Содержание

[Список используемых сокращений 3](#_Toc30971634)

[Введение 4](#_Toc30971635)

[1 Исследование характеристик объекта защиты и действующей системы контроля и управления доступом 7](#_Toc30971636)

[1.1 Общая характеристика аэропорта, его информационная и физическая структура 7](#_Toc30971637)

[1.2 Анализ существующей системы контроля и управления доступом на базе аэропорта 10](#_Toc30971638)

[1.3 Выявление недостатков существующей системы и обоснование необходимости модернизации 15](#_Toc30971639)

[Выводы по первой главе 20](#_Toc30971640)

[2 Разработка проектного решения по модернизации системы контроля и управления доступом аэропорта 21](#_Toc30971641)

[2.1 Разработка структуры модернизированной СКУД и алгоритма функционирования 21](#_Toc30971642)

[2.2 Выбор оборудования и программного обеспечения СКУД, необходимого для модернизации 28](#_Toc30971643)

[2.3 Внедрение модернизированной системы СКУД на объекте 46](#_Toc30971644)

[Выводы по второй главе 48](#_Toc30971645)

[3 Показатели продолжительности проекта модернизации 49](#_Toc30971646)

[3.1 Расчет трудоемкости и продолжительности разработки проекта 49](#_Toc30971647)

[3.2. Составление календарного плана выполнения работ 51](#_Toc30971648)

[Выводы по третьей главе 52](#_Toc30971649)

[4 Безопасность и экологичность проекта 53](#_Toc30971650)

[4.1 Разработка рекомендаций по обеспечению охраны труда в процессе реализации проекта 53](#_Toc30971651)

[4.2 Защита сотрудников в чрезвычайных ситуациях 56](#_Toc30971652)

[4.3 Экологичность проекта 57](#_Toc30971653)

[Выводы по четвертой главе 57](#_Toc30971654)

[Заключение 58](#_Toc30971655)

[Список используемых источников 60](#_Toc30971656)

# Список используемых сокращений

АРМ – автоматизированное рабочее место

АС – автоматизированная система

БД – база данных

ИБ – информационная безопасность

ИТ – информационные технологии

ЛВС – локальная вычислительная сеть

ОПС – охранно-пожарная сигнализация

ПК – персональный компьютер

ППП – пакеты прикладных программ

ПО – программное обеспечение

РНЦ – Российский научный центр

СВТ – средства вычислительной техники

СЗИ – средства защиты информации

СКУД – система контроля управления доступом

СПС – система пожарной сигнализации

СОИ – системы обработки информации

СУБД – система управления базами данными

ТБ – техника безопасности

ТЗ – техническое задание

ЭВМ – электронная вычислительная машина

# Введение

В настоящее время с развитием информационным систем актуальной становится задача внедрения систем информационной безопасности для обеспечения сохранности информации и безопасности предприятий.

Надежную защиту объектов на сегодняшний день невозможно обеспечить, не внедряя современные средств контроля и управления доступом. В последнее время все более часто имеют место кражи информационных носителей, которые содержат информацию конфиденциального характера. Поэтому все чаще принимаются организационные и технические методы, которые направлены на повышение качества систем защиты информации. Задача обеспечения надежной защиты корпоративных систем – базовая задача в сфере обеспечения защиты для любой организации. С развитием предприятий, переходом к распределенной структуре организаций, они начинают выходить за пределы отдельных зданий. С учетом вышеуказанных фактов, с уверенностью можно заявить о том, что проблематика обеспечения защиты информационных ресурсов на данный момент не в полной мере разрешена. Так как у большинства организаций остаются не решенными вопросы обеспечения контроля и управления доступом, они терпят финансовые убытки [3].

Тема данной выпускной квалификационной работы – «Модернизация системы контроля и управления доступом на базе аэропорта».

В физической безопасности термин «контроль доступа» относиться к практикам ограничения доступа к собственности, в здания или помещения, доступ к которым разрешён только для авторизованных людей. Физический контроль доступа, может быть, достигнут путём использования человека (охранник, вышибала или служащий в приёмной), через механические способы, такие как замки и ключи на двери, или через технологические средства, такие как системы доступа, основанные на картах доступа или биометрической идентификации.

Автоматизированная система для обеспечения функций администратора СКУД включать в себя компоненты: ведение классификаторов; автоматизации учета заявок на доступ в охраняемые помещения, мониторинг посещаемости охраняемых помещений, автоматизации формирования отчетности, ведение картотеки оборудования.

В настоящее время создание и внедрение СКУД является актуальной задачей, так как способствует повышению эффективности работы предприятий и защиты информации.

Актуальность темы данной выпускной квалификационной работы определяется:

- увеличением рисков из-за появления физических угроз ресурсам компании;

- современными темпами и уровнем развития методов обеспечения контроля и управления доступом;

- рост анализируемой компании, увеличение числа сотрудников кредитного центра и объема обрабатываемых данных;

Цель выпускной квалификационной работы – реализация проекта модернизация системы контроля и управления доступом на базе аэропорта.

Для достижения цели выпускной квалификационной работы необходимо разрешение следующих задач:

– дать общую характеристику аэропорта, его информационной и физической структуре;

– произвести анализ существующей системы контроля и управления доступом на базе аэропорта;

– выявить недостатки существующей системы и обосновать необходимость модернизации;

– разработать структуру модернизированной СКУД и алгоритм ее функционирования;

– произвести выбор оборудования и программного обеспечения СКУД, необходимого для модернизации;

– разработать проект внедрения модернизированной системы СКУД на объекте;

– произвести расчет технико-экономических показателей проекта;

– разработать рекомендации по обеспечению охраны труда в процессе реализации проект и защите сотрудников в чрезвычайных ситуациях.

Методы исследования: изучение литературных источников, нормативно-правовой базы, изучение технической документации средств защиты информации, анализ технологий работы СКУД, методы сравнения, наблюдения.

Практическая значимость проекта состоит в том, что его результат позволит модернизировать систему контроля и управления доступом исследуемого объекта, что обеспечить высокий уровень его безопасности. Модернизированная система будет соответствовать всем современным требованиям безопасности. При этом будет затрачено минимальное количество временных и материальных ресурсов.

# 1 Исследование характеристик объекта защиты и действующей системы контроля и управления доступом

# 1.1 Общая характеристика аэропорта, его информационная и физическая структура

Данная выпускная квалификационная работа выполнена на базе типовой модели аэропорта.

Аэропорт – комплекс сооружений, предназначенный для приема, отправки воздушных судов и обслуживания воздушных перевозок, имеющий для этих целей аэродром, аэровокзал и другие наземные сооружения и необходимое оборудование.

Аэровокзал (терминал аэропорта) – здание для обслуживания пассажиров воздушного транспорта и операций с багажом, обычно в аэропортах.

Аэровокзальный комплекс – включает в себя собственно аэровокзал, предназначенный для обслуживания пассажиров. В аэровокзале базируются большинство служб, обслуживающих пассажиров от момента входа на территорию аэропорта до вылета и от момента подачи трапа к самолёту до покидания аэропорта: представительства авиакомпаний; служба организации пассажирских перевозок; службы безопасности; багажная служба; службы пограничного, иммиграционного и таможенного контроля; различные организации и предприятия, направленные на отдых, развлечения пассажиров и т. п.: рестораны и кафе, точки торговли периодикой и сувенирами, магазины, и т. д. Грузовой комплекс. Принимает к отправке, оформляет, обрабатывает, загружает на борт воздушных судов груз и почту. Оснащается крытым отапливаемым складом, средствами доставки и механизированной погрузки-разгрузки, средствами обработки груза «в навал» и в контейнерах.

Инфраструктура аэропорта включает:

– ангарный комплекс для технического обслуживания и мойки ВС, в том числе отапливаемый ангар площадью 5100 м2, что позволяет обслуживать BC вплоть до типа MD-11, и неотапливаемый ангар площадью 5700 м2;

– складские помещения и инструментальные кладовые с круглосуточным доступом площадью более 700 м2;

– лаборатории АиРЭО с производственной площадью 1300 м2;

– участок расшифровки и анализа полетной информации площадью 180 м2;

– слесарно-механический участок площадью 72 м2;

– группы неразрушающих методов контроля с производственной площадью 103 м2;

­ – лаборатория авиационной метрологии общей площадью 579,15 м2;

­– наземное штурманское обеспечение;

– грузовой терминал, расположенный на территории 23 000 м2, включающий складские и офисные помещения общей площадью 10 300 м2;

– топливозаправочные комплексы;

– цеха бортового питания.

Исследуем архитектурную схему аэропорта.

Под архитектурой предприятия понимается структурное описание организации как системы управления в терминах бизнеса и информационных технологий, включающее характеристику существенных элементов этой системы и связей между ними. Основная задача архитектуры предприятия – сфокусировать внимание IT-блока предприятия на реализации его миссии и достижении стратегических целей бизнеса.

Создание корпоративных архитектур, за редким исключением, не носит обязательного регламентирующего характера. Если говорить о коммерческих организациях, то обычно этот вопрос находится в сфере полномочий высшего руководства организации. Но, по оценкам аналитиков, ежегодно будет увеличиваться число предприятий, нацеленных на создание комплексных архитектур. При этом архитекторам предприятий, проектирующим исключительно информационно-технологические архитектуры, придется обосновывать результаты своей деятельности и ее полезность с точки зрения потребностей основного бизнеса организации.

Современное гражданское авиапредприятие – это сложное многофункциональное объединение, обеспечивающее пассажирские и грузовые авиаперевозки, с большим количеством потребителей и поставщиков услуг.

Авиапредприятие в своей информационной структуре имеет компьютерную сеть, в которую включены рабочие компьютеры сотрудников. Доступом к данной компьютерной сети обладают только сотрудники организации. Рассмотрим типовое решение информационной архитектуры для авиапредприятия.

Вся сеть располагается в пределах комплекса зданий авиапредприятия. Сеть организована по топологии типа «звезда». Основными преимуществами компьютерных сетей с данным типом топологии является высокая производительность и устойчивость к различным сбоям в работе, которые связаны неполадками в конкретных элементах сети либо с повреждениями сетевых кабелей.

Основная деятельность организации сосредоточена на документальном обеспечении процессов обслуживания пассажиров и продаж билетов, организации полетов, а также технической поддержке работы всей системы.

Схема компьютерной сети авиапредприятия приведена на рисунке 1.1.

Рисунок 1.1 – Схема компьютерной сети авиапредприятия

Действующая СКУД функционирует на базе ЛВС аэропорта.

# 1.2 Анализ существующей системы контроля и управления доступом на базе аэропорта

В наше неспокойное время для пассажиров стали нормой чрезвычайные меры безопасности, предпринимаемые перед посадкой в самолет. Новые процедуры досмотра и современное оборудование гарантируют, что представляющие опасность предметы не попадут на территорию аэропорта и борт самолета. И все же безопасность аэропорта предполагает гораздо больше, чем предотвращение возможных атак. Растущий пассажиропоток, увеличение скорости перемещения людей, обработки багажа и других процессов могут спровоцировать многие неприятности.

Задачи СКУД аэропорта:

• Автоматизация пропуска сотрудников с разными уровнями допуска.

• Учет рабочего времени сотрудников.

• Реализация СКУД автопаркинга;

• Реализация зон доступа - по сотрудникам, по времени.

• На особо важных объектах должно происходить многократное подтверждение идентификационных данных.

• Металлодетекторы для всех пассажиров.

• Отслеживание багажа пассажиров при помощи специальных меток.

• Интеграция СКУД в системы видеонаблюдения, противопожарные системы.

• Система идентификации для пассажиров по билетам.

Компоненты СКУД аэропорта:

• Большое количество персональных идентификаторов для персонала.

• Идентификаторы для пассажирского багажа.

• Считыватели самого разнообразного типа.

• Система видеонаблюдения, тревожные кнопки.

• Центральный сервер и пульты управления СКУД и системами безопасности.

• Рамки металлоискателей, идентификации багажа.

• Большое количество энергонезависимых контроллеров доступа, объединенных в единую сеть.

• Система распознавания номерных знаков автотранспорта.

• Система распознавания лиц с целью выявления подозрительных пассажиров, попавших в черные списки аэропортов.

На исследуемом объекте СКУД построена на базе системы SALTO XS4 RFID.

SALTO XS4 RFID – универсальная сетевая система контроля доступа, которая способна решить все вопросы по организации доступа сотрудников, подрядчиков и посетителей в любые зоны и помещения аэропорта или объекта транспортной инфраструктуры. SALTO XS4 RFID позволит Вам создавать единую СКУД всего объекта, значительно экономя как на стоимости управляющих элементов СКУД, так и на административных расходах на управление системой. При этом имеется возможность делегировать необходимые полномочия в административные подразделения и государственные службы (службы пограничного, иммиграционного и таможенного контроля), чтобы они могли полноценно управлять и контролировать свой подраздел СКУД.

Основная особенность: построение территориально-распределенной масштабируемой СКУД с административно-правовым разделением полномочий, включение в единую систему онлайн точек доступа для управления входными группами и критически важными точками доступа (турникеты на входе в здание или его части, разделение таможенной / миграционной / пограничной и входных зон) - и беспроводных электронных замков и цилиндров (для дверей отдельных кабинетов и помещений). Благодаря отсутствию проводов, автономному питанию от батарей и продуманной конструкции, электронные замки и цилиндры максимально просто установить как на существующие, так и на новые двери, без необходимости прокладки проводов, замены двери или корпуса замка.

Технология специального антимикробного покрытия электронных замков SALTO BioCote позволяет гарантировать санитарную безопасность при установке СКУД в местах с большой проходимостью и защитит сотрудников и пассажиров от риска заражения болезнями, передаваемыми через кожный контакт.

Состав СКУД SALTO XS4 RFID:

1. Комплекс управления СКУД, который состоит из клиент – серверного приложения SALTO Pro-Access, программатора PPD (Portable Programming Device) и энкодеров (USB или Ethernet версии);

2. Подсистема контроля доступа входных групп и ключевых дверей - настенные считыватели с контроллерами СКУД (онлайн IP);

3. Подсистема контроля доступа к служебным, административным и офисным помещениям – электронные замки серии SALTO XS4 или AElement, электронные цилиндры SALTO GEO (автономные, c технологией "Виртуальная Сеть SALTO" - или онлайн c технологией "SALTO Wireless"), электронные замки серии Секьюрити, настенные считыватели с контроллерами СКУД (онлайн и оффлайн версии);

4. Подсистема контроля доступа к складам, аппаратным и помещениям жизнеобеспечения - электронные цилиндры SALTO GEO, электронные замки серии Секьюрити, настенные считыватели с контроллерами СКУД (онлайн и оффлайн версии);

5. Подсистема контроля доступа к дверям эвакуационных и аварийных выходов - электронные замки с антипаник-баром, решения SALTO для эвакуационных дверей;

6. Подсистема контроля доступа к серверным стойкам, архивным/аппаратным шкафам и мебели – электронные замки для шкафчиков XS4-Lockers, электронные цилиндры SALTO GEO;

7. Подсистема энергосбережения и контроля использования оборудования – активные энергосберегающие контроллеры SALTO ESD;

8. Электронные RFID карты и носители SALTO.

СКУД SALTO XS4 RFID позволяет использовать карты доступа для безналичных платежей внутри учреждения при использовании следующих систем управления точками продаж (POS систем): Micros, InfoGenesis, UCS R-Keeper, Iiko и других.

Структурная схема организованной СКУД приведена на рисунке 1.2.

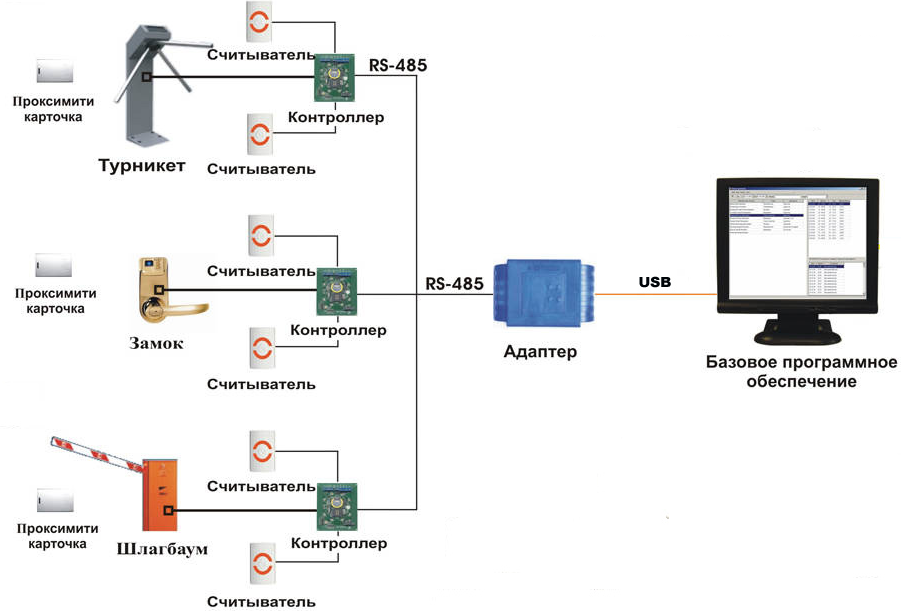


Рисунок 1.2 – Структурная схема организованной СКУД

Возможности СКУД SALTO XS4 RFID:

* Макс. кол-во пользователей в БД: 4 000 000 (4 миллиона);
* Макс. кол-во посетителей: не ограничено;
* Макс. кол-во дверей (точек доступа) в системе: 64 000;
* Пропорция точек доступа Автономные / Беспроводные онлайн / Проводные онлайн (IP): любая;
* Тайм-зон: 256;
* Тайм-периодов в системе: 256;
* Тайм-периодов в памяти замка: 30;
* Календарей в системе: 256;
* Зон доступа: 1024;
* Групп доступа: не ограничено.

# 1.3 Выявление недостатков существующей системы и обоснование необходимости модернизации

Охранная система безопасности должна быть подобрана, в соответствии с конструктивными особенностями объекта, его назначением, площадью и другими параметрами. Сейчас многие здания используют для разных целей. В связи с этим требуется модернизация, улучшение существующей системы безопасности.

Некоторые детали в оборудовании морально устаревают или изнашиваются. Модернизация требуется при необходимости расширить возможности техники из-за увеличения территории объекта или при внедрении новых контролируемых комнат.

Современные изготовители охранного оборудования регулярно совершенствуют модель, вводят в эксплуатацию новые технологические и многофункциональные приспособления. Чтобы модернизация была успешной и эффективной, мировые производители грамотно используют те ресурсы, которыми обладают, придерживаются установленных стандартов и норм.

СКУД аэропорта – это система, которая представляет собой обширный комплекс охранных услуг. Благодаря ей, на объекте добиваются наиболее эффективной охраны объекта. Наблюдается практика, когда при модернизации существующей системы контроля и управления доступом устанавливается техника с похожими функциями. В итоге пользователи должны применять сразу несколько карт, сотрудники охранной компании – обслуживать большое количество приборов. Это влечет за собой неблагоприятные для владельца объекта последствия в виде увеличения текущих затрат на эксплуатацию охранного оборудования.

При длительной эксплуатации охранное оборудование, которое используется на объекте, устаревает, становится непригодным. В результате этого может потребоваться:

* замена тех или иных инструментов, деталей;
* модернизация компьютера, регулярные обновления при использовании интернета;
* монтаж инновационной техники (к примеру, стандартные приборы на входном контроле могут быть заменены биометрическими устройствами);
* при достройке объекта или реорганизации предприятия увеличение количества охранных приборов.

Два требования, которым должна соответствовать исследуемая система контроля доступа: отвечать стандартам безопасности и ключевым бизнес-процессам компании.

Промышленным стандартом физического контроля доступа принято считать идентификаторы 125 кГц. Основная причина их популярности: низкая стоимость. Недостатки: отсутствие возможности перепрограммирования, незащищенность технологии, как следствие, простота подделки и копирования.

Наличие передовых технологий идентификации, реализованных в смарт-картах 13,56 мГц с дополнительными средствами шифрования модели SIO, возможность комбинирования нескольких способов идентификации, включая биометрию, применения карты доступа как единого идентификатора для входа в помещение и к ИТ-ресурсам компании – основные предпосылки для пересмотра корпоративных политик в вопросах аутентификации и идентификации.

Таблица оценки защищенности технологий идентификации приведена ниже.

Таблица 1.1 – Оценка защищенности технологий идентификации

|  |  |  |  |
| --- | --- | --- | --- |
| Угроза безопасности | | | |
| Повторное воспроизведение | Клонирование | Конфиденциальность данных | Дополнительный уровень безопасности |
| Защита от угроз | | | |
| Взаимная аутентификация | Диверсификация ключа | Шифрование DES, 3DES, AES | Привязка к UID/CSN, CMAC 96 |
| EM Marine | Нет | Нет | Нет |
| Mifare | Да, но открытая | Нет | Нет |
| DESFire EV1 | Да | Да | Да |
| iCLASS SE | Да | Да | Да |

Необходимость замены вышедших из строя аппаратных частей системы, потребность в новом функционале и расширении системы, интеграция с корпоративными системами, ставят вопросы о необходимости модернизации аппаратной или программной частей системы контроля доступа.

В действующей системе контроля доступа для сотрудников в качестве считывателя используются бесконтактных карт стандарта EM-Marine с рабочей частотой 125 кГц и преобразования кода считанной карты в код Dallas Touch Memory (или Wiegand-26) и RS-232. Для идентификации пользователя карты и организации системы учета рабочего времени, считыватель подключается к персональному компьютеру, на котором установлено соответствующее программное обеспечение. Считывание карты подтверждается звуковым сигналом встроенного зуммера. Расположенный на лицевой стороне двухцветный светодиод, можно использовать, как дополнительное средство индикации. Для организации входа и выхода из помещения по картам, без использования кнопки выхода, к считывателю подключается дополнительная выносная антенна.

Сначала в память контроллера «Touch Memory» (TM) записывают все карты, которые будут иметь возможность управлять замками. Затем все номера этих карт записывают на компьютер (создается база пользователей с именами, фотографиями). Один считыватель ставится с одной стороны турникета, другой с внутренней. Когда пользователь, карта которого записана в контроллер ТМ, подходит к считывателю, происходит передача ее идентификационного номера на считыватель. Полученный преобразуется в код, имитирующий ключ, который поступает на первый выход (команда на открытие замка). Одновременно осуществляется преобразование кода карты в код стандарта RS-232, который поступает на второй выход, предназначенный для передачи информации на компьютер. На компьютере код сопоставляется с базой данных и на экран выводится фотография пользователя и информация о нем. Пользователь проходит через турникет, при этом срабатывает контакт и на компьютер поступает сигнал о том, что пользователь вошел на охраняемую территорию. При выходе все происходит аналогично. Таким образом, с помощью считывателей осуществляется контроль доступом и учет рабочего времени сотрудников аэропорта.

Недостаток системы в том, что котроллер и компьютер работают независимо друг от друга. Если карта была записана в память контроллера, но не была записана на компьютер, то замок сработает, а на компьютере появится сообщение о входе по незарегистрированной карте. И наоборот, если карта записана на компьютер, но не записаны в контроллер, то на компьютере появится сообщение о поднесении карты пользователя, но турникет не откроется.

Действующая СКУД имеет некоторые недостатки, основной из которых, – низкая эксплуатационная надежность применяемых технических средств и системы в целом. Эксплуатирующий персонал вынужден периодически проводить технические ремонты, связанные с заменой оборудования системы. Оборудование действующей СКУД устарело.

Решение о модернизации действующей системы управления связано с необходимостью:

- повышения уровня эксплуатационной надежности СКУД посредством замены физически и морально устаревшего электрооборудования системы;

- повышения уровня оперативного управления за счет обеспечения оператора оперативной информацией о состоянии объекта;

- уменьшения зависимости результатов работы от квалификации сотрудников;

- сокращения времени поиска и устранения неисправностей систем управления за счет обеспечения сотрудников оперативной информацией о состоянии оборудования;

- создания условий для последующего развития системы;

- повышения комфортности работы оператора и быстрой перенастройки системы.

Различают несколько концепций модернизации оборудования СКУД:

* полная замена программной и/или аппаратной частей;
* замена или обновление программной части;
* поэтапная замена аппаратной части.

Полная замена программной или аппаратной частей системы СКУД – целесообразна, в случае, если система СКУД не соответствует ни критериям безопасности, ни ожиданиям бизнес-заказчика. Основным достоинством данного варианта является возможность не только внедрить передовые технологии, но и обеспечить совместимость и преемственность технологий при последующих обновлениях системы. Ключевой недостаток решения: высокие единовременные инвестиции.

Функциональные ограничения действующей системы с точки зрения программного обеспечения, отсутствие программной поддержки передовых технологий идентификации и форматов карт, недостаточная совместимость и преемственность версий ПО - наиболее частые причины замены управляющего ПО системы СКУД. В данном случае необходима замена или обновление программной части. При выборе управляющего ПО целесообразно обращать внимание на известность марки и поставщика, программную поддержку систем и оборудования.

Поэтапная замена аппаратной части – основными критериями выбора данного способа обновления системы является равномерное распределение затрат на модернизацию системы, возможность заказчика самостоятельно определить временной период перехода на новую систему и какой функционал необходимо внедрить в первую очередь.

Немаловажным является возможность обеспечения бесперебойной работы системы в период перехода на более защищенные технологии, а также безболезненность перехода для администраторов системы и сотрудников компании. При выборе программной части системы необходимо обратить внимание на совместимость и преемственность версий программного обеспечения, возможность расширения системы, мультивендорного подхода поддержки оборудования и вариаций добавления нового функционала. При выявлении угроз, вызванных подделками или копированием идентификаторов, переход на защищенные технологии идентификации можно осуществить постепенно, используя мультитехнологичные считыватели или мультитехнологичные карты.

# Выводы по первой главе

Первая глава выпускной квалификационной работы посвящена исследованию характеристик объекта защиты и действующей системы контроля и управления доступом. В данной главе исследована общая характеристика аэропорта, его информационная и физическая структура. Произведен анализ существующей системы контроля и управления доступом на базе аэропорта. Так же выявлены недостатки существующей системы и обоснована необходимость ее модернизации.

# 2 Разработка проектного решения по модернизации системы контроля и управления доступом аэропорта

# 

# 2.1 Разработка структуры модернизированной СКУД и алгоритма функционирования

Проектируемая СКУД будет включать в своем составе следующие компоненты:

- рабочее место оператора;

- рабочее место администратора;

- центральный сервер СКУД;

- рабочее место сотрудника КПП;

- интерфейсы считывателей;

- идентификаторы сотрудников;

- контроллеры входа в помещения;

- модули учета входов и выходов сотрудников.

Структура взаимодействия компонент СКУД приведена на рисунке 2.1.

В таблице 2.1 приведен перечень функций и назначения компонентов проектируемой СКУД.

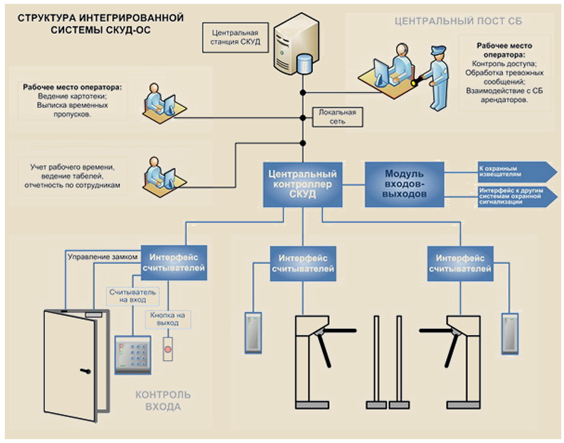


Рисунок 2.1 - Структура взаимодействия компонент СКУД

Таблица 2.1 - Перечень функций и назначения компонентов проектируемой СКУД

|  |  |
| --- | --- |
| Название компонента | Назначение компонента |
| 1. Рабочее место | Управление считывателями, настройка прав доступа, блокирование идентификаторов, выпуск новых идентификаторов, управление учетными записями операторов СКУД, управление доступом в охраняемые помещения |
| 2. КПП | Учет проходов/проездов сотрудников, мониторинг состояния СКУД |
| 3. Центральный сервер СКУД | Хранение базы данных СКУД, управление досту- пом к базе на уровне СУБД, установка и настройка серверного ПО СКУД |

Окончание таблицы 2.1

|  |  |
| --- | --- |
| Название компонента | Назначение компонента |
| 4. Учет времени | Формирование отчетной информации о нахождении сотрудников на объектах предприятия, фактически отработанном времени |
| 5. Контроллеры входа в помещения | Считывание идентификатора сотрудника, определение возможности доступа |
| 6. Идентификаторы сотрудников | Использование для доступа в охраняемые помещения организации |
| 7. Модули учета входов и выходов сотрудников | Программный учет входов и выходов сотрудников в помещения |

Точки прохода представляют собой барьер либо иную преграду, на которой установлен считыватель, который подключен к исполняющему устройству. Точки прохода могут иметь контроль на вход либо быть полностью контролируемыми, когда на проход устанавливается два считывателя – на выход и на вход. Если реализован только контроль прохода внутрь, то выход осуществляется либо свободно, либо с использованием кнопки RTЕ.

В настоящее время СУ для большинства коммерческих СКУД выполняются на основе микроконтроллеров, имеющих проприетарную архитектуру, что существенно снижает возможности перенастройки системы, а также привязывает потребителя к конкретному производителю СКУД.

Особенности режима доступа на различных объектах привели к появлению нескольких алгоритмов прохода.

1. Вход и выход по карте.

Этот алгоритм требует двух считывателей – один устанавливается снаружи, а второй – внутри помещения. После предъявления карты контроллер анализирует полномочия пользователя. Если доступ разрешен, то контроллер включает реле, управляющее замком, замок при этом открывается. Затем, по срабатыванию дверного датчика, в системе регистрируется событие "Штатный вход" или "Штатный выход" с указанием кода предъявленного идентификатора.

Если полномочия карты не позволяют выполнить проход, контроллер передает на сервер событие "Отказ в доступе". Все формируемые контроллерами события записываются в электронный протокол СКУД с указанием времени, даты, а также кода предъявленного идентификатора. Алгоритм применим на любых объектах, где требуется строгая фиксация событий входа и выхода каждого сотрудника.

2. Вход по карте, выход по кнопке.

Для каждой двери требуется только один считыватель. Проверка прав выполняется при входе в помещение, при этом работа системы полностью аналогична предыдущему алгоритму. Для выхода из помещения пользователь нажимает на кнопку, установленную рядом с дверью и подключенную к контроллеру. Дверь открывается без проверки полномочий, а в протоколе регистрируется событие "Штатный выход по кнопке".

Так как при выходе карта не предъявляется, система не может определить, находится конкретное лицо в зоне контроля или покинуло ее. Эта особенность алгоритма позволяет использовать его только в местах, где не требуется точно знать местонахождение пользователя. Типичная область применения – внутренние помещения, не задействованные в системе учета рабочего времени.

Произведем разработку алгоритма функционирования СКУД.

При обмене данными с сервером аудита контроллер СКУД выполняет следующие функции:

1. При подключении к удаленному серверу, посылает сигнал установления соединения.

2. При считывании идентификатора пользователя, посылает сообщение о проходе (попытке проникновения).

3. При приеме сообщения «ReadUserID» контроллер считывает имеющуюся бузу данных идентификаторов и отправляет их на сервер.

4. При приеме сообщения «Update» контроллер удаляет имеющуюся бузу данных идентификаторов.

5. При приеме сообщения «New» контроллер записывает в имеющуюся бузу данных полученный идентификатор пользователя.

6. При приеме сообщения «ReadConf» контроллер считывает начальную конфигурации и отправляет ее на сервер.

7. При приеме сообщения «Conf» контроллер стирает файл настроек и записывает новый, после чего перезагружается. Алгоритм сетевого обмена с сервером аудита событий системы контроля и управления доступом представлен на рисунке 2.2.

На рисунке 2.3 представлен алгоритм процесса идентификации пользователя и управления преграждающим устройством.

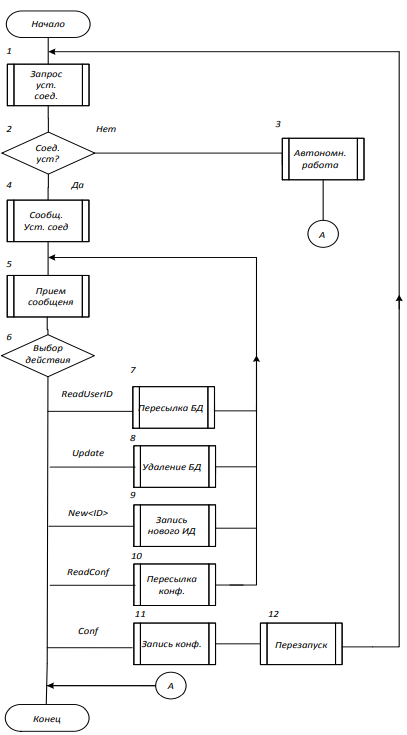


Рисунок 2.2 - Алгоритм сетевого обмена с сервером аудита событий системы контроля и управления доступом

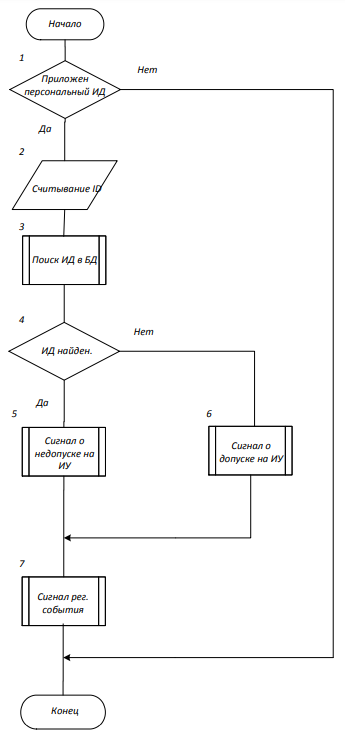


Рисунок 2.3 - Алгоритм процесса идентификации пользователя и управления преграждающим устройством

# 2.2 Выбор оборудования и программного обеспечения СКУД, необходимого для модернизации

Рынок СКУД в России на настоящий момент достаточно обширен и весьма разнообразен, и при этом постоянно расширяется: на нем представлены как отечественные, так и зарубежные производители. Причем это как раз тот случай, когда не стыдно за отечественных производителей: их продукция, по мнению специалистов, как минимум не уступает, а по многим параметрам даже превосходит иностранную [9].

Перед тем как осуществить анализ систем, предлагаемых различными компаниями, определим основные понятия, которые характеризуют оборудование СКУД.

Под максимальным количеством идентификаторов для одной точки прохода понимается количество карточек, которые могут быть записаны на одном контроллере. Наиболее проходимым местом являются контроллеры турникетов на центральном входе, так как через него ходят все сотрудники и посетители. Для рассматриваемого объекта это ограничение не играет большой роли. Максимальное количество контроллеров в сети фактически означает максимальное количество контролируемых точек прохода в системе. Выбирая СКУД для установки, необходимо учитывать, что в дальнейшем систему, возможно, придется масштабировать. И если система «вырастет» из максимального количества контроллеров, то встанет вопрос о её децентрализации [8].

Максимальное количество пользователей в системе – это общее количество карточек, которое может обрабатываться базой данных системы. Как правило, ограничения связаны с типом используемой СКУД базы данных.

Зональная antipassback–функция безопасности системы. Она предотвращает повторный проход через точку доступа по одному идентификатору. Практически во всех современных системах существует возможность организации нескольких зон. То есть, например, не войдя в здание, вы не сможете попасть к себе на этаж. В основном, для связи между контроллерами, используется интерфейс RS-485 или Ethernet. В случае использования RS-485 увеличивается максимальная длина магистрали до контроллера. Связь по этому интерфейсу осуществляется по двум проводам (в большинстве случаев можно использовать пару UTP). Максимальная длина магистрали при подключении по Ethernet должна превышать 100 м, однако в этом случае добавляются дополнительные функции управления контроллером.

Временные зоны в СКУД обычно используются для следующих целей: ограничить доступ в помещение в ночное время и выходные дни тем людям, у которых нет в этом производственной необходимости, а также для корректной настройки учета рабочего времени для людей с ненормированным рабочим днем, плавающим, посменным или свободным графиком [11].

Для удобства использования вышеуказанные параметры были сведены в таблицу по разным производителям.

Таблица 2.2 – Параметры различных производителей СКУД

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Фирма-производитель | Keri systems | Lenel | Lyric (Apollo) | Грифон |
| Параметр |
| Макс. кол. идентификаторов для  точки прохода | 6500 | 12500 | 139900 | 250000 |
| Макс количество контроллеров в сети | 128 | 128 | 352 | 250 |
| Зональный antipassback | да | да | да | да |
| Интерфейс подключения  контроллеров | RS-485 | Ethernet, RS-485 | Ethernet, RS-485 | Ethernet |

Окончание таблицы 2.2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Фирма-производитель | Keri systems | Lenel  Lenel | Lyric (Apollo) | Грифон |
| Фирма-производитель |
| Максимальная длина магистрали до  контроллера | 1200 м | 1200 м | 1200 м | 100 м |
| Наличие временных зон | да | да | да | да |

Для исследуемого объекта относительно технических характеристик подойдет СКУД производства отечественной компании «Грифон», так как характеристики систем других производителей являются недостаточными.

Выбранная компании предлагает бесплатную техническую поддержку по телефону, а также обучение по своей продукции, чего нельзя сказать о других фирмах-производителей СКУД. Учебные центры компании-производителя расположены в Москве и в Санкт-Петербурге. Стоит отметить, что оборудование выбранной компании интегрируется с большим количеством систем контроля и управления доступа различных отечественных и зарубежных производителей.

Аппаратные и программные средства позволяют решить все задачи, поставленные перед системой контроля и управления доступом.

Учет рабочего времени и отчет по проходам через конкретную точку представляется в формате Excel, что позволяет упростить или автоматизировать обработку этих отчетов.

При помощи настраиваемых правил управления системой можно настроить аварийное открытие дверей при наступлении какого-либо события (пожар, тревога, нажатие аварийной кнопки).

Отдельными плюсами являются возможность в дальнейшем с легкостью масштабировать систему и возможность интеграции СКУД с пожарной и охранной системами.

Функциональные возможности у системы очень большие. Система может поддерживать управление от одной до нескольких десятков и даже сотен точек прохода. Каждый контроллер системы ориентирован на комплексную защиту одной области объекта (комнаты, этажа, другой замкнутой территории). Система ориентирована на использование в качестве ключей proximity карт типа StandProx или SlimProx и брелковMiniTag, с которыми работают собственные считыватели системы. Система может работать со считывателями TouchMemory (ключи типа I-Button), либо с любыми стандартными считывате- лями, имеющими выходной интерфейс Wiegand 26 bit или TouchMemory [12].

В качестве датчиков к контроллерам могут подключаться герконовые контакты, инфракрасные или комбинированные датчики либо другие датчики, имеющие «сухой контакт».

Контроллеры КОМ-СКД-01 поддерживают оборудование одной точки прохода.

Ниже приведены основные функциональные возможности контроллера:

− Максимальное количество пользователей 40960;

− Максимальное количество событий 24244;

− Поддержка функции «антипассбэк»;

− Встроенные часы реального времени;

− Количество считывателей 2;

− Типы поддерживаемых считывателей (протоколов) Wiegand26, TouchMemory, Cr-v95 (RS-485), ParsecRDR2.

Контроллеры КОМ-СКД-01 поставляются в металлическом корпусе с источником питания и местом для аккумулятора резервного питания.

На плате контроллера расположены несколько перемычек (джамперов) и переключателей. Правила установки перемычек и переключателей описаны далее в соответствующих разделах.

Контроллеры ориентированы на работу с адресными считывателями се- рии КОМ-ПК-03, считывателями Parsec PR-Axx, PR-Hxx, NR-Axx, NR-Hxx, с любыми считывателями синтерфейсом Wiegand – 26, со считывателями с ин- терфейсом TouchMemory.

Тип интерфейса считывателя определяется положением перемычек JP8, JP9. Конкретный тип считывателя определяется положением перемычек JP10, JP11.

С помощью контроллера обеспечивается управление практически любы- ми исполняющими устройствами за счет применения реле, имеющего с нормально замкнутые (NC) и нормально разомкнутые (NO) контакты, а также за счет реализации возможности программирования по времени срабатывания реле в широких пределах. На рисунке 2.5 изображена схема подключения считывателей к контроллеру. На рисунке 2.6 показана схема подключения замка к контроллеру.

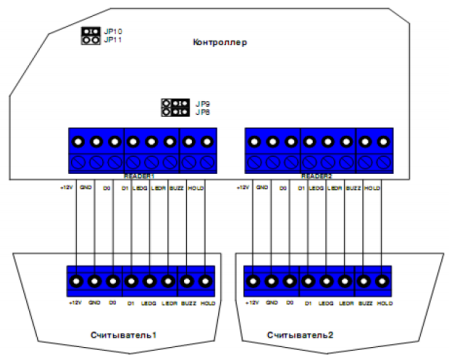


Рисунок 2.5 - Схема подключения считывателей к контроллеру

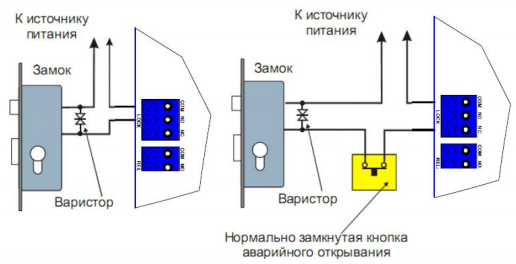


Рисунок 2.6 – Схема подключения замка к контроллеру

Для замков, управление которыми производится путем коммутации силовых обмоток электромагнитов, необходимо производить подавление выбросов по напряжению.

В контроллерах КОМ-СКД-01 используется раздельное управление открыванием турникета на вход и на выход (см. рисунок 2.7).

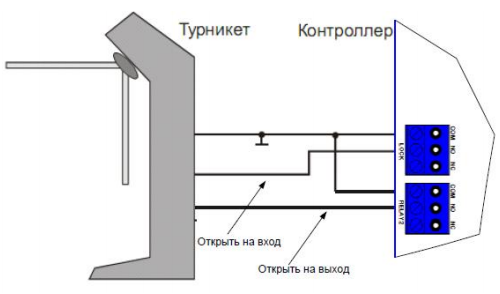


Рисунок 2.7 - Схема подключения турникета

3амковое реле контроллера открывает турникет на вход, а дополнительное реле – на выход турникет на вход, а дополнительное реле – на выход. Необходимо также корректно устанавливать время на управлении замками. Если турникет обладает собственной электроникой, обеспечивающей необходимое время по срабатыванию турникета, то время на замке устанавливается равным нулю (в таком случае значение реальной выдержки составит около 0,5 с) [13].

Для исключения возможности прохода через турникет двоих или более людей по одной карте, необходимо подключение к входам сенсоров S1 и S2 датчиков проворота турникета. В данном случае время замка будет сброшено после поворачивания турникета. Схема подключения датчиков поворота турникета к контроллерам показаны на рисунке 2.8.

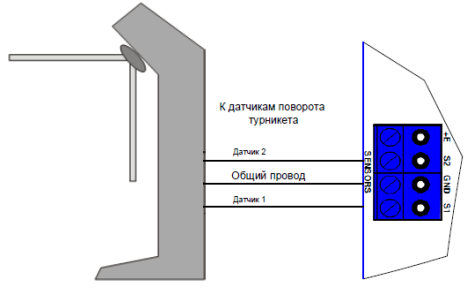


Рисунок 2.8 - Схема подключения датчиков поворота турникета к контроллерам

Аварийный вход (Emergency) используется для проведения аварийных открываний дверей, обслуживаемых контроллерами, например, при возникновении пожара. К указан- ному входу могут быть подключены выходы системы пожарной сигнализации, либо застекленная кнопка для аварийного открывания дверей. Аварийные входы имеют максимальную степень приоритета, поэтому двери будут открыты при подаче сигналов на данный вход даже в случаях, если дверной канал нахо- дится в состоянии блокировки.

Архитектура программного обеспечения СКУД строится на основе ряда механизмов, определяемых требованиями, предъявляемыми к системе.

Трактовка СКУД как системы реального времени требует реализации механизмов диспетчеризации, межобъектного взаимодействия и средств работы с таймерами. Параллелизм в обработке одновременно происходящих внешних событий должен обеспечивается за счет использования многопоточности. Клиент-серверный подход вносит необходимость реализации механизма и способов взаимодействия между сервером и приложениями, а общие требования безопасности и надежности заставляют выбирать особые способы хранения данных и работы с ними.

Некоторые архитектурные механизмы используют нестандартный подход к созданию объектов, требующий передачи строкового имени класса создаваемого объекта. Этот подход также может быть рассмотрен как вспомогательный механизм (или механизм более низкого уровня).

1. Диспетчер сообщений.

Для реализации механизма межобъектного взаимодействия был создан специальный объект – диспетчер. Диспетчер «знает» все объекты, которые желают обмениваться сообщениями, а эти объекты в свою очередь «знают» о существовании диспетчера. Помимо таблицы зарегистрированных объектов, важной частью диспетчера является очередь сообщений. Принцип отправки сообщения можно описать следующим образом (см. рисунок 3.2):

- Объект-отправитель создает сообщение и инициализирует его данными. Затем он вызывает функцию отправки сообщения (SendEvent) диспетчера.

- Диспетчер осуществляет постановку сообщения в очередь, проверяет, запущен ли поток обработки очереди сообщений. Если поток не запущен, то диспетчер его запускает. После этого управление возвращается объекту отправителю.

- Поток обработки сообщений извлекает следующее сообщение из очереди, ищет объект-получатель по таблице зарегистрированных объектов и вызывает функцию обработки сообщения получателя (ProcEvent), передавая ей в качестве параметра объект сообщение. Когда управление возвращается диспетчеру, поток осуществляет проверку наличия сообщений в очереди. Если сообщения отсутствуют, то поток завершается, в противном случае поток осуществляет обработку сообщения.

Перед вызовом функции ProcEvent получателя осуществляется запуск таймера. Если к моменту таймаута управление не возвращено объекту диспетчера, то поток прерывается и запускается снова со следующего элемента очереди сообщений. Если же получатель знает, что время обработки сообщения превышает время таймаута, то он запускает свой поток и возвращает управление диспетчеру.

Диаграмма деятельности, отражающая принцип обработки сообщения приведена на рисунке 2.9.

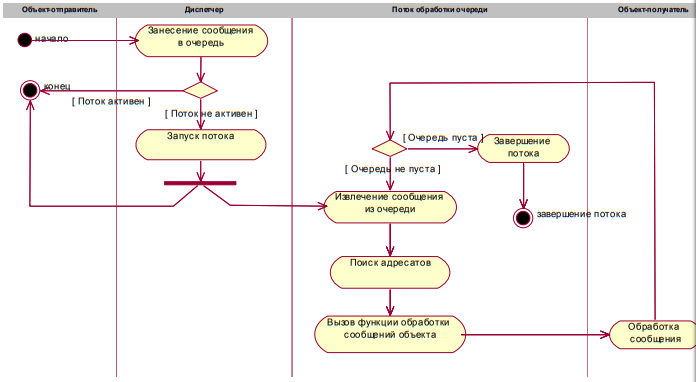


Рисунок 2.9 – Диаграмма деятельности, отражающая принцип обработки сообщения

Очередь сообщений диспетчера представляет собой массив элементов сообщений. Сообщения в очередь укладываются последовательно. При достижении конца очереди следующее сообщение записывается на первое место, таким образом, очередь зациклена. Обработка очереди потоком прекращается, когда номер следующего обрабатываемого элемента равен номеру следующего добавляемого элемента, что означает, что в очереди отсутствуют сообщения.

Выделение объекта диспетчера с его очередью сообщений разрешает все проблемы синхронизации многопоточного приложения, при условии, что взаимодействие объектов осуществляется только через очередь обработки сообщений диспетчера.

Каждый взаимодействующий объект в системе характеризуется тремя значениями: номером класса, номером объекта и дополнительным кодом. Для уникальной идентификации объекта используются первые два значения. Номера объектов выдаются диспетчером последовательно, с заполнением пустот (т.е. объект занимает первый свободный номер). Дополнительный код призван выражать пользовательскую нумерацию объектов. Кроме того, он может быть использован для поиска объектов в системе (Seek, Select).

Каждый взаимодействующий объект в системе характеризуется тремя значениями: номером класса, номером объекта и дополнительным кодом. Для уникальной идентификации объекта используются первые два значения. Номера объектов выдаются диспетчером последовательно, с заполнением пустот (т.е. объект занимает первый свободный номер). Дополнительный код призван выражать пользовательскую нумерацию объектов. Кроме того, он может быть использован для поиска объектов в системе (Seek, Select).

Проведенное тестирование показало, что диспетчер способен поддерживать неограниченное количество объектов. Единственным «узким» местом может выступить очередь сообщений: поскольку она зациклена, то ее переполнение может закончиться потерей ряда начальных сообщений.

2. Диспетчер событий.

Для реализации возможности подписки одних объектов на события других диспетчер сообщений был расширен функциями диспетчера событий. Это выразилось в добавлении таблицы подписчиков и функций работы с событиями. Объект, желающий заявить о событии, создает объект-сообщение и заполняет часть его полей, касающихся события. После этого осуществляется вызов функции уведомления о событии (ThrowEvent). Эта функция находит всех подписчиков, и отправляет им сообщения о событии, удаляя их подписные записи из таблицы. Если объект желает получить событие снова, он должен опять на него подписаться.

Объекты имеют возможность подписываться на события монопольно (для этого в объекте сообщения предусмотрен соответствующий атрибут). При возникновении события диспетчер определяет наличие монопольных подписок, и рассылает сообщения, уведомляя подписчиков, была ли заявлена монопольная подписка и является ли он монопольным подписчиком. В зависимости от этого объект принимает решение о соответствующей реакции на событие.

3. Сохранение объекта в файл.

Некоторые объекты системы требуют сохранения на диск и последующего восстановления. Для этого применяется механизм сериализации (преобразования объекта в последовательную форму и обратно). Принцип работы этого механизма следующий:

- При вызове функции сохранения в файл (Save) объект прежде всего записывает строку с именем своего класса. После этого происходит вызов функции сериализации (Serialize) с параметром «сохранить».

- В этой функции объект осуществляет запись на диск всех своих атрибутов. После этого объект считается сохраненным.

- При вызове функции загрузки объекта (Load) из файла считывается имя класса загружаемого объекта. Эта строка передается механизму параметризованного создания объектов, который осуществляет создание соответствующего объекта. После чего вызывается функция Serialize с параметром «загрузить».

- В функции Serialize происходит считывание из файла атрибутов сохраняемого объекта.

Таким образом, мы можем хранить в одном файле произвольное число объектов. Однако, чтобы получить доступ к какому-либо объекту, нам придется последовательно загрузить все предыдущие.

На рисунке 3.3 представлена диаграмма классов, отображающая структуру данного механизма.

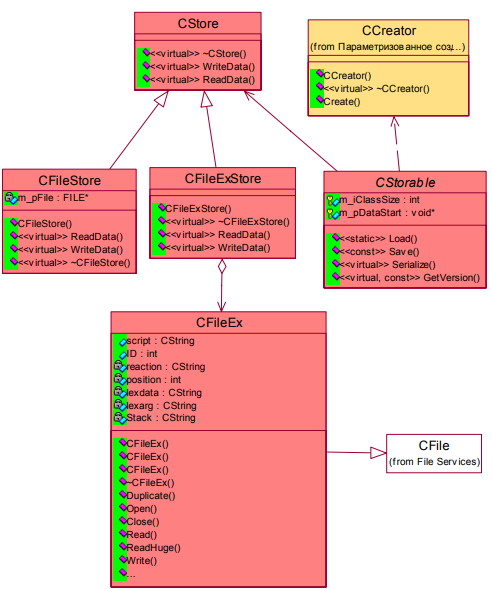


Рисунок 2.10 - Диаграмма классов механизма сериализации

Для использования этого механизма все классы, желающие, чтобы их объекты сохранялись, должны наследовать от класса, задающего интерфейс для сериализации (CStorable, модуль Storable.cpp(h)). Класс CStore задает интерфейс для использования различных типов файловых хранилищ. Например, класс CFileStore использует для работы с файлами функции API, а класс CFileExStore – функции класса CFileEx (реализация в модуле СStore.h). Кроме них могут быть использованы любые классы-обертки, обеспечивающие работу с файлами.

Этот механизм является полностью объектно-ориентированным, так как только сам объект знает порядок загрузки/сохранения своих атрибутов. Сериализация реализована и используется в стандартной библиотеке классов MFC. Однако MFC-реализация этого механизма может быть неприемлема в случаях, когда применяется множественное наследование или предполагается обеспечить кроссплатформенность приложений.

4. Параметризованное создание объектов.

Для параметризации создаваемого объекта именем класса использовался механизм, описанный в шаблоне проектирования «Абстрактная фабрика» (см. [12]). Применяемый подход также описан в [11].

Класс CAbstractFactory задает общий интерфейс для создания продукта (объекта) различными фабриками объектов. Класс CFactory инициализируется создаваемым продуктом и реализует интерфейс абстрактной фабрики. Класс CFactoryListItem представляет собой элемент списка фабрик. Класс CCreator осуществляет перебор списка фабрик для создания конкретного продукта, определенного переданным ему параметром. Диаграмма классов представлена на рисунке 2.11.

Все описанные классы реализованы в модуле dynamic.cpp(h).

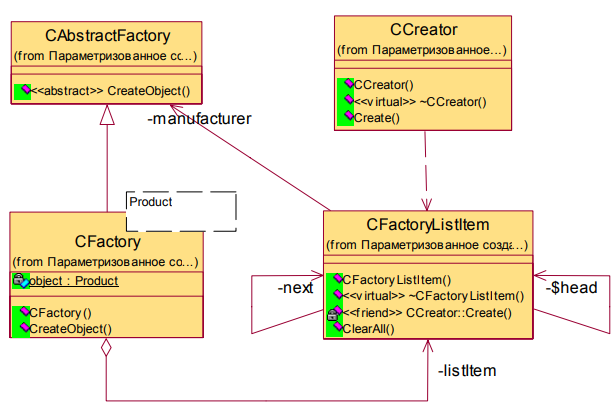


Рисунок 2.11 - Диаграмма классов механизма параметризованного создания объектов

5. Работа с файлами.

Необходимость обеспечения гибкой и надежной работы с файлами в механизмах сохранения объектов требует разработки специальной системы для обработки особых ситуаций – исключений. Они представляют собой некоторые события, которые прерывают нормальный процесс выполнения программы. Многие стандартные библиотеки учитывают возможность возникновения исключений, но обработкой их должен заниматься непосредственно разработчик.

Стандартная библиотека классов Microsoft (MFC) предоставляет особый класс для работы с файлами CFile, который умеет генерировать исключения при работе с файлами. Но, при его прямом использовании в коде программы, придется «защищать» операторами обработки исключения каждую файловую операцию, что приведет к непомерному росту объема программы. Это послужило стимулом для написания собственного класса работы с файлами, который является наследуемым от CFile и дополняет его специальными возможностями.

Помимо непосредственной защиты самих операций программисту - пользователю предоставлена возможность самому назначать функцию обработки для каждого файлового объекта или воспользоваться процедурой обработки по умолчанию. Для обеспечения более эффективного и гибкого управления исключениями был создан специальный язык. При возникновении исключения в режиме интерпретации будет выполняться специальная программа на этом языке - управляющий скрипт.

Разработанный язык позволяет однозначно сопоставить набору стимулов (причин исключения) последовательность действий, которые необходимо выполнить. Причем необходимые действия или последовательности действий могут повторяться любое число раз. Такая конструкция языка является вполне достаточной: количество стимулов конечно, и, сопоставив каждому стимулу последовательность действий, мы определим реакцию системы на все возможные файловые исключения для данного файлового объекта. Использование последовательности, а не единого действия, повышает гибкость языка за счет конструирования сложных действий на основе простых. Операция повторения позволяет строить сложные реакции на основе неоднократного выполнения блоков действий: например, ожидание освобождения файла при совместном его использовании и пр. Для стимулов, требующих одинаковой обработки, предусмотрена возможность сопоставления реакции их набору.

Используя вышеописанные принципы, была разработана схема для представления архитектуры приложения-сервера СКУД. На рисунке 2.12 отражены пакеты, определяющие функциональную группировку классов, и показаны зависимости между ними.

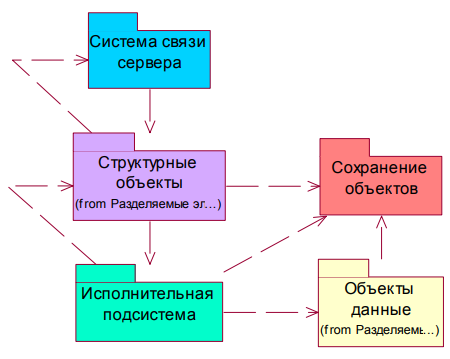


Рисунок 2.12 - Пакеты и связи приложения-сервера СКУД

«Система связи сервера» - пакет, отвечающий за связь клиентов и сервера, а также сервера и оборудования СКУД, такого как турникеты, датчики и т.д.. Он организует прием входящих сообщений и отправку исходящих. Входящие сообщения интерпретируются как события, их публикация осуществляется от лица структурных объектов.

Пакет «Структурные объекты» содержит объекты, являющиеся агентами внешних элементов системы: контроллеров, приложений-клиентов и других. Агенты используют систему связи для общения с внешним миром.

Пакет «Объекты-данные» осуществляет группировку ряда пакетов, представляющих такие элементы предметной области, как карты, счета, группы, ресурсы и персоны.

Пакет «Исполнительная подсистема» отвечает за выполнение запросов от приложений и обработку событий контроллеров. Он представляет собой адаптированную к системе реализацию механизма команд. Команды работают как с объектами-данными, так и со структурными объектами.

Пакет «Сохранение объектов» показывает, каким образом сервер использует механизмы сохранения объектов. Этот пакет используется командами, структурными объектами и объектами-данными.

Произведем разработку диаграммы классов подсистемы для проходной.

Основная задача подсистемы на проходной – проверка прав доступа и пропуск сотрудников на территорию предприятия. Для проверки используется отпечаток пальца сотрудника, который он прикладывает к считывателю отпечатка пальцев. Если отпечаток совпал с одним из отпечатков в базе данных, то сотрудник идентифицируется, и происходит проверка его прав доступа. Если проверка пройдена с положительным результатом, то сотрудник пропускается через турникет, в остальных случаях сотрудник не пропускается. Также в подсистеме присутствует функция ручного пропуска сотрудников, и функция пропуска сотрудников на транспортных средствах.

Use Case диаграмма подсистемы контроля для проходной представлена на рисунке 2.13.

Диаграмма классов подсистемы контроля для проходной представлена на рисунке 2.14.

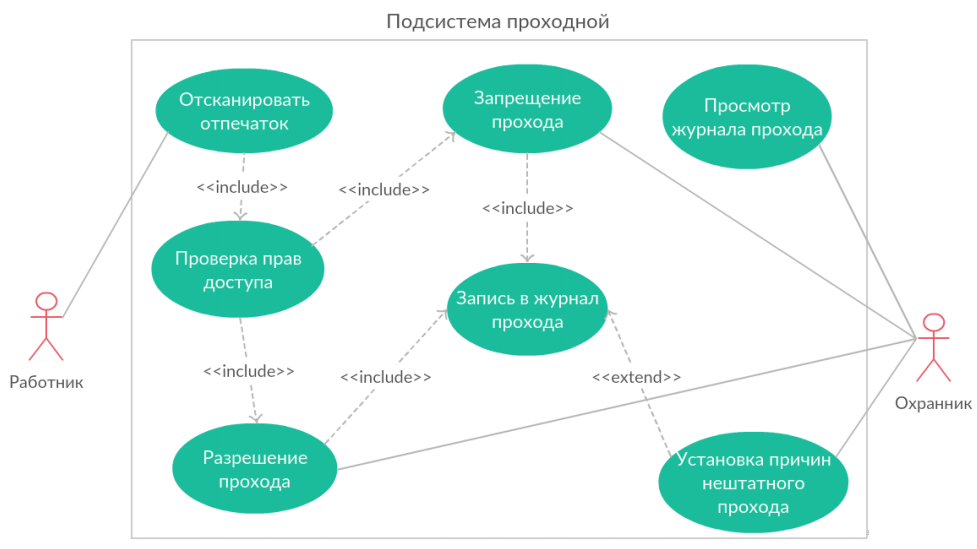


Рисунок 2.13 – Use Case диаграмма подсистемы контроля

Диаграмма классов подсистемы контроля приведена ниже.

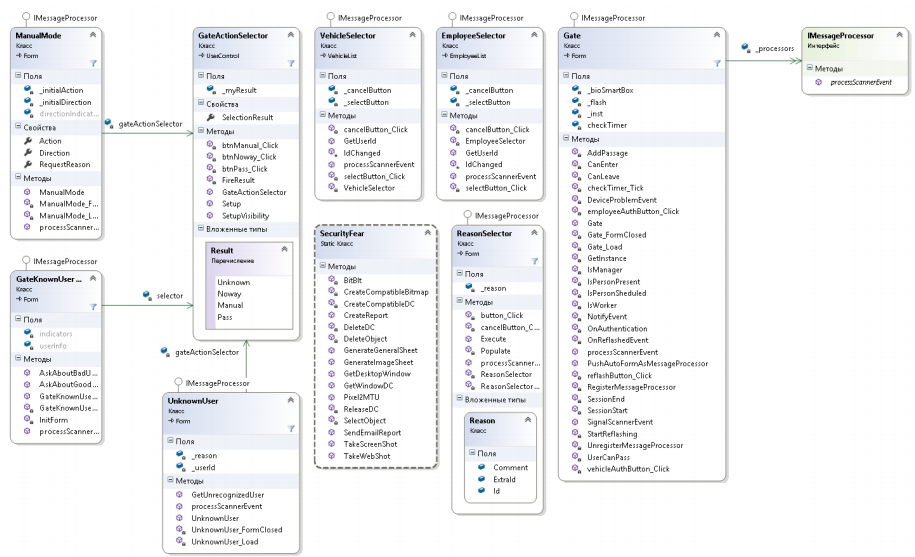


Рисунок 2.14 – Диаграмма классов подсистемы контроля

Класс Gate – основной класс подпрограммы, который взаимодействует со считывателем отпечатков пальцев, и передает ему решение о закрытии/открытии турникета, а также взаимодействует с БД, записывая туда информацию о проходе, и беря из нее данные об отпечатках пальцев и правах доступа.

Класс GateKnownUser – этот класс представляет сотрудника, который есть в БД. Из этого класса идет запрос о пропуске сотрудника в класс GetActionSelector.

Класс UnknownUser – этот класс представляет сотрудника, которого нет в базе данных. Из этого класса идет запрос о пропуске сотрудника в класс GetActionSelector.

Класс ManualMode – класс в котором происходит ручной контроль пропуском сотрудников. Из этого класса идет запрос о пропуске сотрудника в класс GetActionSelector.

Класс GetActionSelector – в этом классе происходит проверка прав доступа и решение о пропуске сотрудника, передающееся по цепочке классу Gate.

Класс EmployeeSelector – форма, в которой выбирается сотрудник при ручном пропуске.

Класс ReasonSelector – форма, в которой выбирается причина нештатного прохода сотрудника.

# 2.3 Внедрение модернизированной системы СКУД на объекте

Рассмотрим работу СКУД.

Структура приоритетности защищаемых зон:

1. Высший приоритет: основное помещение терминала аэропорта, залы ожидания.

2. Средний приоритет: технические помещения персонала.

3. Низший приоритет: пропускные пункты.

Сотрудники аэропорта проходят вход, поднося для этого постоянную карту пропуска к устройству считывания карт, которое расположено на турникете. Факты идентификации личности проходящих сотрудников компании фиксируются на АРМ системы контроля и управления доступом (происходит единовременная регистрация времени идентификации и Ф.И.О. проходящего сотрудника).

СКУД имеет возможность к дальнейшему расширению через установку дополнительных считывателей.

Система имеет следующие функциональные возможности:

* регистрация и протоколирование текущих событий и событий повышенной опасности;
* приоритетное фиксирование тревожных событий;
* организация управления работой преграждающими механизмами в по командам дежурного с поста охраны;
* возможность задать временные режимы действия идентификаторов;
* защита технических и программных средств от несанкционированного доступа;
* автоматизированный контроль работоспособности составных средств, входящих в СКУД, а так же линий передачи данных;
* установка режима свободного доступа с пункта охраны в случае аварийных ситуаций и чрезвычайных происшествий;
* блокирование прохода точек доступа командами с пункта охраны.

Система контроля доступа строится на базе аппаратно-программного комплекса (АПК) «Грифон» российского производства и интегрированной в АПК профессиональной системе контроля доступа. Техническая реализация СКУД основана на использовании головного сетевого контроллера системы. На каждой точке прохода устанавливаются контроллеры, комбинированные считыватели и сканеры штрих кода GFS4100 на КПП устанавливаются всепогодные сканеры штрихкода ID-22. Точки прохода на КПП оборудуются турникетами. Для сокращения времени контроля проезда транспорта КПП оборудуются переносными терминалами RM - 03 (Prоximity + Штрих-код), базовый радио модуль переносного терминала, выносится на улицу со стороны зоны досмотра транспортных средств. Получение сигнала от исполнительных устройств на контроллер осуществляется по интерфейсу Wiegand, связь контроллера с сервером оборудования и базы данных АПК, находящимся на 2 этаже в кроссовой здания КСС аэропорта, осуществляется через Ethernet модуль Elsys-IP по локальной сети аэропорта.

Производится замена шлагбаумов на КПП дополнительно устанавливаются фотоэлементы для предотвращения закрытия шлагбаума во время прохождения под ним транспортных средств. КПП оборудуется Автоматизированным рабочим местом (АРМ) для администрирования управления и мониторинга интегрированной системы контроля доступа. В ходе выполнения выпускной квалификационной работы разработано руководство пользователя СКУД. Документ «Руководство пользователя СКУД» относится к эксплуатационной документации.

Основная функция руководства пользователя заключается в обеспечении пользователя СКУД необходимой информацией для самостоятельной работы с разработанной системой. Таким образом, «Руководство пользователя СКУД» должно отвечать на следующие вопросы: что это за система, что она может, что необходимо для обеспечения ее корректного функционирования и что делать в случае отказа системы.

Руководящим стандартом для создания документа «Руководство пользователя СКУД» является ГОСТ 19.505-79 «Руководство оператора. Требования к содержанию и оформлению». Разработанный документ приведен в приложении 1.

# Выводы по второй главе

Вторая глава выпускной квалификационной работы посвящена разработке проектного решения по модернизации системы контроля и управления доступом аэропорта.

В данной главе разработана структура модернизированной СКУД и алгоритм функционирования.

Произведен выбор оборудования и программного обеспечения СКУД, необходимого для модернизации. Для исследуемого объекта относительно технических характеристик подойдет СКУД производства отечественной компании «Грифон», так как характеристики систем других производителей являются недостаточными. Поэтому решено использовать именно эту систему.

Так же даны рекомендации по внедрению модернизированной системы СКУД на объекте и разработано руководство пользователя СКУД.

# 3 Показатели продолжительности проекта модернизации

# 

# 3.1 Расчет трудоемкости и продолжительности разработки проекта

Определим этапы выполнения проекта, оценим трудоемкость и длительность работы. Результаты представлены в таблице 3.1

Таблица 3.1 – Трудоемкость и продолжительность работ по проекту

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование этапов раз­работки | Исполнители (должность) | Трудоёмкость, час | Продолжительность, дней |
| 1. Подготовительный этап |  |  |  |
| 1.1 Предварительный ос­мотр объекта | Специалист по ЗИ | 16 | 2 |
| 1.2 Анализ и ранжирование по степени важности защищаемой ин­формации | Специалист по ЗИ | 44 | 8 |
| 1.3 Изучение планов поме­щений, схем технических коммуникаций, связи, орга­низации охраны, доступа и других документов | Специалист по ЗИ,  руководитель про­екта | 36 | 9 |
| 1.4 Оформление результа­тов, полученных при прове­дении осмотра помещений и объектов | Специалист по ЗИ,  руководитель про­екта | 16 | 2 |
| Итого |  | 112 | 14 |

Продолжение таблицы 3.1

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование этапов раз­работки | Исполнители (должность) | Трудоёмкость, час | Продолжительность, дней |
| 2. Основной этап |  |  |  |
| 2.1 Монтаж оборудования | Специалист по ЗИ | 8 | 1 |
| 2.2 Проведение измерений | Специалист по ЗИ,  руководитель про­екта | 8 | 1 |
| 2.3 Разработка архитектуры СКУД | Специалист по ЗИ | 8 | 1 |
| 2.4 Формирование списка необходимых технических средств СКУД | Специалист по ЗИ,  руководитель проекта | 16 | 2 |
| Итого |  | 40 | 5 |
| 3. Закупка необходимых технических средств ЗИ |  |  |  |
| 3.1 Анализ рынка, поиск оптимальных поставщиков | Специалист по ЗИ | 24 | 3 |
| 3.2 Покупка оборудования | Специалист по ЗИ,  руководитель про­екта | 8 | 1 |
| Итого |  | 32 | 4 |
| 4. Заключительный этап |  |  |  |
| 4.1 Коммутация оборудования | Специалист по ЗИ | 8 | 1 |

Окончание таблицы 3.1

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование этапов раз­работки | Исполнители (должность) | Трудоёмкость, час | Продолжительность, дней |
| 4.2 Пуско-наладочные работы, проверка функционирования СКУД | Специалист по ЗИ  руководитель про­екта | 24 | 3 |
| 4.3 Экономическое обосно­вание работы | Специалист по ЗИ | 16 | 2 |
| 4.4 Составление проекта | Специалист по ЗИ  руководитель про­екта | 80 | 10 |
| Итого |  | 40 | 5 |
| Всего |  | 224 | 28 |

Из таблицы 3.1 видно, что на разработку проекта и планирование его внедрения потребуется 28 дней.

**3.2. Составление календарного плана выполнения работ**

Календарный план обеспечивает возможность контроля над ходом выполнения работ и его регулирования на всех этапах работ.

План выполнения работ по данному проекту составлен в виде таблицы (таблица 3.2).

Таблица 3.2 – Календарный план разработки и реализации проекта

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование этапов | Период выполнения | | Продолжитель-  ность этапов, дн. |
| дата начала | дата окончания |
| 1. Подготовительный этап | 16.04.2020 | 03.05.2020 | 14 |
| 2. Этап проектирования | 04.04.2020 | 07.05.2020 | 5 |
| 3. Основной этап проведения работ | 09.04.2020 | 12.05.2020 | 4 |
| 4. Заключительный этап | 13.04.2020 | 17.05.2020 | 5 |
| Итого |  |  | 28 |

По итогам таблицы 3.2 дата окончания выполнения проекта 17 мая 2020 года.

Календарный план не учитывает выходные и праздничные дни в году. Поэтому следует предположить, что продолжительность разработки проекта увеличится.

# Выводы по третьей главе

Третья глава работы посвящена расчету показателей продолжительности проекта модернизации.

В данной главе произведен расчет трудоемкости и продолжительности разработки проекта модернизации СКУД.

Так же составлен календарный план выполнения работ. На разработку проекта и планирование его внедрения потребуется 28 дней. Окончание выполнения проекта – 17 мая 2020 года.

Календарный план не учитывает выходные и праздничные дни в году. Поэтому следует предположить, что продолжительность разработки проекта увеличится.

# 4 Безопасность и экологичность проекта

# 4.1 Разработка рекомендаций по обеспечению охраны труда в процессе реализации проекта

Изучение и решение проблем, связанных с обеспечением здоровых и безопасных условий, в которых протекает труд человека - одна из наиболее важных задач в разработке новых технологий и систем проектирования. Изучение и выявление возможных причин производственных несчастных случаев, профессиональных заболеваний, аварий, взрывов, пожаров, и разработка мероприятий и требований, направленных на устранение этих причин позволяют создать безопасные и благоприятные условия для труда человека.

Работа оператора СКУД непосредственно связана компьютером, а соответственно с дополнительным вредным воздействием целой группы факторов, что существенно снижает производительность их труда. К таким факторам можно отнести:

1) воздействие вредных излучений от монитора;

2) неправильная освещенность;

3) не нормированный уровень шума;

4) нарушение микроклимата;

5) наличие напряжения и др.

Проанализируем некоторые факторы, влияющие на условия труда системного администратора сети.

Визуальные эргономические параметры монитора являются параметрами безопасности, и их неправильный выбор приводит к ухудшению здоровья пользователя. Все мониторы должны иметь гигиенический сертификат, включающий в том числе оценку визуальных параметров.

Конструкция монитора должна обеспечивать возможность фронтального наблюдения экрана путем поворота корпуса в горизонтальной плоскости вокруг вертикальной оси в пределах плюс-минус 30 градусов и в вертикальной плоскости вокруг горизонтальной оси в пределах плюс-минус 30 градусов с фиксацией в заданном положении.

Для обеспечения надежности считывания информации при соответствующей степени комфортности ее восприятия должны быть определены оптимальные и допустимые диапазоны визуальных эргономических параметров.

При проектировании и разработке рабочего места сочетания визуальных эргономических параметров мониторов и их значения, соответствующие оптимальным и допустимым диапазонам, полученные в результате испытаний в специализированных лабораториях, аккредитованных в установленном порядке, и подтвержденные соответствующими протоколами, должны быть внесены в техническую документацию на монитор.

Так же, конструкция монитора и ПЭВМ должна обеспечивать мощность экспозиционной дозы рентгеновского излучения в любой точке на расстоянии 0,05 м от экрана и корпуса монитора при любых положениях регулировочных устройств, которая не должна превышать 7,7·10 А/кг, что соответствует эквивалентной дозе, равной 0,1 мБэр/час (100 мкР/час).

Источниками шума на рабочих местах являются сами вычислительные машины (встроенные в стойки ЭВМ вентиляторы, принтеры и т.д.), центральная система вентиляции и кондиционирования воздуха.

В рабочем помещении предприятия уровень шума на рабочих местах не превышает значений, установленных для данных видов работ Санитарными нормами допустимых уровней шума на рабочих местах, и составляет примерно 30 дБА.

В помещении, где работает инженерно-технический персонал, осуществляющий аналитический или измерительный контроль, уровень шума не превышает 60 дБА, что так же соответствует нормативным документам.

На рабочих местах в помещениях, где размещены шумные агрегаты вычислительных машин (факсы, принтеры и т.п.), уровень шума согласно СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» не должен превышать 75 дБА. После анализа уровня шума в данных помещениях получен уровень в 45 дБА. Данное значение удовлетворяет СанПиН 2.2.2/2.4.1340-03.

Шумящее оборудование, уровни шума которого превышают нормированные, согласно нормативной безе, должно находиться вне помещения, в котором организуются рабочие места. Однако такого рода помещения на предприятии отсутствуют.

Согласно СанПиН 2.2.2/2.4.1340-03, под метеорологическим условиям производственной среды понимают сочетания температуры, относительной влажности, скорости движения и запыленности воздуха. Температура воздуха является одним из основных параметров, характеризующих тепловое состояние микроклимата. Скорость движения воздуха - это вектор усредненной скорости перемещения воздушных потоков под действием различных побуждающих сил.

Для характеристики содержания влаги в воздухе используют понятия - абсолютная, максимальная и относительная влажность.

Параметры микроклимата на рабочем месте приведены в таблице 4.1.

При пониженном давлении воздуха ухудшается отвод тепла от элементов ПЭВМ. Рекомендуется создавать небольшое избыточное атмосферное давление, препятствующее подносу пыли.

|  |  |  |  |
| --- | --- | --- | --- |
| Категория работ | Энергозатраты, Вт | Периоды года, температура (°C) | |
| холодный | теплый |
| легкая | до 139 | 22-24 | 23-35 |
| средней тяжести | 175-232 | 18-20 | 21-23 |
| тяжелая | более 290 | 16-18 | 18-20 |

Таблица 4.1 - Параметры микроклимата на рабочем месте

Для обеспечения установленных норм в рабочем помещении применяют вентиляцию, что позволяет также обеспечить чистоту воздуха. Система вентиляции выполняется в соответствии с требованиями СНиП 41-01-2013 «Отопление, вентиляция и кондиционирование».

Проведённый анализ системы вентиляция позволяет утверждать, что имеющаяся вентиляция соответствует СНиП 41-01-2013.

# 4.2 Защита сотрудников в чрезвычайных ситуациях

В настоящее время основными способами защиты сотрудников в чрезвычайной ситуации являются:

- укрытие в защитных сооружениях;

- проведение эвакуационных мероприятий;

- использование средств индивидуальной защиты.

Учитывая, что в условиях ЧС сроки проведения защитных мероприятий могут оказаться крайне ограниченными, необходимо средства защиты готовить заранее, а способы их применения отрабатывать постоянно.

Правильное и целесообразное применение способов защиты обеспечивается своевременным оповещением об опасности и созданием необходимых запасов материальных средств для проведения мероприятий защиты.

Важное место среди перечисленных мероприятий занимает оповещение. Оповестить сотрудников значит предупредить их о надвигающейся ЧС, передать информацию о случившейся аварии или катастрофе. Для этого используются все средства проводной, радио и телевизионной связи.

# 4.3 Экологичность проекта

При создании разрабатываемого проекта негативных воздействий на экологию и окружающую среду осуществлено не будет.

Имеются вторичные отходные материалы, такие как использованная бумага, кабели и так далее, которые утилизируются в соответствии с установленными нормами специализированными организациями. Поэтому разрабатываемая система является экологически безвредной.

# Выводы по четвертой главе

Данная глава выпускной квалификационной работы посвящена исследованию вопросов организации безопасности и экологичности проекта.

В данной главе разработка рекомендаций по обеспечению охраны труда в процессе реализации проекта.

Разработаны рекомендации по защите сотрудников в чрезвычайных ситуациях.

Так же проанализирован вопрос экологической безопасности проекта. Выявлено, что при создании разрабатываемого проекта негативных воздействий на экологию и окружающую среду осуществлено не будет.

# Заключение

Современные атаки, как правило, превосходят обороноспособность защищающихся. До тех пор пока, стоимость и сложность эксплуатации автоматизированных электронных охранных систем будет непомерно великой.

Ведутся активные разработки и прочие меры оптимизации, охранных систем, что позволяет эксплуатировать их даже в домашних условиях, не прибегая к постоянному сопровождению, производимому рядом высококвалифицированных специалистов. Что касается автоматизированных охранных комплексов, ситуация в данной сфере неуклонно улучшается, так как актуальность и экономическая пригодность подобных систем, не вызывает сомнений. Специалисты постоянно стремятся к простой пропорции, при которой эффективность охранной системы, выше экономических затрат.

Автоматизированные системы контроля и управления доступом - совокупность средств контроля и управления, обладающих технической, информационной, программной и эксплуатационной совместимостью. АСКУД решают задачи обеспечения безопасности любого уровня, осуществляют предупреждение о проникновении посторонних лиц на подконтрольную территорию, а также способствуют повышению дисциплины труда благодаря учету рабочего времени сотрудников компании. Сегодня системы контроля и управления доступом являются неотъемлемой частью системы безопасности любой компании.

По завершению выполнения работы получены следующие результаты:

– дана общая характеристика аэропорта, его информационной и физической структуре;

– произведен анализ существующей системы контроля и управления доступом на базе аэропорта;

– выявлены недостатки существующей системы и обосновать необходимость модернизации;

– разработана структура модернизированной СКУД и алгоритм ее функционирования;

– произведен выбор оборудования и программного обеспечения СКУД, необходимого для модернизации;

– разработан проект внедрения модернизированной системы СКУД на объекте;

– разработаны рекомендации по обеспечению охраны труда в процессе реализации проект и защите сотрудников в чрезвычайных ситуациях.

Рассмотрен рынок АСКУД в России, который представлен многими производителями, отечественная продукция которых как минимум не уступает иностранной. В результате анализа выбрана АСКУД производства компании «Грифон». Выбранная система является оптимальной с точки зрения отношения цена/качество. Сформированы практические рекомендации по построению автоматизированной системы контроля и управления доступом на рассматриваемом объекте.

По завершению работы необходимо отметить, что все поставленные задачи выполнены, цель работы достигнута.

# Список используемых источников

1. Афонин В.Л. Интеллектуальные робототехнические системы.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 222 c.
2. Барский А.Г. Оптико-электронные следящие и прицельные системы.— М.: Логос, 2013.— 248 c.
3. Беляев П.С. Системы управления технологическими процессами.— Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2014.— 156 c.
4. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. - М.: Горячая линия - Телеком, 2016. - 272 с.
5. Гаврилов А.Н. Теория автоматического управления технологическими объектами (линейные системы). — Воронеж: Воронежский государственный университет инженерных технологий, 2016.— 244 c.
6. Горелов Г.В. Системы связи с подвижными объектами.— М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014.— 336 c.
7. Греков Э.Л. Исследование системы автоматического управления электроприводом постоянного тока.— Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2017.— 108 c.
8. Дворкович В.П. Цифровые видеоинформационные системы (теория и практика).— М.: Техносфера, 2012.— 1008 c.
9. Денисова Е.В. Автономные информационные системы обнаружения скрытых объектов.— Новосибирск: Новосибирский государственный технический университет, 2012.— 128 c.
10. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 2-e изд. — М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. — 392 с.
11. Кочетков М.В. Системы охраны.— Саратов: Вузовское образование, 2015.— 99 c.
12. Ловцов Д.А. Геоинформационные системы.— М.: Российский государственный университет правосудия, 2012.— 192 c.
13. Лубенцова Е.В. Системы управления с динамическим выбором структуры, нечеткой логикой и нейросетевыми моделями.— Ставрополь: Северо-Кавказский федеральный университет, 2014.— 248 c.
14. Музылева И.В. Компьютерное исследование линейных систем автоматического управления. Часть 3. Простейшие системы автоматического управления. Устойчивость линейных систем.— Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2014.— 81 c.
15. Рыбак Л.А. Теория автоматического управления. Часть I. Непрерывные системы.— Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2012.— 121 c.
16. Рыбак Л.А. Теория автоматического управления. Часть II. Дискретные системы.— Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2012.— 65 c.
17. Сазонова С.А. Автоматизированные системы управления и связь.— Воронеж: Воронежский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 172 c.
18. Удовикин В.Л. Системы и сети связи с подвижными объектами.— Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2012.— 80 c.
19. Кандино Э. Электронные системы охраны.— Саратов: Профобразование, 2017.— 256 c.
20. Яковлева Н.В. Информационно-управляющие системы. Решение задач управления.— Чебоксары: Чебоксарский политехнический институт (филиал) Московского государственного открытого университета им. В.С. Черномырдина, 2011.— 125 c.