ГУАП

КАФЕДРА № 43

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

Старший преподаватель		Т.И. Белая
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №2
Разработка и документирование требований к ПО

по дисциплине: Проектирование программных систем

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР.	4134к		Столяров Н.С.
		подпись, дата	инициалы, фамилия

Санкт-Петербург

2023

Оглавление

1. Введение

1.1 Назначение

Цель данного документа - определить требования к созданию и внедрению системы мониторинга для контроля безопасности информации в организации "Защищённые проходы ООО." Эта система разрабатывается для обеспечения безопасности контроля доступа в здание организации.

1.2 Соглашения, принятые в документах

Документация оформляется согласно установленным соглашениям и стандартам:

- Шрифт и размер шрифта: Вся текстовая часть документации должна быть оформлена шрифтом Times New Roman размером 14 пунктов. Заголовки разделов и подразделов выделяются жирным шрифтом.
- Стиль заголовка: Заголовки форматируются с использованием шрифта Times New Roman размером 14 пунктов, жирным шрифтом и автоматической нумерацией.
- Маркировка требований: Требования пронумерованы в формате "Глава.Название," где "Глава" - номер главы, а "Название" - краткое описание требования.
- Выделение текста: Важные термины и ключевые понятия выделяются жирным шрифтом.
- Цветовая маркировка: Для выделения информации можно использовать цветовую маркировку. Красный цвет используется для предупреждений, а желтый - для подсказок и советов.

1.3 Границы проекта

Продукт и его назначение

Создаваемая система контроля доступа в здание организации " Защищённые проходы ООО" включает следующие ключевые компоненты:

- Электронные Пропускные Устройства: Обеспечение безопасного и эффективного контроля доступа в здание через электронные ключи или карточки сотрудников и посетителей.
- Система Видеонаблюдения: Обеспечение визуального мониторинга безопасности помещений, регистрация событий и обеспечение реагирования на потенциальные угрозы.
- Система Автоматической Фиксации Посещений: Автоматизация учета посещений для эффективного мониторинга присутствия сотрудников и посетителей в организации.

2. Общее описание

2.1 Общий взгляд на продукт

Создаваемый продукт будет направлен на обеспечение безопасности имущества организации. Внедрение этой системы позволит организации:

- Обеспечить Высокий Уровень Безопасности.
- Улучшить Эффективность Управления Посещениями.
- Повысить Прозрачность и Ответственность.

2.2 Связь продукта с пользователями

Система контроля доступа в здание организации будет ориентирована на следующие категории пользователей:

- Сотрудники

Получат удобный и безопасный доступ в здание через электронные пропускные устройства, что повысит уровень комфорта и безопасности в рабочем пространстве.

- Администраторы:

Смогут эффективно управлять правами доступа, мониторить события через систему видеонаблюдения и осуществлять автоматический учет посещений, улучшая общую безопасность и управление офисом.

- IT-специалисты:

Будут вовлечены в интеграцию системы с существующей инфраструктурой и обеспечение ее безопасности, что позволит поддерживать эффективность работы системы.

2.3 Связь с корпоративными целями и стратегией

Создание и внедрение системы контроля доступа в здание организации непосредственно поддерживает корпоративные цели и стратегию организации " Защищённые проходы ООО". Основными целями внедрения являются:

- Безопасность Корпоративных Активов
- Соблюдение Нормативов и Правил
- Улучшение контроля и отчетности.

Система контроля доступа в здание организации позволит организации соблюдать современные стандарты в области безопасности, учета посещений и эффективного управления доступом, способствуя высокому уровню соответствия нормативам и требованиям.

2.4 Предположения и зависимости

Предполагается, что директор компании сможет просматривать всю статистику о сотрудниках, а сами сотрудники просмотреть свою статистику не могут.

3. Функции модулей

3.1 Описание

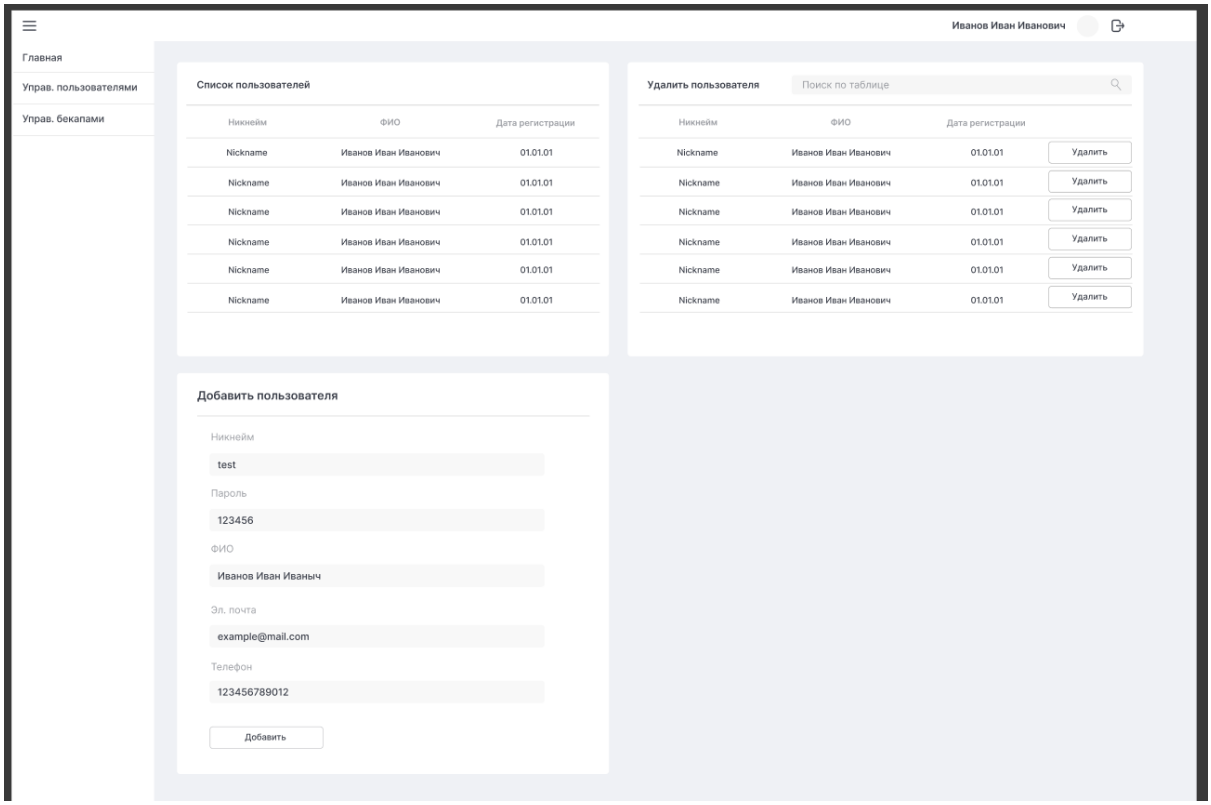
Для описания функций системы контроля доступа в здание организации, включая систему автоматической фиксации посещений и видеонаблюдение "Не защищённые проходы ООО," применим структуру:

3.1.1 Регистрация сотрудников
Особенность: Регистрация новых сотрудников в системе.
- 3.1.1.1 Ввод информации
- 3.1.1.2 Валидация данных
- 3.1.1.3 Сохранение в базе данных

Для регистрации новых сотрудников изначально директор входит в свою систему:
Далее он открывает окно регистрации нового сотрудника:

Чтобы зарегистрировать нового сотрудника нужно добавить все его данные, и нажать на кнопку «Добавить»:

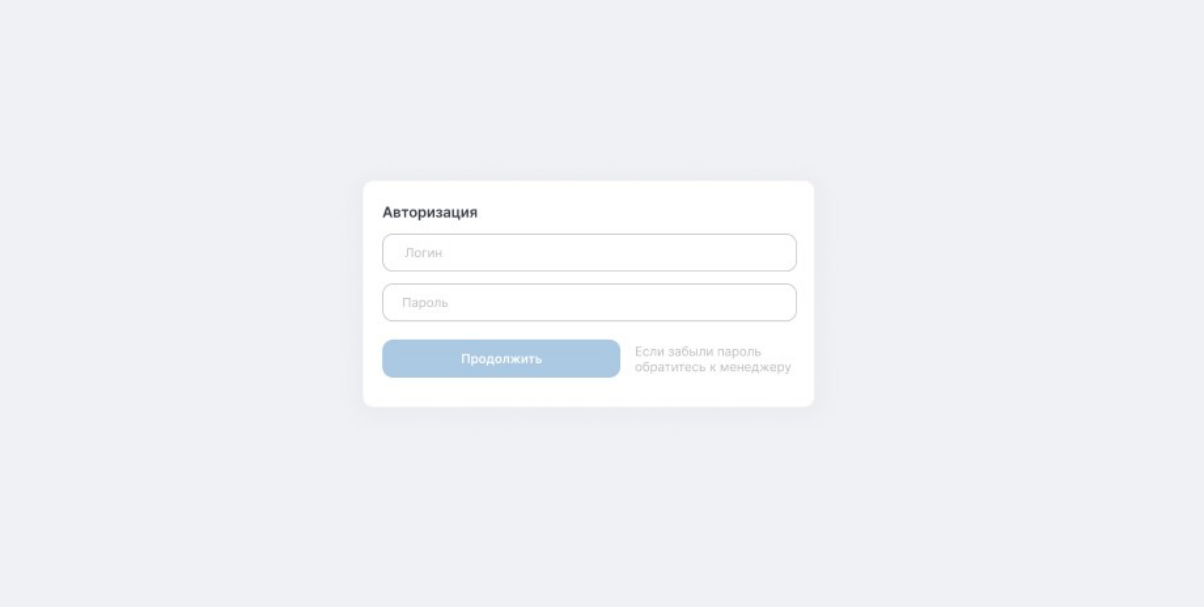
После этого, новый пользователь получить письмо на почту с логином и паролем.
3.1.2 Удаление сотрудника
Особенность: Удаление сотрудника ранее зарегистрированного в системе.
-3.1.2.1 Ввод никнейма сотрудника
-3.1.2.1 Удаление пользователя из бд



Описание:
В пункте “Добавить пользователя” нужно заполнить обязательные поля(Никнейм(уникальное), пароль, ФИО, почта) и по желанию дополнительные поля, а после кликнуть кнопку “Добавить” и пользователь будет добавлен бд.

В пункте “Удалить пользователя” нужно заполнить поле “Никнейм”, а после кликнуть кнопку “Удалить”, затем пользователь будет удален из бд.

3.1.3 Отметка начала сессии
Особенность: Фиксация начала сессии после авторизации пользователя
Подразделы:
- 3.1.3.1 Авторизация сотрудника по логину и паролю
- 3.1.3.2 Запись действий сотрудника



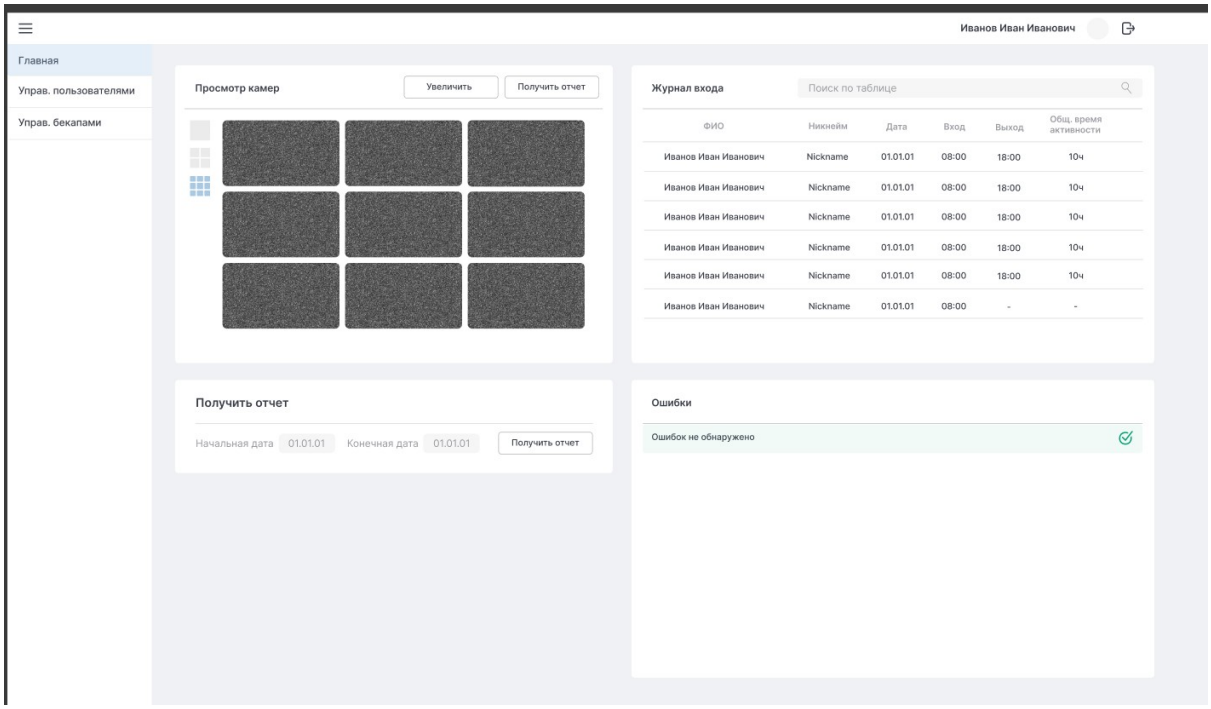
Описание:

При вводе логина и пароля пользователь входит в систему и приложение сворачивается в панель. Если система распознает, что входит пользователь с ролью директора, то перекидывает в окно браузера.

3.1.4 Генерация отчета
Особенность: Автоматическая генерация отчета с информацией о действиях сотрудников и истории системы.
Подразделы:
- 3.1.4.1 Выбор периода отчета
- 3.1.4.2 Формирование отчета
- 3.1.4.3 Экспорт отчета в формате xml
Руководителю нужно зайти в свою систему:
Далее перейти в раздел «Главная»:
Выбрать период и нажать кнопку «Получить отчёт»:

Описание:
Если нужно получить отчет от сервера за определенный период, то сначала выбираются начальная и конечная даты и нажимается кнопка “Получить отчёт”.

В фильтре журнала активности можно выбрать пункт по которому нужно отфильтровать журнал(Бекапы, Активность пользователей, Все, Система или по конкретному пользователю(В этом случае открывается alert где отображаются никнеймы сотрудников и их фио, выбирается сотрудник)) за последний месяц.



Пример отчета:

Отчет за период с 01.10.2023 до 25.10.2023

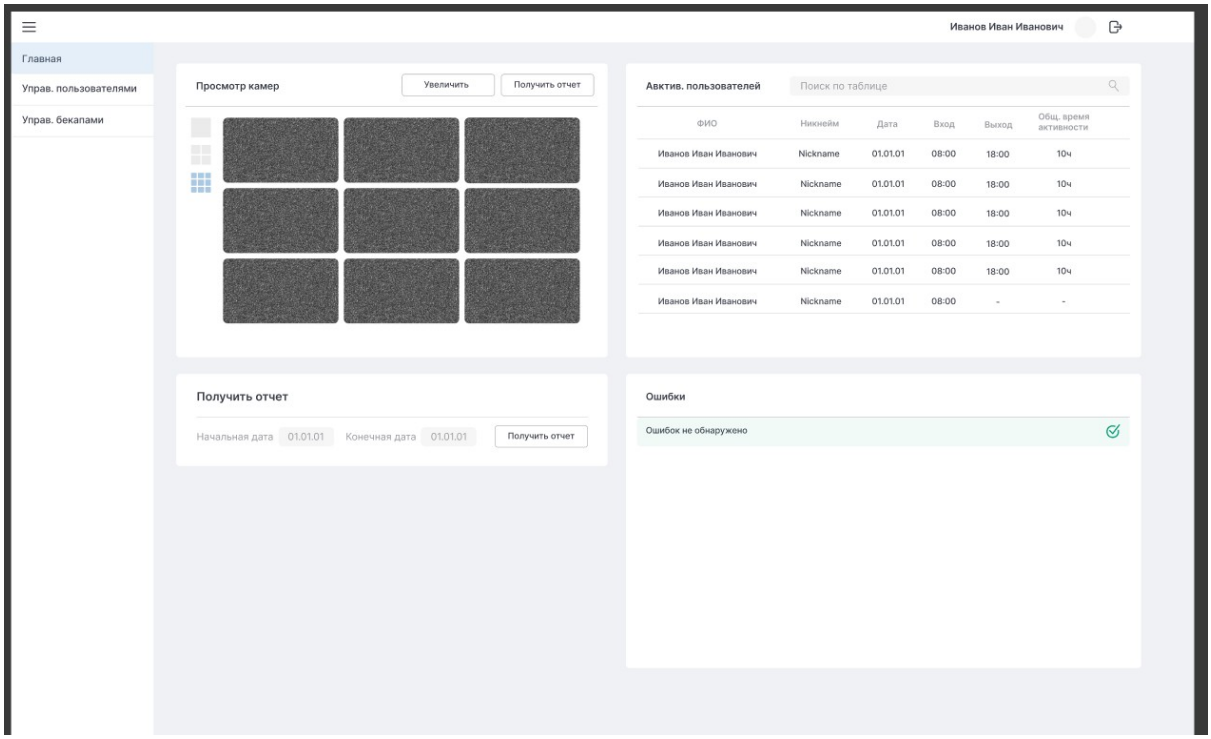
Дата: 25 октября 2023

Подготовлено: ООО " Защищённые проходы "

В данном отчете представлена информация о контроле доступа в здание организации ООО " Защищённые проходы ". Отчет включает в себя результаты аудита доступа к системам, мониторинг вставки внешних устройств, журналы авторизации и выхода, выявление внешних угроз и систему резервного копирования данных.

Журнал входа и выхода

- 21.10.2023 10:00 – Иван Иванов вошёл в здание через пункт под номером 2.
- 21.10.2023 17:45 – Никита Никитин вышел из здания через пункт под номером 6
- 21.10.2023 17:45 – Никита Никитин вошёл из здания через пункт под номером 6
- 21.10.2023 17:45 – Никита Никитин вышел из здания через пункт под номером 3
- 21.10.2023 17:45 – Никита Никитин вошёл из здания через пункт под номером 4
- 21.10.2023 17:45 – Никита Никитин вышел из здания через пункт под номером 2



3.2 Функциональные требования

3.2.1 Аудит доступа к системам

3.2.1.1 Отслеживание событий (!)

Система мониторинга регистрирует и анализирует события, связанные с доступом к объектам. Эти события включают в себя попытки входа в систему, изменения прав доступа, попытки несанкционированного доступа и другие.

Мониторинг представлен в пользовательском интерфейсе директора на странице «Главная» в разделе «Журнал событий».

Пример работы отслеживания событий через RFID метки:

- Пользователь подносит свой RFID-пропуск к считывателю на входе в здание.
- Считыватель передает идентификатор пропуска и код объекта безопасности в программное обеспечение системы контроля доступа.
- Программное обеспечение проверяет, имеет ли пользователь право доступа к данному объекту безопасности в текущее время и дату.
- Если право доступа есть, то программное обеспечение отправляет команду на открытие двери и регистрирует событие входа в базе данных. Также программа активирует видеокамеру, которая записывает видео с входа в здание.
- Если право доступа отсутствует или пропуск недействителен, то программное обеспечение отказывает в доступе и регистрирует событие нарушения в базе данных. Также программа активирует видеокамеру, которая записывает видео с входа в здание, и отправляет уведомление о нарушении администратору системы или охране.
- Пользователь входит или не входит в здание в зависимости от результата проверки прав доступа.
- При выходе из здания пользователь повторяет те же действия, но с другим кодом объекта безопасности. Программное обеспечение регистрирует событие выхода в базе данных и активирует видеокамеру на выходе из здания.
- Программное обеспечение анализирует данные о событиях входа и выхода и формирует отчеты по рабочему времени и посещаемости пользователей.

- Администратор системы или охрана могут просматривать данные о событиях, видеозаписи, отчеты и статистику в интерфейсе программного обеспечения и реагировать на уведомления и алерты.

Пример работы фиксации посещений через машинное зрение:

- Посетитель подходит к входу в здание и смотрит в видеокамеру.
- Видеокамера передает изображение лица посетителя в программное обеспечение системы фиксации посещений.
- Программное обеспечение обрабатывает изображение, определяет положение, размер и угол поворота лица, выделяет его из фона и преобразует его в вектор признаков.
- Программное обеспечение сравнивает вектор признаков лица посетителя с векторами признаков лиц, хранящихся в базе данных, и находит наиболее близкое совпадение или несколько совпадений.
- Если совпадение найдено, то программное обеспечение проверяет, имеет ли лицо право доступа к объекту безопасности в текущее время и дату, а также классифицирует его по различным признакам (например, пол, возраст, настроение и т.д.).
- Если право доступа есть, то программное обеспечение отправляет команду на открытие двери и регистрирует событие входа в базе данных. Также программа может произнести приветствие или сообщение для посетителя, используя синтез речи.
- Если право доступа отсутствует или лицо не распознано, то программное обеспечение отказывает в доступе и регистрирует событие нарушения в базе данных. Также программа может произнести предупреждение или требование для посетителя,

используя синтез речи, и отправить уведомление о нарушении администратору системы или охране.

- Посетитель входит или не входит в здание в зависимости от результата распознавания и проверки прав доступа.
- При выходе из здания посетитель повторяет те же действия, но с другой видеокамерой. Программное обеспечение регистрирует событие выхода в базе данных и может произнести прощание или сообщение для посетителя, используя синтез речи.

3.2.1.2 Анализ угроз

На основе зарегистрированных событий система проводит анализ для выявления потенциальных угроз безопасности. Это может включать в себя обнаружение несанкционированных попыток пройти через проходной пункт.

Анализ угроз представлен в пользовательском интерфейсе директора на странице «Главная» в разделе «Ошибки»

Система контроля и управления доступом должна действовать во время пожара таким образом, чтобы обеспечить безопасную и быструю эвакуацию людей и предотвратить распространение огня. Для этого необходимо выполнить следующие действия:

- Синхронизировать СКУД(Система контроля и управления доступом) с системой пожарной сигнализации (СПС), чтобы получать информацию о состоянии пожарных извещателей и датчиков дыма.
- Настроить автоматическое разблокирование всех эвакуационных выходов и отключение электромагнитных замков при получении сигнала о пожаре от СПС.

- Настроить автоматическое закрытие противопожарных дверей и ворот при получении сигнала о пожаре от СПС, чтобы предотвратить проникновение огня и дыма в соседние помещения.
- Активировать видеонаблюдение на всех точках прохода и эвакуации, чтобы контролировать ситуацию и фиксировать доказательства нарушений.
- Отправлять уведомления и алерты о пожаре администратору системы, охране, пожарным и другим службам, ответственным за ликвидацию пожара.
- Предоставлять доступ к данным о событиях, видеозаписям, отчетам и статистике в интерфейсе программного обеспечения СКУД для анализа причин и последствий пожара.

3.2.1.3 Оповещение

В случае обнаружения потенциальных угроз система может генерировать уведомления и оповещения директора о необходимости принять меры.

Оповещение представлено в пользовательском интерфейсе директора на странице «Главная» в разделе «Ошибки» в статус-баре(Зеленый-с системой всё в порядке, красный-ошибки и угрозы)

3.1.2 Защита от внешних угроз

4. Требования к данным

4.1 Словарь данных

Для корректной работы системы контроля доступа в здание используются следующие типы данных:

- Идентификатор пользователя (User ID)
- Логин (Username)
- Пароль (Password)
- Идентификатор роли (Role ID)
- Название роли (Role Name)
- Почта (User email)
- Идентификатор события (Event ID)
- Тип события (Event Type)
- Время события (Event Timestamp)
- Описание события (Event Description)
- Тип отчета (Report Type)
- Данные отчета (Report Data)
- Идентификатор уведомления (Notification ID)

4.2 Отчеты

Система генерирует в одном отчете следующие составляющие:

- Журнал посещений

4.3 Утилизация данных

Для управления данными и их утилизации используется система архивирования и контроля доступа к данным. Утилизация данных проводится по решению директора.

5. Атрибуты качества

6.1 Удобство использования

- Изучения: Интерфейс системы должен быть эргономичным и простым для изучения новыми пользователями. Рекомендуется использовать стандартные элементы управления и логическое размещение функционала и генерации отчетов. Интерфейс должен быть минималистичным.
- Предотвращение ошибок и восстановление: Система должна предоставлять механизмы для предотвращения ошибок, включая проверку данных, предупреждения о возможных проблемах и подсказки для правильного использования функций. Возможность восстановления данных в случае сбоев или непредвиденных ситуаций должна быть предусмотрена.
- Эффективность взаимодействия: Система должна обеспечивать пользователям быстрый и эффективный доступ ко всем необходимым функциям. Отклик на действия пользователя должен быть мгновенным.
- Специальные возможности: Система должна предоставлять специальные возможности для различных категорий пользователей, такие как руководители и сотрудники. Например, руководители должны иметь возможность управлять доступом сотрудников и просматривать общий отчет, а сотрудники – авторизацию и выход из системы.

6.2 Производительность

Для обеспечения высокой производительности системы следует соблюдать следующие требования:

Время отклика: Продукт должен обеспечивать мгновенный отклик на действия пользователя. Время между запросом пользователя и получением результата не должно превышать 1 секунду.

Загрузка данных: Продукт должен быстро загружать большие объемы данных, такие как отчеты. Время загрузки не должно превышать 5 секунд для типичных наборов данных.

Обработка данных: Продукт должен эффективно обрабатывать данные, особенно при выполнении сложных аналитических операций. Время обработки данных не должно превышать 10 секунд для типичных запросов.

Ресурсы: Продукт не должен значительно нагружать ресурсы компьютера пользователя, такие как процессор и память. Ресурсы должны использоваться эффективно.

Поддержка платформ: Продукт должен эффективно работать на разных операционных системах и аппаратных платформах.

6.3 Безопасность

Безопасность данных и доступа имеет высший приоритет. Следующие аспекты безопасности должны быть обеспечены:

- Авторизация: Доступ к конфиденциальным данным и функциям должен строго ограничиваться на основе ролей и прав пользователей. Только авторизованные пользователи должны иметь доступ к чувствительным данным.
- Шифрование: Все передаваемые данные, особенно конфиденциальная информация, должны быть зашифрованы с использованием надежных протоколов шифрования.
- Система оповещения в экстренных ситуациях: Должна быть предусмотрена система, которая в случае возникновения критических проблем оповещало руководство письмом на электронную почту.

6. Требования по интернационализации и локализации

- Локализация: Продукт должен поддерживать русский интерфейс. Должна быть предусмотрена возможность добавления и локализации новых языков.
- Формат дат и времени: Продукт должен поддерживать формат времени (ЧЧ.ММ.СС) и дат (ДД.ММ.ГГГГ) в зависимости от локации пользователя.