Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем
Направление подготовки 09.03.02 – Информационные системы и технологии
Направленность (профиль) образовательной программы: Безопасность информационных систем

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____ А.В. Бушманов
«_____»_____201_ г.

БАКАЛАВРСКАЯ РАБОТА

на тему: Разработка системы анализа log-файлов серверов в локальной сети предприятия ООО «Компания АЮСС»

Исполнитель
студент группы 355об _____ М.А. Левковец
(подпись, дата)

Руководитель
доцент, канд. техн. наук _____ Н.П. Семичевская
(подпись, дата)

Консультант
по безопасности и экологичности
доцент, канд. техн. наук _____ А.Б. Булгаков
(подпись, дата)

Нормоконтроль
инженер кафедры _____ В.В. Романико
(подпись, дата)

Благовещенск 2017

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем

УТВЕРЖДАЮ
Зав.кафедрой
_____А.В.Бушманов
«_____»_____2017 г.

З А Д А Н И Е

К бакалаврской работе студента Левковца Михаила Андреевича.

1. Тема бакалаврской работы: Разработка системы анализа log-файлов серверов в локальной сети предприятия ООО «Компания АЮСС».

(утверждено приказом от 25.04.2017 № 929-уч)

2. Срок сдачи студентом законченной работы 21.06.2017 г.

3. Исходные данные к бакалаврской работе: отчет по преддипломной практике.

4. Содержание бакалаврской работы: анализ деятельности предприятия, проектирование информационной системы, разработка программного обеспечения, исследование вопросов информационной безопасности, рассмотрение аспектов безопасности жизнедеятельности.

5. Перечень материалов приложения: организационная линейная структура, диаграммы DFD, ERD, техническое задание, схемы базы данных.

6. Консультант по бакалаврской работе консультант по безопасности и экологичности доцент, канд. техн. наук Булгаков А.Б.

7. Дата выдачи задания 09.05.2017 г.

Руководитель бакалаврской работы Бушманов Александр Вениаминович, доцент, канд. техн. наук.

Задание принял к исполнению (дата):_____М.А. Левковец

РЕФЕРАТ

Бакалаврская работа содержит 66 с., 38 рисунков, 22 таблицы, 6 приложений, 15 источников.

ПРОЕКТИРОВАНИЕ, РАЗРАБОТКА, БАЗА ДАННЫХ, LOG-ФАЙЛЫ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, СИСТЕМА, АНАЛИЗ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

Для данной выпускной квалификационной работы объектом исследования была выбрана деятельность предприятия ООО «Компания АЮСС».

Целью работы является разработка системы анализа log-файлов серверов в локальной сети.

Работа выполнялась последовательно в соответствие со следующими этапами: анализ деятельности предприятия, проектирование информационной системы, разработка приложения, рассмотрение вопросов информационной безопасности, а также исследование аспектов безопасности жизнедеятельности.

Разработанное программное обеспечение позволит облегчить деятельность системного администратора по контролю и защите данных на серверах предприятия.

Система разработана для системного администратора предприятия ООО «Компания АЮСС».

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ

В настоящей бакалаврской работе использованы ссылки на следующие стандарты и нормативные документы:

ГОСТ 2.104-68 ЕСКД Основные надписи

ГОСТ 2.105-95 ЕСКД Общие требования к текстовым документам

ГОСТ 2.106-96 ЕСКД Текстовые документы

ГОСТ 2.111-68 ЕСКД Нормоконтроль

ГОСТ 2.306-68 ЕСКД Обозначение графических материалов и правил нанесения их на чертежах

ГОСТ 2.316-68 ЕСКД Правила нанесения на чертежах надписей, технических требований и таблиц

ГОСТ 2.701-84 ЕСКД Схемы. Виды и типы. Общие требования к выполнению

ГОСТ 2.721-74 ЕСКД Обозначения условно-графические в схемах. Обозначения общего применения

ГОСТ 3.1103-83 ЕСКД Основные надписи

ГОСТ 3.1105-84 ЕСКД Правила оформления документов общего нзначения

ГОСТ 3.1130-93 ЕСКД Основные требования к формам и бланкам документов

ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания

ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

ГОСТ 34.602-89 Техническое задание на создание автоматизированной системы

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АС – автоматизированная система;

БД – база данных;

ВКР – выпускная квалификационная работа;

ООО – общество с ограниченной ответственностью;

ИС – информационная система;

ЛВС – локальная вычислительная сеть;

НСД – несанкционированный доступ;

ОС – операционная система;

ПК – персональный компьютер;

ПО – программное обеспечение;

СУБД – система управления базами данных;

ТЗ – техническое задание;

FTP – протокол передачи файлов;

SSH – безопасная оболочка;

URL – единый указатель ресурса.

ВВЕДЕНИЕ

В настоящее время невозможно представить работу даже маленькой компании без использования компьютерных технологий. А, следовательно, необходимо создание локальных или по-другому корпоративных сетей, в которых обычно задействованы практически все компьютеры любой компании. Однако со времени появления сетей появилась проблема и их безопасности. Многие руководители фирм даже и не задумываются о том, как может повлиять на работу организации несанкционированное проникновение в корпоративную сеть. Каждый руководитель должен понимать важность защиты своей сети от несанкционированных посягательств, атак из глобальной сети и т.д.

Для защиты сети применяется целый комплекс технических и программных средств различного назначения. Но как правило простейшую безопасность можно обеспечить просто, проводя анализ информации, содержащуюся в файлах, создаваемых самими серверами предприятия. Но в крупных компаниях таких событий может создаваться огромное количество, и обработка всей этой информации вручную является нецелесообразной. Для этого применяют специальные программные средства, называемые анализаторами log-файлов.

Объектом исследования выступает предприятие ООО «Компания АЮСС». Основной целью данной работы является создание системы анализа log-файлов серверов.

Задачами для разрабатываемой системы являются сбор и анализ log-файлов серверов, последующее их занесения в базу данных и представления в веб-интерфейсе. Её внедрение позволит облегчить деятельность системного администратора по контролю и защите данных на серверах предприятия.

Для достижения поставленной цели необходимо решить следующие задачи:

- провести анализ предприятия;
- обосновать необходимость создания данной системы;

- выполнить проектирование ИС;
- произвести разработку и тестирование спроектированной информационной системы.

Данная система представляет собой индивидуальный проект, полностью ориентированный на особенности деятельности ООО «Компания АЮСС».

1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

Анализ предметной области общий этап при проектировании и разработке ИС. Он позволяет собрать сведения об объекте и на их основе формировать видение будущей системы, выбирать технологии создания, а также определять набор требований к системе.

1.1 Общие сведения о компании ООО «Компания АЮСС»

В результате прохождения производственной практики на предприятии ООО «Компания АЮСС» был сформирован отчёт, в котором содержатся основные сведения о предприятии [1].

Общество с ограниченной ответственностью «Компания АЮСС» – крупная торговая компания, присутствующая более 25 лет на Дальневосточном рынке в сегменте промышленных товаров народного потребления – парфюмерия, бытовая химия, косметика и необходимые товары для дома.

ООО «Компания АЮСС» является коммерческой организацией. Основная цель её деятельности – это извлечение прибыли и последующее её распределение между участниками.

Предприятие состоит из следующих подразделений: 6 филиалов по всему Дальнему Востоку, осуществляющих как оптовую, так и розничную продажу [2]. Главный офис компании находится в городе Хабаровск. Каждый филиал осуществляет свою деятельность под руководством директора, каждый из которых централизованно взаимодействует с главным офисом.

1.2 Организационная структура предприятия

Подробнее рассмотрим структуру Благовещенского филиала компании. В приложении А представлена организационно-линейная структура данного филиала. Согласно [3, с.5], по данной схеме можно сказать, что предприятие имеет линейную структуру управления. В штате организации достаточно большое количество сотрудников и профиль их деятельности достаточно широк. ООО «АЮСС» имеет 10 отделов. За каждым отделом закреплен свой ру-

ководитель, который несет ответственность за деятельность своего отдела. Руководитель отдела следит за своевременным исполнением обязанностей подчиненных, старается наиболее рационально задействовать свой отдел, назначает лиц на премирование.

В приложении Б представлены диаграммы потоков данных, которые позволят определить различные пути следования информации в организации и ее передачу к внешним объектам.

На рисунке Б.1 представлена контекстная диаграмма потоков данных внешнего документооборота компании. На рисунке Б.2 подробно рассмотрен внутренний обмен данными между отделами организации.

Так как местом прохождения практики был отдел информационных технологий компании, рассмотрим его более подробно.

Отдел информационных технологий (ИТ) обеспечивает качественное и бесперебойное функционировании информационных систем и информационно-технической инфраструктуры компании, занимается внедрением новых решений и модернизацией существующих. У руководителя отдела ИТ в подчинении находятся:

– системный администратор;

– программист 1С;

– два инженера.

Каждый работник ИТ отдела имеет свой узкий профиль и обязан обеспечивать своевременную поддержку по своему направлению.

Программист 1С занимается гибкой настройкой комплекса программ 1С: Предприятие, а также программирование модулей 1С, в частности изменение конфигураций для более удобного доступа к нужным функциям, путем добавления внешних обработок, удаления неиспользуемого функционала.

Инженеры следят за исправностью парка компьютерной техники, устраняют неисправности комплектующих персональных компьютеров, периферийной техники, компонентов сети и так далее. В отличии от других инфор-

мационных должностей, зачастую инженеры работают вне офиса, т.е. непосредственно на объектах компании, таких как склад, розничные точки продаж и т.д.

Системный администратор является сотрудником, в должностные обязанности которого входит контроль за состоянием локальной сети и ПО (программного обеспечения), а также обеспечение информационной безопасности в организации. Также обязан следить за обеспечением штатной работы парка компьютерной техники, включающей как персональные рабочие места сотрудников всех отделов, так и обеспечение постоянной и стабильной работы всех серверов предприятия.

Помимо всех перечисленных обязанностей, сотрудники отдела ИТ решают проблемы, основанные на заявках пользователей. На рисунке 1 представлена схема решения таких проблем.

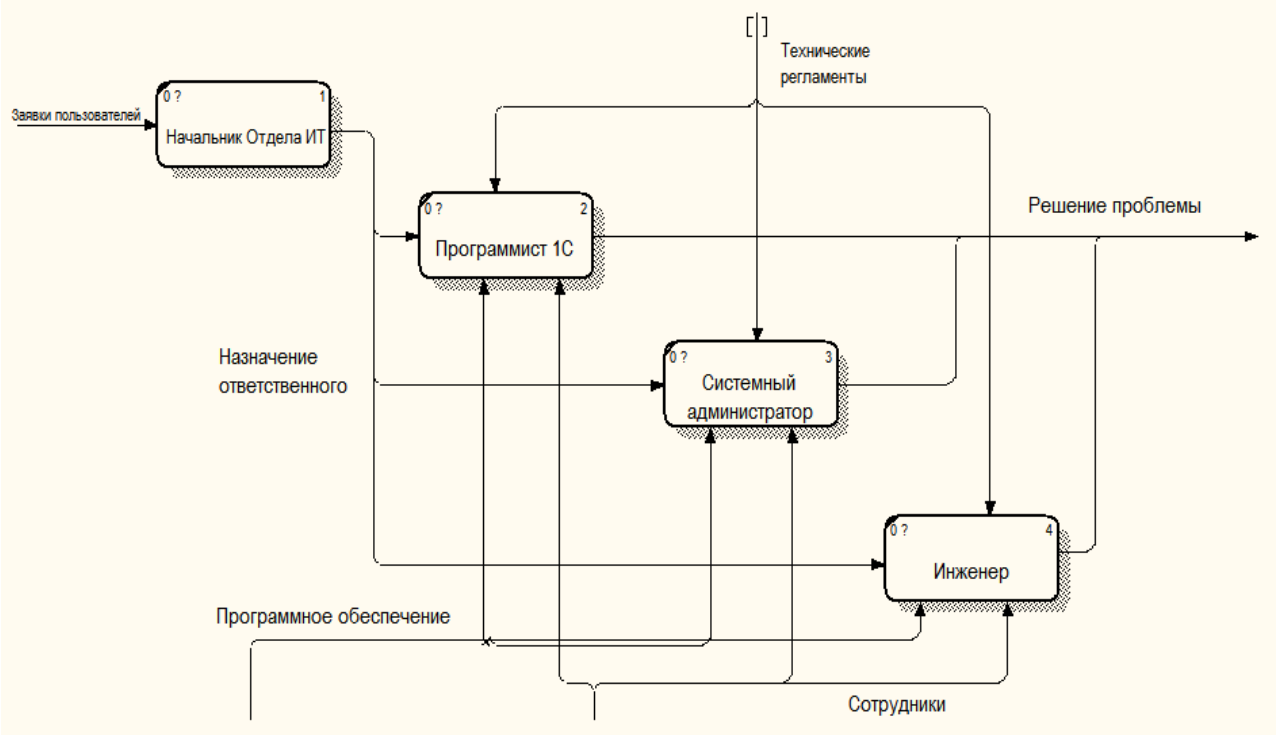

Рисунок 1 – Работа отдела ИТ

Работа отдела устроена следующим образом: начальнику отдела приходят заявки от пользователей с указанием проблемы, он определяет к какой области относится эта проблема и уже даёт распоряжения определённому сотруднику отдела, в круг полномочий которого входит эта проблема.

В целом можно сказать, что организация обладает цельной структурой и является крупным частным коммерческим предприятием.

1.3 Описание программного и технического обеспечения

На данный момент времени компьютерный парк ООО «Компания АЮСС» насчитывает более 400 единиц различной вычислительной техники.

Компания располагает десктопными и планшетными персональными компьютерами, различной оргтехникой, периферийными устройствами, терминалами, интерактивными досками, фото и видеотехникой, и т.д.

В качестве рабочих станций используются компьютеры на базе архитектуры Intel с установленными операционными системами семейства Microsoft Windows – Windows XP, Windows 7, Windows 8.1.

Работники ИТ-отдела активно проверяют состояние персональных компьютеров и стараются по возможности обновлять или полностью заменять устаревшее оборудование. Помимо технической составляющей, обновлению подвергается программное обеспечение.

Все компьютеры включены в домен под управлением серверов на платформе Microsoft Windows Server 2012. В качестве стандартного офисного пакета программ используется Microsoft Office 2013.

Антивирусная защита компьютеров компании обеспечена программным продуктом фирмы «AVAST», а роль межсетевого экрана выполняет Comodo Firewall.

ООО «Компания АЮСС» имеет 15 выделенных серверов, каждый из которых выполняет определенные функции:

- файловый сервер;
- интернет-шлюз;
- web-сервер и почтовый сервер;
- сервера 1С;
- сервер баз данных;
- back-up сервер;
- контролеры домена;

– сервер корпоративной связи и др.

Полная схема серверного парка компании представлена на рисунке 2.

Рисунок 2 – Серверный парк компании

Рассмотрим подробнее назначения серверов, наиболее актуальных в теме данной ВКР.

Почтовый сервер. Основная задача такого сервера состоит в распознавании адресов входящей электронной почты, а также отправка исходящей, обеспечение внутренней переписки. Почтовый сервер обеспечивает надежную фильтрацию спама и вредоносных программ, распространяемых с сообщениями, и защищает внутреннюю информацию от нежелательного доступа.

Сервер корпоративной связи. Представляет собой Openfire-сервер. Это, согласно [4], сервер, основанный на протоколе Extensible Messaging and Presence Protocol (XMPP), т.е. свободный для использования протокол для мгновенного обмена сообщениями в режиме, близком к режиму реального времени. Основная задача – обмен мгновенными сообщениями.

FTP-сервер. Сервер, используемый для передачи файлов между основным офисом компании и магазинами розничной торговли. Использование

этого сервера очень важно для осуществления коммерческой деятельности организации.

Схема ЛВС ООО «Компания АЮСС» представлена на рисунке 3.

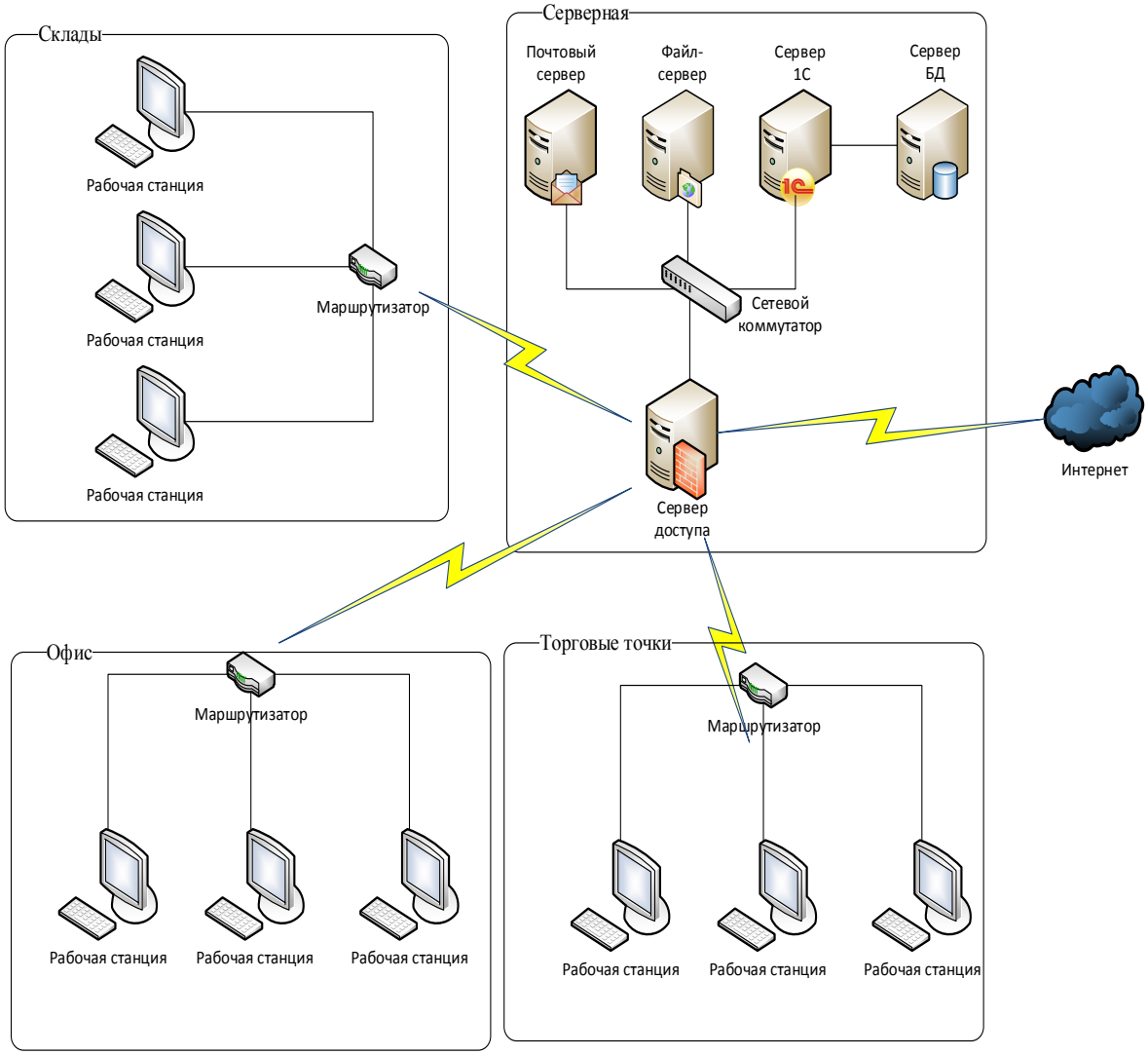

Рисунок 3 – Схема сети ООО «Компания АЮСС»

Данная ЛВС имеет топологию звезда, что удовлетворяет условию для создания системы.

1.4 Обоснование необходимости создания системы анализа данных

Все угрозы информационным ресурсам предприятия можно отнести к одной из следующих категорий:

– угрозы доступности информации;

– угрозы целостности информации;

– угрозы конфиденциальности информации.

Наличие такого немалого количества серверов в организации, должно предполагать, что они должны быть всегда доступны для пользователя, защищены от НСД и неправомерного изменения информации. Это будет удовлетворять всем условиям безопасности ИС.

За защитой серверного парка предприятия следит системный администратор. В его обязанности входит следить как за физическим доступом к серверам (непосредственно в серверной комнате), так и за удалённым доступом. Одним из способов обеспечения безопасности, является наблюдение за данными, которые поступают в специальный файл, называемый log-файл.

Согласно [5], log-файл (файл регистрации) – файл, содержащий системную информацию о работе сервера и информацию о действиях пользователей на нём.

Log-файлы различаются своим содержанием. Оно зависит от того какая служба сервера составляет этот файл и какую информацию в него записывает. Например, все файлы, называющиеся auth.log хранят в себе информацию об авторизации пользователей на сервере. Часть такого файла показана на рисунке 4.

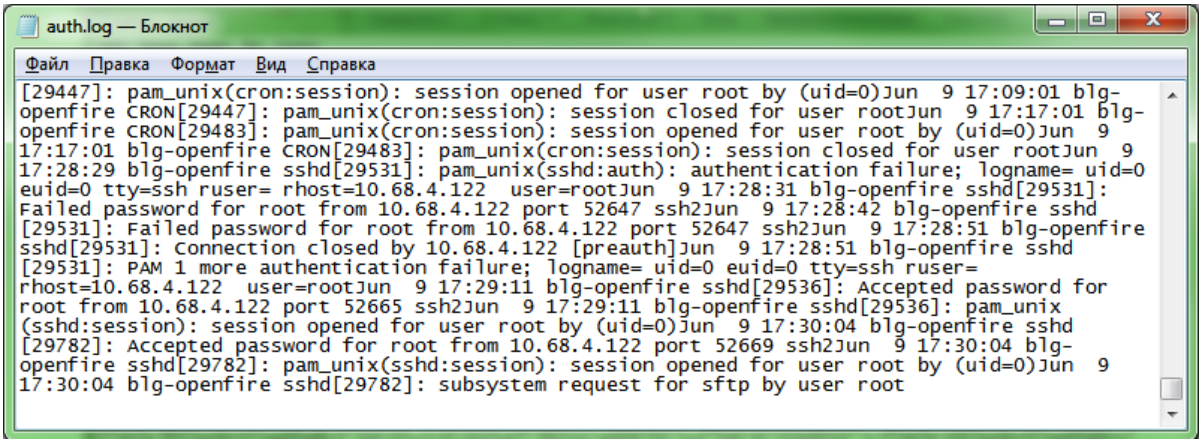

Рисунок 4 – часть log-файла auth.log

Как видно на рисунке, файл представляет собой неструктурированную информацию, записываемую по определённому правилу. Системный администратор, посмотрев такой log-файл может увидеть данные о подключенных к серверу пользователях. Это позволяет отследить совершаемые ими несанкционированные операции.

Но чтение и анализ log-файлов вручную очень неудобно и весьма трудоёмко из-за огромного количества данных, которые в них поступают. Для получения отчётов и представления информации в более удобном виде используют специальные программные продукты, называемые анализаторами log-файлов.

Создание такой системы позволит достигнуть целей, которые были выделены в соответствие с подразделом 2.2 приложения В:

– своевременное обнаружение несанкционированного доступа к серверам;

– упрощение работы системного администратора;

– уменьшение времени на сбор и обработку информации о состоянии серверов.

1.5 Постановка задачи

В данном подразделе необходимо точно сформулировать условия задачи разработки с описанием входной и выходной информации.

В качестве входной информации для создания ИС служит техническое задание, сформированное в соответствие со стандартом ГОСТ 34.602-89 «Техническое задание на создание автоматизированной системы». Разработка ТЗ осуществляется во взаимодействие с заказчиком и на основе данных, полученных в ходе анализа предметной области. ТЗ на разработку данной ИС представлено в приложение В. Оно, согласно подразделу 2.1 приложения В, включает:

– общие положения, представляющие собой основные наименования участвующих сторон (заказчика, исполнителя);

– назначение и цели создания системы, которые установлены с точки зрения заказчика. Они определяют его ожидания от создания и внедрения системы;

– характеристика объекта автоматизации, определяет текущее состояние части исследуемого предприятия с точки зрения заказчика;

– требования к системе, определяют то, какую систему хочет получить заказчик в результате проведения работ по ее созданию;

– состав и содержание работ по созданию системы, регламентируют различные технико-экономические аспекты и временные затраты на создание системы;

– требование к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие, устанавливает последовательность действий необходимых для ввода системы в эксплуатацию;

– требования к документированию, состав комплекта документов, образующийся в ходе проектирования и разработки данной системы;

– источники разработки, описываются различные информационные ресурсы, послужившие основой для разработки.

Для выполнения данной ВКР необходимо в соответствие с требованиями заказчика, разработать ПО, которое реализует оговоренные с заказчиком функции. В соответствие с пунктом 4.1.1 приложения В, выделим функциональные подсистемы, которые должны присутствовать в системе:

– подсистема идентификации, аутентификации и авторизации, которая позволит однозначно определить работающего в системе администратора;

– подсистема сбора данных;

– подсистема обработки данных, которая позволит агрегировать информацию;

– подсистема работы базы данных;

– подсистема графического интерфейса пользователя.

Выходной информацией должны служить сведения о прохождении системой этапов, определенных порядком контроля и приемки системы, представленным в разделе 6 приложения В, по следующим пунктам:

– анализ готовой системы;

– сравнение разработанной системы с техническим заданием на ее разработку, с целью определения выполнения всех предъявленных требований;

– выполнение доработки и изменений системы при необходимости;

– опытная эксплуатация системы в режиме бета-тестирования;

– доработка системы и исправление ошибок.

Постановка задачи разработки четко определяет дальнейшие действия по проектированию и разработке приложения.

Действия, произведенные на этапе анализа деятельности предприятия, позволяют нам сформировать видение предметной области, определить цели и необходимость создания системы, а также в общих чертах ознакомиться с требованиями заказчика.

2 ПРОЕКТИРОВАНИЕ СИСТЕМЫ АНАЛИЗА ДАННЫХ

Этап проектирования информационной системы является основополагающим, поскольку именно от приложенных усилий и уровня проработки данного аспекта зависит успешность будущего проекта.

2.1 Общая структура системы

Схема общей структуры системы показана на рисунке 5.

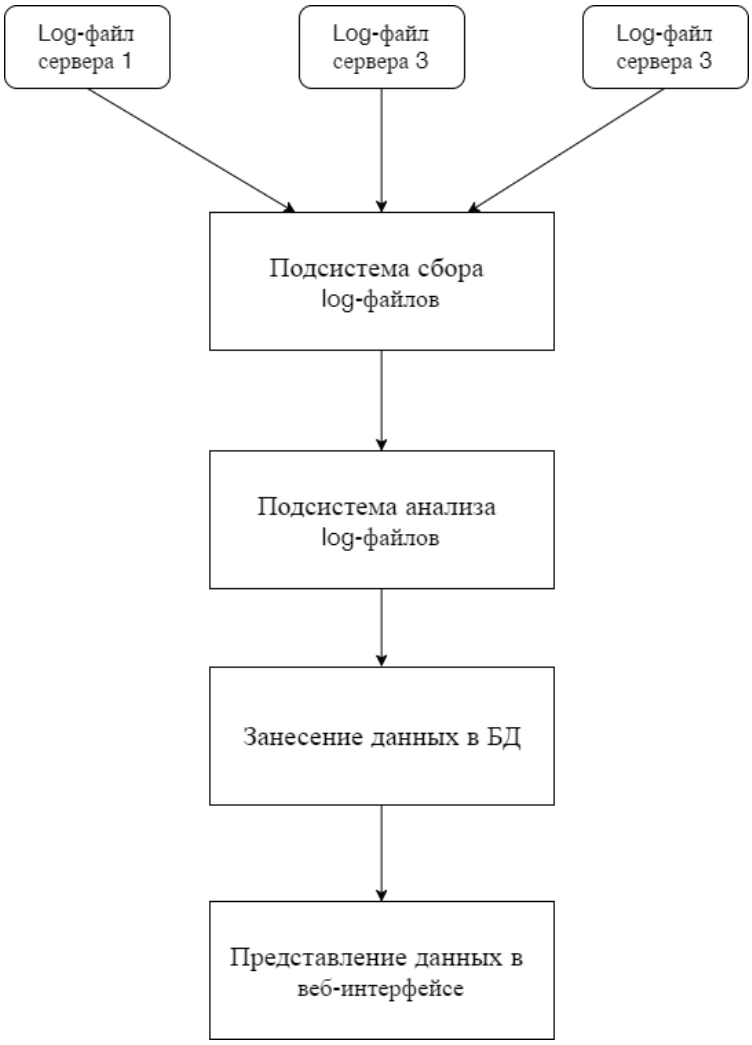

Рисунок 5 – Общая структура системы

Из данной схемы видно, что система состоит из нескольких подсистем. В качестве серверов с которых осуществляется сбор log-файлов были выбраны почтовый и FTP серверы, сервер корпоративной связи. Были выбраны именно эти серверы, т.к. именно по их работе возникает наибольшее число заявок от

пользователей и системному администратору приходится вручную просматривать log-файлы и решать возникшие проблемы.

2.2 Проектирование функциональных подсистем

В данном разделе более подробно будут рассмотрены функциональные подсистемы с целью более полного понимания решаемых ими задач и, тем самым, выбора наиболее точного способа их дальнейшей реализации.

2.2.1 Характеристика подсистемы сбора

Согласно пункту 4.2.2 в приложении В, подсистема сбора данных должна решать одну главную задачу – это передача log-файлов на сервер по сети.

Подсистема сбора исходных log-файлов предназначена для автоматизации процесса передачи файлов по сети, для дальнейшей работы с ними подсистемы анализа. Необходимый log-файл передаётся на сервер, на котором находится система анализа данных.

2.2.2 Характеристика подсистемы анализа

Для данной подсистемы в пункте 4.2.3 приложения В также выделена одна основная задача, которую она должна решать – это обработка и анализ данных, полученных с сервера.

Исходные log-файлы, получаемые системой сбора, представляют собой неструктурированный файл с огромным количеством данных. Ручная обработка таких файлов весьма трудоёмка и занимает немалое количество времени. Для автоматизации данного процесса необходима разработка подсистемы анализа, которая будет находить в исходных log-файлах необходимую информацию, выбирать её и заносить в БД.

2.2.3 Характеристика подсистемы идентификации, аутентификации и авторизации

Для веб-интерфейса данной системы должен быть разработан блок подсистем идентификации, аутентификации и авторизации, так как его компоненты участвуют во всех информационных обменах, а также с него начинается работа администратора системы.

Модуль разбивается на 3 компонента: идентификация, аутентификация и авторизация.

Компонент идентификации реализуется предоставлением пользователю уникального идентификатора в БД. Далее система должна соотносить все его действия с идентификатором, который представляет собой число.

Так как система предназначена для одного пользователя – администратора, то компоненты аутентификации и авторизации были объединены.

Компонент аутентификации должен удостоверять подлинность субъекта, пытающегося войти в систему. Данная операция проводится по введенному пользователем логину и паролю. При успешной аутентификации администратор попадает на веб-интерфейс системы где у него появляются все права для работы с данной системой.

2.3 Характеристика обеспечивающих подсистем

Данный тип систем является общим для всех компонентов ИС. Подробно этот вопрос рассмотрен в подразделе 4.3 приложения В.

В данном разделе стоит остановиться лишь на некоторых подсистемах, имеющих наибольшую важность для разработки.

Для начала отметим информационное обеспечение. Данные в веб-интерфейсе должны быть представлены в различных форматах: объекты, текст, реляционные таблицы и т.п. Их преобразование должно осуществляться без потери. Для работы системы необходим начальный набор данных, получаемых с исходных log-файлов серверов.

Для разработки подсистем сбора и анализа данных наиболее оптимальным выбором является язык программирования Python. При разработке веб-интерфейса лучше всего использовать PHP для серверных функций, JavaScript – для клиентских и SQL – для взаимодействия с БД.

Так же стоит отметить выбор нотаций проектирования: DFD – для описания предметной области, UML – для проектирования приложения, ERD, IDEF1.X – для описания БД.

2.4 Обоснование выбора средств разработки

На сегодняшний день на рынке информационных технологий существует большое количество различных средств разработки и проектирования. При разработке должны быть исключены рутинные действия программиста, использоваться шаблоны и другие компоненты.

Для описания предметной области и составления схем при проектировании были выбраны программы MS Visio (версии 2007), Ramus Educational (версии 1.1.1), IBM Rational Rose (версии 7.0) и ERWin Data Modeler (версии 7.2).

Visio является программой для составления общих схем описания предметной области.

Ramus имеет конкретную реализацию для нотации DFD, поэтому наиболее подходит для составления данных диаграмм.

Rational Rose необходим для составления UML-диаграмм.

ERWin Data Modeler – комплексная система для проектирования БД, также позволяет в дальнейшем преобразовывать схемы в SQL-код.

2.4.1 Обоснование выбора СУБД

Выбор СУБД определяет способ взаимодействия с ней, поэтому от этого строится все дальнейшее проектирование и разработка.

Для создания небольших и средних веб-приложения из всего многообразия современных СУБД наиболее распространена СУБД MySQL. Данная СУБД имеет свободно распространяемую лицензию, она хорошо документирована и имеет большую пользовательскую базу. Система поддерживает весь необходимый функционал для создания БД, а также большое количество разнообразных инструментов, которые добавляют интерактивность и ускоряют разработку. Например, MySQL Workbench или PHPMyAdmin.

2.4.2 Обоснование выбора программных платформ и языков программирования

В пункте 4.3.2 приложения В указаны требования, применяемые к лингвистическому обеспечению системы.

Согласно данным требованиям, для разработки функционала системы должны быть использованы языки программирования PHP, JavaScript, Python.

Для разработки подсистем сбора и анализа был выбран язык программирования Python. Согласно [6], Python это высокоуровневый, интерпретируемый, интерактивный и объектно-ориентированный скриптовой язык программирования. Python был разработан как «легкочитаемый» язык, часто использующий в качестве ключевых слов слова английского языка.

Согласно [7, с. 32], его преимущества заключаются в:

- качество программного обеспечения;
- высокая скорость разработки;
- переносимость программ;
- библиотеки поддержки;
- интеграция компонентов.

Для реализации функционала web-интерфейса была выбрана связка PHP и JavaScript. Связка вида PHP + JavaScript + MySql + Apache (веб-сервер) + браузер великолепно демонстрирует разделение программы в рамках технологии Клиент-Сервер. При этом запросы обрабатываются на машинах конечных пользователей, без установки специального программного обеспечения, что делает систему обработки данных гибкой и легко модифицируемой, при этом обеспечиваются все преимущества клиент-серверной обработки данных. Также следует отметить, то что все компоненты, кроме браузера являются бесплатными или условно бесплатными продуктами, что также снижает расходы на разработку ПО.

2.4.3 Обоснование выбора программных платформ дизайна

Согласно пункту 4.1.5 приложения В, при работе с веб-интерфейсом системы экранные формы и интерфейс должны быть интуитивно понятны, обладать общим дизайном и не содержать, раздражающих глаз элементов.

Для веб-приложения характерно использования связки технологий HTML+CSS (каскадные таблицы стилей). Первая определяет структурную составляющую дизайна, а вторая стилевое оформление.

2.5 Проектирование БД

Разработка проекта БД осуществляется в три этапа и на выходе получается схема БД, из которой можно получить SQL-описание для дальнейшего импорта в СУБД.

2.5.1 Инфологическое проектирование

На данном этапе необходимо специфицировать сущности, их атрибуты и связи между ними. В результате получить схему сущностей и их связей.

Для данной системы были выделены сущности, представленные в таблице 1. Незаполненные ячейки количества экземпляров для сущности, говорят о том, что ее заполнение будет осуществляться в ходе работы приложения и заранее нельзя обозначить точное количество экземпляров. Заполненное количество экземпляров определено для таблиц-справочников. Название сущностей для хранения данных log-файлов обозначены названием службы, использующей этот log-файл.

Таблица 1 – Определение сущностей

Название	Описание	Количество экземпляров
Сервер	содержит информацию об имени сервера	3
Тип сервера	расширяет сущность Сервер, добавляя тип сервера	3
Пользователь	данная сущность содержит персональные данные для входа администратора	1
Лог	содержит информацию о дате добавления лога	3
iredapd	содержит данные почтового сервера	
auth_mail	сущность, содержащая данные о подключениях к почтовому серверу	
access	содержит данные о запросах к серверу корпоративной связи	
auth_openfire	сущность, содержащая данные о подключениях к серверу корпоративной связи	
vsftpd	содержит данные о передаче файлов по ftp	
auth_ftp	сущность, содержащая данные о подключениях к ftp-серверу	

Далее были выявлены атрибуты сущностей, которые описаны в таблицах 2 – 11.

Таблица 2 – Атрибуты сущности Сервер

Название	Описание	Диапазон значений	Единица измерения	Пример
Код сервера	уникальный идентификатор сервера	1, 2, …	-	1
Имя сервера	название сервера	-	-	Mail

Таблица 3 – Атрибуты сущности Тип сервера

Название	Описание	Диапазон значений	Единица измерения	Пример
Код типа	уникальный идентификатор типа сервера	1, 2, …	-	1
Имя типа	название типа сервера	-	-	Почтовый сервер

Таблица 4 – Атрибуты сущности Пользователь

Название	Описание	Диапазон значений	Единица измерения	Пример
Код пользователя	уникальный идентификатор пользователя	1, 2, …	-	4
Логин	Идентификатор для входа	-	-	Login
Пароль	пароль пользователя в зашифрованном виде	-	-	a57a5a7438

Таблица 5 – Атрибуты сущности Лог

Название	Описание	Диапазон значений	Единица измерения	Пример
Код лога	уникальный идентификатор лога	1, 2, …	-	3
Дата добавления	содержит дату добавления лога	-	год, месяц, число	2017-06-04

Таблица 6 – Атрибуты сущности iredapd

Название	Описание	Диапазон значений	Единица измерения	Пример
1	2	3	4	5
Код записи	уникальный идентификатор записи лога	1, 2, …	-	4

Продолжение таблицы 6

1	2	3	4	5
Дата письма	дата когда пришло письмо	-	год, месяц, число	2017-06-04
Время письма	время когда пришло письмо	-	час, минута, секунда	23:14:21
Ip от	Ip-адрес отправителя	0.0.0.1-255.255.255.254	-	127.0.0.1
Письмо от	адрес отправителя	-	-	exam-ple@mail.ru
Письмо кому	адрес получателя	-	-	exam-ple@mail.ru

Таблица 7 – Атрибуты сущности auth_mail

Название	Описание	Диапазон значений	Единица измерения	Пример
Код записи	уникальный идентификатор записи лога	1, 2, …	-	4
Дата	дата входа на сервер	-	год, месяц, число	2017-06-04
Время	время входа на сервер	-	час, минута, секунда	23:14:21
Пользователь	пользователь на сервере	-	-	root
Ip-адрес	Ip-адрес с которого совершён вход	0.0.0.1-255.255.255.254	-	127.0.0.1

Таблица 8 – Атрибуты сущности access

Название	Описание	Диапазон значений	Единица измерения	Пример
1	2	3	4	5
Код записи	уникальный идентификатор записи лога	1, 2, …	-	4
Ip-адрес	Ip-адрес с которого был запрос	0.0.0.1-255.255.255.254	-	127.0.0.1
Дата	дата входа на сервер	-	год, месяц, число	2017-06-04
Время	время входа на сервер	-	час, минута, секунда	23:14:21
Url к	Url к которому было обращение	-	-	https://www.google.ru/

Продолжение таблицы 8

1	2	3	4	5
Url от	Url от которого было обращение	-	-	https://www.google.ru/

Таблица 9 – Атрибуты сущности auth_openfire

Название	Описание	Диапазон значений	Единица измерения	Пример
Код записи	уникальный идентификатор записи лога	1, 2, …	-	4
Дата	дата входа на сервер	-	год, месяц, число	2017-06-04
Время	время входа на сервер	-	час, минута, секунда	23:14:21
Пользователь	пользователь на сервере	-	-	root
Ip-адрес	Ip-адрес с которого совершён вход	0.0.0.1-255.255.255.254	-	127.0.0.1

Таблица 10 – Атрибуты сущности vsftpd

Название	Описание	Диапазон значений	Единица измерения	Пример
Код записи	уникальный идентификатор записи лога	1, 2, …	-	4
Дата	дата входа на сервер	-	год, месяц, число	2017-06-04
Время	время входа на сервер	-	час, минута, секунда	23:14:21
Ip-адрес	Ip-адрес с которого совершён вход	0.0.0.1-255.255.255.254	-	127.0.0.1
Статус	статус передачи файлов	-	-	Ok

Таблица 11 – Атрибуты сущности auth_ftp

Название	Описание	Диапазон значений	Единица измерения	Пример
1	2	3	4	5
Код записи	уникальный идентификатор записи лога	1, 2, …	-	3
Дата	дата входа на сервер	-	год, месяц, число	2017-06-04

Продолжение таблицы 11

1	2	3	4	5
Время	время входа на сервер	-	час, минута, секунда	23:14:21
Пользователь	пользователь на сервере	-	-	root
Ip-адрес	Ip-адрес с которого совершён вход	0.0.0.1-255.255.255.254	-	127.0.0.1

Все выявленные взаимосвязи между сущностями представлены в таблице 12.

Использование термина привязки характеризует вспомогательные таблицы, позволяющие избежать возникновения связей многие-ко-многим.

Таблица 12 – Распределение связей между сущностями

Название первой сущности, участвующей в связи	Название второй сущности, участвующей в связи	Название связи	Тип связи	Обоснование выбора типа связи
1	2	3	4	5
Сервер	Тип сервера	расширяет	один-ко-многим	Одной записи сущности Сервер соответствует одна запись сущности Тип сервера, каждой записи сущности Тип сервера соответствует множество записей сущности Сервер. Сервер соответствует только одному типу, в то время как каждый тип могут иметь несколько серверов.
Лог	Сервер	содержится	один-ко-многим	Одной записи сущности Лог соответствует одна запись сущности Сервер, каждой записи сущности Сервер соответствует множество записей сущности Лог. Лог соответствует только одному серверу, в то время как каждый сервер может иметь несколько логов.

Продолжение таблицы 12

1	2	3	4	5
Лог	Пользователь	владеет	один-ко-многим	Одной записи сущности Лог соответствует одна запись сущности Пользователь, каждой записи сущности Пользователь соответствует множество записей сущности Лог. Один лог соответствует только одному пользователю, в то время как каждый пользователь может иметь несколько логов.
iredapd	Лог	содержит	один-ко-многим	Одной записи сущности iredapd соответствует одна запись сущности Лог, каждой записи сущности Лог соответствует множество записей сущности iredapd. Одной записи в iredapd соответствует только один лог, в то время как каждый лог может иметь несколько записей в ireapd.
auth_mail	Лог	содержит	один-ко-многим	Одной записи сущности auth_mail соответствует одна запись сущности Лог, каждой записи сущности Лог соответствует множество записей сущности auth_mail. Одной записи в auth_mail соответствует только один лог, в то время как каждый лог может иметь несколько записей в auth_mail.

Продолжение таблицы 12

1	2	3	4	5
access	Лог	содержит	один-ко-многим	Одной записи сущности access соответствует одна запись сущности Лог, каждой записи сущности Лог соответствует множество записей сущности access. Одной записи в access соответствует только один лог, в то время как каждый лог может иметь несколько записей в access.
auth_openfire	Лог	содержит	один-ко-многим	Одной записи сущности auth_openfire соответствует одна запись сущности Лог, каждой записи сущности Лог соответствует множество записей сущности auth_openfire. Одной записи в auth_openfire соответствует только один лог, в то время как каждый лог может иметь несколько записей в auth_openfire.
vsftpd	Лог	содержит	один-ко-многим	Одной записи сущности vsftpd соответствует одна запись сущности Лог, каждой записи сущности Лог соответствует множество записей сущности vsftpd. Одной записи в vsftpd соответствует только один лог, в то время как каждый лог может иметь несколько записей в vsftpd.

Продолжение таблицы 12

1	2	3	4	5
auth_ftp	Лог	содержит	один-ко-многим	Одной записи сущности auth_ftp соответствует одна запись сущности Лог, каждой записи сущности Лог соответствует множество записей сущности auth_ftp. Одной записи в auth_ftp соответствует только один лог, в то время как каждый лог может иметь несколько записей в auth_ftp.

В результате выделения сущностей, их атрибутов и связей была составлена схема «сущность-связь», которая представлена в приложении Г.

2.5.2 Логическое проектирование

2.5.2.1 Отображение на реляционную модель

Целью данного этапа является построение реляционной логической модели. Реляционная логическая модель представляет собой совокупность нормализованных отношений, в которых реализованы связи между объектами предметной области и выполнены все преобразования, необходимые для ее эффективной реализации в среде конкретной СУБД.

Выполним отображение сущностей инфологической модели на отношения реляционной модели.

Связь «Сервер – Тип сервер» является связью типа один–ко–многим. При отображении ключ порожденной сущности добавляется в исходную сущность. Исходной сущностью является сущность Сервер, порожденной – Тип сервера. Связь показана на рисунке 6, на рисунке 7 приведены итоговые отношения.

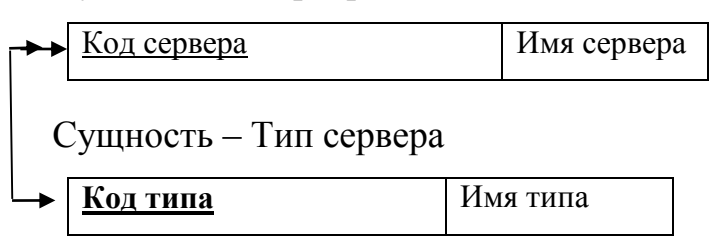

Рисунок 6 – Связь Сервер-Тип сервера

Сущность – Сервер

Код сервера	Имя сервера	***Код типа***

Сущность – Тип сервера

Код типа	Имя типа

Рисунок 7 – Отображение связи Сервер-Тип сервера

Связь «Лог - Сервер» является связью типа один–ко–многим. При отображении ключ порожденной сущности добавляется в исходную сущность. Исходной сущностью является сущность Лог, порожденной – Сервер. Связь показана на рисунке 8, на рисунке 9 приведены итоговые отношения.

Сущность – Лог

Код лога	Дата добавления

Сущность – Сервер

Код сервера	Имя сервера	Код типа

Рисунок 8 – Связь Лог-Сервер

Сущность – Лог

Код лога	Дата добавления	Код сервера

Сущность – Сервер

Код сервера	Имя сервера	Код типа

Рисунок 9 – Отображение связи Лог-Сервер

Связь «Лог - Пользователь» является связью типа один–ко–многим. Исходной сущностью является сущность Лог, порожденной – Пользователь. Связь показана на рисунке 10, на рисунке 11 приведены итоговые отношения.

Сущность – Лог

Код лога	Дата добавления	Код сервера

Сущность – Пользователь

Код пользователя	Логин	Пароль

Рисунок 10 – Связь Лог-Пользователь

Сущность – Лог

Код лога	Дата добавления	Код сервера	Код пользователя

Сущность – Пользователь

Код пользователя	Логин	Пароль

Рисунок 11 – Отображение связи Лог-Пользователь

Связь «iredapd - Лог» является связью типа один–ко–многим. При отображении ключ порожденной сущности добавляется в исходную сущность. Исходной сущностью является сущность iredapd, порожденной – Лог. Связь показана на рисунке 12, на рисунке 13 приведены итоговые отношения.

Сущность – iredapd

Код записи	Дата письма	Время письма	Ip от
Письмо от	Письмо кому		

Сущность – Лог

Код лога	Дата добавления	Код сервера	Код пользователя

Рисунок 12 – Связь iredapd - Лог

Сущность – iredapd

Код записи	Дата письма	Время письма	Ip от
Письмо от	Письмо кому	Код лога	

Сущность – Лог

Код лога	Дата добавления	Код сервера	Код пользователя

Рисунок 13 – Отображение связи iredapd - Лог

Связь «auth_mail - Лог» является связью типа один–ко–многим. При отображении ключ порожденной сущности добавляется в исходную сущность, причем сущность имеет два атрибута, содержащие отличные друг от друга ключи сущностей одного типа. Исходной сущностью является сущность auth_mail, порожденной – Лог. Связь показана на рисунке 14, на рисунке 15 приведены итоговые отношения.

Сущность – auth_mail

Код записи	Дата	Время	Ip-адрес
Пользователь			

Сущность – Лог

Код лога	Дата добавления	Код сервера	Код пользователя

Рисунок 14 – Связь auth_mail - Лог

Сущность – auth_mail

Код записи	Дата	Время	Ip-адрес
Пользователь	Код лога		

Сущность – Лог

Код лога	Дата добавления	Код сервера	Код пользователя

Рисунок 15 – Отображение связи auth_mail - Лог

Связь «access - Лог» является связью типа один–ко–многим. При отображении ключ порожденной сущности добавляется в исходную сущность. Исходной сущностью является сущность access, порожденной – Лог. Связь показана на рисунке 16, на рисунке 17 приведены итоговые отношения.

Сущность – access

Код записи	Дата	Время	Ip-адрес
Url от	Url к		

Сущность – Лог

Код лога	Дата добавления	Код сервера	Код пользователя

Рисунок 16 – Связь access - Лог

Сущность – access

Код записи	Дата	Время	Ip-адрес
Url от	Url к	Код лога	

Сущность – Лог

Код лога	Дата добавления	Код сервера	Код пользователя

Рисунок 17 – Отображение связи access - Лог

Связь «auth_openfire - Лог» является связью типа один–ко–многим. Исходной является сущность auth_openfire, порожденной – Лог. На рисунке 18 показана связь, на рисунке 19 итоговые отношения.

Сущность – auth_openfire

Код записи	Дата	Время	Ip-адрес
Пользователь			

Сущность – Лог

Код лога	Дата добавления	Код сервера	Код пользователя

Рисунок 18 – Связь auth_openfire - Лог

Сущность – auth_openfire

Код записи	Дата	Время	Ip-адрес
Пользователь	Код лога		

Сущность – Лог

Код лога	Дата добавления	Код сервера	Код пользователя

Рисунок 19 – Отображение связи auth_openfire - Лог

Связь «vsftpd - Лог» является связью типа один–ко–многим. На рисунке 20 показана связь, на рисунке 21 итоговые отношения.

Сущность – vsftpd

Код записи	Дата	Время	Ip-адрес
Статус			

Сущность – Лог

Код лога	Дата добавления	Код сервера	Код пользователя

Рисунок 20 – Связь vsftpd - Лог

Сущность – vsftpd

Код записи	Дата	Время	Ip-адрес
Пользователь	Код лога		

Сущность – Лог

Код лога	Дата добавления	Код сервера	Код пользователя

Рисунок 21 – Отображение связи vsftpd - Лог

Связь «auth_ftp - Лог» является связью типа один–ко–многим. При отображении ключ порожденной сущности добавляется в исходную сущность. Исходной сущностью является сущность auth_ftp, порожденной – Лог. Связь показана на рисунке 22, на рисунке 23 приведены итоговые отношения.

Рисунок 22 – Связь auth_ftp - Лог

Рисунок 23 – Отображение связи auth_ftp – Лог

По завершению этапа логического проектирования была сформирована логическая модель, схема которой изображена на рисунке Д1.

2.5.3 Физическое проектирование

После этапа логического проектирования следует этап физического проектирования. Физическое проектирование – создание схемы базы данных для конкретной СУБД. Специфика конкретной СУБД может включать в себя ограничения на именование объектов базы данных, ограничения на поддерживаемые типы данных и т. п. Кроме того, специфика конкретной СУБД при физическом проектировании включает выбор решений, связанных с физической средой хранения данных (выбор методов управления дисковой памятью, разделение БД по файлам и устройствам, методов доступа к данным), создание индексов и т. д. Согласно пункту 2.4.1, в качестве СУБД используется MySQL, поэтому в таблицах 13-22 представлены данные в соответствующей форме.

Таблица 13 – Сервер

Название поля	Тип данных	Длина	Ограничения	Значения по умолчанию	NULL	Индексация
Код сервера	int	11	-	-	нет	да (совпадения не допускаются)
Код типа	int	11	-	-	нет	нет
Имя сервера	varchar	45	-	-	нет	нет

Таблица 14 – Тип сервера

Название поля	Тип данных	Длина	Ограничения	Значения по умолчанию	NULL	Индексация
Код типа	int	11	-	-	нет	да (совпадения не допускаются)
Имя типа	varchar	45	-	-	нет	нет

Таблица 15 – Пользователь

Название поля	Тип данных	Длина	Ограничения	Значения по умолчанию	NULL	Индексация
Код пользователя	int	11	-	-	нет	да (совпадения не допускаются)
Логин	varchar	15	-	-	нет	нет
Пароль	varchar	15	-	-	нет	нет

Таблица 16 – Лог

Название поля	Тип данных	Длина	Ограничения	Значения по умолчанию	NULL	Индексация
Код лога	int	11	-	-	нет	да (совпадения не допускаются)
Код сервера	int	11	-	-	нет	нет
Код пользователя	int	11	-	-	нет	нет
Дата добавления	date	-	-	-	нет	нет

Таблица 17 – iredapd

Название поля	Тип данных	Длина	Ограничения	Значения по умолчанию	NULL	Индексация
Код записи	int	11	-	-	нет	да (совпадения не допускаются)
Код лога	int	11	-	1	нет	нет
Дата письма	date	-	-	-	NULL	нет
Время письма	time	-	-	-	NULL	нет
Ip от	varchar	15	-	-	NULL	нет
Письмо от	varchar	45	-	-	NULL	нет
Письмо кому	varchar	45	-	-	NULL	нет

Таблица 18 – auth_mail

Название поля	Тип данных	Длина	Ограничения	Значения по умолчанию	NULL	Индексация
Код записи	int	11	-	-	нет	да (совпадения не допускаются)
Код лога	int	11	-	1	нет	нет
Дата	date	-	-	-	NULL	нет
Время	time	-	-	-	NULL	нет
Ip-адрес	varchar	15	-	-	NULL	нет
Пользователь	varchar	20	-	-	NULL	нет

Таблица 19 – access

Название поля	Тип данных	Длина	Ограничения	Значения по умолчанию	NULL	Индексация
Код записи	int	11	-	-	нет	да (совпадения не допускаются)
Код лога	int	11	-	2	нет	нет
Дата	date	-	-	-	NULL	нет
Время	time	-	-	-	NULL	нет
Ip-адрес	varchar	15	-	-	NULL	нет
Url от	varchar	60	-	-	NULL	нет
Url кому	varchar	60	-	-	NULL	нет

Таблица 20 – auth_openfire

Название поля	Тип данных	Длина	Ограничения	Значения по умолчанию	NULL	Индексация
Код записи	int	11	-	-	нет	да (совпадения не допускаются)
Код лога	int	11	-	2	нет	нет
Дата	date	-	-	-	NULL	нет
Время	time	-	-	-	NULL	нет
Ip-адрес	varchar	15	-	-	NULL	нет
Пользователь	varchar	20	-	-	NULL	нет

Таблица 21 – vsftpd

Название поля	Тип данных	Длина	Ограничения	Значения по умолчанию	NULL	Индексация
Код записи	int	11	-	-	нет	да (совпадения не допускаются)
Код лога	int	11	-	3	нет	нет
Дата	date	-	-	-	NULL	нет
Время	time	-	-	-	NULL	нет
Ip-адрес	varchar	15	-	-	NULL	нет
Статус	varchar	20	-	-	NULL	нет

Таблица 22 – auth_ftp

Название поля	Тип данных	Длина	Ограничения	Значения по умолчанию	NULL	Индексация
Код записи	int	11	-	-	нет	да (совпадения не допускаются)
Код лога	int	11	-	3	нет	нет
Дата	date	-	-	-	NULL	нет
Время	time	-	-	-	NULL	нет
Ip-адрес	varchar	15	-	-	NULL	нет
Пользователь	varchar	20	-	-	NULL	нет

Правила ссылочной целостности не указываются, так как в данной СУБД не предусмотрены ограничения внешнего ключа. Все таблицы имеют искусственные первичные ключи и их изменение осуществляться не будет.

Схема физической модели представлена в приложении Е.

На этом завершается проектирование БД. Полученное описание позволит сохранить целостность и непротиворечивость хранящихся в ней данных, а функционал системы проектирования ERWin позволит перенести ее в SQL формат, для последующей реализации.

3 РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

После завершения этапов анализа предметной области и проектирования системы, можно приступать к непосредственной реализации системы.

Первой разрабатывается подсистема сбора данных, затем подсистема анализа. Последней идёт разработка web-интерфейса.

3.1 Разработка подсистемы сбора данных

Подсистема сбора данных представляет собой скрипт на языке программирования Python. Основной задачей, которую должна выполнять подсистема является передача log-файлов с исходных серверов на сервер разрабатываемой системы. Для выполнения этой задачи были рассмотрены несколько вариантов реализации.

Первый вариант представлял из себя создание клиент-серверного приложения на основе языка Python. Схема работы такого приложения показана на рисунке 24.

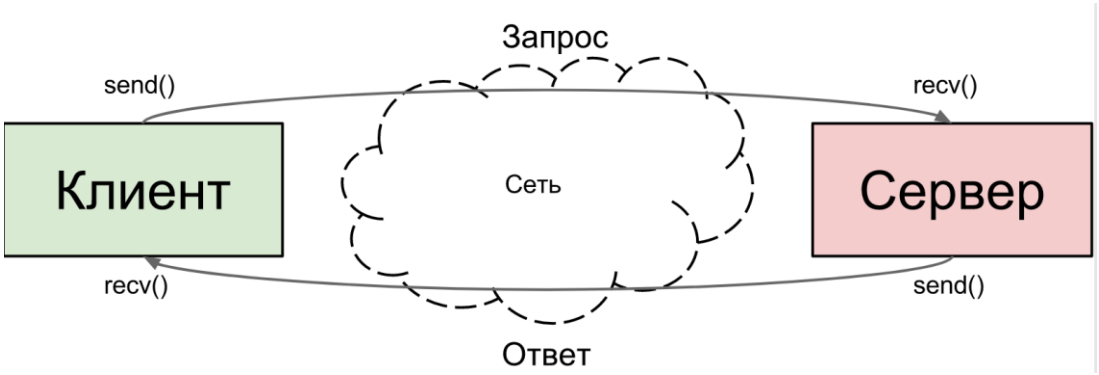

Рисунок 24 – Схема работы клиент-серверного приложения

При более детальном рассмотрении данного варианта реализации появились сложности, не позволяющие без значительных временных потерь на изучение работы клиент-серверного приложения осуществить передачу файлов данным способом. Также использование клиент-серверного приложения не безопасно, так как нет шифрования при подключении и передаче файлов.

Второй вариант реализации представляет из себя использование протокола SFTP. Согласно [8], SFTP (англ. *SSH File Transfer Protocol*) — протокол

прикладного уровня, предназначенный для копирования и выполнения других операций с файлами поверх надёжного и безопасного соединения.

Схема передачи файлов, используя протокол SFTP показана на рисунке 25.

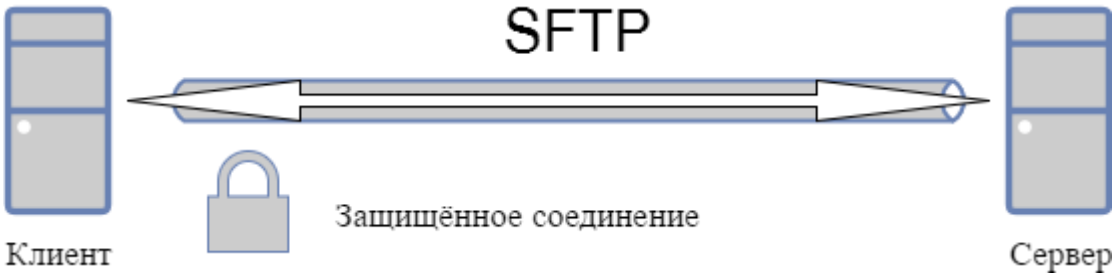

Рисунок 25 – Схема работы SFTP

Согласно [9], в ЯП Python существует модуль для работы с ssh – paramiko. Используя данный модуль, мы можем подключиться к необходимому компьютеру по безопасному протоколу ssh и передать на сервер необходимый нам файл.

Ниже представлен листинг подсистемы сбора для подключения и передачи необходимого нам файла:

```
import paramiko
ssh=paramiko.SSHClient()
ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
ssh.connect("192.168.0.106",username="name",password="pass")
ftp=ssh.open_sftp()
ftp.chdir("/var/log")
ftp.get("auth.log","/home/ubuntu/Python/transport/auth.log")
print('transport done')
```

Таким образом была реализована подсистема сбора log-файлов серверов и их передачи на сервер, на котором располагается система.

3.2 Разработка подсистемы анализа данных

Основная задача подсистемы анализа данных заключается в выделении определённой информации из log-файла и последующее занесение её в БД.

Информация в log-файлы записывается по определённым правилам. Например, рассмотрим часть содержимого log-файла почтовой службы Iredapd на рисунке 26.

Рисунок 26 – Часть log-файла Iredapd.log

Как видно на рисунке, все данные записаны строго по одному правилу: дата отправки письма, время, Ip-адрес отправителя, адрес электронной почты отправителя и получателя. Именно эти данные необходимо отправить в БД, чтобы в дальнейшем их можно было выводить в удобном виде на web-интерфейс, и, например, совершать по ним поиск.

Для поиска и отделения определенной информации (например, дата, время, Ip-адрес) воспользуемся специальными регулярными выражениями. Согласно [10], регулярные выражения (англ. *regular expressions*) — формальный язык поиска и осуществления манипуляций с подстроками в тексте, основанный на использовании метасимволов. Для поиска используется строка-образец (англ. *pattern*, по-русски её часто называют «шаблоном», «маской»), состоящая из символов и метасимволов и задающая правило поиска.

Для ЯП Python существуют свои специальные метасимволы, с помощью которых и задаётся правило для поиска. Вот полный список таких метасимволов: . ^ $ * + ? { [ ] \ | ( ).

Используя регулярные выражения и Python, разработаем подсистему для поиска всех дат, времени, Ip-адресов и адресов электронной почты.

Ниже приведён листинг регулярных выражений, осуществляющий такой поиск:

```
regexpip = r'\d{1,3}\.\d{1,3}.\d{1,3}\.\d{1,3}'
regexpemail = r'[-a-z0-9._]+@(?:[a-z0-9-A-Z]+\.)+[a-zA-z]{2,6}'
regexdate = r'\d{4}-\d{2}-\d{2}'
regextime = r'\d+:\d+:\d+'
```

Результатом выполнения этого скрипта будут массивы, которые затем необходимо записать в базу данных, причём каждый вид данных имеет своё поле в таблице в БД. Взаимодействие Python и MySql происходит благодаря Python DB-API. Согласно [11], Python DB-API – это не конкретная библиотека, а набор правил, которым подчиняются отдельные модули, реализующие работу с конкретными базами данных. Отдельные нюансы реализации для разных баз могут отличаться, но общие принципы позволяют использовать один и тот же подход при работе с разными базами данных. На рисунке 27 показаны основные методы работы Python с базами данных

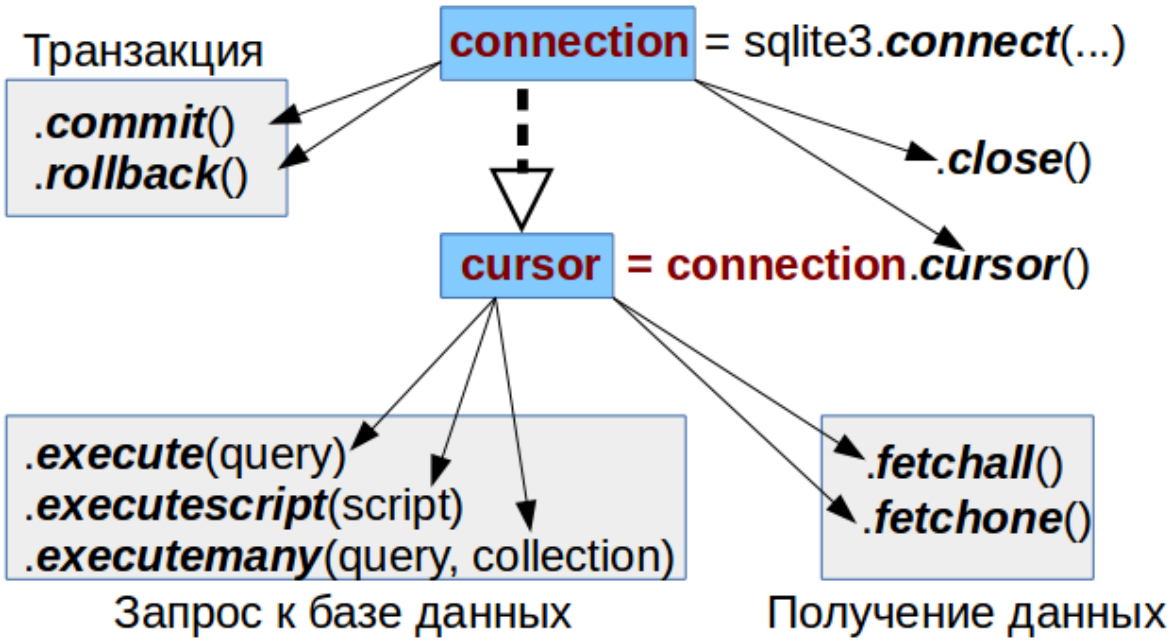

Рисунок 27 – Методы DB-API

Используя данные методы было реализовано занесение данных в БД прямо из скрипта на Python. Ниже приводится листинг работы с БД:

```
con = MySQLdb.connect(host="localhost",user="root",passwd="Qwerty123",db="alf")
cur = con.cursor()
insert = """INSERT INTO iredapd(mail_date, mail_time, ip_from, mail_from, mail_to) VALUES (%s,%s,%s,%s,%s)"""
cur.executemany(insert, data)
cur.close()
con.commit()
con.close()
```

Достигнув поставленной задачи, на этом заканчивается разработка подсистемы анализа.

3.3 Разработка графического интерфейса пользователя

Одной разработки подсистем сбора и анализа данных log-файлов недостаточно. Необходима разработка графического представления работы системы. Для этого был разработан веб-интерфейс системы. Как было обозначено в пункте 2.4.2 была использована связка вида PHP + JavaScript + MySql + Apache (веб-сервер) + браузер.

После запуска сайта мы попадаем на страницу авторизации, где необходимо ввести логин и пароль для дальнейшего использования системы. Окно авторизации показано на рисунке 28.

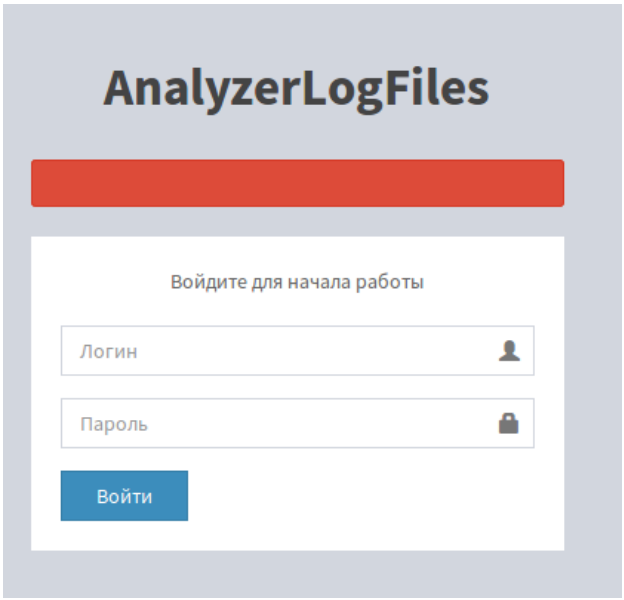

Рисунок 28 – Окно авторизации

После успешного входа в систему мы попадаем на главный экран, где подсказка сообщает нам, о необходимости выбрать нужный сервер в боковом меню. Главная страница показана на рисунке 29.

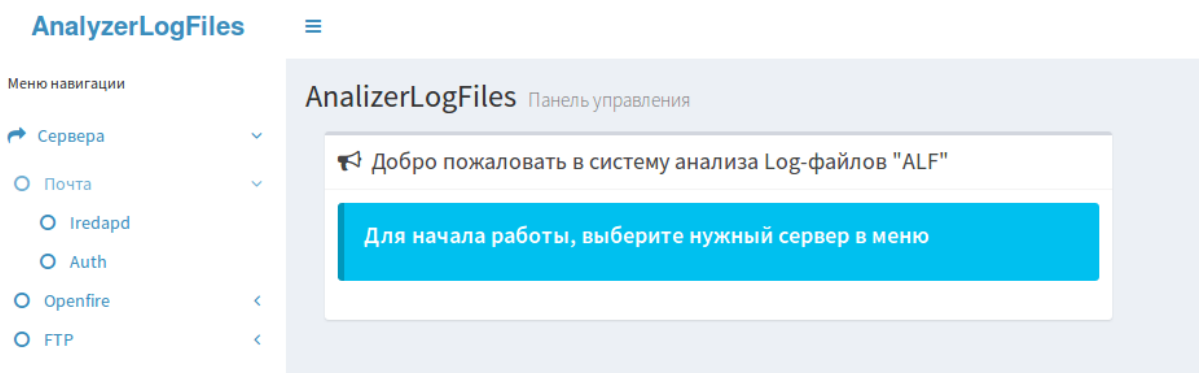

Рисунок 29 – Главная страница системы

Полной автоматизации процесса не добиться, если администратор будет вручную запускать подсистемы сбора и анализа Log-файлов. Поэтому были реализованы кнопки, выполняющие свои функции с помощью PHP+JavaScript. Они запускают на выполнение подсистемы на Python прямо из браузера администратора. На рисунке 30 показаны кнопки очистки БД, запуска подсистем сбора и анализа.

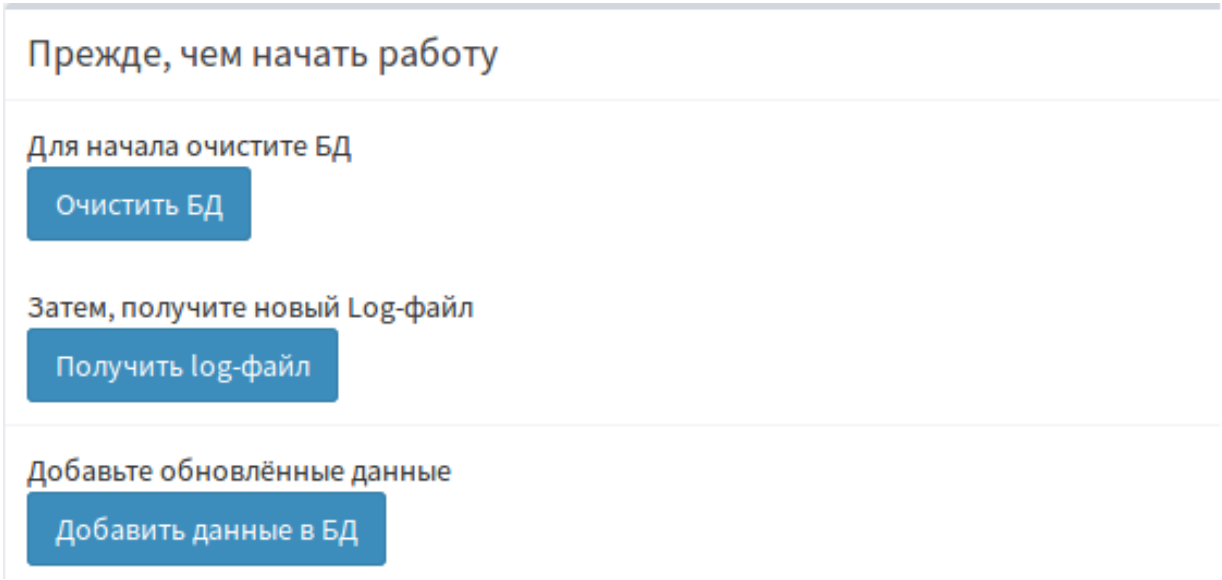

Рисунок 30 – Кнопки выполнения подсистем

После выбора сервера и необходимого log-файла, мы переходим на страницу работы с ним. На рисунках 31-33 можно посмотреть на работу log-файла авторизации серверов, показывающего последних подключившихся к серверам пользователей и их Ip-адреса.

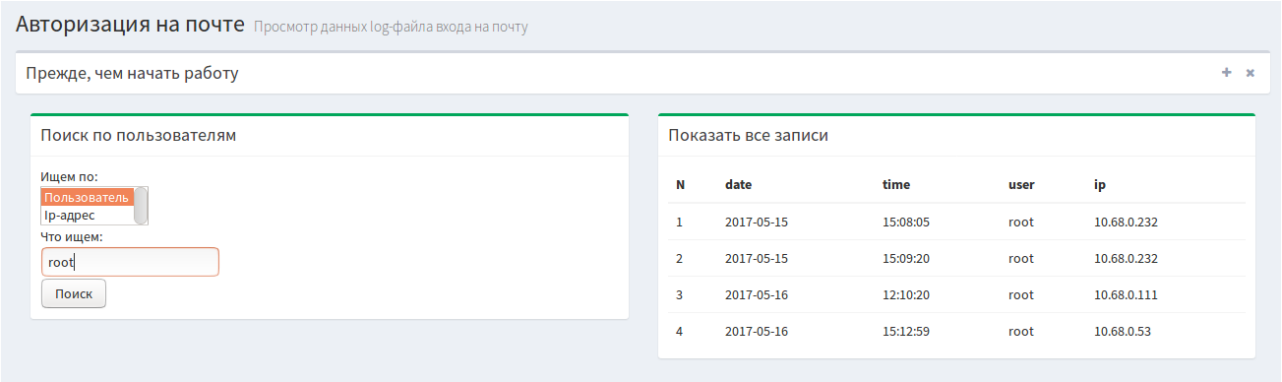

Рисунок 31 – Страница log-файла авторизации почтового сервера

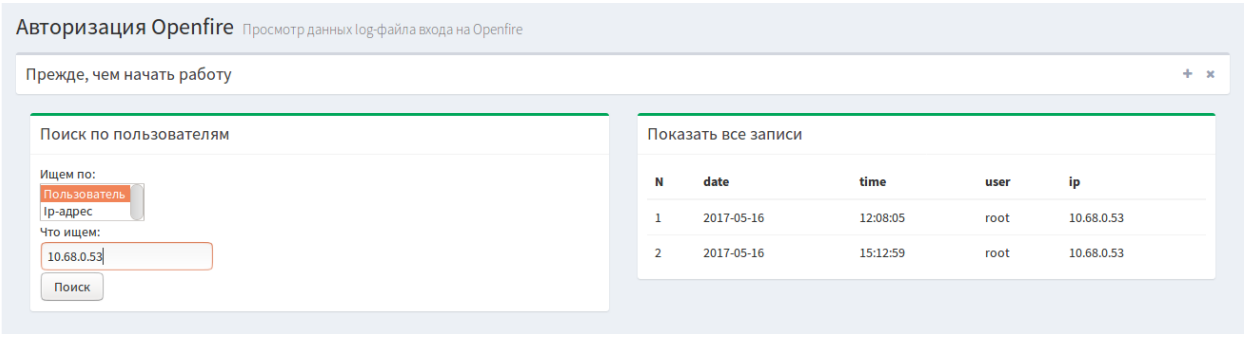

Рисунок 32 – Страница log-файла авторизации Openfire-сервера

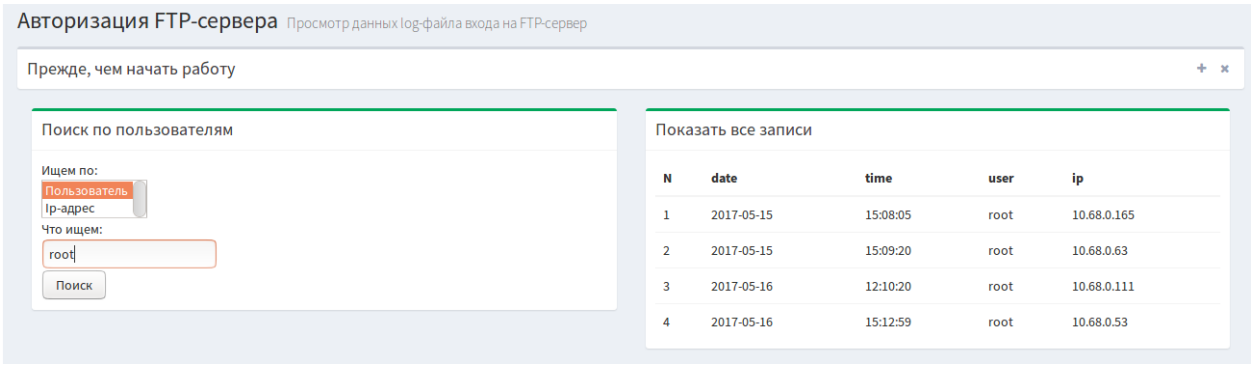

Рисунок 33 – Страница log-файла авторизации FTP-сервера

Для просмотра данных почтовой службы Iredapd, мы переходим на страницу, изображённую на рисунке 34.

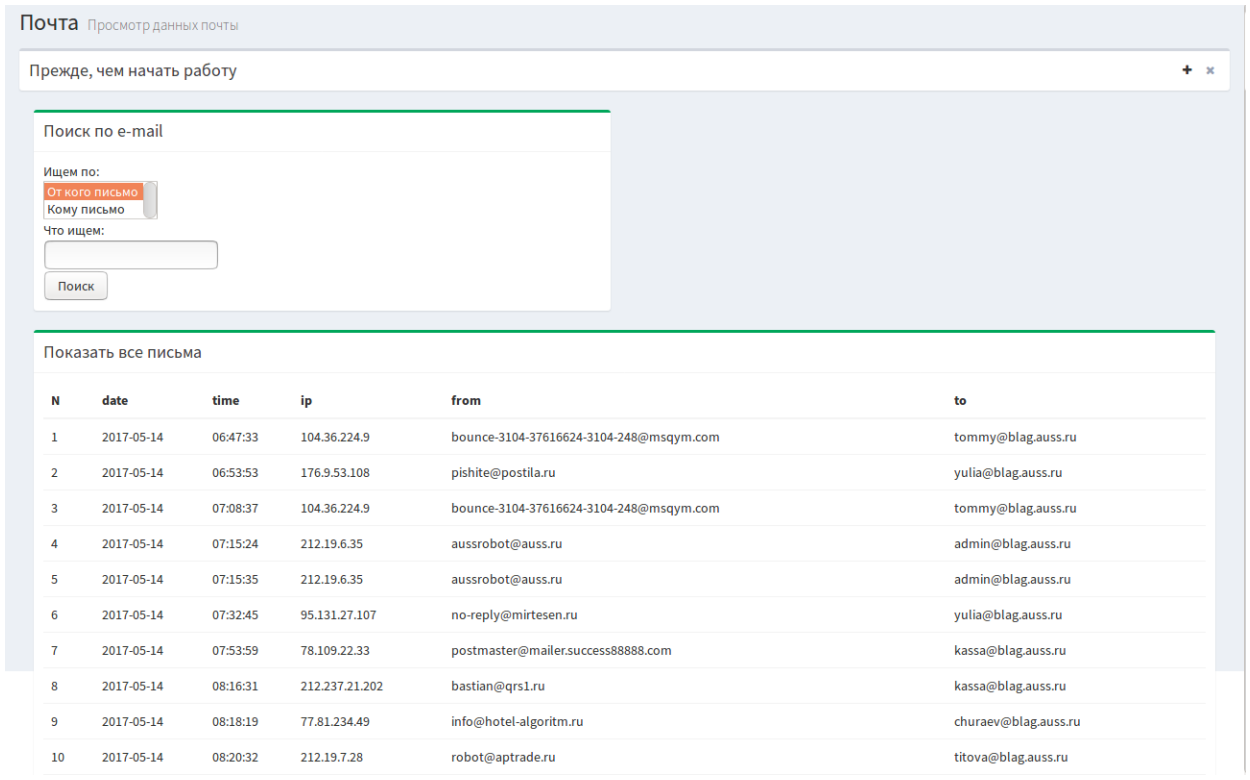

Рисунок 34 – Страница log-файла iredapd

Данные log-файла сервера Openfire, созданного службой access, показывают дату, время, Ip-адрес и URL к которому обращается пользователь. Страница этого log-файла показана на рисунке 35.

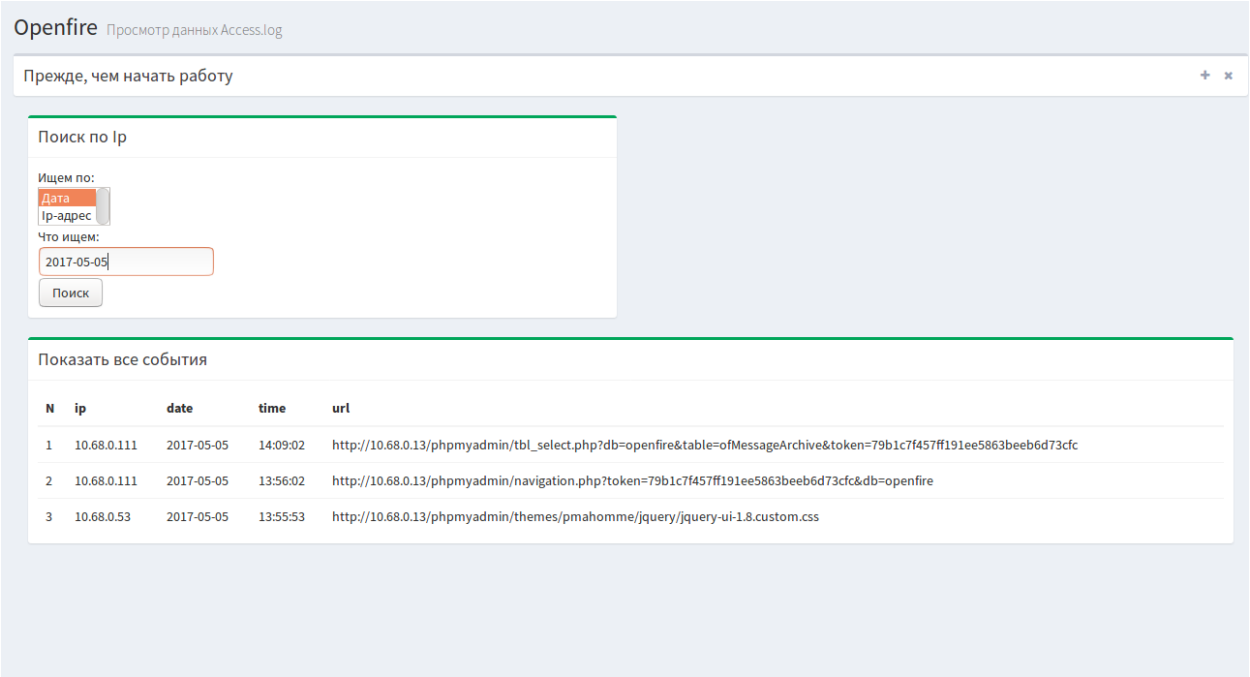

Рисунок 35 – Страница log-файла access

Данные log-файла FTP-сервера, созданного службой vsftpd, показывают дату, время, Ip-адрес и статус подключения к серверу и выгрузки файлов. Страница показана на рисунке 36.

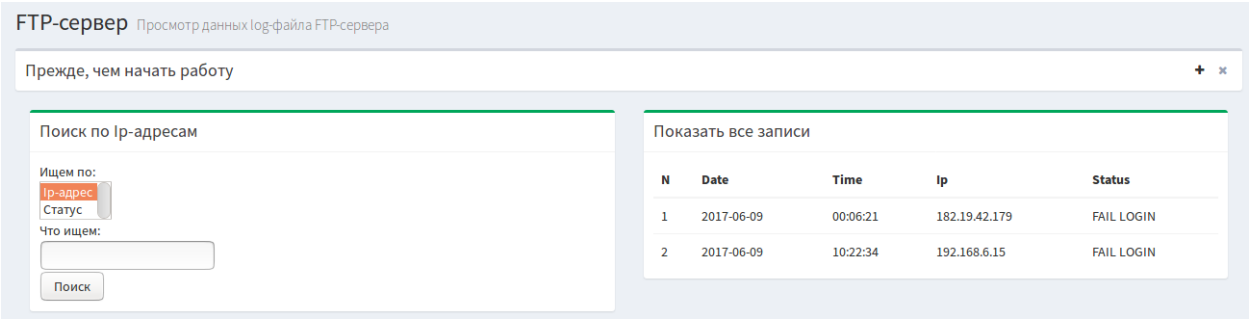

Рисунок 36 – Страница log-файла vsftpd

На этом завершается этап ознакомления с разработанной системой. Рассмотрена реализация подсистем сбора и анализа данных, а также основные данные веб-интерфейса системы.

4 БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ

4.1 Угрозы информационной безопасности

Определим основные угрозы информационной безопасности, которым может быть подвержена разработанная информационная система. Классификация угроз ИБ представлена на рисунке 37.

Рисунок 37 – Классификация угроз информационной безопасности

Согласно данной классификации рассмотрим сначала источники антропогенных угроз.

В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Антропогенные источники угроз по отношению к информационной системе могут быть как внешними, так и внутренними.

Среди внешних антропогенных источников можно выделить случайные и преднамеренные источники.

Случайные (непреднамеренные) источники могут использовать такие уязвимости, как ошибки, совершенные при проектировании информационной системы предприятия и ее элементов, ошибки в программном обеспечении;

различного рода сбои и отказы, повреждения, проявляемые в информационной системе.

Преднамеренные источники проявляются в корыстных устремлениях нарушителей. Основная цель таких источников – умышленная дезорганизация, вывод систем предприятия из строя, искажение информации за счет проникновения в информационные ресурсы предприятия путем несанкционированного доступа.

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями, и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети.

Для внутренних источников угроз особое место занимают угрозы в виде ошибочных действия и (или) нарушений требований эксплуатационной и иной документации сотрудниками учреждения.

Наибольшую опасность представляют преднамеренные угрозы, исходящие как от внешних, так и от внутренних антропогенных источников.

Техногенные источники угроз напрямую зависят от свойств техники. Данные источники также могут быть как внешними, так и внутренними.

К внешним источникам относятся инфраструктурные элементы информационных систем: средства связи (телефонные линии, линии передачи данных и т.п.), сети инженерных коммуникаций (водоснабжение, канализация, отопление и пр.).

К внутренним источникам относятся некачественные технические и программные средства обработки информации, вспомогательные средства (охраны, сигнализации, телефонии), другие технические средства, применяемые в информационных системах, а также вредоносное программное обеспечение и аппаратные закладки.

Согласно [12], стихийные источники угроз отличаются большим разнообразием и непредсказуемостью и являются, как правило, внешними по отношению к предприятию. Под ними, прежде всего, рассматриваются различные природные катаклизмы: пожары, землетрясения, ураганы, наводнения. Возникновение этих источников трудно спрогнозировать и им тяжело противодействовать, но при наступлении подобных событий нарушается штатное функционирование самой инфраструктуры предприятия и ее средств защиты, что потенциально может привести к нарушению конфиденциальности, целостности, доступности и других характеристик безопасности информации.

4.2 Характеристика атак и методы защиты

Так как разрабатываемая ИС работает в локальной сети и не доступна для подключения извне, то основные угрозы ИБ сводятся к атакам изнутри сети. Самые уязвимые места в системе – это подсистема сбора данных и веб-интерфейс.

4.2.1 Защита подсистемы сбора log-файлов.

Уязвимость этой подсистемы состоит в возможном перехвате файла при передаче его по сети. Для защиты от данной угрозы была реализована передача файлов по безопасному протоколу SFTP.

Принцип работы этого протокола состоит в следующем. Сначала устанавливается безопасное соединение с сервером посредством протокола SSH, а затем уже передаётся необходимый файл.

Протокол SSH разрабатывался для предоставления безопасности передаваемых данных путем реализации стойкого алгоритма шифрования данных, надежной системы аутентификации пользователя и сервера, предоставлением системы контроля целостности передаваемых данных, а также инкапсуляцией приложений, работающих на основе протокола TCP для установления безопасных туннелей.

На рисунке 38 показано, что при установлении SSH-сессии обеспечивается защищённый канал связи, и при использовании специальных анализаторов пакетов содержимое трафика будет зашифровано.

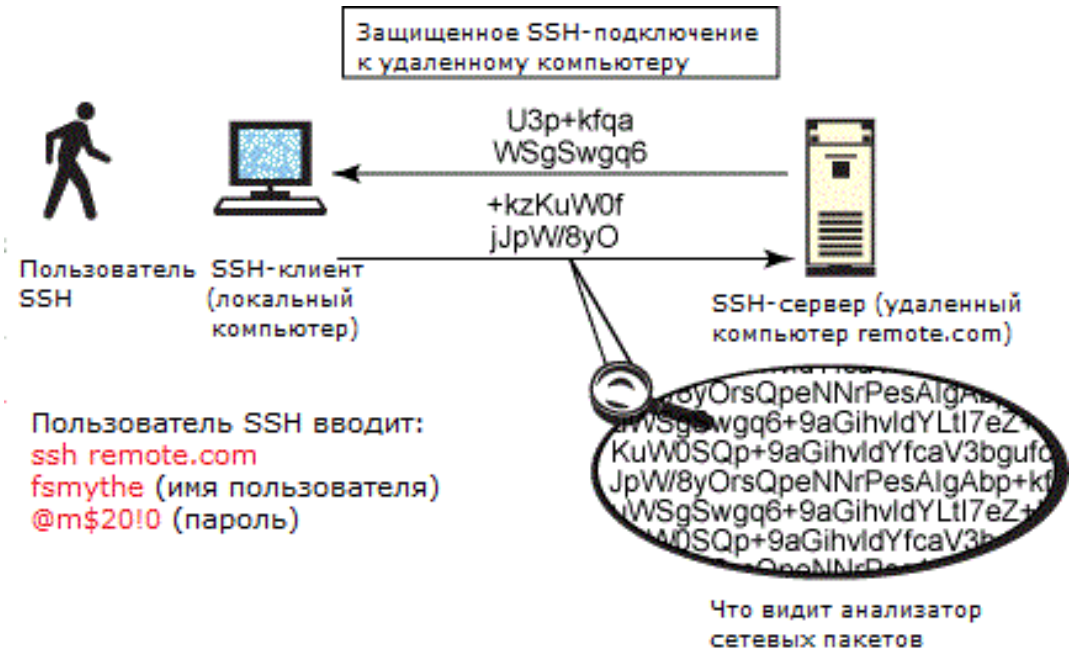

Рисунок 38 – Типовая схема SSH-подключения

Криптографическая защита протокола SSH не фиксирована, возможен выбор различных алгоритмов шифрования. Клиенты и серверы, поддерживающие этот протокол, доступны для различных платформ. Кроме того, протокол позволяет не только использовать безопасный удалённый shell на машине, но и туннелировать графический интерфейс – X Tunnelling (только для Unix-подобных ОС или приложений, использующих графический интерфейс X Window System). SSH также способен передавать через безопасный канал (Port Forwarding) любой другой сетевой протокол, обеспечивая (при надлежащем конфигурировании) возможность безопасной пересылки не только X-интерфейса, но и, например, звука.

Использование протокола SFTP обеспечивает безопасную работу подсистемы сбора log-файлов.

4.2.2 Защита веб-интерфейса.

Второе звено ИС подверженное уязвимостям ИБ – это веб-интерфейс системы. При получении доступа в систему, злоумышленник получает доступ к данным, содержащимся в log-файлах серверов, а эти данные могут содержать конфиденциальную информацию. Поэтому необходима защита веб-интерфейса от НСД.

Для предотвращения НСД подсистема аутентификации и авторизации задает идентификатор администратору при входе в систему, по нему разрешается или запрещается доступ.

Также пароли в БД хранятся в виде хешей. Таким образом, даже если злоумышленник завладеет данными из БД, он все равно не сможет узнать пароли пользователей. Для проверки введенного пароля, он шифруется тем же способом. В качестве алгоритма хэширования в данной системе используется алгоритм, предоставленной модулем шифрования паролей языка PHP, CRYPT_BLOWFISH с солью.

На этом завершается рассмотрение данного этапа. Поскольку ЗИ является комплексным и сложным процессом, который требует постоянных обновлений, нельзя говорить о полноценной защите данного приложения. Но оно имеет должный уровень защиты, от основных потенциальных угроз.

5 ЭКОЛОГИЧНОСТЬ И БЕЗОПАСНОСТЬ

Данный раздел посвящен вопросам безопасности жизнедеятельности пользователей приложения. Необходимо определить на основе санитарно-эпидемиологических норм правила работы за ПК, способы безопасной утилизации носителей информации и компонентов ИС, а также меры, позволяющие предотвратить чрезвычайные ситуации, форс-мажоры и их нежелательные последствия. Исследоваться будут 3 положения: безопасность, экологичность и защита от ЧС.

В этом разделе описаны некоторые рекомендации по организации труда при работе с ЭВМ, а также требования, представленные в СанПиН 2.2.2/2.4.1340-03.

5.1 Безопасность

5.1.1 Требования к эргономике и технической эстетике

Согласно ГОСТ Р ИСО 6385-2007 учет эргономических аспектов при построении графических интерфейсов позволит добиться оптимизации производственной нагрузки, исключить эффекты расслабления, а также снизить вероятность появления производственного стресса.

Эргономичный интерфейс должен быть логичным, интуитивно-понятным, простым и удобным для пользователя. Эргономичность интерфейса достигается:

- отказом от избыточных функций;
- структуризацией и упрощением структуры сайта;
- сокращением числа и видов элементов управления и информации, содержащейся на страницах сайта до минимально необходимых;
- выбором цветовой схемы приемлемой контрастности.

Взаимодействие пользователей с входящим в состав системы прикладным программным обеспечением осуществляется посредством web-интерфейса.

Web-интерфейс системы должен быть понятным и удобным, не должен быть перегружен графическими элементами и должен обеспечивать быстрое отображение экранных форм. Навигационные элементы должны быть выполнены в удобной для пользователя форме. Средства редактирования информации должны удовлетворять принятым соглашениям в части использования функциональных клавиш, режимов работы, поиска, использования оконной системы. Ввод-вывод данных системы, прием управляющих команд и отображение результатов их исполнения должны выполняться в интерактивном режиме.

Интерфейс должен обеспечивать удобный доступ к основным функциям и операциям системы. Все надписи экранных форм, а также сообщения, выдаваемые пользователю (кроме системных сообщений) должны быть на русском языке.

Система должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях система должна выдавать пользователю соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

Экранные формы должны проектироваться с учетом требований унификации:

- все экранные формы пользовательского интерфейса должны быть выполнены в едином графическом дизайне, с одинаковым расположением основных элементов управления и навигации;
- для обозначения сходных операций должны использоваться сходные графические значки, кнопки и другие управляющие (навигационные) элементы;
- внешнее поведение сходных элементов интерфейса (реакция на наведение указателя «мыши», переключение фокуса, нажатие кнопки) должны реализовываться одинаково для однотипных элементов.

От цветового оформления системы зачастую зависит визуальный опыт работы с приложением.

Наиболее активными для привлечения внимания являются красный и синий цвета, далее желтый, зеленый и белый. Поэтому красный и синий рекомендуется применять для кодирования наиболее важных объектов. Синий цвет из-за его тенденции к размытости границ малопригоден для окраски мелких графических элементов, требующих предельной четкости изображения.

Цвета по яркости и контрастности не должны выходить за пределы, вызывающие утомление зрения. Пониженная светимость изображения вызывает перенапряжение мышц хрусталика глаза и, как следствие, снижение остроты зрения. Повышенная яркость приводит к снижению цветовой чувствительности.

Существует определенное количественное соотношение между изображением и фоном («равновесие» фигуры и фона), характеризующее оптимальную для восприятия величину изображения – его масштаб.

Масштаб не должен быть, с одной стороны, слишком мелким, чтобы объект не терялся в отведенном ему поле экрана, а с другой - чересчур крупным, чтобы не возникало ощущение «тесноты» на экране.

Величина оптимального масштаба зависит от выбранной цветовой гаммы. Изображение, построенное на насыщенных цветах, резко контрастирующих по яркости с фоном, «требует» меньшего размера, чем изображение с нюансными отношениями по яркости и насыщенности.

5.1.2 Требования к освещению

Помещения для эксплуатации ЭВМ должны иметь естественное и искусственное освещение. Эксплуатация ЭВМ в помещениях без естественного освещения допускается только при соответствующем обосновании и наличии положительного санитарно-эпидемиологического заключения, выданного в установленном порядке. Естественное и искусственное освещение должно соответствовать требованиям нормативной документации.

Окна в помещениях, где эксплуатируется вычислительная техника, в основном должны быть ориентированы на север и северо-восток. Оконные проемы должны быть оборудованы регулируемыми устройствами типа: жалюзи, занавесей, внешних козырьков и др.

Искусственное освещение в помещениях для эксплуатации ЭВМ должно осуществляться системой общего равномерного освещения. Освещение не должно создавать бликов на поверхности экрана. В качестве источников света при искусственном освещении следует применять преимущественно люминесцентные лампы типа ЛБ и компактные люминесцентные лампы (КЛЛ). При устройстве отраженного освещения в производственных и административно-общественных помещениях допускается применение метало-галогенных ламп.

5.2 Экологичность

Данный аспект рассмотрим с точки зрения сбора и утилизации отходов в виде ЭВМ, их составных частей, вспомогательного оборудования и оргтехники. ФЗ № 89 от 24.06.1998 г. является основным в вопросах регулирования обращения с отходами производства и потребления с целью предотвращения вредного воздействия отходов на здоровье человека и окружающую среду.

В данном НПА определяется разделение отходов на классы опасности. Всего определенно 5 классов опасности. В Федеральном классификационном каталоге отходов выделены отдельные технические средства и их комплектующие. Для многих из них неопределенны классы, и они устанавливаются в частном порядке. Например, системный блок компьютера определяется, как изделие из нескольких материалов, и имеет класс опасности – IV (малоопасные отходы). Аккумуляторы ноутбуков имеют класс опасности – II (высокоопасные отходы) и т.д.

В целом утилизация ЭВМ комплексный и сложный процесс, поэтому его стоит рассмотреть с разных сторон.

Во-первых, наиболее простым этот процесс представляется для физических лиц. Им необходимо обратиться в организацию, занимающуюся непосредственно утилизацией отходов. Такие организации должны пройти обязательное лицензирование своей деятельности.

Для юридических лиц этот процесс намного сложнее. Он также основан на передаче вычислительных средств сторонней организации, но этому должен предшествовать этап списания аппаратного оборудования. Списание оборудования сопровождается оценкой их экологических свойств штатным или приглашенным экспертом, который составляет паспорт отходов оргтехники и компьютеров (вычислительной техники). Соответственно, организации выгоднее накапливать единицы непригодной в работе техники, а затем утилизировать ее в больших объемах. После этого она передается специализированной организации по утилизации.

Отдельно стоит отметить утилизацию информации на носителях и компонентах ЭВМ. Данным вопросом может заниматься как сторонняя организация, так и владелец техники. Способы и требования по уничтожению информации с носителей описываются в ГОСТ Р 50739-95, а также в РД от 30.03.1992 1 и 2, защита от НСД к информации. Согласно этим нормативам уничтожение может производиться, как с помощью блокирования доступа к информации на носителях, ее затиранию, а также дополнительным включением маскирующей информации.

Наличие в компонентах ЭВМ технического золота или других драгоценных металлов накладывает на организацию дополнительную ответственность. Эти аспекты регулируются законодательством в соответствие с ФЗ № 41. Несоблюдение данных требований может повлечь административную ответственность.

5.3 Аспект пожарной безопасности при работе с ЭВМ

Согласно Нормам пожарной безопасности НПБ 105-03, помещения с ЭВМ и ПЭВМ относятся к категории В (пожароопасные). Согласно СНиП 21-01-97, вычислительные центры должны располагаться в зданиях не ниже II

степени огнестойкости, залы ЭВМ – не ниже первого этажа (допускается III степень огнестойкости). Наиболее вероятные классы пожаров в помещениях с ПЭВМ - «А» и «Е» (т.е. могут гореть в основном твердые вещества, горение которых сопровождается тлением - класс А; или возможны пожары, вызванные возгоранием электроустановок -класс Е).

Специфика эксплуатации ЭВМ подразумевает наличие большого количества электрических приборов, токопроводящих кабелей и высоких нагрузок на электросеть. Поэтому их установка, эксплуатация, техническое обслуживание, проверка, замена и утилизация должны соответствовать принятым законодательным нормам и стандартам.

Хранение технических средств должно осуществляться в закрытых контейнерах для предотвращения накопления пыли в их составных частях.

При эксплуатации ЭВМ и оргтехники необходимо проверять целостность токопроводящих кабелей, вилки и розетки, отсутствие повреждений аппаратуры.

Компоненты ЭВМ должны иметь функцию самоотключения при повышении температуры входе неисправности систем охлаждения и кондиционирования. Для предотвращения перегрева.

Так же в помещениях, оборудованных ЭВМ, необходима установка средств пожаротушения. К таким средствам относятся огнетушители различных конструкций: порошковые (ПСБ, ПФ, ОП), пенные (ОХП- 10), углекислотные (ОУ-2, ОУ-5). Так же распространение получили установки водяного, пенного и газового пожаротушения.

Таким образом, в данном разделе мы рассмотрели основные вопросы, связанные обеспечением БЖД при использовании ЭВМ. Подробны рассмотрели темы эргономичного проектирования интерфейсов взаимодействия с пользователем, проблемы утилизации ЭВМ, ее компонентов и вспомогательной техники, а также вопросы обеспечения пожарной безопасности.

ЗАКЛЮЧЕНИЕ

Выполнение работ в ходе выполнения выпускной квалификационной работы позволило создать систему анализа log-файлов серверов.

Этапы по анализу предметной области, проектированию информационной системы, разработке программного приложения, исследования вопросов информационной безопасности и рассмотрении аспектов безопасности жизнедеятельности определили следующие результаты:

– исследована предметная область предприятия;

– обоснована цель создания приложения;

– проанализированы, дополнены и оформлены требования к будущему приложению;

– рассмотрен стэк технологий разработки и выбраны наиболее подходящие из них;

– выявлены функциональные и обеспечивающие подсистемы;

– разработан проект БД;

– реализованы функциональные подсистемы;

– выполнена реализация БД в СУБД;

– согласно проектному описанию разработана система на языках программирования;

– исследованы угрозы ИБ, а также меры противодействия им;

– рассмотрены вопросы проектирования эргономичного графического интерфейса пользователя, утилизации ПК, их компонентов, оргтехники и комплектующих, а также вопросы противопожарной безопасности при работе с ЭВМ.

В совокупности были выполнены все поставленные для бакалаврской работы задачи.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Бьюли, А. Изучаем SQL / Пер. с англ. – М. Издательство «Символ-Плюс» 2013. – 312 с.

2 Википедия [Электронный ресурс]: офиц. сайт. – 15.01.2001 – Режим доступа: https://ru.wikipedia.org/wiki/Линейная_организационная_структура. - 04.06.2017.

3 Бизли, Д. Python. Подробный справочник / Пер. с англ. – М. Издательство «Символ-Плюс» 2014. – 864 с.

4 Жигулин, Г.П., Новосадов, С.Г. Информационная безопасность / Жигулин Г.П., Новосадов С.Г. – СПб: СПб ГУ ИТМО, 2014. – 560 с.

5 Маклафлин, Б. PHP и MySQL. Исчерпывающее руководство / Пер. с англ – СПб.: Питер, 2013. – 512 с.

6 Марк, Лутц Изучаем Python. / Пер. с англ. – М. Издательство «Символ-Плюс» 2011. – 1280 с.

7 Марк, Лутц Программирование на Python, 4-е издание. / Пер. с англ. – М. Издательство «Символ-Плюс» 2011. – 992 стр.

8 Олифер, В.Г. Компьютерные сети 3-е издание / Олифер В.Г. – СПб СПб.: Питер, 2012. – 960 с.

9 Сейед, Тахагхогхи Руководство по MySQL / Пер. с англ. – М. Издательство «Русская Редакция» 2007. – 544 с.

10 Тузовский, А.Ф. Проектирование и разработка web-приложений учебное пособие / Тузовский А.Ф. – Томск: Томский политехнический университет, 2014. – 219 с.

11 Флэнаган, Д. JavaScript. Подробное руководство, 6-е издание. – Пер. с англ. – СПб: Символ-Плюс, 2012. – 478 с.

12 Фримен, Э. Изучаем программирование на HTML5 / Фримен Э. – СПб.: Питер, 2013. – 251 с.

13 Чепак Л. В., Масловская А. Г. Разработка и реализация баз данных: методическое руководство к курсовому проектированию / Л.В. Чепак, А.Г. Масловская. – Благовещенск: Изд-во АмГУ, 2011. – 56 с.

14 Шаньгин В.Ф. Информационная безопасность и защита информации / Шаньгин В.Ф. – Саратов: Профобразование, 2017. – 702 с.

15 IBM developerWorks©: офиц. сайт. – Режим доступа: https://www.ibm.com/developerworks/ru/. - 04.06.2017.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1 Отчет о прохождении производственной практики на предприятии ООО «Компания АЮСС».

2 Официальный сайт ООО «Компания АЮСС» [Электронный ресурс]: офиц. сайт. URL: http://au-ss.ru/blog/o-kompanii/(дата обращения 10.06.17).

3 Отчет о прохождении производственной практики на предприятии ООО «Компания АЮСС», с.5.

4 XMPP: статья (дата опубликования 20.02.2016) // Википедия: офиц. сайт. 15.01.2001. URL: https://ru.wikipedia.org/wiki/XMPP (дата обращения 10.06.17).

5 Файл регистрации: статья (дата опубликования 26.04.2017) // Википедия: офиц. сайт. 15.01.2001. URL: https://ru.wikipedia.org/wiki/Файл_регистрации (дата обращения 10.06.17).

6 Python - обзор: статья (дата опубликования 17.01.2015) // Pythonic way: офиц. сайт. URL: http://pythonicway.com/python-overview (дата обращения 10.06.17).

7 Марк, Лутц Изучаем Python. / Пер. с англ. – М. Издательство «Символ-Плюс» 2011. – 1280 с.

8 SFTP: статья (дата опубликования 26.04.2017) // Википедия: офиц. сайт. 15.01.2001. URL: https://ru.wikipedia.org/wiki/SFTP (дата обращения 10.06.17).

9 Работа с shh в Python: статья (дата опубликования 27.07.2012) // Habrahabr: офиц. сайт. URL: https://habrahabr.ru/post/150047/ (дата обращения 10.06.17).

10 Регулярные выражения: статья (дата опубликования 26.04.2017) // Википедия: офиц. сайт. 15.01.2001. URL: https://ru.wikipedia.org/wiki/Регулярные_выражения (дата обращения 10.06.17).

11 Python: Работа с базой данных, часть 1/2: Используем DB-API: статья (дата опубликования 14.02.2017) // Habrahabr: офиц. сайт. URL: https://habra-habr.ru/post/321510/ (дата обращения 10.06.17).

12 Угрозы информационной безопасности: статья (дата опубликования 20.03.2017) // Википедия: офиц.сайт. 15.01.2001. URL: https://ru.wikipedia.org/wiki/Угрозы_информационной_безопасности (дата обращения 10.06.17).

ПРИЛОЖЕНИЕ А

Схема организационная линейная структура предприятия ООО «Компания АЮСС»

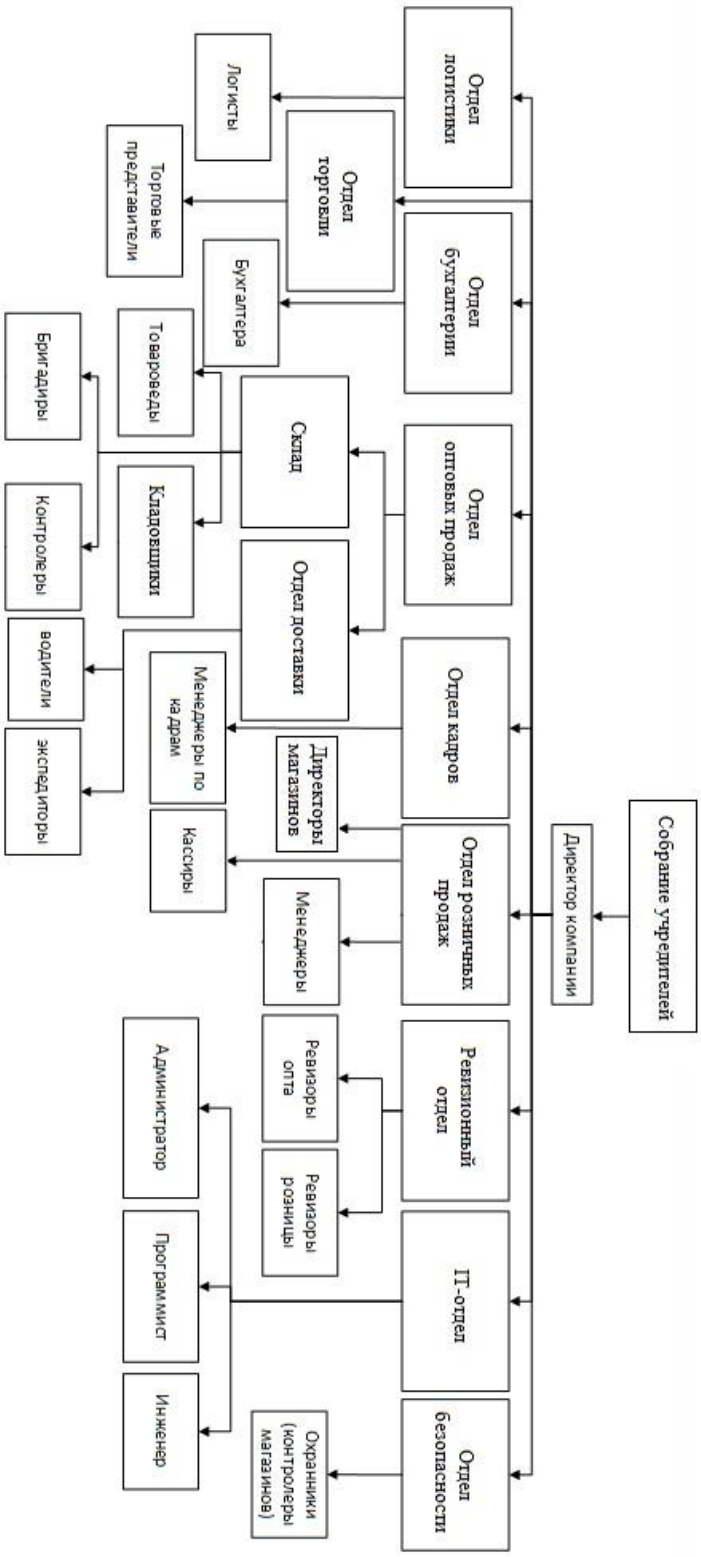

Рисунок А.1 – Организационная линейная структура предприятия

ПРИЛОЖЕНИЕ Б

Схема потоков данных для предприятия ООО «Компания АЮСС»

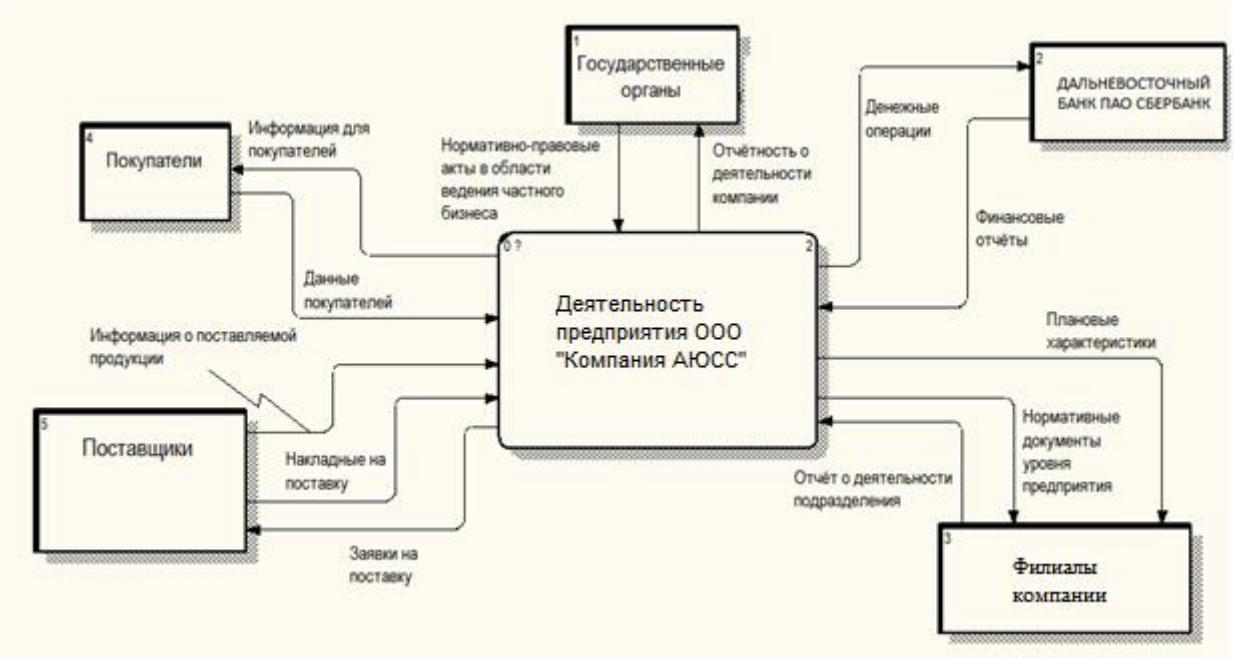

Рисунок Б.1 – Внешний документооборот

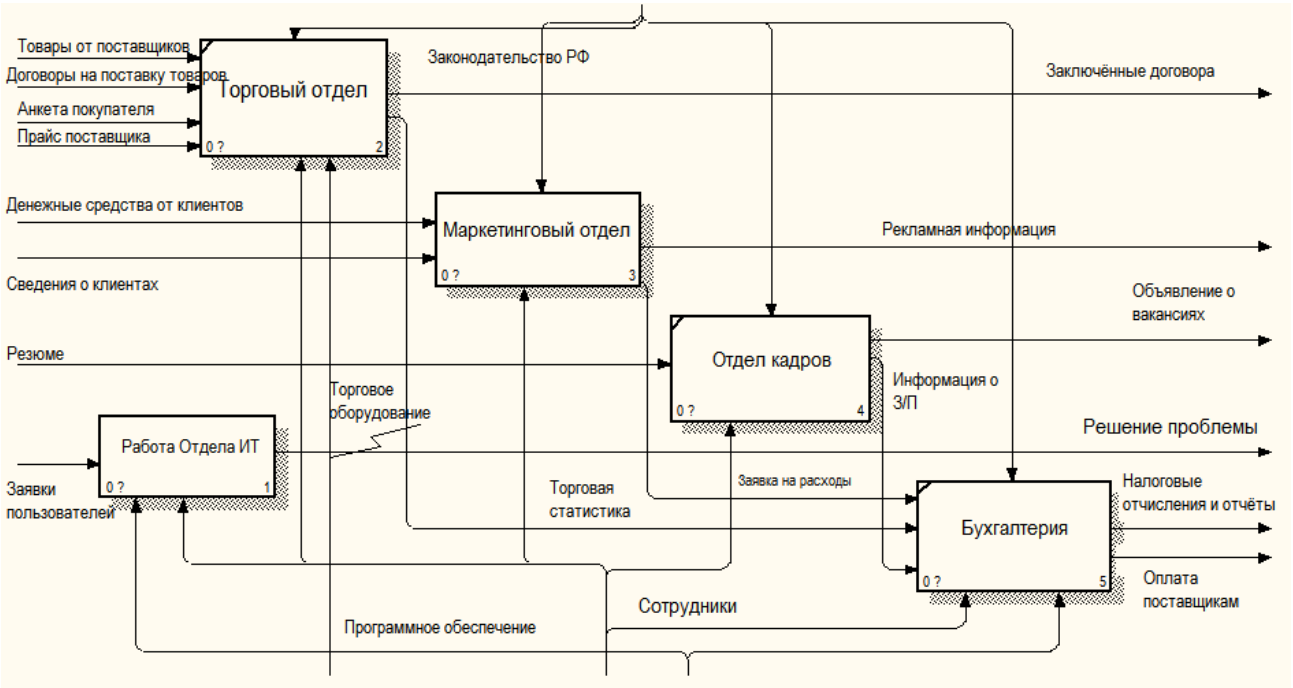

Рисунок Б.2 – Внутренний документооборот предприятия ООО «Компания АЮСС»

ПРИЛОЖЕНИЕ В

Техническое задание

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Полное наименование системы

Полное наименование разрабатываемой информационной системы: Разработка системы анализа log-файлов серверов в локальной сети предприятия ООО «Компания АЮСС»

1.2 Код темы или код (номер) договора

Код системы:

Код договора:

1.3 Наименование предприятий (объединений) разработчика и заказчика (пользователя) системы и их реквизиты

Разработчик: Левковец Михаил Андреевич

Реквизиты разработчика:

Название учреждения разработчика: ФГБОУ ВО «АмГУ»

Юридический Адрес разработчика: 675027, Амурская область, г. Благовещенск, Игнатьевское шоссе, 21.

Телефон разработчика: 8(924)1497713

E-mail разработчика: lev-1995@mail.ru

Заказчик: ООО «Компания АЮСС»

Реквизиты заказчика: ИНН 2725021724, ОГРН 1022701404032

Название учреждения заказчика: Общество с ограниченной ответственностью «Компания АЮСС»

Юридический Адрес заказчика: 675000, Амурская область, г. Благовещенск, Северо-Западный Промышленный узел, Литер А

Офис заказчика: 675000, Амурская область, г. Благовещенск, Северо-Западный Промышленный узел, Литер А

Телефон заказчика: 8 (416) 235-02-98

E-mail заказчика: admin@blag.auss.ru

1.4 Основания для проведения работ

Основание для проведения работ обусловлено заявкой на создание информационной системы.

1.5 Плановые сроки начала и окончания работы

Срок начала работ: 06 сентября 2016 года.

Срок окончания работ: июнь 2017 года.

В процессе разработки сроки могут быть уточнены.

1.7 Порядок оформления и предъявления заказчику результатов работ

Работы по созданию системы сбора и анализа log-файлов серверов предприятия. Заказчику предоставляется итоговый программный продукт, а также его описание в виде проектных документов, схем и диаграмм.

2 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

2.1 Назначение системы

Система анализа данных предназначена для упрощения получения, обработки и представления в удобном виде данных log-файлов серверов.

2.2 Цели создания системы

Целью создания данной информационной системы облегчения деятельности системного администратора по контролю и защите данных на серверах предприятия.

Так же внедрение системы позволит добиться:

– своевременного обнаружения несанкционированного доступа к серверам;

– упрощения работы системного администратора;

– уменьшение времени на сбор и обработку информации о состоянии серверов.

Продолжение ПРИЛОЖЕНИЯ В

3 ХАРАКТЕРИСТИКА ОБЪЕКТОВ АВТОМАТИЗАЦИИ

3.1 Краткие сведения об объекте автоматизации

Объектом автоматизации для организации является веб-приложение для ПК. Подсистема будет установлена на компьютер и позволит оптимизировать деятельность системного администратора. Для контроля нормального функционирования системы необходим администратор, в обязанности которого входит:

– наблюдение и анализ;

– мониторинг работы приложения, выявление и устранение технических ошибок;

3.2 Сведения об условиях эксплуатации и о характеристике окружающей среды

Система будет располагаться на сервере предприятия, который должен функционировать в режиме 24/7. Эксплуатационные характеристики от окружающей среды не зависят.

4 ТРЕБОВАНИЯ К СИСТЕМЕ

4.1 Требования к системе в целом

4.1.1 Требования к структуре и функционированию системы

Система анализа должна быть централизованной, то есть все данные должны располагаться в центральном хранилище.

В системе выделяются следующие функциональные подсистемы:

– подсистема идентификации, аутентификации и авторизации, которая позволит однозначно определить работающего в системе администратора;

– подсистема сбора данных;

– подсистема обработки данных, которая позволит агрегировать информацию;

– подсистема работы базы данных;

– подсистема графического интерфейса пользователя;

Система должна функционировать в основном режиме работы. В нём система должна обеспечивать выполнение всех своих функций и быть доступна администратору для работы 24 часа в день, 7 дней в неделю (24x7).

4.1.2 Требования к численности и квалификации персонала системы

Для подержания работоспособности и эксплуатации системы на этапе ее функционирования необходим, как минимум один квалифицированный специалист – администратор.

Для эксплуатации системы администратору необходимо соответствовать следующей квалификации:

– уверенный пользователь ПК, опыт системного и сетевого администрирования, работа с СУБД (MYSQL), знание основ ООП, опыт в программировании на языках программирования, умение делать резервные копии БД, а также восстанавливать систему при сбоях.

4.1.3 Требования к надежности

Режим работы системы (24x7) накладывает на систему условие обеспечения высокой отказоустойчивости, что должно достигаться за счет применения организационно-технических мероприятий.

Заданный уровень надежности должен обеспечиваться за счет:

– своевременного выполнения процессов администрирования системы;

– поддержания соответствия уровня квалификации персонала заданным требованиям;

– соблюдения правил эксплуатации и технического обслуживания применяемых программно-технических средств;

– выполнения периодического снятия резервных копий на отчуждаемые носители БД и системы.

Во время работы системы возможно возникновение следующих аварийных ситуаций:

– ошибки работы системы, не выявленные на этапе тестирования;

– сбои в электропитании компьютера, на котором располагается подсистема;

4.1.4 Требования к безопасности

Для обеспечения безопасности работы системы, необходимо выполнять проверку авторизации администратора. Проверку необходимо осуществлять в следующих направлениях:

– ошибки ввода данных, вызванные человеческим фактором;

– вредоносный программный код и скрипты;

– умышленно искаженные данные.

4.1.5 Требования к эргономике и технической эстетике

Основное назначение данной системы состоит во взаимодействии с пользователем, поэтому экранные формы и интерфейс должны быть интуитивно понятны, обладать общим дизайном и не содержать, раздражающих глаз элементов. Все надписи, предоставляемые пользователю, должны быть представлены на русском языке.

При возникновении сбоев в работе системы сообщения об ошибках должны быть оформлены соответственно общему оформлению системы.

4.1.6 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы

Условия эксплуатации, а также виды и периодичность обслуживания технических средств системы должны соответствовать требованиям по эксплуатации, техническому обслуживанию, ремонту и хранению, изложенным в документации завода-изготовителя (производителя) на них.

4.1.7 Требования к защите информации от несанкционированного доступа

Обеспечение защиты информации в системе должно происходить на всех этапах взаимодействия с информацией (сбор, обработка, передача, хранение и т.д.).

Модули обеспечения защиты информации не должны существенно ухудшать основные функциональные характеристики системы.

Для обеспечения защиты информации от несанкционированного доступа все взаимодействия в системе должны вестись от лица конкретного, однозначно идентифицируемого пользователя.

Доступ к БД из СУБД должен осуществляться на основании пользователей СУБД, для которых должны быть разграничены команды взаимодействия по принципу "что не разрешено, то запрещено".

4.1.8 Требования по сохранности информации при авариях

Для обеспечения сохранности информации при авариях и возможности восстановления после сбоев, должно производиться периодическое резервное копирование информации, содержащейся в БД, а также копирование состояний самой системы на отчуждаемые носители.

4.1.9 Требования к защите от внешней среды

Технические средства, обеспечивающие функционирование системы, должны быть надежно защищены от вредоносных внешних воздействий, способных вывести из строя части программно-аппаратного комплекса, в частности от перепадов электрического напряжения, от физических воздействий и излучения.

4.1.10 Требования к стандартизации и унификации

При проектировании подсистемы должны быть учтены следующие стандарты:

ГОСТ 19.001-77 общие положения;

ГОСТ 19.004-80 термины и определения;

ГОСТ 19.101-77 виды программ и программных документов;

ГОСТ 19.102-77 стадии разработки;

ГОСТ 19.103-77 обозначение программ и программных документов;

ГОСТ 19.104-78 основные надписи;

ГОСТ 19.105-78 общие требования к программным документам;

ГОСТ 19.106-78 требования к программным документам, выполненным печатным способом;

ГОСТ 19.402-78 описание программы;

ГОСТ 19.502-78 описание применения. Требования к содержанию и оформлению;

ГОСТ 19.505-79 руководство оператора. Требования к содержанию и оформлению;

ГОСТ 19.508-79 руководство по техническому обслуживанию. Требования к содержанию и оформлению;

ГОСТ 34.602-89 техническое задание на создание автоматизированной системы);

ГОСТ 34.201-89 виды, комплектность и обозначение документов при создании автоматизированных систем;

ГОСТ 24.104-85 автоматизированные системы управления. Общие требования;

ГОСТ 34.601-90 автоматизированные системы. Стадии создания.

ГОСТ 25.861-83 АСУ. Требования по безопасности средств вычислительной техники.

Разработка системы должна осуществляться с использованием стандартных методологий функционального моделирования: IDEF0, IDEF3, DFD, UML и информационного моделирования IE и IDEF1X в рамках рекомендаций по стандартизации Р50.1.028-2001 «Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования».

Моделирование должно выполняться в рамках стандартов, поддерживаемых программными средствами моделирования ERWin 4.x и BPWin 4.x.

Для работы с БД должнен использоваться язык запросов SQL в рамках стандарта ANSI SQL-92.

Для разработки подсистем сбора и анализа данных должен использоваться язык программирования Python.

Для разработки пользовательских интерфейсов и средств генерации отчетов должны использоваться языки программирования HTML 5, CSS 3, JavaScript.

4.2 Требования к функциям, выполняемым системой

4.2.1 Подсистема идентификации, аутентификации и авторизации

Данная подсистема решает задачи:

а) присвоение администратору уникального идентификатора;

б) подтверждение повторного входа в систему на основе идентификатора и пароля;

в) предоставление функций работы с системой на основе роли пользователя и администратора;

Временной регламент доступности функций подсистемы - весь период работы системы, при необходимости вызова задач.

Форма представления выходной информации – данные в структурах БД.

Характеристики точности и времени выполнения – функции доступны с момента запуска системы, время выполнения функций должно быть не заметно пользователю и не превышать 4 секунд.

4.2.2 Подсистема сбора данных

Данная подсистема решает задачи:

а) передача log-файлов на сервер по сети;

Временной регламент доступности функций подсистемы - весь период работы системы, при отправке системой данных на сервер.

Форма представления выходной информации – исходные данные, хранимые на сервере.

Характеристики точности и времени выполнения – функции доступны с момента запуска системы, время выполнения функций должно быть не заметно пользователю и не превышать 4 секунд.

4.2.3 Подсистема анализа данных

Данная подсистема решает задачи:

а) обработки и анализа данных, полученных с сервера;

Форма представления выходной информации – представление информации в графическом интерфейсе пользователя.

Характеристики точности и времени выполнения – функции доступны с момента запуска системы, время выполнения функций должно быть не заметно пользователю и не превышать 4 секунд.

4.3 Требования к видам обеспечения

4.3.1 Требования к программному обеспечению

Сервер должен содержать следующее программное обеспечение:

– СУБД MySQL 5.6 и выше;

– интерпретатор PHP 5.5 и выше;

– установленный пакет языка программирования Python 2.x;

– средства резервного копирования и восстановления.

Клиент для работы с системой должен также иметь установленный веб-браузер.

4.3.2 Требования к лингвистическому обеспечению

Для проектирования данной системы должны быть использованы нотации IDEF0, IDEF1.X, IDEF3, DFD, ERD и UML.

Для разработки дизайна системы должны быть использованы языки программирования HTML, CCS, JavaScript.

Для разработки функционала системы должны быть использованы языки программирования PHP, JavaScript, Python.

Для организации взаимодействия с БД должен быть использован язык SQL.

Кодирование данных в системе и БД должно осуществляться в кодировке Unicode – utf-8.

4.3.3 Требования к техническому обеспечению

Сервер, на котором будет располагаться система, должен соответствовать следующим требованиям:

– процессор на архитектуре x64 (Intel или AMD) от 1,5 ГГц, для достижения нормального уровня производительности работы системы;

– оперативная память от 4 Гбайт, для достаточного уровня быстродействия подсистемы;

– 1 HDD для обеспечения сохранности информации

– встроенный сетевой интерфейс Ethernet 1000 Мбит/с.

4.3.4 Требования к организационному обеспечению

Эксплуатацией и обслуживанием системы занимается техническое подразделение Заказчика.

Состав сотрудников, администрирующих систему определяется штатным расписанием Заказчика, которое, в случае необходимости, может изменяться.

4.3.5 Требования к метрологическому обеспечению

Автоматическая синхронизация времени всех подсистем от сервера.

4.3.6 Требование к методическому обеспечению

Требования к методическому обеспечению не предъявляются.

5 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ

5.1 Перечень стадий и этапов работ по созданию системы

Создание системы должно быть сопряжено со следующими этапами:

1 этап – Анализ деятельности компании. Данный этап включает: исследование общей организационной структуры и ее основных характеристик, а также анализ, используемых в организации программно-технических средств.

По окончании данного этапа будут принято решение об необходимости создания системы, поставлена задача разработки, а также разработаны контекстные диаграммы, диаграммы потоков данных и другие схемы.

2 этап – Составление технического задания. Данный этап включает: выяснение требований заказчика к разрабатываемой системе, определение технических и программных средств, необходимых для реализации проекта, уточнение функций системы. В результате должно быть разработано Техническое Задание на разработку данной системы.

3 этап – Проектирование БД. Этап состоит из следующих работ:

– инфологическое проектирование базы данных;

– логическое проектирование;

– физическое проектирование.

Результатом выполнения данного этапа служит разработанная средствами выбранной СУБД база данных, а также ее описание в нотации «сущность-связь».

4 этап – Проектирование программного приложения. На данном этапе должны быть проведены следующие работы:

– выделение функциональных подсистем;

– разработка иерархии функциональных подсистем в соответствии с ООП;

– выделение подсистемы обеспечения информационной безопасности;

– обоснование выбора программных платформ разработки и дизайна, а также языков программирования;

– разработка документации, связанной с нормами безопасности жизнедеятельности;

– выделение задач функциональных подсистем.

В результате должна быть получена проектная документация для последующего кодирования системы.

5 этап – Программная реализация системы. Данный этап состоит из кодирования подсистем, их тестирования и объединение в законченный программный продукт.

6 этап – Согласование созданной информационной системы с требованиями заказчика, учет всех полученных замечаний и указаний.

7 этап – Внедрение и сопровождение системы: установка и настройка программно-аппаратных средств, обучение пользователей работе с системой, выявление и устранение неполадок.

5.2 Сроки выполнения

Разработка информационной системы определяется периодом с сентября 2016 по июнь 2017.

5.3 Состав организации исполнителя работ

Исполнителем всех вышеперечисленных работ является студент ФГБОУ ВО Амурский Государственный Университет Левковец Михаил Андреевич.

5.4 Вид и порядок экспертизы технической документации

Вид и порядок экспертизы технической документации определяет Заказчик в одностороннем порядке.

Будет осуществлена проверка всей документации на плагиат.

6 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ

Приемка и контроль подученной в ходе разработки системы будет осуществляться по следующим пунктам:

– анализ готовой системы;

– сравнение разработанной системы с техническим заданием на ее разработку, с целью определения выполнения всех предъявленных в нем требований;

– выполнение доработки и изменений системы при необходимости;

– опытная эксплуатация системы в режиме бета-тестирования;

– доработка системы и исправление ошибок;

Приемка работ осуществляется государственной аттестационной комиссией ФГБОУ ВО «АмГУ», в соответствие с календарным планом и учебной программной.

Так же будет осуществлена приемка готового программного продукта представителями Заказчика по завершению всех предыдущих этапов.

7 ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ОБЪЕКТА АВТОМАТИЗАЦИИ К ВВОДУ СИСТЕМЫ В ДЕЙСТВИЕ

7.1 Преобразование входной информации к машиночитаемому виду

Для использования входной информации в работе системы, эти данные необходимо преобразовать в форму понятную ЭВМ.

Перед эксплуатацией Заказчик определяет необходимый набор предварительной информации в соответствие с результатами бета-тестирования.

7.2 Создание условий функционирования объекта

Готовый программный продукт загружается Заказчиком на сервер, где развертывается и начинает свое функционирование.

7.3 Сроки и порядок комплектования и обучения персонала

Заказчик до загрузки системы на сервер, организует рабочее место, а также подготавливает специалиста для работы с системой. Далее данный специалист занимается загрузкой системы, ее первоначальным тестирование и дальнейшим сопровождением.

8 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

8.1 Перечень подлежащих обработке документов

При сдаче подсистемы в эксплуатацию пакет сопровождающих документов должен включать:

– техническое задание;

– описание программного продукта;

– руководство пользователя;

8.2. Перечень документов на машинных носителях

Документация из подраздела 8.1 должна быть представлена на машинных носителях.

9 ИСТОЧНИКИ РАЗРАБОТКИ

Источниками разработки автоматизированной системы являются:

1 ГОСТ 34.201-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем;

2 ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы;

3 Левковец М. А. Отчёт по прохождению производственной практики. 2016.

4 Марк, Лутц Изучаем Python. / Пер. с англ. – М. Издательство «Символ-Плюс» 2011. – 1280 с.

5 Маклафлин Б. PHP и MySQL. Исчерпывающее руководство / Пер. с англ. – СПб.: Питер, 2013. — 512 с.

6 Чепак Л. В., Масловская А. Г. Разработка и реализация баз данных: методическое руководство к курсовому проектированию / Л.В. Чепак, А.Г. Масловская. – Благовещенск: Изд-во АмГУ , 2011. – 56 с.

7 Жигулин, Г.П., Новосадов, С.Г. Информационная безопасность / Жигулин Г.П., Новосадов С.Г. – СПб: СПб ГУ ИТМО, 2014. – 560 с

8 Олифер, В.Г. Компьютерные сети 3-е издание / Олифер В.Г. – СПб СПб.: Питер, 2012. – 960 с.

9 Фримен, Э. Изучаем программирование на HTML5 / Фримен Э. – СПб.: Питер, 2013. – 251 с.

ПРИЛОЖЕНИЕ Г

Диаграмма «сущность-связь»

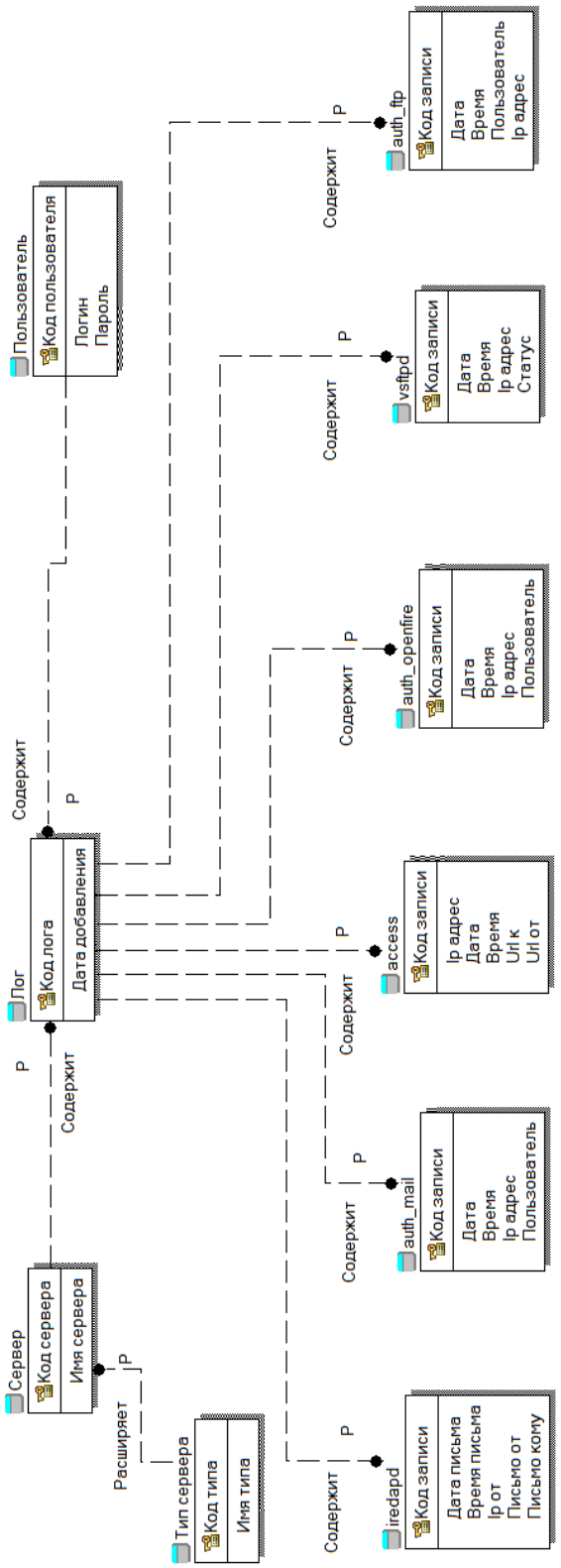

Рисунок Г.1 – диаграмма «сущность-связь»

ПРИЛОЖЕНИЕ Д

Логическая модель БД

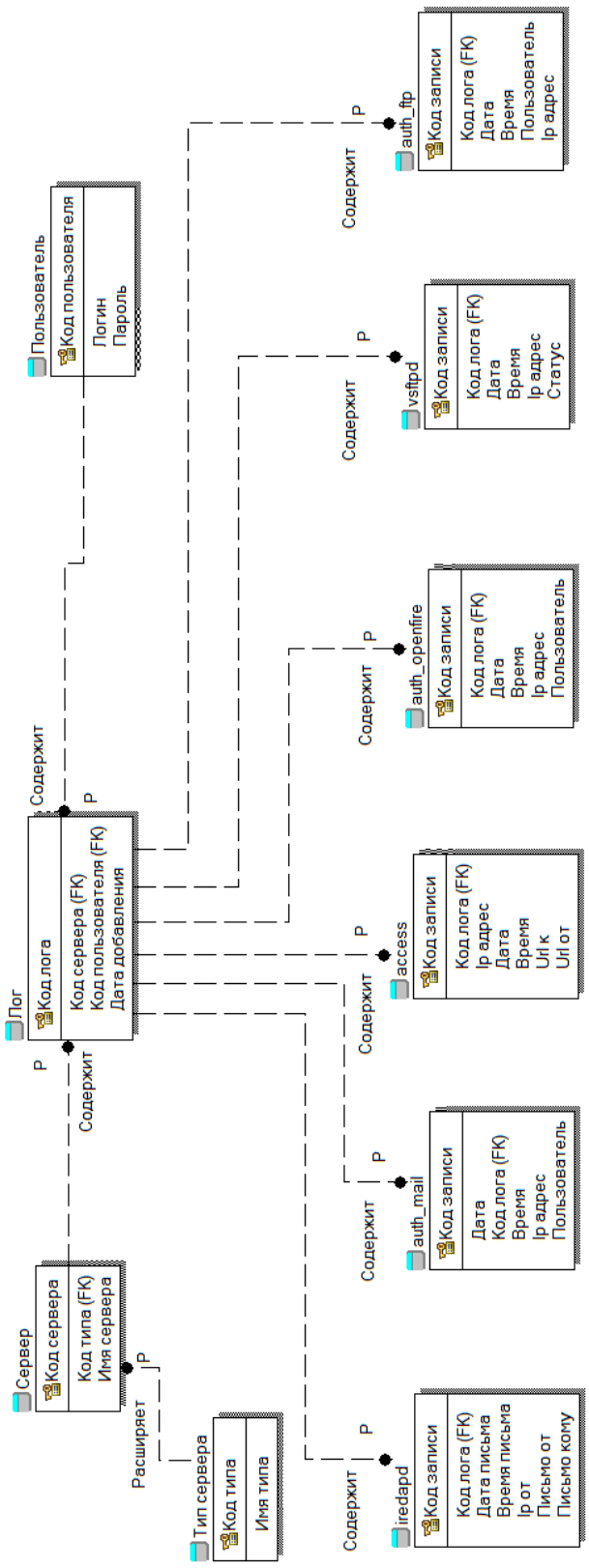

Рисунок Д.1 - Логическая модель БД

ПРИЛОЖЕНИЕ Е

Физическая модель БД

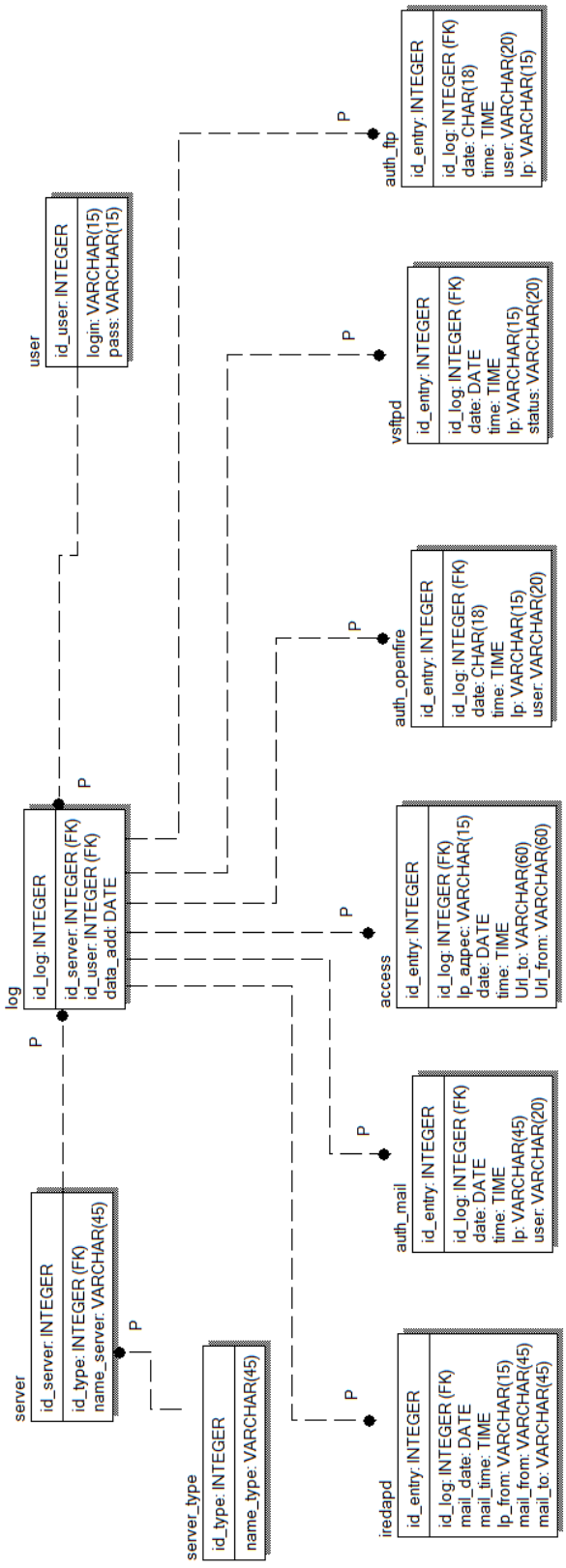

Рисунок Е.1 – Физическая модель БД