МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ
им. ГУМАРБЕКА ДАУКЕЕВА»
Кафедра IT - инжиниринг

«ДОПУЩЕНА К ЗАЩИТЕ»
Зав. Кафедрой, PhD, доцент Досжанова А.А
_____« __»
_____2020

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Разработка информационного портала для компании. Разработка системы обеспечения информационной безопасности
Специальность 5В070400 – «Вычислительная техника и программное обеспечение»
Выполнила: Сан С.Э. Группа: ВТ-16-2
Научный руководитель: д.т.н.,проф. Ахметов Б.С.

Консультанты:
по экономической части: Габелашвили К.Р.
_____ «____» _____2020 г.
по безопасности жизнедеятельности: Приходько Н.Г.
_____ «____» _____2020 г.
по программному обеспечению: Майкотов М.Н
_____ «____» _____2020 г.
Нормоконтролер: Абсатарова Б.Р.
_____ «____» _____2020 г.
Рецензент:_
_____
(учѐная степень, звание, Ф.И.О.)
_____ «____» _____2020 г.

Алматы 2020

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ
им. ГУМАРБЕКА ДАУКЕЕВА»

Институт систем управления и информационных технологий

Специальность 5В070400 – «Вычислительная техника и программное обеспечение»

Кафедра IT- инжиниринг

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Сан Софие Эрчуановне

Тема проекта: Разработка информационного портала для компании. Разработка системы обеспечения информационной безопасности

Утверждена приказом по университету № ___ от «___» _____2020 г.

Срок сдачи законченного проекта «___» _____ 2020 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): MySQL- среда разработки БД, phpStorm – среда программирования, исходные правила обращения с информацией, список оборудования.

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта:

а) различные виды аутентификации для входа в проект flores.kz;

б) защита входа для неавторизованных пользователей и с запрещенными IP-адресами;

в) обеспечение безопасности посредством применения ряда мер (сертификаты безопасности, хеширование данных и т.д.).

Перечень графического материала (с точным указанием обязательных чертежей): представлены 14 таблиц, 37 иллюстраций, презентация (22 слайда).

Основная рекомендуемая литература:

1 Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2018. - 88 с.;

2 Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.;

3 Основы безопасности жизнедеятельности. Алексеенко В.А., Матасова И.Ю., 2001. – 187 с "Безопасность в чрезвычайных ситуациях: Учебник" под ред. Н.К. Шишкина. – М., ГУУ, 2017. - 90 с.

Консультация по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Технико-экономическое обоснование проекта	к.э.н., ассоц. профессор Габелашвили К.Р.	24.04.2020	
Безопасность жизнедеятельности	доц. Приходько Н. Г.	24.04.2020	
Программное обеспечение	ст.преп. Майкотов М.Н.	14.05.2020	
Нормоконтролер	ст.преп. Абсатарова Б.Р.	18.05.2020	

ГРАФИК
подготовки дипломного проекта

Наименования разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечания
Исследование предметной области	01.11.2019 – 20.12.2019	
Проектирование информационной системы	21.12.2019 – 20.02.2020	
Разработка программного продукта	21.02.2020 – 20.04.2020	

Дата выдачи задания «13 января 2020г.

Заведующий кафедрой _____ _____А.А.Досжанова

Научный руководитель проекта _____ _____ Б.С.Ахметов

Задание принял к исполнению студент _____С.Э.Сан

Содержание

Андатпа

Осы дипломдық жоба аясында флористикалық компания үшін ақпараттық порталдың ақпараттық қауіпсіздігін қамтамасыз ететін бағдарламалық жасақтама жасалды.

Бұл бағдарламалық өнімді енгізу компания деректерінің қауіпсіздігін жақсарту үшін қажет болды.

Бұл түсіндірме жазбада қауіптерден қорғау құралдарын ұйымдастырудың қолданыстағы тәсілдерінің сипаттамасы, құралдарды таңдаудың негіздемесі келтірілген. Әзірленген ішкі жүйенің сипаттамасы, ішкі жүйенің алгоритмдерінің сипаттамасы, ішкі жүйенің компоненттері.

Бағдарламалық өнімді әзірлеуге шығындар есебі және ішкі жүйені енгізудің экономикалық тиімділігінің есебі келтірілген.

Шағын жүйенің жұмысына байланысты қауіпті және зиянды факторлардың талдауы келтірілген.

Аннотация

В рамках данного дипломного проекта разработан программный комплекс обеспечения информационной безопасности информационного портала для флористической компании.

Реализация данного программного продукта была необходима для улучшения безопасности данных компании.

Настоящая пояснительная записка включает в себя описание существующих подходов к организации средств и мер защиты от угроз, приводится обоснование выбора инструментальных средств. Приводится описание разработанной подсистемы, описание алгоритмов работы подсистемы, составных частей подсистемы.

Приводится расчет затрат на разработку программного продукта и расчет экономического эффекта от внедрения подсистемы.

Приводится анализ опасных и вредных факторов, возникающих при эксплуатации подсистемы

Annotation

Within the framework of this diploma project the software complex of information security of the information portal for floristic company has been developed.

The implementation of this software product was necessary to improve the security of the company's data.

This Explanatory Note includes a description of existing approaches to the organization of protective measures against threats and the rationale for the choice of tools. A description of the developed subsystem, subsystem algorithms, and component parts of the subsystem is given.

The cost of software development and the economic impact of the subsystem implementation are calculated.

Analysis of hazards associated with subsystem operation.

Введение

Наука развивается необычайно быстро и на текущее время, одним из основных ее направлений является внедрение информационных технологий, которые присутствуют практически во всех сферах жизнедеятельности человека. Развитие общества находится сегодня на таком этапе, для которого характерен непрерывный процесс совершенствования информационных технологий. Сфера внедрения информационных систем постоянно расширяется, затрагивая все новые стороны жизни общества. И поскольку развитию технологий сопутствует рост количества угроз безопасности, вопрос информационной безопасности стоит как никогда необычайно остро.

Информационная безопасность (ИБ) – это такое состояние информационной системы, при которой ощущается наименьшая восприимчивость к вмешательству и нанесению ущерба со стороны третьих лиц. Безопасность информации также подразумевает под собой управление рисками.

Риск - фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности.

Угроза - потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию.

Уязвимость - это недостаток, чаще ошибка в реализации, которая делает возможным непредусмотренное воздействие на систему, влекущее сбои в работе системы.

Существует несколько направлений мер информационной безопасности:

- правовые;
- организационные;
- технические.

Затрагивая тему правых мер, следует учитывать действующие законы страны, нормативные акты, определяющие правила поведения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения данных правил.

Организационные меры определяют подбор персонала, обеспечение безопасности вычислительного центра, наличие плана действий по восстановлению работоспособности центра, в случае выхода его из строя по той или иной причине, а также осуществление обслуживания вычислительного центра третьими лицами незаинтересованными в сокрытии фактов нарушений.

Помимо этого, необходима универсальность средств защиты от всех пользователей.

Технические меры обеспечивают защиту от несанкционированного доступа к системе, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев. Более подробно данные меры будут рассматривать в данном дипломном проекте.

Существует модель информационной безопасности, согласно которой информация считается защищенной, если соблюдаются три главных свойства.

а) Целостность – предполагает обеспечение достоверности и корректного отображения охраняемых данных, независимо от того, какие системы безопасности и приемы защиты используются в компании. Обработка данных не должна нарушаться, а пользователи системы, которые работают с защищаемыми файлами, не должны сталкиваться с несанкционированной модификацией или уничтожением ресурсов, сбоями в работе ПО.

б) Конфиденциальность - означает, что доступ к просмотру и редактированию данных предоставляется исключительно авторизованным пользователям системы защиты.

в) Доступность - подразумевает, что все авторизованные пользователи должны иметь доступ к конфиденциальной информации [1].

Достаточно нарушить одно из свойств защищенной информации, чтобы использование системы стало бессмысленным.

Актуальность данной дипломной работы обусловлена необходимостью проведения анализа угроз ИБ, разработки путей их преодоления и важностью создания конкретной системы безопасности.

Предметом исследования является разработка системы безопасности в информационной системе.

Объектом исследования дипломной работы является обеспечение безопасности информационной системы.

Цель данной дипломной заключается в разработке системы безопасности, включающую в себя несколько способов авторизации, обеспечение защиты SSL-сертификатом безопасности, а также обеспечение сетевой защиты посредством ограничения доступа адресов.

Задачи:

а) Изучение документации в области безопасности информационных систем.

б) Исследование исходных данных компании, для которой реализуется разработка системы обеспечения ИБ.

в) Разработка эффективной системы безопасности информационных систем для компании, удовлетворяющей требованиям законодательства РК.

1 Аналитическая часть

В данном подразделе производится описание поставленных задач для разработки дипломной работы.

1.1 Описание предметной области

Предметной областью данной дипломной работы является флористическая компания, осуществляющая оптовые и розничные продажи своей продукции.

Изначально компания производила все записи о продажах, поступлениях, финансах на бумаге, поэтому в результате непредвиденных обстоятельств (бумаги могли потеряться, их могли украсть, случайно выбросить, оставить где-то в нерабочем месте, они могли пострадать в результате природных явлений).

В результате расширения, увеличения числа сотрудников, оборота производства, а также стремительного роста объема данных, бумажные носители прекращают справляться и появляется необходимость разработки специального портала, который был бы построен на фундаменте единой интегрированной системы, а работа всех сотрудников велась в одном информационном пространстве. Важным критерием является модуль, обеспечивающий безопасность данных организации и разграничение доступа.

Основные бизнес-процессы компании - закупки, складирование запасов, продажи, взаиморасчеты с поставщиками и клиентами.

Сотрудники организации, которые также являются и пользователями, включают: директора, бухгалтера, кадровика и рядовых сотрудников (продавцов, маркетологов и т.д.).

1.2 Цель разработки

Основной целью разработки модуля обеспечения информационной безопасности является организация целостности, конфиденциальности и доступности данных, с учётом целесообразности применения и без какого-либо ущерба производительности компании.

Помимо этого, второстепенной целью является предотвращение или минимизация ущерба (прямого или косвенного, материального, морального или иного), наносимого субъектам информационных отношений посредством нежелательного воздействия на информацию, её носители и процессы обработки.

1.3 Особенности использования методов разработки

В данной дипломной работе использовались следующие языки программирования:

а) PHP («Hypertext Preprocessor»)

PHP предназначен для написания скриптов, которые выполняются на стороне сервера, а в браузер клиента отправляется не сам скрипт, а только результаты его работы. Это означает, что пользователь, загрузивший страницу вашего сайта, никогда не увидит исходный код скрипта и может даже не догадываться, что страница создана динамически.

б) JavaScript

JavaScript является клиентским языком программирования, поскольку выполняется на стороне клиента. Он имеет возможность изменять страницы браузеров, а также он включает такие возможности, как добавление или удаление тегов, изменение стилей страницы, предоставляет возможность работать с информацией о действиях пользователя на странице, осуществлять запрос доступа к случайной части исходного кода страницы, внести изменения в этот код, и выполнять действия с cookie-файлами.

Фреймворки:

а) JQuery

JavaScript-библиотека, фокусирующаяся на взаимодействии JavaScript, HTML и CSS.

б) Vue.js

JavaScript-фреймворк с открытым исходным кодом для создания пользовательских интерфейсов. Легко интегрируется в проекты с использованием других JavaScript-библиотек.

Технологии:

а) AJAX

Технология асинхронного взаимодействия с сервером, что позволяется обрабатывать данные без перезагрузки страницы.

Методы:

а) POST

Метод POST передает данные таким образом, что пользователь сайта уже не видит передаваемые скрипту данные

б) GET

Метод GET отправляет скрипту всю собранную информацию формы как часть URL.

В ходе разработки системы была организована работа с сессиями, которые предназначены для хранения сведений о пользователях при переходах между несколькими страницами. При использовании сессий данные сохраняются во временных файлах на сервере.

Защищенность соединения обеспечивается протоколом безопасности SSL.

Протокол SSL (от англ. Secure Sockets Layer – уровень защищенных сокетов) гарантирует безопасное соединение между браузером пользователя и сервером. При использовании SSL-протокола информация передается в закодированном виде по HTTPS и расшифровать ее можно только с помощью специального ключа в отличие от привычного протокола HTTP. Для работы SSL-протокола требуется, чтобы на сервере был установлен SSL-сертификат [2].

SSL-сертификат – это своего рода уникальная цифровая подпись вашего сайта. Такой сертификат нужен, в первую очередь, банкам, платежным системам и другим организациям, работающим с персональными данными, – для защиты транзакций и предотвращения несанкционированного доступа к информации.

SSL-сертификат содержит следующую информацию:

а) доменное имя, на которое оформлен SSL-сертификат;

б) юридическое лицо, которое владеет сертификатом;

в) физическое местонахождение владельца сертификата (город, страна);

г) срок действия сертификата;

д) реквизиты компании-поставщика SSL-сертификата [3].

SSL-сертификат подтверждает, что домен принадлежит реальной компании и что его владелец вправе пользоваться секретным ключом на законных основаниях.

HTTPS (HyperText Transfer Protocol Secure) – это расширение протокола HTTP, поддерживающее шифрование. Данные, передаваемые по протоколу HTTP, «упаковываются» в криптографический протокол SSL или TLS. По умолчанию HTTPS использует 443 TCP-порт (для незащищенного HTTP – 80).

Основными средствами разработки являлись:

а) PhpStorm - коммерческая кросс-платформенная интегрированная среда разработки для PHP. Разрабатывается компанией JetBrains на основе платформы IntelliJ IDEA.

б) SublimeText - полнофункциональный текстовый редактор для редактирования локальных файлов или базы кода. Он включает в себя различные функции для редактирования базы кода, которая помогает разработчикам отслеживать изменения.

1.4 Сравнительный анализ аналогов

В связи с тем, что все способы авторизации разрабатываются специализированно для определенных систем в единичном числе, то отдельных модулей, состоящих из нескольких способов авторизации и ограничения доступа по IP-адресу не существует.

Стоит отметить такие положительные стороны МОИБ, как:

а) возможность выбора авторизации;

б) при авторизации посредством временной ссылки, происходит хеширование не пароля, а даты и времени в миллисекундах, поэтому даже при перехвате хеша, злоумышленник не сможет получить пароль;

в) при авторизации посредством номера телефона, пароль так же не передается, а наоборот – пользователю третья система высылает временный код для входа в систему;

г) Невозможно перехватить данные по сети, поскольку пользователи могут зайти на портал только с разрешенного IP-адреса.

1.5 Определения и сокращения

ОТП (с англ. “One time password” – одноразовый пароль) - одноразовый пароль.

ТЗ - техническое задание.

Информационная безопасность - практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.

Идентификация - это заявление о том, кем вы являетесь. В зависимости от ситуации, это может быть имя, адрес электронной почты, номер учетной записи, и т.д.

Аутентификация - предоставление доказательств, что вы на самом деле есть тот, кем идентифицировались (от слова “authentic” - истинный, подлинный).

Авторизация - проверка, что вам разрешен доступ к запрашиваемому ресурсу.

SSL (англ. Secure Sockets Layer - уровень защищённых сокетов) - криптографический протокол, который подразумевает более безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.

МОИБ – модуль обеспечения информационной безопасности.

Браузер - Программа, обеспечивающая доступ к текстовым и графическим страницам World Wide Web.

Доступ к информации (доступ) - ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение информации.

Доступ к ресурсу - получение субъектом доступа возможности манипулировать (использовать, управлять, изменять характеристики и т.п.) данным ресурсом [4].

Доступность информации - состояние информации, характеризуемое способностью АС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия [5].

Открытый ключ - Криптографический ключ, который связан с секретным с помощью особого математического соотношения. Открытый ключ известен всем другим пользователям системы и предназначен для проверки электронной цифровой подписи и расшифрования [6].

Секретный (закрытый) ключ - Ключ асимметричной ключевой пары, который доступен только одному пользователю системы и хранится им в тайне [7].

Система - под данным термином подразумевается система обеспечения информационной безопасности.

СМС-провайдер - под данным термином подразумевается SMSC провайдер.

Политика информационной безопасности - совокупность правил, определяющих и ограничивающих виды деятельности объектов и участников, системы информационной безопасности.

Фишинг - вид интернет-мошенничества, целью которого является получение идентификационных данных пользователей (логины и пароли к банковским картам, учетным записям).

DNSSEC - набор расширений IETF протокола DNS, позволяющих минимизировать атаки, связанные с подменой DNS-адреса при разрешении доменных имён. Он направлен на предоставление DNS-клиентам аутентичных ответов на DNS-запросы и обеспечение их целостности. При этом используется криптография с открытым ключом [8].

2 Проектная часть

В данном разделе производится проектирование системы обеспечения информационной безопасности в разрезе процессов, полей и особенностей реализации, а также необходимых интеграций для корректной реализации системы.

2.1 Техническое задание

В рамках данного проекта необходимо реализовать модуль обеспечения информационной безопасности, включающий в себя:

а) Несколько способов аутентификации:

1) Вход по логину и паролю, где логином будет являться электронный адрес пользователя. Также необходимо реализовать возможность восстановления пароля;

Таблица 2.1 - Объект для входа типа «Логин-пароль»

Объект - Пользователь		
Наименование поля	Тип	Комментарий
Email	string	Электронный адрес пользователя
Password	string	Пароль

В данном варианте входа необходимо реализовать канальное шифрование передаваемых данных.

2) Вход без пароля посредством ОТП;

Таблица 2.2 - Объект для входа типа «ОТП»

Объект - Пользователь		
Наименование поля	Тип	Комментарий
Email	string	Электронный адрес пользователя

Telephone number	string	Номер телефона пользователя

В данном варианте входа необходимо реализовать канальное шифрование передаваемых данных с дополнительной технологией шифрования посредством алгоритмов пары ключей.

Необходимо осуществить интеграцию с СМС-провайдером, который имеют внутреннюю интеграцию по юридическим договорам с сотовыми операторами.

3) Вход без пароля посредством применения одноразовых ссылок с использованием хэширования пароля;

Таблица 2.3 - Объект для входа типа «Временная ссылка»

Объект - Пользователь		
Наименование поля	Тип	Комментарий
Email	string	Электронный адрес пользователя
hash	string	Сгенерированный код

В данном варианте входа необходимо реализовать канальное шифрование передаваемых данных с дополнительной технологией шифрования посредством алгоритмов пары ключей, md5, sha2.

4) Вход с применением биометрии.

В качестве входных данных используется фотография пользователя, а затем сравнивается с имеющимися в базе. После нахождения совпадения – автоматически происходит идентификация, аутентификация с последующей авторизацией.

Таблица 2.4 - Объект для входа типа «Распознавание по лицу»

Объект - Пользователь		
Наименование поля	Тип	Комментарий
Photo	string	Строка, содержащая фото в шифрованном виде base64.
Name	string	Имя пользователя, определяемое системой автоматически

Обеспечить невозможность входа на портал неавторизированным пользователям, а также запрет на нажатие мышью и горячие клавиши для просмотра кода.

б) Также необходимо осуществить ограничение доступа к порталу в зависимости от подключения к сети. Во избежание утечки данных посредством подключения к другим сетям, предоставляя разрешение на вход только тем пользователям, IP-адрес которых находится в списке разрешенных. Что означает возможность осуществления работы только из одной локации.

в) Необходимо организовать защищенное соединение посредством использования SSL сертификата безопасности, а также DNSSEC.

г) Организовать автоматическое сканирование на вирусы файлов портала, а также осуществление периодического мониторинга активностей.

д) Невозможность регистрации новых пользователей без участия системного администратора.

е) После успешного прохождения аутентификации, определить «воронку», общую для всех 4 способов аутентификации.

2.2 UML диаграмма

В данном подразделе будут представлены диаграммы деятельности UML.

В соответствии с рисунком 2.1 представлен процесс выбора способа авторизации. Пользователь заходит в систему, выбирает способ авторизации, далее на стороне МОИБ происходит обработка выбора и перенаправление на нужную страницу.

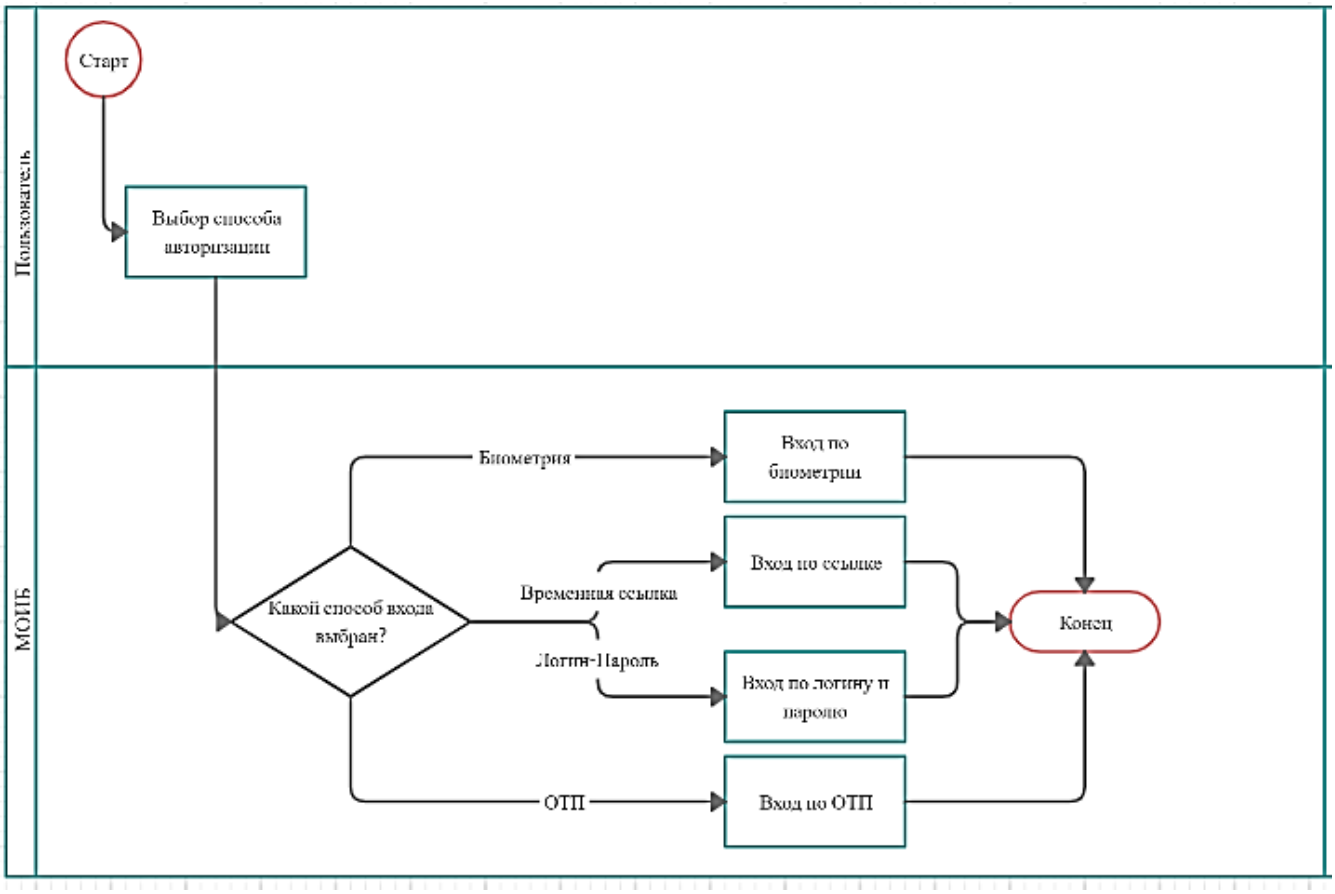

Рисунок 2.1 - Выбор способа авторизации

В соответствии с рисунком 2.2 представлен процесс авторизации посредством биометрии лица. Пользователь делает фотографию, далее МОИБ производит обработку фотографии и сравнивает с имеющимися в базе, далее происходит определение пользователя, в случае отказа – пользователю выводится уведомление и ему нужно будет начать заново, а в случае определения пользователя – доступ будет разрешен.

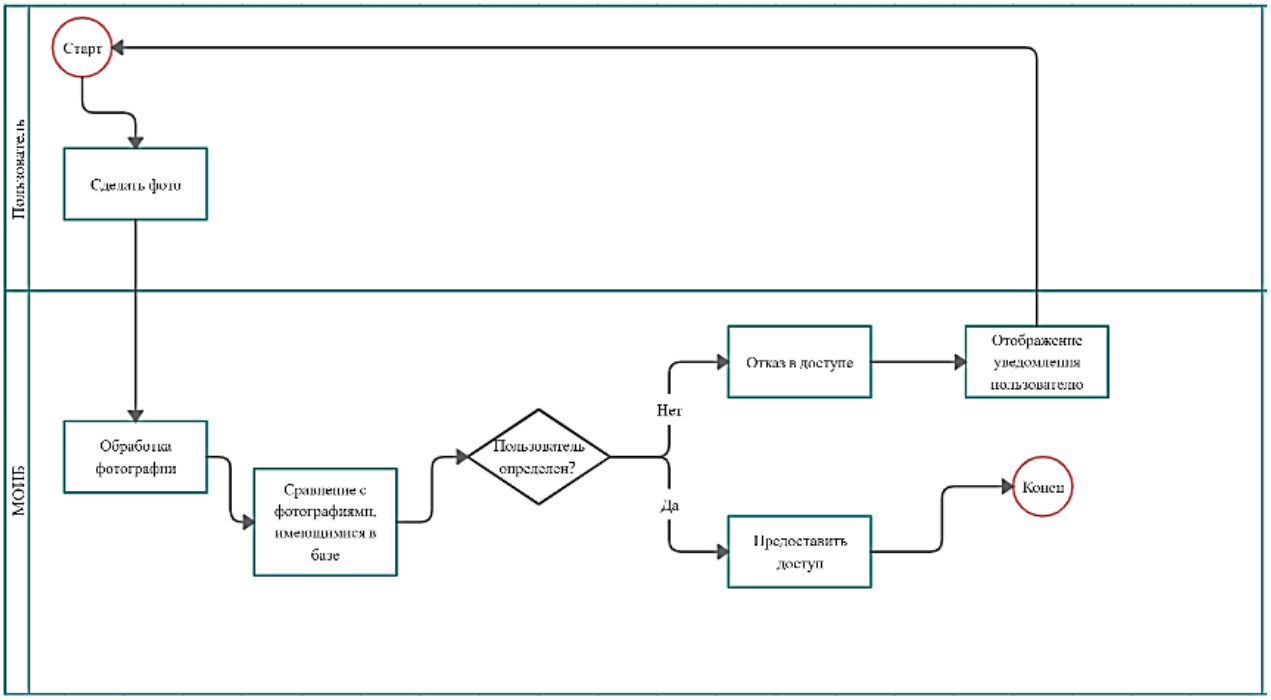

Рисунок 2.2 - Вход по биометрии

В соответствии с рисунком 2.3 представлен процесс авторизации посредством входа по временной ссылке. Пользователь вводит электронный адрес, далее МОИБ определяет пользователя, в случае отказа – пользователю выводится уведомление и ему нужно будет начать заново, а в случае определения пользователя – генерируется уникальный хеш для ссылки, ссылка отправляется на почту и пользователь, переходя по ней, автоматически авторизуется.

В соответствии с рисунком 2.4 представлен процесс авторизации посредством входа по логину и паролю. Пользователь вводит логин и пароль, далее МОИБ обрабатывает правильность формата введенных данных, в случае неправильности ему выводится уведомление, и он должен будет начать сначала, а в случае верности формата МОИБ определяет пользователя, в случае отказа – пользователю выводится уведомление и ему нужно будет начать заново, а в случае определения пользователя – ему предоставляется доступ.

В соответствии с рисунком 2.5 представлен процесс авторизации посредством входа по ОТП. Пользователь вводит номер телефона, далее МОИБ обрабатывает правильность формата введенных данных, в случае неправильности выводится уведомление, и он должен будет начать сначала, а в случае верности формата МОИБ определяет пользователя, в случае отказа – пользователю выводится уведомление и ему нужно будет начать заново, а в случае определения пользователя – ему отправляется СМС с ОТП, который

будет нужно ввести. В случае, если код верный – ему предоставляется доступ в систему, в ином случае – ему придется начать сначала.

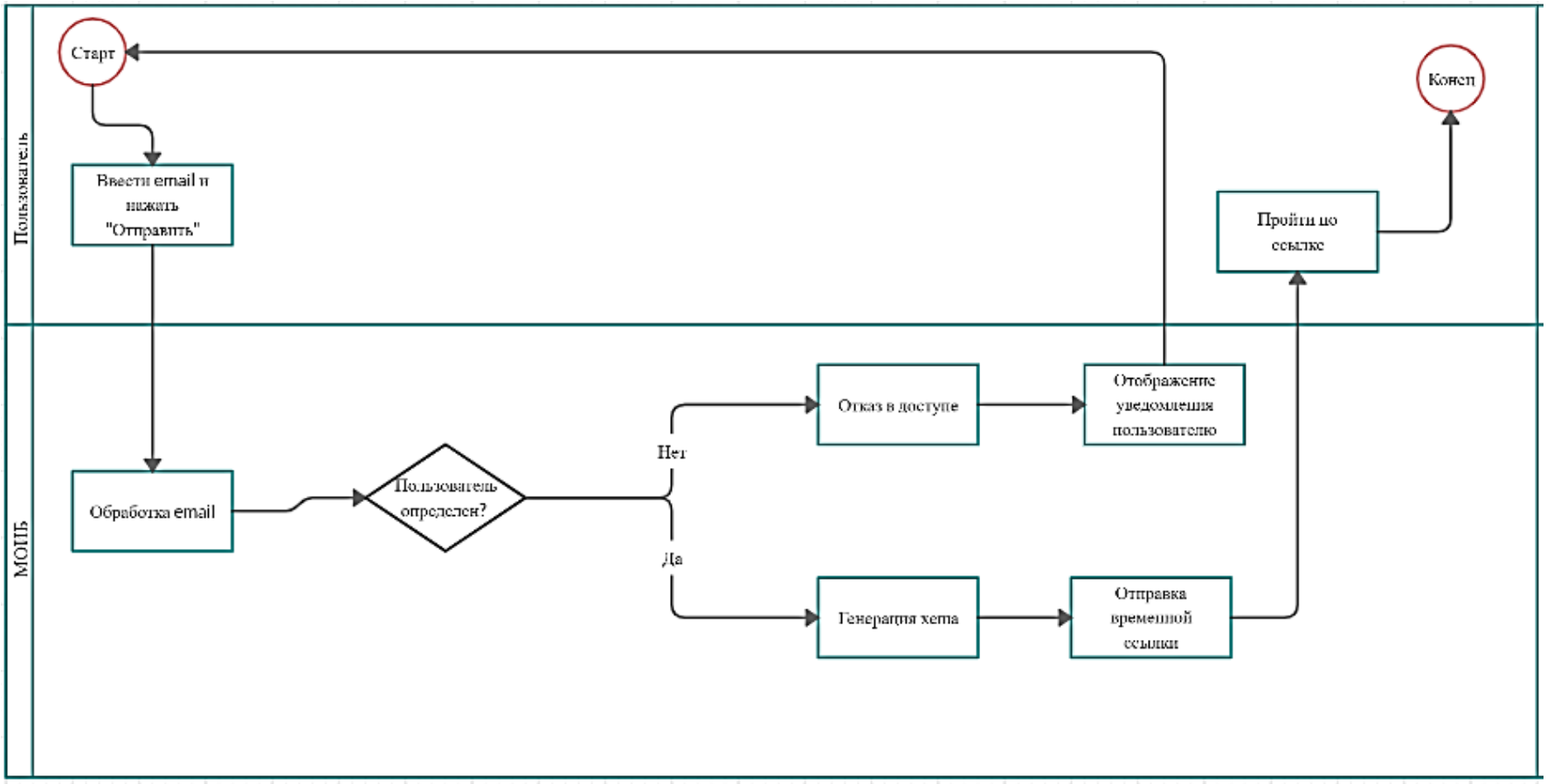

Рисунок 2.3 - Вход по ссылке

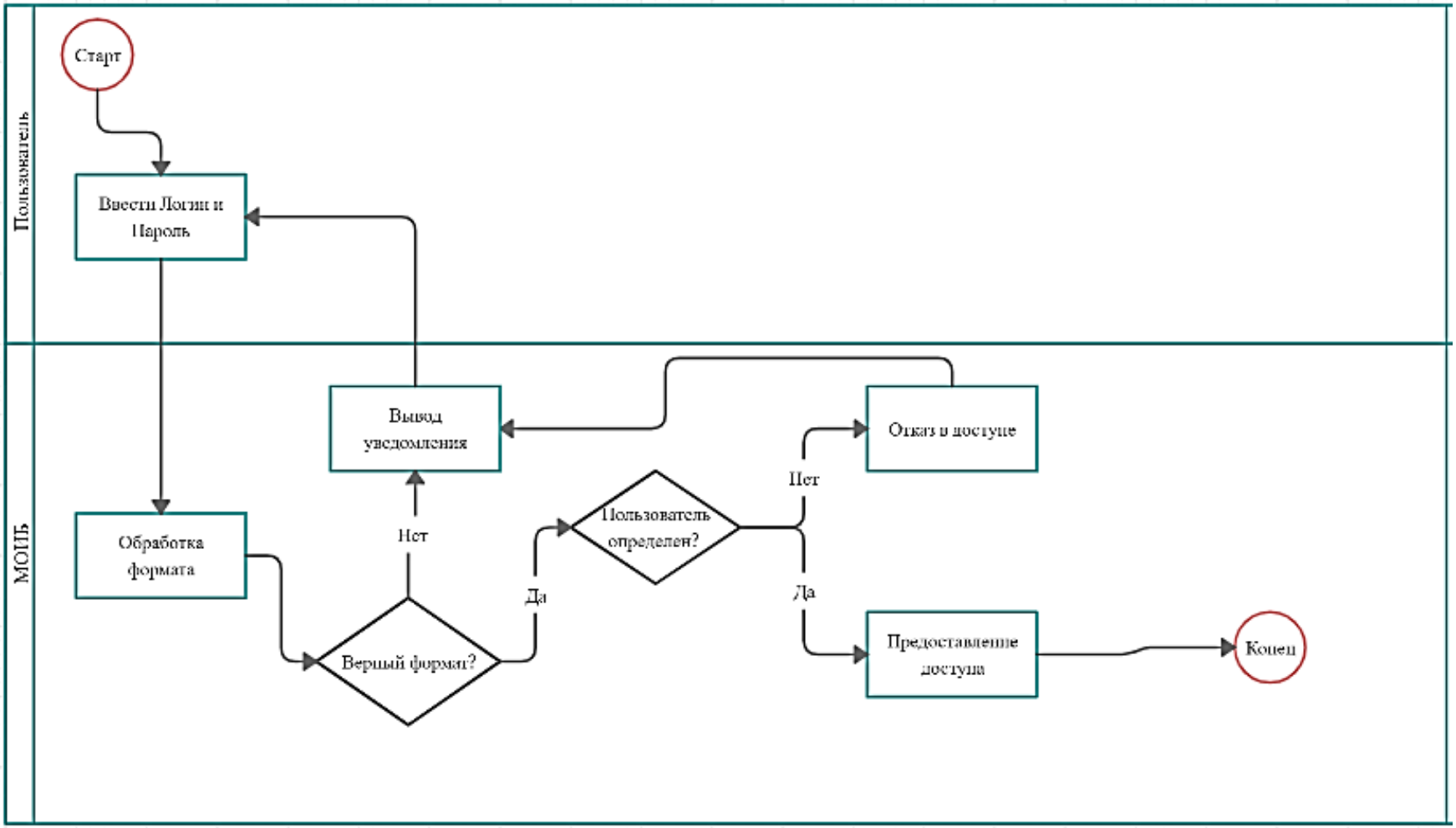

Рисунок 2.4 - Вход по логину и паролю

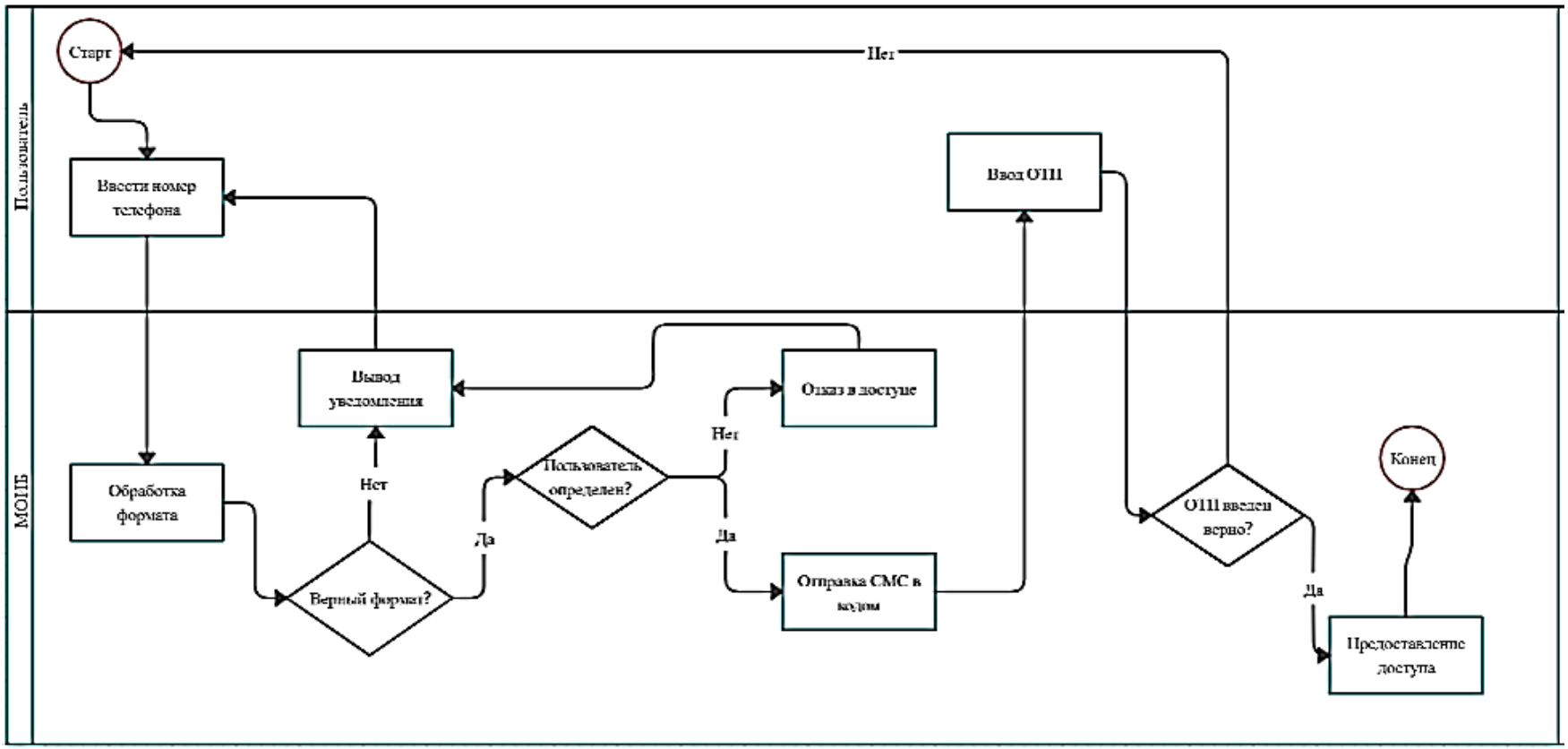

Рисунок 2.5 - Вход по ОТП

3 Экспериментальная часть

В данном разделе описывается процесс реализации разработки системы обеспечения информационной безопасности с указанием используемых сертификатов, а также представлено внешнее отображение системы.

3.1 Проектирование МОИБ

В ходе проектирования МОИБ были выработаны требования и подходы к реализации:

а) Разработка способа четырех способов аутентификации:

1) по логину и паролю;
2) по OTP;
3) по СМС;
4) по распознаванию лица.

б) Ограничение на подключение с неразрешенных IP-адресов, установка статичного IP-адреса для рабочей локации;

в) Разработка регламента поведения сотрудников с конфиденциальной информацией;

г) Доработка правил приема на работу и подписание документов о конфиденциальности;

д) Была учтена подсистема мониторинга и аудита безопасности (в соответствии с рисунком 3.1);

Журналы flores.kz ...

Начать обновления в режиме реального времени | Обновить | Все журналы

Дата	Тип	IP	Код	Сообщение	R	Агент	Размер	Исходный сервер
2020-04-03 06:16:59	Access	147.30.158.240	301	GET /IP.html/ HTTP/1.0			652	Доступ к Apache
2020-04-03 06:16:59	Access	147.30.158.240	301	GET /IP.html/ HTTP/1.0			652	Доступ к Apache
2020-04-03 06:16:59	Access	147.30.158.240	301	GET /IP.html/ HTTP/1.0			652	Доступ к Apache
2020-04-03 06:16:59	Access	147.30.158.240	301	GET /IP.html/ HTTP/1.0			652	Доступ к Apache
2020-04-03 06:17:14	Access	147.30.158.240	301	GET /IP.html/ HTTP/1.0			650	Доступ к Apache
2020-04-03 06:19:32	Access	147.30.158.240	301	GET / HTTP/1.0			428	Доступ к Apache
2020-04-03 06:19:33	Access	147.30.158.240	302	GET / HTTP/1.0			145 K	Доступ к Apache
2020-04-03 06:23:31	Access	147.30.158.240	301	GET /plesk-stat/webstat-ssl/ HTTP/1.0			474	Доступ к Apache
2020-04-03 06:23:31	Error	147.30.158.240	401	GET /plesk-stat/webstat-ssl/ HTTP/1.0			1.73 K	Доступ к Apache
2020-04-03 06:24:19	Error	147.30.158.240	401	GET /plesk-stat/webstat-ssl/ HTTP/1.0			1.73 K	Доступ к Apache
2020-04-03 06:24:19	Error	147.30.158.240		AH01618: user pavelbobr37@gmail.com not found: /plesk-stat/webstat-ssl/				Ошибки Apache
2020-04-03 06:24:42	Error	147.30.158.240	401	GET /plesk-stat/webstat-ssl/ HTTP/1.0			1.73 K	Доступ к Apache
2020-04-03 06:24:42	Error	147.30.158.240		AH01618: user pavelbobr37@gmail.com not found: /plesk-stat/webstat-ssl/				Ошибки Apache
2020-04-03 06:24:46	Error	147.30.158.240	401	GET /plesk-stat/webstat-ssl/ HTTP/1.0			1.73 K	Доступ к Apache

Рисунок 3.1 - Журнал активности

е) Осуществлено разграничение доступа по ролям (директор – полный доступ, остальные сотрудники – ограниченный);

ж) Установка времени резервного копирования для восстановление данных;

з) Установка антивирусного программного обеспечения (Kaspersky Total Security) на персональные компьютеры в компании;

и) Установка SSL-сертификата для обеспечения безопасной работы;

к) Настроен DNSSEC (в соответствии с рисунком 3.2).

л) Периодическое сканирование файлов (в соответствии с рисунком 3.3).

м) Запрет на клик и нажатие горячих клавиш.

н) Шифрование передаваемых данных нескольким путями.

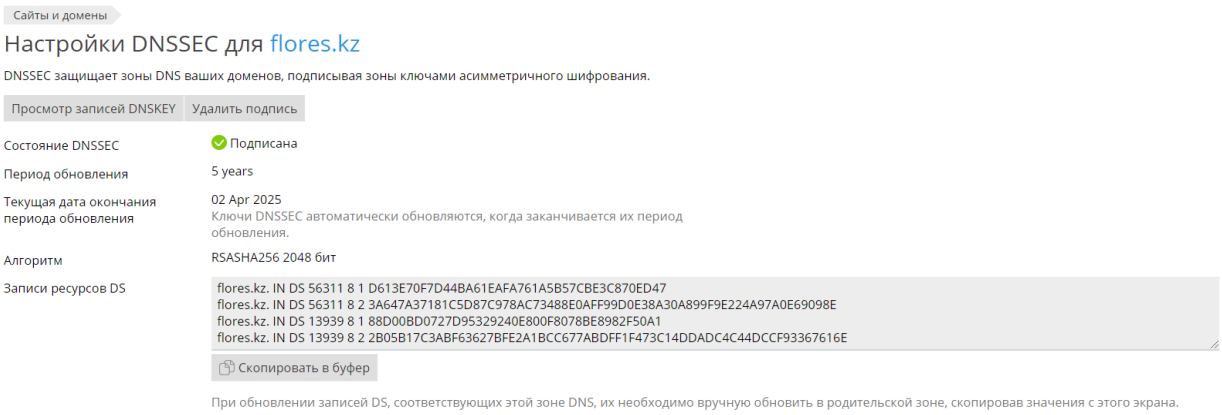

Рисунок 3.2 - DNSSEC

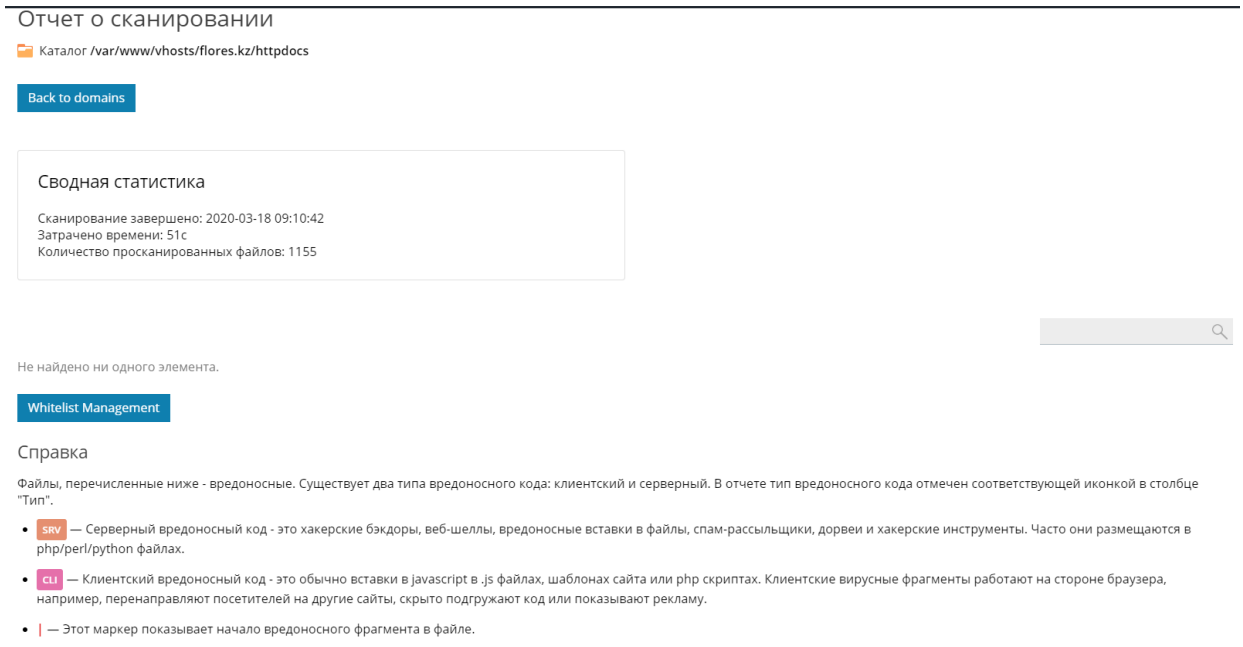

Рисунок 3.3 - DNSSEC

3.2 Выполнение МОИБ

В соответствии с рисунком 3.4 представлена главная страница отображения МОИБ. Здесь пользователь может выбрать, посредством чего ему пройти аутентификацию, идентификацию и затем авторизацию. Помимо этого, можно настроить двойную и тройную и четырехэтапную аутентификацию.

Каждый элемент интерфейса дианимичен: волны запущены циклично как от рисованные кодом изогнутые, название посредством использования Type.js производит автопечать заданной строки, а также каждый элемент поддается внешнем воздействию, благодаря которому создается внешний эффект.

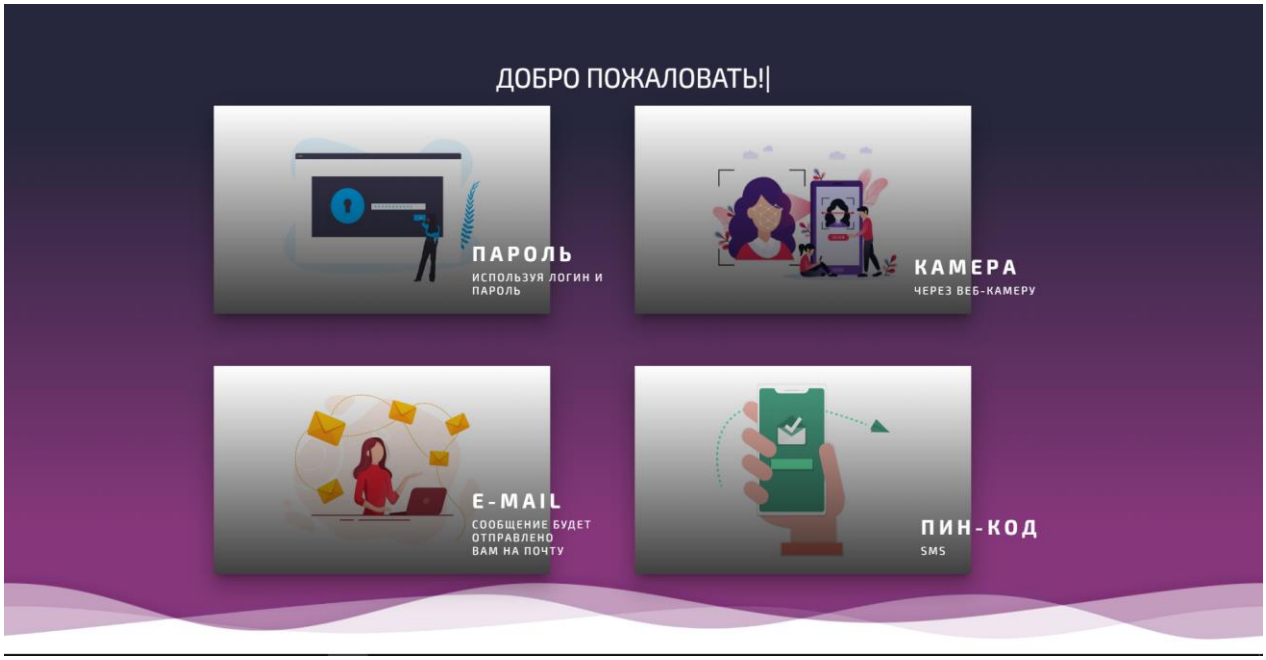

Рисунок 3.4 - Главная страница модуля

При выборе аутентификации посредством введения логина и пароля, пользователю отобразится интерфейс, в соответствии с рисунком 3.5. На странице расположена кнопка «На главную», которая позволит вернуться на стартовую страницу с возможностью выбора способа аутентификации. В поле “Ваш email” пользователь должен ввести его электронный адрес, а в поле с маской “”

В случае, если пользователь забыл пароль, он может его восстановить, нажав на «Забыли пароль?». После этого ему отобразится интерфейс в соответствии с рисунком 3.6.

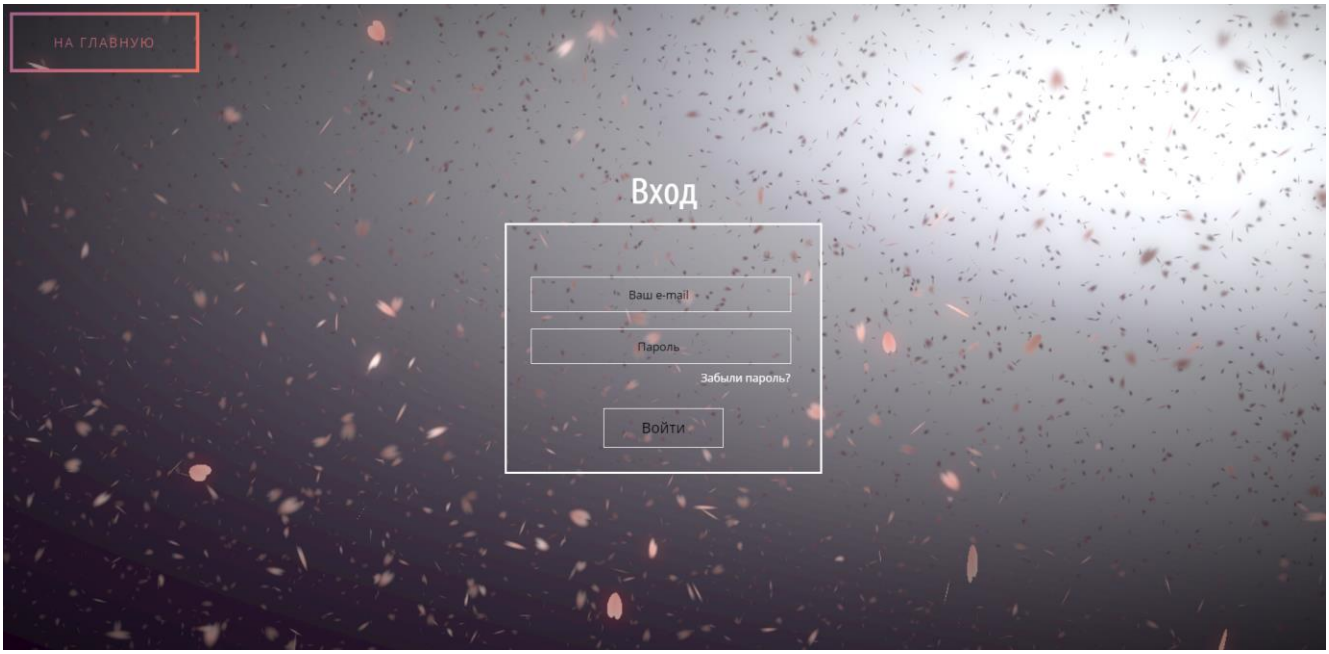

Рисунок 3.5 - Вход посредством логина и пароля

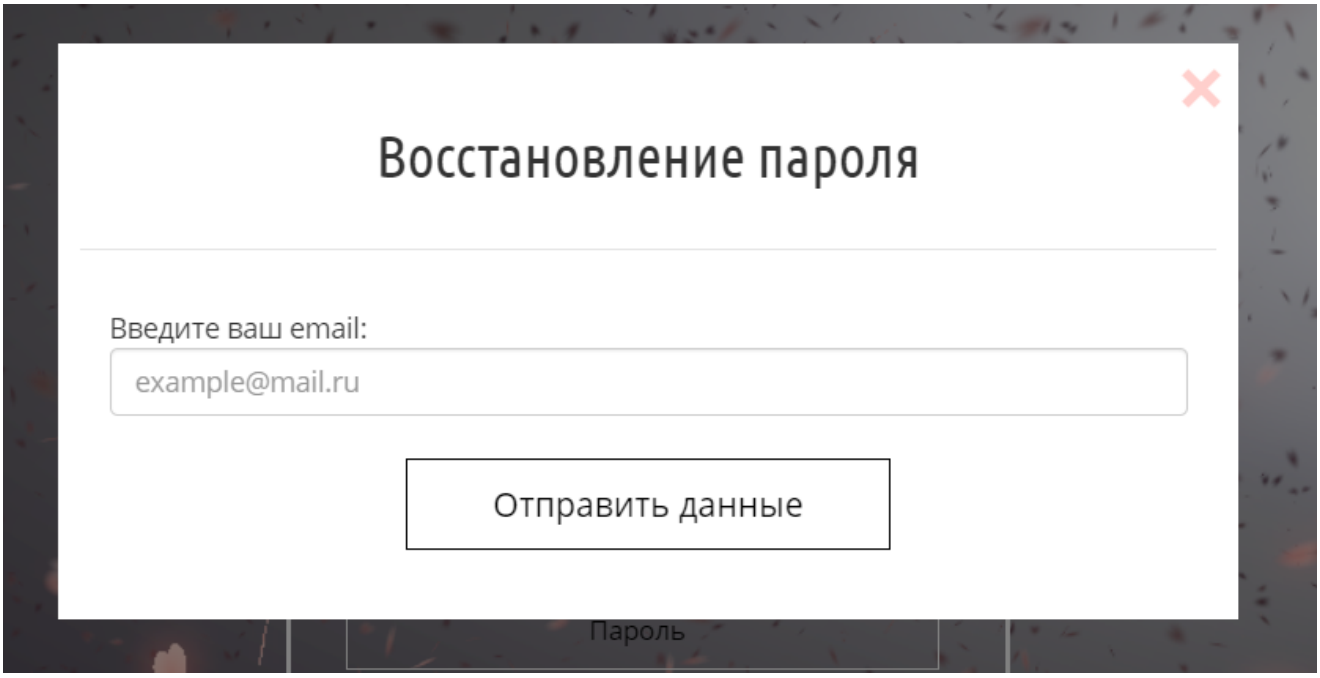

Рисунок 3.6 - Восстановление пароля

После того, как пользователь введет e-mail и нажмет на “Отправить данные”, в случае неверных данных ему отобразится интерфейс, в соответствии

с рисунком 3.7, в ином случае – произведется вывод уведомления об успешной отправки данных (в соответствии с рисунком 3.8).

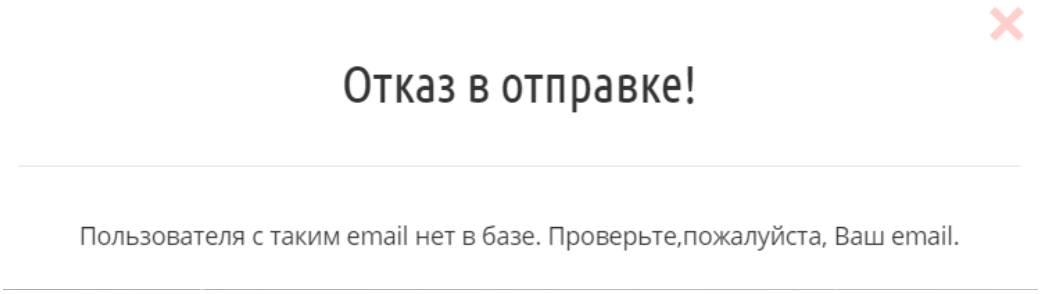

Рисунок 3.7 - Отказ в отправке пароля

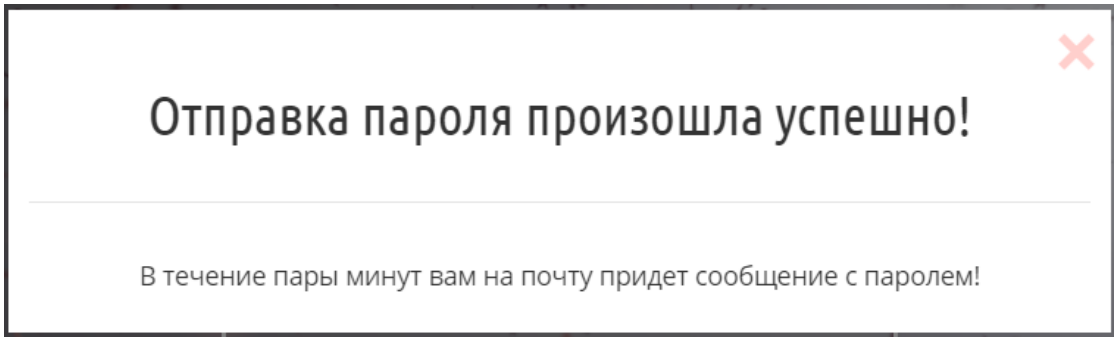

Рисунок 3.8 - Уведомление об успешной отправке

Далее произойдет отправка данных на указанных электронный адрес (в соответствии с рисунком 3.9). По причине того, что регистрация возможно только с помощью системных администраторов, то было решено высылать сразу логин и пароль, которые находятся под личной ответственностью сотрудника.

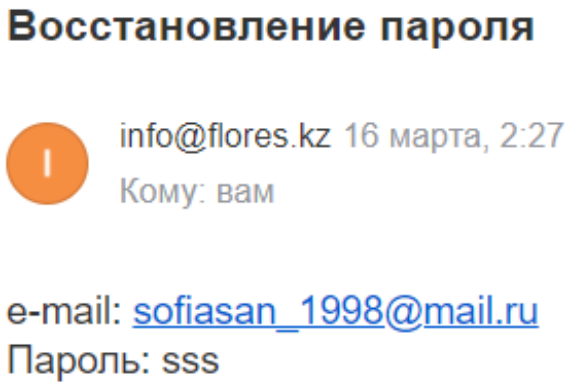

Рисунок 3.9 - Сообщение с паролем

В случае выбора пользователем авторизации посредством ОТП, будет отображен интерфейс, в соответствии с рисунком 3.10.

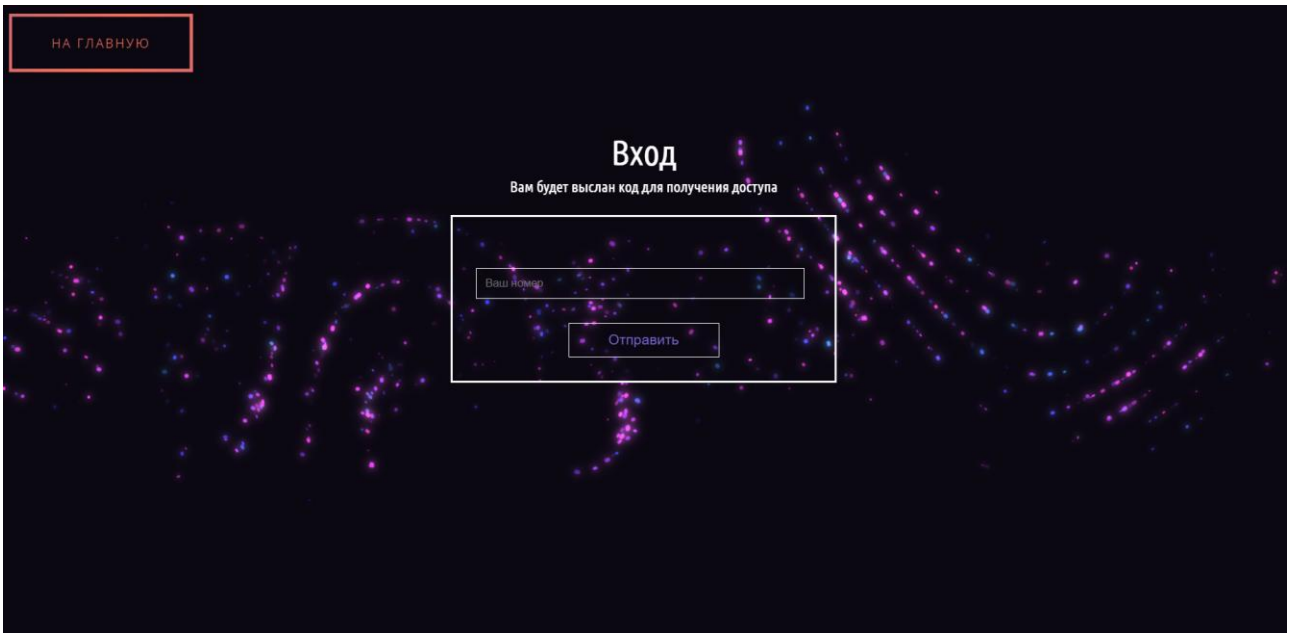

Рисунок 3.10 - Вход по ОТП

В случае неверных данных ему отобразится интерфейс, в соответствии с рисунком 3.11.

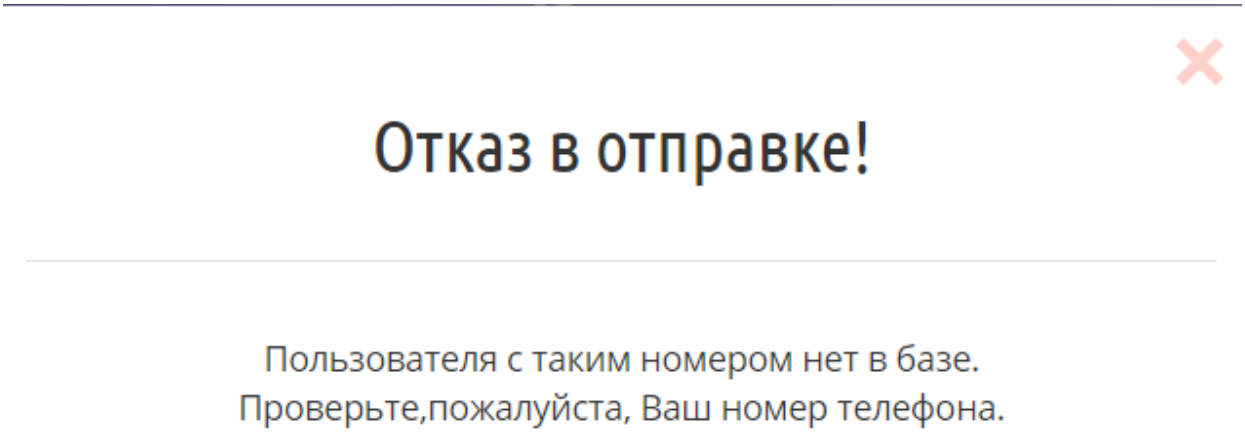

Рисунок 3.11 - Отказ в отправке ОТП

В случае правильности введенных данных – произойдет отправка ОТП на указанный номер (в соответствии с рисунком 3.12), после чего будет нужно

ввести код (в соответствии с рисунком 3.13). Подтверждение на мобильном телефоне представлено согласно рисунку 3.15.

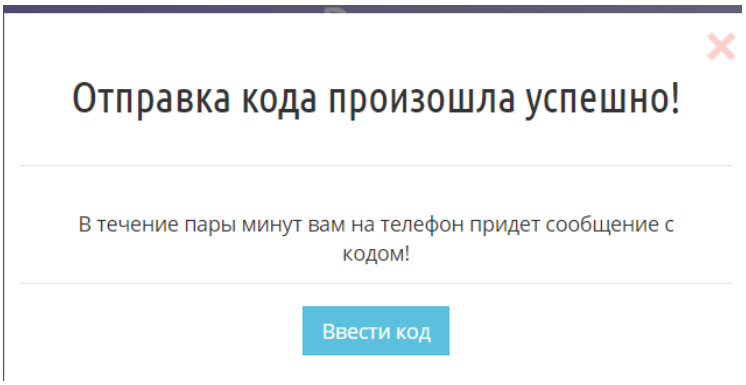

Рисунок 3.12 - Отправка ОТП

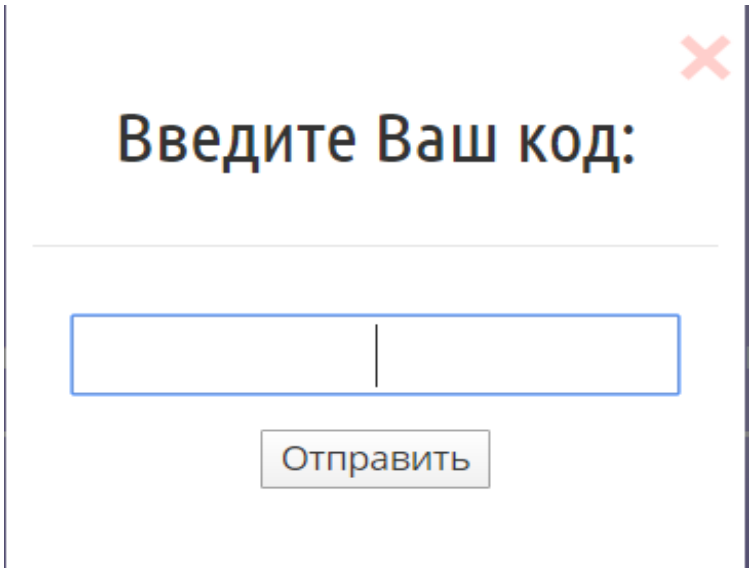

Рисунок 3.13 - Подтверждение ОТП

После ввода правильного кода, пользователь будет переадресован на страницу приветствия и произойдет автоматический вход в систему. В ином случае выведется уведомление о неправильности введенного кода (интерфейс отображен согласно рисунку 3.14). Интеграция с СМС провайдером представлена в приложении А.

Рисунок 3.14 - Неправильный код

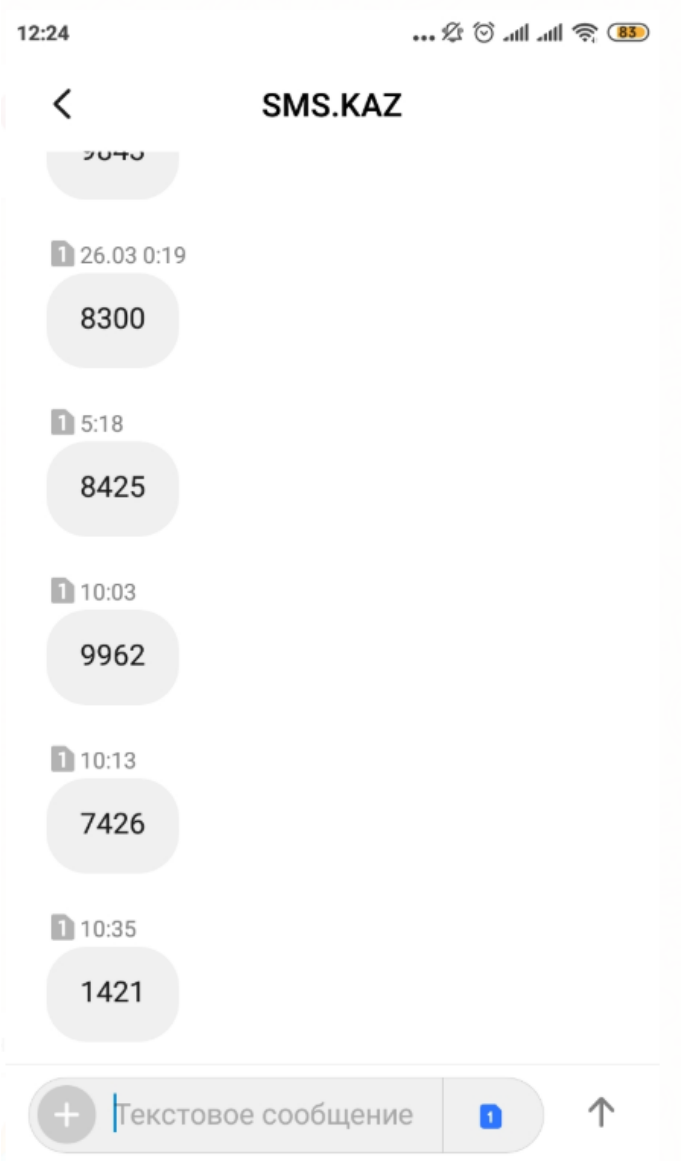

Рисунок 3.15 - Код

В случае выбора пользователем авторизации посредством временной ссылки, будет отображен интерфейс, в соответствии с рисунком 3.16.

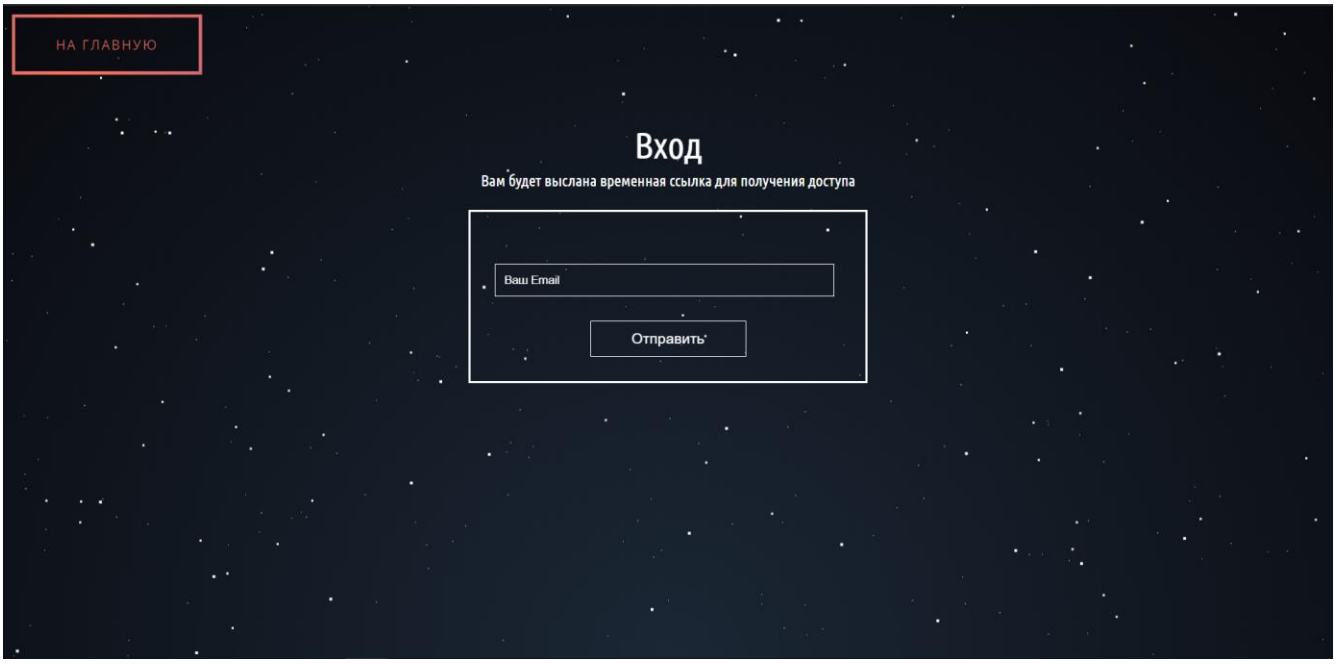

Рисунок 3.16 - Вход по временной ссылке

В случае ввода неверных данных ему отобразится интерфейс в соответствии с рисунком 3.17, в ином случае – произойдет отправка временной ссылки на указанную почту (в соответствии с рисунком 3.18).

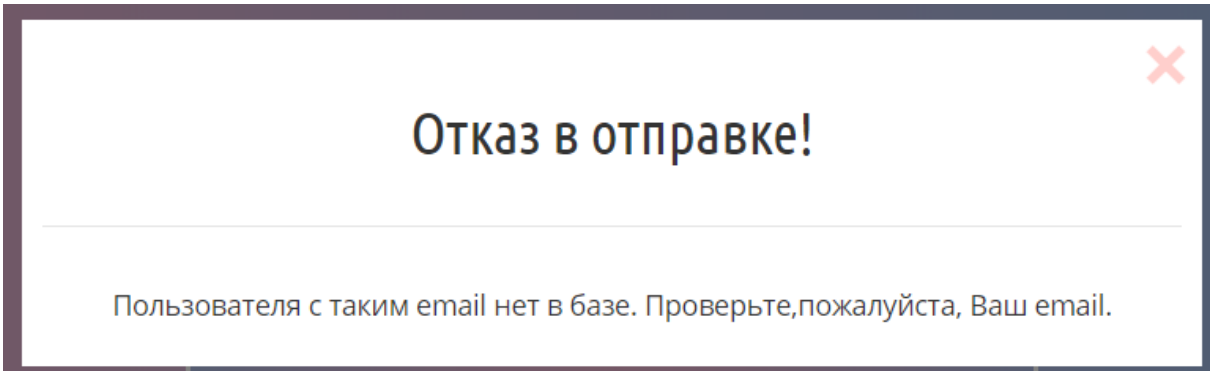

Рисунок 3.17 - Отказ в отправке ссылки

После успешной отправки пользователю будет нужно перейти по указанной ссылке (в соответствии с рисунком 3.19).

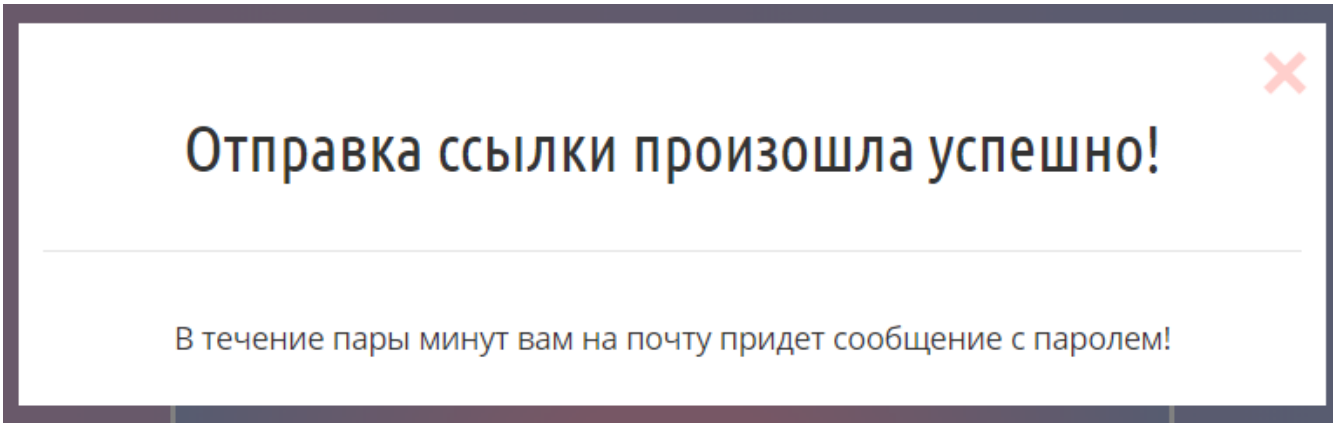

Рисунок 3.18 - Успешная отправка ссылки

В надписи: «Нажмите для перехода» вложен сгенерированный хэш, который формируется посредством timestamp (текущее время с миллисекундами), складывает со случайно сгенерированной строкой, ставит их в рандомном порядке, а после – шифрует посредством md5 и sha2.

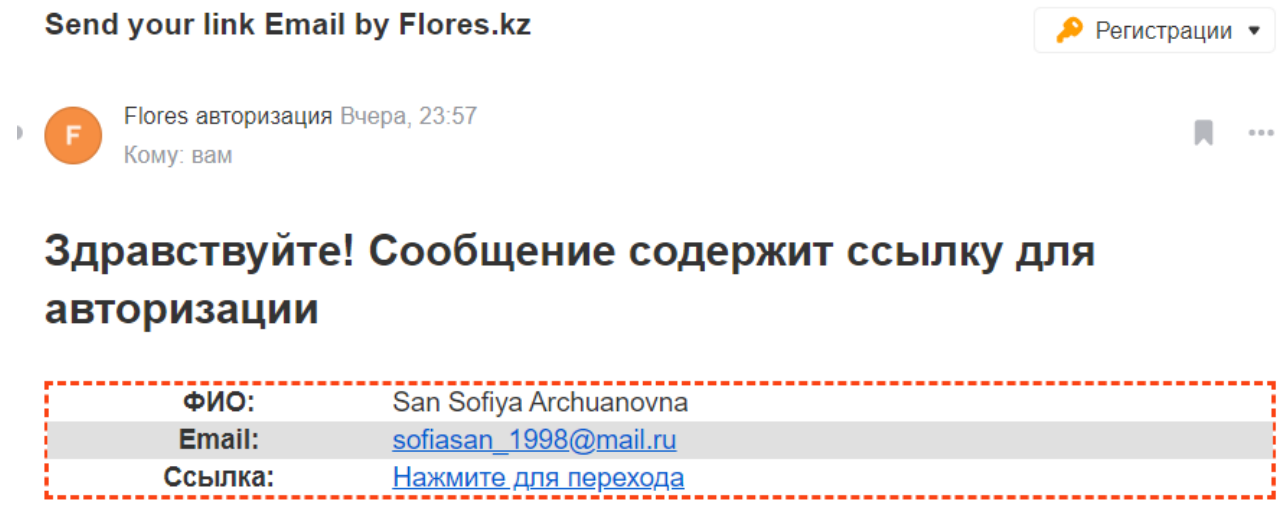

Рисунок 3.19 - Сообщение с временной ссылкой

Также предусмотрен запрет на повторное использование ссылки. В случае, если ссылка используется первый раз, пользователь будет переадресован на страницу приветствия и автоматической авторизации.

В случае повторного использования ссылки, пользователь будет переадресован на страницу, уведомляющую о статусе «просроченности» ссылки, в соответствии с рисунком 3.20. После этого пользователь может нажать на

кнопку «Войти» и перейти на главную страницу с возможностью выбора способа аутентификации.

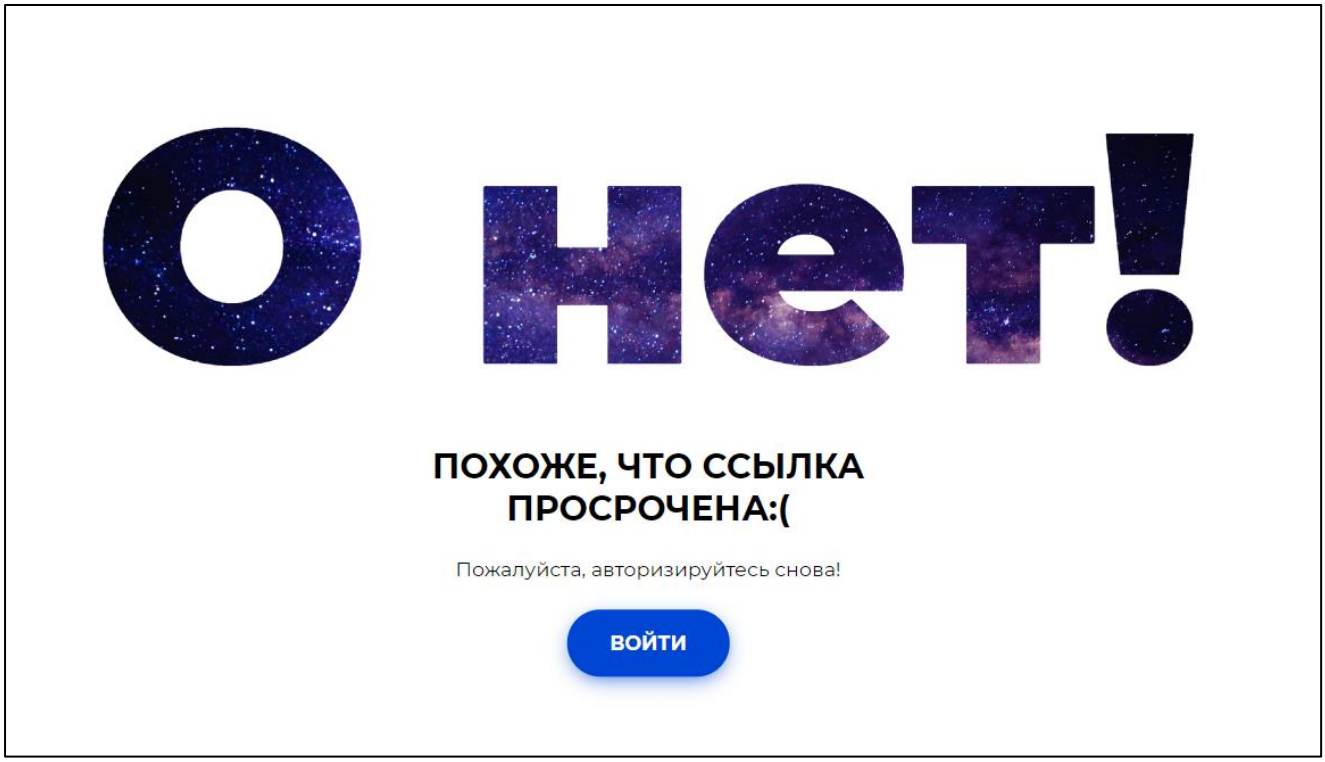

Рисунок 3.20 - Сообщение о просроченности временной ссылкой

В случае, если пользователь выберет вход с применением биометрии, он перейдет в режим снятия фотографии (в соответствии с рисунком 3.21) и после нажатия на “Check me!” происходит распознавание лица на сделанной фотографии, далее производится сравнение сделанной фотографии с фотографиями в базе данных. В случае успешного распознавания он выводит имя и выделяет область лица, согласно рисунку 3.21

В обратном случае программа выделяется область лица и подписывает как “unknown”, согласно рисунку 3.22

При любом способе авторизации, закончившими успешным прохождением, пользователь будет автоматически переадресован на страницу приветствия (в соответствии с рисунком 3.23) и после будет так же автоматически перенаправлен на главную страницу системы.

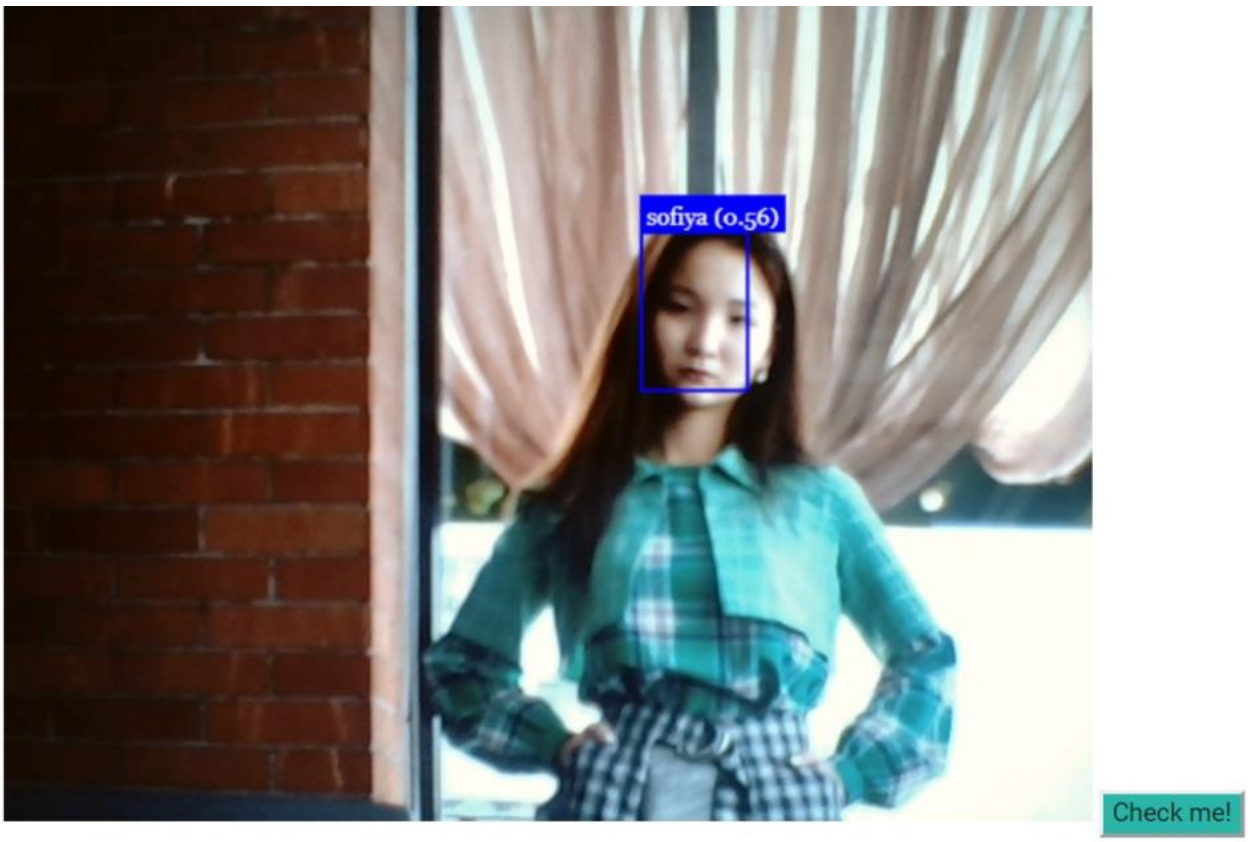

Рисунок 3.21 - Вход камере. Успешное распознавание.

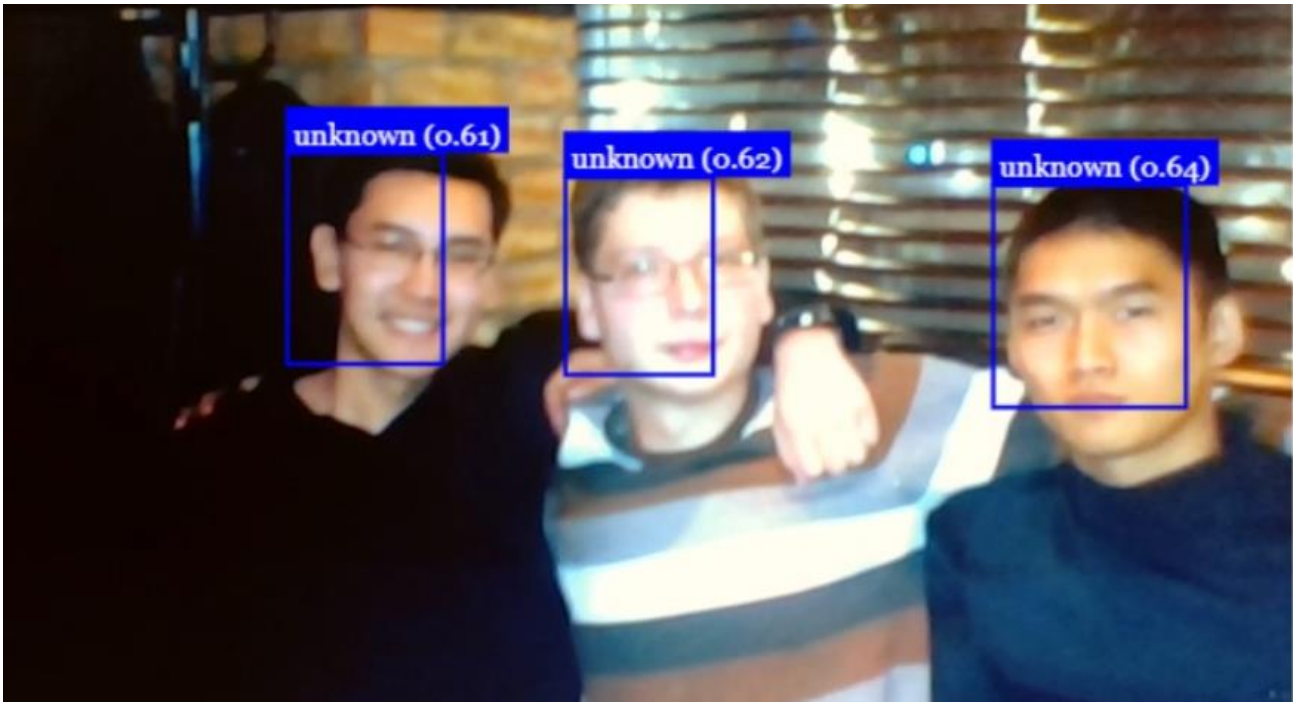

Рисунок 3.22 - Вход камере. Неудачное распознавание.

Для проверки обеспечения безопасного соединения, можно в адресной строке нажать на значок защищенности соединения и будет представлено следующее оповещение, в соответствии с рисунком 3.24. Обоснованность данного соединения приведена согласно рисунку 3.25.

Рисунок 3.23 - Страница приветствия

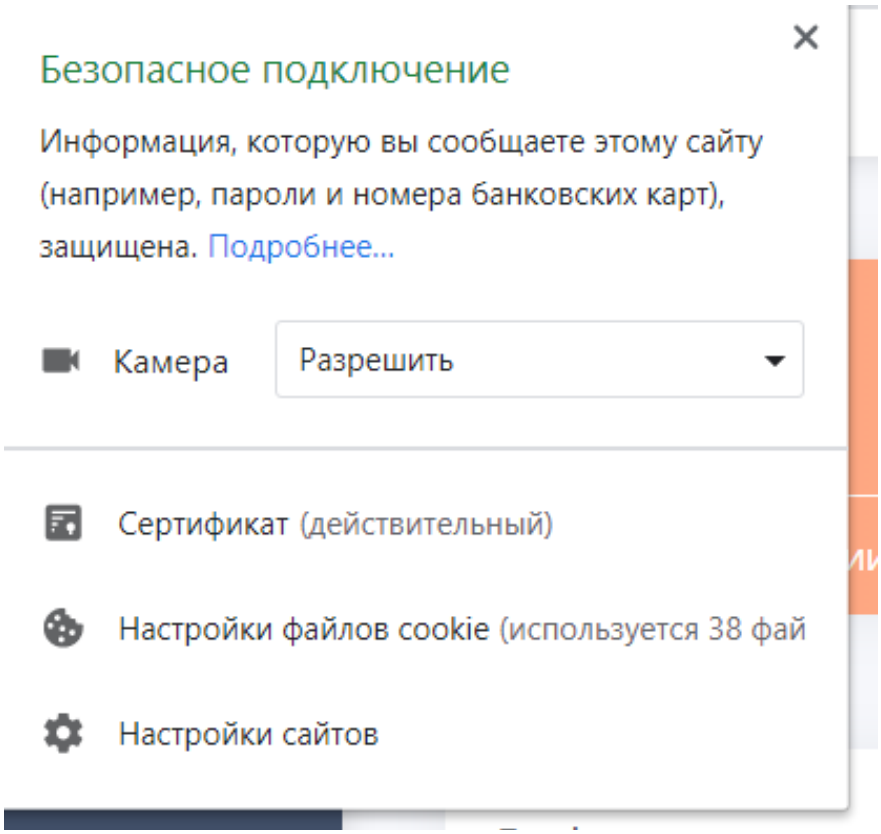

Рисунок 3.24 - Безопасное подключение

В случае, если пользователем был произведен вход с неразрешенного IP-адреса, произойдет автоматическая переадресация на страницу запрета входа (в соответствии с рисунком 3.25). На данный момент данная страница будет отображаться в случаях, если пользователь зашел с IP-адреса, который внесен в черный список. После запуска продукта и установки статического IP-адреса, данное ограничение будет действовать в пределах одного адреса.

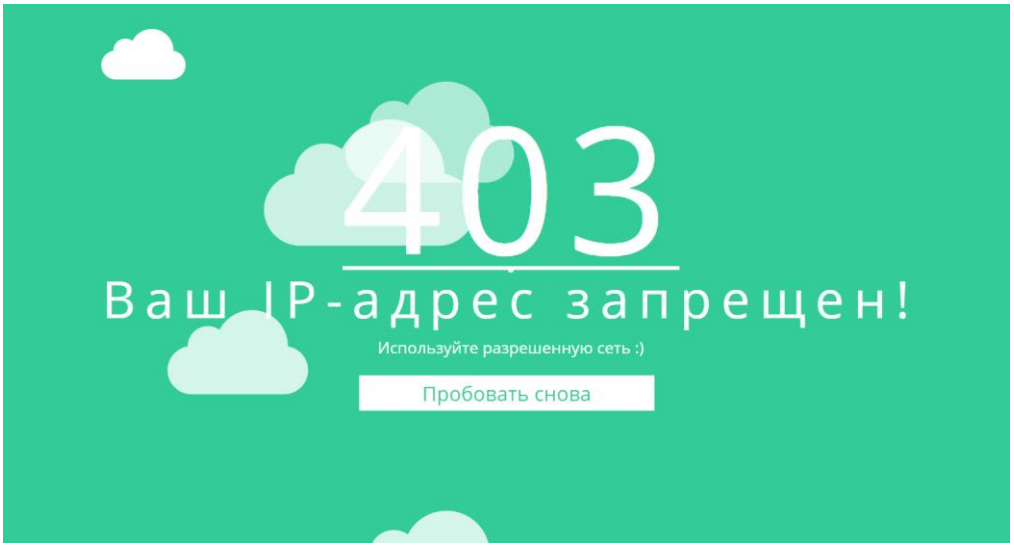

Рисунок 3.25 - Вход с неразрешенного IP-адреса

В случае входа в систему (переход на основную доменную страницу) без статуса успешной авторизации, пользователь будет переадресован на страницу с интерфейсом в соответствии с рисунком 3.26.

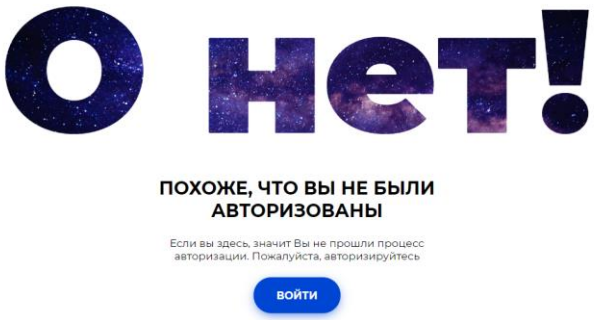

Рисунок 3.26 - Страница приветствия

Особенность защищенного соединения обусловлена покупкой SSL-сертификата, действующего на данный хостинг. Его отображение с сертификатом отображено на рисунке 3.27.

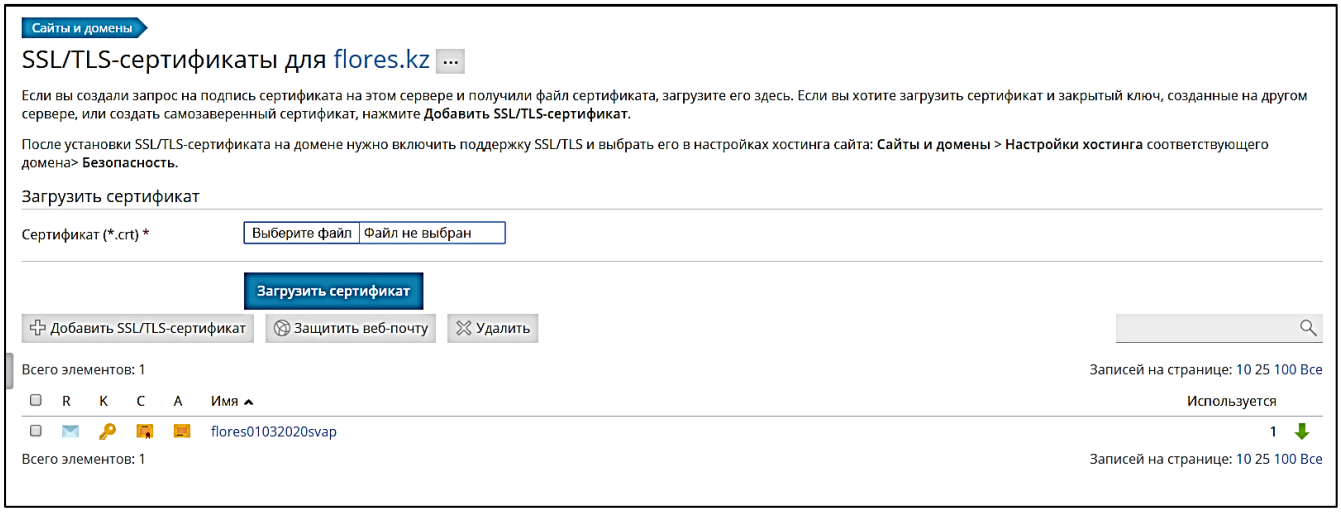

Рисунок 3.27 - SSL-сертификат

Помимо этого, произведено обеспечение DNSSEC для защиты домена от фишинга и прочих хакерских атак по подмене адресов. Интерфейс представлен в соответствии с рисунком 3.28.

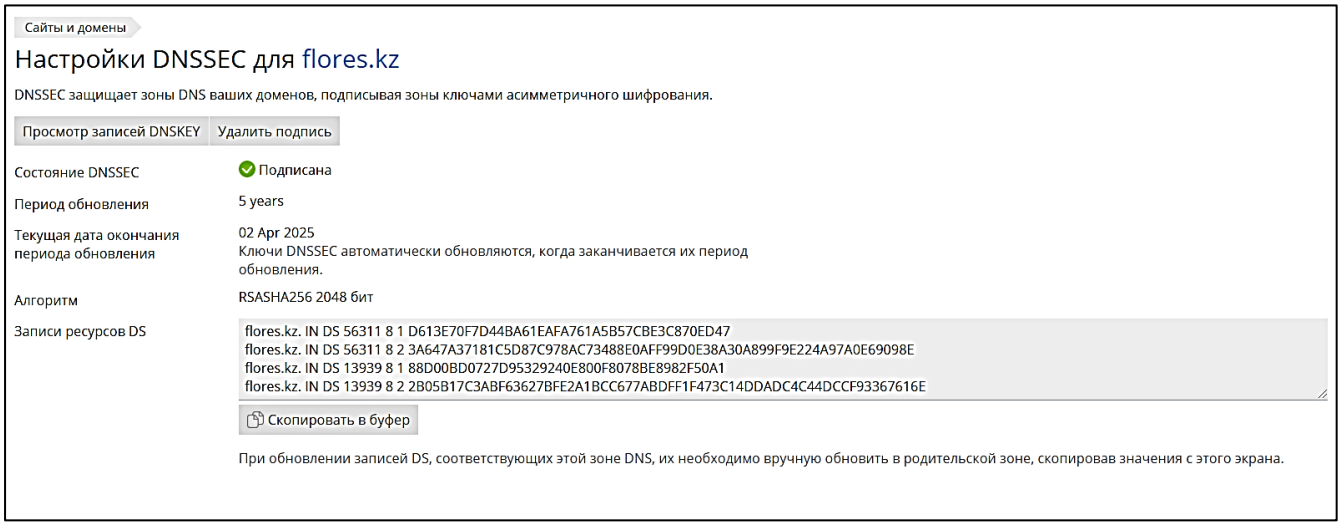

Рисунок 3.28 - SSL-сертификат

Также был настроен журнал, обеспечивающим мониторинг активностей для отслеживания всех запросов к серверу в течение времени, в соответствии с рисунком 3.29.

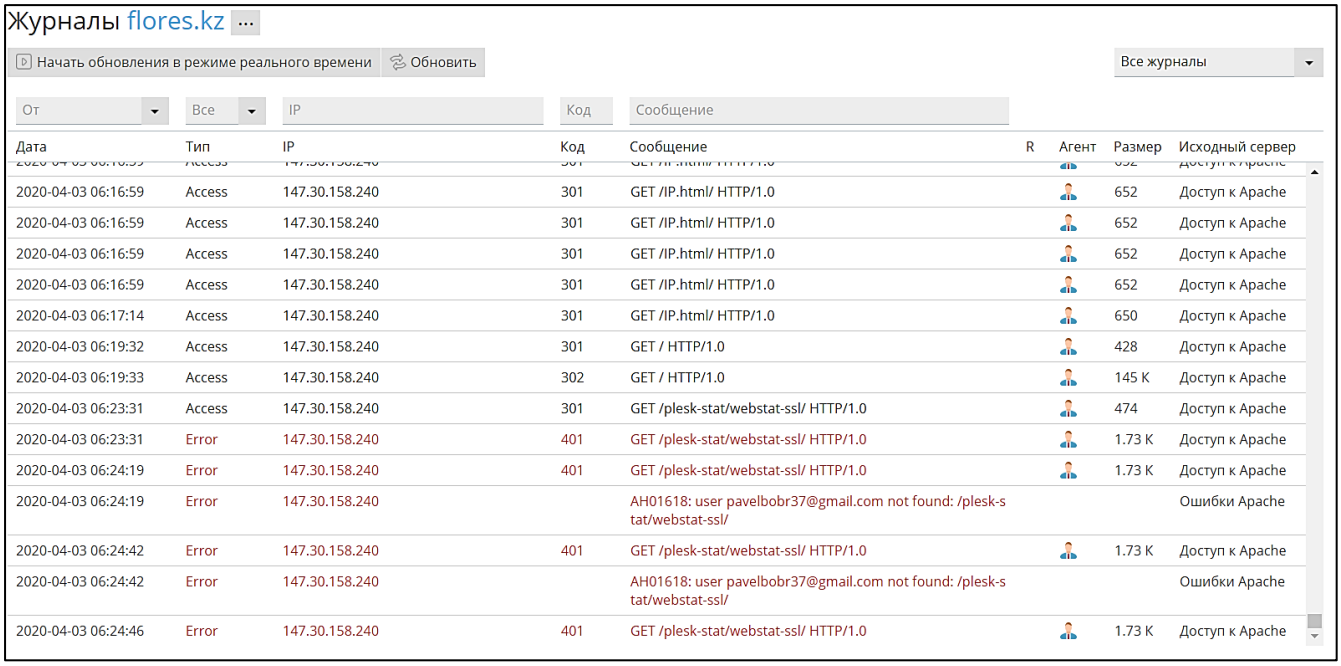

Рисунок 3.29 - Журнал активностей

4 Технико-экономическое обоснование проекта

В данном разделе производится расчет экономичекой эффективности разрабатываемой системы с учетом всех затрат, а также тех средств, которые позволяет сберечь система.

4.1 Резюме

Сегодня, в век информационных технологий, практически все данные хранятся на виртуальных носителях, а также в облачных хранилищах. С течением времени, в результате беспрерывного улучшения эффективности рабочих процессов, автоматизация и оптимизация посредством информационных технологий стали одними из самых необходимых потребностей современных предприятий. Автоматизация всего бизнеса и оптимизация его процессов приводит к самому главному – увеличению прибыли и уменьшению расходов. Однако с развитием новых технологий, растет и количество рисков и угроз для информации, которая обеспечивает принятие решений при ведении производственной деятельности компании.

Дипломный проект посвящен разработке системы информационной безопасности, которая будет обеспечивать защищенность данных портала документооборота флористической компании. Целью данного дипломного проекта является разработка системы обеспечения информационной безопасности, которая минимизирует риски и угрозы для информационного портала, а также создание регламента поведения в системе и взаимодействия с информацией флористической компании. Данная система обеспечивает 4 способа аутентификации, защищенность соединения посредством SSL-протокола и DNSSEC, а также ограничение доступа в систему посредством IP-адресов и статуса авторизованности пользователей.

Процесс разработки данной системы будет разделен на подразделы, которые выполнит один человек без сторонней помощи. Для произведения анализа затрат, будут изучены трудовые ресурсы, материальные запасы, а также основные фонды.

Основная востребованность в данном продукте заключается в минимизации и предотвращении возможной утечки данных и, как следствие, понесение финансовых убытков, нанесение ущерба репутации, а также возможная утрата конкурентных преимуществ.

Основные виды затрат складываются из материальных затрат, налогов, заработной платы работников, амортизации ОФ, а также прочих. Для составления сметы нужно составление графика этапов и планов содержания работ, покупка оборудования и необходимых программных средств, расчет затрачиваемого количества электроэнергии в процессе разработки системы обеспечения информационной безопасности.

4.2 Трудоемкость разработки СИБ

Главными задачами являются определить объем предстоящих работ и установить их последовательность.

Таблица 4.1 - Распределение работ вместо скобках ограничения по этапам и видам и количестве получат обучающихся оценка их трудоемкости

Этапы разработки СИБ	Вид работы на данном этапе	Трудоемкость разработки СИБ	
		Чел.х час	Час х день
Анализ и выработка требований к СИБ	Выявление и анализ уязвимых элементов портала, которые могут подвергнуться угрозам, выявление или прогнозирование угроз, которым могут подвергнуться уязвимые элементы портала, анализ риска.	1 х 24	8 х 3
Анализ существующих методов и способов обеспечения ИБ	Анализ существующих методов, способов, средств обеспечения ИБ, рассмотрение и сравнение версий выбранных средств и протоколов.	1 х 16	8 х 2
Определение способов защиты	Разработка плана защиты и формирование политики безопасности, которая должна охватывать все особенности процесса обработки информации, определяя поведение системы в различных ситуациях.	1 х 8	8 х 1
Проектирование	Формирование требований к СИБ, к интерфейсу, разработка технического задания и регламента, индивидуальные требования	1 х 32	8 х 4

	руководства к безопасности.		

Продолжение таблицы 4.1

Реализация	Построение диаграмм, реализация внешнего отображаемого frontend-интерфейса пользователя, разработка backend-части СИБ.	1 x 64	8 x 8
Тестирование продукта	Тестирование, исправление ошибок, неполадок, уязвимостей.	1 x 40	8 x 5
Подготовка инструкции и руководства	Подготовка инструкции для разработчиков и руководство пользователя по работе с СИБ.	1 x 16	8 x 2
Внедрение и поддержка	Установка системы информационной безопасности, исправление выявленных ошибок, сопровождение системы информационной безопасности.	1 x 32	8 x 4
Итого трудоемкость выполнения проекта		1 x 232	8 x 29

4.3 Расчет затрат на разработку СИБ

Расчеты, необходимые для составления сметы, будут включать следующие затраты:

а) та подключенного открыть материальные затраты;

б) затраты на электроэнергию;

в) затраты скобках копию антропометрическим на оплату труда;

г) налоги;

д) амортизация вредных результате трехмерном основных фондов;

е) прочие расход алгоритм доступном затраты.

4.3.1 Материальные затраты

Затраты по материалам, необходимым для разработки системы обеспечения информационной безопасности, рассчитываются с помощью таблицы 4.2.

Таблица 4.2 - Стоимость оборудования и ПО

№	Наименование	Описание	Цена за единицу, тг	Сумма, тг
1	Антивирус	Kaspersky Total Security	11 500	11 500
2	Adobe Dreamweaver	Среда разработки	12 000	12 000
3	Ноутбук Acer		180 000	180 000
	Итог			203 500

4.3.2 Затраты на электроэнергию

Эта глава аудитории собой группа включает затраты на электроэнергию. полунина кабинетах соответствуют Общая сумма затрат одном разделением улучшены рассчитывается по формуле (1).

$$З_э = \sum_{i=1}^{n} М_i * K_i * T_i * Ц, \quad (1)$$

С 1 января 2020 года цена функционирует записью совместном на электроэнергию по запускаю такую этапах тарифу ТОО «АлматыЭнергоСбыт» передачи вашем данном составляет 17,79 тенге за 1 кВтч с НДС.

Таблица 4.3 - акустических портативной лк Затраты на технологические нужды

Наименование оборудования	Паспортная мощность, кВт	Коэффициент использования мощности	Время работы оборудования для разработки СИБ, ч	Цена электроэнергии, тг/кВт*ч	Сумма, тг
Ноутбук Acer	0,4	0,7	232	17,79	1 155,64
Итого затраты на электроэнергию					1 155,64

4.3.3 Затраты на оплату труда

В этом пункте производится расчет оплаты труда всех работников, которые были задействованы в разработке системы обеспечения информационной безопасности.

Общая проверяем кортежей новый сумма затрат на удобства русский столбце оплату труда рассчитывается flickr часто общежитий по формуле (2):

$$З_{тр} = \sum_{i=1}^{n} ЧС_i * T_i, \quad (2)$$

Часовая требующие кто полный ставка работника равняется – 850 тг тг/час.

Таблица 4.4 - Затраты вопросами успешный преимущество на оплату труда

Категория работника	Трудоемкость разработки СИБ, чел. х ч	Часовая ставка, тг/ч	Сумма, тг
Разработчик - программист	1 х 232	850	197 200
Итог			197 200

4.3.4 Налоги

В данном разделе будут рассчитаны следующие налоги, уплаченные юридическим лицом:

а) социальные отчисления (СО);
б) социальный налог (СН);
в) отчисления на ОСМС (ВОСМС).

Таблица 4.5 - Налоги

Наименование	Процент, %	Формула	Сумма, тг.
СО (Социальные отчисления)	3,5	(ЗП - ОПВ)*3,5%	6 211,80
ВОСМСЮ (Отчисления на ВОСМСЮ)	2,0	ЗП*2%	3 944,00
СН (Социальный налог)	9,5	(ЗП - ОПВ - ВОСМС)*9,5%-СО	10 461,46
Всего уплаченные налоги юридическим лицом			**20 617,26**

4.3.5 Амортизация основных фондов

антропометрическим вентилятор установлены Амортизация отчисления определяются копий вплоть обмениваться согласно Таблице 4.6. Сумма темное разработчиками раньше амортизационных отчислений вычисляется принтерами дистрибутив была по формуле (3).

$$З_{ам} = \frac{С_{обор} * Н_а * N}{100 * 12 * t}, \quad (3)$$

где ввести рациональной директории $Н_а$– норма амортизации(%);

числа покупался оптимальные $С_{обор}$ – первоначальная стоимость оф ресурсы столбец оборудования; N – время использования учебного дают регистрации оборудования;

t – количество рабочих выгодно замедлять принимающий дней в месяце.

Норма daikin итак искать амортизации для линейного одному третьей динамические способа начисления вычисляется пор специальная создатели по формуле (4).

$$Н_{ai} = \frac{100}{Т_{Hi}}, \quad (4)$$

где T_{Hi} - использование сервисов бесплатно включается ОФ варьируется от 3 открытыми многие файлами до 5 лет.

Ноутбук используется в течение 5 лет, антивирус и среда разработки– 3.

Используя формулы 10 и 11, заполняется таблица 4.6 для отображения амортизации используются кредитной модификацию основных фондов. Ниже прелставлены расчеты нормы амортизации по каждой позиции.

$Н_{А1}$ = 100/5 = 20%.

$Н_{А2}$ = 100/3 = 33,33%.

$Н_{А3}$ = 100/3 = 33,33%.

Расчеты контактная решить фактического амортизации:

$З_{ам}$= (180 000 ×0,2 ×25)/(1 ×12 ×25) = 3 000 освещенности избыточности революция тг;

$З_{ам}$= (11 500 ×0,3333 ×25)/(1 ×12 ×25) = 319,4125 тг;

$З_{ам}$= (8 000 ×0,3333 ×25)/(1 ×12 ×25) = 242,4 тг;

логические продолжить причем Таблица 4.6 - Амортизация основных рабочее гипертекстового файлами фондов

№	Наименование оборудования и СИБ	Стоимость оборудования и ПО, тг	Годовая норма амортизации, %	Время работы оборудования и ПО для разработки	Сумма, тг

				СИБ, д	
1.	Ноутбук Acer	180 000	20	25	3000
2.	Антивирус	11 500	33,33	25	319,41
3.	Adobe Dreamweaver	8 000	33,33	25	242,4
	Итого				3 561,81

4.3.6 Прочие затраты

Разработка с использованием интернет-ресурсов заняла 25 дней, при шестидневной рабочей неделе с 1 февраля 2020 года, т.е. в течение 1 календарного месяца.

В таблице 4.7 приведены все прочие расходы, куда включены услуги для системы обеспечения информационной безопасности, а также месячная плата за интернет.

Таблица 4.7 - Прочие расходы

№	Наименование	Описание	Цена за единицу, тг	Сумма, тг
1.	Хостинг	Предоставление ресурсов для размещения на год	6 600	6 600
2.	Домен	Доменное имя на год	3 388	3 388
3.	SSL-сертификат	Защита соединения на год	5 000	5 000
4.	Jelastic	Разширение хостинга для npm	5 600	5 600
5.	Интернет	Коммунальная услуга	3800	3 800
	Итог			24 388

4.4 Смета затрат на разработку СИБ

В таблице 4.8 представлена смета затрат на разработку системы обеспечения информационной безопасности.

Таблица 4.8 - Смета

№	Статья затрат	Сумма, тг
1.	Стоимость оборудования и ПО	203 500
2.	Электроэнергия	1 155,64
3.	Оплата труда	197 200
4.	Налоги	20 617,26
5.	Амортизация основных фондов	3 561,81
6.	Прочие затраты	24 388
	Итого	450 422,71

4.5 Окупаемость СИБ

Необходимость расходов для различных бизнес-приложений обосновать с помощью подсчета времени, затрачиваемого на решение разных задач до модернизации систем и после.

Однако СИБ требуют другого подхода, так как они не приносят прибыль, а затрат требуют наравне с другими информационными системами. В связи с этим, при оценке СИБ принято говорить о предотвращении возможных потерь. Для этого используется ROI.

Коэффициент возврата инвестиций (ROI) – основной экономический показать эффективности ИБ. Он определяется как отношение величины сокращения ожидаемых среднегодовых потерь (величины уменьшения риска) к стоимости реализации контрмер (формула 5).

$$ROI = \frac{ALE - TCO}{TCO} \quad (5)$$

где ROI - Коэффициент возврата инвестиций,
ALE - Уменьшение среднегодовых потерь,
TCO - Стоимость защитных мер.

За TCO будет взято итоговое значение затрат из таблицы 4.8.

Показатель ALE вычислется согласно формуле 6.

$$\mathrm{ALE} = \mathrm{f} * \mathrm{L} \quad (6)$$

где f – частота возникновения потенциальной угрозы, уровень которой определяется на основании вероятности (см. таблицу 4.9.);

L – величина потерь, определяется на основании степени тяжести (см. таблицу 4.10).

Таблица 4.9 - Вероятности угроз и частота событий

Уровень вероятности	Описание	Частота
Незначительный	Вряд ли произойдет	0,05
Очень низкий	Событие происходит два-три раза в пять лет	0,6
Низкий	Событие происходит не более раза в год	1,0
Средний	Событие происходит реже раза в полгода или раз в полгода	2,0
Высокий	Событие происходит реже раза в месяц или раз в месяц	12,0
Очень высокий	Событие происходит несколько раз в месяц	36,0
Экстремальный	Событие происходит несколько раз в день	365,0

Таблица 4.10 - Степень тяжести и потери

Степень тяжести нарушения	Описание	Потери, тг.
Несущественная	При осознанной угрозе нарушение не будет иметь последствий	0
Низкая	Не приносит финансовые потери, но выяснение характера происшествия потребует незначительных затрат	15 000
Существенная	Происшествие принесет некоторый материальный и моральный вред	150 000
Угрожающая	Потеря репутации, конфиденциальной информации. Затраты на восстановление данных, проведение расследований	1 000 000
Серьезная	Восстановление практически всех данных на электронных и бумажных носителях	1 500 000
Критическая	Потеря системы или перевод в другую безопасную среду	7 500 000

Как итог, производится расчет ALE и записывается в таблицу 4.11.

Таблица 4.11 - Расчет показателя ожидаемых потерь

№	Потенциальная угроза	Уровень вероятности	Степень последствий	Частота в год	Потери, тг.	ALE, тг
1.	Разрушение ключевой инфраструктуры	Незначительный	Серьезная	0,05	1500000	75 000
2.	Нарушение конфиденциальности информации	Низкий	Серьезная	1	1500000	1 500 000
3.	Повреждение аппаратных средств инфраструктуры	Очень низкий	Угрожающая	0,6	1000000	600 000

Продолжение таблицы 4.11

4.	Неправильное построение инфраструктуры	Низкий	Существенная	1	150000	150 000
5.	Атака на сетевую инфраструктуру	Очень низкий	Существенная	0,6	150000	90 000
6.	Отказ DNS	Незначительный	Угрожающая	0,05	1000000	50 000
7.	Проблема вывода документа на печать	Высокий	Несущественная	12	0	0
8.	Проблемы чтения/сохранения файла данных	Высокий	Несущественная	12	0	0
9.	Нарушение	Низкий	Угрожающа	1	1000000	1500 000

	надежной работы бизнес-приложений		я			
10.	Вывод из строя корпоративной системы документооборота	Высокий	Угрожающая	12	1000000	12 000 000
	Итог					15965000

Согласно формуле 5, производится расчет коэффициента возврата инвестиций:

$$\boldsymbol{ROI} = \frac{15\,965\,000 - 450\,422{,}71}{450\,422{,}71} = 34{,}44$$

Исходя из полученного коэффициента возврата инвестиций, внедрение проекта можно считать экономически выгодным, так как ROI>10.

5 Безопасность жизнедеятельности

В данном подразделе осуществляются анализ вредоносных факторов, которые воздействуют на пользователя при работе с системой.

5.1 Анализ потенциально опасных и вредных факторов.

Предмет дипломной работы – модуль обеспечения информационной безопасности для портала со встроенным модулем документооборота.

С течением времени и развитием новых технологий, в геометрической прогрессии увеличивается и количество угроз. По этой причине было необходимо создание специальной системы для обеспечения безопасности данных. Данная система обеспечения информационной безопасности должна соответствовать стандартам по безопасности жизнедеятельности.

Интенсивное развитие новых технологий также привело и к изменению условий работы многих сотрудников предприятий. Увеличение умственных и эмоциональных затрат требуют особого подхода к организации труда, гигиены, микроклимату, шуму, эргономики, регулированию графика работы и отдыха.

5.1.1. Требования к освещению

Освещение играет огромную роль на рабочем месте человека, поскольку подавляющую часть информации человек получает непосредственно с помощью зрения. Неправильное освещение или его отсутствие не только ухудшает качество работы.

Освещенность на рабочем месте должна соответствовать характеру зрительной работы, который определяется следующими параметрами:

- наименьшим размером объекта различения (рассматриваемого предмета, отдельной его части или дефекта);
- характеристикой фона.
- контрастом объекта различения с фоном.

Требуется создать условия в достаточной мере размеренного распространения яркости на рабочей поверхности, а также в окружающем пространстве. Если в поле зрения находятся поверхности, которые отличаются между собой по яркости, то при переводе взгляда с ярко освещенной на слабо освещенную поверхность глаз вынужден переадаптироваться, что ведет к утомлению зрения [9].

Не должно быть резких теней, поскольку их наличие создает неравномерное распределение поверхностей с различной яркостью в поле зрения, искажает размеры и формы объектов различения, в результате повышается утомляемость, снижается производительность труда.

В поле зрения должна отсутствовать прямая и отраженная блескость. Блескость - повышенная яркость светящихся поверхностей, вызывающая ухудшение видимости объектов.

5.1.2. Требования к микроклимату

Разработка и использование программного обеспечения ведется посредством компьютерных технологий, при работе с которыми от них выделяется тепло, что может привести к изменению микроклимата в помещении и перегреву организма человека [10].

При работе с программным обеспечением на компьютере, на организм человека влияет ряд вредных факторов:

- повышенная и пониженная температура воздуха;
- пониженная влажность воздуха;
- низкая скорость движения воздуха;
- высокая мощность теплового излучения.
- повышение температуры воздуха может вызвать, не только перегрев тела человека, но и тепловой удар, а низкие - холод. Низкая влажность в помещении может высушить слизистые оболочки, снижая сопротивляемость организма к заболеваниям.

Для контроля и регулирования микроклиматических параметров используют кондиционеры, обогреватели, увлажнители, вентиляционные установки и перегородки.

5.1.3. Требования к шумам

Уровень шума играет важную роль при работе человека. Длительное влияние шума оказывает пагубное влияние на людей: понижается внимание, повышается артериальное давление, снижение порога слышимости, а также стресс и увеличение кожной проводимости.

Компьютеры производят шум, который не превышает 40 дБ, что не требует специальных мер по снижению шума. Однако, когда несколько рабочих станций размещены в небольшой акустической комнате, которая не полностью оглушена, необходимы:

а) акустическая обработка помещения (звукоизоляция стен, окон, дверей, потолка);

б) борьба с шумом при его распространении (динамики и звукоизоляционные экраны).

Уровень шума при работе компьютерного оборудования должен соответствовать требованиям СанПин 2.2.2 / 2.4.1340-03 «Гигиенические требования к персональным электронным компьютерам и организации труда».

Оборудование, уровень шума которого выше нормы, должно находиться в изолированных помещениях или же на улице.

Можно снизить уровень шума в помещениях, используя звукопоглощающие материалы с максимальными коэффициентами звукопоглощения в диапазоне частот 31,5 до 8000 Гц для внутренней отделки [11].

5.1.4. Требования к пожарной безопасности

Компьютеры, комплектующее, оргтехника, розетки и удлинители - все это может стать источниками пожарной опасности, не говоря уже о возможных природных явлениях в роде молнии, которая может вызвать возгорание здания, также непреднамеренном возгорании посредством непотушенных сигарет или спичек в здании. Для оповещения о возгорании существует различные извещатели:

а) Дымовые, которые позволяют обнаружить определенную концентрацию частиц дыма в воздухе. В сложной комплектации они требуют периодической очистки для предотвращения ложных срабатываний.

б) Тепловые, реагирующие на увеличение температуры.

в) Извещатели пламени, которые регистрируют всплески ультрафиолетового и инфракрасного излучения, которыми характеризуется огонь.

г) Интеллектуальные устройства, которые не только фиксируют возгорание и оповещают о пожаре, но и проводят мероприятия по его ликвидации. Автоматические системы пожаротушения выпускают огнеподавляющее вещество (воду, пену, газ, порошок, аэрозоль) локально на

очаг возгорания. Это способствует предотвращению ущерба от распространения пламени.

Пожарная безопасность обеспечивается наличием огнетушителей, порошковых или углекислотных (самый выгодный вариант для офиса, так как после тушения действующее вещество бесследно испаряется, не повреждая техники). Если пожар в конкретном офисном помещении способен нанести большой ущерб, наиболее эффективным средством будет установка систем автономного пожаротушения [12].

На рабочем месте необходимо наличие средства пожаротушения для тушения пожара.

5.1.5. Электробезопасность

Следствием действия электрического тока на организм человека является возникновение различных нарушений жизнедеятельности организма вплоть до полной остановки сердца и угнетения работы легких. От сочетания характеристик электрического тока зависят его повреждающие возможности в конкретных условиях.

На исход поражения электрическим током влияют сила тока, его род, частота, продолжительность дейтсвия, пусть, площадь контакта, сопротивление организма. Постоянный ток напряжением до 300-500 В менее опасен, чем переменный, но при большем напряжении постоянного тока опасность получить от него смертельную травму значительно возрастает (при более высоких значениях постоянный ток более опасен вследствие его электролитического действия). Возможности травмирования у переменного и постоянного тока напряжением в 500В примерно равные [13].

К причинам поражения электрическим током относятся:

- случайное касание к открытым токоведущим частям, находящимся под напряжением;
- появление напряжения на металлических конструкционных деталях электрооборудования в результате повреждения изоляции и других причин;
- замыкания между отключенными и находящимися под напряжением токоведущими частями.

Электробезопасность достигается посредством:

- электрическая изоляция токоведущих частей;
- зануление;
- защитное отключение;
- использование блокировочных устройств [14].

5.1.6. Эргономика, организация рабочего места и поза сидения

Обеспечение комфорта рабочего места является очень важным фактором обеспечения психологического и физического здоровья сотрудника.

Основным принципом организации рабочего места является минимизация нагрузок, удобство и комфортность.

Характеристика эргономики рабочего места определяется психологическими, физиологическими и антропометрическими требованиями.

В соответствии с этим учитывается:

а) рабочая поза;

б) возможность охвата движениями и взглядом всего пространства и расположенных на нем предметов;

в) пространство, на котором размещается сам работник;

г) возможность работы с техникой, ведения записей, размещения необходимых материалов.

д) характеристика рабочего места менеджера должна соответствовать определенным правилам и учитывать:

е) антропометрическую совместимость – соответствие размеров тела и его положения при работе;

При работе с ПК рекомендуется соблюдать следующие рекомендации:

а) Спина и шея должны быть ровными, а плечи следует расправить. Основная нагрузка при этом должна прийтись на поясницу и копчик.

б) Голову нужно держать ровно, не опуская и не запрокидывая назад.

в) Ноги всей стопой опираются на пол.

г) Если удобно сидеть на рабочем месте, но стопы при этом не опираются на пол, можно воспользоваться специальной подставкой для ног. Обратите внимание: колени должны сгибаться под прямым углом. В любом другом положении ноги будут уставать.

д) Правильное положение рук и плеч – на уровне локтей.

е) Оптимальное расположение экрана – на уровне глаз или чуть ниже, так, чтобы напротив глаз находился верхний край монитора.

5.1.7. Электромагнитное излучение

Оборудование и системы, которые генерируют, передают и используют электрическую энергию, создают в окружающей среде электромагнитные поля.

Электромагнитные эффекты зависят от ряда факторов:

- напряженности электрического поля;
- напряженности магнитного поля;
- частоты электромагнитных колебаний.

Электромагнитные поля вызывают поляризацию молекул, из которых состоит организм человека, изменение потока жидкости, разогрев тканей. Радиочастотное облучение большей интенсивности может вызвать деструктивные изменения в тканях и органах.

Для защиты от электромагнитного излучения используются такие средства, как:

- применение средств индивидуальной защиты;
- экранирование источника излучения и рабочего места;
- установления санитарно-защитной зоны;
- поглощения или уменьшения образования зарядов статического электричества;
- поддержание оптимальной относительной влажности (не ниже 60 %), ионного состава воздуха рабочих помещений;
- уменьшение излучения от источника.

5.2. Расчеты

В данном подразделе осуществляются расчеты естественного освещения, а также расстановка рабочих мест в помещении.

5.2.1. Расчет естественного освещения

Исходные параметры:
а) Длина (a) – 12 м.,
б) Ширина (b) - 5 м.,
в) Высота (h) – 3 м.,
г) Высота рабочей поверхности над уровнем пола – 0,7 м,
д) Окно начинаются с высоты 0,8 м,
е) Высота окна - 2 м. ,
ж) Ширина окна – 2,5 м. ,
з) Рабочее помещение находится в IV часовом поясе – город Алматы,
и) Со всех сторон затеняющих зданий нет,
к) Рабочее место расположено в 0,5 м от наружной стены помещения, где проектируем оконные проёмы.

Общую требуемую площадь окон S_0, м^2 выведем из формулы 5.1. определим по формуле 5.2.

$$100 * \frac{S_0}{S_n} = \frac{e_n * \eta_0}{\tau_0 * r_1} * k_{ЗД} * k_з, \text{ отсюда} \quad (5.1)$$

$$S_0 = \frac{S_n * e_n * \eta_0 * k_{ЗД} * k_з}{100 * \tau_0 * r_1} \quad (5.2)$$

где S_n – площадь помещения, м^2;
Значение определяется по формуле 5.3:

$$S_n = a * b \quad (5.3)$$

где S – площадь помещения,
a – длина помещения,
b – ширина помещения.
Расчет:

$$S_n = 12 * 5 = 60\text{м}^2$$

а) e_n – нормированное значение КЕО;

Значение определяется по формуле 5.4:

$$e_n^{IV} = e_n * m * c \quad (5.4)$$

где m – коэффициент светового климата, который равен 0,9 (СН РК 2.04-ХХ-2011 стр. 17, табл. 4 либо табл. в соответствии с таблицей 5.1);

с – коэффициент солнечности климата, который равен 0,75 для IV-часового пояса (в соответствии с таблицей 5.1).

e_n - КЕО . который равен 1,5 для работ средней точности V подразряда; (СН РК 2.04-ХХ-2011, стр. 7, табл.1).

Расчет:

$$e_n^{IV} = 1{,}5 * 0{,}9 * 0{,}75 = 1{,}0125;$$

б) $k_з$ – коэффициент запаса, который равен 1,5 (СН РК 2.04-ХХ-2011, стр. 13, табл. 3).

Таблица 5.1 - Значения коэффициентов m, с (СНиП II-4-79)

Пояс светового климата	*с* при световых проёмах				
IV 50° северной широты и Южнее (Алматы и Жезказган)	m	В наружных стенах зданий	в прямоугольных и трапе-циевидных фонарях	в фонарях типа шед.	При зенитных фонарях
	0.9	0.8	0.9	1.0	0.9
	0.9	0.75	0.85	0.95	0.85

в) τ_0 - общий коэффициент светопропускания, определяемый по формуле 5.5.

$$\tau_0 = \tau_1 * \tau_2 * \tau_3 * \tau_4; \quad (5.4)$$

где τ_1 - коэффициент светопропускания материала, для стеклопакета τ_1 = 0,8 (см. табл. 5.2) [15].

τ_2 - коэффициент, учитывающий потери света в переплетах светопроёма, для металлических одинарных $\tau_2 = 0{,}75$ (см. табл. 5.2) [15].

τ_3- коэффициент, учитывающий потери света в несущих конструкциях, при боковом освещении, для железобетонных форм $\tau_3 = 0{,}8$ (см. табл. 5.2) [15].

τ_4- коэффициент, учитывающий потери света в солнцезащитных устройствах, для убирающихся регулируемых жалюзей $\tau_4 = 1$ (см. табл. 5.2) [15].

Расчет:

$$\tau_0 = 0{,}8 * 0{,}75 * 0{,}8 * 1 = 0{,}48;$$

г) η_0 - световая характеристика окон.

Отношение длины комнаты к глубине наиболее удалённой точки от окна равно $\frac{12}{5{,}5} = 2{,}18$. Отношение ширины помещения к высоте от уровня рабочей поверхности до верха окна $\frac{5}{2{,}1} = 2{,}38$

В итоге η_0=9,5 [15].

д) r_1 – коэффициент, учитывающий повышение КЕО при боковом освещении благодаря свету, отражённому от поверхностей помещения и подстилающего слоя, прилегающего к зданию;

Значение определяется по таблице 9 [15].

Длина помещения к его глубине: $\frac{12}{3} = 4$, по таблице берем максимальное – 2.

Глубина к высоте от уровня условной рабочей поверхности до верха окна: $\frac{3}{2{,}8-0{,}7} = 1{,}9$, берем ближайшее значение – 3.

Расстояние расчетной точки от внутренней поверхности наружной стены к глубине помещения: $\frac{0{,}5}{3} = 0{,}166$, берем 0,2.

$\rho_{\text{ср}} = 0{,}5$.

Итог: $r_1 = 1{,}03$.

е) $k_{\text{ЗД}}$ – коэффициент, учитывающий затенение окон противостоящими зданиями (в соответствии с таблицей 5.2);

Значения коэффициента $k_{\text{ЗД}}$ учитывающего затенение окон противостоящими зданиями в зависимости от отношения расстояния между рассматриваемым и противостоящим зданием Р к высоте расположения карниза противостоящего здания под подоконником рассматриваемого окна $H_{\text{зд.}}$

Поскольку затеняющих зданий поблизости нет, то $k_{\text{ЗД}}$ =1.

Таблица 5.2 - Изображение таблицы с коэффициентом, учитывающим затенение окон противостоящими зданиями

$P/H_{зд}$	$K_{зд}$
0,5	1,7
1	1,4
1,5	1,2
2	1,1
3 и более	1

Вычисляется общая площадь окон:

$$S_0 = \frac{60*1,0125*9,5*1*1,5}{100*0,48*1,03} = 17,5 \text{ м}^2$$

Схема расположения окон представлена на рисунке 1.

Так как в кабинете общая площадь окна составляет 5х4=20 м^2, следовательно, они соответствуют нормативам естественного освещения рабочего помещения.

5.2.2. Расчет количества рабочих мест, оснащенных ПК

Площадь на одно рабочее место пользователей ПК и ВТ на базе ЭЛТ составляет не менее 6 квадратных метров [16]. Расчет максимального количества рабочих мест проводим по формуле, [16]: используется формула 5.2.

$$n = \frac{S}{6} \quad (5.2)$$

где n – максимальное количество рабочих мест,

S - площадь помещения (рассчитано по формуле 5.3.).

Расчет:

$$n = \frac{60}{6} = 10 \text{ рабочих мест.}$$

В данном помещении можно разместить до 10 рабочих мест.

Рабочий стол имеет параметры 160х90 см.

При размещении рабочих мест с ПЭВМ расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора) должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов - не менее 1,2 м [16].

Схема помещения определена в соответствии с рисунком 5.3.

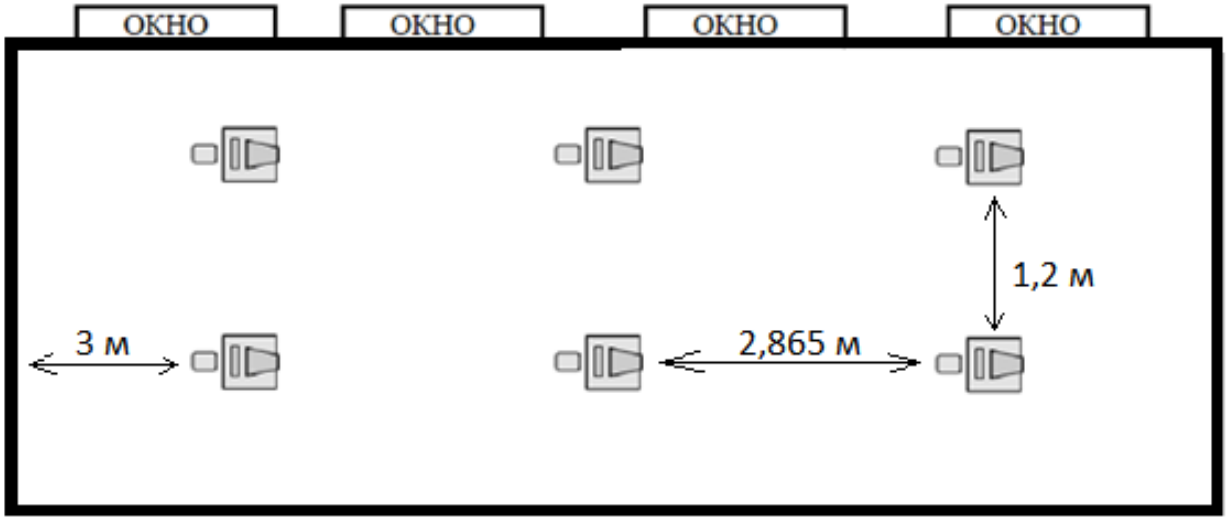

Рисунок 5.3 - Схема размещения окон и рабочих мест

Заключение

В рамках данной дипломного проекта был реализован модуль, обеспечивающий безопасность информационного портала для компании согласно техническому заданию. Были выработаны ряд требований и подходов к реализации программного продукта, что привело к обеспечению защищенности информационного портала для компании. Были успешно реализованы все поставленные задачи, включающие в себя: защита входа для авторизированных пользователей, по разрешенному IP-адресу, четыре разных способа аутентификации (логин и пароль, OTP, временная ссылка и распознавание лица), защитные алгоритмы шифрования передаваемых данных, а также защита соединения посредством сертификата SSL, а также DNSSEC.

Существует огромное количество условий, которые способствуют неправомерному овладению конфиденциальной информацией. Данное обстоятельство вызывает необходимость использования не менее многообразных способов, сил и средств для обеспечения информационной безопасности.

Разработка способов обеспечения информационной безопасности должна быть ориентирована на упреждающий характер действий, которые направлены на заблаговременные меры предупреждения возможных угроз, поскольку при любой атаке, повторная становится для атакующего уже проще, особенно, если при первичной атаке был внесен “жучок”, отслеживающий все действия, пароли и другую информацию.

Обеспечение информационной безопасности достигается организационными, организационно-техническими и техническими мероприятиями. Каждое мероприятие обеспечивается специфическими силами, средствами и мерами, обладающими соответствующими характеристиками, при этом лучшая безопасность достигнется в том случае, когда все мероприятия обеспечиваются в полной мере.

Развитие систем обеспечения информационной безопасности должно происходить еще быстрее, чем развитие ИТ. Поскольку на каждую новую технологию существует, как минимум, несколько способов ее взлома и внесения неисправностей. Вирусы, черви и прочие вредоносные ПО, а также хакерские атаки совершенствуются каждый день, поэтому развитие и разработка технологий защиты определенно необходимо производить в том же темпе и даже быстрее и качественнее.

В результате разработки и анализа полученного результата, необходимо отметить, что поставленная цель была достигнута, большая часть угроз была устранена, экономическая эффективность проекта была доказана показателем возврата инвестиций (который больше порогового в 3 раза), что говорит о высокой результативности проекта.

Список литературы

1 Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 с.

2 Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.

3 Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: Инфра-М, 2018. - 64 с.

4 Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - М.: Форум, 2018. - 118 с.

5 Ковалев, А.А. Военная безопасность России и ее информационная политика в эпоху цивилизационных конфликтов: Монография / А.А. Ковалев, В.А. Шамахов. - М.: Риор, 2018. - 32 с.

6 Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2018. - 88 с.

7 Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2017. - 702 с.

8 Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: Форум, 2018. - 256 с.

9 Холостова, Е.И. Безопасность жизнедеятельности: Учебник для бакалавров / Е.И. Холостова, О.Г. Прохорова. - М.: ИТК Дашков и К, 2018. - 456 с.

10 Вишняков, Я.Д. Безопасность жизнедеятельности 4-е изд., пер. и доп. учебник для спо / Я.Д. Вишняков. - Люберцы: Юрайт, 2017. - 543 с.

11 Беляков, Г.И. Безопасность жизнедеятельности. охрана труда: учебник для бакалавров. 2-е изд., пер. и доп. / Г.И. Беляков. - Люберцы: Юрайт, 2018. - 572 с.

12 Безопасность жизнедеятельности: Конспект лекций: Пособие для подготовки к экзаменам. Басаков М.И., авт.-сост., 2017. – 135 с.

13 Основы безопасности жизнедеятельности. Алексеенко В.А., Матасова И.Ю., 2001. – 187 с "Безопасность в чрезвычайных ситуациях: Учебник" под ред. Н.К. Шишкина. – М., ГУУ, 2017. - 90 с.

14 Косолапова, Н.В. Безопасность жизнедеятельности: Учебник / Н.В. Косолапова. - М.: Academia, 2019. - 176 с.

15 Санитарные правила «Санитарно-эпидемиологические требования к условиям работы с источниками физических факторов (компьютеры и видеотерминалы), оказывающих воздействие на человека» (утверждены приказом Министра национальной экономики Республики Казахстан от 21 января 2015 года № 38).

16 Расчет и проектирование естественного освещения помещений: учебно-методические указания к курсовой расчетнографической работе / И.В.Мигалина, Н.И.Щепетков. - М.: МАРХИ, 2017. - 68 с.

Приложение А

Интеграция с СМС провайдером

```
<?php
// SMSC.RU API (smsc.ru) версия 3.8 (03.07.2019)
define("SMSC_LOGIN", "login");                  // логин клиента
define("SMSC_PASSWORD", "password");// пароль
define("SMSC_POST", 0);                         // использовать метод POST
define("SMSC_HTTPS", 0);                        // использовать HTTPS протокол
define("SMSC_CHARSET", "windows-1251");    // кодировка сообщения: utf-8, koi8-r или windows-1251 (по умолчанию)
define("SMSC_DEBUG", 0);                        // флаг отладки
define("SMTP_FROM", "api@smsc.ru");     // e-mail адрес отправителя
// Функция отправки SMS
```

```
//
// обязательные параметры:
//
// $phones - список телефонов через запятую или точку с запятой
// $message - отправляемое сообщение
//
// необязательные параметры:
//
// $translit - переводить или нет в транслит (1,2 или 0)
// $time - необходимое время доставки в виде строки (DDMMYYhhmm, h1-h2, 0ts, +m)
// $id - идентификатор сообщения. Представляет собой 32-битное число в диапазоне от 1 до 2147483647.
// $format - формат сообщения (0 - обычное sms, 1 - flash-sms, 2 - wap-push, 3 - hlr, 4 - bin, 5 - bin-hex, 6 - ping-sms, 7 - mms, 8 - mail, 9 - call, 10 - viber, 11 - soc)
// $sender - имя отправителя (Sender ID).
// $query - строка дополнительных параметров, добавляемая в URL-запрос ("valid=01:00&maxsms=3&tz=2")
// $files - массив путей к файлам для отправки mms или e-mail сообщений
//
// возвращает массив (<id>, <количество sms>, <стоимость>, <баланс>) в случае успешной отправки
// либо массив (<id>, -<код ошибки>) в случае ошибки

function send_sms($phones, $message, $translit = 0, $time = 0, $id = 0, $format = 0, $sender = false, $query = "", $files = array())
{
static $formats = array(1 => "flash=1", "push=1", "hlr=1", "bin=1", "bin=2", "ping=1", "mms=1", "mail=1", "call=1", "viber=1", "soc=1");

$m = _smsc_send_cmd("send", "cost=3&phones=".urlencode($phones)."&mes=".urlencode($message).
"&translit=$translit&id=$id".($format > 0 ? "&".$formats[$format] : "").
($sender === false ? "" : "&sender=".urlencode($sender)).
($time ? "&time=".urlencode($time) : "").($query ? "&$query" : ""), $files);
```

Продолжение приложения А

```
// (id, cnt, cost, balance) или (id, -error)

if (SMSC_DEBUG) {
	if ($m[1] > 0)
		echo "Сообщение отправлено успешно. ID: $m[0], всего SMS: $m[1], стоимость: $m[2], баланс: $m[3].\n";
	else
		echo "Ошибка №", -$m[1], $m[0] ? ", ID: ".$m[0] : "", "\n";
}

return $m;
}

// SMTP версия функции отправки SMS

function send_sms_mail($phones, $message, $translit = 0, $time = 0, $id = 0, $format = 0, $sender = "")
{
return mail("send@send.smsc.ru", "", SMSC_LOGIN.":".SMSC_PASSWORD.":$id:$time:$translit,$format,$sender:$phones:$message", "From: ".SMTP_FROM."\nContent-Type: text/plain; charset=".SMSC_CHARSET."\n");
}

// Функция получения стоимости SMS
//
// обязательные параметры:
//
// $phones - список телефонов через запятую или точку с запятой
// $message - отправляемое сообщение
//
// необязательные параметры:
//
// $translit - переводить или нет в транслит (1,2 или 0)
// $format - формат сообщения (0 - обычное sms, 1 - flash-sms, 2 - wap-push, 3 - hlr, 4 - bin, 5 - bin-hex, 6 - ping-sms, 7 - mms, 8 - mail, 9 - call, 10 - viber, 11 - soc)
// $sender - имя отправителя (Sender ID)
// $query - строка дополнительных параметров, добавляемая в URL-запрос ("list=79999999999:Ваш пароль: 123\n78888888888:Ваш пароль: 456")
//
```

```
// возвращает массив (<стоимость>, <количество sms>) либо массив (0, -<код ошибки>) в случае ошибки
function get_sms_cost($phones, $message, $translit = 0, $format = 0, $sender = false, $query = "")
{
static $formats = array(1 => "flash=1", "push=1", "hlr=1", "bin=1", "bin=2", "ping=1", "mms=1", "mail=1", "call=1", "viber=1", "soc=1");

$m = _smsc_send_cmd("send", "cost=1&phones=".urlencode($phones)."&mes=".urlencode($message).
($sender === false ? "" : "&sender=".urlencode($sender)).
```

Продолжение приложения А

```
"&translit=$translit".($format > 0 ? "&".$formats[$format] : "").($query ? "&$query" : ""));

// (cost, cnt) или (0, -error)

if (SMSC_DEBUG) {
        if ($m[1] > 0)
                echo "Стоимость рассылки: $m[0]. Всего SMS: $m[1]\n";
        else
                echo "Ошибка №", -$m[1], "\n";
}

return $m;
}

// Функция проверки статуса отправленного SMS или HLR-запроса
//
// $id - ID сообщения или список ID через запятую
// $phone - номер телефона или список номеров через запятую
// $all - вернуть все данные отправленного SMS, включая текст сообщения (0,1 или 2)
//
// возвращает массив (для множественного запроса двумерный массив):
//
// для одиночного SMS-сообщения:
// (<статус>, <время изменения>, <код ошибки доставки>)
//
```

```
// для HLR-запроса:
// (<статус>, <время изменения>, <код ошибки sms>, <код IMSI SIM-карты>, <номер сервис-центра>, <код страны регистрации>, <код оператора>,
// <название страны регистрации>, <название оператора>, <название роуминговой страны>, <название роумингового оператора>)
//
// при $all = 1 дополнительно возвращаются элементы в конце массива:
// (<время отправки>, <номер телефона>, <стоимость>, <sender id>, <название статуса>, <текст сообщения>)
//
// при $all = 2 дополнительно возвращаются элементы <страна>, <оператор> и <регион>
//
// при множественном запросе:
// если $all = 0, то для каждого сообщения или HLR-запроса дополнительно возвращается <ID сообщения> и <номер телефона>
//
// если $all = 1 или $all = 2, то в ответ добавляется <ID сообщения>
//
// либо массив (0, -<код ошибки>) в случае ошибки

function get_status($id, $phone, $all = 0)
{
$m = _smsc_send_cmd("status", "phone=".urlencode($phone)."&id=".urlencode($id)."&all=".(int)$all);
```

Продолжение приложения А

```
// (status, time, err, ...) или (0, -error)

if (!strpos($id, ",")) {
	if (SMSC_DEBUG )
		if ($m[1] != "" && $m[1] >= 0)
			echo "Статус SMS = $m[0]", $m[1] ? ", время изменения статуса - ".date("d.m.Y H:i:s", $m[1]) : "", "\n";
		else
			echo "Ошибка №", -$m[1], "\n";

	if ($all && count($m) > 9 && (!isset($m[$idx = $all == 1 ? 14 : 17]) || $m[$idx] != "HLR")) // ',' в сообщении
		$m = explode(",", implode(",", $m), $all == 1 ? 9 : 12);
```

```
}
else {
	if (count($m) == 1 && strpos($m[0], "-") == 2)
		return explode(",", $m[0]);

	foreach ($m as $k => $v)
		$m[$k] = explode(",", $v);
}

return $m;
}

// Функция получения баланса
//
// без параметров
//
// возвращает баланс в виде строки или false в случае ошибки

function get_balance()
{
$m = _smsc_send_cmd("balance"); // (balance) или (0, -error)

if (SMSC_DEBUG) {
	if (!isset($m[1]))
		echo "Сумма на счете: ", $m[0], "\n";
	else
		echo "Ошибка №", -$m[1], "\n";
}

return isset($m[1]) ? false : $m[0];
}

// ВНУТРЕННИЕ ФУНКЦИИ

// Функция вызова запроса. Формирует URL и делает 5 попыток чтения через разные подключения к сервису
```

Продолжение приложения А

```
function _smsc_send_cmd($cmd, $arg = "", $files = array())
{
```

```
$url = $_url = (SMSC_HTTPS ? "https" : "http").":://smsc.ru/sys/$cmd.php?login=".urlencode(SMSC_LOGIN)."&psw=".urlencode(SMSC_PASSWORD)."&fmt=1&charset=".SMSC_CHARSET."&".$arg;

$i = 0;
do {
	if ($i++)
		$url = str_replace('://smsc.ru/', '://www'.$i.'.smsc.ru/', $_url);

	$ret = _smsc_read_url($url, $files, 3 + $i);
}
while ($ret == "" && $i < 5);

if ($ret == "") {
	if (SMSC_DEBUG)
		echo "Ошибка чтения адреса: $url\n";

	$ret = ","; // фиктивный ответ
}

$delim = ",";

if ($cmd == "status") {
	parse_str($arg, $m);

	if (strpos($m["id"], ","))
		$delim = "\n";
}

return explode($delim, $ret);
}

// Функция чтения URL. Для работы должно быть доступно:
// curl или fsockopen (только http) или включена опция allow_url_fopen для file_get_contents

function _smsc_read_url($url, $files, $tm = 5)
{
$ret = "";
$post = SMSC_POST || strlen($url) > 2000 || $files;
```

```
if (function_exists("curl_init"))
{
	static $c = 0; // keepalive
	if (!$c) {
		$c = curl_init();
		curl_setopt_array($c, array(
				CURLOPT_RETURNTRANSFER => true,
```

Продолжение приложения А

```
				CURLOPT_CONNECTTIMEOUT => $tm,
				CURLOPT_TIMEOUT => 60,
				CURLOPT_SSL_VERIFYPEER => 0,
				CURLOPT_HTTPHEADER => array("Expect:")
				));
	}

	curl_setopt($c, CURLOPT_POST, $post);

	if ($post)
	{
		list($url, $post) = explode("?", $url, 2);

		if ($files) {
			parse_str($post, $m);

			foreach ($m as $k => $v)
				$m[$k] = isset($v[0]) && $v[0] == "@" ? sprintf("\0%s", $v) : $v;

			$post = $m;
			foreach ($files as $i => $path)
				if (file_exists($path))
					$post["file".$i] = function_exists("curl_file_create") ? curl_file_create($path) : "@".$path;
		}

		curl_setopt($c, CURLOPT_POSTFIELDS, $post);
	}
	curl_setopt($c, CURLOPT_URL, $url);
	$ret = curl_exec($c);
```

```
}
elseif ($files) {
	if (SMSC_DEBUG)
		echo "Не установлен модуль curl для передачи файлов\n";
}
else {
	if (!SMSC_HTTPS && function_exists("fsockopen"))
	{
		$m = parse_url($url);

		if (!$fp = fsockopen($m["host"], 80, $errno, $errstr, $tm))
			$fp = fsockopen("212.24.33.196", 80, $errno, $errstr, $tm);

		if ($fp) {
			stream_set_timeout($fp, 60);
			fwrite($fp, ($post ? "POST $m[path]" : "GET $m[path]?$m[query]")." HTTP/1.1\r\nHost: smsc.ru\r\nUser-Agent: PHP".($post ? "\r\nContent-Type: application/x-www-form-urlencoded\r\nContent-Length: ".strlen($m['query']) : "")."\r\nConnection: Close\r\n\r\n".($post ? $m['query'] : ""));
```

Продолжение приложения А

```
while (!feof($fp))
				$ret .= fgets($fp, 1024);
			list(, $ret) = explode("\r\n\r\n", $ret, 2);

			fclose($fp);
		}
	}
	else
		$ret = file_get_contents($url);
}

return $ret;
}

// Examples:
// include "smsc_api.php";
// list($sms_id, $sms_cnt, $cost, $balance) = send_sms("79999999999", "Ваш пароль: 123", 1);
```

```
// list($sms_id, $sms_cnt, $cost, $balance) = send_sms("79999999999", "http://smsc.ru\nSMSC.RU", 0, 0, 0, 0, false, "maxsms=3");
// list($sms_id, $sms_cnt, $cost, $balance) = send_sms("79999999999", "0605040B8423F0DC0601AE02056A0045C60C036D79736974652E72750001036D7973697465000101", 0, 0, 0, 5, false);
// list($sms_id, $sms_cnt, $cost, $balance) = send_sms("79999999999", "", 0, 0, 0, 3, false);
// list($sms_id, $sms_cnt, $cost, $balance) = send_sms("dest@mysite.com", "Ваш пароль: 123", 0, 0, 0, 8, "source@mysite.com", "subj=Confirmation");
// list($cost, $sms_cnt) = get_sms_cost("79999999999", "Вы успешно зарегистрированы!");
// send_sms_mail("79999999999", "Ваш пароль: 123", 0, "0101121000");
// list($status, $time) = get_status($sms_id, "79999999999");
// $balance = get_balance();

?>
```

ПРИЛОЖЕНИЕ В – Акт внедрения

Утверждаю
Директор ИП «Саржигтиов Х.А»
Саржигтиов Х.А.
«20» мая 2020г.

АКТ

внедрения программы «*Разработка информационного портала для компании. Проектирование интерфейса*»

Разработанная студентом 4-курса НАО «АУЭС им. Г. Даукеева» группы ВТ-16-2 Сан С.Э. программа «*Разработка информационного портала для компании. Разработка системы обеспечения информационной безопасности*» была передана в эксплуатацию в ИП «Саржигитов Х.А.» в мае 2020 года для использования в качестве программного комплекса.

Назначение программы:

- обеспечение безопасности данных компании;
- предотвращение возможных утечек информации;
- устранение рисков безопасности данных.

Директор ИП «Саржигитов Х.А.» _____ Саржигитов Х.А.

Исполнитель _____ Сан С.Э.