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 математикаи 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 ЛВС»

Обучающийся А.Ю. Жуков
(И.О. Фамилия) (личная подпись)

Руководитель Старший преподаватель В.В. Дружинкин
(ученая степень, звание, И.О. Фамилия)

Тольятти 2022

Аннотация

Тема выпускной квалификационной работы «Разработка системы мониторинга ЛВС».

Разработанасистема мониторинга ЛВС для администрации муниципального образования «Озёрский муниципальный округ».В работе представленатехнико-экономическая характеристика администрации муниципального образования «Озёрский муниципальный округ»: описание основных бизнес-процессов, анализ аппаратного и программного обеспечения, описание бизнес-процесса по модели «Как есть» с использованием методологии IDEF0. Сформулированы задачи на разработку системы мониторинга, проанализированы существующие разработки на соответствие сформулированным требованиям. Построена модель бизнес-процесса «Как должно быть» с использованием методологии UML. Проведён выбор и обоснование технологии логического проектирования системы. Посредством декомпозиции модели «Как должно быть» разработана логическая модель системы. Произведено моделирование архитектуры системы мониторинга. Сформулированы требования к аппаратно-программному обеспечению системы мониторинга ЛВС. Выбрано и описано программное обеспечение для реализации серверной и клиентской части системы. Произведено тестирование разработанной системы.

Объём работы – 71 страниц. Пояснительная записка содержит 7 таблиц, 35 рисунков, список использованной литературы, состоящий из 21 источника, а также 2 приложения.

Оглавление

Введение

Развитие информационных технологий в последнее десятилетие набрало очень высокие темпы, и сегодня даже небольшая компания не может обойтись без функционирующей локальной вычислительной сети (ЛВС), где даже небольшие инциденты могут означать полный паралич всей компании и значительные финансовые потери.Для эффективного администрирования сетевой инфраструктуры нельзя полагаться только на информацию от пользователей, но можно получать информацию об инцидентах заблаговременно посредством автоматизированного и непрекращающегося контроля. Таким образом, постоянный мониторинг состояния ЛВС и её узлов является основой эффективного решения различного рода проблем, возникающих в процессе повседневной эксплуатации компьютерной сети.

Тема выпускной квалификационной работы предложена кафедрой.

Объект исследования – система мониторинга ЛВС.

Предмет исследования – процессы по проверке работоспособности ЛВС в администрации муниципального образования «Озёрский муниципальный округ Калининградской области» В данной организации нет своей системы мониторинга ЛВС, что определяет актуальность предложенной темы.

Цель данной работы – проектирование, разработка, внедрение и тестирование системы мониторинга ЛВС для нужд администрации муниципального образования «Озёрский муниципальный округ Калининградской области».

Задачи исследования:

- анализ деятельности организации;
- разработка концептуальной и логической моделей проектируемой системы;
- моделирование архитектуры проектируемой системы;
- реализация и тестирование системы.

В первой главе приведена характеристика деятельности организации, её основных бизнес-процессов,проведён анализ аппаратного и программного обеспечения проанализирована эффективность текущей методики мониторинга ЛВС. Далее обосновывается необходимость разработки системы мониторинга ЛВС, приводится анализ существующих разработок.

Во второй главе выбраны технологии логического проектирования системы мониторинга ЛВС, разработана логическая модель системы, сформулированы требования к аппаратно-программному обеспечению. Третья глава содержит обоснование выбранных технологии реализации серверной и клиентской части, описание процесса реализации системы мониторинга ЛВС и её тестирования в виртуальной среде, а также результаты данного тестирования.

Глава 1 Анализ деятельности администрации Озёрского муниципального округа Калининградской области

1.1 Технико-экономическая характеристика организации

1.1.1 Характеристика организации

Администрация Озёрского муниципального округа является исполнительным и распорядительным органом муниципального образования «Озёрский муниципальный округ Калининградской области», который был образован 1 января 2022 года путем преобразования муниципального образования «Озёрский городской округ» в муниципальный округ. Администрация Озёрского муниципального округа является правопреемником администрации Озёрского городского округа. В соответствии с Уставом муниципального образования, в зону ответственности администрации Озёрского муниципального округа Калининградской области входит решение различных вопросов в границах округа и осуществление отдельных государственных полномочий, которые были переданы муниципальному образованию федеральными законами и законами Калининградской области.

Согласно Уставу муниципального образования, основная сфера деятельности организации [3]:

– формирование местного бюджета и его исполнение;

– обеспечение населения коммунальными, медицинскими и социальными услугами в пределах своих компетенций, организация и обеспечение населения транспортными услугами;

– обеспечение проживающих в муниципальном округе и нуждающихся в жилых помещениях граждан жильём;

– предупреждение и ликвидация последствий чрезвычайных ситуаций, создание условий для повышения туристической и инвестиционной привлекательности округа;

– обеспечение население средствами массовой информации;

– создание современной и комфортной городской среды;

– утверждение местных нормативных правовых актов и организация их соблюдения.

Правовой режим администрации Озёрского муниципального округа Калининградской области обозначен Уставом муниципального образования от 2 октября 2014 года (с изменениями на 25 января 2022 года), Законом Калининградской области о правовом регулировании вопросов организации местногосамоуправления от 7 марта 2006 года (с изменениями на 2 ноября 2021 года), федеральным законом обобщих принципах организации местного самоуправления в Российской Федерации от 6 октября 2003 года (в редакции от 30 декабря 2021 года). АдминистрацияОзёрского муниципального округа Калининградской области подчиняется окружному Совету депутатов, а также государственным органам.

Миссия организации – эффективно и своевременно предоставлять разнообразные услуги местным предприятиям, предпринимателям и жителям округа; стремиться к инновациям и устойчивому повышению уровня качества жизни в округе; максимизировать возможности для социального иэкономического развития, сохраняя при этом комфортные и безопасные условия для отдыха жителей и гостей округа.

На рисунке 1 изображена структурная схема организации с отделами, обеспечивающими её деятельность [7].

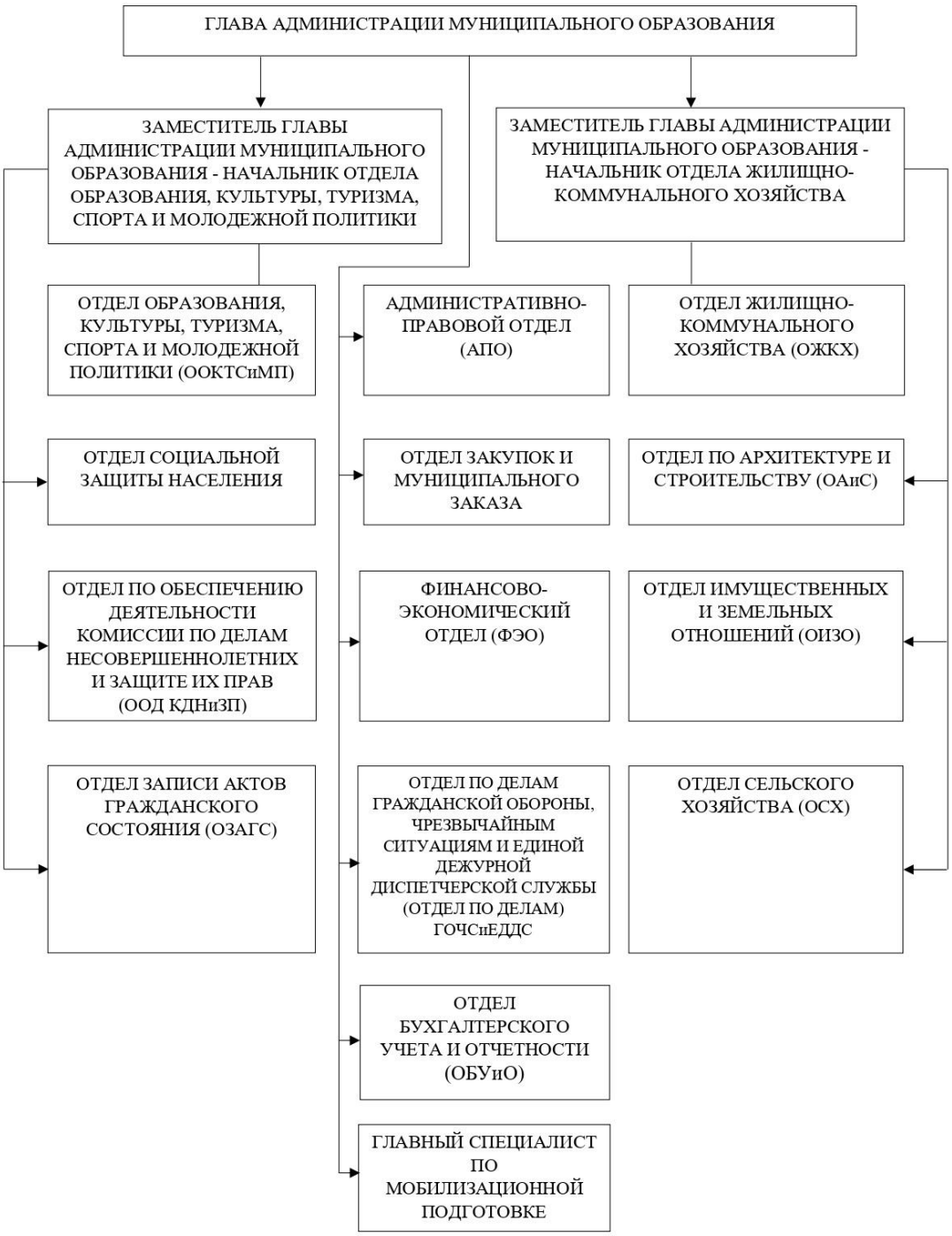

Рисунок 1 – Структура администрации Озёрского муниципального округа Калининградской области

На схеме организации видно, что общее руководство деятельностью администрации осуществляет глава администрации. В непосредственном подчинении у главы администрации находятся его заместители и все

структурные подразделения организации. Заместители главы курируют работу отделов, отнесенных к их компетенции. Отдел бухгалтерского учёта и отчётности производит расчёт окладов, начисление заработной платы сотрудникам, выполняет расчёт налоговых отчислений, проводит счета от поставщиков и подрядчиков.

В каждом отделе есть начальник отдела. Начальник отдела даёт поручения своим подчинённым и осуществляет контроль за их деятельностью, и именно начальник отдела несёт ответственность за все действияи результаты работы своих подчинённых.

Структурой организации не предусмотрен отдел информационных технологий (ИТ). Специалист, осуществляющий функции системного администратора и системного инженера, отнесен к административно-правовому отделу и подчиняется непосредственно главе администрации и начальнику отдела. Системный администратор отвечаютза установку, поддержку и техническое обслуживание серверов, рабочих станций, периферийных и сетевых устройств, других компьютерных систем. В обязанности системного администратора также входят установка и обновление программного обеспечения, резервное копирование данных и обеспечение бесперебойной работы ЛВС. Системный администратор планирует расширение ЛВС, документирует весь процесс и составляет внутреннюю вики-базу для других сотрудников. Порядок работы системного администратора определён его должностной инструкцией и положением об административно-правовом отделе.

SMM-специалист, отнесённый к административно-правовому отделу, отвечает за позиционирование и положительный имидж администрации в Интернете, а также взаимодействует с гражданами в социальных сетях, отвечая на их обращения.

Одним из основных документов в любой современной организации должна быть политика безопасности. Политика безопасности является краеугольным камнем информационной безопасности любой компании.Это

документ, определяющий основную концепцию защиты информации организации.Документ политики безопасности определяется как набор стандартов, правил и действий, которые определяют, как информация компании должна обрабатываться, защищаться и распространяться [8].Данный документ содержит толкование принципов и стандартов безопасности, определение ответственности за управление информационной безопасностью, включая отчётность об инцидентах безопасности.

В администрации муниципального образования «Озёрский муниципальный округ Калининградской области» политика информационной безопасности закреплена постановлением № 816 от 13 сентября 2019 года[4]. В частности, политика информационной безопасности распространяется на всех сотрудников администрации и информацию, которая обрабатывается. Степень конфиденциальности, целостности и доступности информации зависит от классификации информации.

1.1.2 Основные бизнес-процессы организации

К числу основных бизнес-процессов организации можно отнести следующие: управление организацией, управление кадрами, распоряжение бюджетом, управление функциями.

Функциональные процессы организации формируют внутри каждого отдела отдельные бизнес-процессы, включающие в себя управленческие мероприятия.

Бизнес-процессы отдела, обеспечивающего приём, регистрацию и обработку обращений граждан, состоят из следующих мероприятий: приём обращений, регистрация обращений, передача обращений главе администрации и начальникам отделов для их рассмотрения, выдача поручений исполнителям по каждому отдельно взятому обращению, контроль исполнения поручений по обращениям, оформление и отправка ответов на обращения.

Дополнительные бизнес-процессы обеспечивают нормальное течение основных процессов внутри организации. К таковым относится управление

ИТ, поскольку поддержка информационной инфраструктуры неразрывно связана со всеми другими бизнес-процессами организации.

Бизнес-процессы административно-правого отдела, в состав которого, как уже было отмечено, входит системный администратор, заключаются, помимо всего прочего, в поддержании работы бизнес-процессов других отделов администрации, которые взаимодействуют между собой посредством информационных систем (ИС) и ЛВС. Для обеспечения бесперебойного доступа к сетевым ресурсам, таким как финансовые и бухгалтерские системы, система учёта и обработки обращений граждан, базы данных (БД), очень важен постоянный мониторинг работы отдельных устройств и сервисов, а также сетевой инфраструктуры в целом.

Рассмотрев деятельность окружной администрации и её бизнес-процессы, рассмотрим аппаратную и программную части её инфраструктуры ИТ.

1.1.3 Анализ аппаратного и программного обеспечения в организации

В помещении организации расположены офис и серверная комната. В серверной комнате находится стойка с маршрутизатором и управляемыми коммутаторами, сервер, сетевое хранилище и сервер системы управления базами данных (СУБД) Microsoft SQL Server. В офисе находится обычные маршрутизаторы, рабочие станции сотрудников с операционными системами Windows 7 и 10, принтерыTriumph-Adler. Для работы с текстовыми документами и электронными таблицами на рабочих станциях сотрудников установлен офисный пакет MicrosoftOffice 2019. Топология локальной сети – звезда.

В таблицах 1 и 2 представлен анализ аппаратных и программных средств в администрации муниципального образования «Озёрский муниципальный округ Калининградской области» и результат оценки необходимости их обновления.

Таблица 1 – Анализ технических средств

Техническое средство	Требует обновления (Да/Нет)
Серверное оборудование (серверы, файловое хранилище, сетевое оборудование)	Нет
Серверы программных средств	Нет
Сетевое оборудование, обеспечивающее работу ЛВС и маршрутизацию трафика	Нет
Рабочие станции сотрудников, принтеры	Да

В качестве программного обеспечения на сервере и сервереСУБД используется операционная система WindowsServer 2019. Маршрутизаторы Mikrotik работают на собственной операционной системе RouterOS. «RouterOS – сетевая операционная система на базе Linux. RouterOS предназначена для установки на маршрутизаторы MikroTik RouterBoard» [17].

Для автоматизации ведения бухгалтерского учёта администрация использует программный комплекс «1С: Бухгалтерия 8».

В качестве системы электронного документооборота (СЭД) в администрации «Озёрский муниципальный округ Калининградской области» используется система «ДЕЛО». Данная система предназначена для автоматизации работы с документами, ведения электронного документооборота, хранения документов, контроля работы предприятия, фиксации заявок и обращений физических и юридических лиц, гибкого анализа всей отчётности.

Приём обращений осуществляется с помощью онлайн-формы через сайт компании, телефонного звонка или визита в офис администрации. При использовании любого из способов в конечном итоге обращение попадает в СЭД «ДЕЛО», установленную на сервере.

Таблица 2 – Анализ программных средств

Программное средство	Требует обновления (Да/Нет)
Система «1С: Бухгалтерия 8»	Нет
Система электронного документооборота	Нет
Операционные системы на серверах	Нет
Операционные системы на рабочих станциях сотрудников	Да
Офисные пакеты на рабочих станциях сотрудников	Нет

Анализ аппаратного и программного обеспечения показывает, что рабочие станции и используемые на них операционные системы устарели. Для эффективного и быстрого решения задач сотрудниками рабочие станции и операционные системы необходимо заменить на более актуальные.

Кроме того, анализ даёт понять, что в организации широко применяются сети передачи данных и сетевые технологии, в том числе критически важное программное обеспечение, которое работает по принципу «клиент-сервер».

В серверной комнате установлено несколько серверов, доступ к которым должных быть бесперебойным и беспроблемным, фактически постоянным. Таким образом, одной из важнейших задач системного администратора организации должен быть постоянный контроль за работой компонентов ЛВС, чтобы предотвратить сбои или свести их к минимуму.

1.2 Концептуальное моделирование предметной области и обоснование необходимости разработки системы мониторинга ЛВС

Из всейсовокупности задач административно-правового отдела была рассмотрена задача по мониторингу ЛВС.

Для раскрытия сущности рассматриваемого процесса необходимо провести обследование методики мониторинга ЛВС.

Для описания бизнес-процессов по модели «Как есть» сформируем схемы IDEF0 в приложении AllFusionERwinDataModeler с различным уровнем детализации.

В модели «Как есть» показано, как на данный момент происходит процесс мониторинга ЛВС. Блок А-0 – мониторить ЛВС. Вход – диапазон IP-адресов. Управление – методы мониторинга ЛВС. Механизм – системный администратор, набор утилит для работы с TCP/IP. Выход – отчётность (рисунок 2).

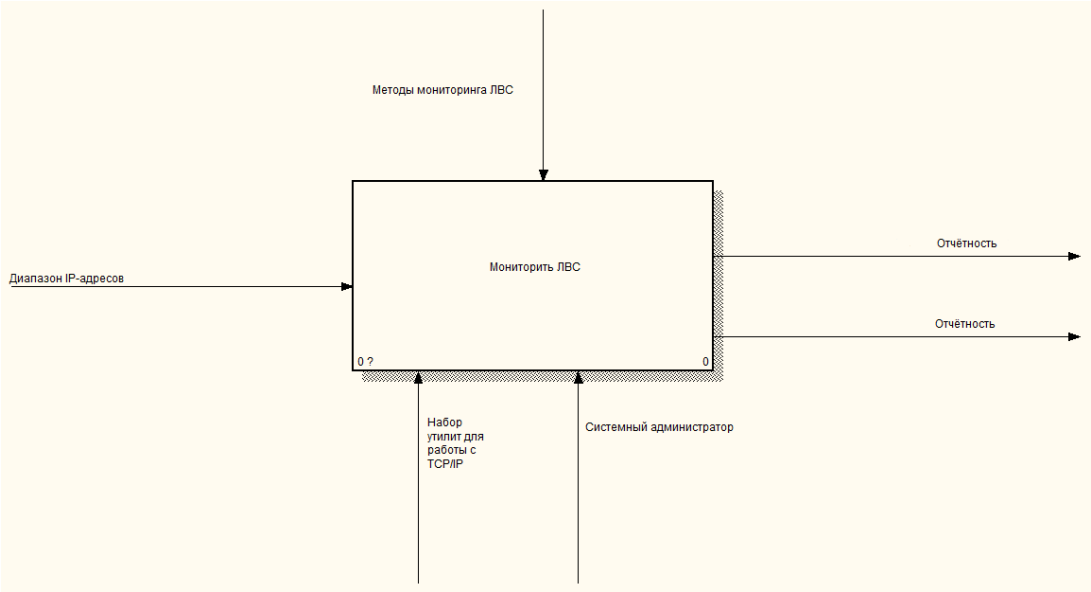

Рисунок 2 – Контекстная модель процесса мониторинга ЛВС

Для детализации бизнес-процесса построим диаграмму декомпозиции IDEF0 первого уровня (рисунок 3).

Вблок А0 входятблоки А1, А2, А3, А4. Блок А1 – проверить целостность и качество соединений в ЛВС. Вход – диапазон IP-адресов. Управление – методы мониторинга ЛВС. Механизм – системный администратор, набор утилит для работы с TCP/IP. Выход – результаты сканирования.

Блок А2 – обнаружить SNMP-устройства в ЛВС. Вход – диапазон IP-адресов. Управление – методы мониторинга ЛВС. Механизм – системный администратор, набор утилит для работы с TCP/IP. Выход – отчётность.

Блок А3 – мониторинг трафика. Вход – диапазон IP-адресов. Управление – методы мониторинга ЛВС. Механизм – системный администратор, набор утилит для работы с TCP/IP. Выход – отчётность.

Блок А4 – отслеживать состояние узлов в ЛВС (подключён/отключён). Вход – диапазон IP-адресов. Управление – методы мониторинга ЛВС. Механизм – системный администратор, набор утилит для работы с TCP/IP. Выход – отчётность.

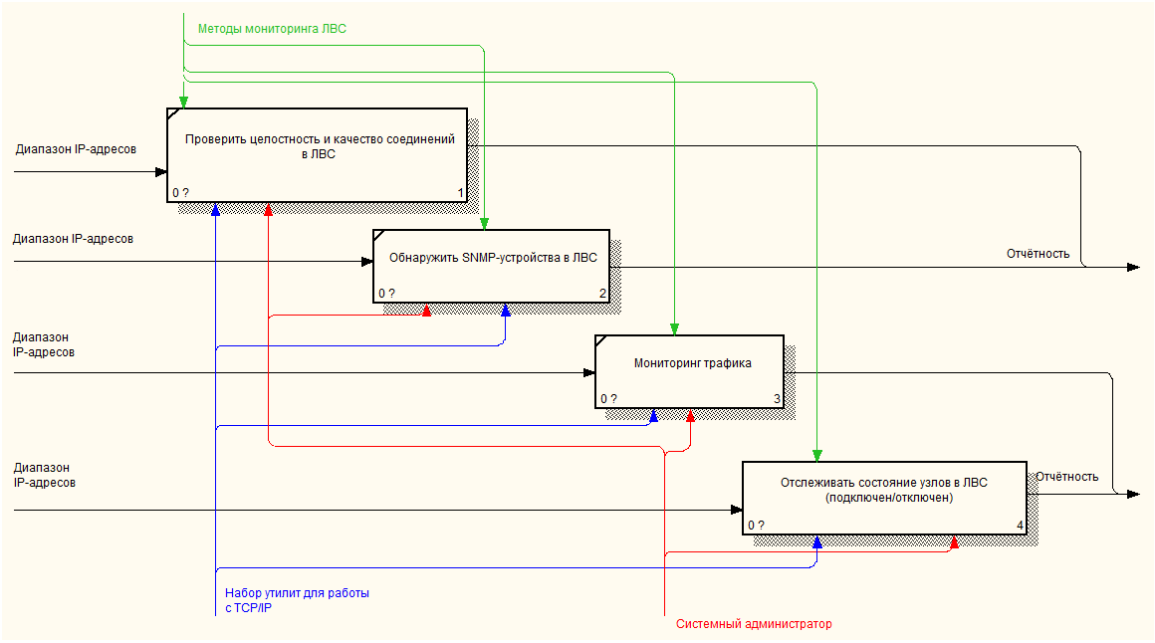

Рисунок 3 – Декомпозиция модели процесса мониторинга ЛВС

Проведение дальнейшей декомпозиции не является целесообразным, поскольку в процессе не получим никакой дополнительной информации о методике мониторинга ЛВС, которая в настоящее время применяется в организации.

Анализ-бизнес процесса показал, что для мониторинга ЛВС системный администратор использует набор утилит для работы с TCP/IP, входящих в

состав программного продукта IP-Tools. Данный бизнес-процесс был декомпозирован на несколько подпроцессов, которые необходимы для достижения цели основного бизнес-процесса. В частности, системный администратор:

– запускает IP-Tools;

– указывает диапазон IP-адресов;

– запускает утилиты, которые позволяют проверить целостность и качество соединений в ЛВС (ping), обнаружить SNMP-устройства в ЛВС, отслеживать трафик в сети и состояние узлов в ЛВС;

– на выходе системный администратор получает результаты тестирования и отчёты, содержащие информацию о задержках в сети, количестве потерянных пакетов; о состоянии отдельных хостов, сетевых устройств в сети и т.д.

Таким образом, в данном пункте было произведено моделирование и анализ методики мониторинга ЛВС, применяемой в организации на текущий момент. Применение программных средств, которые системный администратор использует для анализа сетевого трафика и, кроме того, для считывания рабочих параметров сетевых устройств, не является оптимальным методом получения данных о состоянии ЛВС. В частности, после анализа можно выделить следующие основные недостатки применяемой методики:

– необходимость вручную проводить мониторинг ЛВС, что является утомительным и неэффективным;

– отсутствие постоянного контроля за состоянием ЛВС;

– системному администратору приходится тратить слишком много времени на обнаружение проблемы, поскольку сетевая инфраструктура состоит из множества узлов и сетевых устройств;

– невозможность оперативного принятия мер по устранению неполадок в ЛВС из-за отсутствия механизма уведомлений о неполадках по электронной почте или СМС.

Таким образом, для оптимизации процесса мониторинга ЛВС целесообразным является применение автоматизированной ИС. Для автоматизированного мониторинга ЛВС может быть разработана и внедрена система мониторинга, требования к которой будут поставлены в следующем пункте.

1.3 Постановка задачи на разработку системы мониторинга ЛВС

В администрации муниципального образования «Озёрский муниципальныйокруг Калининградской области» нет обособленного отдела ИТ, где упрофильного специалиста было бы время постоянно следить заисправностью всех ключевых компонентов сетевой инфраструктуры.Поэтому во многом эту задачу должна взять на себя система мониторинга ЛВС и автоматически сообщать о состоянии всей инфраструктуры.

Система мониторинга ЛВС должна в автоматическом режиме контролировать работу рабочих станций,серверов и активных сетевых устройств. Для рабочих станций необходиммониторинг нагрузки на систему: загрузка центрального процессора (ЦП), оперативного запоминающего устройства (ОЗУ) и использованиежёсткого диска. Кроме того, система мониторинга ЛВС должна отслеживатьи хранить информацию о перемещении сотрудников организации в данной сети.Для серверов необходимо мониторить рабочую нагрузку на всю систему, атакже её доступность, или доступность ключевых серверных служб ипотенциальные инциденты безопасности. Например, при смене пароляадминистратора сервера необходимо, чтобы система мониторинга уведомилаоб этом факте.На предмет доступности должны отслеживаться все активные сетевыеустройства. Система мониторинга должна уведомлять об инцидентах всехпредопределённых пользователей путём отправки электронных писем. Система мониторинга должна отображать выходные данные в удобной

дляпользователя форме, которая должна быть понятна даже пользователям,обладающим базовыми знаниями об отслеживаемой инфраструктуре ИТ.Система мониторинга должна быть развёрнута на существующих аппаратных мощностях. Затраты на разработку и внедрение системы мониторинга ЛВС должны быть минимальными или полностью отсутствовать.

Таким образом, в данном пункте была описана цель создания системымониторинга ЛВС, обусловлена необходимость разработки и выявленыосновные требования к системе.

1.4 Анализ существующих разработок на предмет соответствия сформулированным требованиям

В следующем параграфе описываются имеющиеся аналоги для мониторинга ЛВС и их основные функции.

Помимо обнаружения неполадок, системы мониторинга ЛВС проверяют доступность сетевых служб, формируют данные об использовании сети, формируют перечни сетевых узлов, позволяют просматривать данные об использовании ресурсов ЦП, ОЗУ, жёстких дисков и т.д. Отдельные системы данной категории проводятанализ ошибок и составляют отчёты с выводами, беря за основу собранную статистическую информацию.

На сегодняшний день разработаны десятки программных продуктов для мониторинга сети. Все условно можно разделить на платные и бесплатные. Однако идеальной системы не существует. Каждый продукт имеет свои преимущества и недостатки. Проанализируем возможности некоторых из них. В ходе исследования данной темы были выбраны самые известные системы мониторинга сети: Zabbix, Nagios и Cacti. На рисунке 4 приведена статистика обращений пользователей к поисковой системе Google

за последние 5 лет по запросам «zabbixmonitoring», «cactimonitoring»и «nagiosmonitoring» [15].

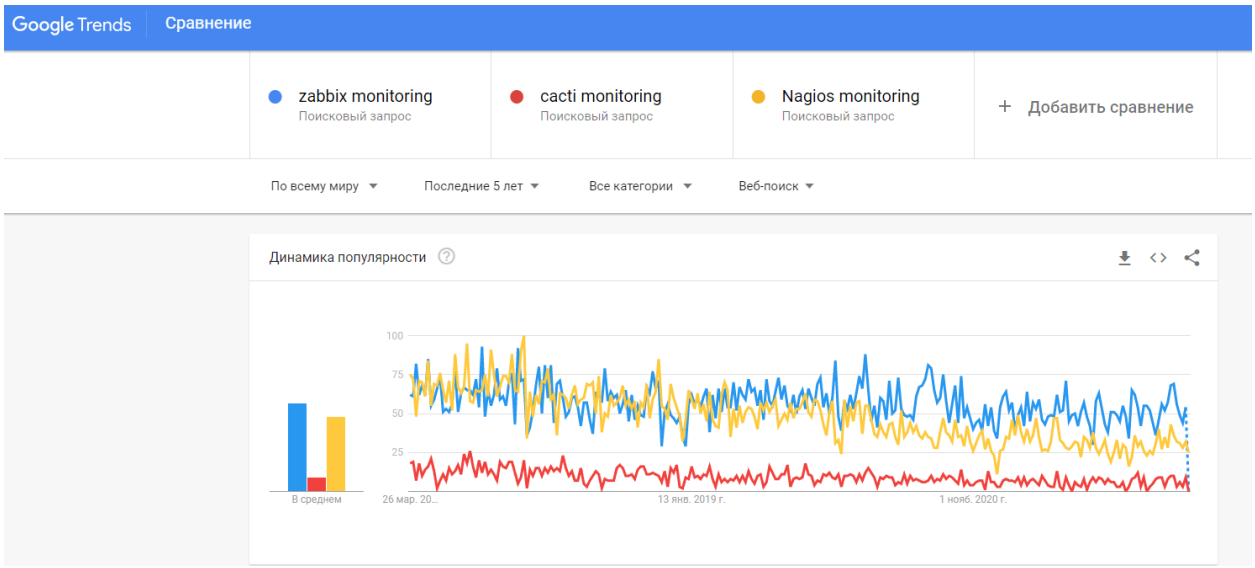

Рисунок 4 – Статистика обращений к Google

Видно, что самой популярной системой мониторинга в настоящее время является Zabbix, в то время как популярность Nagios постепенно снижается. Популярность Cacti ещё ниже.

1.4.1 Программа Nagios

Nagios – это программа с открытым исходным кодом, разработанная под лицензией General Public License (GPL). Онав первую очередь предназначена для ОС Linux, но при определённых условиях может работать и в других Unix-подобных операционных системах.

Ядро приложения содержит основные функции для мониторинга сетевых устройств и серверных служб, таких как HTTP, HTTPS, SSH, SMTP и другие. В Nagios можно установить дополнительные надстройки для наблюдения за состоянием операционной системы и рабочих станций в локальных сетях: информация о запущенных системных процессах, занятость жёсткого диска, ОЗУ, использование ЦП. При обнаружении проблемы Nagios может автоматически предпринять шаги для её устранения. Примером такого

действия является перезапуск службы веб-сервера при обнаружении недоступности протокола HTTP.

Проект разрабатывается с 1999 года, благодаря чему для него доступно большое количество плагинов. Предупреждения о нештатных ситуациях отображаются в веб-интерфейсе приложения и при необходимости могут быть отправлены по электронной почте, СМС или на мессенджер.

Конфигурация системы мониторинга достаточно сложная в базовом варианте. В ядре Nagios отсутствует графический интерфейс для настройки, поэтому конфигурация осуществляется исключительно путём редактирования конфигурационных файлов в текстовом формате. Чтобы упростить настройку и администрирование, можно использовать сторонние инструменты, например, Lilac, NagiosQL, NConf, OneCMDB.

Nagios подходит для мониторинга крупномасштабных сетей. Функции системы мониторинга могут быть разделены на несколько серверов, каждый из которых отслеживает выбранные клиенты, а собранная информация собирается в центральной базе данных и доступна в комплексном виде на центральной консоли (рисунок 5) [16].

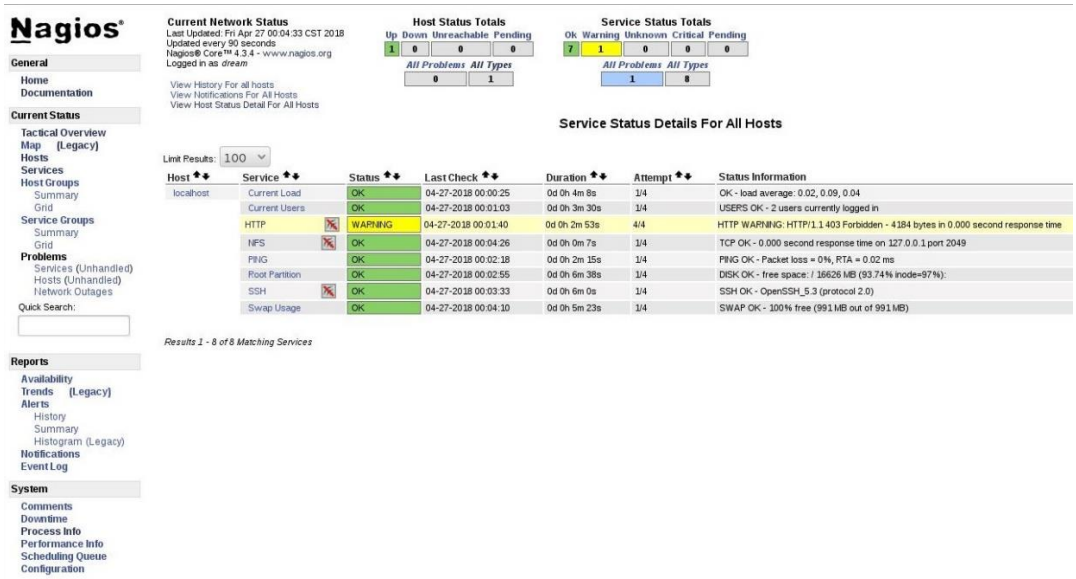

Рисунок 5 – Веб-консоль управления Nagios

1.4.2 Программа Cacti

Cacti – это программа с открытым исходным кодом, разработанная под лицензией GPL. Для запуска ей нужен инструмент RRDtool, который занимается сбором данных; база данных MySQL и веб-сервер с поддержкой PHP [19].Cactiможет работать в Windows, Linux или других Unix-подобных операционных системах. Поддерживает мониторинг по протоколу SNMP (англ. Simple Network Management Protocol – простой протокол сетевого управления) или SSH (англ. Secure Shell – «безопасная оболочка»). Таким образом, можно контролировать работу различных платформ, таких как Windows, Linux, сетевая операционная системаNetWare, а также широкий спектр сетевых устройств, таких как коммутаторы, маршрутизаторы, сетевые принтеры.

Отчёты Cacti отображаются в веб-интерфейсе, его сильной стороной являются графики, которые можно настроить под себя. Базовая конфигурация содержит шаблоны для различных операционных систем, из которых затем можно выбрать, какие данные будут отслеживаться. Можно редактировать шаблоны или создавать собственные. Большое количество шаблонов доступно на официальном сайте проекта, в том числе шаблоны для определённого типа сетевого элемента, для конкретной операционной системы.Ещё одним мощным инструментом является возможность писать собственные скрипты. Скрипты выполняют необходимые операции в отслеживаемой системе и возвращают выходные данные в консоль мониторинга (рисунок 6).К приложению имеется ряд дополнений, которые также можно скачать с сайта проекта. Например, надстройка Thold может отправлять уведомления по электронной почте, включая график измеренных значений, в случае превышения отслеживаемых значений.Таким образом, можно получить обзор развития ситуации, не входя в веб-интерфейс приложения.

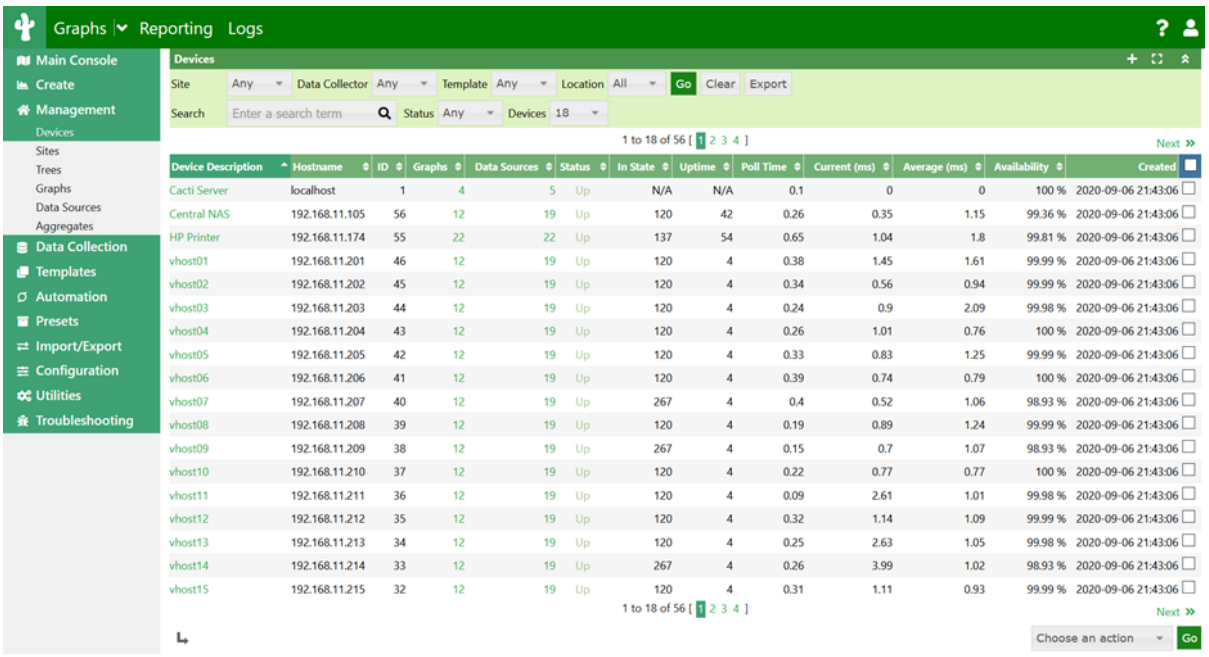

Рисунок 6 –Веб-консоль управления Cacti

Представлена Веб-консоль управления (рисунок 6)

1.4.3 Программа Zabbix

Zabbixиспользуется для мониторинга активных сетевых устройств, таких как рабочие станции, серверы под управлением различных платформ, принтеры, коммутаторы и другие подобные устройства, подключенные к компьютерной сети.Это программное обеспечение с открытым исходным кодом, разработанное под лицензией GPL. Поддерживается несколько методов мониторинга и определения состояния устройств.Основным методом является отправка запросов ICMP (ping) с использованием более сложных методов, таких как SNMP, IPMI (англ. Intelligent Platform Management Interface – интеллектуальный интерфейс управления платформой)и JMX(англ. Java Management Extensions – управленческие расширения Java). Также можно использовать протоколы SSH, Telnet или агенты мониторинга, которые доступны для большинства используемых сегодня операционных систем.При использовании агента можно отслеживать наибольший объем информации: состояние оборудования (ОЗУ, загрузка ЦП,

занятость жёсткого диска, загрузка сетевого интерфейса и т.д.), состояние запущенных служб [6].

Zabbix не требователен к ресурсам аппаратного обеспечения. 2-ядерного процессора и 2 ГБ оперативной памяти (примерно до 500 контролируемых устройств) должно хватить для нужд организации среднего размера. Однако вс зависит от количества контролируемых устройств, выбранного типа базы данных и продолжительности хранения данных.

Система мониторинга доступна через веб-интерфейс, который также служит средой администратора для управления данными и их оценки. Веб-интерфейс позволяет создавать различные учётные записи пользователей и группы в соответствии с требуемым доступом. Выходом пользовательского интерфейса являются графики и изображения контролируемых значений конкретных устройств или всей сети (рисунок 7). У каждого пользователя может быть настроен канал связи, по которому ему доставляются оповещения системы мониторинга.Каналом связи могут быть СМС, мессенджер или электронная почта.Серверная часть доступна для любой Unix-подобной системы или любого дистрибутива GNU/Linux.

Рисунок 7 – Веб-консоль управления Zabbix

Поддерживаются следующие операционные системы:

– Linux;
– IBM AIX;
– FreeBSD, OpenBSD, NetBSD;
– HP-UX;
– macOS;
– Solaris.

Еще одним условием работы серверной части является установка службы базы данных для хранения всех системных данных. Поддерживаются следующие СУБД:

– IBM DB2;
– MySQL;
– Oracle;
– PostgreSQL;
– SQLite.

Характеристики всех рассмотренных систем мониторинга для ясности перечислены в таблице 3.Требования для работы отдельных систем представлены в таблице 4.

Таблица 3 –Сравнение характеристик систем мониторинга

Система мониторинга	Преимущества	Недостатки	Особенности	Риски
Nagios	Большое и активное сообщество пользователей, поддержка оповещений, настройка с помощью шаблонов, расширение функций спомощью плагинов	Сложная установка и настройка, ограниченные возможности вывода на графиках	Возможность интеграции пользовательских сред со многими проектами с открытым исходным кодом	Риск увеличения затрат на системное администрирование из-за сложной конфигурации

Продолжение таблицы 3

Система мониторинга	Преимущества	Недостатки	Особенности	Риски
Zabbix	Поддержка оповещений, поддержка построения графиков, качественная документация	Официально поддерживает только Unix-подобные операционные системы	Может мониторить конкретный процесс и приложения для Windows	–
Cacti	Поддержка построения графиков с возможностью пользовательских настроек, отличная поддержка со стороны сообщества разработчиков	Неподдерживает мониторинг с агентом, сложная настройка и установка, поддерживает только СУБД MySQL	Поддерживает пользовательские скрипты для мониторинга через SSH	–

Таблица 4 –Требования к эксплуатации систем мониторинга

Система мониторинга	Операционная система	База данных
Nagios	Linux	MySQL, SQLite
Zabbix	Linux, BSD, macOS, Solaris, Windows	IBM DB2, MySQL, Oracle, PostgreSQL
Cacti	Linux, Windows	MySQL

Таким образом, из сравнительной таблицы видно, что ни одна из систем мониторинга не является явным фаворитом, выбор конкретной системы всегда будет зависеть от конкретных требований организации. Благодаря преимуществуZabbix в плане простоты использования, поддержки большого количества платформ, на которых может работать система, и возможности адаптации под большое количество требований, данная система мониторинга представляется наиболее подходящей для развёртывания. Качественная и подробная документация – ещё одно большое преимущество в пользу развертыванияданной системы мониторинга ЛВС.

1.5 Разработка модели бизнес-процесса «Как должно быть»

Для описания модели «Как должно быть» была выбрана диаграмма вариантов использования методологии UML, описывающая сценарии использования программной системы и их действующих лиц. Это может помочь разобраться в необходимых функциональных возможностях. Данный тип диаграмм был выбран за простоту и наглядность.

Диаграмма процесса «Как должно быть» изображена на рисунке 8. В данной модели задействован 1 актёр: «Системный администратор» – сотрудник, осуществляющий управление автоматизированной системой мониторинга ЛВС для отслеживания состояния сетевой инфраструктуры.

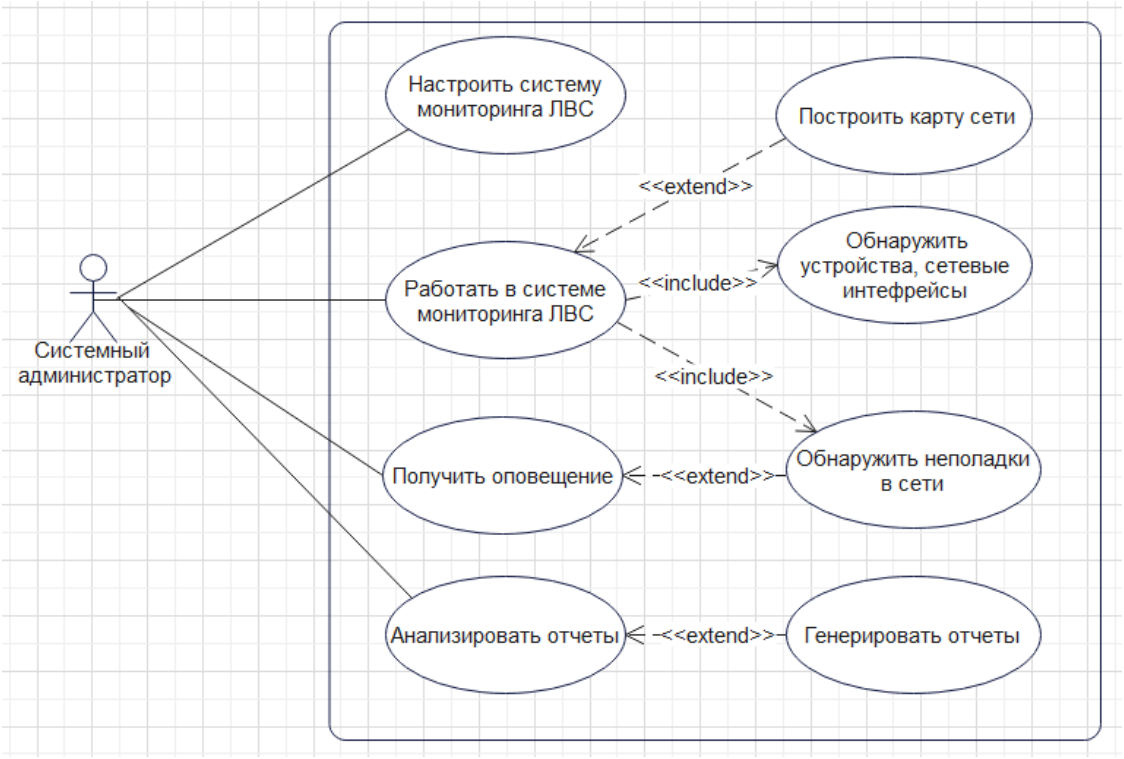

Рисунок 8 – Модель «Как должно быть»

Системный администратор осуществляет управление системой мониторинга путём варианта использования «Работа в системе мониторинга ЛВС», а также ряда других вариантов использования:

– системный администратор производит настройку системы мониторинга посредством варианта использования «Настроить систему мониторинга ЛВС»;

– системный администратор получает оповещения о неполадках в сети, отправленные системой мониторинга ЛВС;

– системный администратор просматривает отчёты, которые генерирует система мониторинга;

– при необходимости системный администратор проводит анализ отчётов.

Системный администратор осуществляет мониторинг сети посредством варианта использования «Обнаружить устройства, сетевые интерфейсы». Модель «Как должно быть» также содержит варианты использования «Обнаружить неполадки в сети», «Построить карту сети», «Генерировать отчёты». При обнаружении неполадок в сети система мониторинга ЛВС отправляет оповещение системному администратору.

Таким образом, внедрение автоматизированной системы мониторинга ЛВС повысит эффективность работы системного администратора при обнаружении возможных аномалий в работе сетевой инфраструктуры, позволив значительно сократить время простоя сети, а также время, необходимое для решения неполадок.

Выводы по главе 1

Была выполнена технико-экономическая характеристика деятельности организации, выделены основные бизнес-процессы, разработана и проанализирована модель «Как есть», на основе чегобыла разработана и проанализирована модель «Как должно быть». Былипоставлены и определены требования и задачи, основываясь на которыхвыявлена необходимость разработки автоматизированной системы мониторинга локальной вычислительной сети для нужд администрации муниципального образования «Озёрский муниципальный округ Калининградской области».

Было проведено сравнение нескольких существующих программ для мониторинга компьютерных сетей: они во многом похожи, но тщательный анализа каждого инструмента в отдельности показал, что величина недостатков программ Nagiosи Cactiзначительно перевешивает их преимущества, поэтому разрабатываемая система мониторинга локальной вычислительной сетибудет создана на основе свободного программного обеспеченияZabbix.Преимуществами Zabbixявляется несложный процесс установки и конфигурации, простая эксплуатация, обширная документация, а также наличие всех необходимых функций, которые из «коробки» включены в состав программного продукта. В отличие от Nagiosи Cacti, это исключает необходимость устанавливать дополнительные модули.

Глава 2 Логическое проектирование системы мониторинга ЛВС

2.1 Выбор технологии логического проектирования системы мониторинга ЛВС

При выборе технологии логического проектирования методологии целесообразно произвести сравнительный анализ популярных методологий моделирования предметной области: IDEF0 (Integration Definition for FunctionModeling), ARIS (Architecture of Integrated Information Systems), UML (Unified Modeling Language). При сравнении будут учитываться следующие условия:

- сложность освоения;
- удобство построения диаграмм;
- возможность декомпозиции;
- логическое выражение;
- метод проектирования;
- актуальность.

Методология IDEF0 предназначена для моделирования решений, действий, процессов в организации или системе, и используется особенно при создании функциональных моделей компании (моделей, фиксирующих производственные и другие функции компании и взаимосвязи между ними).С точки зрения количества элементов IDEF0 – очень простая модель. Модели состоят из подблоков: вход, управление, выход, механизм. Каждыйблок показывает определенную деятельность и её входы, выходы, основной механизм и управляющие входы.Окончательная модель, состоящая из набора блоков, представляет собой организованное представление отдельных видов деятельности и взаимосвязей между ними[11].

ARIS – это методология моделирования бизнес-процессов и связанных с ними других бизнес-компонентов, таких как организационная структура или структура данных.ARIS можно понимать как один из методов

реинжиниринга процессов, который делает упор на поддержку управления процессами с помощью ИТ-системы.Методология ARIS не направлена на создание точной процедуры подхода к реинжинирингу процессов, а скорее стремится предоставить ряд различных точек зрения, которые можно использовать для моделирования отдельных ситуаций.ARIS основана на тщательном анализе бизнес-процессов, моделируемых с разных точек зрения. В результате может получиться очень сложная и запутанная модель, которая становится намного понятнее благодаря разделению на отдельные виды. Отдельные представления могут быть описаны с помощью специальных методов, соответствующих конкретному представлению и моделируемой ситуации[14].

UMLявляется стандартизованнымязыком моделирования с широким применением. Язык UML был разработан на основе метода моделирования объектов. Он содержит спецификации основных типов диаграмм, включая возможность дальнейшейдекомпозиции.UML в первую очередь предназначен для использования в разработке программного обеспечения, но благодаря своей высокой универсальности он также позволяет моделировать бизнес-процессы[13]. В таблице 5 приведено сравнение методологий IDEF0, ARIS и UML.

Таблица 5 – Сравнительный анализ методологий

Критерий сравнения	Методология IDEF0	Методология ARIS	Методология UML
Сложность освоения	Низкая	Очень высокая	Низкая
Удобство построения диаграмм	Высокая	Низкая	Высокая
Декомпозиция	Неограниченная	Неограниченная	Неограниченная
Логическое выражение	Сложные данные можно выразить логически	Многие данные сложны, логическое выражение затруднено	Сложные данные можно выразить логически
Метод проектирования	Функциональный	Процессный	Объектный

Продолжение таблицы 5

Критерий сравнения	Методология IDEF0	Методология ARIS	Методология UML
Актуальность	Применяется редко, считается устаревшей	Применяется редко	Применяется часто

После сравнительного анализа можно заключить, что для логического проектирования целесообразнее использовать методологию UML, потому что она удобна, проста в освоении и основана на объектномметоде проектирования. Методология ARISсложна для понимания и освоения, а нотация IDEF0 остановилась в своём развитии и считается морально и функционально устаревшей [10].

2.2 Разработка логической модели проектируемой системы мониторинга ЛВС

Логическаямодель проектируемой системы мониторинга ЛВС будет разработана с использованием модели «Как должно быть»(рис. 1.8), которая представляет процесс работы системы мониторинга ЛВС, а также показывает все действующие лица и звенья, которые задействованы в данном процессе.

В ходе работы была проведена декомпозиция модели «Как должно быть» с позиции пользователя системы мониторинга ЛВС, потому что главным актёром, задействованным в работе с системой, является системный администратор. Декомпозиция позволит сделать вывод о том, как необходимо смоделировать архитектуру системы. Диаграмма декомпозиции представлена на рисунке 9.

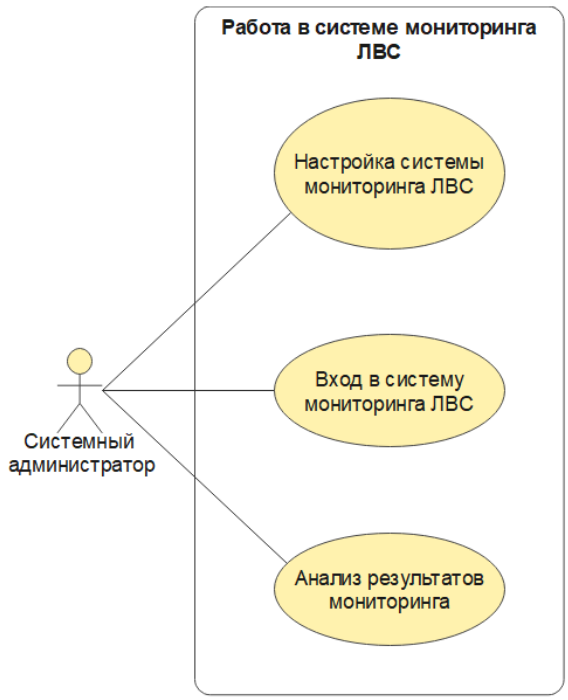

Рисунок 9 – Диаграмма декомпозиции модели «Как должно быть»

Описание прецендентов модели «Как должно быть» представлено в таблице 6.

Таблица 6 – Описание прецендентов

Описание прецендента «Настройка системы мониторинга ЛВС»	
Основной поток: 1. Открыть раздел с настройками системы мониторинга ЛВС. 2. Внести настройки в конфигурацию системы мониторинга ЛВС. 3. Сохранить настройки.	Альтернативный поток: *A1 Если необходимо отредактировать внесённые настройки* 1. Отобразить раздел с настройками системы мониторинга ЛВС. 2. Применить настройки.
Описание прецендента «Вход в систему мониторинга ЛВС»	
Основной поток: 1. Ввести адрес панели управления системой мониторинга ЛВС в браузере. 2. Ввести логин и пароль для входа в панель мониторинга. 3. Успешно войти в панель управления системой мониторинга ЛВС.	Альтернативный поток: *A1 Если введены неверные учётные данные* 1. Ввести адрес панели управления системой мониторинга ЛВС в браузере. 2. Ввести неверные учётные данные. 3. Получить сообщение о том, что введены неверные учётные данные.

Продолжение таблицы 6

Описание прецендента «Анализ результатов мониторинга»	
Основной поток: 1. Открыть раздел с отчётами. 2. Просмотреть отчёты.	Альтернативный поток: *A1 Если необходимо принять решение об исправности ЛВС и отдельных узлов* 1. Отобразить раздел с отчётами. 2. Просмотреть отчёты. 3. Просмотреть сообщение о наличии/отсутствии неполадок.

В приложении А на рисунке А.1 представлена диаграмма последовательности бизнес-процесса «Работа в системе мониторинга ЛВС». Диаграммапоследовательностинаглядно демонстрирует логическую цепочку работы системы мониторинга ЛВС и описывает последовательность выполнения операций. Главным действующим лицом в ходе выполнения процесса «Работа в системе мониторинга ЛВС»является системный администратор,который взаимодействует с системой мониторинга ЛВС через веб-интерфейс в браузере, атакже получаетоповещения впроцессе работы системы мониторинга ЛВС. Система мониторинга ЛВС взаимодействует с системным администратором,обрабатывая заданные им данные, отправляяему оповещения и отрисовывая веб-интерфейс для управления системой мониторинга ЛВС и просмотра результатов мониторинга через браузер.Оповещения системы мониторинга ЛВС могут содержать описание инцидентов в контролируемой сетевой инфраструктуре. Процесс завершается анализом полученных оповещений,принятием решения и устранением проблемы.

Таким образом, можно сделать вывод о функциональных особенностях, а также о том, что проектируемая система мониторинга ЛВС позволит автоматизировать процесс мониторинга сети.

2.3 Моделирование архитектуры проектируемой системы мониторинга ЛВС

При развёртывании системы мониторинга необходимо учитывать размер контролируемой сети и соответственно выбрать подходящую архитектуру. Сегодня чаще всего используются две архитектуры систем мониторинга – централизованная (сервер-клиент) и распределённая (сервер-прокси-клиент) [5].

В централизованном решении для всех компонентов системы мониторинга используется только один сервер.При этом данный сервер оценивает полученные данные, реагирует на инциденты и представляет выходную информацию с помощью графического интерфейса. Централизованная система мониторинга подходит для небольших предприятий, где ЛВС сравнительно простая, а контролируемых устройств сравнительно мало.

В распределённом решении применяются прокси-серверы, задачей которых является сбор данных и их последующая отправка на центральный сервер. Распределенное решение снижает нагрузку на центральный сервер. При выходе из строя одного из распределённых серверов остальная часть системы работает без сбоев.Распределённые серверы могут использовать простые системы баз данных, а центральный сервер, где хранятся все данные, может использовать надёжную систему баз данных, такую как Oracle или PostgreSQL. Распределённая архитектура подходит для средних и крупномасштабных сетевых инфраструктур.

Для реализации системы мониторинга ЛВС в администрации Озёрского муниципального округа была выбрана централизованная архитектура, которая наглядно представлена на рисунке 10.

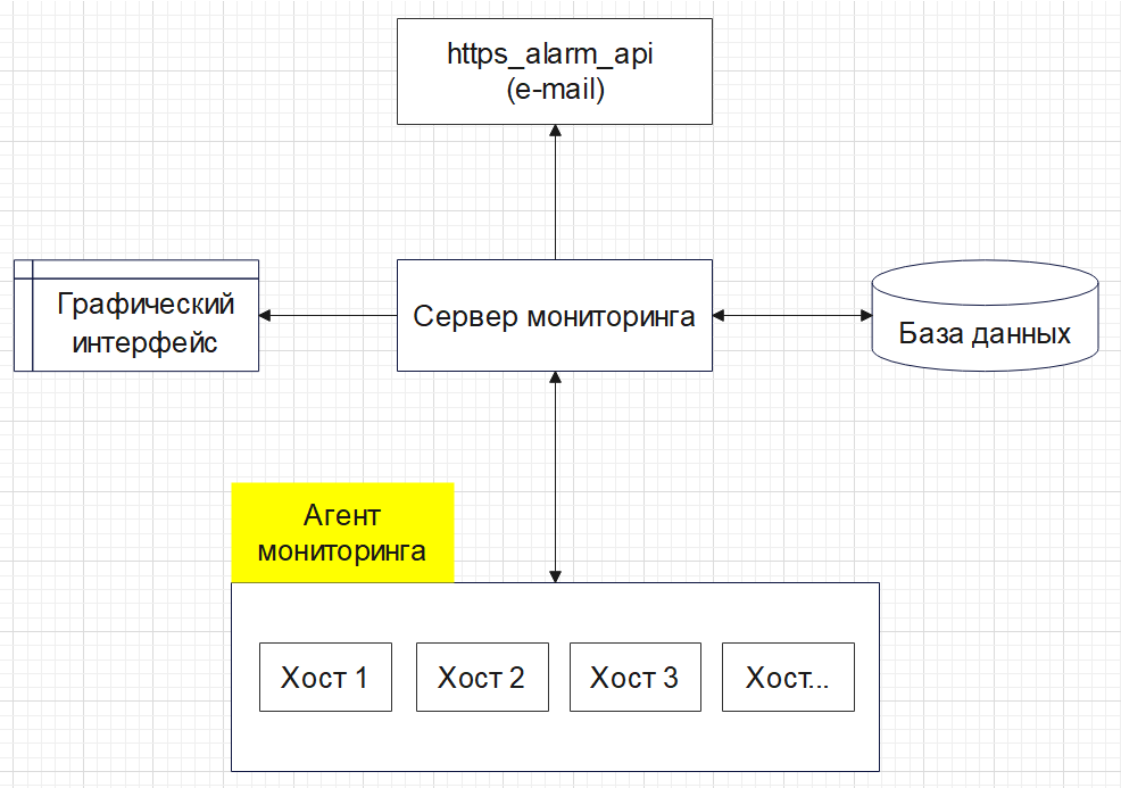

Рисунок 10– Архитектура системы мониторинга ЛВС

С точки зрения пользователя система мониторинга ЛВС делится на пять частей:

– сервер мониторинга, который размещён на физической машине;

– база данных, в которой хранится вся информация о конфигурации и данные, собранные системой мониторинга;

– графический интерфейс, который выводит информацию с сервера мониторинга на рабочую станцию сотрудника;

– агент мониторинга – специальное приложение, которое развёртывается на цели мониторинга. Агент запускается на отслеживаемом устройстве как процесс и постоянно собирает информацию о работе устройства. Агент регулярно передаёт эту информацию в систему мониторинга. Помимо сбора данных, агент может выполнять действия по автоматическому исправлению обнаруженных проблем, в том числе перезапускать зависшие службы. Объем информации, которую может

собрать агент, зависит от конкретной системы мониторинга, а также от операционной системы, на которой он работает. Именно при мониторинге с помощью агента можно получить наибольшее количество информации, а именно: загруженность ЦП, наличие свободного места в ОЗУ и дисковой памяти, состояние операционной системы и прикладных программ, состояние сети;

– система оповещений «https_alarm_api», которая выполняется на сервере мониторинга и по электронной почте предупреждает овозникновении ситуаций, требующих вмешательства системного администратора.

Следовательно, для работы проектируемой системы мониторинга ЛВС требуются следующие компоненты:

– физический сервер с предустановленным необходимым программным обеспечением и настроенным окружением;

– рабочая станция с предустановленным необходимым программным обеспечением.

Таким образом, была построена модель архитектуры системы мониторинга ЛВС и определены компоненты, необходимые для работы системы.

2.4 Проектирование БД системы мониторинга ЛВС

В проектируемой системе мониторинга ЛВС будет использоваться готовая к работе БД, поэтому проектирование логической и физической модели БД не требуется. Диаграмма логической модели данной БД представлена в приложении Б на рисунке Б.1. Модель БД была сформирована в нотации IDEF1X при помощи функции Reverse Engineering в программе MySQL Workbench 8.0 [20].

Ниже перечислены основные сущности БД:

roles – роли пользователей;

– users – пользователи;

– host_inventory – инвентарные данные сетевых устройств;

– host-groups – устройства в сети, которые необходимо мониторить;

– config – настройки системы мониторинга ЛВС;

– dashboard – панель управления системой мониторинга ЛВС;

– alerts – оповещения;

– service_status – состояние служб;

– triggers – оценка и отражение состояния узлов в сети на основе триггеров;

– mapping – карта сети;

– problem –описание возникшей проблемы;

– report – обзор собранных данных;

– interface_snmp – интерфейс SNMP;

– escalations – пользовательские скрипты для отправки оповещений;

– sla – мониторинг услуг;

– operations – добавление, удаление, активация, деактивация узлов.

Таким образом, были выделены основные сущности БД проектируемой системы.

2.5 Требования к аппаратно-программному обеспечению системы мониторинга ЛВС

Чтобы разрабатываемая система мониторинга ЛВС работала результативно и производительно, имеющееся в организации аппаратное оборудование и программное обеспечение должно отвечать определённым техническим условиям.

Аппаратно-программные средства должны удовлетворять следующим требованиям: клиентский компьютер: ОС – Windows 8.1 (или выше), либо

GNU/Linux; ЦП – двухъядерный с тактовой частотой не менее 2 ГГц; ОЗУ – 8 ГБ и больше; свободное место на диске – 5 ГБ и больше; веб-браузер – MozillaFirefox, Opera, Google Chrome или Яндекс.Браузер с включённым JavaScript.

Сервер системы мониторинга: непрерывная работа; GNU/Linux; ЦП – IntelXeonE5-2620 2 ГГцилиновее; ОЗУ – 8 ГБ и больше; дисковая подсистема – от 120 ГБ.

Основное требование к защите системы мониторинга: возможность определения ролей, действующих в системе мониторинга (администратор, супер-администратор, пользователь и т.д.). Анализ требований к аппаратно-программному обеспечению показал, что имеющиеся в организации технические и программные средства пригодны для нормальной и бесперебойной работы проектируемой системы мониторинга ЛВС. Тем самым, были рассмотрены и обозначены требования к аппаратно-программному обеспечению и требования к безопасности системы мониторинга ЛВС.

Выводы по главе 2

Во второй главе выполненологическое проектирование системы мониторинга ЛВС. Длямоделирования логики использовалась нотация UML, также была задействована модель бизнес-процесса «Как должно быть».Былапостроена диаграмма вариантов использования и диаграмма деятельности, на которой были описаны операции и последовательность их выполнения. Была выбрана и смоделирована архитектура проектируемойсистемы мониторинга ЛВС,на которой были описаны основные узлы.

В пункте «Проектирование БД системы мониторинга ЛВС» были выделены основные сущности БД проектируемой системы. В пункте 2.5 были изложены требования к техническим и программным средствам, обозначены требования к защите проектируемой системы мониторинга ЛВС.

Глава 3 Физическое проектирование системы мониторинга ЛВС

3.1 Выбор технологии реализации системы мониторинга ЛВС

3.1.1 Выбор технологии реализации серверной и клиентской части

Серверная часть выбранной системы мониторинга на основе программы Zabbix будет реализована с использованием следующих компонентов:

– PHP (англ. PHP: HypertextPreprocessor) – сценарныйязык, предназначенныйдля программирования динамических веб-приложений. Однако его также можно использовать для программирования настольных приложений. PHP – это одна из серверных технологий, в которых выполняются сценарии, а результирующая страница, написанная на HTML (или JavaScript), передается на клиентскую сторону.Исходный код страницы содержит основные теги HTML и код PHP, заключенный между тегами <?phpa ?>. PHPработает в любой операционной системе, имеет простой синтаксис и является одним из самых используемых сценарных языков программирования [2].PHPбудет обеспечивать работу веб-интерфейса (панели управления) в реализуемой системе мониторинга ЛВС. Для работы PHP требуется веб-сервер;

– Nginx – веб-сервер с открытым исходным кодом, рассчитанный на максимальную производительность и стабильность. Помимо возможностей HTTP-сервера, Nginx также может выступать в качестве прокси-сервера для электронной почты (IMAP, POP3 и SMTP), а также обратного прокси-сервера и балансировщика нагрузки для серверов HTTP, TCP и UDP.Nginxподдерживает UNIX-подобные операционные системы и Microsoft Windows. Согласно рейтингу HostAdvice, Nginx является вторым по популярности веб-сервером в мире [1];

– MySQL – СУБД (система управления базами данных) является наиболее широко используемым в мире программным обеспечением баз

данных с открытым исходным кодом, использующим язык запросов SQL или его диалект. Самым большим преимуществом MySQL является её скорость, доступность и простота использования[9]. В реализуемой системе мониторинга ЛВС СУБД будет использоваться для хранения и последующей работы с данными. Данные хранятся в базе данных в виде таблиц, в которых строки соответствуют каждой записи, а столбцы содержат часть записи одного типа (имя, дата и т.д.);

– Ubuntu – один из самых известных и часто используемых домашних и серверных дистрибутивов Linux, который распространяется совершенно бесплатно.Благодаря этому с ним связано большое и активное сообщество пользователей и разработчиков. К самым большим преимуществам Ubuntu можно отнести регулярно выпускаемые обновления.Ubuntu основан на дистрибутиве Debian. Как и Raspberry Pi OS, Ubuntu имеет монолитное ядро. Ubuntu – это дистрибутив, разрабатываемый Canonical и сообществом других разработчиков. Дистрибутив Ubuntuбудет развёрнут на сервере системы мониторинга ЛВС. Данный дистрибутив был выбран потому, что он является одним из самых стабильных и наиболее популярных дистрибутивов Linux[12];

– Zabbix-сервер –центральный компонент системы мониторинга ЛВС, который будет выявлять неполадки в сети сразу после их возникновения и оповещать об этом системного администратора, отслеживать состояние узлов.Zabbix-сервер может визуализировать полученную информацию в виде графиков, контролировать загруженность и производительность сетевых узлов. Zabbix-сервер не требователен к ресурсам аппаратного обеспечения: 2-ядерного процессора и 2 ГБ оперативной памяти (примерно до 500 контролируемых устройств) должно быть достаточно для нужд организации среднего размера. По умолчанию Zabbix-сервер работает на порту 10051. Zabbix-сервер имеет модульную архитектуру, что позволит расширять функциональные возможности

системы мониторинга при помощи плагинов, написанных на языке программирования Go;

– pfSense – бесплатное программное обеспечение, обеспечивающееебазовые функций коммерческих брандмауэров. Брандмауэр pfSense позволяет установить основные правила безопасности для защиты корпоративной сети и перехода в публичную сеть Интернет.Он поддерживает функции VPN (англ. Virtual Private Network, «виртуальная частная сеть») как от клиента к сайту, так и от сайта к сайту.Таким образом, это позволяет соединять несколько филиалов друг с другом с помощью Интернета, где сеть выглядит как единое целое для пользователей, или подключать пользовательские ПК из Интернета к внутренней сети и доступным в ней службам. Почти все настройки брандмауэра производятся через графический интерфейс, доступный через веб-браузер по протоколу HTTP или HTTPS.pfSenseдопускает установку ряда расширений, позволяющих расширить функции брандмауэра, например, прокси-сервером или почтовым шлюзом с возможностью фильтрации спама или писем, содержащих вирусы [18].

Для реализации клиентской части необходимо установить агенты мониторинга на клиентские компьютеры. Данные агенты позволят системе мониторинга ЛВС взаимодействовать с контролируемыми сетевымиузлами. Подробно назначение агентов мониторинга было сформулировано в пункте 2.3. Для контроля доступности устройств, на которые нельзя установить агенты мониторинга (роутеры, маршрутизаторы, сетевые принтеры, источники бесперебойного питания), будет использоваться протокол ICMP (англ. InternetControlMessageProtocol – протокол межсетевых управляющих сообщений) илиSNMP. При использовании ICMP система мониторинга через регулярные интервалы времени отправляет сообщение, на которое ожидает ответа о доступности узла. Если данное сообщение не приходит в указанное время, отслеживаемый узел считается недоступным.SNMP – это протокол для мониторинга состояния устройств в компьютерной сети.Он основан на

модели клиент-сервер. Система мониторинга устанавливает соединение с SNMP-службой, запущенной на контролируемом устройстве.Соединение SNMP является асинхронным, т. е. контролируемое устройство может отправлять информацию об изменении состояния без предварительного запроса этой информации системой мониторинга.

Для доступа к веб-интерфейсу системы мониторинга ЛВС с компьютера системного администратора будет использоваться актуальная версия веб-браузера MozillaFirefox.

3.2 Реализация системы мониторинга ЛВС

Для нужд тестирования разрабатываемой системы мониторинга ЛВС будет построена виртуальная тестовая среда, имитирующая работу сети вымышленной организации среднего размера.

3.2.1 Описание виртуальной среды для тестирования системы мониторинга ЛВС

Отдельные компоненты, участвующие в виртуальной тестовой среде, показаны на рисунке11.

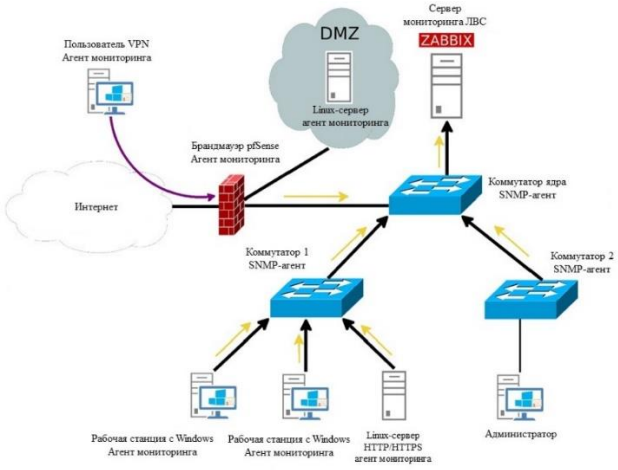

Рисунок11 – Компоненты виртуальной тестовой среды для мониторинга ЛВС

Данная сеть будет содержать:

– рабочие станции с операционной системой Windows;

– Linux-сервер, предоставляющий службу веб-сервера для внутренней информационной системы;

– три коммутатора;

– Linux-серверс установленной и сконфигурированной системой мониторинга ЛВС;

– брандмауэр, отделяющий локальную сеть от внешней сети Интернет и DMZ (англ. Demilitarized Zone – демилитаризованная зона).

Демилитаризованная зона будет содержать сервер, предлагающий сервисы, доступные как из Интернета, так и из внутренней локальной сети.На брандмауэре будет установлена служба VPN, которая позволит сотрудникам подключаться к предопределенным службам ЛВС и DMZ через Интернет.

3.2.2 Описание основных модулей выбранной системы мониторинга ЛВС

Система мониторинга Zabbix может получать информацию о состоянии рабочих станций пользователей с помощью установленного в операционной системе агента, который получает информацию о состоянии и работе данных рабочих станций. Например, Zabbix может получить информацию об использовании ресурсов ЦП, заполненности жёсткого диска или пропускной способности сетевой карты.При подключении внешних сотрудников с использованием VPN-доступа также будет возможен мониторинг за их рабочими станциями.

На Linux-серверы, расположенные как в локальной сети, так и в сети DMZ, будут установлены агенты, поэтому будет доступна подробная информация о нагрузке на сервер и его работе. Также будет возможным отслеживание состояния выбранных серверных служб. Брандмауэр pfSense построен на платформе FreeBSD. Мониторинг брандмауэра при помощи Zabbix будет осуществляться посредством протокола SNMP.

Коммутаторы локальной сети можно контролировать с помощью SNMP. Наблюдение за виртуальными коммутаторами виртуальной тестовой среды является невозможным, поэтому мониторинг коммутатора будет протестирован с конкретным аппаратным коммутатором.

Брандмауэр pfSense будет физически разделятьЛВС, сеть Интернет и DMZ, весь трафик между данными сетями будет проходить через брандмауэр и фильтроваться в соответствии с предопределенными политиками безопасности.Вся информация о прохождении данных через брандмауэр будет отслеживаться, при этом будет возможность для дальнейшей обработки информации.Брандмауэр также позволит распознавать тип трафика отдельных пользователей с идентификацией типа приложения (браузер, клиент электронной почты, мессенджер и т.д.).В случае интернет-трафика также будет возможным получение информации о том, с каким интернет-ресурсом работал конкретный пользователь («ВКонтакте», «Одноклассники» и т.д.). Таким образом, из выходных данных брандмауэра можно будет получить информацию о сетевом трафике конкретного пользователя.

3.2.3 Установка программы Zabbix

Чтобы внедрить выбранное решение для мониторинга ЛВС, сначала необходимо выбрать платформу операционной системы и приложения базы данных. Как уже было отмечено в пункте 3.1.1, среда операционной системы Linux наиболее подходит для нужд данного проекта. Был выбран дистрибутив Ubuntu 20.04, куда можно установить всё приложение целиком, включая необходимые компоненты из инсталляционных пакетов дистрибутива.

Первым шагом установки являетсяподключение репозитория Zabbix и обновление диспетчера пакетов с помощью команды, показанной на рисунке 12.

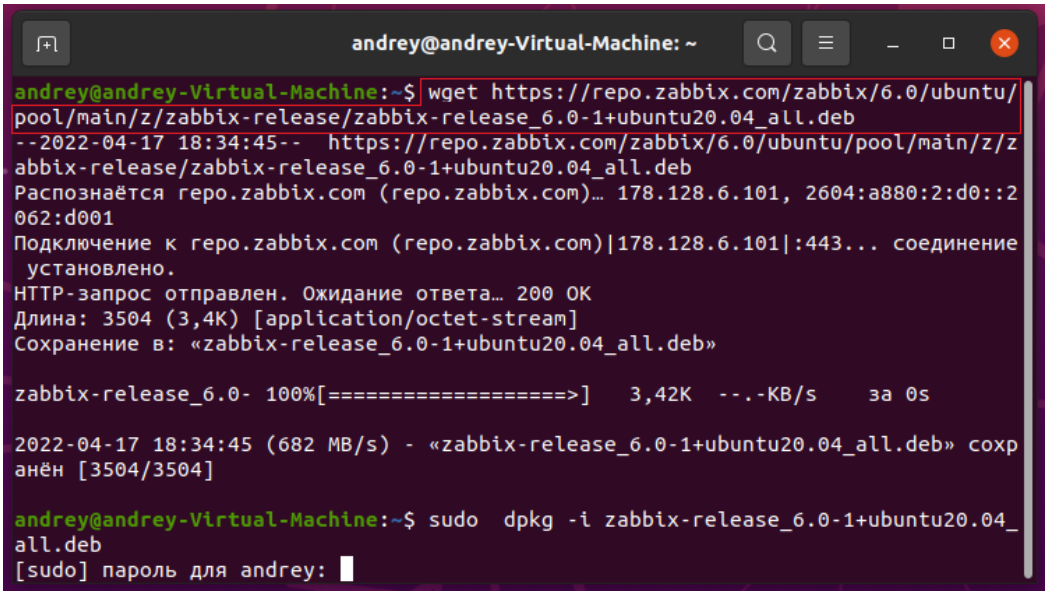

Рисунок 12 – Подключение репозитория Zabbix в среде операционной системы Ubuntu

Поскольку для хранения данных требуется внешняя база данных, то следующим шагом является установка одной из поддерживаемых СУБД.Zabbixподдерживает базы данных MySQL, PostgreSQL, Oracle и SQLite. В соответствии с рекомендациями официальной документации, была выбрана база данных MySQL. Также желательно установить phpMyAdmin – веб-интерфейс, который обеспечит более удобное администрирование базы данных. На рисунке 13 представлена команда для установки MySQL и phpMyAdmin.

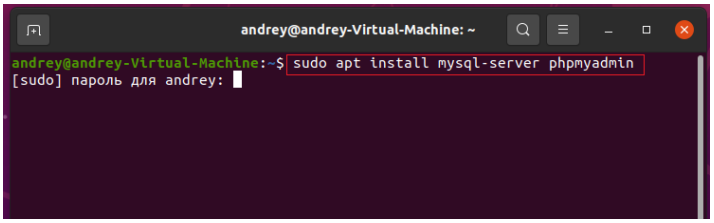

Рисунок 13 – Установка MySQL и phpMyAdmin в среде операционной системы Ubuntu

Теперь сервер готов к установке самого Zabbix-сервера и веб-сервера Nginx. Команда для установки представлена на рисунке 14.

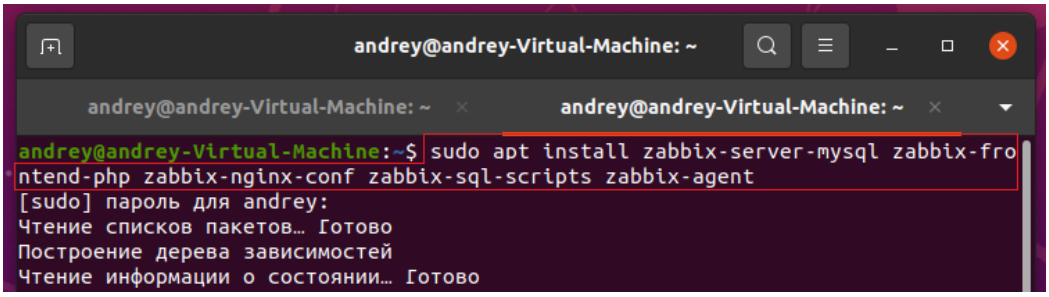

Рисунок 14 – Установка Zabbix-сервера и Nginx в среде операционной системы Ubuntu

После завершения установки необходимо подготовить базу данных, это можно сделать в среде приложения phpMyAdmin. Для базы данных должна быть установлена кодировка UTF8. Также необходимо внести изменения в предустановленные значения настроек веб-сервера Nginx.В частности, в конфигурационном файле /etc/zabbix/nginx.conf в директиве server_name необходимо прописать IP-адрес системы мониторинга, а затем перезапустить службу веб-сервера командой sudosystemctlrestartnginx.Теперь система мониторинга доступна через веб-браузер по адресуhttp://ip_сервера/zabbix.

Далее необходимо завершить установку в среде веб-браузера (рисунок 15). В несколько шагов проверяется правильность настроек всех необходимых сервисов и их версий, устанавливаются разрешения на доступ к базе данных и порту, и адрес для доступа.После этого можно войти в систему мониторинга, используя имя пользователя и пароль по умолчанию.

По умолчанию подключение к системе мониторинга ЛВС осуществляется по протоколу HTTP. Данный способ небезопасен из возможности перехвата отправляемых данных (пароль, логин администратора и т.д.), поэтому целесообразно изменить предопределённую настройку на работу по HTTPS-соединению, по которому данные будут шифроваться с помощью закрытого и открытого ключей перед отправкой пользовательских данных.

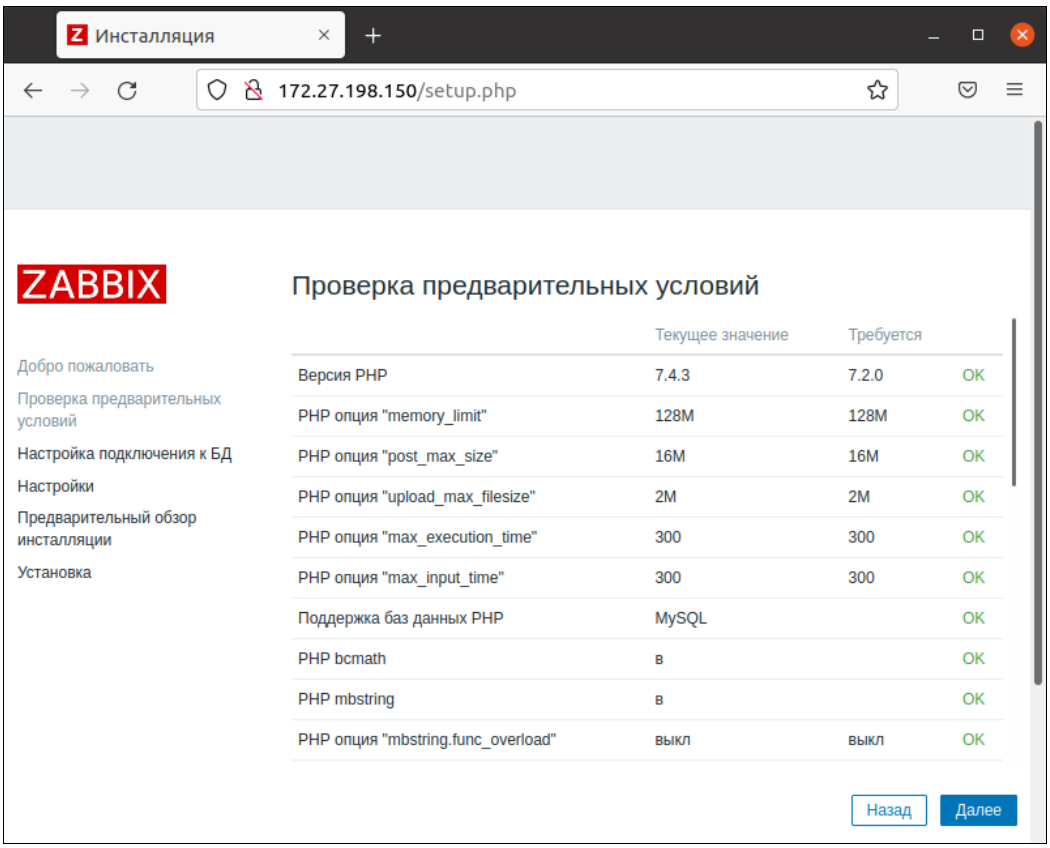

Рисунок 15 – Ход установки Zabbix

Для включения оповещений по электронной почте, которые система мониторинга будет автоматически рассылать при обнаружении новых инцидентов, необходимо выполнить установку и базовые настройки соответствующих служб.Zabbix позволяет использовать внешний почтовый сервер или службы, установленные на том же сервере. Чтобы установить службу передачи почты Postfixв среде Ubuntu, можно использовать консольную команду sudoapt install postfix (рисунок16).

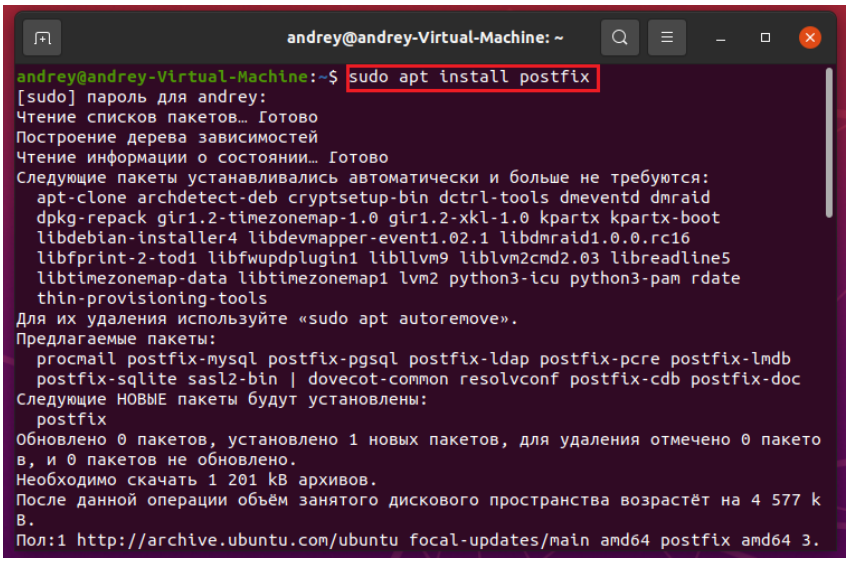

Рисунок 16 – Установка почтовой службы Postfix

После завершения установки необходимо настроить систему мониторинга для использования этой службы.Необходимо задать адрес сервера, значение SMTP helo и адрес, с которого будет уходить сообщение.Эти значения задаются через графический интерфейс системы мониторинга в меню «Администрирование» - «Способы оповещения» - «Email» (рисунок17).

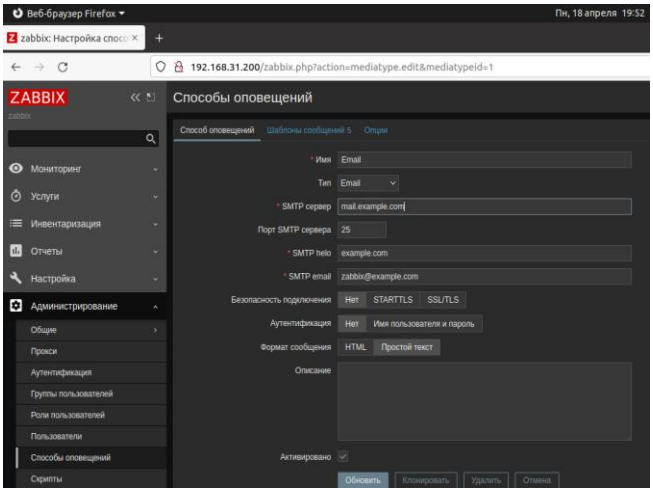

Рисунок 17 – Настройка оповещений системы мониторинга ЛВС по электронной почте

Таким образом, в данном пункте была описана тестовая виртуальная среда для реализации системы мониторинга ЛВС. Была произведена установка и настройка программы Zabbix, которая представляет собой основу реализуемой системы мониторинга ЛВС.

3.3 Установка брандмауэра pfSense

Установка брандмауэра pfSense осуществляется при помощи загрузочного диска, созданного на основе операционной системы FreeBSD (рисунок 18). После запуска загрузочного диска брандмауэр можно установить на жёсткий диск. Программа установки запускается в текстовой консоли и требует ввода основных параметров брандмауэра, таких как конфигурация сетевого интерфейса.

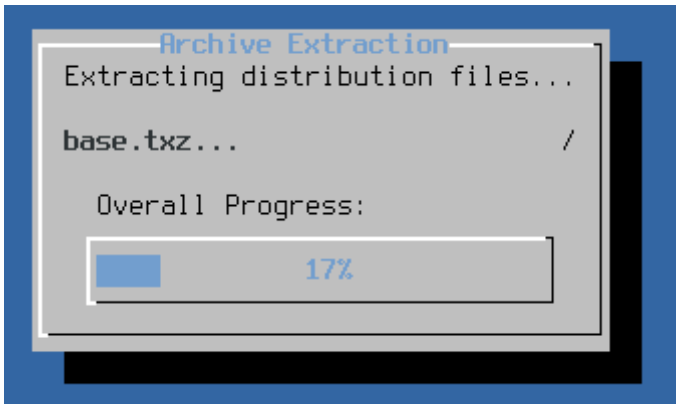

Рисунок 18 – Процесс установки брандмауэра pfSense

Консольный режим после установки позволяет выполнить базовые настройки, в том числе основных политик безопасности брандмауэра, запустить средства диагностики, чтобы убедиться в правильности сетевых параметров или восстановить настройки по умолчанию после системного сбоя. Доступ к консоли также возможен по протоколу SSH.

В целяхбезопасности доступ к настроенной конфигурации брандмауэра должен быть доступен только по защищенному протоколу HTTPS и исключительно из локальной сети с определённых адресованной сети.

Расширение основных функциональных возможностей брандмауэра осуществляется путём установки дополнительных пакетов.Пакеты устанавливаются через веб-интерфейс, в котором также доступны другие функции, в том числе агент системы мониторинга Zabbix (рисунок 19).

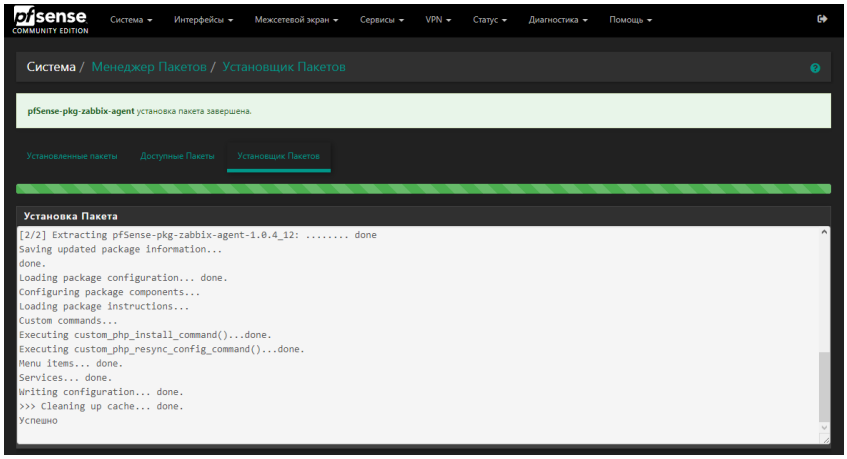

Рисунок 19 – Установка агента мониторинга Zabbix в брандмауэр pfSense

Таким образом, в данном пункте был описан процесс установки межсетевого экрана pfSense, являющегося одним из компонентов, необходимых для реализации системы мониторинга ЛВС.

3.4 Установка, конфигурирование и настройка агента мониторинга

3.4.1 Установка и конфигурирование агента мониторинга в среде операционной системы Linux

В операционной системе Linuxдля установки агента мониторинга рекомендуется использовать официальные репозитории Zabbix, которые доступны для большинства распространённых Linux-дистрибутивов.

Поскольку для установки программы Zabbixбыл выбран дистрибутив Ubuntu 20.04, ниже будет описана установка агента мониторинга Zabbix для того же дистрибутива. Процесс установки в других дистрибутивах в целом аналогичен.Подробное описание установки для различных дистрибутивов можно найти на официальном сайте программы.

Сначала необходимо добавить репозитории Zabbix и обновить список пакетов, это можно сделать с помощью команд, представленных на рисунке 20.

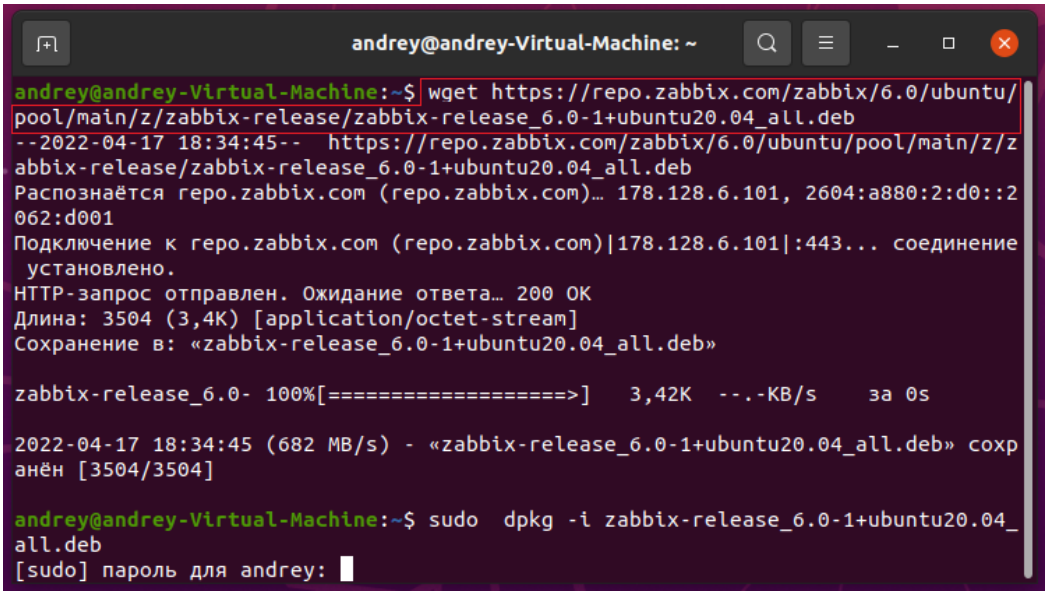

Рисунок 20 – Добавление репозитория Zabbix и обновление списка пакетов

Затем можно установить сам агент мониторинга (рисунок21).

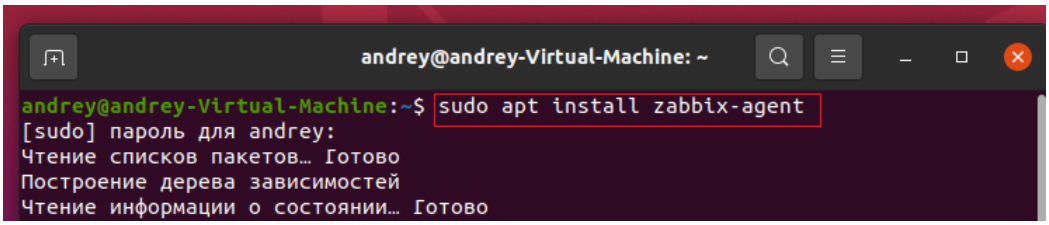

Рисунок 21 – Установка агента мониторинга

Настройка агента мониторинга выполняется путём редактирования конфигурационного файла, который находится в структуре каталогов /etc/zabbix/zabbix_agentd.conf.Агент, работающий в наблюдаемом устройстве, ожидает входящего соединения от сервера мониторинга. Данное соединение принимается только с предопределённых IP-адресов. Разрешенные адреса определяются путём изменения переменной «Server=», где можно ввести несколько адресов, разделённых точкой с запятой.Другим важным параметром файла конфигурации является коммуникационный порт, через который агент мониторинга ожидает входящее TCP-соединение. По умолчанию это порт 10050, который можно изменить на любой другой в диапазоне 1025-32767, изменив параметр «ListenPort=».После изменения конфигурации необходимо перезапустить службу агентас помощью команды, представленной на рисунке 22.

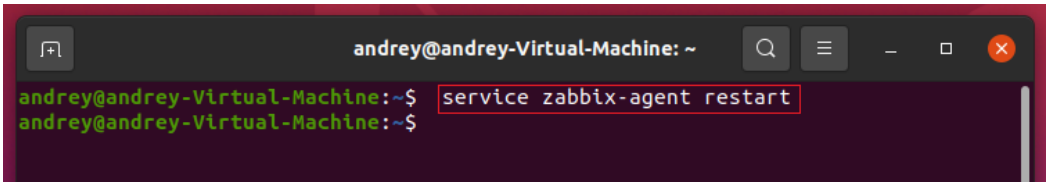

Рисунок 22 – Перезапуск службы агента мониторинга

Чтобы убедиться, что агент работает на нужном порту, необходимо ввести команду, которая представлена на рисунке 23. Данная команда возвращает сетевые интерфейсы и порты, которые прослушивает агент мониторинга.В возвращенном списке на рисунке 23показано, что агент прослушивает все адреса IPv4 и IPv6 на порту по умолчанию 10050.

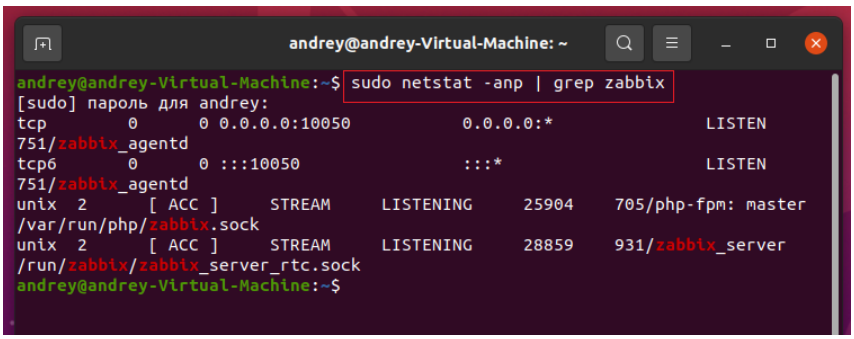

Рисунок 23 – Консольная команда для проверки порта, на котором работает агент мониторинга, и результат выполнения данной команды

Консольная команда для проверки порта дает прекрасный результат

3.4.2 Установка и конфигурация агента мониторинга в среде операционной системы Windows

Агент мониторинга для всех версий операционной системы Windows можно скачать с официального сайта проекта Zabbix. Агент доступен в ZIP-архивах, а также в формате файла-установщика с расширением .msi. При установке агента с использованием msi-файла весь процесс сводится к нажатию кнопки «Next». На одном из этапов установки необходимо указать IP-адрес сервера мониторинга и номер порта (рисунок 24).

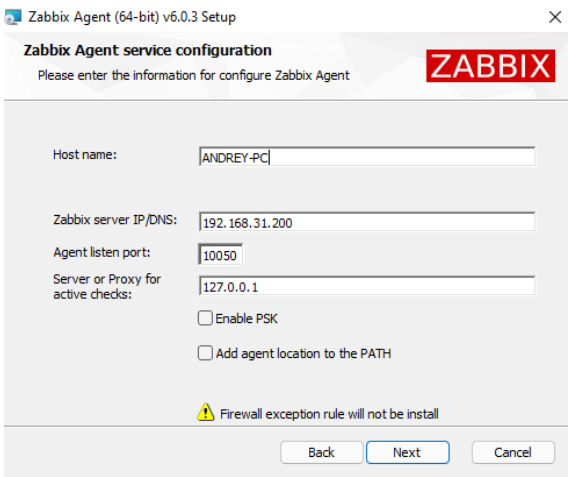

Рисунок 24 – Указание IP-адреса сервера мониторинга и номера порта в процессе установки агента мониторинга в среде Windows

IP-адрес сервера мониторинга и номера порта можно указать позднее путём редактирования конфигурационного файла zabbix_agentd.conf, который по умолчанию находится в каталоге C:\Program Files\Zabbix Agent\zabbix_agentd.conf. В данном файле необходимо изменить основные параметры службы, как было описано в предыдущем пункте, т.е. путём изменения параметров «Server=» и «ListenPort=» (рисунок 25).

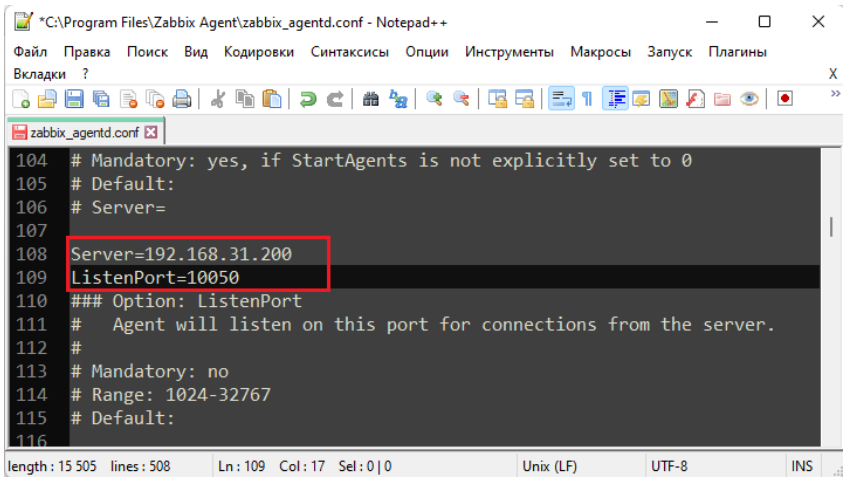

Рисунок 25 – Указание IP-адреса сервера мониторинга и номера порта в конфигурационном файле zabbix_agentd.conf в среде Windows

По завершению установки агент мониторинга будет установлен в качестве службы Windows (рисунок26).

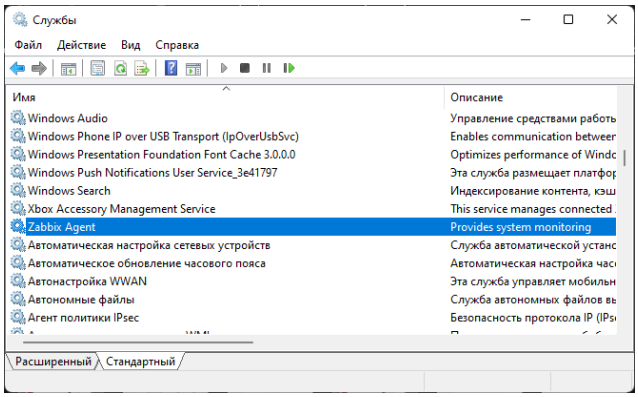

Рисунок 26 – Служба агента мониторинга

Также в брандмауэре Windows необходимо открыть портдля входящих соединений, иначе сервер мониторинга не сможет «достучаться» до агента мониторинга. Сделать это можно с помощью команды, представленной на рисунке 27.

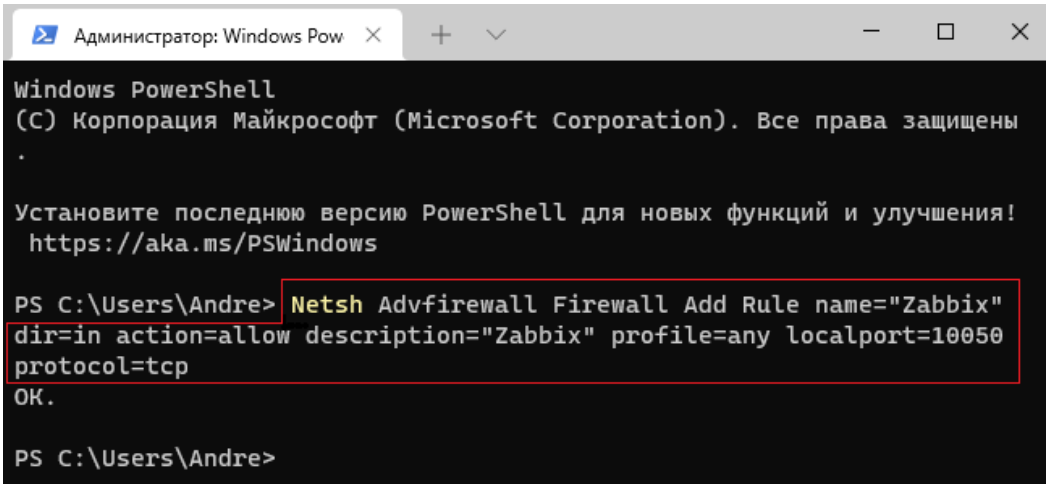

Рисунок 27 – Консольная команда для открытия порта, на котором работает агент мониторинга

В данной команде в параметре «localport=» необходимо указать номер порта, который указан в конфигурационном файле «zabbix_agentd.conf». Как уже было сказано, по умолчанию это 10050.

3.4.3 Настройка агента мониторинга в среде сервера Zabbix

Добавление нового устройства в графическое окружение сервера мониторинга Zabbixосуществляется после авторизации пользователя с достаточными привилегиями. По умолчанию это пользователь admin.

Добавление наблюдаемого устройства выполняется в меню «Настройка» - «Узлы сети», где после нажатия на кнопку «Создать узел сети» вызывается меню добавления наблюдаемого устройства, где необходимо заполнить основные параметры конфигурации агента (рисунок 28). Как минимум должны быть заполнены параметры с именем узла, под которым устройство будет в дальнейшем идентифицироваться в системе мониторинга, IP-адрес/DNS-имя контролируемого устройства и

коммуникационный порт.Во вкладке шаблона необходимо выбрать подходящий шаблон для данного устройства. Для ранее установленных агентов это будут шаблоны «LinuxbyZabbixagent» и «WindowsbyZabbixagent». Затем конфигурацию можно сохранить.Если добавление прошло успешно, сигнал тревоги о недоступности агента вновь добавленного устройства должен исчезнуть в течение примерно 1 минуты, после чего начнут отслеживаться параметры добавленного устройства.

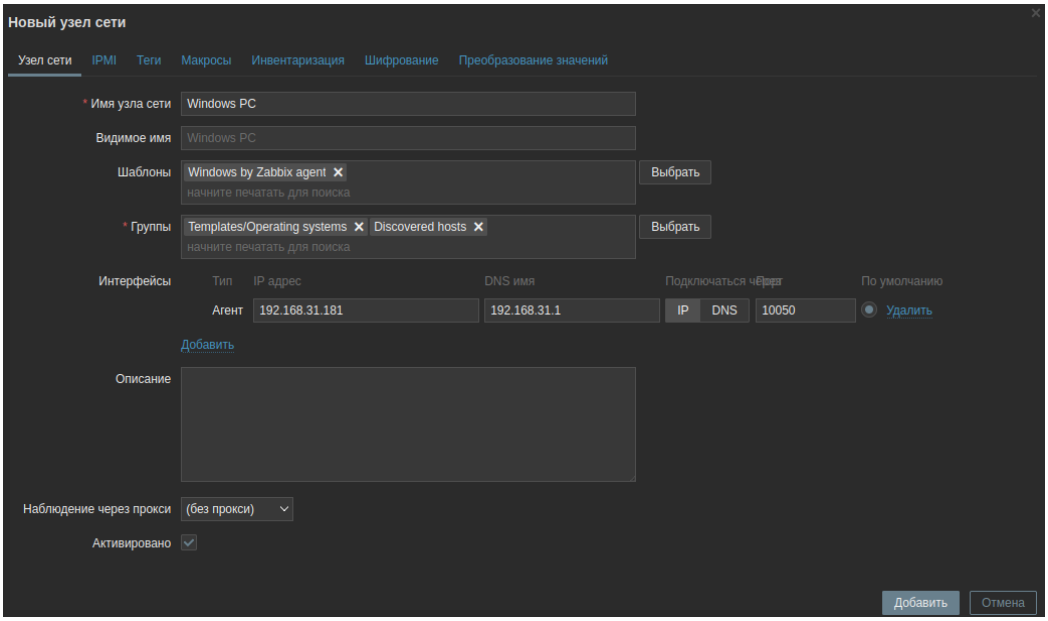

Рисунок 28 – Добавление нового узла сети и настройка параметров агента мониторинга

При необходимости можно изменить конфигурацию некоторых триггеров или полностью отключить данные триггеры. Это следует делать при мониторинге рабочих станций, которые будут часто выключаться или перезапускаться.

Таким образом, в данном пункте был описан процесс установки агентов мониторинга в средах операционных систем Linux и Windows, была произведена настройка агентовмониторинга.

3.5 Настройка мониторинга ICMP/SNMP

Для мониторинга доступности сетевых устройств целесообразно использовать протокол SNMP или ICMP PING. Для простых коммутаторов без поддержки SNMP необходимо использовать ICMP PING, для устройств с поддержкой SNMP можно использовать данный протокол для обеспечения более детального мониторинга.

Как для ICMP PING, так и для мониторинга базовой информации об устройствах с поддержкой SNMP можно использовать предварительно настроенные шаблоны.Для отслеживания подробной информации необходимо создать новый шаблон. Добавление цели мониторинга осуществляется в веб-интерфейсе системы мониторинга ЛВС в меню «Настройки» - «Узлысети», где необходимо заполнить имя хоста, IP-адрес и выбрать соответствующий шаблон (рисунок 29).

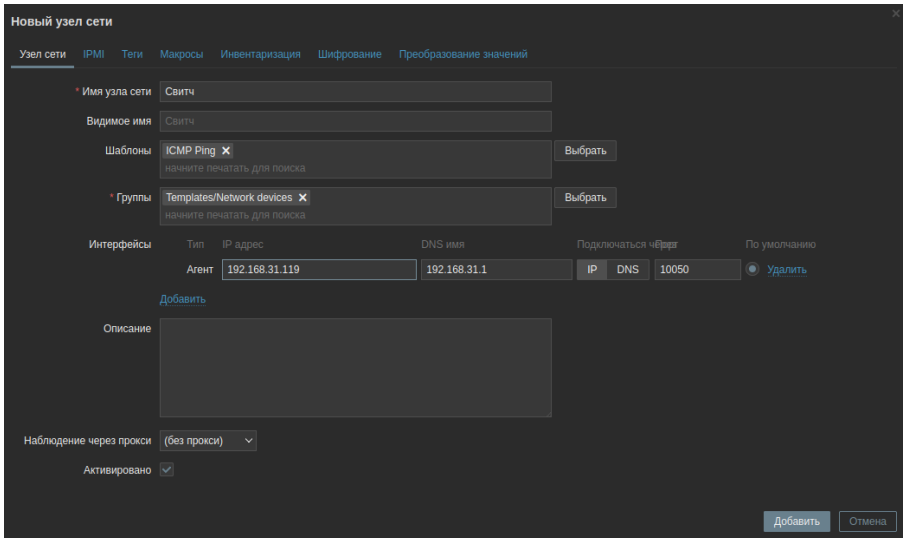

Рисунок 29 – Добавление нового узла сети и настройка мониторинга ICMP PING

Таким образом, была произведена настройка мониторинга посредством инструмента ICMP PING.

3.6 Настройка графического отображения контролируемых устройств

В среде системы мониторинга ЛВС можно настроить карту сети. Карта содержит значки, представляющие отдельные устройства наблюдаемой сети, включая представление об их взаимосвязи.Отдельные значки могут содержать текстовую информацию о состоянии устройства.Преимуществом такого отображения является информация о логической целостности контролируемой сети. Это очень полезно, например, в случае отказа коммутатора, когда система мониторинга обнаруживает не только отказ коммутатора, но и всех контролируемых устройств, подключенных за данным коммутатором.Система мониторинга ЛВС генерирует большое количество инцидентов, которые могут запутать пользователя без знания сетевой инфраструктуры, что может привести к неправильной оценке ситуации. Отображение сетевой инфраструктуры на карте во многом снимает эту проблему.

Карта контролируемой ЛВС в Zabbix, реализованная для нужд данного проекта, представлена на рисунке 30.

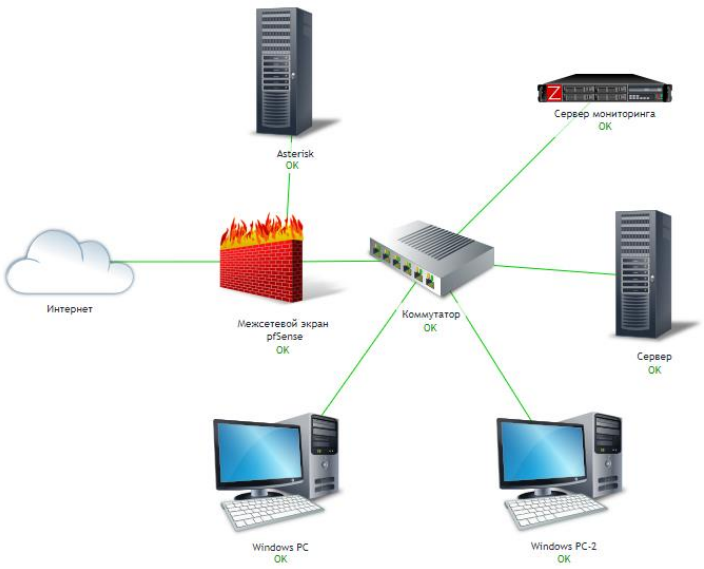

Рисунок 30 – Карта наблюдаемойЛВС

Редактирование или создание карт осуществляется в меню «Мониторинг» - «Карты сетей». При создании новой карты необходимо задать её размер в пикселях, данную информацию потом можно изменить в любой момент.После создания новой карты нажатием на значок «Создать карту сети» можно вставлять или удалять значки на карте сети помощью ссылки «Добавить/Удалить».Значок обозначает устройство или элемент наблюдаемой сети.Значок может содержать ссылку на другую карту.Тип значка необходимо выбрать в параметре «Тип».После выбора двух значков можно добавить или удалить связь между данными элементами, щёлкнув ссылку «Связь: Добавить/Удалить». Можно изменить цвет и тип линии коннектора.

3.7 Тестирование реализованной системы мониторинга ЛВС

В следующем пункте будет протестирована реализованная система мониторинга ЛВС. Для тестирования будет смоделирован трафик внутри корпоративной сети и искусственно спровоцированы инциденты.

3.7.1 Моделирование действий пользователей и недоступности устройств в тестовой сети

Моделирование действий пользователя будет выполняться на виртуальном компьютере с операционной системой Windows путём запуска приложений офисного пакета, браузера и передачи больших объёмов данных по локальной и глобальной сетям.

После начала первых испытаний очень быстро последовала первая реакция системы мониторинга ЛВС с предупреждением о высокой загрузке ЦП на наблюдаемой рабочей станции (рисунок31).Высокая загрузка ЦП определялась путём установки минимальных пороговых значений производительности для виртуальной тестовой среды.

После загрузки большого количества данных на жёсткий диск, где ёмкость диска была использована более чем на 50% от доступного размера,

система мониторинга выдала ещё один инцидент, информирующий администратора о данной проблеме (рисунок 32).

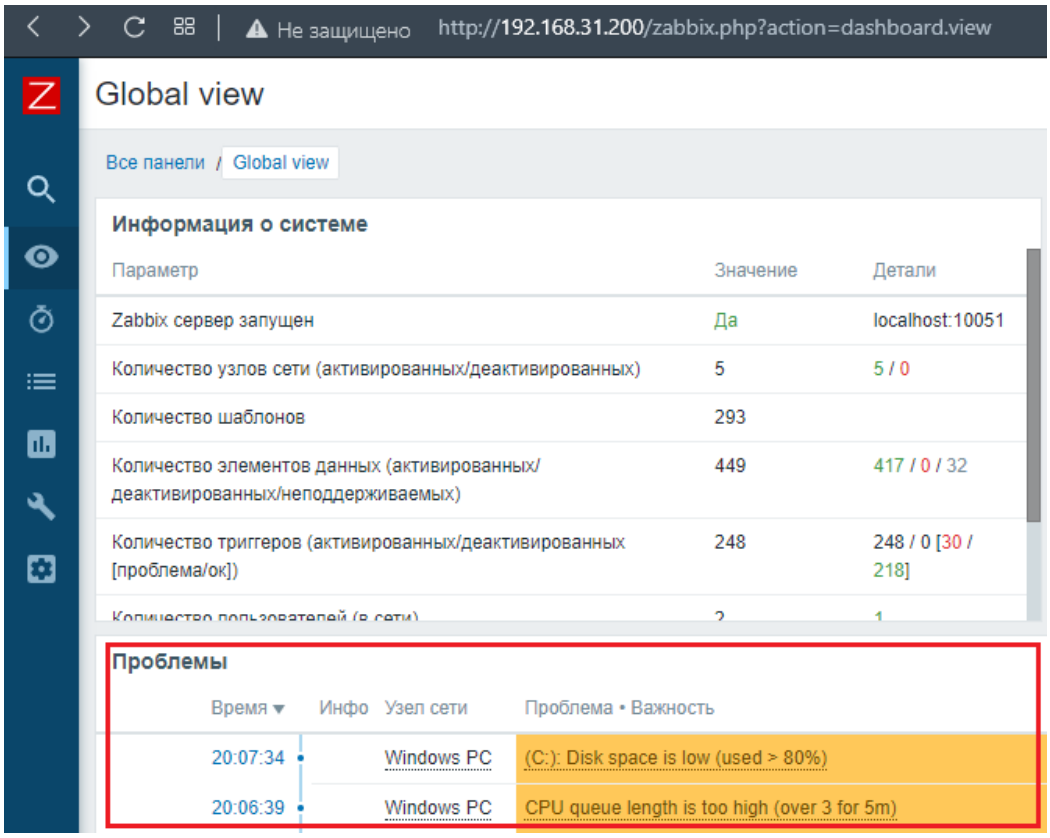

Рисунок 31 – Оповещение о высокой нагрузке на ЦП и чрезмерно высоком уровне занятости диска на одном из компьютеров в ЛВС

После перевода одного из устройств сети в состояние недоступности, система мониторинга незамедлительно предупредила о данном факте (рисунок 32). Имитация недоступности производилась путём выключения данного устройства.

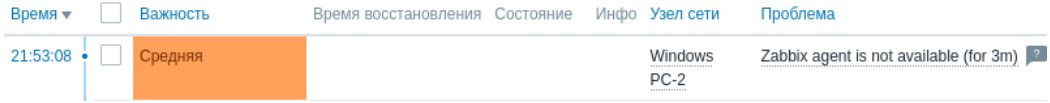

Рисунок 32 – Оповещение о недоступности одного из компьютеров в ЛВС

Передаваемые данные по локальной и глобальной сетям отображаются на графике пропускной способности сетевой карты (рисунок 33).

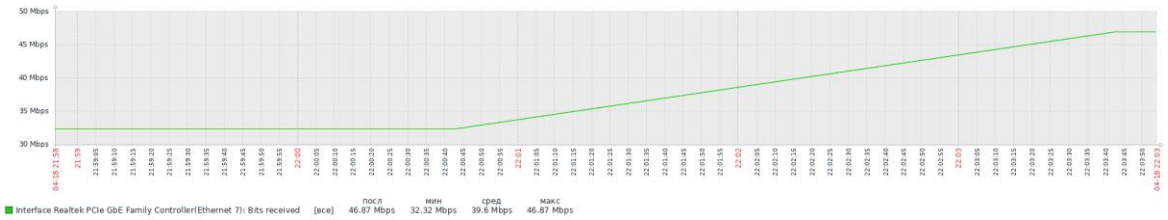

Рисунок 33 – График изменения пропускной способности сетевой карты

Трафик в глобальную сеть, проходящий через брандмауэр, можно более подробно отслеживать в интерфейсе pfSense (рисунок34).

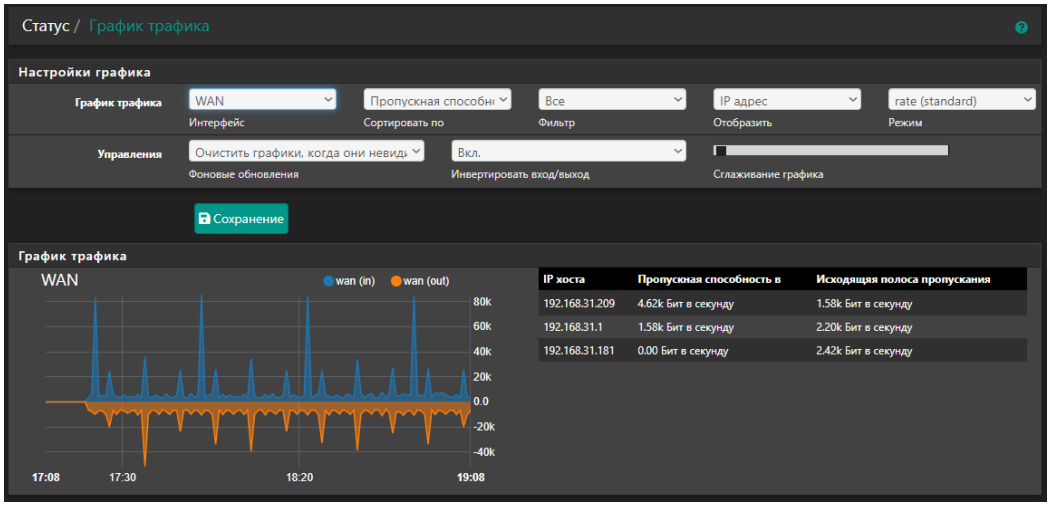

Рисунок 34 – График трафика в брандмауэре pfSense

Также в интерфейсе брандмауэра можно получить сведения о разрешённом и несанкционированном трафике отдельно взятого пользователя в направлении глобальной сети и DMZ.

3.7.2 Измерение значений нагрузки на систему мониторинга

Описанная выше тестовая система была установлена в виртуальной среде, где система мониторинга ЛВС была установлена на виртуальный ПК с

одним виртуальным процессором с ограничением по частоте 1.5 ГГц и 1.5 ГБ ОЗУ. Осуществлялся мониторинг 5 ПК, на которых был установлен агент мониторинга и одного сетевого элемента по протоколу ICMP. Мониторинг ICMP также использовался для мониторинга наличия подключений к общедоступной сети Интернет по 5 IP-адресам. Рекомендуемая конфигурация аппаратного обеспечения в зависимости от количества контролируемых устройств представлена в таблице 7.

Таблица 7– Рекомендуемая аппаратная конфигурация системы мониторинга ЛВС на основе программы Zabbix

Операционная система	ЦП/ОЗУ	База данных	Количество контролируемых устройств
CentOS	Виртуальная машина	MySQL InnoDB	100
CentOS	2 ядра/2 ГБ	MySQL InnoDB	500
RedHat Enterprise Linux	4ядра/8 ГБ	RAID10 MySQL InnoDBИли PostgreSQL	>1000
RedHat Enterprise Linux	8 ядер/16 ГБ	Быстрый RAID10 MySQL InnoDBИли PostgreSQL	>10000

Во время работы тестовой системы были измерены значения загрузки ЦП (23% в среднем) и занятости ОЗУ (32% в среднем) (рисунок 35).

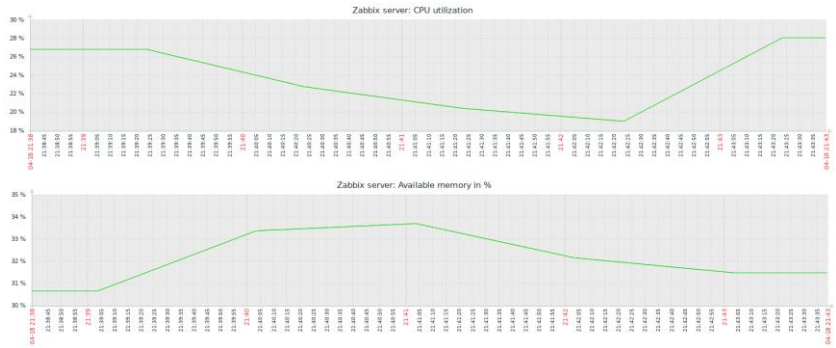

Рисунок 35 – Загруженность ЦП и потребление ОЗУ на сервере мониторинга

Поскольку количество наблюдаемых устройств было небольшим, полученные значения показывают, что виртуальная тестовая средасоответствует требованиям к оборудованию, приведённым в официальной документацииZabbix[21].Для развёртывания решения для нужд компании среднего размера, где есть реальная потребность в мониторинге максимум 100 устройств, подойдёт развёртывание системы мониторинга в среде виртуальной машины с двумявиртуальными процессорами с ограничением по частоте 1 ГГц и 2 ГБ ОЗУ.Эта гипотеза была проверена путём изменения конфигурации тестовой среды, где значение загрузки ЦП снизилось до 10%, а оперативная память была занята на22%.

Таким образом, было произведено успешное тестирование реализованной системы мониторинга ЛВС.

Выводы по главе 3

В третей главе был произведён выбор технологий для реализации серверной и клиентской части системы мониторинга ЛВС. Затем была описана виртуальная тестовая среда, в которой реализовывалась и тестировалась система мониторинга ЛВС. Также были описаны основные компоненты системы мониторинга ЛВС. С использованием данных модулей была реализована система мониторинга ЛВС:

- установлена и настроена программа Zabbix;
- установлен и настроен брандмауэр pfSense;
- установлены и настроены агенты мониторинга в средах операционных систем Linuxи Windows;
- настроен мониторинг ICMP/SNMP;
- настроено графическое отображение наблюдаемой ЛВС.

Затем было произведено тестирование реализованной системы мониторинга ЛВС. Для этого была сымитирована высокая загруженность ЦП и занятость жёсткого диска, а также недоступность устройства в сети. По итогу все тесты были успешно пройдены.

Заключение

Итогом выпускной квалификационной работы является готовая к использованию система мониторинга ЛВС для нужд администрации муниципального образования «Озёрский муниципальный округ Калининградской области», которая может собирать в одном месте статистическую информацию, а также информацию о доступностикомпонентов сетевой инфраструктуры, представлять данную информацию внаглядной форме и уведомлять системных администраторов о любых инцидентах в ЛВС.

В своей работе автор создал понимание того, что такое инструмент мониторинга сети, продемонстрировал преимущества, которые он приносит, и его ключевые компоненты. Для осуществления мониторинга была выбрана программа Zabbix. Однако, прежде чем это было сделано, автор сравнил Zabbix с другими известными системами мониторинга.Основываясь на этих знаниях, было проведено успешное тестирование Zabbix. Несмотря на то, что тестирование проводилось в виртуальной сети небольшого размера, данный метод мониторинга ЛВС может быть легко масштабирован для более крупных сетей.

Благодаря возможностям реализованной системы мониторингаЛВС можно контролировать ИТ-инфраструктуру организации как с точки зрения сети, так и с точки зрения работы приложений, серверов и узлов. В сети можно контролировать работу маршрутизаторов, коммутаторов и мостов. Система мониторинга ЛВС позволяет обнаруживать конфликты и сбои IP-адресов, и графически представлять топологию наблюдаемой сети. В случае с приложениями и серверами можно получать всю необходимую информацию, такую как: загруженность процессора, заполненность дисков и использование ОЗУ.Графики загрузки сети, серверов, состояния отдельных приложений и сетевых узлов отображаются в интерфейсе системы мониторинга.

В ходе выполнения работы автор показал, что хорошая система мониторинга не обязательно должна быть дорогой, а её внедрение сложным и трудоёмким. Реализованная система мониторинга ЛВС полностью бесплатна. Кроме того, она может работать на большинстве операционных систем, включая бесплатные дистрибутивы Linux. Установка и настройка данной системы мониторинга ЛВС настолько просты, что каждый системный администратор сможет сделать это самостоятельно, а в случае возникновения проблем в его распоряжении будет обширная техническая поддержка, подробная документация и множество интернет-форумов, на которых можно обратиться за помощью и советами к другим пользователям подобных систем мониторинга.

Список используемой литературы

1. Глобальный рейтинг веб-серверов на 2022[Электронныйресурс]:HostAdvice.URL: https://ru.hostadvice.com/marketshare/server (дата обращения: 02.04.2022).

2. Зачем изучать PHP: рейтинг, перспективы, сферы применения[Электронныйресурс]: онлайн-школа программирования «Хекслет». URL: https://ru.hexlet.io/blog/posts/zachem-izuchat-php-reyting-perspektivy-sfery-primeneniya (дата обращения: 02.04.2022).

3. Об Уставе муниципального образования «Озёрский муниципальный округ Калининградской области»[Электронный ресурс]: Решение окружного Совета депутатовот 31.08.2021 № 68).URL: https://ozyorsk.ru/svedeniya-o-municzipalnom-obrazovanii/ (дата обращения: 05.03.2022).

4. О назначении должностных лиц, ответственных за техническую защиту информации: постановлении администрации муниципального образования «Озёрский городской округ» [Электронный ресурс]: Постановление администрации Озерского городского округа от 13.09.2019 № 816. URL: https://ozyorsk.ru/wp-content/uploads/2022/03/816.doc (дата обращения: 05.03.2022).

5. Описание серверных ролей[Электронный ресурс]:DEPO Computers. URL:https://www.depo.ru/article_a13155_r991.aspx(дата обращения: 11.03.2022).

6. Обзор возможностей Zabbix[Электронныйресурс]:Zabbix. URL: https://www.zabbix.com/ru/features(дата обращения: 01.04.2022).

7. О структуре администрации муниципального образования «Озёрский городской округ»: [Электронный ресурс]: Решение окружного Совета депутатов от 25.02.2021 № 7.URL: https://ozyorsk.ru/resheniya-soveta-deputatov/ (дата обращения: 05.03.2022).

8. Политика безопасности [Электронный ресурс]: Авторы Википедии //Википедия, свободная энциклопедия.

URL:https://ru.wikipedia.org/wiki/Политика_безопасности (дата обращения: 05.03.2022).

9. Самые популярные базы данных – 2006–2021 гг[Электронныйресурс]: «Хабр».URL: https://habr.com/ru/company/otus/blog/560278/ (дата обращения: 02.04.2022).

10. Самые популярные нотации описания и моделирования бизнес-процессов[Электронный ресурс]: «Организации эффективного управления».URL:https://rzbpm.ru/knowledge/samye-populyarnye-notacii-opisaniya-i-modelirovaniya-biznes-processov.html(дата обращения: 11.03.2022).

11. С.В. Черемных, И.О. Семенов, В.С. Ручкин. Моделирование и анализ систем. IDEF-технологии: практикум. М.:Финансы и статистика. 2006. 192 с.

12. ТОП дистрибутивов Linux 2021[Электронныйресурс]:losst.ru.URL:https://losst.ru/top-distributivov-linux-2021 (дата обращения: 02.04.2022).

13. Фаулер М. UML. Основы. Краткое руководство по стандартному языку объектного моделирования. М.:Символ-Плюс. 2018. 192 с.

14. ШеерА.В.ARIS- моделирование бизнес-процессов.М.:Вильямс, 2009. 224 с.

15. Google[Электронный ресурс]:GoogleTrends.URL: https://trends.google.ru/trends/explore?date=today%205-y&q=zabbix%20monitoring,cacti%20monitoring,nagios%20monitoring (дата обращения: 09.03.2022).

16. MainConfigurationFileOptions [Электронныйресурс]: Nagios. URL:https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/configmain.html (датаобращения: 01.04.2022).

17. MikroTik [Электронный ресурс]: Авторы Википедии //Википедия, свободнаяэнциклопедия. URL: https://ru.wikipedia.org/wiki/MikroTik#RouterOS (дата обращения: 09.03.2022).

18. pfSense Overview [Электронныйресурс]:Netgate. URL: https://www.netgate.com/pfsense-features (дата обращения: 15.04.2022).

19. Requirements [Электронныйресурс]: The Cacti Manual. URL: https://files.cacti.net/docs/html/requirements.html(дата обращения: 01.04.2022).

20. Reverse Engineering a Live Database [Электронныйресурс]:MySQLDeveloper Zone.URL: https://dev.mysql.com/doc/workbench/en/wb-reverse-engineer-live.html (датаобращения: 11.03.2022).

21. ZabbixRequirements[Электронныйресурс]:Zabbix. URL: https://www.zabbix.com/documentation/current/en/manual/installation/requirements (дата обращения: 15.04.2022).

Приложение А

Диаграмма логической модели БД

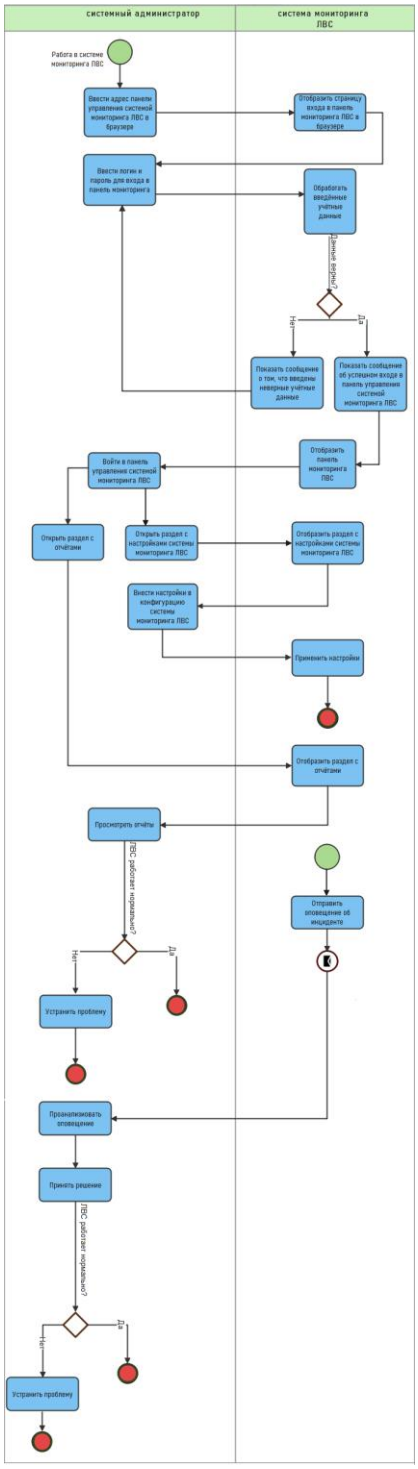

Рисунок А.1 – Диаграмма последовательности бизнес-процесса «Работа в системе мониторинга ЛВС»

Приложение Б

Диаграмма логической модели БД

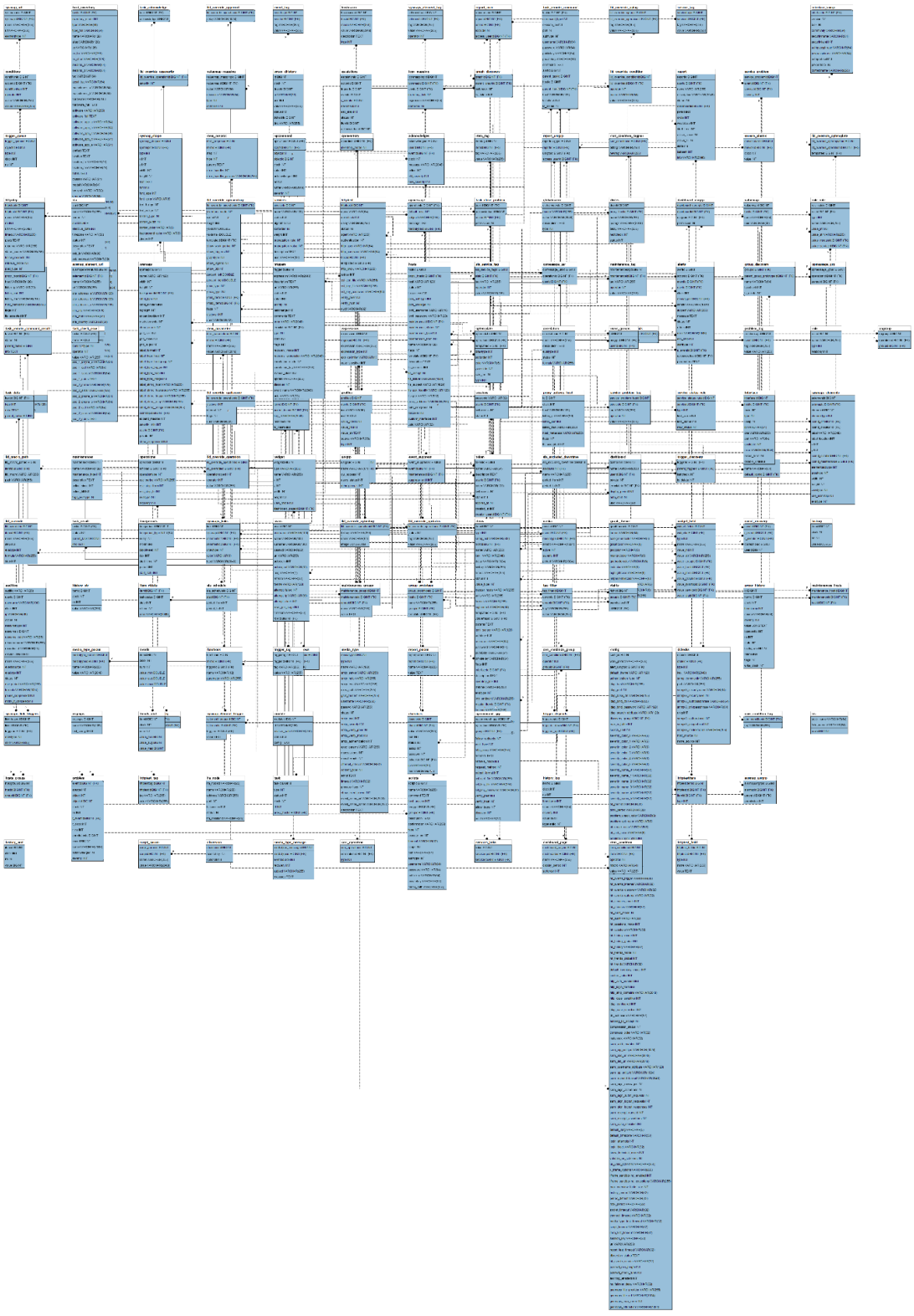

Рисунок Б.1 – Диаграмма логической модели БД