 - Классификация состояния сети

Статус сети	
Актеры	Администратор сервера и клиентский пользователь получают доступ.
Описание	Серверный администратор имеет доступ к данным сетевого оборудования, расположенного на стороне сервера, в то время как информация о клиентских сетевых устройствах доступна пользователю с клиентской стороны.
Нормативные документы	--
Предпосылка	Определение подходящего сетевого интерфейса
Результат	Админ сервера и клиентский пользователь могут оценить статус сетевой инфраструктуры.

Секция мониторинга сети касается данных о сетевом оборудовании, актуальных как для серверного администратора, так и для конечного пользователя. Здесь серверная инфраструктура позволяет аудит оборудования в собственной сети, в то время как клиент может провести аналогичную проверку своих сетевых компонентов.

Эта возможность, как ясно из её наименования, гарантирует мониторинг и регулирование работы сетевых аппаратов и, при возникновении любой проблематики, система идентифицирует её и предложит методику для решения возникших трудностей. Пользователь, уведомленный о любом сбое или прекращении работы в сети, что будет детально описано в данном разделе, может либо применить предложенное решение для исправления ситуации, либо

направить данные о сложности администратору сети для получения профессиональной поддержки.

Передача данных может происходить посредством чат-платформы. Раздел сетевого маршрутизирования детализирован в таблице номер 5.

Таблица 5 - Описание процесса трассировки сетевого пути

Трассировка сети	
Актеры	Права доступа назначаются администратором сервера.
Описание	Мониторинг IP-адресов целевого назначения
Нормативные документы	Конфигурация предпочитаемого IP для мониторинга
Предпосылка	Должен быть выбран действующий IP-адрес
Результат	Администратор сервера способен отслеживать определённый IP-адрес.

Этот сегмент остается под управлением серверной составляющей приложения. Введя в систему доменное имя или IP-адрес целевого узла, системный администратор получит возможность осуществить проверку функционирования связи между собственным сервером и указанным узлом. Данный процесс включает в себя верификацию доступности сетевых устройств, таких как роутеры и свитчи, расположенных в маршруте следования данных от сервера к цели. Детальное изложение функционала удаленного доступа содержится в разделе, отмеченном как таблица 6.

Таблица 6 - Определение удаленного управления

Удаленный доступ	
Актеры	Права доступа выдаются системным администратором сервера.
Описание	Администратор сервера будет обладать возможностью удаленного управления клиентскими устройствами, которые подключены к серверу.
Нормативные документы	Серверный администратор определит конкретного клиента, используя выпадающий список, после чего выберет желаемое действие.
Предпосылка	--
Результат	Серверу будет присвоен доступ для обслуживания удаленного клиента.

Секция удаленного управления ориентирована на функциональность серверной стороны, предоставляя административный доступ исключительно

для администратора сервера. Это соединение между серверной и клиентской сторонами дает администратору возможность осуществлять контроль над клиентскими устройствами, присоединенными к сети сервера. Благодаря этой опции, администратор может при необходимости выполнить определенные операции на удаленных клиентских устройствах. Варианты операций включают выключение, перезагрузку, остановку процессов и закрытие сессий на клиентских компьютерах. Процесс управления начинается с выбора целевого клиентского устройства из списка и определения желаемого действия для его выполнения.

В приложении реализована функциональность чата, который доступен как для серверной, так и для клиентской части. Обе стороны имеют возможность инициировать диалог. Однако для того, чтобы сервер мог отправить сообщение клиенту, ему необходимо сперва выбрать адресата. Это обеспечивает обеим сторонам возможность взаимодействия через чат в случае установленного соединения между ними. Данная процедура детально описана в седьмой таблице документации.

Таблица 7 – Описание возможностей мессенджера

Чат	
Актеры	Права доступа разграничиваются между администраторами Серверной и Клиентской сторон.
Описание	Как сервер, так и клиент имеют возможность инициировать общение.
Нормативные документы	--
Предпосылка	Только сервер обладает правом выбора адресата для доставки сообщения клиенту.
Результат	Реализована поддержка взаимодействия между сервером и пользовательским приложением

Таблица 8 содержит детализацию процедуры деактивации.

Таблица 8 - Классификация отключений

Отключение	
Актеры	Права доступа выдаются админу Клиентских и Серверных ресурсов.
Описание	И как клиент, так и сервер будут иметь возможность выключать свои устройства.
Нормативные документы	--

Продолжение таблицы 8

Предпосылка	--
Результат	Соединениебудетразорвано

Клиентская и серверная архитектуры обладают функцией деактивации своих систем, что позволяет как пользователям, так и серверам прекращать их функционирование по необходимости.

Диаграмма классов представляет собой важную составляющую фазы проектирования в рамках Объединенного моделирования языка (UML). Такие диаграммы обычно применяются при разработке, основанной на объектно-ориентированном подходе, и показывают архитектурный план системы.

На рисунке 9 представлена схема классов для проектируемой системы наблюдения за сетью.

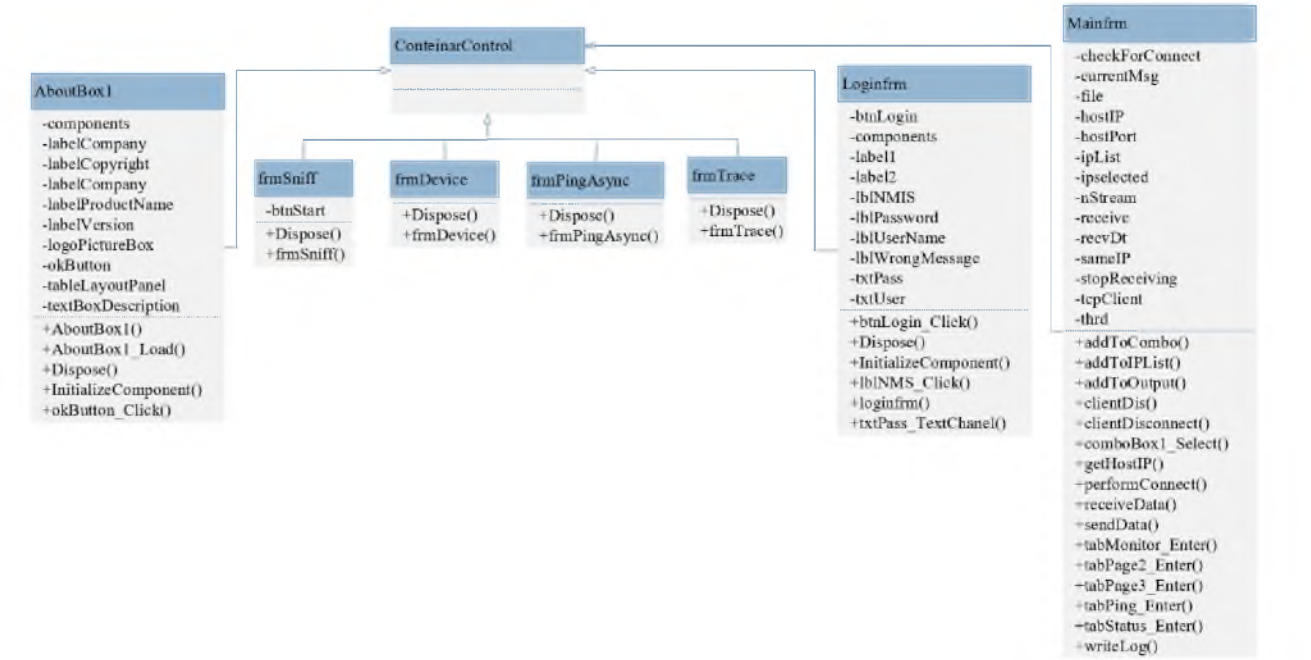


Рисунок 9 - Диаграмма классов

UML-диаграмма классов представляет собой выразительное средство визуализации структуры системы, обозначая классы с их наименованиями, типы связей между ними, а также включая атрибуты и методы, необходимые для построения системы. В контексте разработки данного приложения, для иллюстрации взаимодействия между клиентом и сервером в процессе

установления соединения была разработана и представлена на рисунке 10 UML-диаграмма последовательности, демонстрирующая последовательность обмена сообщениями.

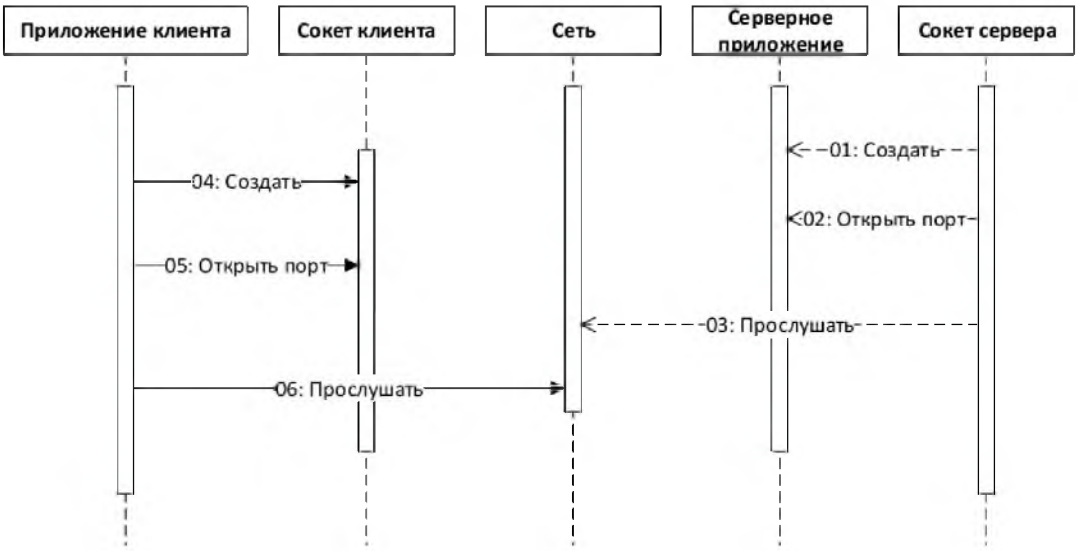


Рисунок 10 - Схема последовательности, демонстрирующая процедуру соединения

Диаграмма последовательности является одним из элементов, используемых в Унифицированном языке моделирования (UML), и иллюстрирует взаимосвязь между объектами в приложении через временную последовательность их взаимодействий. Стрелочные линии на диаграмме демонстрируют обмен сообщениями или вызовы методов, в то время как прямоугольники отображают экземпляры классов, участвующих в процессе. Оптимальное количество диаграмм последовательности зависит от сложности и специфики проекта.

Разработка системы обозначает процесс создания проекта для будущей системы, определяющий её внешний вид и функциональность после запуска и внедрения в эксплуатацию.

Унифицированный язык моделирования (UML) предлагает обширную систему символов, способствующую плавному переходу от анализа к проектированию. UML является комплексом визуальных символов, применяемых разработчиками для визуализации архитектуры программных

продуктов.

На рисунке 11 изображена цепочка операций, проводимых системным администратором.

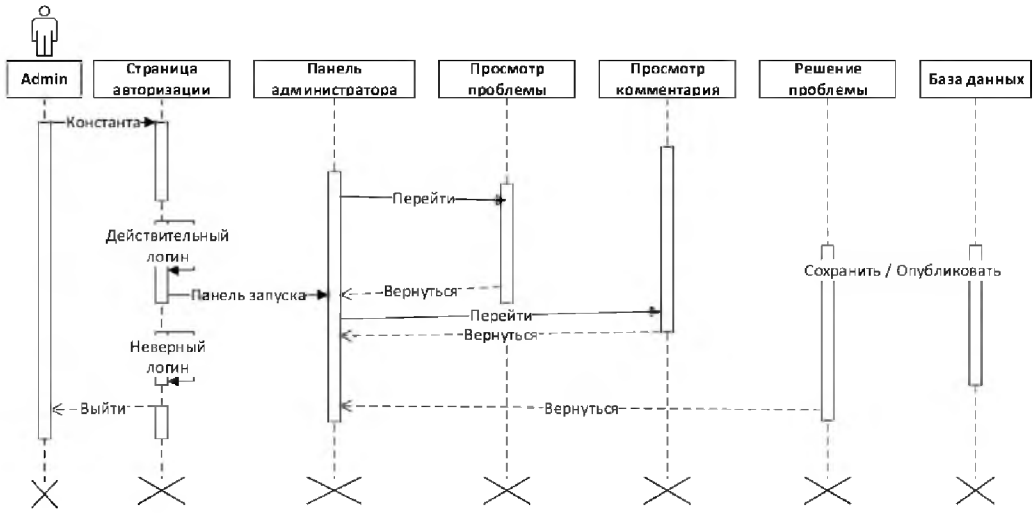


Рисунок 11 - Схематическое изображение последовательности операций администрирования задач

На рисунке 12 показан ряд операций, совершаемых пользователем.

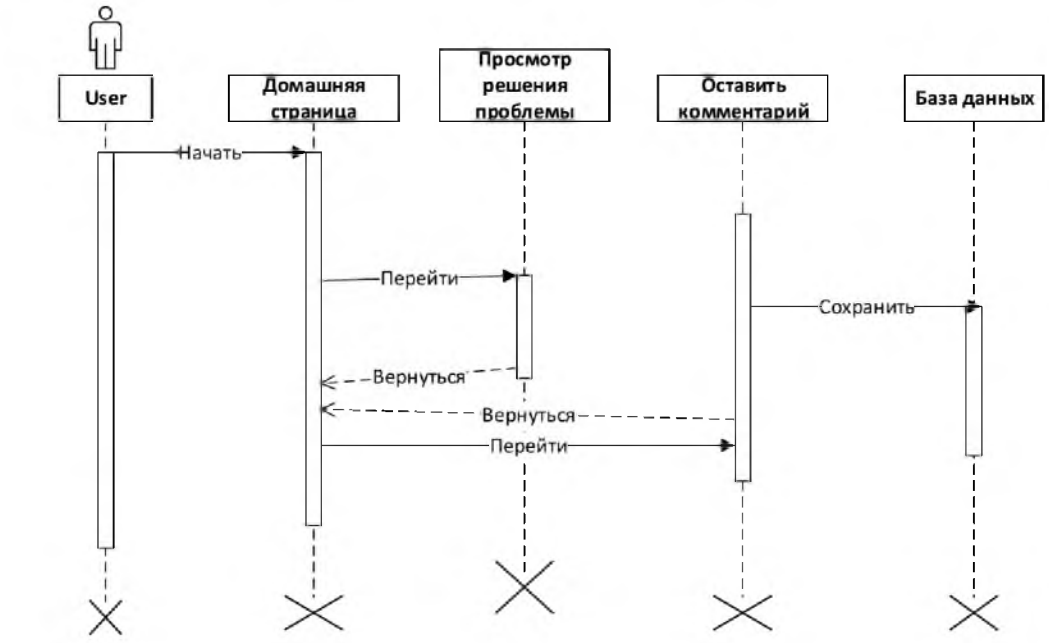


Рисунок 12 - Схема взаимодействия элементов с участием пользователя

Activity Diagram разбивает сложные процессы на управляемые элементы, улучшая понимание архитектуры разрабатываемого программного продукта. По рисунку 13, диаграмма активности демонстрирует последовательность

операций внутри системы удаленного доступа.

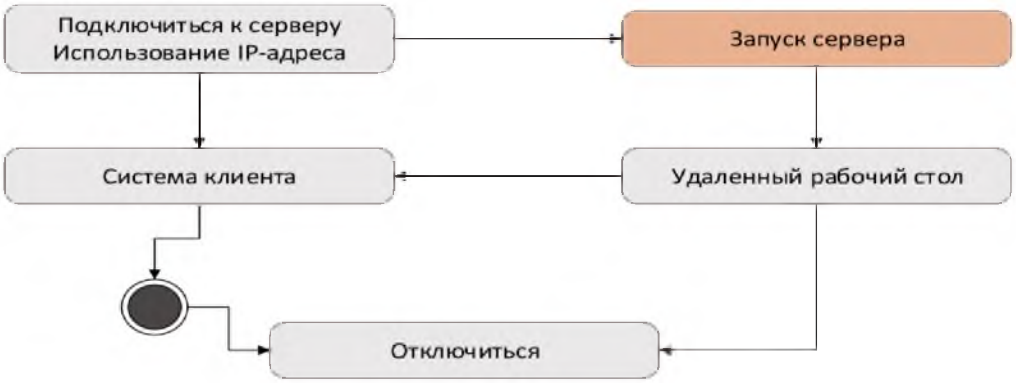


Рисунок 13 - Схема активностей, демонстрирующая удаленное подключение

На рисунке 14 демонстрируется процесс, при котором мониторинговая система верифицирует доступность дистанционного сервера до осуществления запроса данных по отслеживаемым метрикам.

Безагентный мониторинг выполняется на том же сервере, где установлено программное обеспечение системы мониторинга. Первым шагом является проверка доступности удаленного сервера. Для этого используется команда ping, чтобы убедиться, что дальнейшие шаги могут быть выполнены успешно. Если проверка доступности проваливается, процесс мониторинга для данного сервера прекращается.

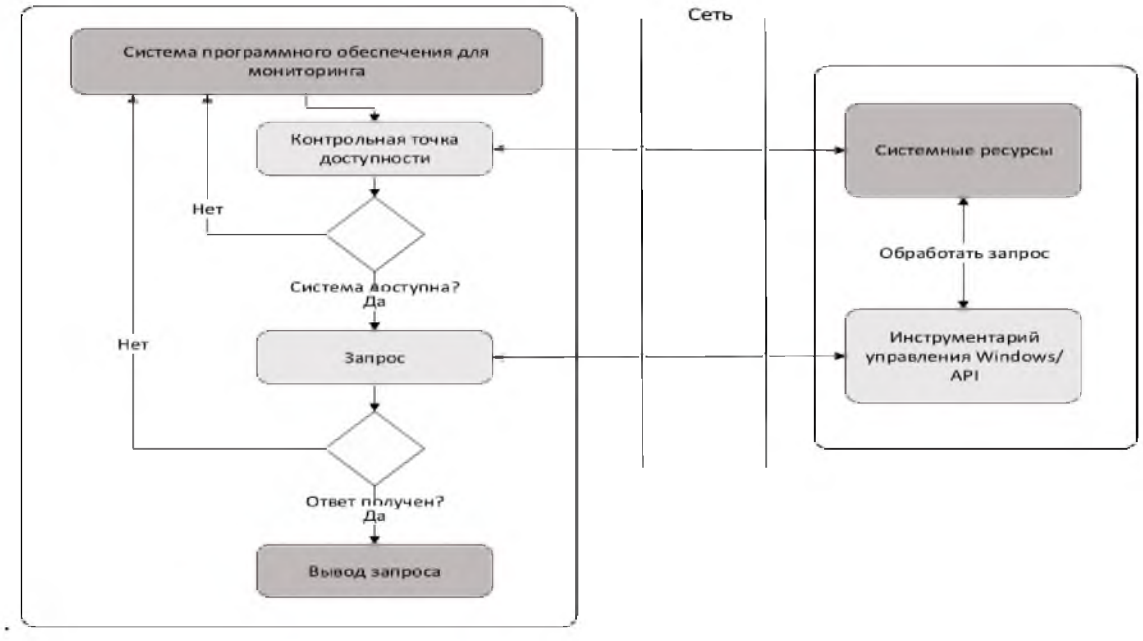


Рисунок 14 - Детализированное описание процесса передачи данных в системе мониторинга, основанной на технологии без установки агентов

После успешного подтверждения доступа, системный мониторинг инициирует запрос к удаленному хосту для изучения наличия инцидента безопасности и выявления трех инцидентов, связанных с операционной системой. Для установления связи используется либо Windows Management Instrumentation (WMI), либо утилита Sysinternals PsLogList, предварительно установленная на мониторинговом сервере. После этого отслеживаемый сервер получает детализированные команды для генерации отчетов по интересующим параметрам. Этот запрос обрабатывается, а полученная информация отправляется обратно на мониторинговый сервер. Полученные данные могут быть напрямую интегрированы в ПО системы мониторинга или сохранены в виде локального файла для дальнейшей обработки.

Архитектурное строение типа клиент-сервер [21], применяемое для создания данного приложения, демонстрируется на рисунке 15.

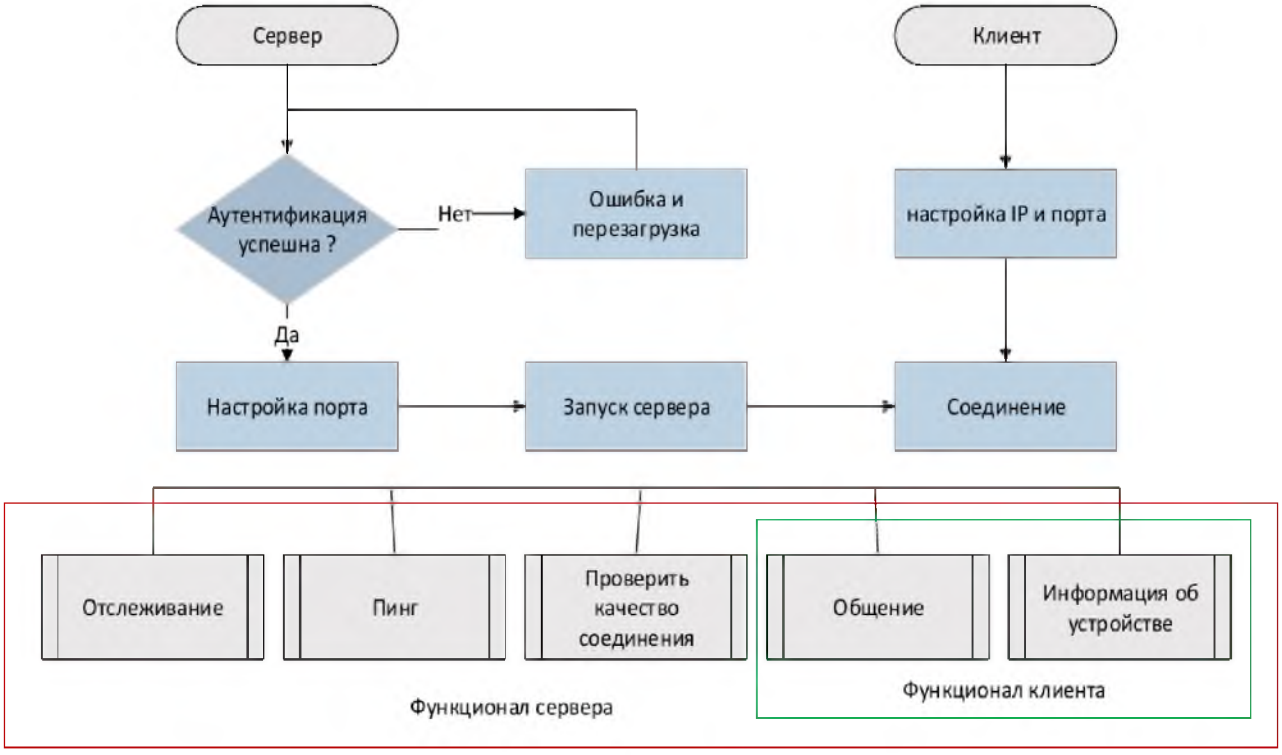


Рисунок 15 - Клиент-серверная архитектура

3 Внедрение и оценка экономической выгоды системы контроля локально-вычислительных сетей

3.1 Внедрение системы контроля за вычислительной сетью предприятия

В этом разделе описывается разработка предложенной системы для наблюдения за сетью. Для создания системы выбран язык C# и интегрированная среда разработки Visual Studio, благодаря возможностям платформы Microsoft .Net, которая предоставляет обширные инструменты для разработчиков сетевого ПО. Выбор C# обусловлен его мощными встроенными сетевыми библиотеками под Windows, что позволяет эффективно использовать функционал .Net Framework для создания приложений, предназначенных для работы под управлением Windows.

Это приложение реализовано с использованием клиент-серверной архитектуры. Основа функционирования заложена в присутствии приложения на устройствах как клиента, так и сервера. Благодаря тому, что сервер находится в сети, клиенты могут осуществлять подключение к нему, применяя уникальный порт и IP-адрес сервера [13].

Давайте более подробно остановимся на архитектуре серверной стороны рассматриваемой системы. Серверная часть предоставляет весь спектр функциональностей, которыми обладает реализованный проект. В качестве начальной точки развертывания была создана авторизационная страница. Это позволяет администратору получить доступ к сервисным возможностям системы посредством введения специально установленных учетных данных: логина и пароля. Эти данные предварительно занесены в специализированную базу данных и используются для верификации личности.

Модуль удаленного управления [15] — это начальный раздел, разработанный специально для управления сервером администратором.

В сегменте управления на расстоянии можно выделить четыре ключевых элемента: конфигурация портов, дистанционное руководство, регистрация событий, а также платформа для обмена сообщениями.

Секция управления на расстоянии представлена на рисунке 16.

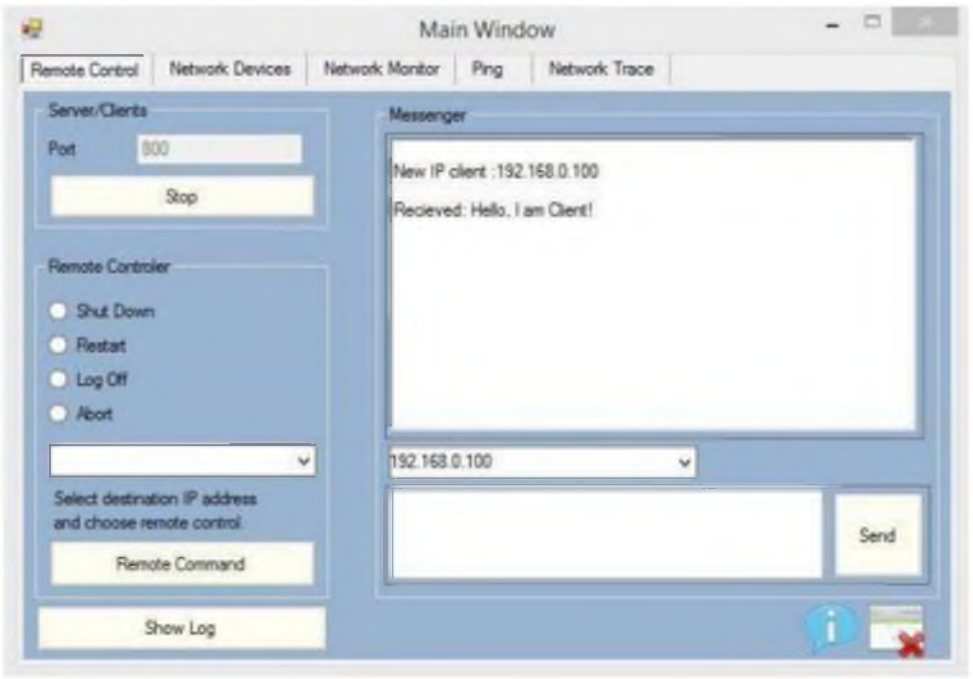


Рисунок 16 - Управление на расстоянии

Основной функцией сервера является инициация соединения, обеспечивающая возможность подключения к нему клиентских приложений. Для удобства использования был задан стандартный порт, тем не менее, при необходимости, администратор имеет возможность модифицировать его значение.

В сегменте удаленного управления, последующем установлению связи между клиентом и сервером, доступны специфические настройки для эксплуатации администратором сервера [24].

На следующей стадии администрации сервера, необходимо осуществить выбор конкретного IP-адреса подключённого к сети клиентского устройства из предложенного списка в данном интерфейсе. Определившись с нужным клиентом, сервер получает возможность направления целевых сообщений напрямую этому устройству и, кроме того, обретает привилегии доступа к его системе для выполнения операций на рабочем столе клиента. При активации функции просмотра журналов через соответствующую кнопку в интерфейсе, администратору представляется возможность ознакомления с

архивированными записями событий, структурированными в специфичном для журнала формате.

Как можно увидеть из изображения 16, каждое подключение нового клиента к серверу в сегменте мессенджера этой платформы генерирует уведомление для пользователя сервера, содержащее IP-адрес подключившегося клиента. В дополнение, администратор на серверной стороне, выбрав определенный IP-адрес клиента, получает возможность выполнения различных заранее установленных действий. Например, в функционале дистанционного управления после выбора IP, сервер имеет опцию дистанционного выключения устройства клиента через активацию соответствующей команды.

Изучим категорию сетевых компонентов [16]. Ниже представленный код на рисунке 17 демонстрирует ключевой элемент данной категории.

```
private void frmMain_Load(object sender, EventArgs e)
{
    try
    {
        m_Index = -1;
        NetworkManager.Instance.StarMonitor();
        m_IsAlive = true;
        UIInvoke = new MetodInvoker(UpdateUI);
        Initial();
        _thread = new Thread(new ThreadStart(UpdateStatus));
        _thread.Start();
    }
    catch (Exception)
    {
        Messagebox.Show()
    }
}
```

Рисунок 17 – Часть исходного кода для контроля сетевой активности

Изначально переменная с именем m_Index должна быть неинициализированной, что достигается путем присвоения ей значения -1 для ее инициализации с нулевым значением. В контексте мониторинга сетевых устройств, хост должен находиться в состоянии активности. Для определения активности хоста применяется метод StartMonitor. В случае обнаружения

активности хоста, через вызов MethodInvoker происходит активация пользовательского интерфейса, который последовательно перенаправляется в специфически заданную область внутри системного интерфейса.

Раздел управления сетью разбит на две секции. Первая секция предусматривает выбор информации о сетевом оборудовании из заранее заданного выпадающего списка (см. рисунок 18). Вторая секция представляет собой системную сводку, отображающую данные о конкретном выбранном сетевом устройстве [8].

Следовательно, при выборе любого устройства из выпадающего списка сетевых устройств, соответствующие данные будут мгновенно отображены в заранее определенном поле.

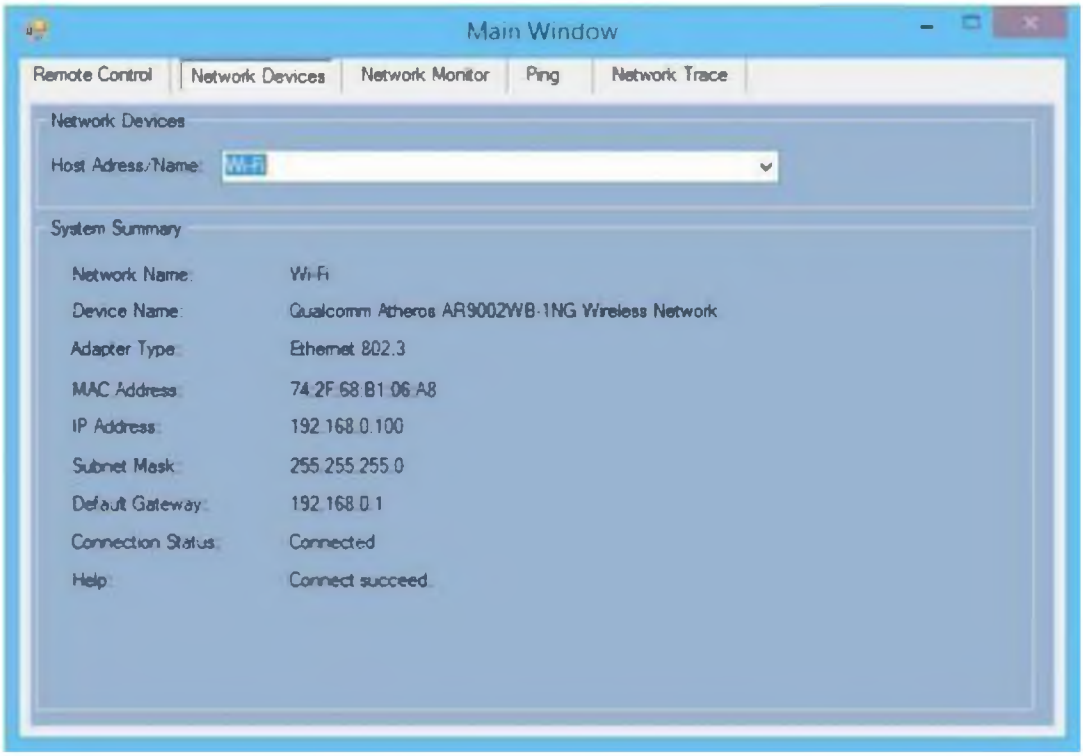


Рисунок 18 - Сетевой компонент

На рисунке 18 проиллюстрирован выбор подключения через Wi-Fi, представлены детальные спецификации [24]. К примеру, представлена спецификация используемого в сервере беспроводного адаптера, указанного в наименовании устройства. Дополнительно, демонстрируется текущее состояние подключения, где указывается, что связь установлена без ошибок, исключая

необходимость в использовании справочного раздела. Однако, в случае возникновения трудностей при подключении, секция справки предложит рекомендации по их решению.

В интерфейсе сетевой аналитики, пользователи могут из меню выбрать интересующий их IP-адрес для мониторинга. Активация процесса мониторинга происходит через нажатие на «Старт», после чего система начинает сбор данных о всех исходящих и входящих пакетах, ассоциированных с выбранным IP. Отображение этой информации происходит в заранее заданном разделе интерфейса. Для удаления собранных данных используется специальная функция, активируемая кнопкой, расположенной рядом с «Старт».

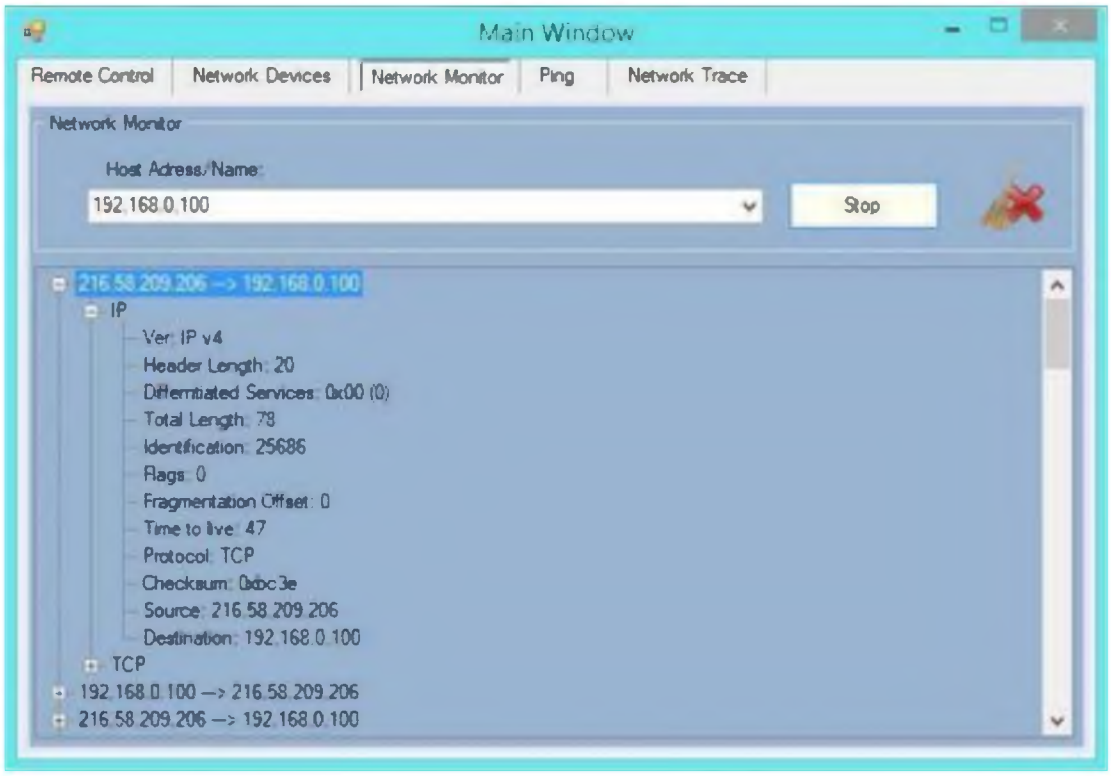


Рисунок 19 - Инструмент мониторинга сети отображает интернет-протокол

На рисунке 19 иллюстрируется процесс, в котором один из сетевых пакетов демонстрирует свое содержание для визуализации данных, содержащихся в IP-сегменте. В этом контексте, раскрыта важная информация, включая версию Интернет-протокола, размер заголовка пакета, используемый протокол, а также IP-адреса отправителя и получателя, в дополнение к другим значимым данным. Такой подход предоставляет администратору сети ценные

сведения о трафике, проходящем через сеть, что позволяет ему отслеживать и анализировать взаимодействия, осуществляемые клиентами в рамках сетевой инфраструктуры.

Протокол пользовательских дейтаграмм (UDP) представляет собой коммуникационный протокол, обеспечивающий базовый набор функций для передачи данных между устройствами в IP-сети.

На рисунке 20 демонстрируется образец описания сегмента UDP, содержащего исчерпывающие сведения [14][18].

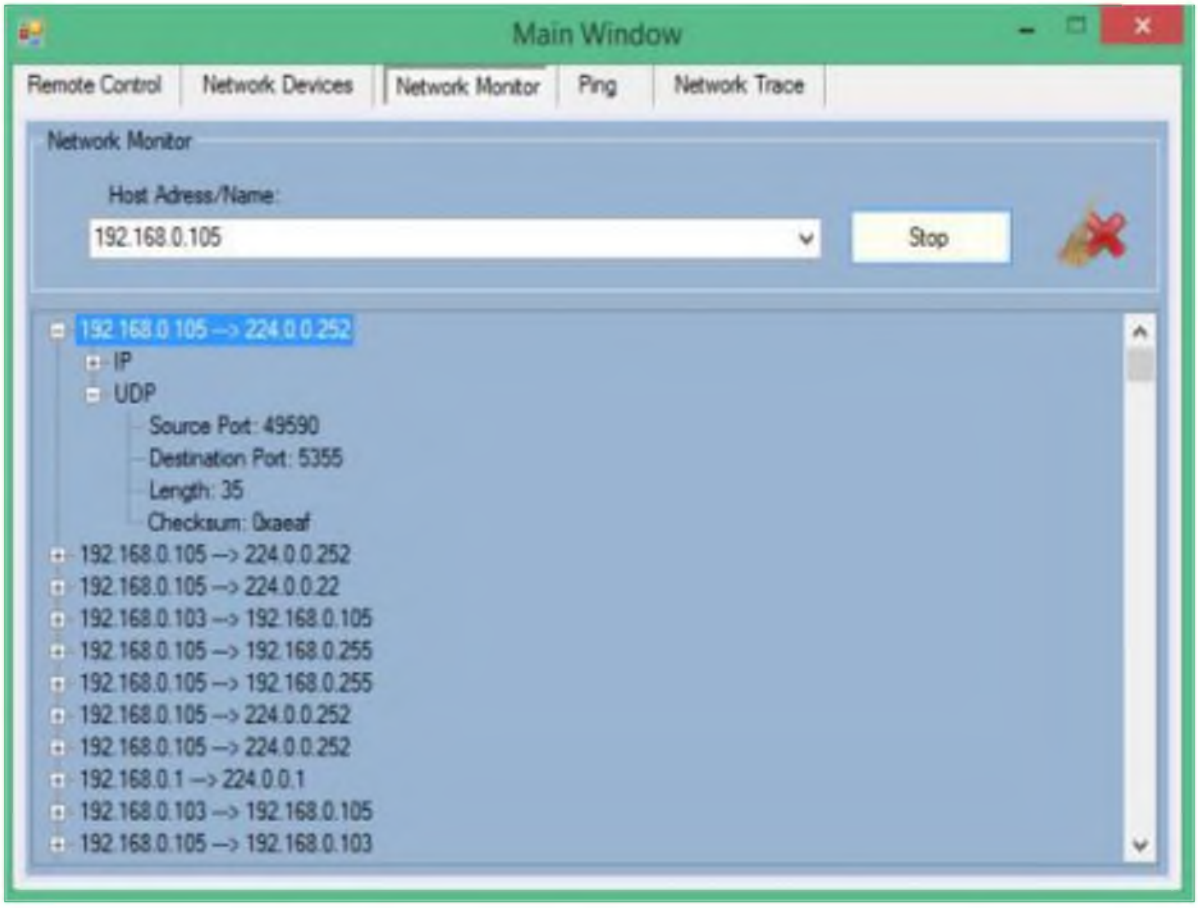


Рисунок 20 - Инструмент мониторинга сети демонстрирует протокол UDP

На рисунке 20 демонстрируются данные раздела мониторинга сетевых операций, охватывая порты отправителя и получателя, размер передаваемого пакета и его контрольную сумму для проверки целостности данных.

На иллюстрации 21 демонстрируется образец структуры сегмента TCP. В данном случае представлена детализированная спецификация заголовков индивидуальных пакетов, транслируемых через сеть, в контексте TCP.

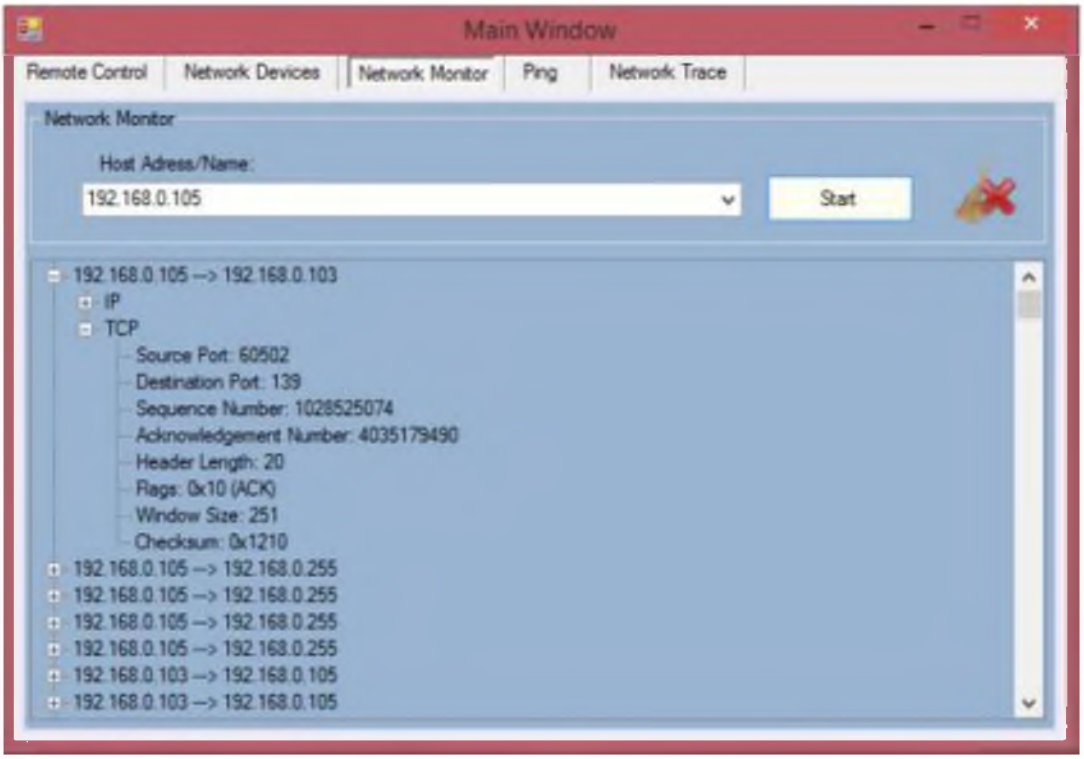


Рисунок 21 - Отслеживание активности сети (пример протокола TCP)

В иллюстрации 21 подробно изложены данные сетевой коммуникации, охватывая ключевые элементы, такие как локальные и удаленные порты связи, идентификаторы передачи, подтверждающие реакции принимающей стороны, размеры структур управления данными, а также управляющие биты, указывающие на текущее состояние передачи и другие параметры.

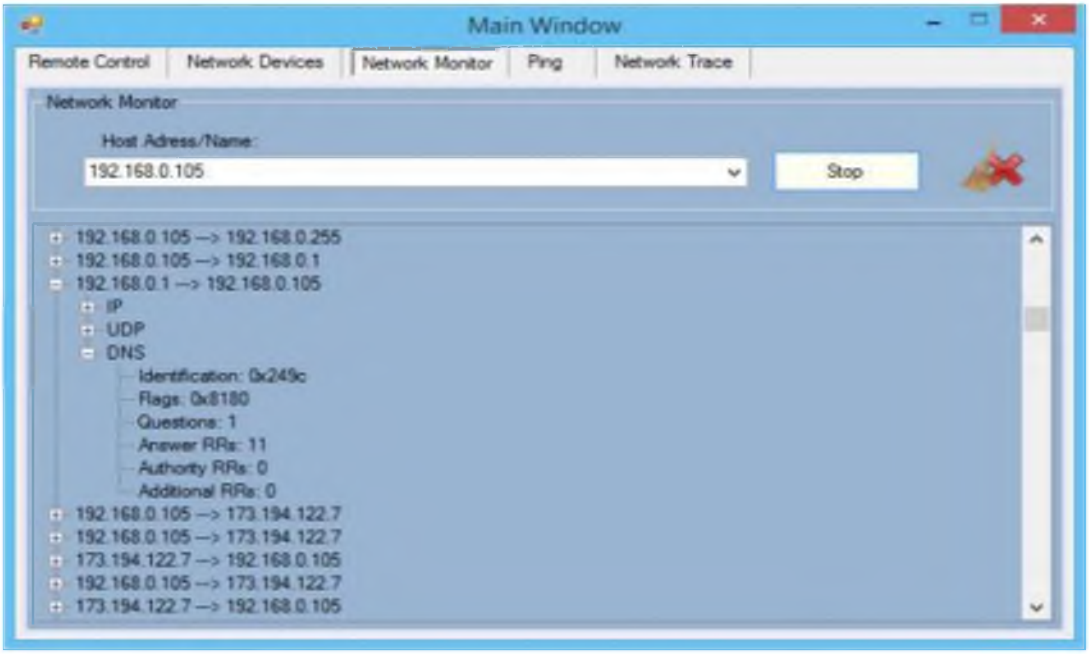


Рисунок 22 –Мониторинг сети

На рисунке 22 демонстрируется образец представления сегмента системы доменных имен (DNS), где детально отображены данные о заголовках пакетов внутри DNS раздела.

Давайте подробнее проанализируем раздел, посвященный тестированию соединения, указанный как [12]. Рисунок примера кода для функции ping представлена на рисунке 23.

```
private void cmdPing_Click(object sender, System.EventArgs e)
{
    if (txtHostname.Text == null || txtHostname.Text.Length == 0)
        return;
    cancel = false;
    lstResponses.Items.Clear();
    result = netMon.BeginPingHost(new AsyncCallback(EndPing), txtHostname, Text, 4);
    if (result != null)
    {
        cmdCancel.Visible = true;
        writelog("Ping \t + txtHostname.text + "\t- " + System.Datetime.Now.ToString());")
    }
}
```

Рисунок 23 - демонстрация фрагмента использования метода Ping

Этап программирования подразделяется на две ключевые проверки, ассоциированные с заранее заданным полем для введения имени хоста либо IP-адреса. Первое правило вступает в силу, когда данное поле остается пустым, что подразумевает отсутствие введенной информации. В такой ситуации вызов к команде ping через соответствующий метод для сбора данных не инициируется. Если же поле заполнено, активируется процесс отправки четырех ICMP-запросов на указанный адрес через функцию BeingPingHost, которая работает асинхронно с использованием AsyncCallback для обработки ответов. Ответ от процедуры пингования выводится в специально предназначенном для этого пользовательском интерфейсе элементе, называемом списочным полем. Вторая проверка касается записи полученных результатов в лог. Если данные в поле для ввода присутствуют, то результаты эхо-запросов фиксируются в специфическом лог-листе, предназначенном для хранения истории операций.

В секции ping клиент сервера вводит IP-адрес или доменное имя целевого хоста в соответствующее текстовое окно и активирует процесс, нажимая на

кнопку «Старт». Отображаемые данные ниже демонстрируют статус хоста, информируя сервер о его работоспособности или недоступности. Рисунок 24 отображает интерфейс секции ping.

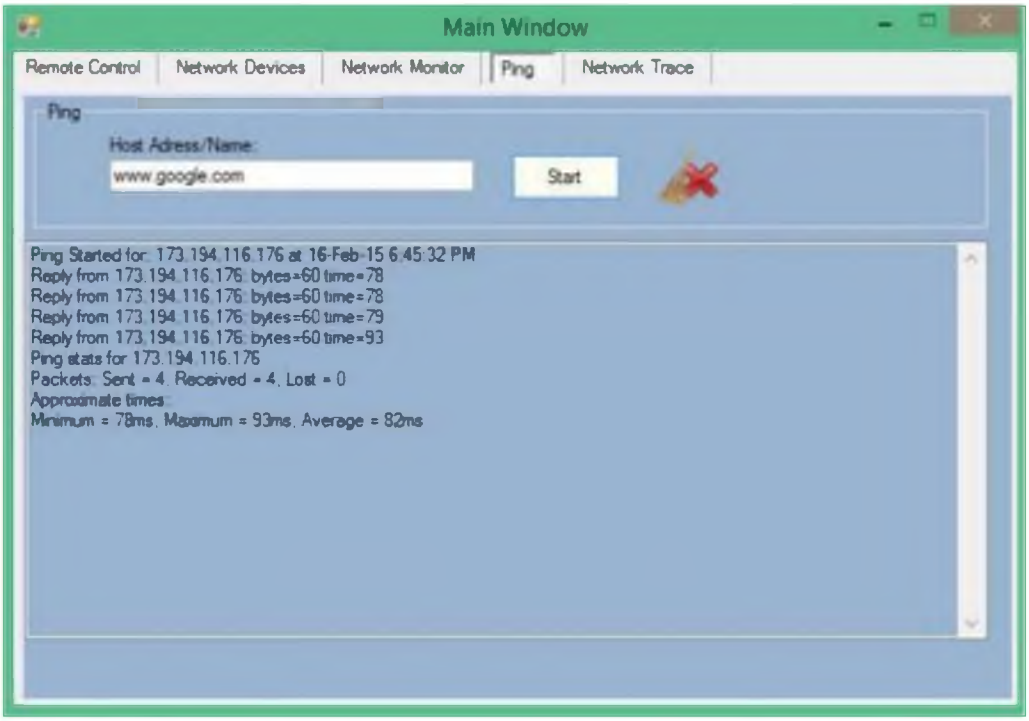


Рисунок 24 - Раздел проверки коммуникации

На рисунке 24 описывается использование инструмента ping для проверки доступности веб-сайта Google посредством его доменного имени и детализируется весь механизм отправки ICMP-запросов и получения ICMP-ответов для налаживания связи между клиентским и серверным оборудованием. Процедура ping заключается в инициации серии ICMP эхо-запросов к целевому хосту и анализе эхо-ответов. В ходе этой операции измеряется задержка (RTT) - время, необходимое запросу для достижения хоста и возвращения ответа, а также фиксируется статистика по потерянным пакетам. Выводимые данные включают в себя статистику по минимальной, максимальной и средней задержке, обеспечивая также сведения о количестве потерянных и успешно доставленных пакетов.

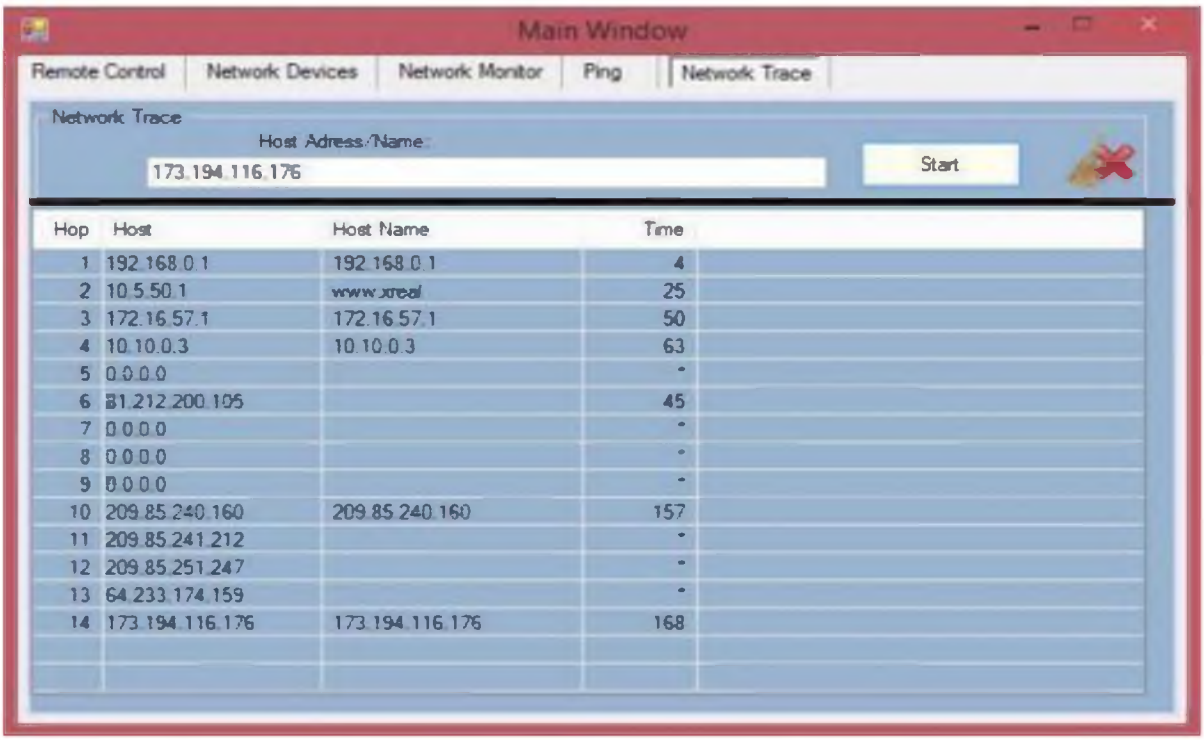
На рисунке 25 представлен сегмент кода, относящийся к выполнению сетевой трассировки. Из представленного фрагмента видно, что процесс начинается с ввода IP-адреса или доменного имени в специализированную

текстовую форму, которые затем подлежат трассировке. В дальнейшем, для обеспечения готовности к получению новых данных о пути следования данных, производится очистка ранее отображаемого списка элементов. Следование пакетов данных от отправителя к целевому серверу анализируется посредством функции tracert, позволяющей выявить маршрут передачи данных в сети. Все полученные в ходе трассировки сведения фиксируются и сохраняются в специализированном журнале для дальнейшего анализа.

```
private void startTrace_Click(object sender, EventArgs e)
{
    try
    {
        tracert.HostNameOrAddress = destination.Text;
        routeList.Items.Clear();
        tracert.Trace();
        writeLog("Trace \t" + destination.Text + "\t- " + System.DateTime.Now.ToString());
    }
    catch (SockedException ex)
    {
        Messagebox.Show(ex.Message, "Tracert Demo");
    }
}
```

Рисунок 25 - сегмент трассировки в сети

На рисунке 26, в секции сетевого мониторинга, системный администратор может внести необходимый IP-адрес узла в специальное поле.



Hop	Host	Host Name	Time
1	192.168.0.1	192.168.0.1	4
2	10.5.50.1	www.xreal	25
3	172.16.57.1	172.16.57.1	50
4	10.10.0.3	10.10.0.3	63
5	0.0.0.0		*
6	81.212.200.105		45
7	0.0.0.0		*
8	0.0.0.0		*
9	0.0.0.0		*
10	209.85.240.160	209.85.240.160	157
11	209.85.241.212		*
12	209.85.251.247		*
13	64.233.174.159		*
14	173.194.116.176	173.194.116.176	168

Рисунок 26 - Трассировка сети

Активация процессы через соответствующую кнопку позволяет вывести данные о трассировке маршрута от сервера до указанного узла в дизайнированном интерфейсе.

На рисунке 26 демонстрируется траектория связи от серверного оборудования до целевого IP-адреса, который в данном случае соответствует ресурсу www.google.com. Этот пример выделяет ряд маршрутизаторов и точек доступа, расположенных вдоль пути передачи данных от исходного сервера к веб-порталу Google. Важно подчеркнуть, что идентификационные номера IP международных маршрутизирующих узлов скрыты в интересах сетевой безопасности. Представленная информация включает в себя IP-адреса промежуточных сетевых элементов, обеспечивающих связность между отправителем и назначением. Дополнительно предоставляется хост-имя, если оно присвоено, для удобства идентификации. Временные показатели, как и другие детали, фиксируются в миллисекундах и отражают предполагаемую задержку обработки данных каждым элементом сети на выбранном пути.

В контексте архитектуры сервера, критично обеспечить его назначение с фиксированным IP-адресом.

Обусловлено это потенциальной проблемой во взаимодействии с функциональностью мониторинга сетевых подключений, где динамический IP-адрес клиентского устройства не будет корректно идентифицирован и отражен в пользовательском интерфейсе, конкретно в выпадающем списке доступных адресов.

Это связано с тем, что данная система функционирует на основе сетевого уровня модели OSI, а именно на третьем уровне, который отвечает за логику пересылки данных в сети Internet на основе протоколов TCP/IP. Переход к аспектам взаимодействия с системой со стороны клиента предполагает дальнейшее обсуждение.

В пользовательском интерфейсе данного приложения, как демонстрируется на рисунке 27, доступны различные настройки для соединения клиента с сервером.

Рисунок 27 - Сторона клиента

Введя IP адрес сервера и задав соответствующий номер порта, который должен быть аналогичен порту на сервере, пользователь может успешно подключиться к серверной системе. Это позволяет начать обмен данными между клиентом и сервером. Более того, пользовательское программное обеспечение позволяет мониторить состояние сетевого оборудования. В случае обнаружения сбоев или отключений, система предложит варианты решения проблем, детально описанные на рисунке 28.

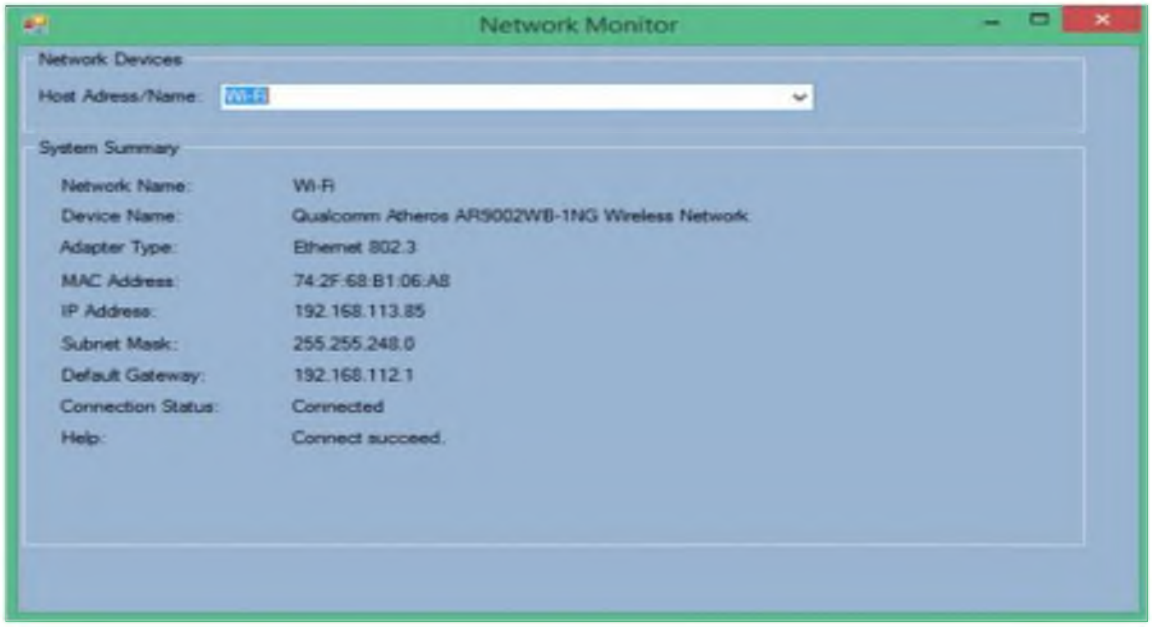


Рисунок 28 - Данные об аппаратном средстве для заказчика

Рисунок 27 демонстрирует передачу данных от пользователя к центральному компьютеру, согласно источнику [22]. На рисунке 28 изображена спецификация аппаратуры с точки зрения пользователя.

В докладе по анализу доступности (рисунок 29) представлены данные о мониторинге состояний серверной инфраструктуры во временном разрезе на протяжении одного года. Визуализация статусов выполнена с использованием цветовой дифференциации, где красный цвет обозначает недоступность сервера или его отключение, зеленый — обеспечивает информацию о его полной функциональности, желтый цвет указывает на периоды простоя оборудования, в то время как серый – сигнализирует о неподключении мониторингового агента к серверу.

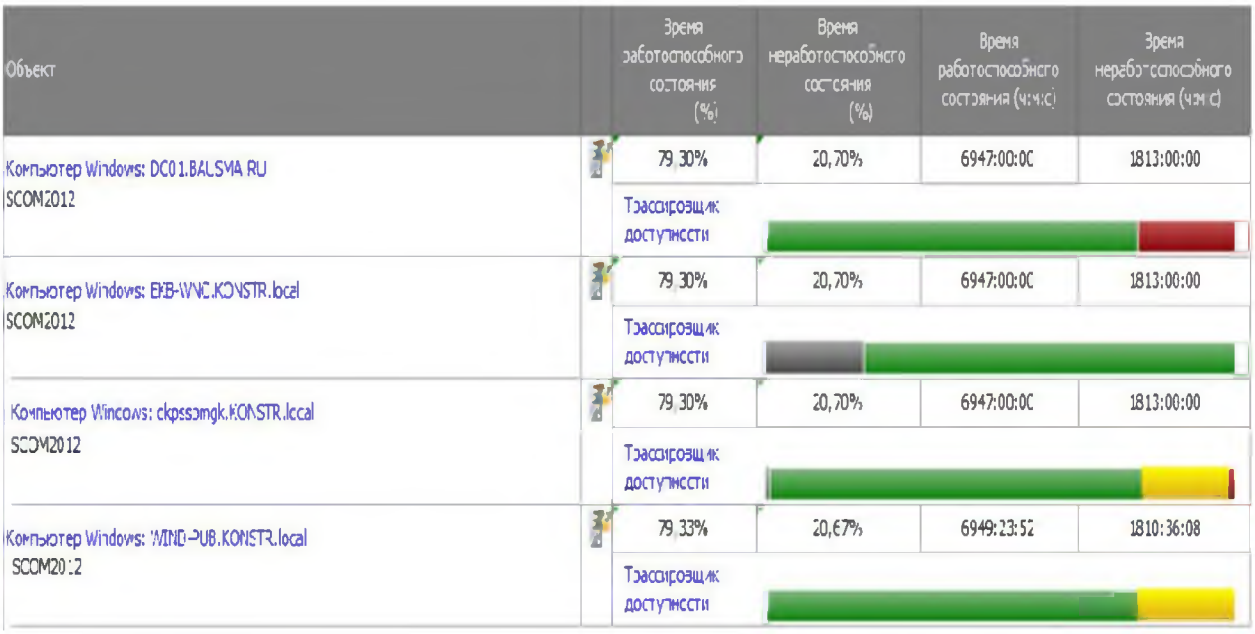


Рисунок 29 - Анализ функционирования серверной инфраструктуры

Аналитический отчет предоставляет глубокий анализ эффективности работы серверов и прочих компонентов сетевой инфраструктуры за заданный интервал времени, представляя неоценимый инструментарий для системного администратора. Этот инструмент выявляет неиспользуемые ресурсы, а также идентифицирует нефункционирующее или вышедшее из строя оборудование. Дополнительная функциональность включает возможность автоматической отправки этих отчетов на электронную почту не только системным

администраторам, но и руководящему звену, обеспечивая основу для оперативного реагирования на возможные инциденты, что может потребовать экстренного вмешательства для ремонта или корректировки распределения нагрузки между устройствами.

3.2 Вычисление параметров экономического результата деятельности

Оценка экономической эффективности позволяет рационально оценить целесообразность инвестиций в новые программные решения для бизнеса. Исходно, технические специалисты обрабатывали запросы клиентов вручную, без помощи специализированных информационных систем. В качестве альтернативы предложено использование инновационной автоматизированной системы, разработанной в рамках исследовательского проекта бакалавриата.

В таблице 9 изложены однократные капитальные расходы на разработку информационной системы.

Таблица 9 - Расходы на разработку информационной системы

Затраты	Состав затрат	Планируемая сумма (руб.)
Затраты на проектирование ИС	Затраты на заработную плату проектировщиков	21000
	Затраты на инструментальные программные средства для проектирования	0
	Затраты на средства вычислительной технически для проектирования	831
	Прочие затраты на проектирование	654
Затраты на технические средства управления		600
Затраты на создание линий связи локальных сетей		0
Затраты на программные средства		0
Затраты на формирование информационнойбазы	ЗП разработчика	10000
	Работа ЭВМ	296
Затраты на обучение персонала	ЗП обучаемого	1660
Затраты на опытную эксплуатацию	ЗП разработчика	7000
	Работа ЭВМ	237

В итоге, общий объем расходов на содержание и обслуживание достигает 42361 рубля.

На рисунке 30 изображена схема, демонстрирующая распределение элементов капитальных инвестиций в проекте.

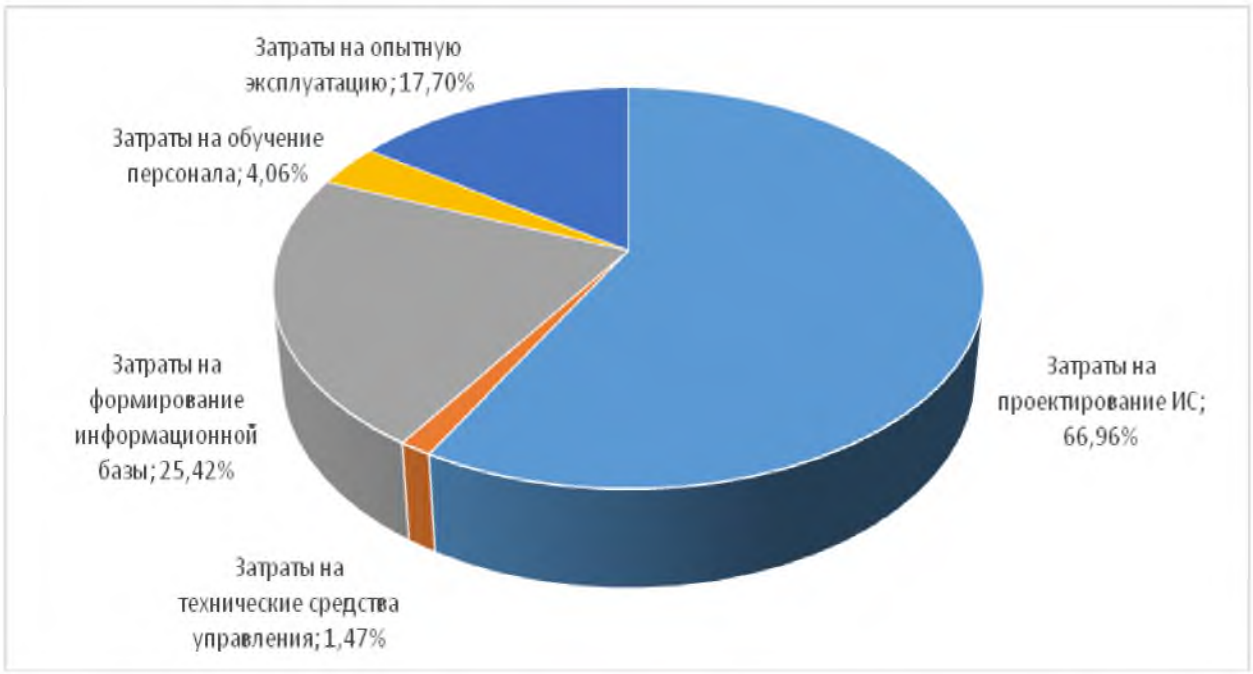


Рисунок 30 – Распределение статей расходов на капитальные вложения в проекте

Таблица 10 содержит информацию о затратах на эксплуатацию.

Таблица 10 – Затраты на эксплуатацию при разработке системы мониторинга.

Затраты	Сумма, руб
Оклад системного администратора	0
Амортизационные отчисления	7500
Расходы на техобслуживание	6000
Расходы, ассоциируемые с применением мировых информационно-вычислительных сетей Интернет	4200
Затраты на носители информации	0
Прочи езатраты	354

В итоге, общая величина годовых операционных расходов достигает 21240 рублей.

На изображении 31 изображена диаграмма, иллюстрирующая распределение различных статей операционных расходов в рамках проекта.

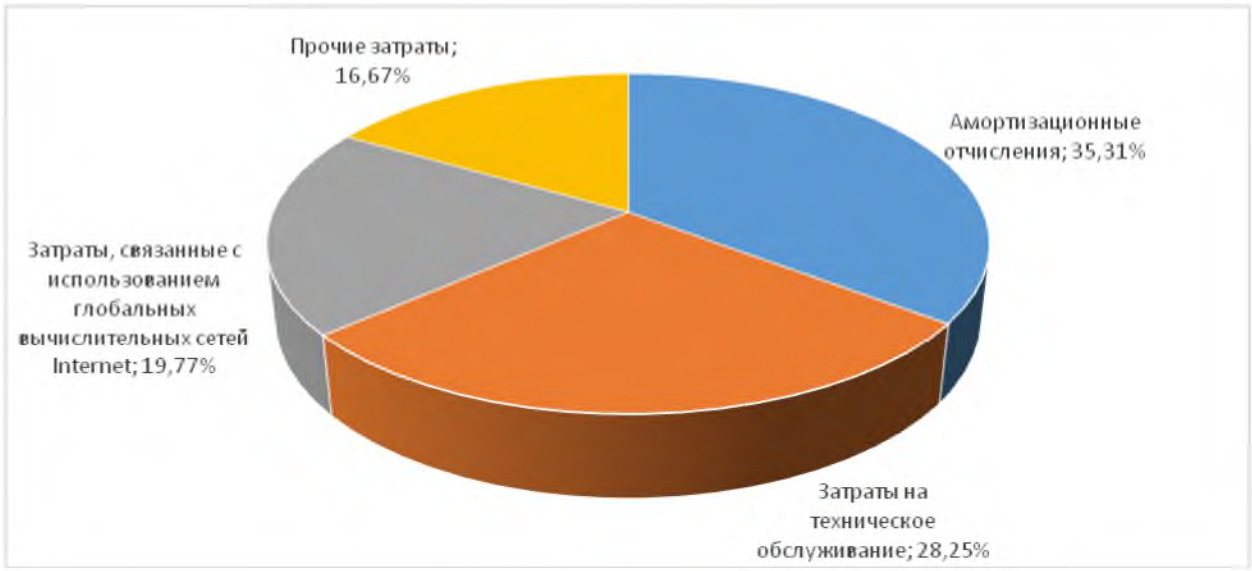


Рисунок 31 – Структура операционных расходов

Операционные издержки, в отличие от инвестиционных вложений, носят регулярный характер и возникают при каждом производственном цикле, при этом их величина подсчитывается на годовой основе. Они совершаются параллельно с процессами производства товаров или предоставления услуг. Такие затраты прямо влияют на формирование себестоимости выпускаемой продукции или оказываемых услуг.

Следовательно, ясно, что применение проектного подхода способствует значительному сокращению временных и финансовых потерь. Этот исход тем самым подтверждает, что рекомендуемая методика обеспечивает решение целей с двойной скоростью и продуктивностью по сравнению с исходным методом, представляя значительные преимущества для бизнеса. Представленное решение способствует оптимизации расходов и улучшению качества и производительности труда персонала.

Заключение

В выпускной квалификационной работе (ВКР) подробно изложены ключевые принципы управления сетевым мониторингом, обеспечения безопасности через удаленный доступ, а также другие связанные технологические понятия. Анализируется ряд подобных исследований в данном направлении, с осуществлением сопоставления функциональных возможностей разработанного программного обеспечения с альтернативными решениями на рынке. Дополнительно, детализированно представлены этапы развертывания, протоколы взаимодействия и необходимые условия для эффективной интеграции реализованного продукта в существующую инфраструктуру, обеспечивая четкое понимание процессов на каждом шаге.

Исследование рынка инструментов для мониторинга производительности сетевых инфраструктур выявило, что такие системы обеспечивают возможность наблюдения и управления параметрами производительности, аналитикой и диагностикой ошибок в сетях на базе Интернет-протокола (IP). Оказалось, что такой инструментарий представляет собой ценный ресурс для системного администратора, дающий способность непрерывно контролировать состояние сети, основываясь на равномерно собранных данных через установленные интервалы времени.

На основе анализа можно заключить, что стандартная сетевая инфраструктура включает в себя ряд устройств, включая мосты, репитеры, свитчи и роутеры. Отслеживание состояния этих компонентов, а также поддержание эффективной передачи данных является критически важным для гарантии непрерывности операций в компьютерных системах организации. Предложенный продукт будет похож на текущие решения на рынке, но отличаться предоставлением привлекательного пользовательского интерфейса и функционалом обмена сообщениями в реальном времени.

В контексте выпускной квалификационной работы создана базовая система для наблюдения за сетью. Обзор литературы выявил, что

представленные на рынке решения для мониторинга сетевых активностей обладают комплексным пользовательским интерфейсом, кроме тех, что функционируют на принципах командной строки.

Преминаной задачей выпускной квалификационной работы стало разработка системы мониторинга сети с интуитивно понятным интерфейсом, охватывающей основные требуемые возможности. Функциональность по мониторингу и анализу трафика обеспечит оператору возможность надзора за безопасностью сетевой инфраструктуры.

Система соответствовала всем заявленным функциональным критериям, включая:

1) платформа предоставляет решение возникшей у пользователя задачи и дает возможность ему разместить описание проблемы,

2) Данные хранятся в дата-центре, доступ к которому имеют только авторизованные сотрудники, обеспечивая эффективное управление IP-адресацией.

Электронная система контроля сети способна выполнить любые возложенные на нее функции, включая:

1) надежная функционирующая система управления базами данных для передачи информации о неполадке.

2) созданная мультифункциональная база данных для обмена информацией о регистрации инцидентов,

3) платформа, предназначенная для запроса данных о неполадках и способах их устранения, связанных с клиентами, подразделениями и объектами недвижимости, доступная из различных локаций.

Внедрена система наблюдения за локальной вычислительной сетью, обеспечивающая анализ производительности серверов и периферийных устройств за определенные интервалы времени. Экономическая оценка проекта подтвердила его высокую эффективность за счет оптимизации операционных процессов и минимизации ошибок, что значительно снижает операционные риски сети организации.

Сетевая мониторинговая система может находить применение как среди студентов, так и среди новичков в данной области. Следовательно, данное приложение может служить в качестве учебного инструмента.

Список литературы

1. Авдеева, В.В., Васильева, Е.А. Проектирование и внедрение систем мониторинга. – М.: ИНФРА-М, 2021. – 432 с.

2. Белокуров, В.П., Калмыкова, С.В. Мониторинг и анализ производительности серверов. – СПб.: Питер, 2022. – 496 с.

3. Воробьев, А.В., Якушев, Д.В. Системы мониторинга и управления сетевыми инфраструктурами. – М.: Горячая линия-Телеком, 2021. – 528 с.

4. Горбунов, А.А., Зайцев, А.В. Проектирование систем мониторинга и диагностики вычислительных комплексов. – М.: Лаборатория знаний, 2022. – 368 с.

5. Дмитриев, В.А., Кузнецов, А.В. Разработка и проектирование систем мониторинга серверов и сетевого оборудования. – М.: Солон-Пресс, 2021. – 640с.

6. Егошин, А.В., Михайлов, А.С. Современные подходы к мониторингу и анализу производительности серверов. – М.: Техносфера, 2022. – 352 с.

7. Зайцева, Е.В., Кузьмин, А.В. Оптимизация производительности серверов и сетевых инфраструктур. – СПб.: Питер, 2021. – 304 с.

8. Иванова, С.В., Смирнова, А.В. Методы и инструменты мониторинга и анализа производительности серверов. – М.: Инфра-М, 2022. – 320 с.

9. Климова, Е.В., Петров, В.Н. Информационные системы и их мониторинг. – СПб.: Питер, 2021. – 672 с.

10. Колесникова, Е.В., Орлов, А.В. Проектирование и реализация систем мониторинга IT-инфраструктуры. – М.: Бином-Пресс, 2022. – 560 с.

11. Максимов, Н.В., Голицына, О.Л., Попов И.И. Информационные технологии: учеб. для вузов. – М.: Форум, Инфра-М, 2022. – 416 с.

12. Новиков, А.В., Сидоров, А.В. Анализ и оптимизация производительности серверных систем. – М.: ДМК Пресс, 2021. – 768 с.

13. Павлова Е.В., Федоров А.А. Информационная безопасность и

защита информации. – М.: Горячая линия-Телеком, 2022. – 544 с.

14. Рудаков, А.В., Степанов ,А.В. Современные методы мониторинга и анализа производительности серверов. – М.: Техносфера, 2021. – 360 с.

15. Сергеев, А.В., Тихонова, Е.В. Проектирование и администрирование серверов. – М.: Вильямс, 2022. – 608 с.

16. Смирнов, А.В., Шипилов, А.В. Мониторинг и диагностика компьютерных систем. – М.: Академия, 2021. – 480 с.

17. Степанов, А.В., Чернышов, А.В. Сети ЭВМ и телекоммуникации. – М.: Интернет-Университет Информационных Технологий, 2022. – 704 с.

18. Тарасов, А.В., Устинов, А.В. Компьютерные сети и их мониторинг. – СПб.: Питер, 2021. – 800 с.

19. Уваров, А.В., Федотов, А.В. Архитектура компьютеров и их мониторинг. – М.: Лаборатория знаний, 2022. – 624 с.

20. Чернявский, А.В., Щукин, А.В. Защита информации в компьютерных системах и сетях. – СПб.: Питер, 2021. – 592 с.

21. Шамрай, А.В., Яковлев, А.В. Управление производительностью информационных систем. – М.: Горячая линия-Телеком, 2022. – 320 с.

22. Kurose J.F., Ross K.W. Computer Networking: A Top-Down Approach. – Pearson Education, Inc., 2022. – 896 p.

23. Mike O'Leary. Cyber Operations: Building, Defending, and Attacking Modern Computer Networks. — Towson, MD, USA — 2019. — 1151 pForouzan B.A. Data Communications and Networking. – McGraw-Hill, 2022. – 928 p.

24. Hartmann T., Kremer H.-J. Monitoring and Management of IT Infrastructure. – Springer, 2021. – 504 p.

25. Янг Алекс, Мек Б., Кантелон М. Node.js в действии / Алекс Янг, Брэдли Мек, Майк Кантелон, 2-е изд. — СПб.: Питер, 2018. — 432 с.

26. Nw.js [Электронный ресурс]. - URL: https://nwjs.io/ (дата обращения 20.12.2024).

27. Десктопные приложения на html, css и js для winows, mac os, linux. Подробный обзор nw.js (бывший node-webkit) – URL: https://html5.by/blog/nwjs/

(дата обращения 20.12.2024).

28. Node.JS приложения с почти нативной производительностью URL: https://dzen.ru/a/X3SDDqS1XxqRlaWe (дата обращения 20.12.2024).

29. Nodejs / node-gyp. URL: https://github.com/nodejs/node-gyp (дата обращения 20.12.2024).

30. Костяков И. Многопоточность на фронте: абсурд или прекрасное архитектурное решение. URL: https://habr.com/ru/articles/701914/ (дата обращения 20.12.2024).