МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование)

09.03.03 Прикладная информатика
(код и наименование направления подготовки / специальности)

«Бизнес-информатика»
(направленность (профиль) / специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

на тему Разработка системы мониторинга локально-вычислительной сети организации

Обучающийся Ю.С. Мишушин
(Инициалы Фамилия) (личная подпись)

Руководитель В.В. Дружинкин
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2022

Аннотация

Тема бакалаврской работы «Разработка системы мониторинга локально-вычислительной сети организации».

Бакалаврская работа посвящена разработке системы мониторинга локально-вычислительной сети организации. В работе проведет анализ существующих моделей и инструментов мониторинга сетей, рассмотрен процесс проектирования и реализации локальной вычислительной сети организации, приведена оценка экономической эффективности предложенной системы.

Целью ВКР является проектирование и разработка системы мониторинга локально-вычислительной сети организации.

Объектом исследования является – система мониторинга вычислительной сети. Предмет исследования – особенности процесса мониторинга локальной вычислительной сети.

Практическая значимость ВКР состоит в том, что спроектированная и реализованная система мониторинга позволит отслеживать производительность и эффективность сети организации.

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 проекта.

Результатом ВКР является разработанное приложение для мониторинга локальной сети организации, которое обеспечит возможность автоматизированного отслеживания производительности и эффективности сети, что позволит сократить временные затраты в процессе решения данных задач.

Оглавление

Введение

Система мониторинга сети играет важную роль в обеспечении безопасности и управлении сетью. Мониторинг сети относится к наблюдению за событиями, происходящими в сети, с целью обеспечения безопасности и устойчивости сети. Однако многие малые и средние компании и организации предпочитают избегать этого факта. Самая важная причина для таких компаний заключается в том, что у них нет профессиональных сетевых администраторов, которые могли бы использовать доступную на рынке систему мониторинга сети. Это может повлечь затрат ими больших средств или даже потери капитала в случае сбоя сети.

В данной выпускной квалификационной работе будет предложена система мониторинга локальной вычислительной сети, которая поможет решить эту проблему благодаря простоте использования, а также предоставлению необходимых функций для мониторинга сети. Таким образом, преимуществом использования предлагаемой системы будет возможность ее использования даже начинающими пользователями, которые имеют только базовое представление об использовании компьютерных приложений. Таким образом, предложенное приложение мониторинга сети может быть использовано для малых и средних организаций, в случае отсутствия профессиональных сетевых администраторов.

Целью ВКР является проектирование и реализация системы мониторинга локально-вычислительной сети организации.

Для достижения поставленной цели необходимо решить следующие задачи:

– описать существующие модели мониторинга компьютерной сети,

– проанализировать существующие разработки и обосновать выбор технологии проектирования,

– спроектировать систему мониторинга сети,

– осуществить концептуальное проектирование системы локальной вычислительной сети организации,

– выполнить логическое моделирование системы мониторинга сети,

– построить физическую модель вычислительной сети организации,

– реализовать систему мониторинга вычислительной сети организации,

– рассчитать показатели экономической эффективности работы.

Объектом исследования является – система мониторинга вычислительной сети.

Предмет исследования – организация процесса мониторинга локальной вычислительной сети.

Практическая значимость ВКР состоит в том, что спроектированная и реализованная система мониторинга позволит отслеживать производительность и эффективность сети организации.

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.

Результатом ВКР является разработанное приложение для мониторинга локальной сети организации, которое обеспечит возможность автоматизированного отслеживания производительности и эффективности сети, что позволит сократить временные затраты в процессе решения данных задач.

Глава 1 Анализ существующих моделей и инструментов сетевого мониторинга

1.1 Описание существующих моделей мониторинга компьютерной сети

Первые компьютеры, которые были изобретены много лет назад, имели корпус размером с комнату с автономным процессором, способным выполнять некоторые простые математические вычисления. За эти долгие годы, прошедшие с изобретения первых компьютеров, компьютеры совершенствовались. В настоящее время подключение является самой большой проблемой для этой технологии.

Компьютерная сеть представляет собой совокупность автономных компьютеров, связанных между собой единой технологией. Основными аппаратными компонентами (или узлами) компьютерной сети являются мосты, коммутаторы, маршрутизаторы и т. д. Эти компоненты подключаются через проводную среду (оптические волокна, коаксиальные кабели и т. д.) или беспроводную среду (WLAN, микроволновая печь, инфракрасный порт и т. д.). В зависимости от масштаба сети компьютерные сети можно разделить на персональную сеть (PAN), локальную сеть (LAN), городскую сеть (MAN), глобальную сеть (WAN), магистральную сеть и Интернет [2].

Мониторинг производительности сетевых систем позволяет пользователю просматривать и управлять качеством производительности, анализом данных и ошибками сети Интернет-протокола (IP). Инструмент мониторинга производительности является важным активом для системного администратора, позволяющим постоянно отслеживать работу сети на основе данных, собираемых через регулярные промежутки времени. Типичная сеть состоит из различных аппаратных устройств, таких как мосты, повторители, коммутаторы, маршрутизаторы и т. д. Мониторинг сети включает в себя

проверку правильности функционирования этих устройств, а также обеспечение доступности связующей среды.

Рассмотрим некоторые существующие модели сетевого мониторинга. Система мониторинга сети выполняет три основные функции: обеспечение бесперебойной и исправной работы сети, предоставление отчетов о состоянии сети и предоставление отчетов об отчетах о событиях.

Моррис Сломан [23] предложил модель мониторинга сети, которая модифицирует управление событиями в ранее предложенных моделях. Основное внимание в этой модели уделялось событиям и состоянию систем, подключенных к сети, а целью было создание отчета о мониторинге для отправки администратору сети.

В рассмотренной модели были созданы отчеты о событиях и состоянии, чтобы администратор мог анализировать производительность сети, а также взаимодействие между рабочими станциями. На рисунке 1 представлена конструкция рассмотренной системы.

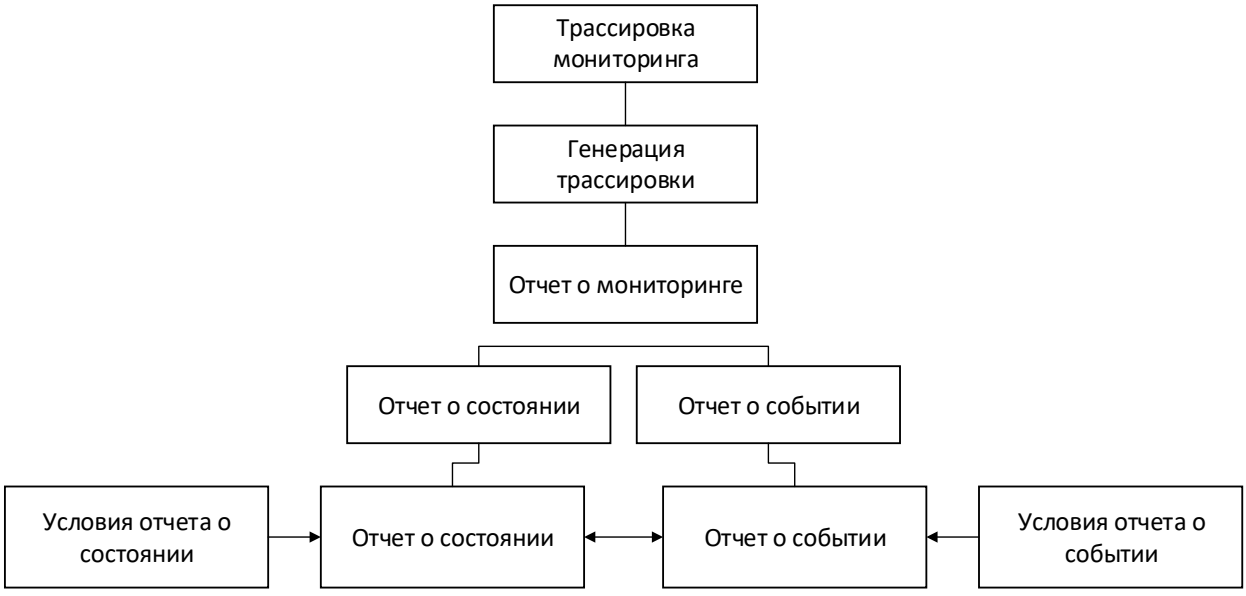


Рисунок 1 - Режим управления сетью

Другой моделью, которая была проанализирована, является модель DiMAPI [25]. Модель DiMAPI предлагает интерфейс прикладного

программирования (API) для мониторинга сети, который добавляет некоторые модификации к традиционным моделям мониторинга. Эта предлагаемая модель была вдохновлена традиционными моделями с использованием метода ping. Эта модель предполагает, что гладкая сеть должна контролироваться из множества точек. DiMAPI внес некоторые изменения в ранее предложенный метод, названный MAPI. Модель MAPI, которая была предложена до DiMAPI, опирается на единую систему мониторинга.

DiMAPI, в отличие от MAPI, фокусируется на мониторинге пакетов через ping, выполняя сетевой мониторинг в различных точках сети. DiMAPI предполагает, что использование метода ping может быть полезно для многих целей, таких как расчет пропускной способности, мониторинг событий, проверка состояния сети и так далее.

В [25] авторы представили основные функции DiMAPI, которые включают мониторинг трафика в сети и мониторинг одноранговых (P2P) взаимодействий. P2P, как сетевая терминология, относится к архитектуре клиент-сервер, в которой должен быть сервер и несколько рабочих станций, подключенных к этому серверу, для коммутации и взаимодействия. В предлагаемой модели для мониторинга трафика в сети использовался метод ping. Ping, отправляя пакеты на разные рабочие станции, подключенные к сети, а также получая их обратно, предоставляет ценную информацию о сетевом трафике.

Кроме того, в системах мониторинга сети важным моментом является предоставление предустановленных функций для пакетов, чтобы они могли доставлять конкретную информацию.

В предлагаемой в данной ВКР модели рабочие станции также должны быть оснащены клиентской версией системы мониторинга сети. Однако мониторинг активной и сложной сети, такой как сеть на производственном предприятии, может быть затруднен, если он выполняется вручную. В связи с этим вместо ручного мониторинга активной сети была представлена модель

интеллектуального мониторинга. В модели интеллектуального мониторинга в заданный интервал времени пакеты будут отправляться сервером и возвращаться обратно рабочей станцией, чтобы иметь фиксированное соединение между рабочими станциями и сервером. Согласно тестам, проведенным при активном мониторинге сети, модель DiMAPI представляет собой интеллектуальную систему мониторинга сети, которая помогает в мониторинге в реальном времени, а также обеспечивает более безопасную сеть.

Рассмотрим, как осуществляется удаленный доступ. В системе мониторинга сети удаленный доступ предоставляет администратору сети авторизованный доступ для выполнения необходимых действий в системах, подключенных к сети, таких как коммутаторы, маршрутизаторы и рабочие станции.

Для предоставления удаленного доступа информация протокола управления передачей (TCP) будет транслироваться прокси-сервером на консольный порт маршрутизатора и приниматься обратно. Что касается этого процесса, все устройства, подключенные к указанному прокси-серверу, будут готовы к удаленному доступу, осуществляемому пользователем сервера. Администратор сервера принимает решение о необходимой активности на каждом подключенном устройстве.

Рисунок 2 отображает этот процесс.

Сетевой администратор устанавливает соединение между двумя маршрутизаторами, подключенным к интерфейсу системы сетевого мониторинга, и маршрутизатором, подключенным к рабочим станциям. Как было сказано ранее, каждая рабочая станция должна быть оснащена клиентской версией системы. Установив соединение между сервером и рабочими станциями, можно выполнять все необходимые действия между ними.

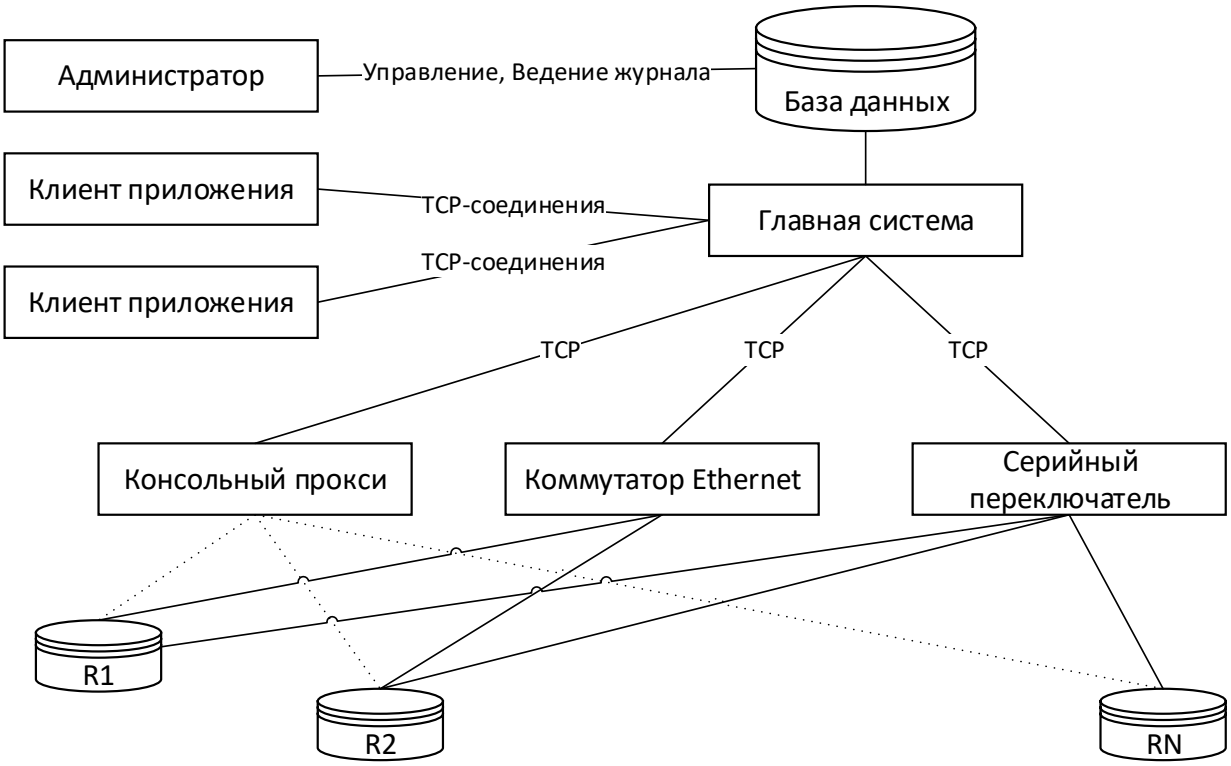


Рисунок 2 - Процесс систем удаленного доступа

IP-адрес каждого подключенного устройства будет храниться на сервере для обеспечения возможности выбора конкретного клиента или рабочей станции сервером для выполнения любых необходимых действий на нужном устройстве [17].

1.2 Анализ существующих разработок и обоснование выбора технологии проектирования

В данном пункте будут рассмотрены решения, аналогичные предлагаемому приложению для мониторинга сети. Для каждого упомянутого программного обеспечения будут рассмотрены плюсы и, возможно, минусы.

Одним из самых известных инструментов для мониторинга и анализа сети является Wireshark. Wireshark предоставляет множество функций, таких как мониторинг и анализ пакетов, анализ передачи голоса по интернет-

протоколу (VoIP), мониторинг трафика и так далее. Это приложение захватывает пакеты в сети и позволяет анализировать и сохранять захваченные пакеты. Этот инструмент имеет много преимуществ, а также некоторые недостатки. В некоторых случаях его бесплатность, открытый исходный код и возможность работы во всех операционных системах можно считать одними из его сильных сторон. Помимо того, что он является замечательным анализатором пакетов, его интерфейс сложен в использовании [20]. Кроме того, Wireshark требует полного понимания протокола управления передачей/протокола Интернета (TCP/IP). Упомянутые сложные проблемы можно рассматривать как некоторые недостатки этого инструмента.

Еще один известный инструмент для мониторинга сети - Spiceworks. Этот инструмент позволяет пользователям отслеживать события, происходящие в сети. Еще одна функция этого инструмента - анализ пропускной способности и производительности сети. Это программное обеспечение, как встроенный сервер, позволяет администратору управлять конфигурациями сети. Кроме того, Spiceworks позволяет администратору просматривать информацию о каждом подключенном устройстве, а также иметь доступ к своим учетным записям и своим данным. Кроме того, администратор сможет помогать рабочим станциям по любым запросам сетевого администрирования. Хотя Spiceworks — мощная и простая в использовании система мониторинга сети, ее нельзя запускать в операционных системах на базе Linux. Еще одним слабым местом этого программного обеспечения является то, что Spiceworks не дает своим пользователям возможности контролировать сеть, и пользователь может только видеть, что происходит в контролируемой сети.

Еще одна мощная и известная система мониторинга сети для предприятий — OpManager. Вся сеть была показана в виде карты (также включенной в карты Google) со списком подключенных устройств. Таким образом, пользователь сможет увидеть каждую рабочую станцию на карте.

Методы визуализации являются одними из лучших функций OpManager. Используя методы визуализации, администратор сможет управлять сетью. Это программное обеспечение также предоставляет возможность создания индивидуальной карты сети для своих пользователей. Таким образом, пользователи смогут настраивать карту сети в зависимости от своего бизнеса и местоположения рабочих станций. Помимо основных функций, предоставляемых этим программным обеспечением, оно также помогает в распознавании и настройке устройств, что аналогично Spiceworks. OpManager также предоставляет инструмент управления MySQL, который может быть полезен сетевому администратору для проверки всех сохраненных данных. OpManager, как и другие предлагаемые на рынке приложения, помимо сильных сторон имеет некоторые недостатки. Это приложение необходимо настраивать вручную, что отнимает много времени, а его пользовательский интерфейс не прост в использовании. Упомянутый момент - это некоторые факты о программном обеспечении OpManager, которые можно рассматривать как некоторые из его недостатков.

Tcpdump — еще один известный инструмент для мониторинга сети. Обычно пакеты, не адресованные в сеть, игнорируются в сетевом интерфейсе. Это программное обеспечение захватывает все пакеты в сети, независимо от адресации, переводя интерфейс в неразборчивый режим. Таким образом, используя этот инструмент для мониторинга сети, администратор сможет проверять пакеты, а также на основе типа информации, хранящейся в заголовке пакетов, администратор сможет анализировать сетевой трафик. Tcpdump — это мощный инструмент, который можно запускать на платформах на базе UNIX, и его структура представляет собой командную строку. На практике это программное обеспечение похоже на Wireshark, и обе они являются программами захвата пакетов, которые захватывают пакеты любых протоколов и отображают захваченные пакеты администратору.

Сравнение четырех существующих на рынке инструментов и предлагаемой системы мониторинга сети показано в таблице 1.

Таблица 1 - Сравнение предлагаемой системы с другими системами

Функции	Wireshark	TCPdump	OpManager	SolarWinds	Предлагаемая система мониторинга
Чтение пакетов	+	+	+	+	+
Захват пакетов	+	+	+	+	+
Фильтры для отображения данных	+	-	-	-	-
Обнаружение вызовов VoIP	+	-	+	-	-
Графический интерфейс	+	-	+	+	+
На основе командной строки	-	+	-	-	-
Мониторинг оборудования	-	+	+	+	+
Среднее время отклика	+	+	+	-	+
Сетевая трассировка	+	+	+	+	+
Система чата	-	-	-	-	+
Клиент-серверная архитектура	-	-	+	+	+
Потеря пакетов	+	+	+	-	-
Сохранение журнала	+	+	+	+	+
Статистический отчет	+	-	-	+	+

Сравнение, представленное в таблице 1, основано на функциональных возможностях каждого инструмента. Функциональные возможности предлагаемой системы в этой ВКР будут аналогичны существующим системам сетевого мониторинга.

Дополнительным функционалом предлагаемой системы, по сравнению с аналогичными системами, является система чата. Система чата является дополнительной функцией, которая была предоставлена для простоты.

Кроме того, система мониторинга сети будет иметь простой в использовании пользовательский интерфейс.

Выводы по главе 1

Анализ существующих систем мониторинга производительности сетевых систем показал, что подобные системы позволяют пользователю просматривать и управлять качеством производительности, анализом данных и ошибками сети Интернет-протокола (IP).

Было выявлено, что инструмент мониторинга производительности является важным активом для системного администратора, позволяющим постоянно отслеживать работу сети на основе данных, собираемых через регулярные промежутки времени.

Основываясь на проведенном анализе, можно сделать вывод, что типичная сеть состоит из различных аппаратных устройств, таких как мосты, повторители, коммутаторы, маршрутизаторы и т. д.

Мониторинг сети включает в себя проверку правильности функционирования этих устройств, а также обеспечение доступности связующей среды и нужен, чтобы обеспечивать бесперебойную работу вычислительной системы в организации.

А предлагаемое решение будет аналогично существующим системам, но будет иметь интерактивный интерфейс и возможность быстрого обмена сообщениями через чат.

Глава 2 Проектирование системы мониторинга сети

2.1 Концептуальное проектирование системы локальной вычислительной сети организации

На рисунке 3 представлена модель, описывающая процесс управления локальной вычислительной сетью.

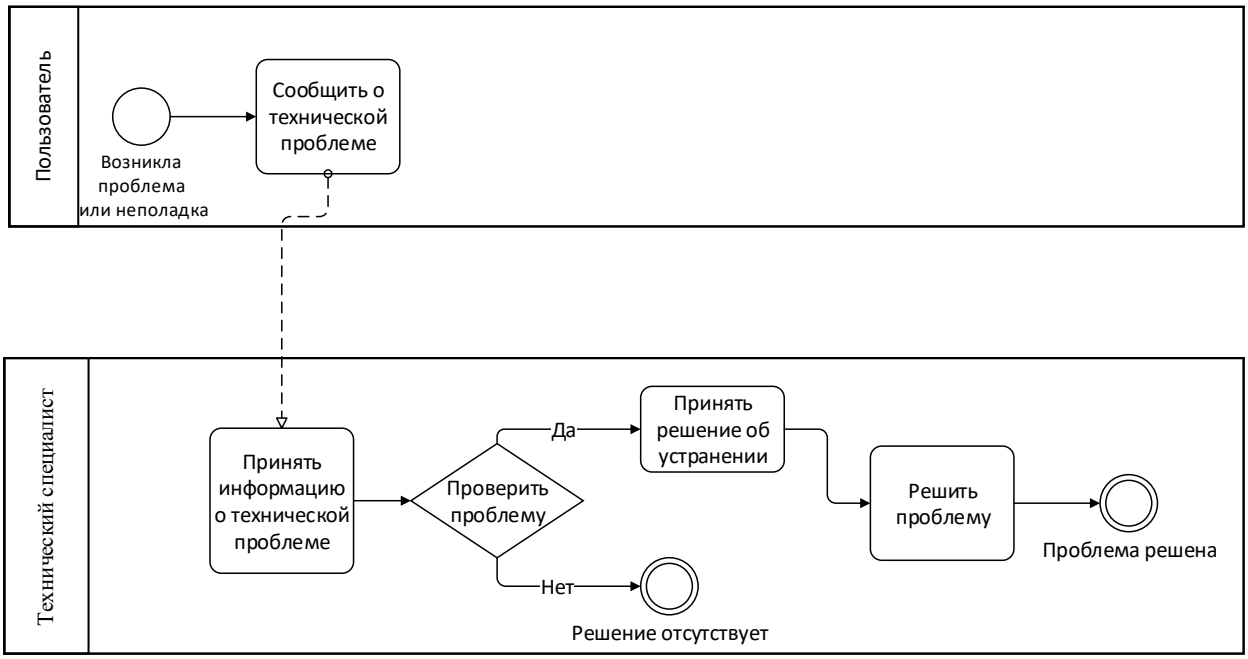


Рисунок 3 – BPMN-диаграмма процесса управления локальной вычислительной сетью (как есть)

Процесс управление локальной вычислительной сетью включает следующие особенности [5]:

– в случае возникновения проблемы у пользователя необходимо вызвать ИТ-специалиста;

– 1-ая оценка проводится физически, ИТ-специалист направляется на место/место/здание, где было сообщено о проблеме;

– технический специалист проверяет проблему и по возможности немедленно предоставляет решение, в противном случае проблема будет решена через определенное время;

– все виды помощи являются физическими, которые требуют времени.

– в случае возникновения проблемы у пользователя необходимо вызвать ИТ-специалиста.

На рисунке 4 представлена блок-схема, демонстрирующая алгоритм управления вычислительной сетью.

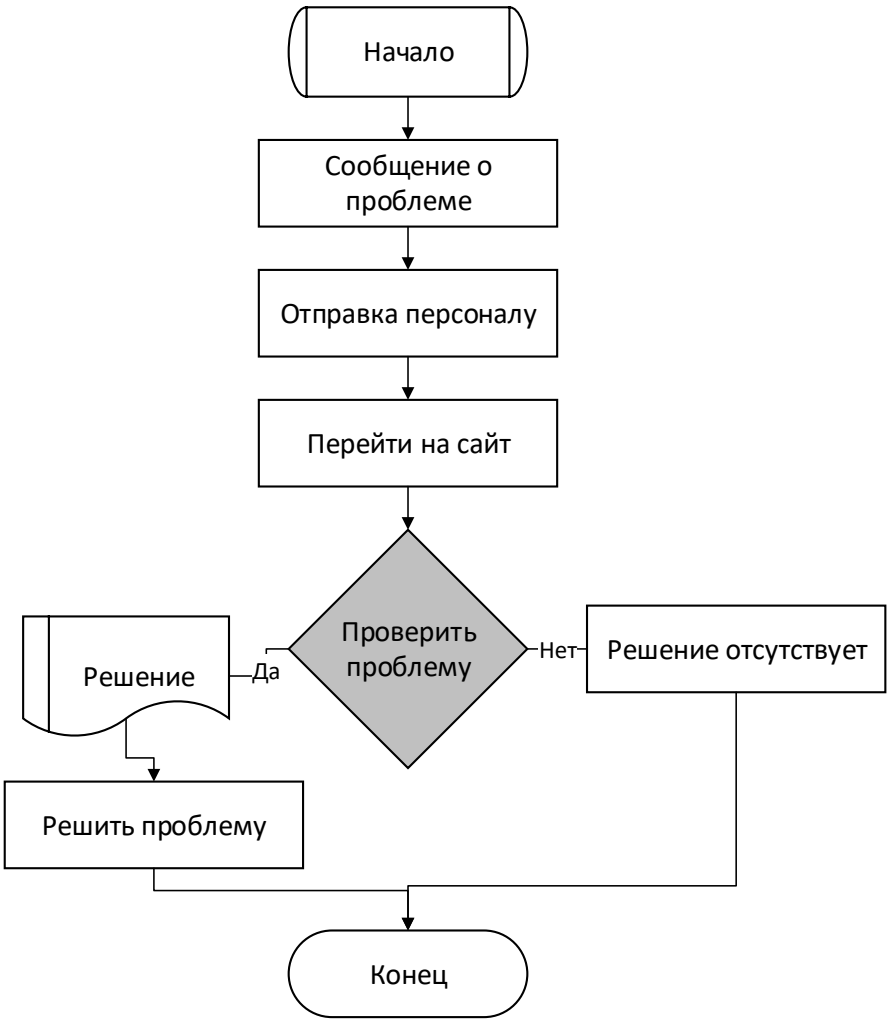


Рисунок 4 - Блок-схема процесса управления вычислительной сетью

Анализируя процесс управления локальной вычислительной сетью, можно выделить следующие проблемы:

– нет ссылки на предыдущую проблему,

– несмотря на ручную систему, перемещение из одного здания в другое для решения проблемы с сетью занимает довольно много времени,

– медленное время отклика приводит к неэффективности и неэффективности потока повседневной деятельности,

– отсутствует постоянная служба поддержки для решения повседневных проблем и запросов пользователей/клиентов.

На рисунке 5 представлена блок-схема работы планируемой системы мониторинга локальной вычислительной сети организации.

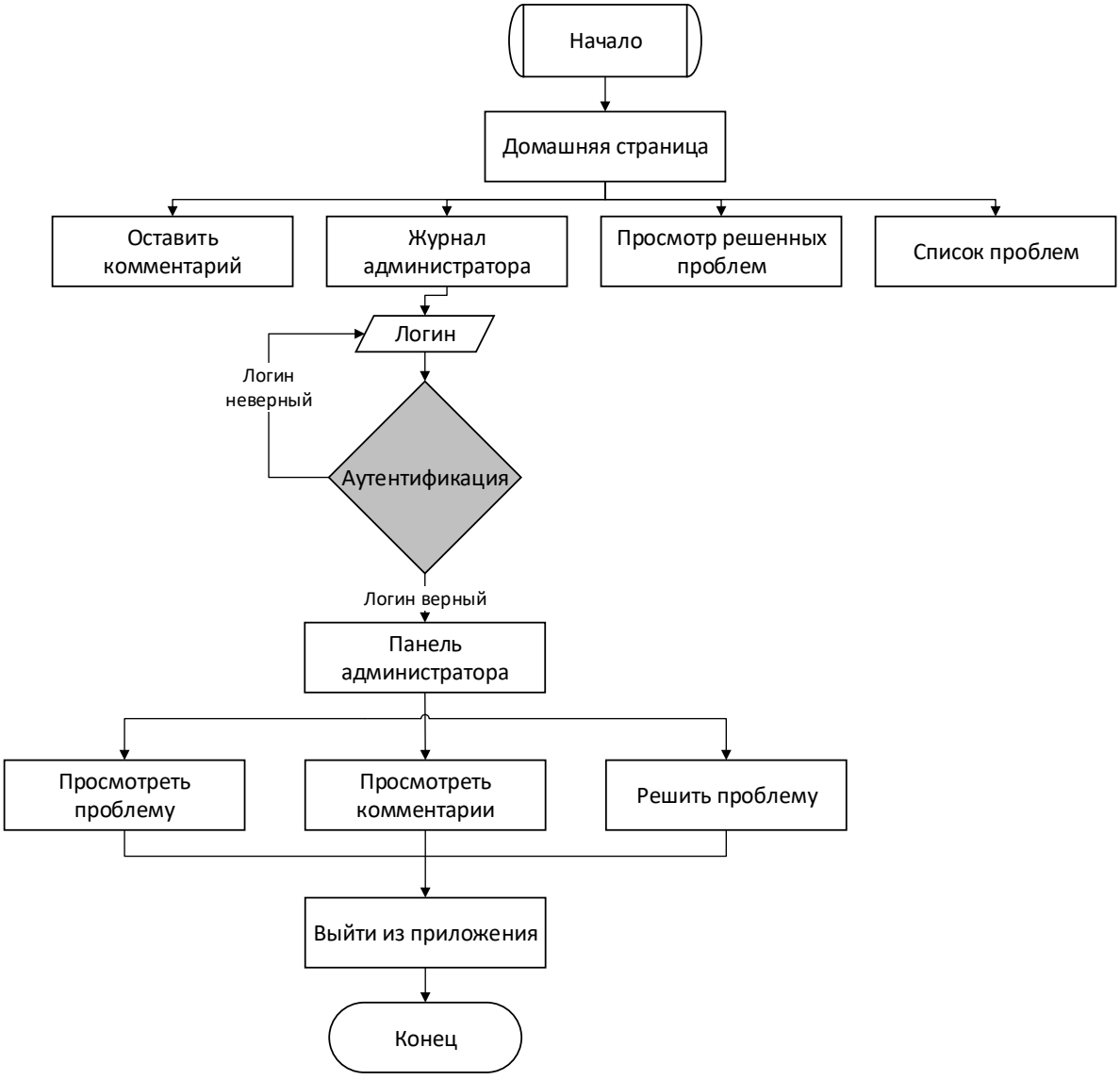


Рисунок 5 - Блок-схема алгоритма работы предлагаемой системы

Таким образом, можно предложить решение, направленной на минимизацию отрицательных откликов текущей системной проблемы:

– система позволит пользователю публиковать свои проблемы и запросы, а пользователь сможет запросить онлайн-помощь,

– система поможет пользователю проверить решение проблемы онлайн без помощи службы поддержки,

– система позволит сэкономить время и ресурсы и формировать еженедельный отчет по запросам пользователей,

– система позволит сетевому администратору и техническому специалисту отслеживать проблему в зависимости от местоположения запроса.

На рисунке 6 представлена модель, описывающая автоматизированное решение для процесса управления локальной вычислительной сетью.

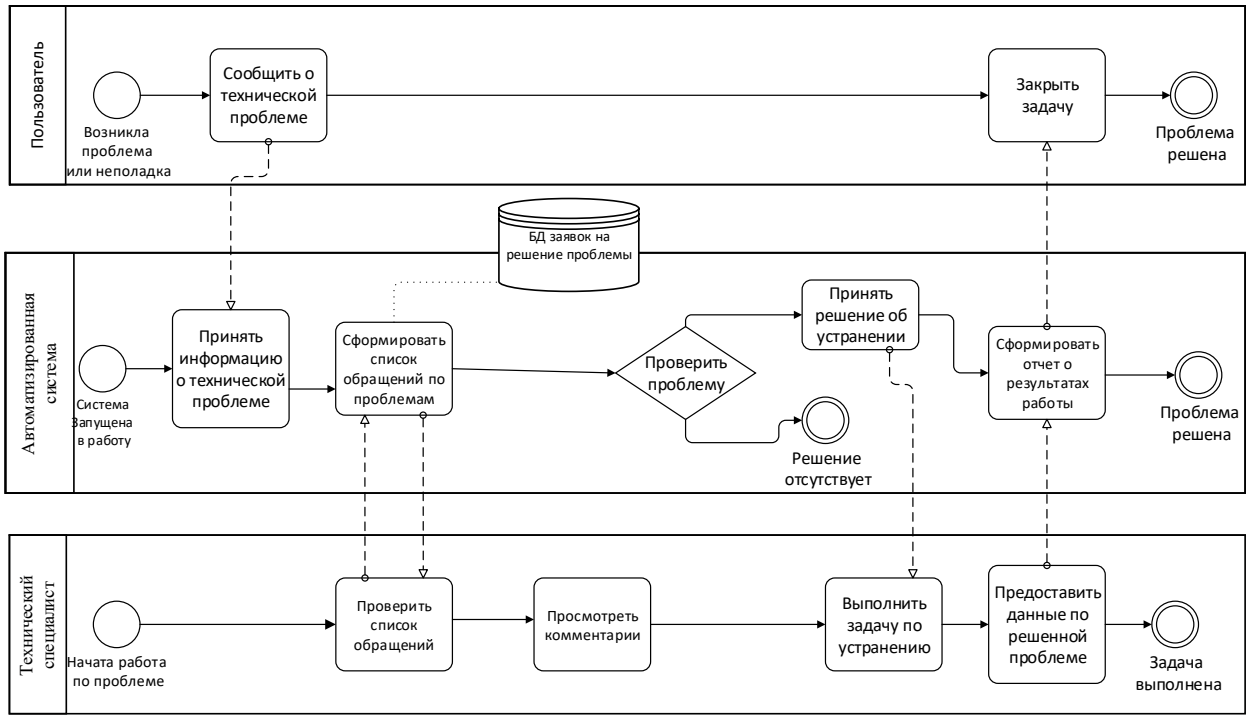


Рисунок 6 – BPMN-диаграмма процесса управления локальной вычислительной сетью (как будет)

Отслеживание запросов в первую очередь автоматизирует процесс управления проблемами и запросами клиента/пользователя. Администрация сможет хранить запросы клиентов/пользователей онлайн и отслеживать их из любого места [1]. И, благодаря использованию базы данных, каждая проблема/запрос будет однозначно идентифицирована, поэтому не будет проблем с использованием одних и тех же идентификаторов, а процесс получения файлов инцидентов будет быстрее.

На рисунке 7 представлена диаграмма деятельности предлагаемой системы.

Данное приложение основано на архитектуре клиент-сервер. Базовая система построена на основе наличия этого приложения как на клиентских, так и на серверных устройствах. Поскольку сервер подключен к сети, клиентам разрешено подключаться к серверу, используя соответствующий номер порта и IP-адрес сервера

В разделе дистанционного управления после запуска соединения между клиентом и сервером предоставляются некоторые параметры для использования администратором сервера

Результаты в этом примере представлены в виде информации о минимальном, максимальном и среднем времени этого процесса, а также информации о потере пакетов, отправленных и полученных пакетах.

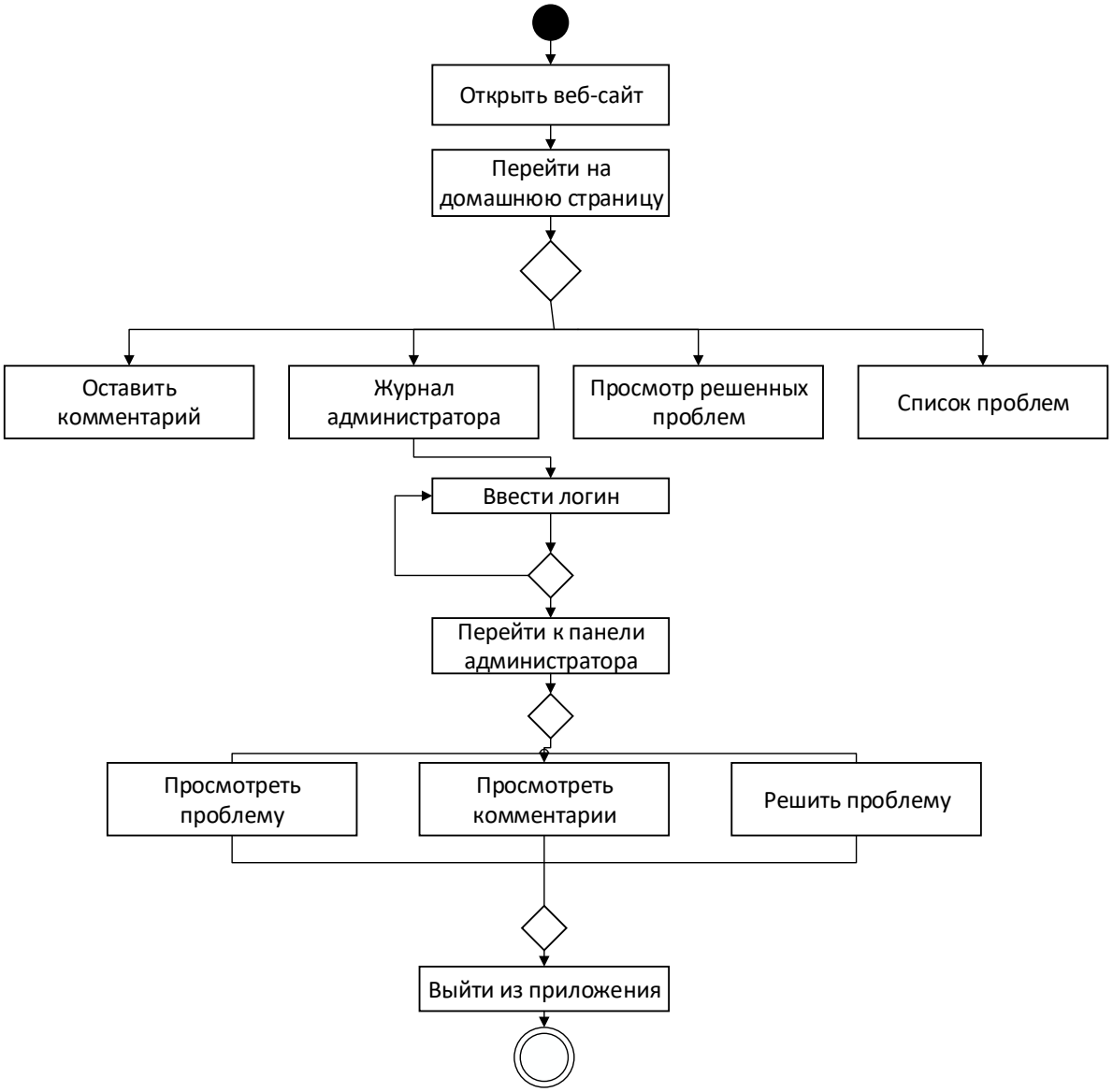


Рисунок 7 - Диаграмма деятельности предлагаемой системы

Поскольку система подключена к сети, администратор имеет доступ к истории запросов из любого места при наличии подключения к Интернету и наличии соответствующих учетных данных для входа [4].

Представим иерархическую модель проектирования для разбиения проекта на модульные группы. Выделим следующие три уровня:

– Уровень доступа: обеспечивает доступ рабочей группы/пользователя к сети,

– Уровень распределения: объединяет уровни доступа и обеспечивает подключение к службам,

– Базовый уровень: обеспечивает соединение между уровнями распределения для больших сред LAN.

Таким образом, разрабатываемая система мониторинга будет представлять собой иерархическую модель взаимосвязанных узлов.

2.2 Логическое моделирование системы мониторинга сети

Для логического моделирования системы мониторинга сети был выбран унифицированный язык моделирования (UML). UML — это стандартная графическая символизация для объяснения дизайна реализованного программного обеспечения или системы.

Как правило, UML включает пять диаграмм и спецификаций, чтобы осуществить некоторое знакомство с предлагаемой системой для каждой функции [10].

Первым шагом в UML построим диаграмму вариантов использования, которая представляет собой графическое представление основных функций предлагаемой системы.

Предоставленный вариант использования в этой работе, показывает доступность двух акторов, которые являются клиентом и сервером.

На следующей диаграмме показаны основные функциональные возможности реализованного приложения (рисунок 8).

Рисунок 8 - Диаграмма вариантов использования

В следующих таблицах 2-8 представлена спецификация вариантов использования, т.е. подробная информация о представленных функциональных возможностях.

Таблица 2 описывает процесс запуска серверного приложения.

Таблица 2 - Определение начального 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

Как можно понять из указанной таблицы, доступ предоставляется только админу сервера. Первым шагом процесса мониторинга сети будет запуск сервера администратором. Также очищается разрешение в упомянутой таблице, которой администратору разрешено запускать сервер. На этом этапе нет предварительного запроса, так как это первый шаг этой заявки. Таким образом, к концу этого шага сервер будет запущен, и клиент сможет к нему подключиться.

Следующий шаг связан с процессом подключения, как показано в таблице 3.

Таблица 3 - Определение подключения к системе

Связь	
Актеры	Доступ назначается Серверу и Клиенту
Описание	Сервер, а также клиент могут подключаться к системе
Нормативные документы	Администратор сервера устанавливает соединение, после чего клиент сможет подключиться к серверу
Предпосылка	Сервер устанавливает номер порта, поэтому клиент, используя номер порта и IP-адрес сервера, может подключиться к серверу
Результат	Соединение между клиентом и сервером будет установлено

Представленная таблица является определением этого процесса. Подключиться может как пользователь сервера, так и пользователь клиента. Таким образом, обе стороны этого приложения, клиентская и серверная, смогут подключаться к системе. Процедура устанавливает соединение сервером, после чего клиент сможет подключиться к серверу. Этот шаг имеет значительный предварительный запрос, который использует номер порта и IP-адрес сервера клиентом. Таким образом, сервер должен установить номер порта, и клиент, используя этот номер порта и IP-адрес сервера, может подключиться к серверу. Конечным результатом этого шага будет установление соединения между клиентом и сервером.

Следует отметить, что в предлагаемой системе номер порта предустановлен, что делает систему более простой в использовании.

Раздел состояния сети можно увидеть в таблице 4.

Таблица 4 - Определение статуса сети

Статус сети	
Актеры	Доступ предоставляется администратору Сервера и пользователю Клиента
Описание	Информация о сетевых устройствах на стороне сервера будет видна администратору сервера, а информация о стороне клиента будет видна клиенту
Нормативные документы	--
Предпосылка	Выбор нужного сетевого адаптера
Результат	Администратор сервера и пользователь клиента смогут проверить состояние сети

Раздел состояния сети связан с информацией о сетевых устройствах. Эта функция предусмотрена как для администратора сервера, так и для пользователя клиентской части. В этом разделе серверная сторона сможет проверить сетевые устройства на стороне сервера, а клиент сможет проверить сетевые устройства на стороне клиента.

Эта функция, как следует из названия, обеспечивает возможность проверки и управления сетевыми устройствами, и в случае возникновения какой-либо проблемы система обнаружит ее и предоставит решение для устранения неполадок. Клиент, получив информацию о любой неисправности или отключении в сети, которая будет предоставлена в этом разделе, может либо использовать решение для устранения неполадок, чтобы исправить это, либо передать информацию о проблеме администратору сервера для получения дополнительной помощи.

Процесс передачи информации может осуществляться через систему чата.

Участок трассировки сети описан в таблице 5.

Таблица 5 - Определение трассировки сети

Трассировка сети	
Актеры	Доступ предоставляется админу Сервера
Описание	Отслеживание IP-адресов желаемого пункта назначения
Нормативные документы	Вставка предпочтительного IP-адреса для отслеживания
Предпосылка	Выбранный IP-адрес должен существовать
Результат	Администратор сервера сможет отследить желаемый IP-адрес

Доступ к этому разделу закреплен за серверной частью данного приложения. Вставив имя хоста или IP-адрес желаемого места назначения, администратор сервера сможет проверить соединение между сервером и местом назначения. Это было бы возможно путем проверки подключения к таким устройствам, как маршрутизаторы и коммутаторы, которые находятся на пути между сервером и пунктом назначения.

Описание раздела удаленного доступа представлено в таблице 6.

Таблица 6 - Определение удаленного доступа

Удаленный доступ	
Актеры	Доступ предоставляется администратору Сервера
Описание	Администратор сервера сможет иметь удаленный доступ к клиентам, подключенным к серверу
Нормативные документы	Администратор сервера выберет нужного клиента из выпадающего списка, а затем выберет предпочтительное действие
Предпосылка	--
Результат	Удаленный доступ будет назначен серверу для подключенного клиента

Раздел удаленного доступа предназначен для серверной части, поэтому доступ предоставляется администратору сервера. После установления соединения между сервером и клиентом администратор сервера сможет иметь удаленный доступ к клиентам, подключенным к серверу. Эта функция позволяет администратору в случае необходимости выполнять некоторые необходимые действия на клиентском устройстве. Действия удаленного доступа: выключение, перезагрузка, прерывание и выход из клиентского

устройства. Процедура заключается в том, что администратор сервера выбирает нужного клиента из выпадающего списка, а затем выбирает предпочтительное действие.

Функция чата была назначена как на стороне клиента, так и на стороне сервера этого приложения. Они оба смогут начать общение. Для отправки сообщения клиенту только сервер должен выбрать получателя. Таким образом, результатом будет возможность общения в чате на стороне клиента и сервера в случае соединения друг с другом.

Этот процесс описан в таблице 7.

Таблица 7 – Определение функции чата

Чат	
Актеры	Доступ предоставляется админу Сервера и Клиента
Описание	И сервер, и клиент смогут начать чат
Нормативные документы	--
Предпосылка	Для отправки сообщения клиенту только сервер должен выбрать получателя
Результат	Обеспечена возможность общения между сервером и клиентом

В таблице 8 показано описание процесса отключения.

Таблица 8 - Определение отключения

Отключение	
Актеры	Доступ предоставляется администратору Клиента и Сервера
Описание	И клиент, и сервер смогут отключать свои системы
Нормативные документы	--
Предпосылка	--
Результат	Соединение будет разорвано

Возможность отключения системы возложена как на клиентскую, так и на серверную сторону. Таким образом, и клиент, и сервер смогут отключить свои системы.

Диаграмма классов — это еще один шаг проектирования в нотации UML. Диаграммы классов, как правило, используются для объектно-ориентированного проектирования и предлагают, как будет спроектирована система [21].

На рисунке 9 показана диаграмма классов разрабатываемой системы мониторинга сети.

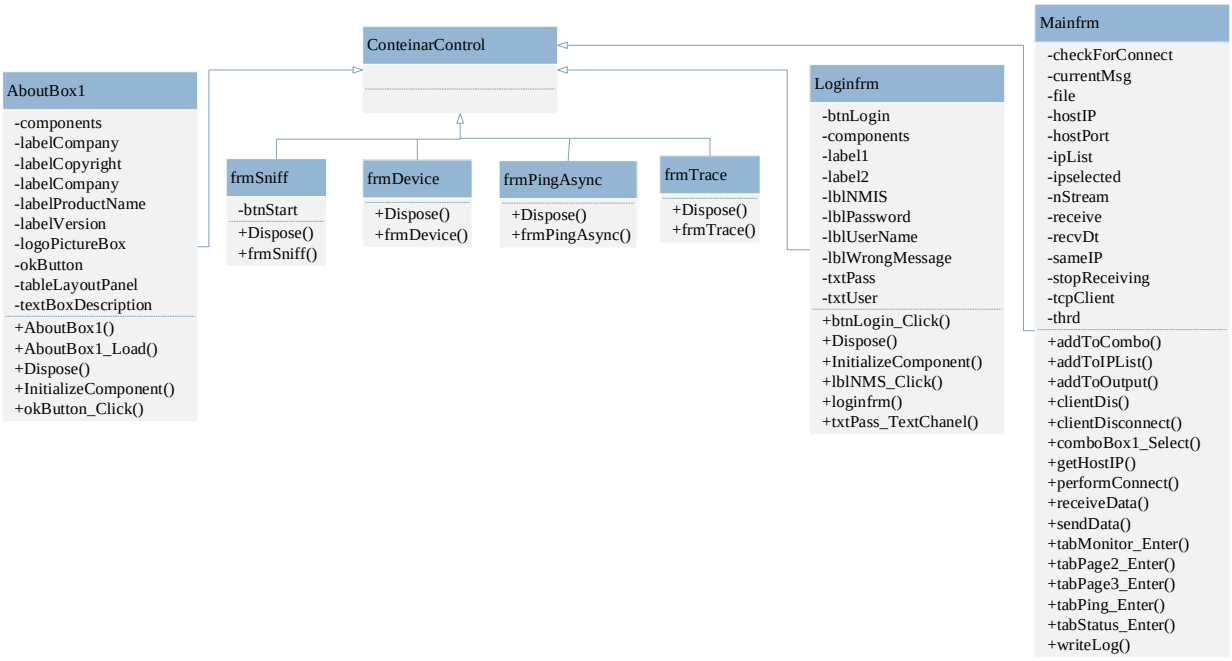


Рисунок 9 - Диаграмма классов

Диаграмма классов UML включает имена классов, отношения между классами, свойства и атрибуты, используемые при реализации предлагаемой системы.

2.3 Физическое моделирование вычислительной сети организации

Диаграмма последовательности — это еще одна диаграмма в нотации UML. Данная диаграмма представляет последовательность действий в этом приложении. На этой диаграмме стрелки представляют методы, а

прямоугольники — классы. Как правило, необходимое количество диаграмм последовательности должно определяться в зависимости от характера применения. Для приложения, реализованного в данной работе, для процесса подключения, в котором участвуют и клиент, и сервер, была создана диаграмма последовательности, представленная на рисунке 10.

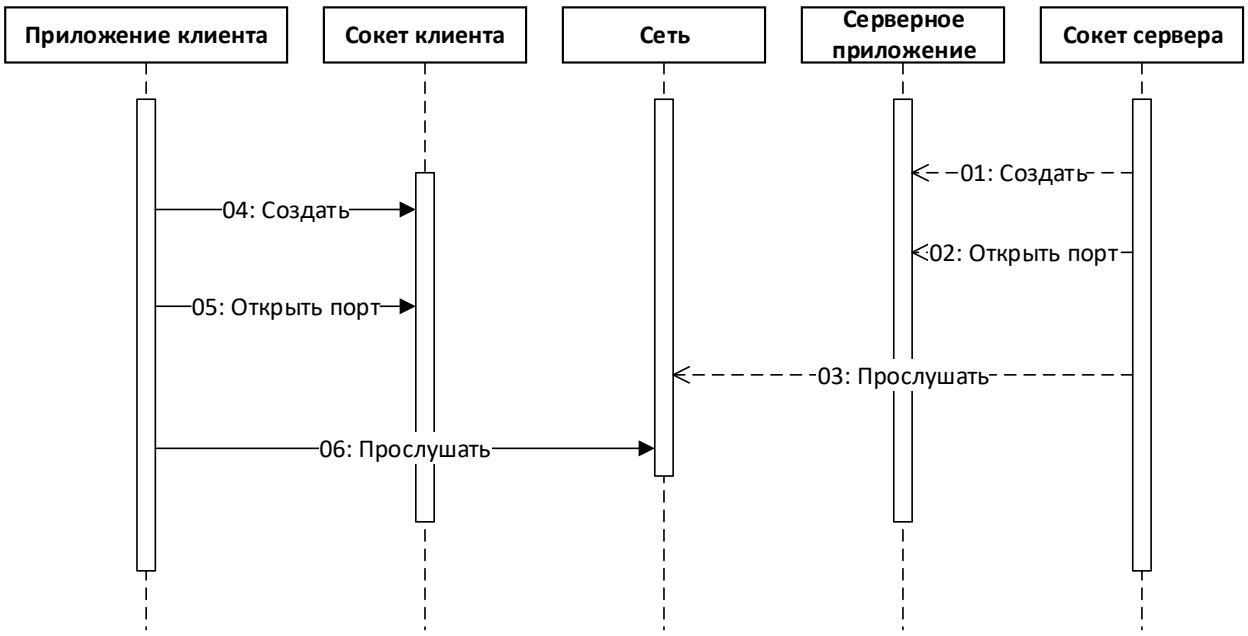


Рисунок 10 - Диаграмма последовательности, показывающая процесс подключения

Проектирование системы — это процесс проектирования того, как предполагаемая система будет выглядеть после того, как она будет введена в эксплуатацию.

Унифицированный язык моделирования (UML) предоставляет очень надежный набор обозначений, который расширяется от анализа к проектированию. UML в основном представляет собой набор графических обозначений, которые методы используют для представления проектов.

На рисунке 11 представлена последовательной действий, выполняемых администратором.

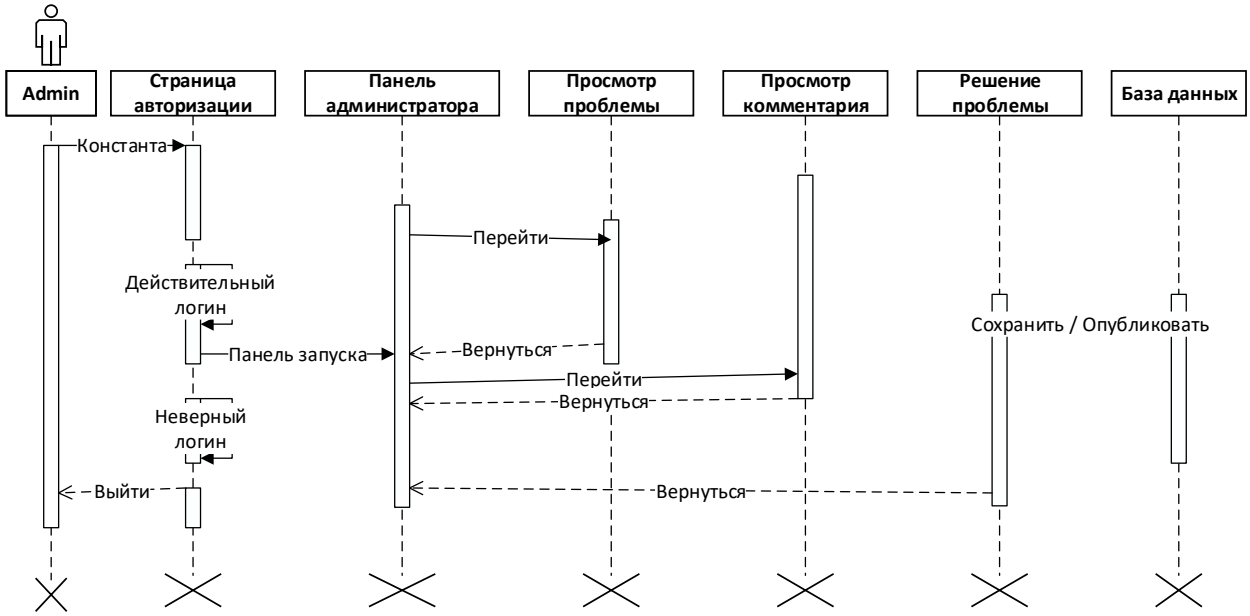


Рисунок 11 - Диаграмма последовательности для задач администратора

На рисунке 12 представлена последовательной действий, выполняемых пользователем.

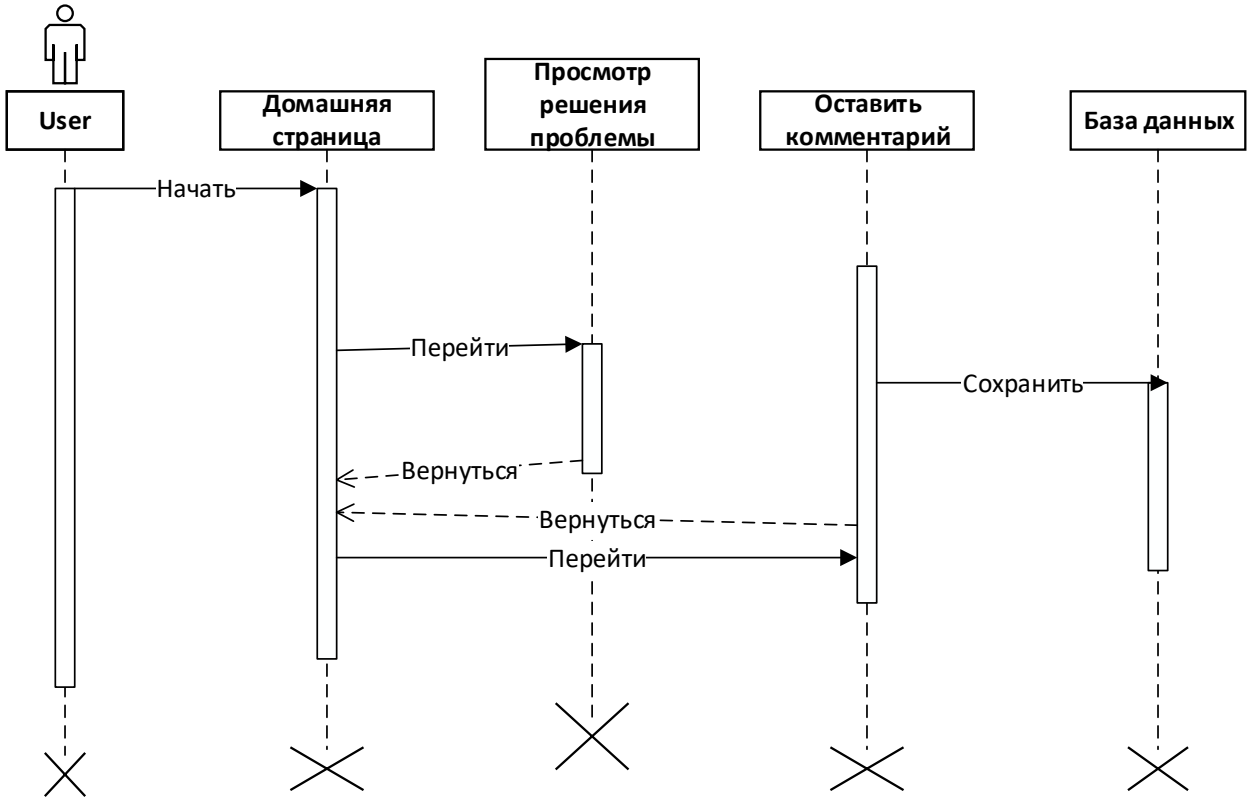


Рисунок 12 - Диаграмма последовательности для пользователя

Диаграмма активности представляет структуру сложных операций путем разделения всего процесса на более мелкие действия для лучшего понимания функциональности реализованного приложения. Как видно на рисунке 13, диаграмма действий для реализованного приложения представляет структуру действий, которые происходят в процессе удаленного доступа.

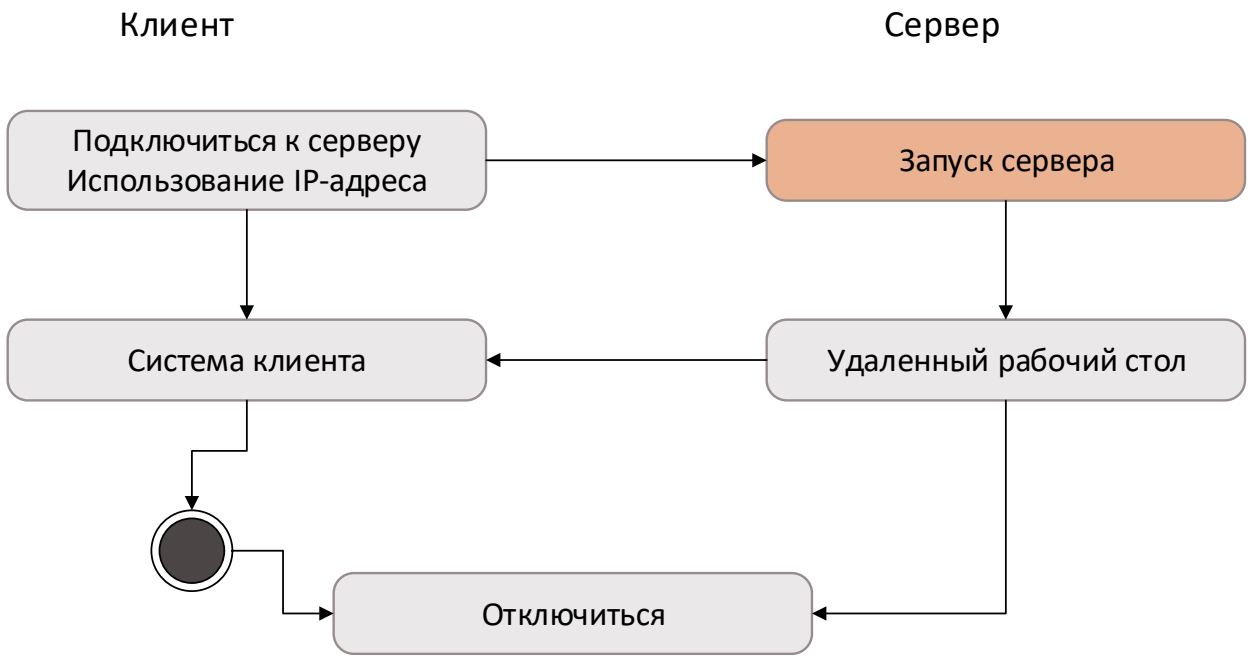


Рисунок 13 - Диаграмма активности, показывающая удаленный доступ

На рисунке 14 показано, как программное обеспечение системы мониторинга проверяет доступность удаленного сервера перед запросом данных для отслеживаемых показателей.

Безагентный мониторинг запускается на сервере, на котором запущено программное обеспечение системы мониторинга. Первое действие — проверить, доступен ли удаленный сервер. Это достигается с помощью команды ping и гарантирует, что выполнение дальнейших шагов возможно

или нет. При сбое контрольной точки доступности процесс мониторинга для этого сервера завершается.

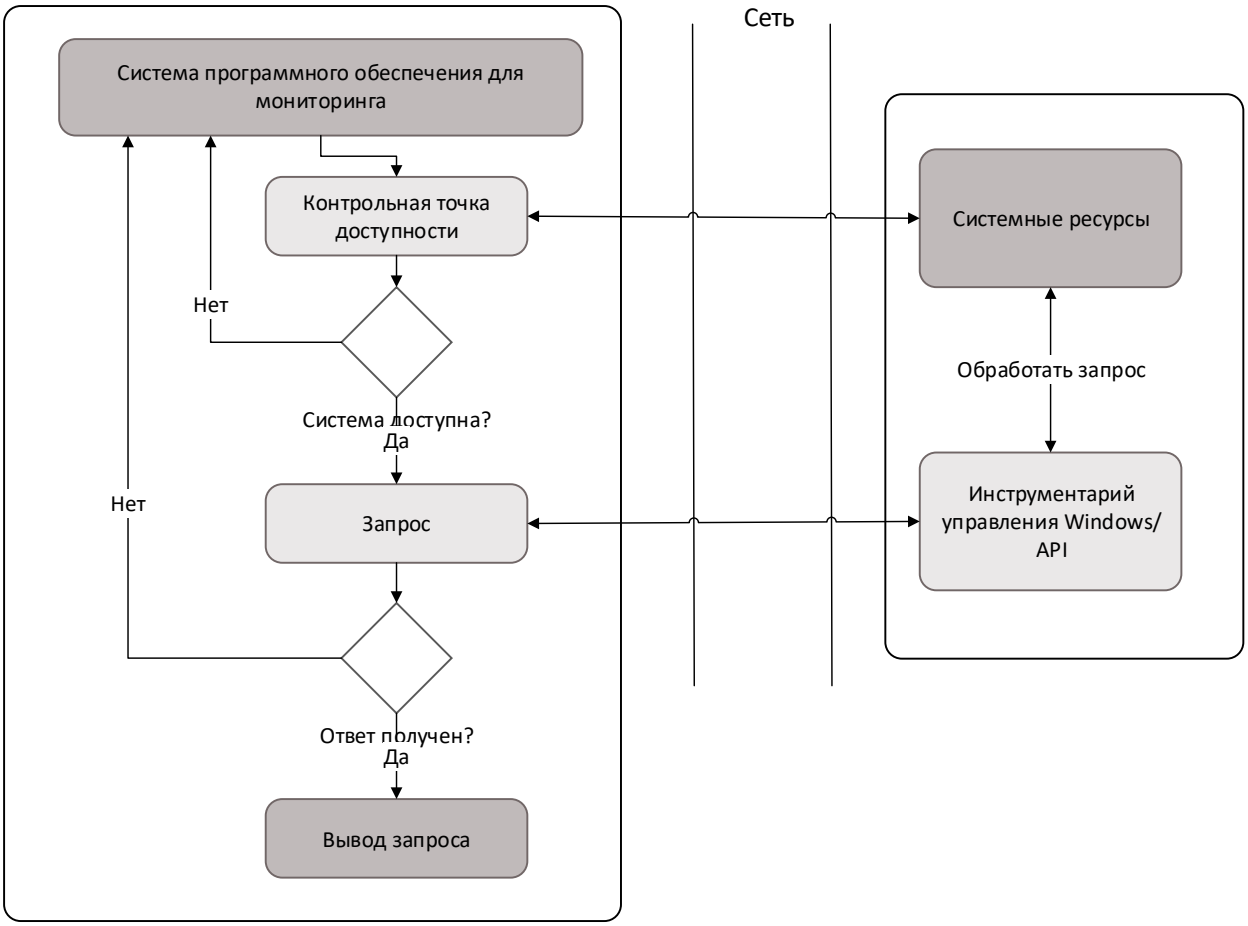


Рисунок 14 - Подробная информация о потоке данных в решении для мониторинга с использованием безагентного подхода

В случае успешной проверки доступности программное обеспечение системы мониторинга опрашивает удаленный сервер на наличие одного события безопасности и трех событий операционной системы. Соединение устанавливается с помощью технологии WindowsManagementInstrumentation (WMI) или программы SysinternalsPsLogList, установленной на сервере мониторинга. Теперь отслеживаемый сервер получает специальные инструкции для отчета о текущих значениях запрошенных показателей. Запрос обрабатывается, и данные возвращаются на сервер мониторинга.

Результаты могут быть импортированы непосредственно в программное обеспечение системы мониторинга или сохранены в локальном файле.

Структура клиент-серверной архитектуры [21], которая используется для реализации этого приложения, показана на рисунке 15.

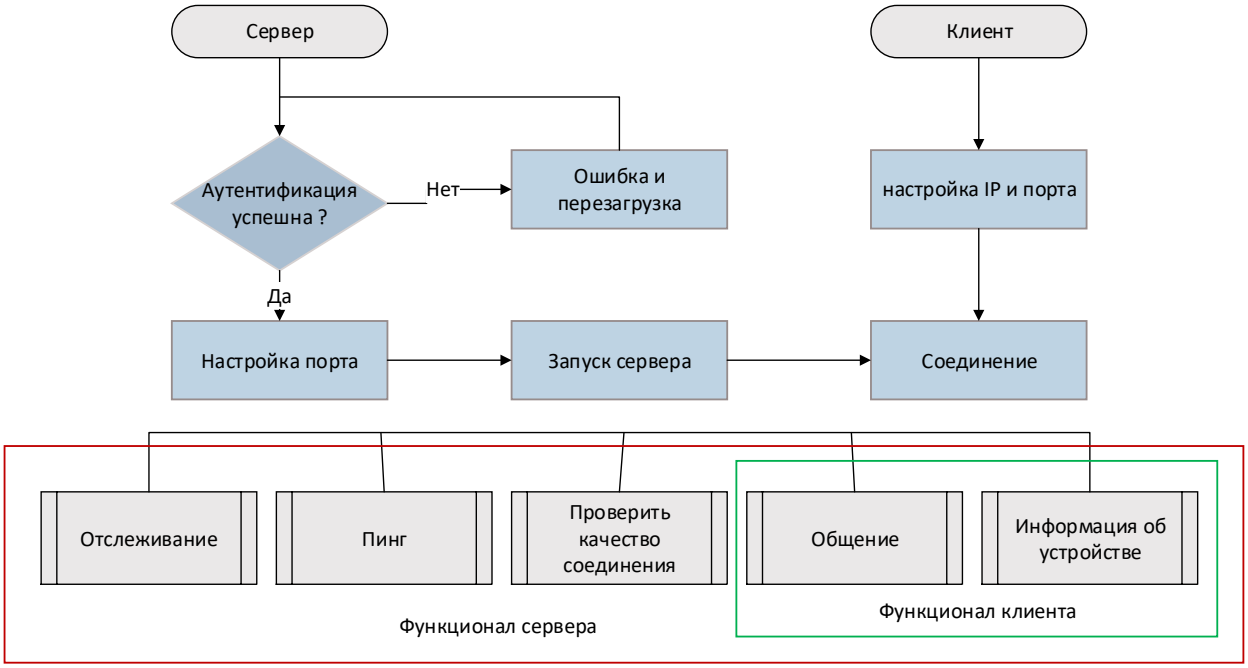


Рисунок 15 - Архитектура клиент-сервер

В третьей главе будет представлена подробная информация о каждой части приложения. Кроме того, структура этого приложения состоит из двух частей: серверной и клиентской. Таким образом, спецификация каждой части будет рассмотрена отдельно.

Выводы по главе 2

Были описаны концептуальная и логические модели проектируемой системы мониторинга вычислительной сети, которые позволили определить дальнейший процесс ее реализации.

Глава 3 Реализация и расчет экономической эффективности системы мониторинга локально-вычислительной сети

3.1 Реализация системы мониторинга вычислительной сети организации

В данной главе представлена реализация предлагаемой системы мониторинга сети. Эта система была реализована с использованием языка программирования C# в среде VisualStudio [3][6]. Платформа Microsoft .Net — это хорошая среда для сетевых программистов. Причина выбора C# заключается в том, что этот язык программирования позволяет программистам разрабатывать сетевые приложения с использованием сетевых функций Windows. Таким образом, что касается использования .Netframework и языка программирования C#, реализованное приложение сможет работать в операционной системе Windows [7][11][19].

Данное приложение основано на архитектуре клиент-сервер. Базовая система построена на основе наличия этого приложения как на клиентских, так и на серверных устройствах. Поскольку сервер подключен к сети, клиентам разрешено подключаться к серверу, используя соответствующий номер порта и IP-адрес сервера [13].

Рассмотрим серверную часть системы. На стороне сервера можно наблюдать все функциональные возможности реализованной системы. На первом этапе была разработана страница входа. Администратор сможет войти на серверную часть системы, используя заранее заданное имя пользователя и пароль. Имя пользователя и пароль установлены в приложении и хранятся в базе данных.

Секция дистанционного управления [15]. Этот раздел является первым разделом, предназначенным для администратора сервера.

В разделе дистанционного управления, как видно на рисунке 16, выделены 4 основные части: настройка номера порта, удаленное управление, журнал показа и, наконец, среда чата.

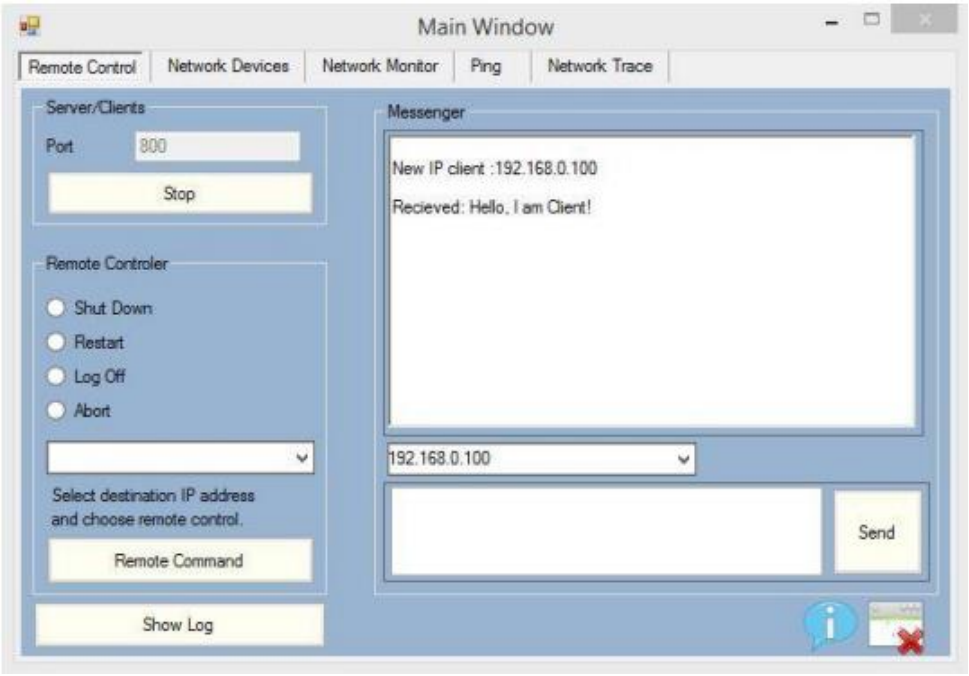


Рисунок 16 - Дистанционное управление

Первой задачей для сервера должно быть установление соединения, позволяющее клиентам подключаться к серверу. Хотя для простоты использования был установлен предварительно установленный номер порта, но в случае необходимости администратор сможет изменить номер порта.

В разделе дистанционного управления после запуска соединения между клиентом и сервером предоставляются некоторые параметры для использования администратором сервера [24].

На следующем шаге пользователь сервера должен выбрать желаемый IP-адрес клиента из выпадающего списка в этом окне. Выбрав предпочтительный клиент, который является устройством, подключенным к серверу, сервер сможет отправить именно этому клиенту сообщение, а также сервер получит доступ к рабочему столу клиента для выполнения

необходимых действий. Нажав кнопку показать журнал в этом окне, администратор увидит сохраненные журналы в предопределенной форме журнала.

Как видно на рисунке 16, при подключении каждого клиента к серверу в чат-части этой системы появится сообщение, информирующее пользователя сервера об IP-адресе нового клиента. Кроме того, пользователь Сервера, выбрав желаемый IP-адрес клиента, сможет выполнять некоторые предопределенные операции. Например, в части удаленного контроллера, после выбора предпочтительного IP-адреса, сервер может выключить устройство клиента, нажав кнопку удаленной команды.

Рассмотрим раздел сетевых устройств [16]. Следующий пример кода, показанный на рисунке 17, описывает одну из важных частей этого раздела.

```
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 – Фрагмент кода мониторинга сети

Сначала предопределенное целое число, которое называется m_Index, должно быть пустым, и для достижения этой цели значение устанавливается равным -1, чтобы быть инициализированным с 0. Для представления

информации о сетевых устройствах хост должен быть активным. Для проверки доступности хоста в сети использовался указанный метод StartMonitor. Если желаемый хост активный, то пользовательский интерфейс должен быть вызван с помощью MethodInvoker, а затем будет направлен в заранее заданное место в системном интерфейсе [9].

Раздел сетевого управления, как видно на рисунке 18, разделен на две части. Первая часть связана с информацией о сетевых устройствах, которую можно выбрать из предустановленного выпадающего меню. Вторая часть — это системная сводка, в которой будет отображаться информация о выбранном сетевом устройстве [8].

Таким образом, при выборе каждого сетевого устройства, представленного в раскрывающемся меню, соответствующая информация будет автоматически отображаться в указанном месте.

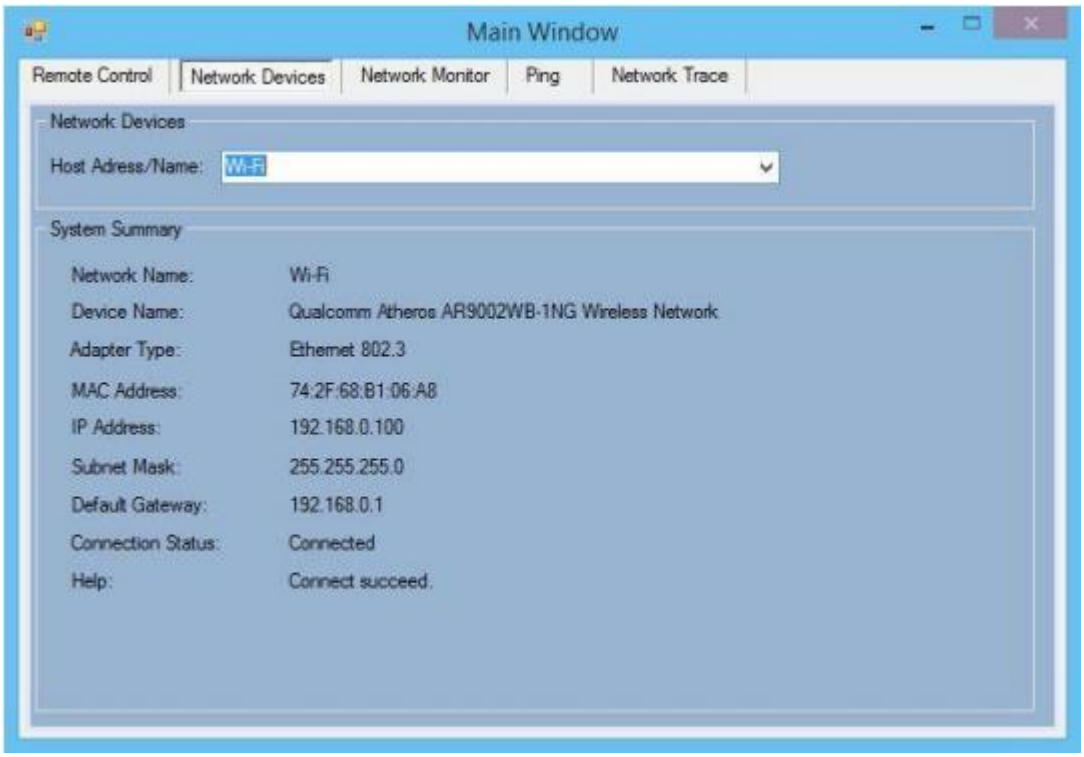


Рисунок 18 - Сетевое устройство

На рисунке 18 выбрано соединение Wi-Fi, и предоставлена вся необходимая информация [24]. Например, информация о марке процессора беспроводной карты, которая используется в серверном устройстве. Рассматриваемый пример показан в строке имени устройства. Также, в качестве другого примера, показано состояние соединения. В этом примере соединение успешно установлено и, соответственно, в помощи не будет необходимости. В случае возникновения проблем с установлением соединения в разделе справки будет предоставлена информация для устранения проблемы.

В разделе сетевого монитора пользователь сервера сможет выбрать желаемый IP-адрес из выпадающего меню [22]. При нажатии кнопки «Старт» вся информация о пакетах, отправленных или полученных с выбранного IP-адреса, будет отображаться в указанном ниже месте. Также собранную информацию можно очистить с помощью кнопки рядом с кнопкой «Старт» (рисунок 19).

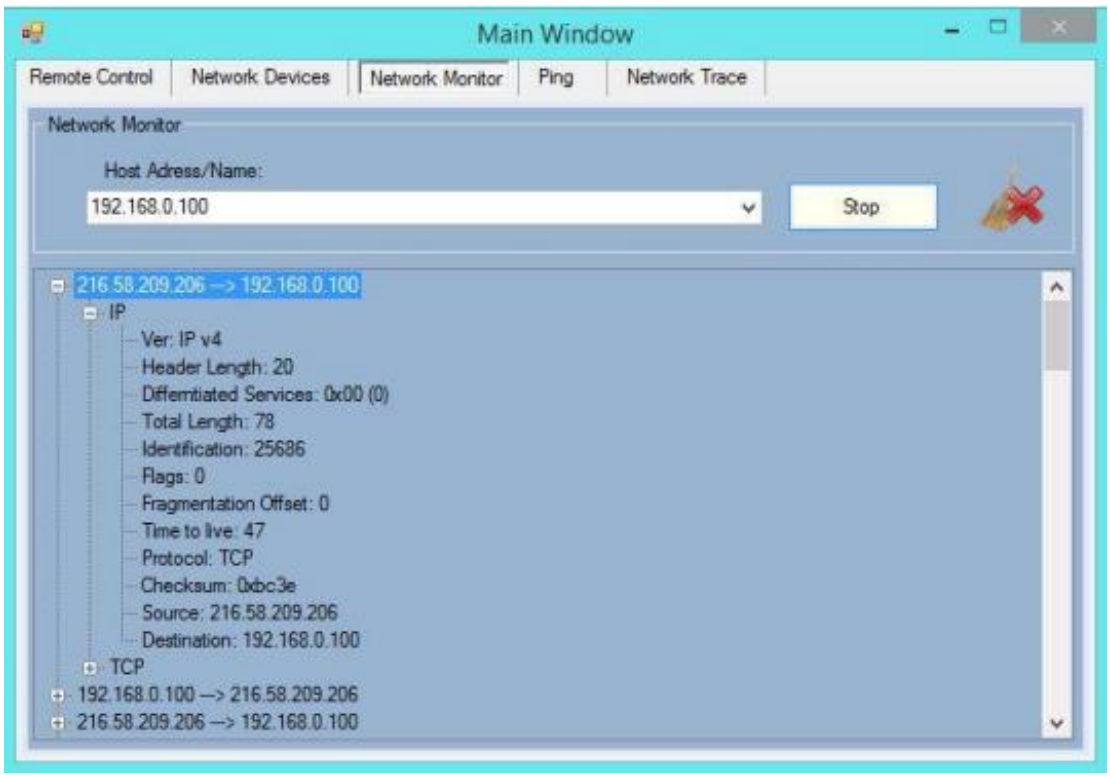


Рисунок 19 - Сетевой монитор показывает IP

В предоставленном примере на рисунке 19 один из пакетов открывается, чтобы показать подробности в одном из его разделов. В этом примере подробная информация находится в разделе IP, в котором представлена версия IP, длина заголовка пакета, протокол, IP-адреса источника и получателя и некоторая другая информация. Предоставленная информация, как было описано выше, помогает пользователю сервера быть в курсе действий, которые были выполнены через сеть выбранным клиентом.

Протокол пользовательских дейтаграмм (UDP) — это протокол связи, предлагающий ограниченный объем услуг при обмене сообщениями между компьютерами в сети, использующей Интернет-протокол (IP).

На рисунке 20 показан пример представления раздела UDP, в котором дана подробная информация [14][18].

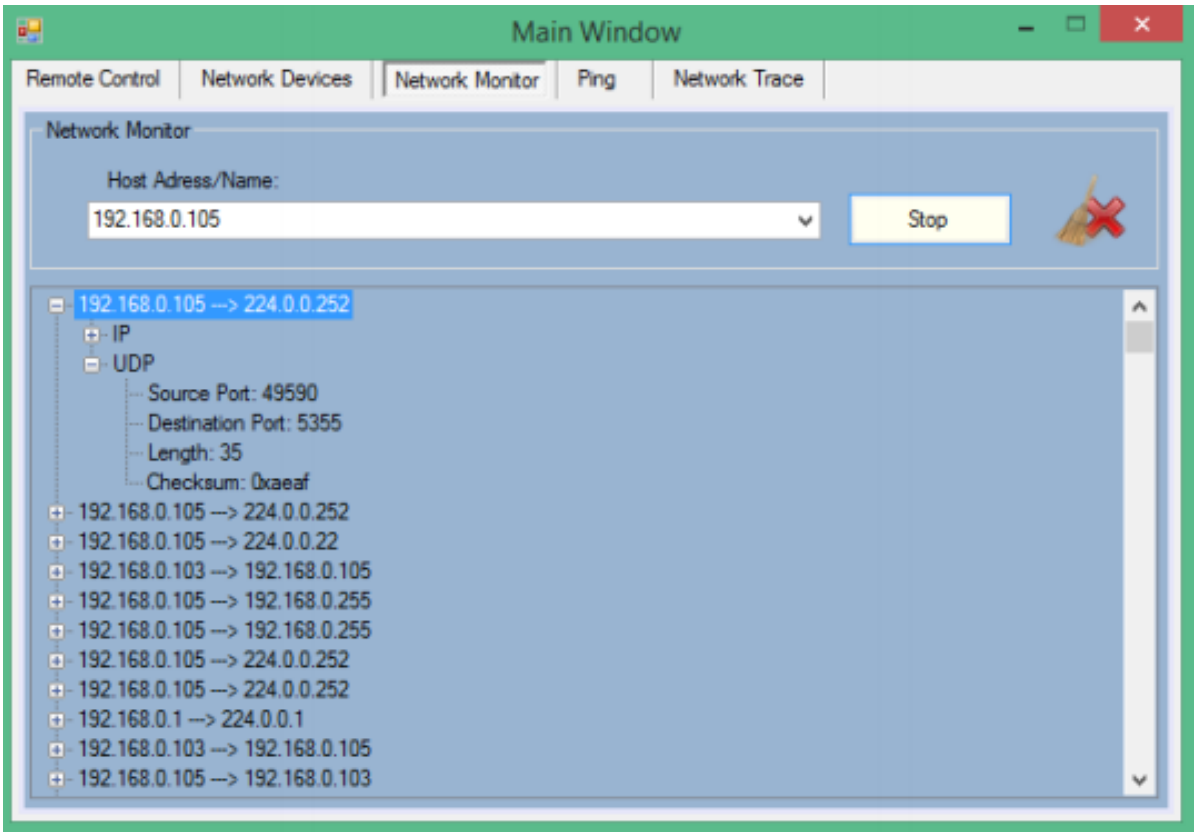


Рисунок 20 - Сетевой монитор показывает UDP

Как видно на рисунке 20, информация, представленная в разделе сетевого мониторинга, включает используемый порт в источнике и получателе, длину сообщения и контрольную сумму.

На рисунке 21 показан пример представления раздела TCP. В этом примере дана подробная информация о заголовке каждого пакета, передаваемого по сети, в разделе TCP.

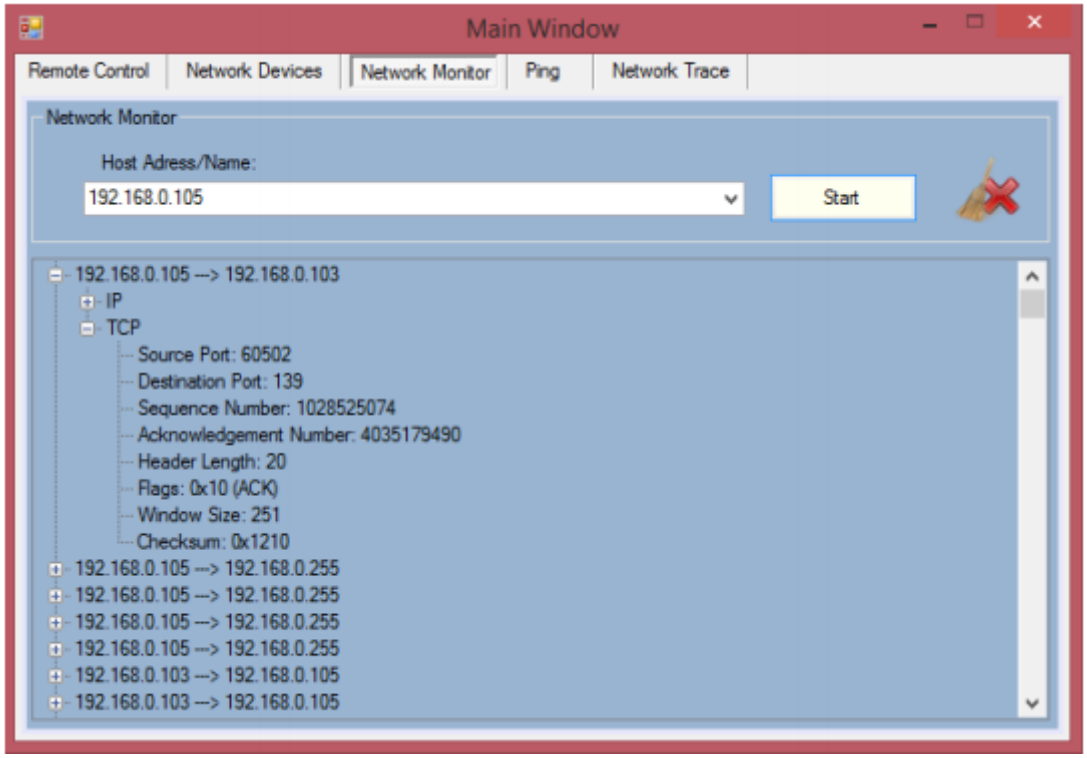


Рисунок 21 - Мониторинг сети (демонстрация TCP)

Как видно из рисунка 21, информация, представленная в этом разделе, включает номер порта источника и получателя, порядковый номер пакета, номер подтверждения, длину заголовка, флаги и так далее.

На рисунке 22 показан пример представления раздела системы доменных имен (DNS). В этом примере показана подробная информация о заголовках пакетов в разделе DNS.

Как видно на рисунке 22, информация, представленная в этом разделе, представляет собой идентификационный номер, флаги, количество вопросов,

количество записей ресурсов ответов (RR), количество авторитетных RR и количество дополнительных RR.

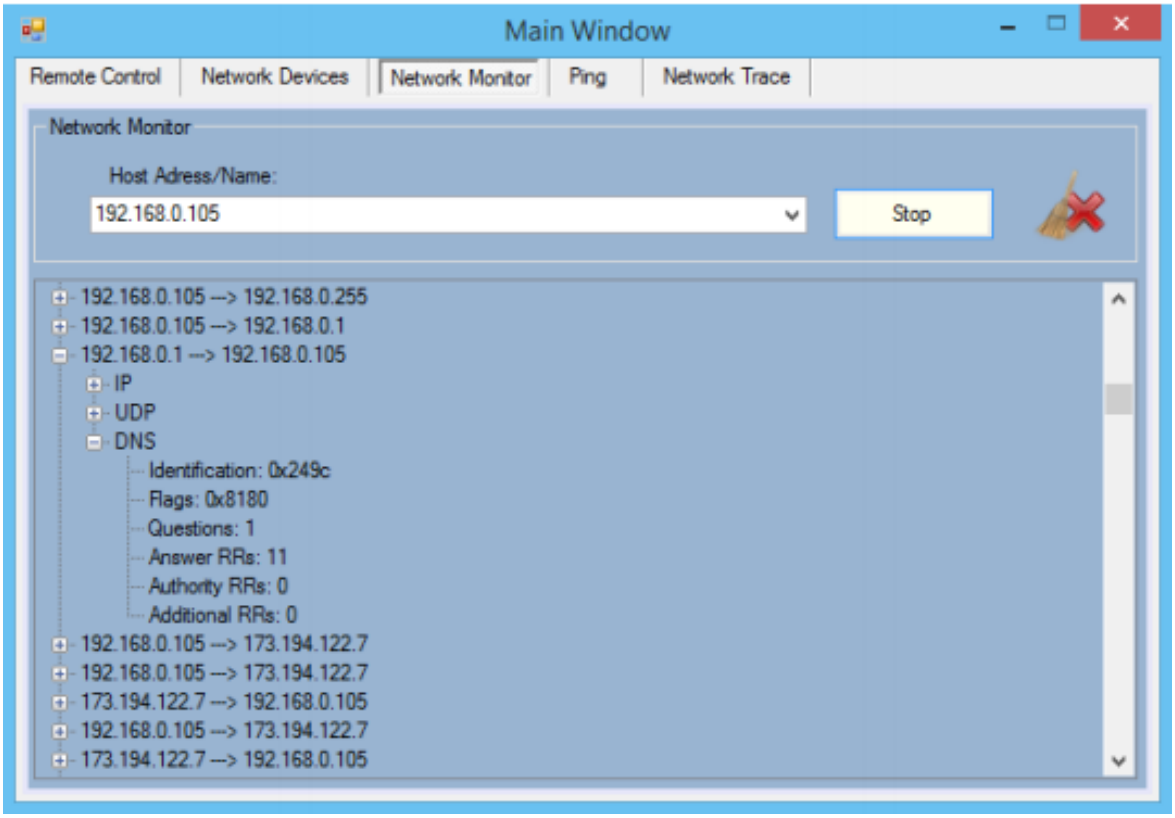


Рисунок 22 - Мониторинг сети (демонстрация DNS)

Рассмотрим подробнее раздел проверки связи [12]. Пример кода для метода ping можно увидеть 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 - Пример фрагмента метода Ping

Эта часть кодирования разделена на два условия, связанные с предустановленным местом для вставки имени хоста или IP-адреса. Первое условие связано с нулевым значением, что означает, что в текстовой области ничего не написано. В этом случае в предусмотренном для сбора информации методом ping ничего не появится. В противном случае программа начнет применять метод ping к адресу 4 раза по методу BeingPingHost, исходя из значения AsyncCallback. Результат этой части будет отображаться в указанном месте, которое является полем элемента списка. Второе условие связано с сохранением результата в лог-листе. Если текстовая область не была нулевой, то результат будет сохранен в предопределенном листе журнала.

В разделе ping пользователь сервера вставляет IP-адрес или имя желаемого хоста в предоставленное текстовое поле и, нажав кнопку «Пуск», вся информация будет отображаться в указанном месте ниже. Данная информация будет о хосте и показывает серверу, что выбранный хост работает или не работает. Рисунок 24 представляет раздел ping.

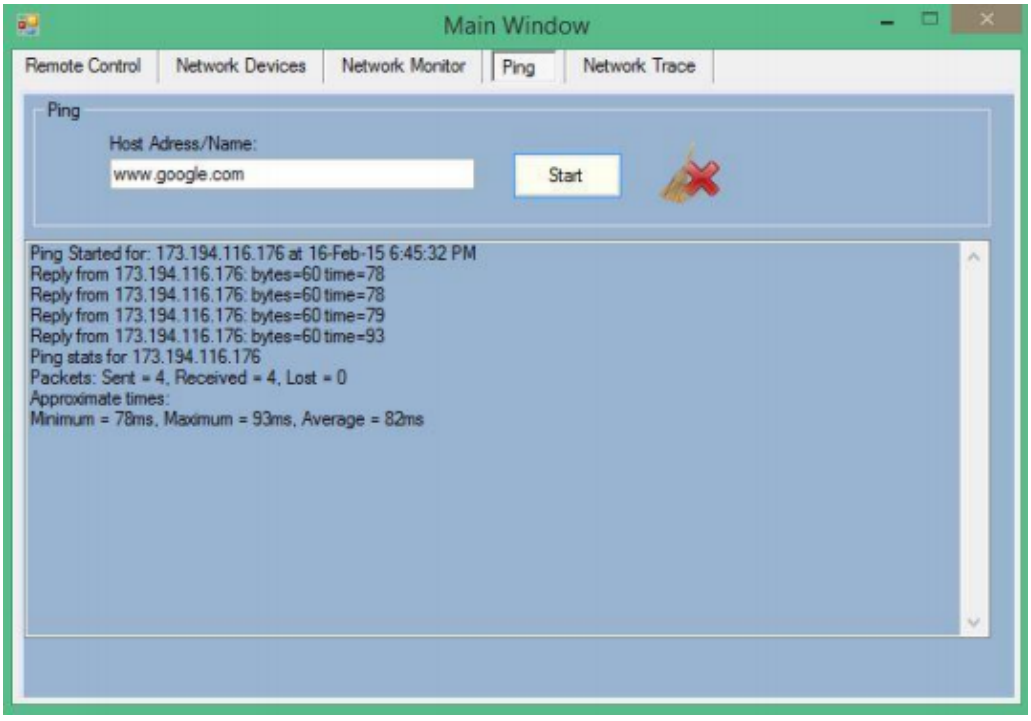


Рисунок 24 - Секция проверки связи

В приведенном примере, показанном на рисунке 24, представлен метод ping для веб-сайта Google с использованием его имени, а также показаны все процессы отправки и получения пакетов для установления соединения между серверным устройством и хостом. Ping выполняется путем отправки пакетов запроса на хост-получатель и ожидания ответа. В этом процессе он рассчитывает время от отправки до ответа и записывает любые потери пакетов. Результаты в этом примере представлены в виде информации о минимальном, максимальном и среднем времени этого процесса, а также информации о потере пакетов, отправленных и полученных пакетах.

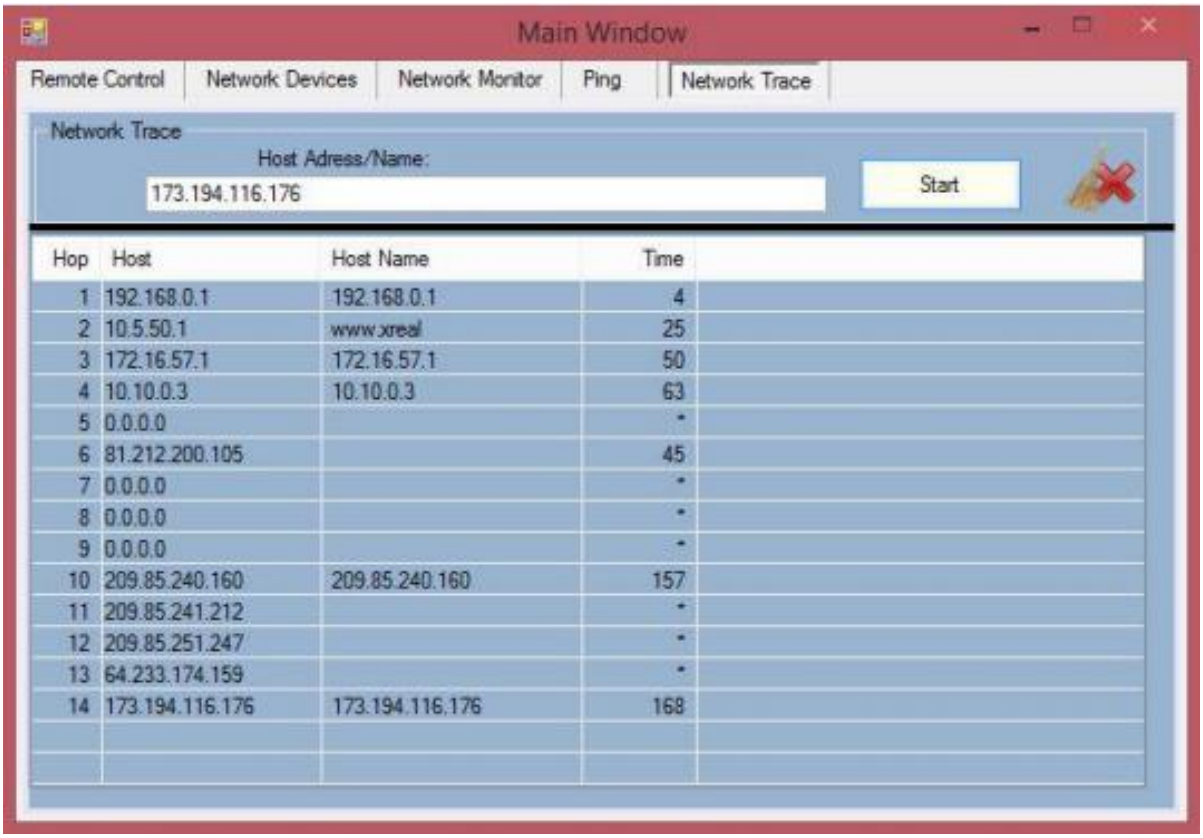
Пример кода раздела сетевой трассировки показан на рисунке 25. Как видно из примера кода, IP-адрес или имя хоста, которые были вставлены в предоставленную текстовую область, будут достигнуты. Затем предоставленный список элементов для отображения информации будет очищен, чтобы быть готовым для новой информации о трассировке. Для отслеживания сети маршрут между хостом и сервером будет исследоваться с использованием метода tracert.Trace. Отображаемая информация об этом процессе будет храниться в журнале.

```
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 - Пример части сетевой трассировки

Как показано на рисунке 26, в разделе трассировки сети администратор сервера сможет вставить желаемый IP-адрес хоста в предоставленную

область. При нажатии кнопки запуска вся информация о пути между серверным устройством и выбранным хостом будет отображаться в предоставленной среде.



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

В приведенном примере, показанном на рисунке 26, показан путь между серверным устройством и желаемым IP-адресом, которым в данном примере является IP-адрес www.google.com. Информация представляет маршрутизаторы и точки доступа, которые находятся в середине пути между серверным устройством и веб-сайтом Google. Следует отметить, что IP-адреса международных маршрутизаторов не будут идентифицированы по соображениям безопасности. Одной из предоставленных сведений является IP-адрес сетевых устройств в середине пути между сервером и пунктом назначения. Другая информация - это имя хоста, которое в случае наличия любого имени будет отображаться. Время, как и другая информация,

измеряется в миллисекундах. Время связано с расчетным временем получения пакета каждым сетевым устройством на маршруте.

В разделе серверной части следует учитывать, что устройство сервера должно иметь статический IP-адрес. В случае наличия динамического IP-адреса в разделе мониторинга сети IP-адрес клиента не будет отображаться в раскрывающемся списке. Причина в том, что эта система реализована на третьем уровне TCP/IP, то есть на сетевом уровне.

Рассмотрим подробнее работу со стороны клиентской части.

На стороне клиента этого приложения, как показано на рисунке 27, были предоставлены некоторые опции для подключения клиента к серверу.

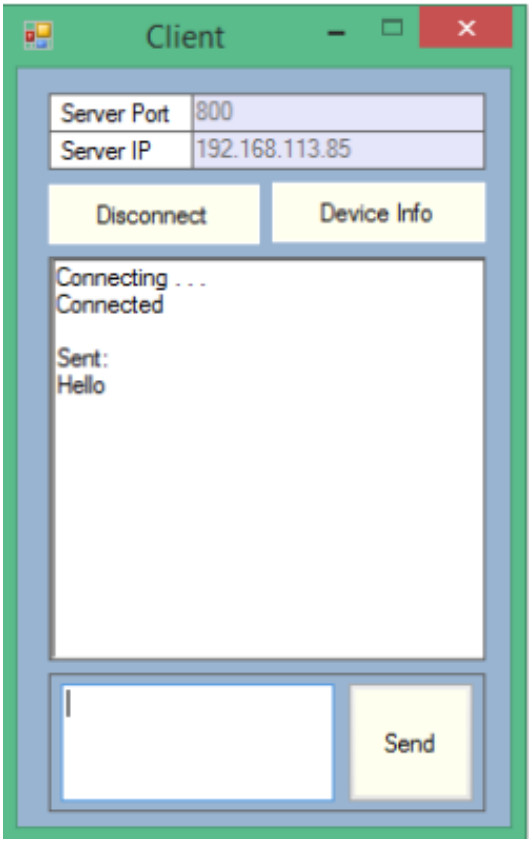


Рисунок 27 - Сторона клиента

Вставив IP-адрес сервера, а также установив номер порта, который должен совпадать с установленным номером порта на стороне сервера, клиент сможет подключиться к системе сервера. После этого шага клиент

сможет общаться с сервером. Кроме того, клиент имеет возможность контролировать информацию о сетевых устройствах, и в случае любого отключения или сбоя в системе будут предоставлены некоторые решения для устранения неполадок, показанные на рисунке 28.

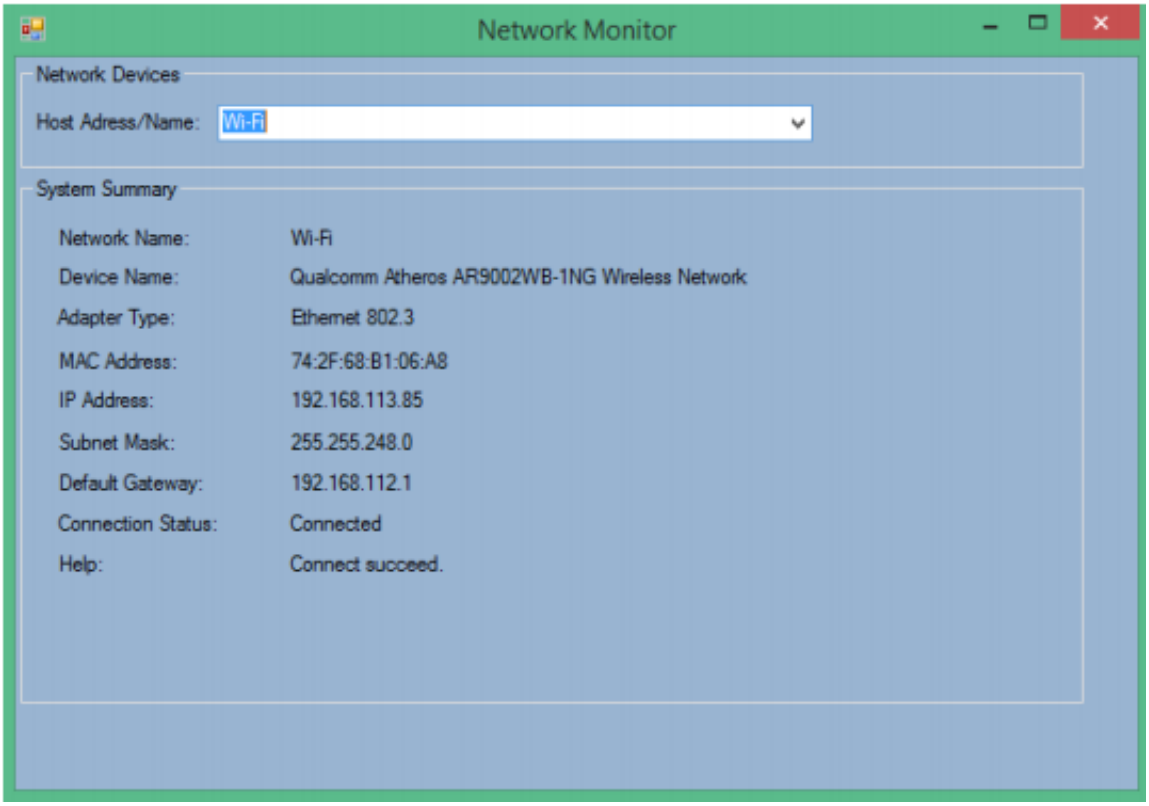


Рисунок 28 - Информация об устройстве для клиентской стороны

Представленный пример, показанный на рисунке 27, показывает отправленные сообщения от клиента к серверу [22]. Пример, представленный на рисунке 28, показывает информацию об устройстве для клиентской стороны.

В отчёте о доступности (рисунок 29) показаны статусы состояний серверного оборудования по времени. Отчет сформирован за год. Различными цветами выделены следующие состояния: красный — сервер выключен или не работает; зеленый — полная работоспособность; желтый —

простой оборудования; серый — агент не подключен к данному оборудованию.

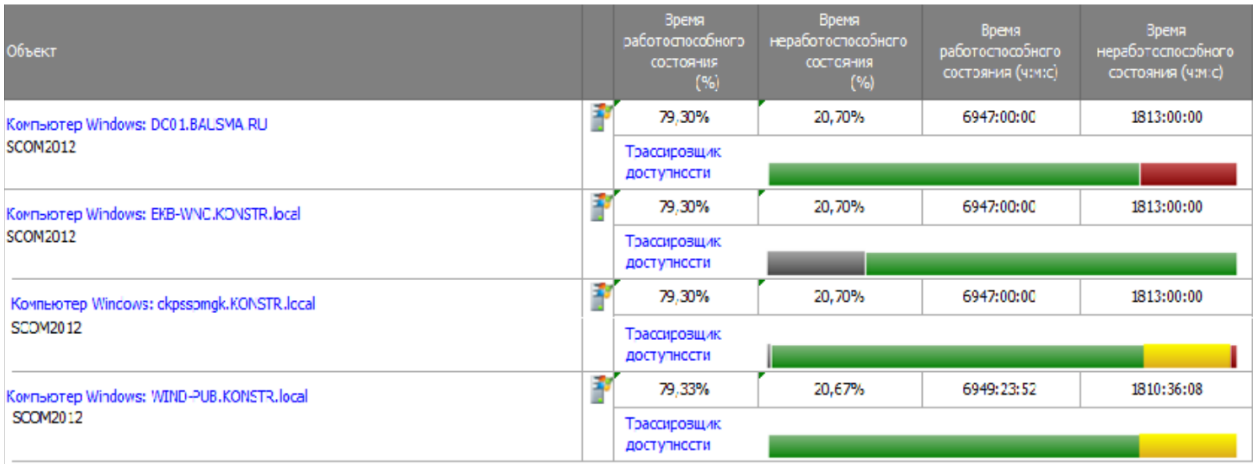


Рисунок 29 - Отчет о доступности серверного оборудования

Отчет позволяет отследить за любой период времени работоспособность серверов и другого оборудования, что очень удобно для администратора, так как показывает, какие сервера простаивают без нагрузки, а как выключены или сломались. Также можно настроить данный отчет, чтоб он приходил на электронную почту, как администратору, так и руководству, для анализа критических ситуаций и быстрого принятия решений. Возможно, требуется срочный ремонт оборудования или перераспределение нагрузки.

3.2 Расчет показателей экономической эффективности работы

Экономическая эффективность даёт возможность обосновать и поставить оценку о нуждаемости предприятия или компании в внедряемом программном продукте. Первичным вариантом технического процесса принималась работа сотрудников технической поддержки в обработке запросов без автоматизированной информационной системы. А в качестве внедряемого варианта предлагалась использовать разработанную

автоматизированную информационную систему в рамках бакалаврской работы.

В таблице 9 представлены капитальные (единовременные) затраты проектирования ИС

Таблица 9 – Капитальные затраты проектирования ИС

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 информационной базы	ЗП разработчика	10000
	Работа ЭВМ	296
Затраты на обучение персонала	ЗП обучаемого	1660
Затраты на опытную эксплуатацию	ЗП разработчика	7000
	Работа ЭВМ	237

Итого**:** сумма эксплуатационных затрат составляет 42361 рублей.

На рисунке 30 представлена диаграмма, отображающая соотношение статей капитальных затрат по проекту

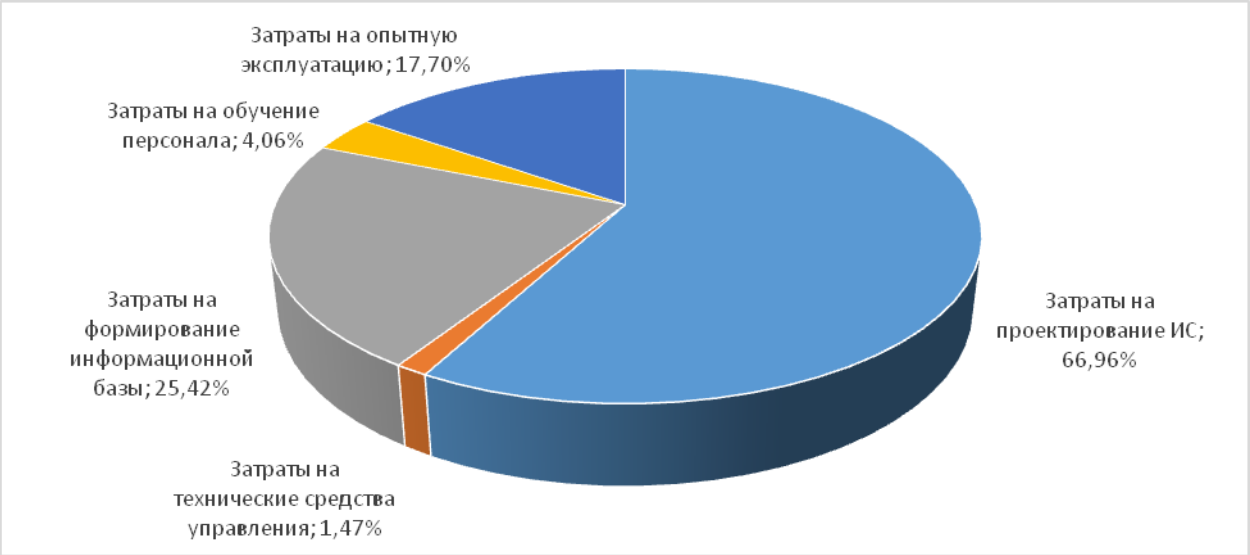


Рисунок 30 – Соотношение статей капитальных затрат по проекту

В таблице 10 представлены эксплуатационные затраты.

Таблица 10 – Эксплуатационные затраты проектирования системы мониторинга.

Затраты	Сумма, руб
Зарплата сетевого администратора	0
Амортизационные отчисления	7500
Затраты на техническое обслуживание	6000
Затраты, связанные с использованием глобальных вычислительных сетей Internet	4200
Затраты на носители информации	0
Прочие затраты	354

Итого: сумма эксплуатационных затрат составляет 21240 рублей в год.

На рисунке 31 представлена диаграмма, отображающая соотношение статей эксплуатационных затрат по проекту

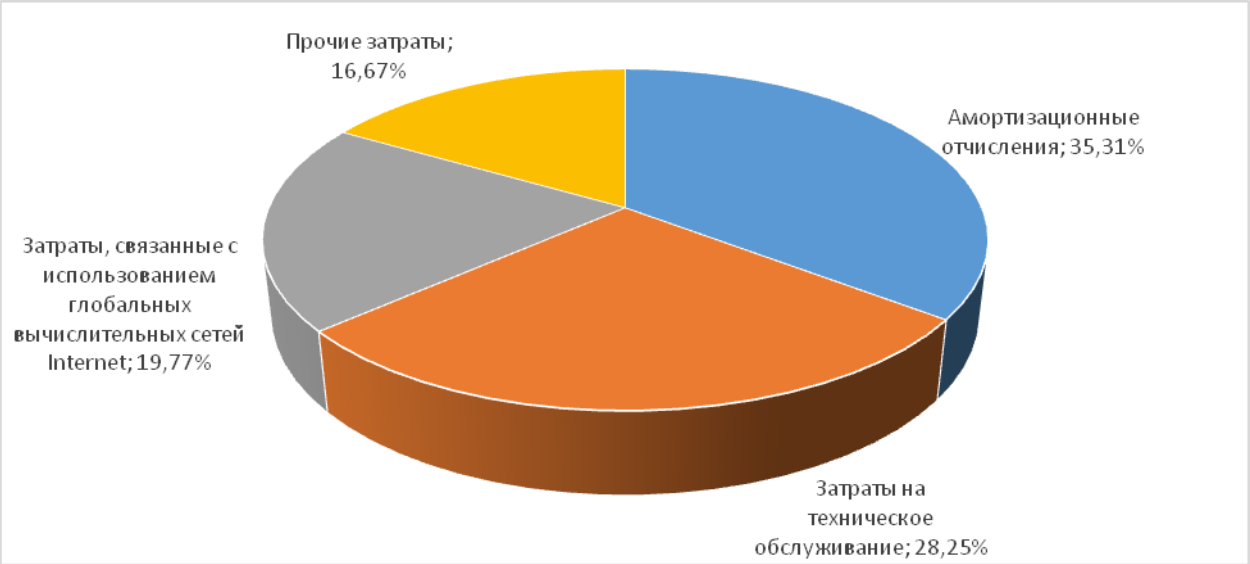


Рисунок 31 – Соотношение статей эксплуатационных затрат

Эксплуатационные затраты, в отличие от капитальных, являются повторяющимися. Они повторяются в каждом цикле производства, а рассчитываются в сумме за год. Эксплуатационные затраты осуществляются синхронно с производством. Эксплуатационные затраты составляют себестоимость продукции или услуг.

Таким образом, видно, что использование второго варианта (проектного) может привести к немалому уменьшению рабочих и стоимостных издержек. Данный результат в общей сложности даёт понять, что предлагаемый вариант решает поставленные задачи в два раза быстрее и эффективнее базового варианта, что для предприятия или для компании очень выгодно. Данный продукт может поддерживать внедрение для снижения расходов и повышения качества и эффективности работы сотрудников.

Выводы по главе 3

Было построено приложение, основанное на архитектуре клиент-сервер. Система мониторинга построена как на клиентских, так и на

серверных устройствах. Поскольку сервер подключен к сети, клиентам разрешено подключаться к серверу, используя соответствующий номер порта и IP-адрес сервера

Была реализована система мониторинга локально-вычислительной сети в организации, которая показала способность оценивать работоспособность за заданный период времени работоспособность серверов и другого оборудования.

А оценка затрат на проект показывает, что решение эффективное: ускоряет процесс выполнения задач и минимизирует возможные ошибки, что приводит к уменьшению рисков в процессе функционирования локально-вычислительной сети в организации.

Заключение

В ВКР были отражены концепции мониторинга сети, удаленного доступа и другие концепции, связанные с этой работой. Кроме того, были исследованы аналогичные работы, которые ранее проводились в этой области, и дано сравнение между реализованным приложением и существующими инструментами. Кроме того, процесс, процедуры и условия внедренного приложения, шаг за шагом, были подробно объяснены.

Анализ существующих систем мониторинга производительности сетевых систем показал, что подобные системы позволяют пользователю просматривать и управлять качеством производительности, анализом данных и ошибками сети Интернет-протокола (IP). Было выявлено, что инструмент мониторинга производительности является важным активом для системного администратора, позволяющим постоянно отслеживать работу сети на основе данных, собираемых через регулярные промежутки времени.

Основываясь на проведенном анализе, можно сделать вывод, что типичная сеть состоит из различных аппаратных устройств, таких как мосты, повторители, коммутаторы, маршрутизаторы и т. д. Мониторинг сети включает в себя проверку правильности функционирования этих устройств, а также обеспечение доступности связующей среды и нужен, чтобы обеспечивать бесперебойную работу вычислительной системы в организации. А предлагаемое решение будет аналогично существующим системам, но будет иметь интерактивный интерфейс и возможность быстрого обмена сообщениями через чат.

В рамках данной ВКР реализована упрощенная система мониторинга сети. Анализ исследований показал, что все существующие на рынке инструменты мониторинга сети имеют сложный пользовательский интерфейс, если они не работают на основе структуры командной строки.

Основной целью проекта ВКР было создание простой в использовании системы мониторинга сети, которая содержит большинство необходимых функций. Мониторинг и анализ пакетов позволит администратору пользователя контролировать безопасность всей сети.

Система отвечала всем заданным функциональным требованиям. В том числе:

– система способна решить проблему, с которой столкнулся клиент, и позволить клиенту опубликовать проблему,

– информация сохраняется в базе данных, к которой уполномоченный персонал может получить удаленный доступ,

– лучшее управление IP-адресами.

Онлайн-система управления сетью может решить все поставленные перед ней задачи. В том числе:

– безопасная работающая СУБД для отправки сведений о проблеме,

– разработанная универсальная база данных для обмена данными о записях проблем,

– система, которая будет запрашивать информацию о проблемах и решениях по клиентам, отделам и зданиям из любого места.

Была реализована система мониторинга локально-вычислительной сети в организации, которая показала способность оценивать работоспособность за заданный период времени работоспособность серверов и другого оборудования. А оценка затрат на проект показывает, что решение эффективное: ускоряет процесс выполнения задач и минимизирует возможные ошибки, что приводит к уменьшению рисков в процессе функционирования локально-вычислительной сети в организации.

Система мониторинга сети может использоваться как студентами, так и начинающими пользователями. Таким образом, это приложение может быть использовано в образовательных и обучающих целях.

Список используемой литературы

1. Артюшенко, В. В. Компьютерные сети и телекоммуникации : учебно-методическое пособие / В. В. Артюшенко, А. В. Никулин. — Новосибирск : Новосибирский государственный технический университет, 2020. — 72 с.

2. Архитектуры и топологии многопроцессорных вычислительных систем : учебник / А. В. Богданов, В. В. Корхов, В. В. Мареев, Е. Н. Станкова. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 135 с.

3. Биллиг, В. А. Основы объектного программирования на C# (C# 3.0, VisualStudio 2008) : учебник / В. А. Биллиг. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 409 с.

4. Виноградов, Г. П. Компьютерные сети. Работа в сети Интернет : учебное пособие / Г. П. Виноградов, Е. Е. Фомина, Г. В. Кошкина. — Тверь :ТвГТУ, 2022. — 116 с.

5. Галас, В. П. Вычислительные системы, сети и телекоммуникации. Часть 1. Вычислительные системы : электронный учебник / В. П. Галас. — Владимир : Владимирский государственный университет им. А.Г. и Н.Г. Столетовых, 2016. — 232 с. [электронный ресурс] Режим доступа: https://www.iprbookshop.ru/57363.html (дата обращения: 17.09.2022)

6. Горелов, С. В. Современные технологии программирования: разработка Windows-приложений на языке C#. В 2 томах. Т.II : учебник / С. В. Горелов ; под редакцией П. Б. Лукьянова. — Москва : Прометей, 2019. — 378 с.

7. Казанский, А. А. Объектно-ориентированное программирование на языке MicrosoftVisual C# в среде разработки MicrosoftVisualStudio 2008 и .NET Framework. 4.3 : учебное пособие и практикум / А. А. Казанский. —

Москва : Московский государственный строительный университет, ЭБС АСВ, 2011. — 180 с.

8. Ковган, Н. М. Компьютерные сети : учебное пособие / Н. М. Ковган. — Минск : Республиканский институт профессионального образования (РИПО), 2019. — 179 с. [электронный ресурс] Режим доступа: https://www.iprbookshop.ru/93384.html (дата обращения: 17.09.2022)

9. Компьютерные сети : учебник / В. Г. Карташевский, Б. Я. Лихтциндер, Н. В. Киреева, М. А. Буранова. — Самара : Поволжский государственный университет телекоммуникаций и информатики, 2016. — 267 с.

10. Кукарцев, В. В. Проектирование и архитектура информационных систем : учебник / В. В. Кукарцев, Р. Ю. Царев, О. А. Антамошкин. — Красноярск : Сибирский федеральный университет, 2019. — 192 с.

11. Мацкевич, А. Г. Лекции по курсу: Информационные технологии с изложением основ программирования на языке C#. Ч. 1 : учебное пособие / А. Г. Мацкевич. — Москва : Московский технический университет связи и информатики, 2016. — 81 с.

12. Минакова, О. В. Надежность информационных систем : учебник / О. В. Минакова. — Саратов : Вузовское образование, 2020. — 283 с.

13. Моделирование вычислительных сетей : методические указания / составители С. А. Олейникова, Т. И. Сергеева. — Воронеж : ВГТУ, 2022. — 40 с.

14. Нужнов, Е. В. Компьютерные сети. Часть 2. Технологии локальных и глобальных сетей : учебное пособие / Е. В. Нужнов. — Таганрог : Издательство Южного федерального университета, 2015. — 176 с.

15. Оливер, Ибе Компьютерные сети и службы удаленного доступа / ИбеОливер ; перевод И. В. Синицын. — 2-е изд. — Саратов : Профобразование, 2019. — 335 с.

16. Проскуряков, А. В. Компьютерные сети. Основы построения компьютерных сетей и телекоммуникаций : учебное пособие / А. В.

Проскуряков. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2018. — 201 с. [электронный ресурс] Режим доступа: https://www.iprbookshop.ru/87719.html (дата обращения: 17.09.2022)

17. Ракитин, Р. Ю. Компьютерные сети : учебное пособие / Р. Ю. Ракитин, Е. В. Москаленко. — Барнаул : Алтайский государственный педагогический университет, 2019. — 338 с. [электронный ресурс] Режим доступа: https://www.iprbookshop.ru/102731.html (дата обращения: 17.09.2022)

18. Сергеев, М. Ю. Компьютерные сети : практикум / М. Ю. Сергеев, Т. И. Сергеева, С. А. Олейникова. — Воронеж : Воронежский государственный технический университет, ЭБС АСВ, 2019. — 154 с. [электронный ресурс] Режим доступа: https://www.iprbookshop.ru/93261.html (дата обращения: 17.09.2022)

19. Bipin Joshi. Beginning XML with C# 7: XML Processing and Data Access for C# Developers. — 301 Pitruchhaya, Thane, India — 2017.— 464 p.

20. Douglas E. Comer. The Internet Book. Everything You Need to Know about Computer Networking and How the Internet Works: Fifth Edition. — CRC Press — 2019. — 405 p.

21. Irv Englander. The architecture of computer hardware, Systems software, & networking. — Bentley University — 2017. — 699 p.

22. Mike O'Leary. Cyber Operations: Building, Defending, and Attacking Modern Computer Networks. — Towson, MD, USA — 2019. — 1151 p.

23. Morris Sloman. A survey of trust in internet applications. - IEEE Communications Surveys & Tutorials. — 2000. — Т3 (№4). — p. 2-16

24. Richard Fox, Wei Hao. Internet Infrastructure: Networking, Web Services, and Cloud Computing. — CRC Press — 2018. — 633 p.

25. Trimintzios P., Polychronakis and over. DiMAPI: An Application Programming Interface for Distributed Network Monitoring. – 2006. – p. 382 - 393.