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 №1** |
| **«Описание основных проектов объекта исследования»** |
| **по дисциплине: Проектирование программных систем** |
|  |

РАБОТУ ВЫПОЛНИЛ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| СТУДЕНТ ГР. № | 4134к |  |  |  | Столяров Н.С. |
|  |  |  | подпись, дата |  | инициалы, фамилия |

Санкт-Петербург 2023

Разработать систему контроля доступа в здание организации, включающую в себя электронные пропускные устройства, видеонаблюдение и систему автоматической фиксации посещений.

# ОБЩАЯ ИНФОРМАЦИЯ О ПРЕДПРИЯТИИ

Задание:  
Разработать систему контроля доступа в здание организации, включающую в себя электронные пропускные устройства, видеонаблюдение и систему автоматической фиксации посещений.

Организация "Защищённые проходы ООО" представляет систему контроля доступа в здание организации, видеонаблюдение и систему автоматической фиксации посещений для контроля безопасности информации для коммерческих организаций. Эта система разработана для обеспечения безопасности имущества компании. Также компания занимается сопровождением этой системы.

Юридический адрес компании: г. Санкт-Петербург, ул. Передовиков, д.6, пом. 423

Дата регистрации компании: 12.09.2023

Штатное расписание компании включает должности:

1) Администратор системы контроля доступа: отвечает за настройку и обслуживание системы мониторинга безопасности.

2) Аналитик безопасности: отвечает за анализ данных, выявление угроз и принятие мер по их предотвращению.

3) Специалист технической поддержки: предоставляет помощь пользователям и решает возникающие проблемы.

4) Директор компании: отвечает за организацию предприятия, поиск клиентов и подписание договоров с ними.

Полные данные о компании изложены в таблице:

|  |  |  |  |
| --- | --- | --- | --- |
| Компания | Вид деятельности | Система налогообложения | Штат |
| ООО «Защищённые проходы» | Эффективная защита имущества компании и обеспечение бесперебойной работы организации в охране. | УСН "Доходы минус Расходы" | 4 сотрудника |

# КЛЮЧЕВЫЕ ТРЕБОВАНИЯ И ГРАНИЦЫ ПРОЕКТА

Разработка системы контроля доступа включает электронные пропускные устройства, видеонаблюдение, систему фиксации посещений, интеграцию с базой данных, обеспечение безопасности данных, с ограничением на физическую инфраструктуру, регулирование доступа, обучение персонала, соблюдение бюджета и соответствие законодательству по конфиденциальности.

Автоматизация должна затронуть такие участки как:

- Управление электронными пропусками

- Синхронизация данных с видеонаблюдением

- Интеграция с системой фиксации посещений

- Обновление прав доступа

- Безопасность данных

- Обучение и поддержка

# ОСНОВНЫЕ ПОЛЬЗОВАТЕЛИ СИСТЕМЫ

1) Администраторы системы - Лица, ответственные за управление и конфигурацию системы контроля доступа, включая настройку электронных пропусков, видеонаблюдение и мониторинг посещений.

2) Безопасностные службы - Специалисты, занимающиеся мониторингом и обеспечением безопасности, использующие данные от видеонаблюдения и системы фиксации посещений.

3) Сотрудники организации - Пользователи системы, использующие электронные пропуска для доступа в здание и автоматической фиксации своих посещений.

4) Техническая поддержка - Специалисты, обеспечивающие техническую поддержку, решающие проблемы с оборудованием и программным обеспечением системы контроля доступа.

5) Аудиторы и аналитики - Лица, занимающиеся анализом данных системы для проведения аудитов и предоставления отчетов об эффективности контроля доступа

# ЦЕЛИ ВНЕДРЕНИЯ

Главная цель внедрения – Главная цель внедрения системы контроля доступа заключается в обеспечении безопасности и эффективного управления доступом внутри здания организации. Целями Внедрения автоматизированной системы являются:

* Эффективность и оптимизация процессов
* Снижение затрат
* Улучшение точности и надежности данных
* Улучшение качества услуг
* Ускорение принятия решений
* Соблюдение нормативов и стандартов
* Повышение уровня безопасности
* Интеграция с существующими системами
* Улучшение отчетности и аналитики

# ДОКУМЕНТООБОРОТ ВНУТРИ КОМПАНИИ

Документооборот осуществляется при помощи Excel - таблицы и графическом виде также используют частично ручной документооборот при написании отчёта об обслуживании для клиента.

В компании есть три типа документов: Отчёт об обслуживании за определённый период.

**5.1. Отчёт об обслуживании за определённый период**

Программа занимается формированием отчётности, исходя из данных, содержащихся в логах системы. Сформированные отчёты просматриваются директором для дальнейшего анализа и управления безопасностью. Отчеты помогают директору принимать информированные решения и следить за общим состоянием системы мониторинга безопасности в организации.

# ПРЕДПОСЫЛКИ ДЛЯ ВНЕДРЕНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

В организации существует ручная система учета посещений и контроля доступа, которая подвергается ряду проблем. Сотрудники или посетители часто предоставляют физические пропуска или подписывают бумажные журналы, что может привести к несанкционированному доступу и поддельным данным. Ручные процессы также подвержены человеческим ошибкам, таким как неверное заполнение данных, задержки в регистрации, что в свою очередь снижает точность и эффективность учета времени пребывания и общей безопасности. Основные предпосылки для внедрения автоматизированной системы являются:

* Увеличение общего объема посещений: Рост числа посетителей и сотрудников, что создает необходимость в эффективной системе управления и контроля доступа.
* Сложность ручного учета: Увеличение сложности и ошибок при ручном учете посещений, требующего более точного и автоматизированного подхода.
* Повышенные требования к безопасности: Растущая необходимость в обеспечении безопасности персонала и активов, особенно в условиях увеличивающихся угроз.
* Недостаточная эффективность текущих процессов: Обнаружение неэффективности и задержек в текущих системах контроля доступа, требующих модернизации для повышения эффективности.
* Потребность в точной системе учета времени: Растущая потребность в точном учете времени прихода и ухода сотрудников, а также посетителей.

# ИСПОЛЬЗУЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

На данный момент отчётность об итогах обслуживания ведётся в Excel и Word – файлах. Версия пакета Microsoft Office 2021 года.  
1. Аудит доступа к системам:

1. **Электронные пропускные устройства:**
   * *HID Global Mobile Access:* Приложение для мобильных устройств, позволяющее использовать смартфоны в качестве электронных пропусков.
   * *ZKTeco ProAccess Space:* Программное обеспечение для управления электронными пропусками, включая возможности выдачи, отслеживания и отзыва.
2. **Видеонаблюдение:**
   * *Milestone XProtect:* Видеоуправление с расширенными возможностями аналитики и интеграции с другими системами безопасности.
   * *Genetec Security Center:* Комплексное программное обеспечение для видеонаблюдения, управления доступом и аналитики.
3. **Система автоматической фиксации посещений:**
   * *ADP Workforce Now:* Интегрированная система учета рабочего времени и фиксации посещений.
   * *ZKTeco ZKTime.Net:* Программное обеспечение для автоматизации учета рабочего времени и фиксации посещений.

# ПРИНЯТАЯ УЧЁТНАЯ ПОЛИТИКА

Ключевые положения учетной политики, определяющей ведение отчетности об обслуживании клиентов и контроль качества обслуживания:

1. Аутентификация и Авторизация:
   * Описание: Все пользователи, включая сотрудников и посетителей, должны проходить процедуру аутентификации для получения доступа. Политика должна определять виды аутентификации, такие как электронные пропуска, биометрические данные или PIN-коды.
   * Авторизация: Определение уровней доступа в соответствии с ролями и обязанностями. Принцип минимальных привилегий должен быть строго соблюден.
2. Управление паролями и Электронными Пропусками:
   * Политика паролей: Установка требований к сложности паролей, их периодичности изменения и мер безопасности при хранении.
   * Электронные пропуска: Определение процедур выдачи, отзыва и обновления электронных пропусков.
3. Мониторинг и Аудит:
   * Системы Мониторинга: Обязательное включение систем мониторинга для реального времени и обнаружения аномальной активности.
   * Аудит Событий: Определение типов событий, которые должны подвергаться аудиту, с четкими правилами регистрации и хранения данных аудита.
4. Физическая Безопасность и Видеонаблюдение:
   * Контроль Доступа: Установление политики контроля доступа к помещениям с использованием электронных пропускных устройств.
   * Видеонаблюдение: Указание на периодичность мониторинга записей видеонаблюдения, обеспечение конфиденциальности данных и обязательное удаление устаревших записей.
5. Управление Устройствами и Автоматическая Фиксация Посещений:
   * Управление Устройствами: Ограничение использования внешних устройств для предотвращения утечек данных.
   * Система Автоматической Фиксации Посещений: Определение процедур автоматической фиксации времени прихода и ухода, а также обработки данных о посещениях.

В итоге, данная учетная политика позволит компании эффективно контролировать и отражать операции с клиентами, обеспечивать высокое качество обслуживания и формировать надежную отчетность о выполненных работах.

# БЛОКИ ПРОЦЕССОВ, ПОДЛЕЖАЩИЕ АВТОМАТИЗАЦИИ

### **Описание процесса мониторинга доступа**

это систематическое отслеживание и контроль за активностью пользователей в системе контроля доступа с целью обеспечения безопасности и эффективности. Процесс мониторинга доступа включает в себя следующие этапы:

1. Сбор данных о доступе:
   * Автоматизированный сбор данных о событиях доступа, включая входы и выходы, использование электронных пропускных устройств, аутентификацию и авторизацию.
2. Фильтрация событий:
   * Анализ собранных данных с целью выделения событий, требующих особого внимания (например, неудачные попытки доступа, попытки взлома, несанкционированные входы).
3. Определение аномалий:
   * Применение алгоритмов и аналитики для выявления аномального поведения или необычных событий, которые могут свидетельствовать о потенциальной угрозе безопасности.
4. Генерация Уведомлений:
   * Автоматическое создание уведомлений для ответственных лиц или служб безопасности в случае выявления подозрительных или критически важных событий.
5. Реагирование на Инциденты:
   * Быстрое и эффективное реагирование на уведомления, включая выяснение причин, предпринятие корректирующих действий и документирование произошедшего.
6. Анализ Эффективности:
   * Периодический анализ эффективности системы мониторинга доступа, внесение коррективов в алгоритмы и правила фильтрации для повышения точности выявления угроз.

### **Описание процесса автоматизации системы автоматической фиксации помещений**

* Интеграция с Электронными Пропускными Устройствами:
  + Автоматическое считывание данных с электронных пропускных устройств для определения времени входа и выхода.
* Система Видеофиксации:
  + Использование системы видеонаблюдения для автоматической фиксации посещений визуальным путем.
* Обработка и Анализ Данных:
  + Автоматизированная обработка данных о времени прихода и ухода с пропускных устройств и видеонаблюдения для сопоставления и анализа.
* Коррекция Несоответствий:
  + Введение механизмов для автоматической коррекции возможных несоответствий данных между различными источниками.
* Генерация Отчетности:
  + Автоматическое формирование отчетов о посещениях с указанием времени прихода и ухода, а также дополнительной информации (если необходимо).
* Уведомления и Оповещения:
  + Настройка системы уведомлений для оперативного оповещения ответственных лиц о несоответствиях или аномалиях в фиксации посещений.
* Интеграция с HR-Системой:
  + Взаимодействие с системой управления персоналом для автоматического обновления данных о посещениях в соответствии с кадровой информацией.
* Система Обратной Связи:
  + Внедрение автоматизированной системы обратной связи сотрудникам и посетителям о фиксации их посещений

### **Описание процесса автоматизации контроля доступа в здание через электронные пропускные устройства**

* Регистрация и Выдача Пропусков:
  + Автоматизированная система регистрации новых пользователей и выдачи электронных пропусков, включая привязку к учетным данным.
* Интеграция с Идентификационными Системами:
  + Связывание электронных пропускных устройств с системами идентификации, такими как карточки доступа или биометрические данные.
* Управление Правами Доступа:
  + Назначение и изменение прав доступа через централизованную систему управления доступом.
* Мониторинг и Регистрация Событий:
  + Автоматическое фиксирование событий доступа через электронные пропускные устройства с указанием времени и идентификационных данных.
* Фильтрация и Анализ Событий:
  + Анализ собранных данных для выявления необычных событий, попыток несанкционированного доступа или аномалий в системе.
* Уведомления и Аварийные Сценарии:
  + Конфигурация системы уведомлений о важных или потенциально опасных событиях, а также настройка аварийных сценариев для оперативного реагирования.
* Интеграция с Системами Учета Рабочего Времени:
  + Связь с системами учета рабочего времени для автоматического отслеживания времени пребывания сотрудников.
* Обновление и Модернизация:
  + Периодическое обновление программного обеспечения и аппаратных компонентов для поддержания безопасности и функциональности.

# ОПИСАНИЕ ТЕКУЩЕГО УРОВНЯ АВТОМАТИЗАЦИИ

На данный момент компания частично внедрила системы автоматизации в операционные процессы, однако автоматизация не охватывает полностью все аспекты нашей деятельности. Ниже представлено описание текущего уровня автоматизации:

* Неэффективное Использование Видеонаблюдения: Недостаточное использование возможностей видеонаблюдения для аналитики и распознавания. Отсутствие технологий искусственного интеллекта снижает эффективность системы в обнаружении подозрительных событий.Отсутствие автоматизации создания резервных копий: На данный момент контроль за созданием резервных копий осуществляется вручную директором компании.
* Сложности в Управлении Правами Доступа: Отсутствие централизованной системы управления правами доступа создает сложности в эффективном и быстром изменении уровней доступа.
* Формирование отчетов: Отчеты о деятельности компании и обслуживании клиентов создаются вручную с использованием Excel и Word. Процесс создания отчетов требует больших усилий и времени.
* Отсутствие Системы Оповещения: Не настроена система автоматических оповещений для персонала безопасности о событиях, требующих немедленного вмешательства.

Текущая система автоматизации сильно зависит от человеческого фактора, что может приводить к случайным ошибкам в файлах, доступ к которым имеют все сотрудники компании. Отсутствие системы отслеживания ошибок и системы контроля доступа к данным увеличивает риск инцидентов и несанкционированного доступа. Формирование отчетов также требует значительных ресурсов. Для оптимизации деятельности и улучшения эффективности необходима более глубокая автоматизация всех аспектов бизнес-процесса.

# ВЫВОДЫ ПО РЕЗУЛЬТАТАМ ПРОЕКТНОГО ОБСЛЕДОВАНИЯ КОМПАНИИ

### **Анализ текущего уровня автоматизации системы автоматической фиксации помещений**

На данный момент организация имеет внедренную систему автоматизации системы автоматической фиксации помещений, которая включает в себя следующие компоненты:

* Методы Фиксации: В настоящее время система использует автоматические методы фиксации посещений, основанные на данных от электронных пропускных устройств.
* Анализ Посещений: Осуществляется базовый анализ данных, такой как общее время пребывания и частота посещений, но без глубокого понимания паттернов и тенденций и.
* Система отчетности: Система предоставляет базовые отчеты о времени пребывания, но отсутствует глубокая аналитика для предоставления структурированных и полезных данных.

**11.2 Автоматизация и оптимизация системы автоматической фиксации посещений**

Однако, несмотря на наличие этих компонентов, существуют некоторые аспекты, которые можно улучшить:

* недрение Технологий Искусственного Интеллекта (ИИ):
  + Использование алгоритмов машинного обучения для автоматического анализа данных, выявления паттернов посещений, и определения аномалий или необычных сценариев.
* Интеграция с Системой Контроля Доступа:
  + Обеспечение тесной интеграции с системой контроля доступа для автоматического сопоставления данных о посещениях с правами доступа, что позволит идентифицировать несанкционированные посещения.
* Оптимизация Использования RFID и NFC Технологий:
  + Использование технологий Radio-Frequency Identification (RFID) и Near-Field Communication (NFC) для оптимизации процесса фиксации посещений и улучшения точности данных.
* Внедрение Системы Оповещений в Реальном Времени:
  + Разработка системы автоматических оповещений, которая мгновенно предупреждает персонал безопасности об аномальных событиях или несанкционированных посещениях.

### **11.3 Внедрение новых компонентов**

Для оптимизации системы мониторинга безопасности информации и повышения уровня безопасности рекомендуется внедрить следующие компоненты:

* Система Резервного Копирования и Восстановления: Введение надежной системы резервного копирования и восстановления данных для быстрого восстановления после инцидентов или чрезвычайных ситуаций.
* Система автоматизированного реагирования: Внедрение системы, которая будет автоматически реагировать на обнаруженные угрозы без участия операторов.
* Технологии Интеграции с Облачными Решениями: Интеграция с облачными системами мониторинга для обеспечения гибкости, масштабируемости и дополнительного уровня безопасности.

# ПОРЯДОК ВНЕДРЕНИЯ ПРОЕКТА АВТОМАТИЗАЦИИ

### **Предпроектное обследование**

Этот этап предпроектного обследования является важным для успешной реализации проекта мониторинга для контроля безопасности информации. В рамках этого этапа включены следующие шаги:

* Начальное ознакомление с организацией: Важно полностью понимать схему работы организации, включая ее бизнес-процессы и структуру.
* Изучение документооборота: Подробное изучение текущей системы документооборота поможет выявить основные потребности в мониторинге информации.
* Отчётная политика: Оценка текущей отчётной политики, включая требования к безопасности информации.
* Политика работы с клиентами: Изучение методов взаимодействия с клиентами и определение требований по защите их данных.
* Оптимизация и внедрение подсистем: Определение оптимальных путей автоматизации процессов и подсистем, которые требуется внедрить

### **Обучение сотрудников компании правилам и методам работы**

Обучение сотрудников ключевым аспектам мониторинга безопасности информации и правилам работы с системой:

* Ввод информации: Внесение необходимых данных в систему, проведение тестирования программы.
* Опытная эксплуатация: Оценка работы системы в реальных условиях.
* Внесение изменений: В случае необходимости, вносит корректировки в созданный программный продукт.

### **Ввод созданной системы автоматизации, исправление найденных по ходу эксплуатации недостатков**

На этом заключительном этапе происходит полноценное внедрение системы мониторинга для контроля безопасности информации:

* Полноценный ввод в эксплуатацию: Система мониторинга начинает использоваться в работе.
* Исправление недостатков: По ходу эксплуатации выявляются недостатки, которые корректируются.
* Установление сроков ввода: Определяется точный срок ввода системы в эксплуатацию, исходя из особенностей проекта.

# ЭКОНОМИЧЕСКАЯ ЦЕЛЕСООБРАЗНОСТЬ ВНЕДРЕНИЯ

Эффективность внедрения системы контроля доступа в здание организации, включающую в себя электронные пропускные устройства, видеонаблюдение и систему автоматической фиксации посещений определяется взаимодействием затрат и ожидаемых результатов. С одной стороны, затраты связаны с установкой и сопровождением системы, а с другой стороны, проект должен привести к уменьшению операционных и трудовых затрат организации, а также к повышению оперативности в работе с посещениями и безопасностью.

Затраты включают в себя:

* Стоимость оборудования и техники: Приобретение и установка необходимого оборудования для системы мониторинга и его настройка.
* Стоимость программного обеспечения: Приобретение необходимых лицензий и программного обеспечения.
* Затраты на настройку и ввод в эксплуатацию: Затраты на консультации, профессиональную настройку системы и обучение сотрудников.
* Затраты на сопровождение: Расходы на обновление, поддержание и регулярное обслуживание системы.

Ожидаемые результаты включают в себя:

* Улучшенная Система Контроля Доступа: Развертывание электронных пропускных устройств для эффективного и безопасного контроля доступа в здание.
* Эффективное Видеонаблюдение: системы видеонаблюдения для повышения безопасности и быстрого реагирования на инциденты.
* Автоматическая Фиксация Посещений: Разработка и внедрение системы, автоматически фиксирующей посещения сотрудников и посетителей.
* Электронная Система Документооборота: Внедрение электронной системы управления документами для более эффективного документооборота внутри организации.

Исходя из этих факторов, можно предположить, что при сохранении среднего потока информации и клиентов, внедрение системы для контроля безопасности позволит повысить оперативность работы компании на 40%. Это обеспечит более быстрое и эффективное взаимодействие с информацией, снижение рисков и сокращение операционных затрат в долгосрочной перспективе.

# Приложение №1

Отчет о контроле доступа в организации

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.

1. Журналы авторизации 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.

2. Выявление внешних угроз

* 23.10.2023 - Внешние атаки были обнаружены в форме попыток несанкционированного доступа через SSH на сервер 192.198.1.11. Атаки были успешно отражены благодаря системе обнаружения вторжений.

3. Система резервного копирования данных

* 22.10.2023 02:00 - Начало автоматического резервирования данных.
* 22.10.2023 02:30 - Проверка целостности резервных копий.
* 22.10.2023 02:35 — Резервирование было завершено не полностью.

4. Ошибки при создании резервных копий

В журналах обнаружены следующие ошибки при создании резервных копий:

Ошибка в создании резервной копии базы данных CRM.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Процесс | Аналитик безопасности | Администратор системы мониторинга | Специалист технической поддержки | Директор | Архив |
| 1. Регистрация заявки |  |  |  |  |  |
| 1. Анализ и устранение причины сбоя |  |  |  |  |  |
| 1. Настройка системы с учетом причины сбоя |  |  |  |  |  |
| 1. Внесение в историю заявок |  |  |  |  |  |

Таблица 1 – Оперграмма работы при возникновении неполадок у клиента