

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет
вычислительной техники

Кафедра
«Вычислительная техника»

Направление подготовки: 09.04.01 «Информатика и вычислительная техника»

Магистерская программа: «Вычислительные машины, комплексы, системы и сети»

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
МАГИСТРА**

на тему

**АЛГОРИТМЫ КОМПЛЕКСНОЙ ИДЕНТИФИКАЦИИ
АВТОТРАНСПОРТНЫХ СРЕДСТВ ДЛЯ СИСТЕМЫ
КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ**

Студент


(подпись, дата)

Янович Илья Владимирович

Руководитель


(подпись, дата)

А.В. Дубравин

Нормоконтролёр


(подпись, дата)

А.В. Кучин

Рецензент

доцент Пенз ГТУ
(должность, место работы)

 05.06.20
(подпись, дата)

Петерский С.В.
(фамилия, инициалы)

Работа допущена к защите (протокол зас. кафедры от 03.06.2020 № 12)

Заведующий кафедрой


(подпись)

М.А. Митрохин

Работа защищена с отметкой

отлично

(протокол заседания ГЭК от 15.06.20 № 5)

Секретарь ГЭК


(подпись)

Е.И. Гурин

Пенза 2020

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет
вычислительной техники

Кафедра
«Вычислительная техника»

«Утверждаю»
Заведующий кафедрой
 М.А. Митрохин
«05» ноября 2019 г.

**ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ
МАГИСТРА**

1. Студент Янович Илья Владимирович гр. 18ВВм1 факультета вычислительной техники.

2. Тема работы: «Алгоритмы комплексной идентификации автотранспортных средств для системы контроля и управления доступом».

Тема утверждена приказом ПГУ № 1210а/о от 05.11.2019 г.

3. Руководитель работы к.т.н., доцент каф. ВТ ПГУ Дубравин А.В.

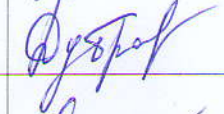
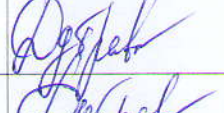
4. Задание на работу (назначение разработки, исходные данные и т.п.).

Назначение разработки – система предназначена для контроля и управления доступом автотранспорта на территорию охраняемого объекта работниками и посетителями. Система должна предусматривать возможность управления шлагбаумами, светофором и принимать сигналы с датчика движения.

5. Перечень подлежащих разработке вопросов.

Требуется произвести анализ предметной области и актуальных технологий, предлагаемых на рынке, выбрать функциональный состав системы и осуществить выбор элементной базы, разработать структурную схему системы, разработать алгоритм работы системы.

6. Календарный график выполнения работы

№ п/п	Наименование этапов работы	Объем работы	Срок выполнения	Подпись руководителя
1.	Анализ предметной области	10	23.01.2019	
2.	Определение функционального состава системы	10	14.02.2019	
3.	Составление структурной схемы системы	10	16.04.2019	
4.	Составление алгоритма работы системы	20	10.05.2019	
5.	Моделирование и поиск уязвимостей, исправление ошибок в работе системы	20	21.05.2019	
6.	Оформление выпускной работы	30	05.06.2019	

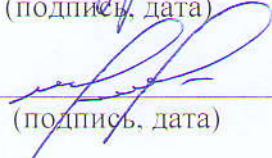
Дата выдачи задания "31" октября 2019г.

Руководитель магистерской диссертации


(подпись, дата)

А.В. Дубравин

Задание к исполнению принял студент


(подпись, дата)

И.В. Янович

Работу к защите допустить

Декан факультета


(подпись, дата)

Л.Р. Фионова

РЕФЕРАТ

Пояснительная записка содержит 60 листов, 24 рисунка, 14 источников, 1 приложение.

СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ, RFID-ТЕХНОЛОГИИ, ВИДЕОИДЕНТИФИКАЦИЯ, МИКРОКОНТРОЛЛЕР, АЛГОРИТМ РАБОТЫ, ВИДЕОФИКСАЦИЯ.

Цель работы – разработать систему контроля и управления доступом автотранспорта на закрытые предприятия и объекты.

Объектом разработки является алгоритм, обеспечивающий в полной мере контроль доступа на территорию, обработку данных, поступающих с видеокамеры и считывателя, в том числе в контроллере должен присутствовать алгоритм принятия решения об открытии шлагбаума. Необходимо провести анализ возможности реализации системы контроля и управления доступом, базирующейся на технологиях распределенных баз данных и топологии mesh-сетей, оценить преимущества работы такой системы в сравнении с централизованной системой контроля и управления доступом, произвести испытания на предмет безопасности и отказоустойчивости системы, предусмотреть возможность удаленного управления системой.

В рамках проведенной работы был создан алгоритм работы системы, удовлетворяющий поставленной задаче.

Разработанная система за счет внедрения технологий создания зон сплошного информационного покрытия отвечает поставленным требованиям о масштабируемости системы, расширяет возможности удаленного управления и контроля. Описанная в работе система может быть внедрена на различных предприятиях, где требуется автоматизированный контроль за лицами, имеющих право доступа на территорию объекта или предприятия, или необходима регистрация и контроль над автомобильными транспортом нахождения их на территории и время пребывания.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	4
1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ	6
1.1 СКУД автотранспорта	6
1.2 Основное предназначение СКУД.....	8
1.3 Типовые сферы применения	8
1.4 Основные функции системы.....	9
1.5 RFID-технология в автомобильных СКУД	10
1.6 Принцип работы RFID-технологии.....	12
1.7 Диапазон частот	14
1.8 Особые требования к автомобильным RFID-системам	15
1.9 Примеры RFID-систем	16
1.10 Интеграция в автомобильных RFID-системах.....	18
1.11 Сетевые системы контроля и управления доступом.....	19
1.12 Известные технологии машинной обработки потокового видео...	22
1.13 Соответствие разрабатываемой системы требованиям ГОСТ	23
1.14 Выводы по разделу 1	27
2 СОСТАВ И СТРУКТУРА КОМПЛЕКСА СКУД С ВИДЕОФИКСАЦИЕЙ.....	28
2.1 Основные компоненты СКУД с видеофиксацией.....	29
2.2 Устройства контроля и управления доступом	30
2.3 Устройства центрального управления.....	36
2.4 Устройства исполнительные.....	37
2.5 Структура комплекса СКУД.....	40
2.6 Выводы по разделу 2	43
3 РАЗРАБОТКА АЛГОРИТМА.....	44
3.1 Принцип работы СКУД с видеофиксацией.....	44
3.2 Считывание автомобильного номера.....	47
3.3 Выводы к разделу 3.....	54
4 ЗАКЛЮЧЕНИЕ	56
СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ	57
Приложение А Презентация	59

ВВЕДЕНИЕ

Система контроля и управления доступом (СКУД) – это программные и технические средства, а также их совокупность, организационно-методические мероприятия, решающие задачи контроля и управления посещением охраняемого объекта.

СКУД решает такие задачи, как оперативный контроль местонахождения персонала и их автотранспорта, время нахождения персонала на объекте, а также зачастую на предприятиях СКУД интегрируется с системой охранно-пожарной сигнализации для комплексного решения задач безопасности. Тем самым можно обеспечить реакции охранной на попытки несанкционированного доступа, проникновения и т.п. Возможность автоматической постановки/снятия с охраны помещений по факту прохода в зону доступа сотрудника; предоставление свободного выхода/выезда в случае возникновения пожара.

При реализации конкретных СКУД используют различные способы и устройства для идентификации и аутентификации личности. Следует отметить, что СКУД являются одним из наиболее развитых сегментов рынка безопасности как в России, так и за рубежом. Число специалистов, работающих в сфере технических систем безопасности, превысило 650 тыс. человек. Это связано с тем, что, во-первых, постепенно повышается информированность рынка, т.е. востребованность новых возможностей, функций и сервисов, которые не могли быть реализованы в рамках более старых классических систем безопасности. Во-вторых, на повышение рыночной динамики значительно влияют такие факторы, как антитеррористическая защищенность, так и рост общего уровня культуры потребителей.

СКУД на данный момент времени большинством пользователей воспринимается как важная составная часть системы безопасности предприятия. Значительную роль в достижении такого результата сыграла и продолжает играть именно информированность конечных потребителей. С ростом информированности закономерно повышается уровень требований к СКУД. На объектах, где требуется обеспечить повышенный уровень безопасности, стали использоваться системы биометрической, в том числе и многофакторной - по комбинации биометрических признаков и пароля или карты доступа. В других организациях, предприятиях, учебных заведениях и т.д. используются турникеты с бесконтактными картами доступа; шлагбаумы с пультом доступа или видеофиксацией.

Современные проблемы требуют современных решений. В настоящей работе будет решаться серьезный вопрос – как выгодно с точки зрения финансирования и эффективно с технической организовать контроль доступа на различные объекты. В настоящее время рынок предлагает множество готовых решений для контроля и управления доступом, но учитывая то, что все они в скором времени безнадежно устареют, поэтому вопрос создания систем контроля и управления доступом (СКУД) является приоритетным, актуальным и интересным.

Система, разрабатываемая в рамках магистерской диссертации, хорошо изучена и имеет множество примеров и способов реализации. Следовательно, разработку описываемой СКУД необходимо начать с анализа предметной области, что позволит на раннем этапе найти слабые и сильные стороны существующих разработок для создания функционального решения. В ходе анализа считаю необходимым произвести обзор как новейших технологий в сфере построения проводных и беспроводных сетей, так и технологий считывания информации с различных носителей.

1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

1.1 СКУД автотранспорта

Система представляет аппаратно-программный комплекс, с помощью которого решается задача организации автоматического или автоматизированного проезда на подконтрольную территорию и учета перемещения транспорта. Основная задача — это управление доступом автотранспорта на территорию предприятия или закрытого охраняемого объекта с учетом данных о водителе, машине, времени посещения и т.д., что в последующем учитывается в базе данных организации.

Система контроля и управления доступом автотранспорта может входить в общую СКУД или действовать независимо. Назначением системы является учет и контроль доступа автотранспорта на территорию объекта, мониторинг его пребывания и перемещения по территории. Это особенно важно для предприятий, доступ к которым проходит через проходную (турникет и др.), и въезд для машин, где не проходят стандартную систему контроля.

При построении поискового запроса в интернете для поиска готовых решений для организации автомобильного КПП можно использовать слова «КПП», «автотранспорт», «СКУД». По данным ресурса wordstat.yandex.ru [7] – СКУД автотранспорта является не самым популярным запросом, так как организации, которые могли бы заказать услугу по установке и обслуживанию подобной системы скорее объявила бы тендер на поиск подрядчика. Данные запросов приведены на рисунках 1 и 2. В таком случае для прохождения условий конкурса необходима сертификация продукта и прохождение требований действующего стандарта.

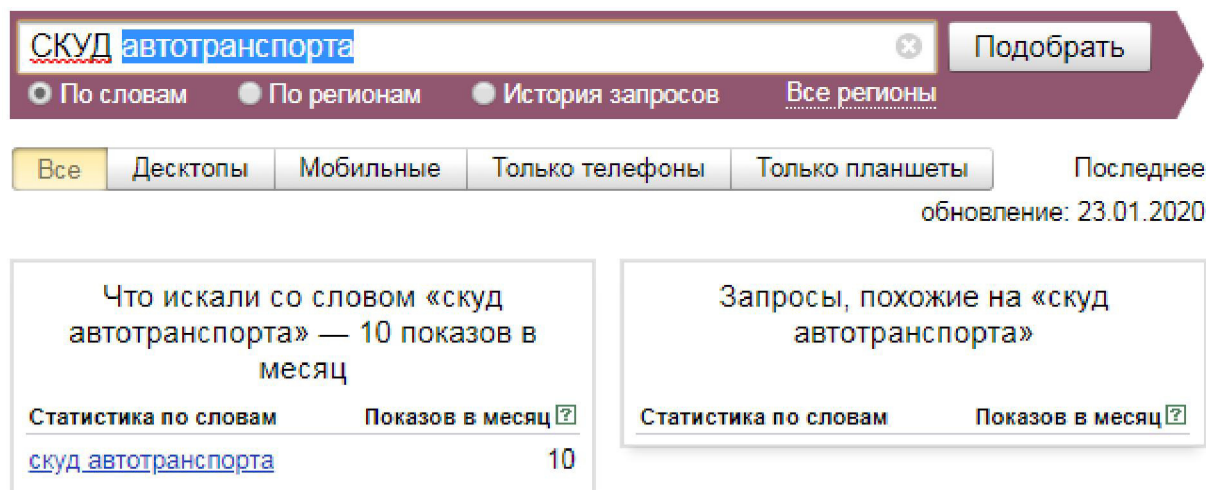


Рисунок 1. Данные wordstat

Дальнейшее исследование привело к выводу, что низкой популярностью также пользуется СКУД на основе видеоидентификации, так как такой способ построения системы является во многих планах новым. В виду быстрого развития перспективных технологий машинного зрения и распознавания изображения, получаемого в виде потока с камеры, можно сделать вывод, что такая система сможет занять свою нишу при наличии решений, предлагаемых на рынке.

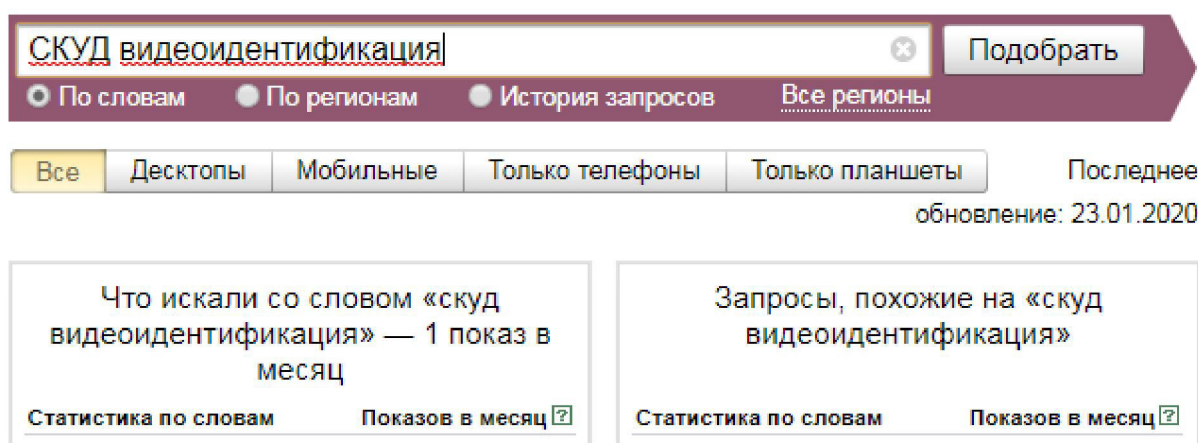


Рисунок 2. Данные wordstat

1.2 Основное предназначение СКУД

Основное предназначение СКУД – настройка порядка доступа персонала, посетителей и автотранспорта на территорию предприятия или закрытого охраняемого объекта с различными вариантами идентификации. СКУД создает различные правила доступа, автоматизирует выдачи временных пропусков, внедряет управление исполнительными механизмами, интегрироваться с системами регистрации, учета и контроля посетителей.

Автоматизированная система управления КТП применяется в целях контроля проезда автотранспорта с организацией требуемого алгоритма проезда и сбора данных об автомобиле.

Данными являются:

- гос.номер автомобиля;
- направление движения;
- наличие пропуска и отношение к группе (категории);
- весовая категория автомобиля пустого и загруженного;
- данные о прохождении точки контроля;
- тип кузова автомобиля.

1.3 Типовые сферы применения

СКУД является многофункциональной системой, за счет этого ее применяют во многих сферах. Система обладает такими обширными возможностями, что ее внедряют как в быту, так и в охранной области. Например, в повседневной жизни данную систему можно встретить во входных дверях подъезда, т.е. домофон, на КПП на предприятия и охранные объекты – это камеры видеофиксации, шлагбаумы и другие устройства. Также система имеет множество областей ее применения:

- Автоматизация проездов автотранспорта на закрытые территории.
- Распознавание автотранспорта, а также определение его относимости к закрытой территории.
- Фиксация перемещения автотранспорта на автобазах, в автобусных парках и таксопарках.
- Разграничение доступа и учет перемещения по территории автосалонов.

1.4 Основные функции системы

1 Контроль проезда автотранспорта на территорию предприятия или организации:

- Распознавание гос.номера автотранспорта и/или RFID-метке/карте
- Его идентификация по внешнему виду.
- СКУД автоматически проверяет разрешения проезда автомобиля на территорию предприятия или организации;
- СКУД не допускает пребывания на территорию чужого автотранспорта без регистрации;

2 СКУД контролирует и архивирует в базе данных все перемещения автотранспорта по территории.

3 Удобное администрирование через web-интерфейсы.

4 Управление шлагбаумами, воротами и другими преградами.

5 Взаимодействие СКУД и другими системами, в том числе учета рабочего времени, охранной и пожарной сигнализации, видеонаблюдения, охраны периметра и др.

1.5 RFID-технология в автомобильных СКУД

В автотранспортной системе контроля и управления доступом очень часто применяются бесконтактные идентификаторы, т.е. RFID-технологии (рис. 3) [8]. Данный идентификатор внедряется в автомобиль для автоматической работы, состоит из электронного чипа и антенны, которые при попадании в рабочее поле считывателя автоматически осуществляют передачу программного кода в контроллер СКУД, где происходит принятие решения о разрешении доступа. Рабочее расстояние СКУД составляет около полутора метров. Это означает, что для продуктивной и бесперебойной работы должна применяться техника более широкого диапазона.



Рисунок 3. RFID-технология.

Также в автомобильной СКУД применяются такие Proximity-технология, которая имеет множество недостатков. Одним из основных недостатков считается небольшой диапазон работы чипов данной технологии. При отдалении применяемого чипа на небольшое расстояние от рабочей области считывателя, весь процесс идентификации сразу же прерывается.

RFID-технологии имеют широкий спрос на рынке продаж, однако ориентировочно 40-45 % специалистов данной области считают, что RFID-метки (рис. 4) имеют множество недостатков, что является неприемлемым в ее использовании. Одной из причин является недостаточная защищенность указанной технологии. По мнению специалистов, RFID-метки действительно недостаточно надежно защищены от элементарных методов взлома. Одной из слабых сторон RFID-метки является уязвимость составляющего ее RFID-чипа, для взлома которого не требуется много усилий и непосредственного контакта, взломщик может осуществить процедуру взлома чипа, находясь на небольшом расстоянии от него. Проанализировав данный вопрос можно сделать вывод, что применение

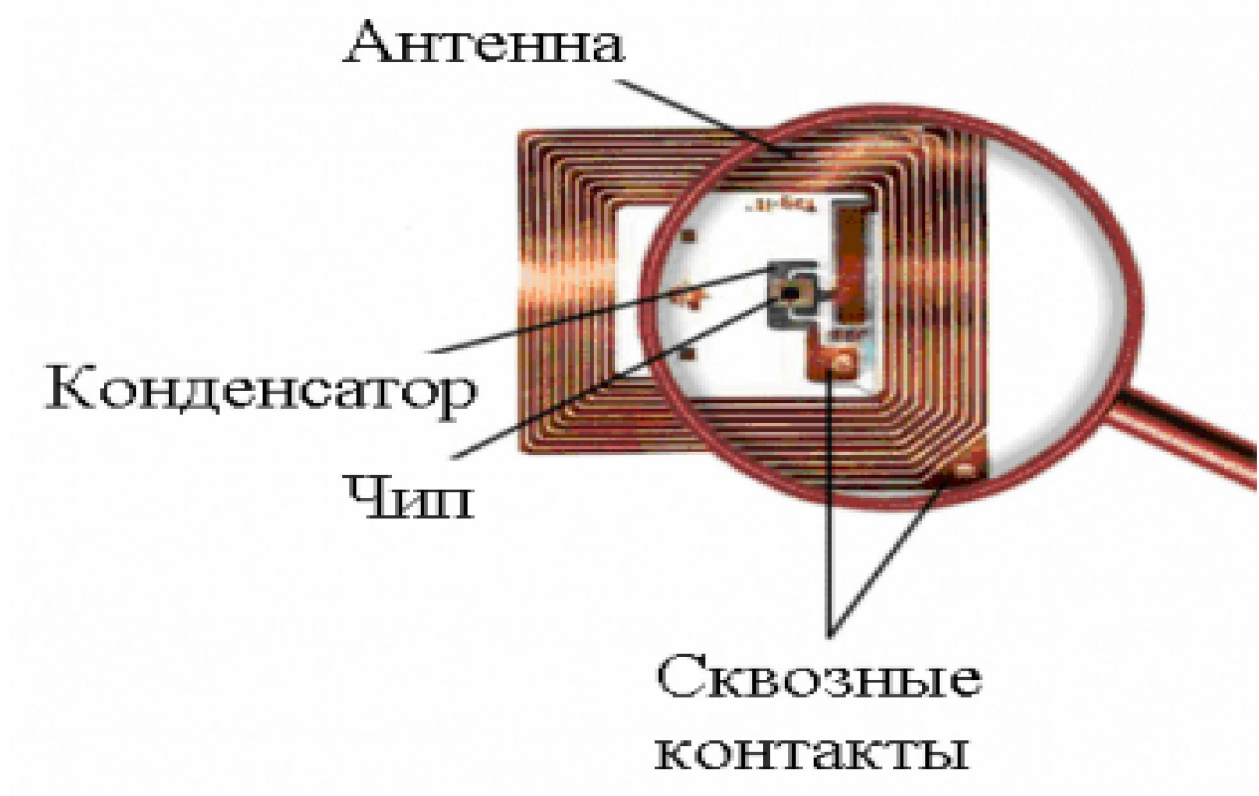


Рисунок 4. RFID-метка.

данной технологии в области, где взлом системы навредит безопасности предприятия, организации или охраняемого объекта, является неприемлемым.

1.6 Принцип работы RFID-технологии

RFID – это Radio Frequency IDentification. В данной технологии передача информации происходит за счет бесконтактной работы чипа, который внедряется либо в пластиковую карточку, либо в кузов или салон автотранспорта, и считывателя, установленный на КПП предприятия или организации. Очень часто используют пассивную систему RFID, которая имеет низкую стоимость на рынке продаж [1]: от 10 рублей за метку и от 500 рублей за считыватель, такие системы смогут обеспечить бесперебойную работу без сбоев и ошибок.

Near field communication – это технология беспроводной передачи данных малого радиуса действия. Часто технология NFC встречается в цифровых мобильных устройствах, связь в такой технологии поддерживается за счет индукции магнитного поля, где две рамочные антенны располагаются в пределах ближнего поля друг друга, эффективно формируя трансформатор с воздушным сердечником. Этот стандарт работает в пределах общественно доступных и нелицензируемых радиочастот - около 13,56 МГц, с шириной полосы пропускания почти 2 МГц.

Приемопередатчик имеет связь с меткой с помощью телекоммуникации [9]. Такие системы не пригодны для использования, но осуществляют автоматическое считывание кодов, которые уже были заложены в базы данных, а также должна быть создана необходимая сетевая инфраструктура или иная система, хранящая и обрабатывающая идентификационные коды, поддерживающая сбор и доставку информации, которая получена считывателями.

Существуют и применяют 2 типа меток: чиповые и бесчиповые. Различие между чиповой и бесчиповой метками заключается в наличии интегральной микросхемы. Чиповые метки существуют трех типов: пассивные, полуактивные и активные метки. В пассивных метках отсутствуют как элементы питания, так и активный передатчик. В полуактивных метках присутствуют только элементы питания, а в активных метках есть и то и другое. Метки классифицируются на считываемые и считываемые/записывающие. Считываемые метки имеют считываемую память, или память, которая однократно программируется и многократно считывается. Считываемые/записывающие метки возможно однократно записывать и многократно перезаписывать информацию.

Положительные характеристики активных меток заключаются в том, что дальность их работы достигает большие расстояния, а связь со считывателем моментальная и надежная. Одним из недостатков активных меток считается дорогая стоимость на рынке. Полуактивные метки в отличие от пассивных имеют высокую дальность и высокие функциональные возможности, однако это также приводит к повышению их стоимости. Пассивные метки обладают дальностью менее 9-10 метров, зависимы от регламентных ограничений и влияния окружающей среды. Тем не менее, они имеют максимальный рыночный потенциал из-за наименьшей стоимости [1].

В качестве примера бесконтактных радиочастотных идентификационных карт, популярных на рынке и обладающих низкой стоимостью, можно назвать модель TK4100 ISO компании Em-Marine. Карта сделана согласно стандарту ISO 7810: ширина — 85,6 мм. $\pm 0,13$ мм, высота — 53,98 мм. $\pm 0,06$ мм, толщина — 0,76 мм. $\pm 0,08$ мм, радиус закругления — 3,18 мм. $\pm 0,3$ мм. Рабочая частота карты – от 100 до 150 кГц, питающая частота – 125 кГц. Емкость памяти – 64 бит. Радиус действия метки

колеблется от 5-10 до 60-70 сантиметров в зависимости от конструктива метки и считывателя.

В качестве примера можно привести реализацию СКУД в Пензенском государственном университете, основанную на считывателях, которые распознают информацию в бесконтактных банковских картах оплаты системы МИР. Они работают в среднечастотном радиодиапазоне, считывание происходит на частоте 13,56 МГц. Удобство использования меток такого класса бесспорно: данные карты имеются у большинства студентов и преподавателей, а так же посредством описанной выше технологии NFC, ставшей чрезвычайно популярной в качестве опции у многих смартфонов и других портативных устройств, стало возможным эмулирование сигнатуры карты используемым устройством.

1.7 Диапазон частот

Диапазона частот идентификатора делится на три группы:

- с низкой частотой (до 500 кГц);
- со средней частотой (от 10 до 15 МГц);
- высокой частотой (от 850 до 950 МГц и 2,4-10 ГГц).

В момент увеличения частоты растет расстояние считывания идентификатора. Так, например, для СКУД автомобилей необходимо расстояние считывания и регистрации в несколько метров. В связи с этим в них используются идентификаторы и считыватели гигагерцевого диапазона. [5]

Идентификаторы подразделяются на две группы: активные и пассивные. Активные имеют встроенный источник питания (батарею, аккумулятор), потребляет меньшую мощность, имеют большую дальность действия. Пассивные в свою очередь получают электроэнергию от встроенной антенны, откуда идет подача тока, которое происходит

во время попадания идентификатора в поле действия считывателя. Пассивные идентификаторы обычно небольшого размера, существенно легче по весу, в ценовой политике являются дешевле активных, а также долгие в использовании. Однако дальность действия пассивных идентификаторов меньше, чем у активных. Поэтому активные идентификаторы чаще используются в автомобильной СКУД.

Стоит отметить существование считывателей УВЧ диапазона, которые значительно превосходят по дальности чтения стандартные proximity и smart-считыватели. СКУД, оборудованные такими считывателями, также встречаются в различной литературе. УВЧ считыватели применяют для:

- Удаленного чтения идентификаторов на транспортных средствах, количество которых известно заранее;
- Создания системы учета, поиска и инвентаризации с большой номенклатурой и необходимостью автоматизации (библиотеки, архивы), которые строятся на тех же основах, что и СКУД;
- Принятия решения на основании данных, записанных в дополнительную область метки;

К недостаткам УВЧ считывателей относят высокую стоимость. [6]

1.8 Особые требования к автомобильным RFID-системам

Основное требование СКУД автотранспорта – это большая дальность регистрации идентификатора, примерно 4-10 м. (рис. 5).

Считыватели, относящиеся к группе гигагерцовых, имеют четко выраженную диаграмму направленности поля, что позволяет производить их установку на не большом расстоянии друг от друга, без опасения возникновения взаимных помех.

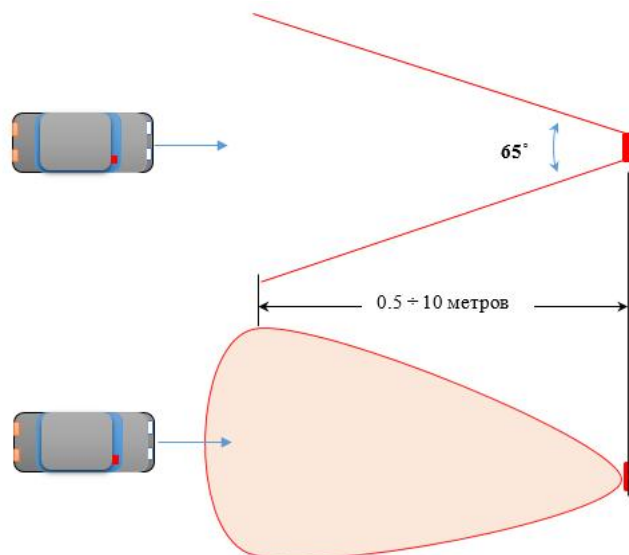


Рисунок 5. Расстояние регистрации идентификатора.

Очень часто считыватели имеют класс защиты IP-54, в которых диапазон температуры их работы должен быть достаточно широк, поэтому в некоторых моделях используется внутренний обогрев. Это значимая особенность транспортных считывателей, поскольку обычно они эксплуатируются снаружи зданий.

1.9 Примеры RFID-систем

В качестве примера рассмотрим три RFID-системы от компаний разных компаний: BALOGH (Франция), NEDAP (Нидерланды) и TagMaster (Швеция).

BALOGH. Существует два типа RFID-считыватели: модулярный считыватель с допустимым расстоянием считывания от 3 до 10 метров и компактный с расстоянием считывания от 50 до 100 см. Оба указанных типа работают на частотах 2,45 ГГц.

Функция антиколлизии позволяет системе правильно проводить регистрацию меток, способна обеспечить устойчивую идентификацию при

наличии в поле считывателя сразу 5 идентификаторов без какой-либо зависимости от расположения считывателей и идентификационного оборудования. Это обеспечивает бесперебойную идентификацию в случае активации метки в рабочей зоне считывателя, который может подключаться к большинству существующих контроллеров СКУД, поскольку имеет набор распространенных интерфейсов для работы, а именно: wiegand 26, RS-232/422/485. Возможна инсталляция нескольких считывателей.

В роли идентификатора выступают небольшие метки, но есть возможность работы с более мощными моделями. Такие идентификаторы осуществляют работу от 5 до 10 лет, в зависимости от конкретной модели. А также есть специальные метки для наружной установки, которые устойчивы к агрессивным средам.

NEDAP. Данный считыватель работает в диапазоне частот от 2,4 до 2,482 ГГц, изначально осуществлял работу на больших расстояниях, и помимо стандартного выхода wiegand 26 бит этот считыватель имеет интерфейсы RS-232, RS-422.

Facility-код (код организации) является принадлежностью считывателя. Код может быть переустановлен как при помощи ПК, так и программой "iTerminal". Код организации передается в считыватель по интерфейсу RS-232, что позволяет интегрировать оборудование данной марки в существующие системы, поддерживающие только один код организации. У считывателя и у метки есть особый засекреченный Customer code (код пользователя). Только при совпадении Customer code карты с Customer code, запрограммированные в firmware считывателя, последний отправляет номер карты в контроллер.

TagMaster. Рабочий диапазон считывателей фирмы TagMaster равен от 2,435 до 2,465 ГГц [10]. Рабочая дальность считывания достигает от 6 до 8 метров..

Подключение считывателей происходит через применяемые в системе интерфейсы. Их настройка и конфигурация осуществляется посредством набора инструкций, связь осуществляется посредством интерфейса RS-232. Отличительная особенность - возможность комплектации специализированным нагревательным элементом (работа до -40°C).

Метка MarkTag (S1255) является идентификатором, которая идентична обычным проксимити-картам от компании HID, используемая в СКУД. Также возможно использовать более мощные идентификаторы для наружной установки – это MarkTag HD (S1455).

1.10 Интеграция в автомобильных RFID-системах

Метка Combi-Booster HID Prox (NEDAP) - это один из наиболее ярких примеров интеграции оборудования разных производителей. Combi-Booster позволяет интегрировать в общую СКУД карты компании HID и передавать их номер на таком же большом расстоянии, что и номер карты NEDAP. Предназначение метки заключается в том, что для передачи считывателем в контроллер двух кодов: кода самой метки и кода вставленной в Combi-booster карты HID. Можно проводить идентификацию как водителя, так и его автомобиля, что позволяет использовать такие режимы повышенной секретности, как вход по двум картам.

TagMaster производит метки двойной технологии - с интегрированным высокочастотным чипом собственного производства и стандартным чипом HID (килогерцевого диапазона), что позволяет применять данные метки

как в автотранспортных, так и в обычных СКУД со считывателями HID. В данном случае заметим то, что расстояние чтения идентификатора HID будет стандартное – от 5 до 75 см в зависимости от модели HID.

1.11 Сетевые системы контроля и управления доступом

Различают также сетевые системы контроля и управления доступом, как правило, они имеют между собой связь посредством проводного или беспроводного интерфейса. Обработка событий возложена на контроллеры, которые также могут являться устройствами хранения информации. В таких системах, как правило, не бывает сущности, которая объединяет все контроллеры в единую сеть с центральным сервером, так как контроллеры могут быть не только автономными, но и после регистрации событий принимать решение о дальнейшем действии сообща. Тем не менее, схема, в которой центральный сервер является основной, ее возможная реализация представлена на рисунке 6.

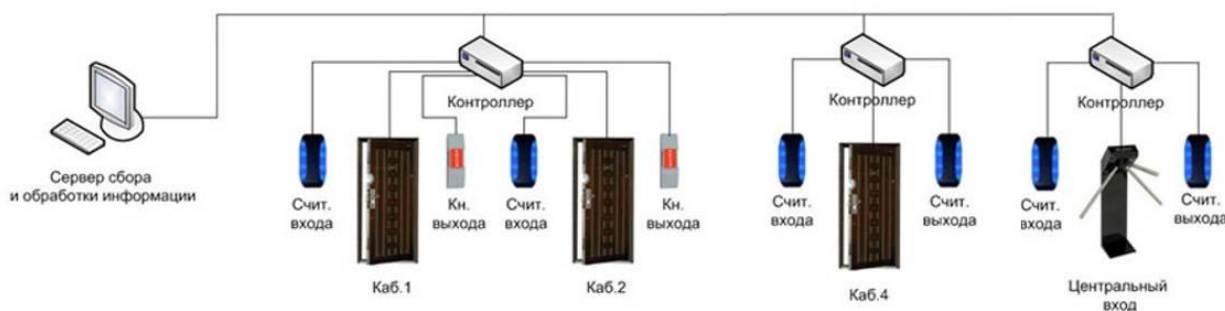


Рисунок 6. Реализация сетевой СКУД с центральным сервером

На сегодняшний день различают два типа контроллеров: автономные и ориентированные на сетевой протокол. Автономные имеют возможность хранить во внутреннем накопителе базу данных ключей, регистрировать события. Их сильная сторона состоит в гарантированной стойкости вне зависимости от состояния центрального сервера, он может быть выведен из строя злоумышленниками, но контроллер продолжит штатную работу. К

минусам можно отнести затруднения в обслуживании и обновлении программного обеспечения и баз данных. В случае инцидента и необходимости доступа к журналу событий, оператор должен загрузить необходимую информацию напрямую с устройства, что времязатратно.

Второй тип контроллеров – ориентированный на сетевой протокол. Такие контроллеры не имеют накопителя и информации о базе данных, работоспособность обеспечивается посредством постоянного общения с сервером. К сильным сторонам такого решения можно отнести отсутствие надобности обновлять базу данных и программное обеспечение на каждом контроллере системы, существует единственная точка истины – центральный сервер. К недостаткам – а штатном режиме, обработка события занимает больше времени, что связано с необходимостью создания запроса к серверу и ожиданием ответа, а при выходе из строя центрального сервера система приостановит свою работу.

В настоящее время идет переход с проводных СКУД на беспроводные. Технологии организации беспроводных сетей для СКУД являются перспективными на рынке, имеют широкие возможности масштабирования систем. Интерес использования таких технологий обоснован тем, что построение беспроводной сетевой системы СКУД имеет меньшую затратность, имеет больший потенциал для масштабируемости, а также возможности для конфигурации системы в соответствии с требованиями заказчика. [11]

Для беспроводных технологий могут быть использованы различные радиоканалы, однако в СКУД используются только некоторые из них:

- *Bluetooth*. Среди преимуществ можно выделить то, что в состав спецификации входят протоколы передачи данных на высокой скорости, а устройства, использующие Bluetooth обладают низким энергопотреблением. На расстояние до 100м могут передаваться данные со скоростью до 1 Мбит/с.

Сопряжение устройств происходит почти мгновенно, при этом безопасность обеспечивается 128-битным AES-шифрованием. Основной недостаток - низкая дальность действия.

- *Wi-Fi*. Основное преимущество – дальность приема и передачи. При помощи последних разработок в данной спецификации, инженерам удалось обеспечить стабильный прием сообщения на расстоянии 14 километров от источника. Скорость передачи также является сильной стороной Wi-Fi. Недостаток – слабая защищенность от помех, так как диапазон радиочастот Wi-Fi очень распространен, на нем работает большинство устройств бытового и промышленного назначения, а также Wi-Fi не отличается энергоэффективностью, что скажется на времени автономной работы контроллеров

- *ZigBee*. Изначально была предназначена для систем охранной и пожарной сигнализаций. ZigBee может использоваться в системах контроля доступа.[12] Преимущества – защищенность и гарантированная стойкость сигнала. Устройства приема и передачи сигнала данной спецификации отличаются длительным временем автономной работы, что связано с особенностью работы устройств и технологией «маячковой передачи». Основной недостаток – устройства, необходимые для построения сети, имеют чрезвычайно высокую рыночную стоимость

- *GSM*. Преимущества – за исключением небольших участков, не оснащенных базовыми станциями, бесшовная зона покрытия, возможность передачи данных в методом GPRS, SMS, устойчивый непрерывный сигнал, возможность установки центрального сервера в любом месте. Мощность передатчика составляет 1Вт, что положительно сказывается на времени автономной работы. Недостатком такого решения можно назвать необходимость оплаты услуг оператора сотовой связи для каждого контроллера. услуг оператора сотовой связи для каждого контроллера системы.

1.12 Известные технологии машинной обработки потокового видео

Машинное зрение — это научное направление в области искусственного интеллекта, в частности робототехники, и связанные с ним технологии получения изображений объектов реального мира, их обработки и использования полученных данных для решения разного рода прикладных задач без участия (полного или частичного) человека. [4]

Началом развития данного направления можно назвать труды Оливера Селфриджа, который в 1955 году опубликовал статью «Глаза и уши компьютера». Значительный вклад в развитие направления науки был сделан Френком Розенблаттом («Компьютерная реализация персептрона», 1958 год), Гансом-Хельмутом Нагель («Теория анализа динамических сцен», 1979 год). В 2003 году в данном направлении появились алгоритмы корпоративных систем распознавания лиц, что приближает нас к созданию подобного алгоритма для анализа и идентификации признаковых характеристик автотранспортного средства, таких как рельеф номерного знака или формы кузова автомобиля.

В качестве компонентов систем машинного зрения используют:

- Камеры, цифровые или аналоговые (от 1 шт. и более);
- ПО для генерации изображений, которые в последствии будут обработаны;
- Процессорная единица;
- Периферийные устройства ввода-вывода и каналы связи для передачи полученных результатов;
- Специализированные световые источники;
- Датчики, синхронизирующие и «склеивающие» полученные изображения в цельный образ.

Все вышеперечисленные пункты, как правило, включают в себя так называемую «умную камеру», оборудованную необходимым периферийным оборудованием для комплексной обработки сложившейся обстановки.

1.13 Соответствие разрабатываемой системы требованиям ГОСТ

Системы, подобные разрабатываемой в данной работе, должны соответствовать требованиям действующих государственных стандартов. Это связано не только с тем, что основными заказчиками СКУД являются государственные предприятия, но и с требованиями рынка в целом. Системы, прошедшие спецификацию и проверки на предмет соответствия требованиям актуальному ГОСТ являются наиболее конкурентными, их распространение возможно в сертифицированных торговых представительствах.

Актуальным ГОСТом, описывающим предъявляемые требования к СКУД, является «Р 54831-2011. Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний». После детального изучения данной документации был сделан вывод, что данный ГОСТ не подходит для описания разрабатываемой системы, так как в соответствии с пунктом 1, описывающим область применения, «настоящий стандарт не распространяется на УПУ, предназначенные для контроля перемещения транспортных средств» [3]. Предыдущий стандарт, «Р 51241-2008», такого пункта в описании не имеет и также является действующим. Следовательно, для спецификации и испытаний системы необходимо руководствоваться тем, что описано в нем.

В пункте 4 настоящего стандарта рассматривается классификация средств и систем КУД. Пункт 4.1.2 предусматривает следующие устройства, разделенные по функциональному назначению:

- преграждающие управляемые;

- исполнительные;
- считывающие;
- идентификаторы (ИД);
- средства управления в составе аппаратных устройств и программных средств. [2]

СКУД может состоять из дополнительных средств: источников электропитания; датчиков состояния УПУ; дверных доводчиков; световых и звуковых индикаторов (оповещатели); кнопок ручного управления УПУ; устройств преобразования интерфейсов сетей связи; аппаратуры передачи данных по различным каналам связи и других устройства, предназначенных для обеспечения работы СКУД.

В состав СКУД могут входить также аппаратно-программные средства – это компьютерное оборудование, оборудование для компьютерных сетей, общее программное обеспечение.

В качестве УПУ является шлагбаум, классификация по виду перекрытия проема прохода. Исполнительное устройство по способу запираения – механизмы привода дверей, ворот. Идентификаторы и считыватели по виду используемых идентификационных признаков – электронные радиочастотные, по способу считывания идентификационных признаков – бесконтактные, считывание кода происходит при поднесении идентификатора на определенное расстояние к считывателю.

СКУД классифицируют по:

- способу управления;
- числу контролируемых точек доступа;
- функциональным характеристикам;

- уровню защищенности системы от несанкционированного доступа к информации.

Разрабатываемая система будет классифицироваться по способу управления как централизованная - с обменом информации через центральный пульт и контролем и управлением системой со стороны центрального устройства управления СКУД, которая должна соответствовать общим функциональным требованиям и дополнительно обеспечивать:

- работу в локальной сети контроллеров СКУД;
- регистрацию и протоколирование тревожных и текущих событий;
- приоритетное отображение на экране управляющего компьютера тревожных событий;
- управление работой УПУ в точках доступа по командам оператора;
- задание временных режимов действия идентификаторов в точках доступа и уровней доступа;
- защиту технических и программных средств от несанкционированного доступа к элементам управления, к установке режимов и к информации;
- автоматический контроль исправности средств, входящих в систему, и линий передачи информации;
- возможность автономной работы контроллеров системы с сохранением контроллерами основных функций при отказе связи с пунктом централизованного управления;
- блокировку прохода по точкам доступа командой с пункта управления в случае нападения;
- возможность подключения дополнительных средств специального контроля, средств досмотра.

По числу контролируемых точек доступа – малой емкости, по функциональным характеристикам – 1-й системы с ограниченными функциями.

Пункт 4.4 описывает порядок определения условного назначения средств и систем КУД. Различают следующие правила именования для СКУД:

- а) наименования "Система контроля и управления доступом" (СКУД);
- б) группы символов в соответствии с 4.4.5;
- в) обозначения ТУ.

Структура группы символов обозначения системы КУД:

$$X_1X_2X_3X_4 - X_5/X_6X_7,$$

где X_1 - способ управления:

- 1 - автономное,
- 2 - централизованное (сетевое);
- 3 - универсальное (сетевое),

X_2 - число контролируемых точек доступа:

- 1 - система малой емкости,
- 2 - система средней емкости,
- 3 - система большой емкости;

X_3 - класс по функциональным характеристикам;

X_4 - класс защищенности системы от несанкционированного доступа к информации для систем повышенной и высокой устойчивости к НСД или буква "Н" для систем нормальной устойчивости;

X₅ - порядковый номер разработки; Порядковый номер регистрируется соответствующим государственным органом, ответственным за проведение технической политики в данной сфере.

X₆ - обозначение конструктивного исполнения;

X₇ - обозначение модернизации (обозначается русской прописной буквой в алфавитном порядке, первая модернизация - А, вторая - Б и т.д.). [2]

Обозначение разрабатываемой системы: СКУД – 211Н-1/9Б

1.14 Выводы по разделу 1

В результате проведенных исследований в области анализа предметной области существующих технологий для создания СКУД был сделан следующий выбор основных технологий для реализации:

— Выбор технологии считывателя был сделан в пользу стандартов NFC и родственного ему RFID. Системы, использующие данных технологии, оптимальны и по цене комплектующих, и по качеству выполнения основной задачи. Эти беспроводные стандарты передачи данных позволяют считывать информацию, находящуюся вне пределов видимости. Идентификационный код хранится в метке, состоящей из микрочипа, прикрепленного к антенне;

— Была выбрана спецификация беспроводной передачи данных Bluetooth. Именно это технологическое решение позволяет создать сеть с минимальными затратами на оснастку и обслуживание системы.

2 СОСТАВ И СТРУКТУРА КОМПЛЕКСА СКУД С ВИДЕОФИКСАЦИЕЙ

В данном разделе будет выполнено описание элементарных звеньев объекта и связей между ними. Под элементарным звеном подразумевается такая часть, которая реализует элементарную функцию. На рисунке 7 представлено графическое изображение структурной схемы системы, по которому будет произведено описание.

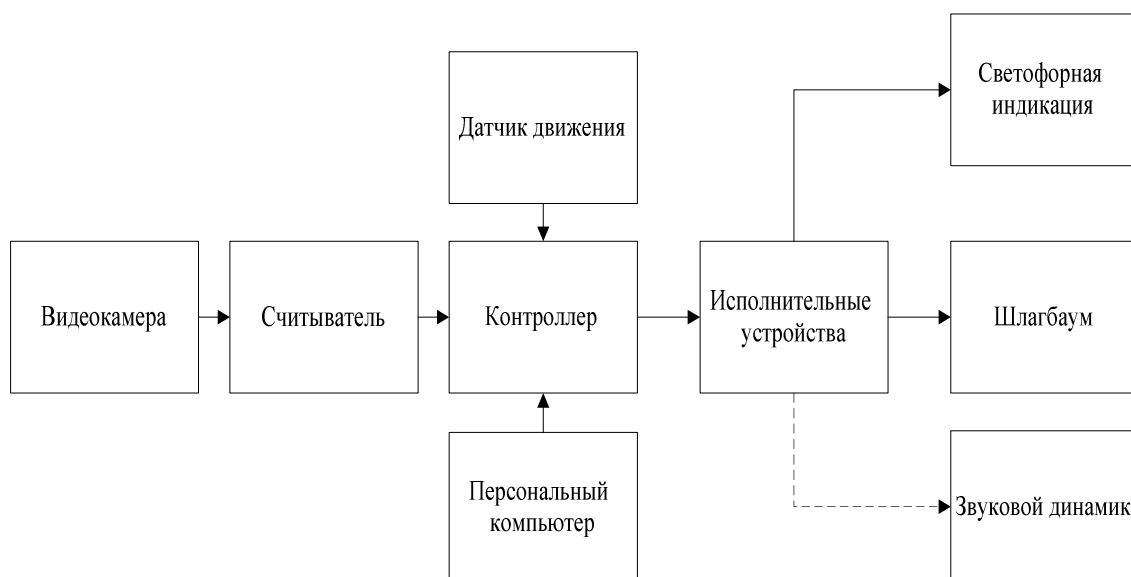


Рисунок 7. Структурная схема

Каждое из устройств в системе контроля и управления доступом состоит из считывателя, блока питания, контроллера и запорного устройства. Устройство имеет именно такую конфигурацию, так как в ее составе присутствуют основные компоненты, позволяющие осуществлять работу по контролю и управлению доступом. Данная конструкция проста и оптимальна.

2.1 Основные компоненты СКУД с видеофиксацией

СКУД состоит из таких компонентов:

- идентификаторов и считывателей (рис.8);
- контроллеров (рис.8);
- управляющего персонального компьютера;
- замков, проводов, дверей, доводчиков, шлагбаумов, индикаторов и т.д. (рис. 8);
- видеокамер (от 1 единицы и более).



Рисунок 8. Идентификатор / Микроконтроллер СКУД / Устройство исполнительное

В зависимости от применяемой СКУД на предприятии или закрытом охраняемом объекте, контроллер со считывателем могут быть объединены в единый блок или отсутствовать.

2.2 Устройства контроля и управления доступом

Контроллер – это электронное устройство, осуществляющее контроль за работой считывателей и управляет исполнительными устройствами (рис. 9).

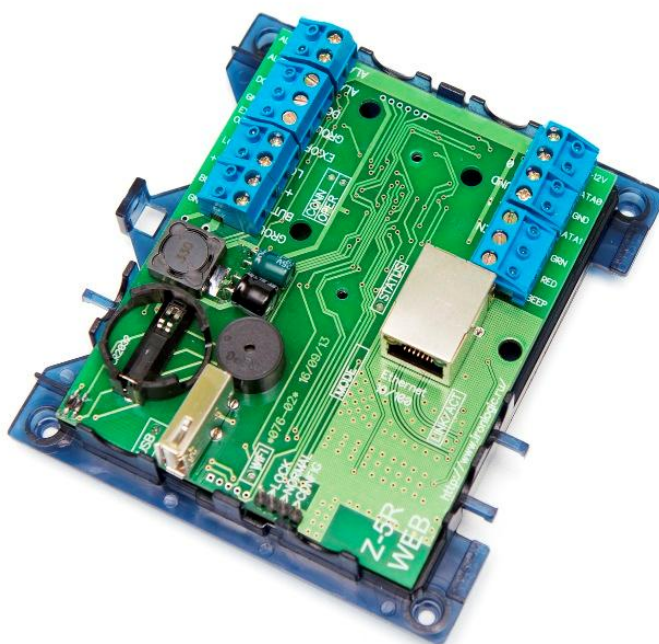


Рисунок 9. Внешний вид контроллера

Контроллеры подразделяются на однофункциональные и многофункциональные.

Функциональным назначением является хранение БД кодов пользователей, программирование режимов работы, прием и обработка информации от считывателя, принятие решений на основании поступившей информации, управление устройствами.

Наиболее существенными дополнительными функциями контроллеров являются:

- предотвращение проезда автотранспорта на территорию предприятия или организации по одним и тем же гос.номерам;
- наличие релейных выходов для подключения средств оповещения и т.д.;
- возможность обработки нескольких систем;
- обеспечение многоуровневого контроля.

Контроллеры рассчитаны на управление несколькими считывателями, а также могут быть объединены в единую систему и подключаться либо к ведущему контроллеру (мастер-контроллеру), либо к компьютеру, управляющему работой всех контроллеров [13]. К ведущему контроллеру возможно подключение управляющий ПК и другие периферийные устройства. Однофункциональные контроллеры осуществляют работу только в автономном режиме. Многофункциональные контроллеры управляют доступом и проводят мониторинг состояния устройств исполнительных и вывода данных на компьютер и печать. С помощью таких многофункциональных контроллеров создаются сложные комплексы, интегрированные с другими подсистемами безопасности, например, с охранно-пожарной сигнализацией и телевизионными системами видеоконтроля. Связь контроллеров между собой в единую сеть осуществляется через стандартный интерфейс RS-485. Для связи ведущего контроллера с компьютером используется стандартный интерфейс RS 232. Многофункциональные контроллеры работают в основном в сетевом режиме (централизованный контроль и управление доступом).

Классические сетевые системы не требуют применения контроллеров с уникальными возможностями, необходима лишь грамотно составленная и качественно отлаженная прошивка, микропроцессорная система

с ресурсами достаточными для обеспечения бесперебойной работы. Поиск контроллеров с характеристиками, удовлетворяющими задачам, привел к компании Particle Industries, которая с 2012 года производит наборы аппаратных и программных средств.

Набор аппаратных средств, предлагаемых компанией в качестве готовых решений для мультифункциональных систем, очень велик. Разработчики делают упор на поддержку любой топологии сети, предлагаемые аппаратные средства позволяют развернуть сеть с использованием шлюзов и ретрансляторов. Аппаратные средства компании Particle появились в продаже в июле прошлого года и уже сейчас пользуются спросом. Существует множество сообществ по поддержке и консультациям по вопросам работы с платами и контроллерами Argon, Boron, Xenon и др.

Для разработки системы контроля и управления рассмотрим изделие с названием Argon – это мощная плата разработки с поддержкой Wi-Fi, которая может выступать в качестве автономной конечной точки Wi-Fi или шлюза с поддержкой Wi-Fi для сетей Particle Mesh. Он основан на Nordic nRF52840 и имеет встроенную схему зарядки аккумулятора с возможностью подключения Li-Pol батарейки и развертывания локальной сети за короткий период времени. Argon отлично подходит в качестве шлюза для подключения всей группы локальных конечных точек. Внешний вид платы Argon представлен на рисунке 10.

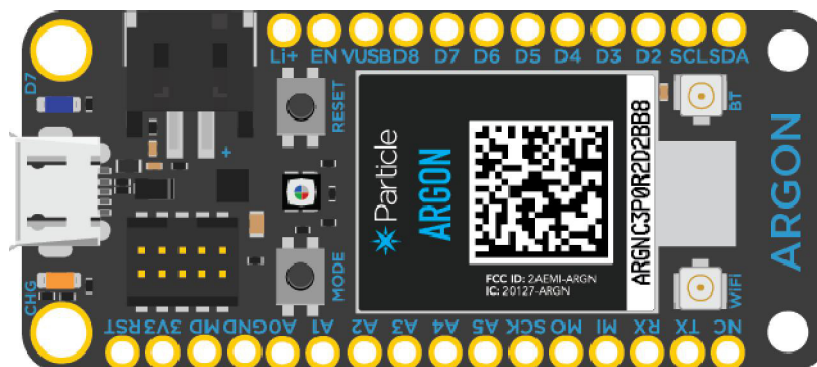


Рисунок 10. Внешний вид платы Argon

Функционал проектировочной платы широк. В литературе, приведенной на сайте разработчика, описаны следующие характеристики [15]:

- Espressif ESP32-D0WD 2.4 GHz Wi-Fi сопроцессор;
 - 4MB постоянной памяти;
 - Поддержка 802.11 b/g/n;
 - 802.11 n (2.4 GHz) со скоростью до 150 Mbps;
- Nordic Semiconductor nRF52840 SoC;
 - ARM Cortex-M4F 32-bit процессор, 64MHz;
 - 1MB флеш-памяти, 256KB RAM;
 - IEEE 802.15.4-2006: 250 Kbps;
 - Bluetooth 5: 2 Mbps, 1 Mbps, 500 Kbps, 125 Kbps;
 - ARM TrustZone, CryptoCell-310 модули криптографии и защиты;
 - До +8 dBm TX мощности (до -20 dBm с шагом 4 dB);
 - NFC-A метка;
- Дополнительная SPI флеш-память на плате - 4MB ;
- 20 смешанных сигналов GPIO (6 x аналоговых, 8 x PWM), UART, I2C, SPI;
- Micro USB 2.0 (до 12 Mbps);
- Встроенная Li-Po зарядка и коннектор для батарейки, напряжение от 3,6В до 4,2В;
- JTAG (SWD) коннектор;
- RGB диод с индикацией состояния;
- Кнопки Reset и Mode;
- PCB антенна на плате;
- U.FL коннектор для внешней антенны.

На рисунке 11 представлена диаграмма блоков платы Argon.

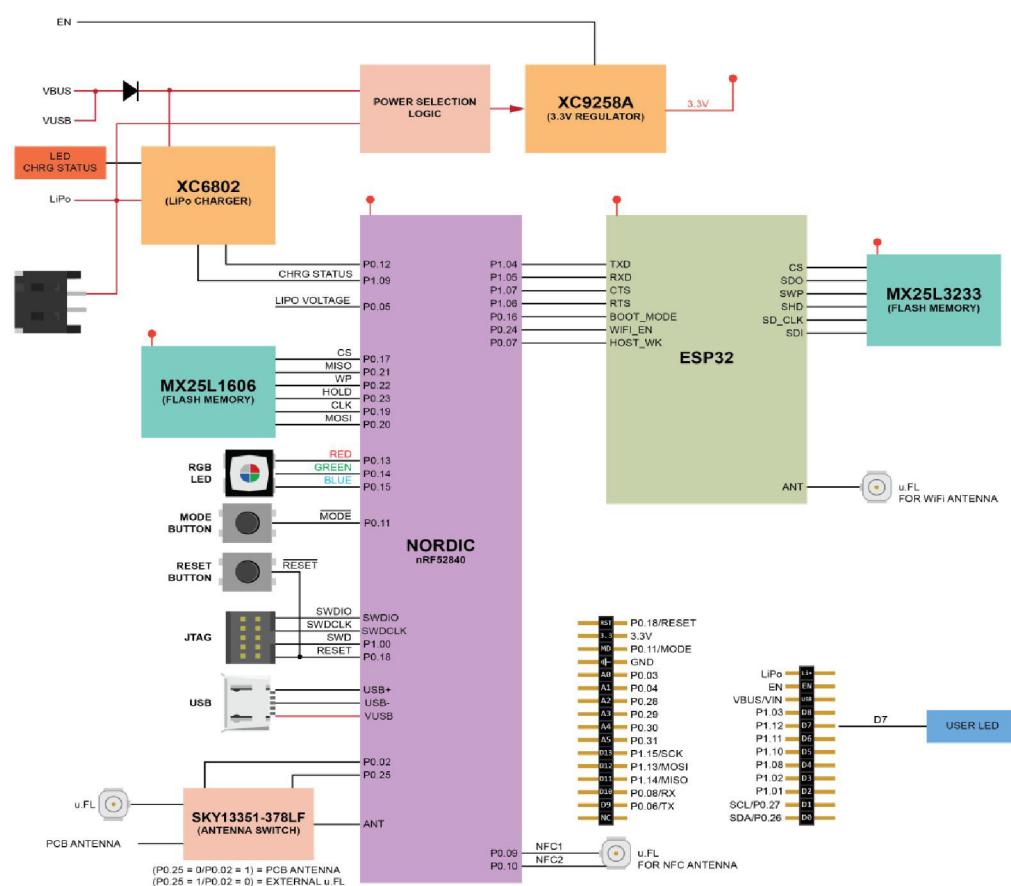


Рисунок 11. Диаграмма блоков платы Argon

Плата имеет размеры 0.9 дюйма на 2 дюйма (2,286x5,08 см). Более подробно плата будет рассмотрена в следующих разделах, так как в зависимости от направления в разработке нас будут интересовать разные показатели, которые демонстрирует данная аппаратная платформа.

Центральный вычислительный модуль описанной платы – система на кристалле компании Nordic Semiconductor, модель – nRF52840. SoC nRF52840 является наиболее продвинутым представителем семейства SoC серии nRF52. Он отвечает требованиям сложных приложений, которым требуется параллелизм протоколов, а также богатый и разнообразный набор периферийных устройств и функций. Он обеспечивает достаточную

доступность памяти как для Flash, так и для оперативной памяти, что является необходимым условием для требовательных приложений.

NRF52840 полностью мультипротокольный, с полным параллелизмом протоколов. Он поддерживает протоколы для фирменных стеков Bluetooth 5.0, Thread, Zigbee, 802.15.4, ANT и 2,4 ГГц.

NRF52840 построен на базе 32-разрядного процессора ARM® Cortex - M4 с модулем с плавающей запятой, работающим на частоте 64 МГц. Он имеет метку NFC-A для использования в упрощенных решениях для сопряжения и оплаты. Криптографическое устройство ARM TrustZone CryptoCell входит в состав микросхемы и предоставляет широкий спектр криптографических опций, которые работают очень эффективно независимо от процессора. Он имеет множество цифровых периферийных устройств и интерфейсов, таких как высокоскоростной SPI и QSPI для сопряжения с внешней вспышкой и дисплеями, PDM и I2S для цифровых микрофонов и аудио, а также высокоскоростное USB-устройство для передачи данных и блок питания для зарядки аккумулятора.

Исключительно низкое энергопотребление достигается благодаря сложной встроенной адаптивной системе управления питанием.

Ключевые характеристики, которые приводятся в технической литературе, представлены ниже:

- 64 МГц Arm® Cortex-M4 с FPU
- 1 МВ Флеш-памяти + 256 Кб RAM
- Bluetooth 5 мультипротокольный радиоканал
- Поддержка IEEE 802.15.4
 - Thread
 - Zigbee
- Диапазон напряжения питания: 1.7-5.5 V

- Полноскоростной USB - 12 Мб/с
- NFC-A метка
- Подсистема безопасности Arm CryptoCell CC310
- Поддержка интерфейсов QSPI/SPI/TWI/I²S/PDM/QDEC
- Высокоскоростной SPI, частота 32 МГц
- Quad SPI интерфейс, 32 МГц
- EasyDMA для всех цифровых интерфейсов
- 128-битный AES/ECB/CCM/AAR сопроцессор
- Встроенный преобразователь постоянного тока
- Регулируемый источник питания для внешних компонентов до 25 мА

Внутренние технические характеристики подкреплены мощной поддержкой программного обеспечения: имеются готовые библиотеки и примеры для создания прошивки, software development kit (SDK).

2.3 Устройства центрального управления

Персональный компьютер предназначен для программирования СКУД, получения информации о пользователях системы, дате и времени проезда пользователей через контрольные устройства, срабатывании средств охранно-пожарной сигнализации, видеоконтроля, попыток несанкционированного проникновения, аварийных ситуаций.

Для работы в СКУД использует любой совместимый персональный компьютер отечественного или зарубежного производства. Компьютер используется в системе для ее программирования и получения отчетов о работе системы. В свою очередь ПК, используя специально разработанное для предприятия и охраняемого объекта ПО (желательно русифицированное), осуществляет общее управление и программирование СКУД, получает и обрабатывает информацию с контроллеров и микроконтроллеров, создает базу данных, формируя различные отчеты и

сводки. Русифицированное ПО под MSDOS и Windows позволяет осуществлять автоматическую запись данных по всем операциям входы/выхода и въезда/выезда. С помощью его всегда можно запросить сведения о местонахождении рабочего персонала или посетителей предприятия или организации. Текущее состояние СКУД отображается в удобной графической форме. В компьютер вводится план охраняемого объекта, на котором стандартными значками указываются считыватели, замки, технические средства охранно-пожарной сигнализации, видеоконтроля и т.п. На плане система автоматически в реальном масштабе времени показывает состояние всех нанесенных объектов контроля - открыт или закрыт шлагбаум, какой именно извещатель сработал в случае тревоги. Таким образом, в любой момент времени можно быстро оценить ситуацию и в случае необходимости или чрезвычайной ситуации оперативно и эффективно принять меры предосторожности.

2.4 Устройства исполнительные

Устройства, принимающие команды с контроллера и обеспечивают безопасность от несанкционированного проникновения через устройства заграждения людей в помещения или автомобиля на территорию предприятия или организации, называются исполнительными. В исполнительных устройствах применяются механизмы электромеханического и электромагнитного принципа действия.



Рисунок 12. Исполнительные механизмы шлагбаума.

Электромеханический принцип действия механизма основан на перемещении закрывающих элементов с помощью включения на время их передвижения электромотора или электромагнита (рис. 12). Для примера рассмотрим принцип работы электромотора в автоматическом шлагбауме. При подаче разрешающего сигнала с компьютера на контроллер, механизм открытия/закрытия проходит алгоритм действий по запуску машины на территорию предприятия или организации или же по выпуску с территории.

В электромагнитных механизмах отсутствуют движущиеся механические открывающие/закрывающие элементы и вся работа заключается в работе с применением сил магнитного притяжения, создаваемых мощным магнитом (рис. 13)



Рисунок 13. Магнитный механизм автоматических ворот.

Очень часто на предприятиях и организациях используют устройства с электромагнитной блокировкой закрывающихся элементов с возможностью перемещения перевода их в ручной режим при открытии/закрытии на случай чрезвычайной ситуации или экстремальных условий.

В закрытое состояние устройство переходит благодаря установке специального устройства - доводчика, без которых система теряет основную функцию - ограничения доступа, так как без них устройство ограждения может находиться в любом состоянии. По виду исполнительного механизма доводчики подразделяются на пружинные, пневматические, гидравлические и электромеханические.

Функция доводчика - не только гарантировать закрытие устройства ограждения, но и оберегать шлагбаум от механических ударов, а при пожаре автоматически раскрывать ворота/шлагбаумы и помогать эвакуации.

В некоторых типах доводчиков используется, так называемая "система торможения с подтягом" - вначале доводчик дает разогнаться, потом тормозит движение и уже в конце, резко подтягивает балку, обеспечивая гарантированное ее закрытие. Кроме того некоторые доводчики могут иметь встроенный режим безопасности, исключающий случайное закрытие над автомобилем в момент проезда через устройство заграждения.

2.5 Структура комплекса СКУД

АСУ КТП имеет модульную структуру и может модифицироваться для выполнения конкретного алгоритма.

АСУ КТП состоит из двух основных функциональных модулей:

- АРМ сбора данных и управления системы контроля автотранспорта. Реализует элемент системы, обеспечивающий распознавание номеров автомобилей, управление исполнительными устройствами, получение результатов взвешивания. Элемент обязателен для системы, должен присутствовать в составе системы минимум один раз (рис. 14)



Рисунок 14. Камера видеофиксации.

- СУБД – система управления базами данных. Базовая СУБД является FireBird 2.5. Дополнительно рассматривается возможность работы системы с СУБД MS SQL 2005/2008 (рис. 15).

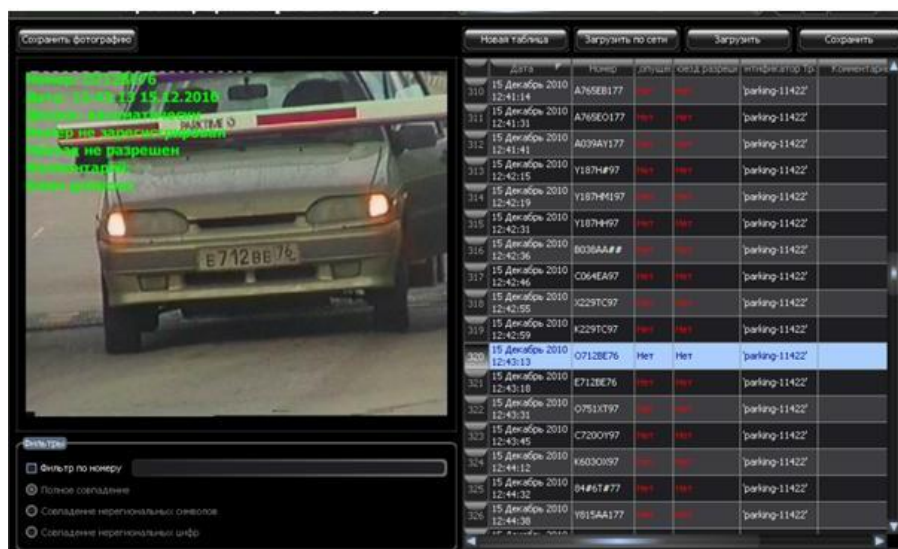


Рисунок 15. Система управления базами данных.

- Распознаватель государственных номерных знаков – элемент автоматического распознавания гос.номеров автомобилей. Занимается обработкой видеоданных от видеокамер распознавания и формирует результат распознавания номера (рис. 16). Может входить только в состав серверов АСУ КТП.

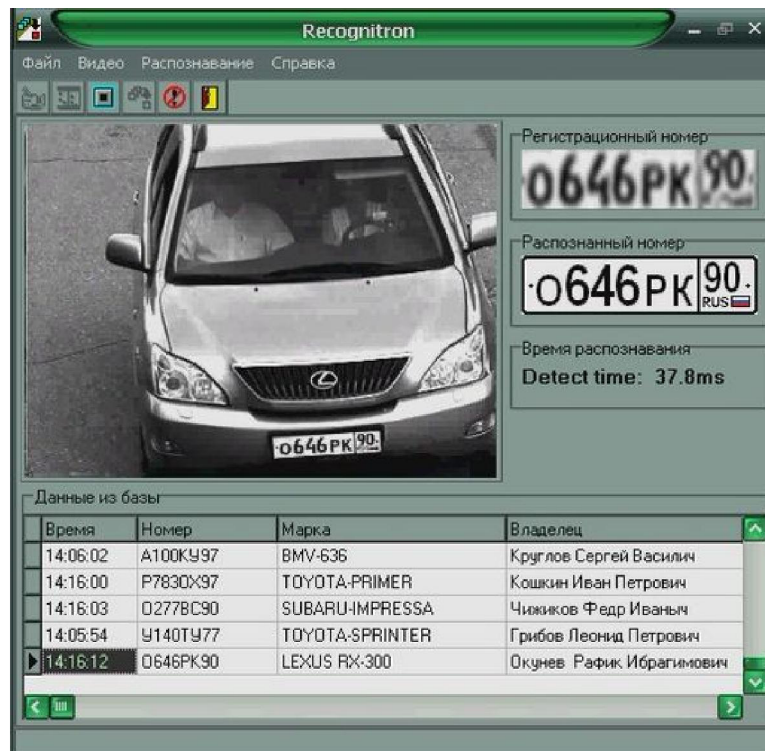


Рисунок 16. Программа распознавателя гос.номеров.

- Элементы светофорной индикации режимов проезда, контроля дополнительных датчиков и/или управления преграждающими устройствами с применением дополнительных средств (контроллеров) (рис. 17).



Рисунок 17. Светофор и датчик движения.

Определение того, что машина проехала шлагбаум или стоит на месте, будет осуществлять датчик RUPARK.

Ультразвуковой датчик присутствия автомобиля предназначен:

- для определения присутствия автомобиля посредством ультразвукового измерения расстояния;
- для выдачи информации на контроллер зоны системы навигации;

Ультразвуковой датчик монтируется на стойке шлагбаума. Надежность работы датчика обеспечивается правильным позиционированием, при установке следует обеспечить параллельность корпуса датчика плоскости пола. Допустимое отклонение не более 10 градусов.

2.6 Выводы по разделу 2

В результате проведенных исследований в области определения состава и структуры комплекса СКУД, выбор основного вычислительного модуля был сделан в пользу платы Argon на базе системы на кристале Nordic Semiconductor nRF52840 было решено организовать сетевую систему контроля доступа. Данное решение позволяет нивелировать обширный ряд уязвимостей, предусматривает масштабирование для системы, повышает безопасность ее использования, а также создает возможности для удаленного администрирования и обслуживания. Выбрана ячеистая топология построения сети для системы, анализ спроса и предложения на рынке позволил сделать вывод, что помимо отличных эксплуатационных показателей, такая система востребована и прогрессивна. Компоненты, выбранные для построения системы, отвечают параметрам энергоэффективности, безопасности и экономичности.

3 РАЗРАБОТКА АЛГОРИТМА

Задачей данного этапа разработки системы является составление алгоритма работы. Выполнение задач этапа разработки алгоритма важно как для последующего написания программы, так и для отладки схемотехнического решения.

Алгоритм - совокупность последовательных шагов, схема действий, приводящих к желаемому результату. Необходимо разбить задачу на логические блоки и описывать каждый из них отдельно.

Работу устройства необходимо разбить на несколько блоков: операции, которые реализуют считывание метрик и получение уникального идентификатора для принятия решения о разрешении доступа.

3.1 Принцип работы СКУД с видеофиксацией

Обычно СКУД используются как одна из составляющих интегрированной системы безопасности. Наиболее распространенная интеграция - с системой видеонаблюдения и системой охранной сигнализации.

Алгоритм работы СКУД (рис. 18): каждый сотрудник получает пропуск, содержащий индивидуальный номер (в нашем случае в базу данных охранной системы вносится государственный номер автомобиля сотрудника). У въезда на предприятие или в любую другую подлежащее контролю территорию устанавливаются считыватели - специальные устройства, камеры, считывающие государственный номер машины и кузов автомобиля. Каждый номер содержит соответствующую информацию о правах владельца пропуска. На основе сопоставления этой информации и ситуации, система принимает одно из следующих решений: открывает шлагбаум, фиксирует время въезда на территорию объекта или включает

сигнал тревоги, т.е. красную индикацию светофора или звуковое оповещение. СКУД запоминает все факты въездов и выездов. Эта информация в дальнейшем используется системой для составления разнообразных отчетов. В зависимости от применяемой СКУД на объекте, отдельные ее устройства могут быть объединены в один блок (контроллер со считывателем) или вообще отсутствовать (персональный компьютер). При появлении автотранспорта на въезде/выезде на территорию предприятия или охраняемого объекта камера видеонаблюдения и идентификации проводит операцию считывания гос.номера автомобиля, как картинки, так и рельефа номерного знака, и в случае если он не разборчивый для системы видеофиксации СКУД, то поступает сигнал на главный компьютер оператору. Оператор читает номер, смотрит тип кузова автомобиля, и после этого проверяет его наличие в системе базы данных. Если тип кузова и гос.номер зарегистрирован в базе данных, то оператор подаёт сигнал, что доступ разрешён. Срабатывает зелёная индикация светофора, шлагбаум открывается и автомобиль проезжает на территорию. В обратном случае подаётся сигнал, что в доступе отказано, срабатывает красная индикация светофора или звуковое оповещение.

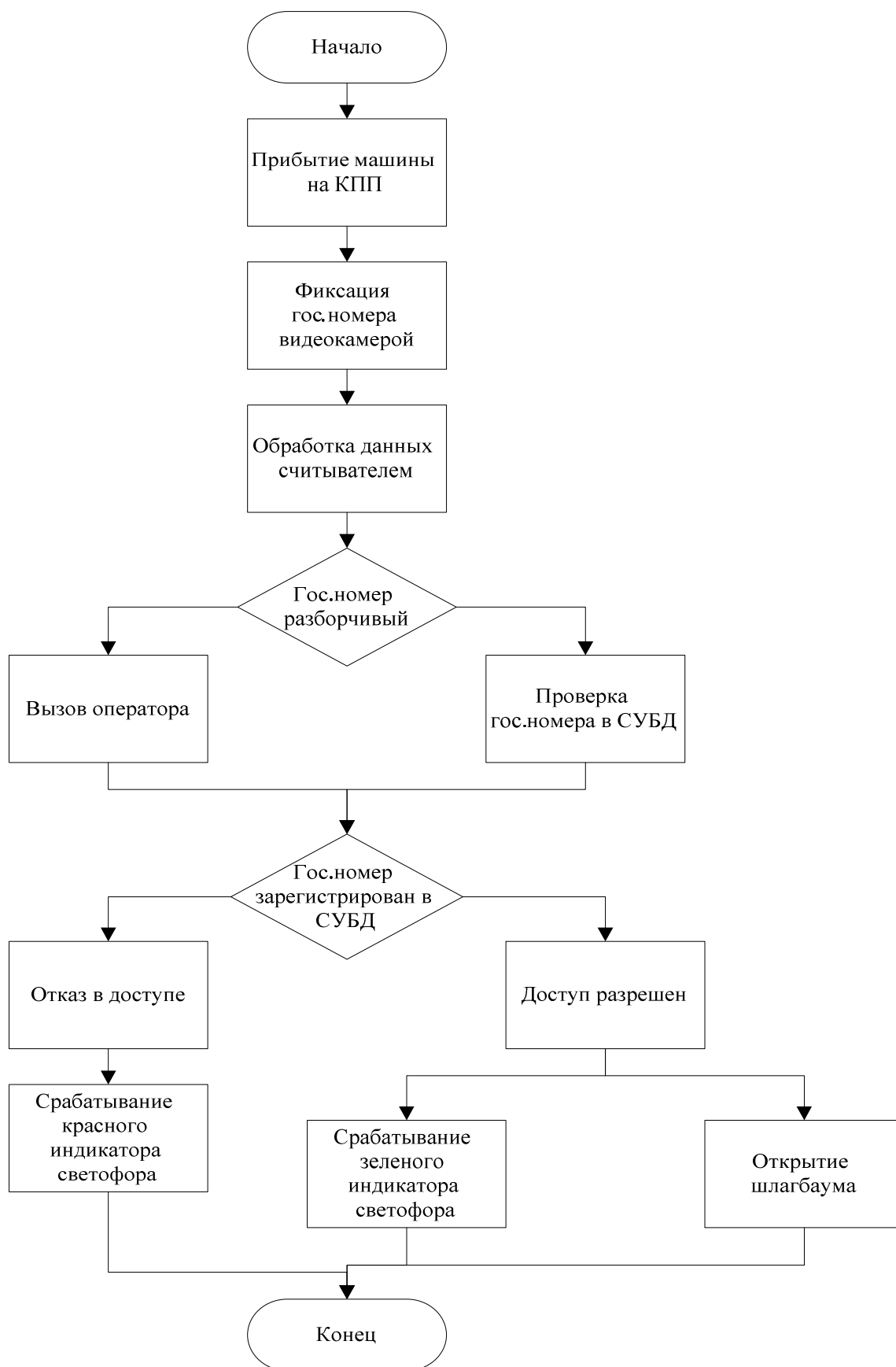


Рисунок 18. Алгоритм работы СКУД.

Контроль доступа на территорию для автомобилей может быть выполнен с логикой распознавания типа кузова по внешнему виду и государственного регистрационного знака транспортного средства. Реализация подобной логики с одновременным считыванием номерного знака автомобиля и типом кузова является средством защиты системы от попытки вызвать ложное срабатывание СКУД в интересах злоумышленника. Аутентификация транспортного средства происходит посредством сравнения фотографических данных, снятых с автомобиля-претендента на въезд и эталонных данных, хранящихся в базе данных. Поисковый запрос в базу данных содержит в себе распознанный государственный номер автомобиля, в случае провала распознавания автомобильного номера, либо несовпадения распознанного номера и кузова эталонной модели администратор получает оповещение

Считыватели СКУД - видеокамеры - являются программно-аппаратными средствами системы.

Контроллеры доступа предназначены для работы в системах контроля и управления доступом (контроллеры СКД). Контроллеры позволяют не только организовать доступ на территорию, но и производить учет рабочего времени, вести табель рабочего времени и пр.

3.2 Считывание автомобильного номера

Система считывает автомобильный гос.номер в несколько этапов. На изображении, полученном с камеры видеофиксации, на КПП предприятия или организации, выделяется область автомобиля, на котором должен быть расположен гос.номер. Среди этих изображений могут оказаться области изображения с другими автомобильными элементами, например, бампер автомобиля, радиаторную решетку или молдинги (рис. 19).

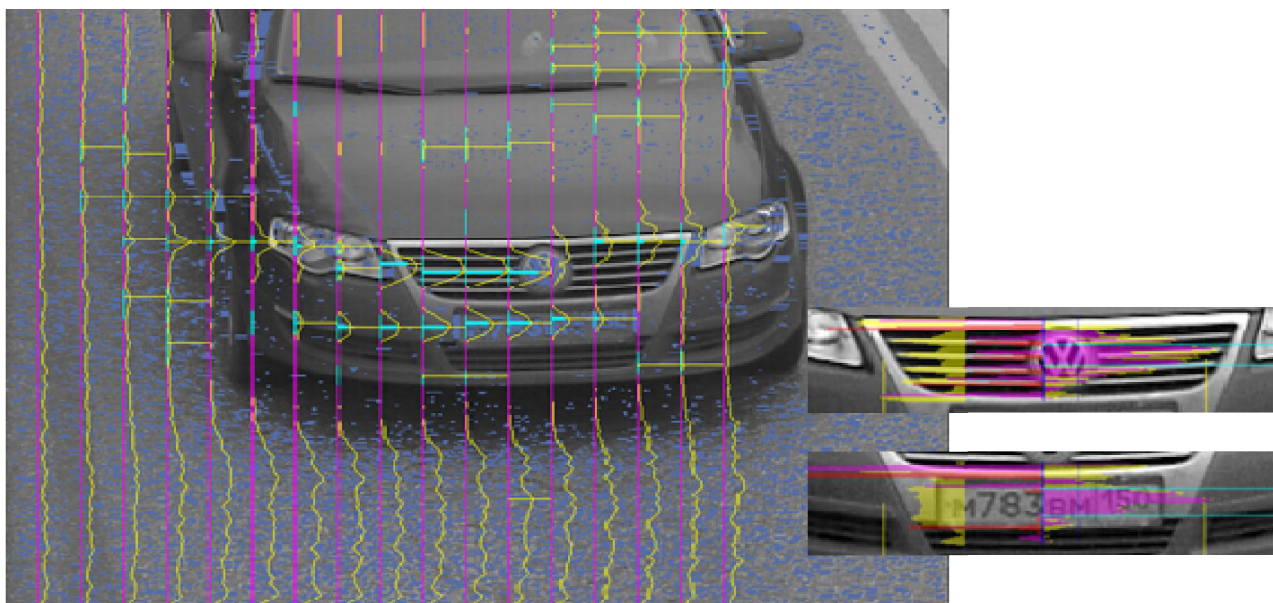


Рисунок 19. Считывание гос.номера по областям.

Выделенные области автомобиля сравниваются с эталонными результатами, записанными в базу данных. Эталонные значения располагают информацией о типах гос.номеров, а так же о параметрах номерных государственных знаков и нормализованные значения объемных позиций. Участки, которые не смогли пройти предварительную проверку с эталоном, получают отказ в доступе на территорию. На данном этапе, по моему мнению, должны определяться точные значения ширины, высоты и геометрии номерного знака, устанавливаться расположение значащих символов (рис. 20).

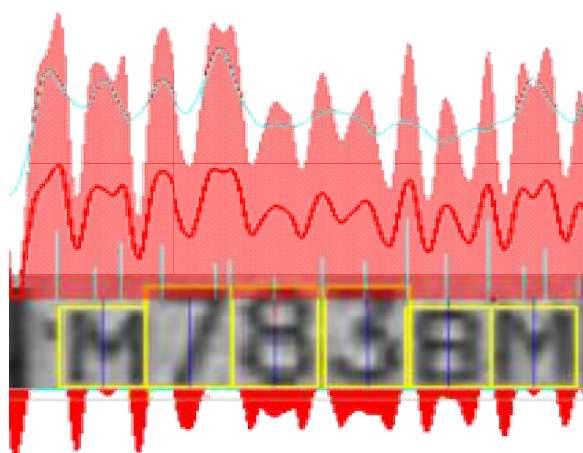


Рисунок 20. Анализ размера номера и совпадения.

Далее происходит распознавание и определение отдельных символов на государственном номерном знаке автотранспорта. Учитывается, что на каждой значащей позиции должен стоять символ из определенного алфавита: существуют позиции, на которых могут быть только цифры, либо только буквы (рис. 21).

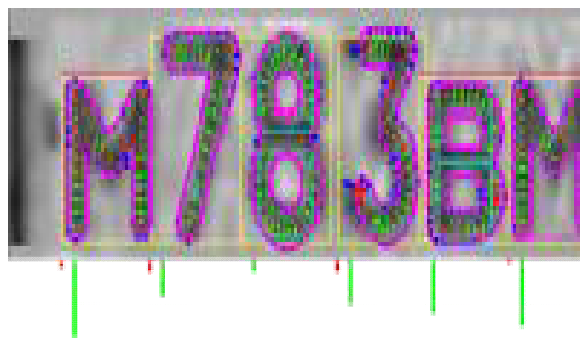


Рисунок 21. Распознавание отдельных символов.

Окончательный результат формируется только после комплексного анализа изображений, относящихся к идентификации автомобиля и определение каждого символа гос.номера, а также формы кузова.

По мнению специалистов, полученному из многочисленных практических ситуаций, на части кадров изображение гос.номера может быть искажено излишним светом фар, уличным искусственным освещением, или затемнено в результате попадания тени на него, что затрудняет распознавание части символов, попавших в искаженную зону. Решить данную проблему возможно посредством совокупности фотографических данных из нескольких кадров, что позволяет привести окончательный вариант государственного регистрационного номера автомобиля к максимально читаемому виду (рис. 22).



Рисунок 22. Распознавание отдельными кадрами.

3.3 Сканирование кузова автомобиля

Сканирование кузова автомобиля производится в несколько шагов. В момент появления автомобиля в так называемом «шлюзе», где происходит проверка автотранспорта (кузова и гос.номера) на наличие его в базе данных предприятия или закрытого охраняемого объекта, камеры видеофиксации и идентификации снимают автомобиль в нескольких проекциях – сверху, снизу и со всех сторон. Для всех зон, отмеченных алгоритмом, производится анализ и сравнение с выбранным эталоном, в котором имеется информация о типах кузова автотранспортного средства (рис. 23).

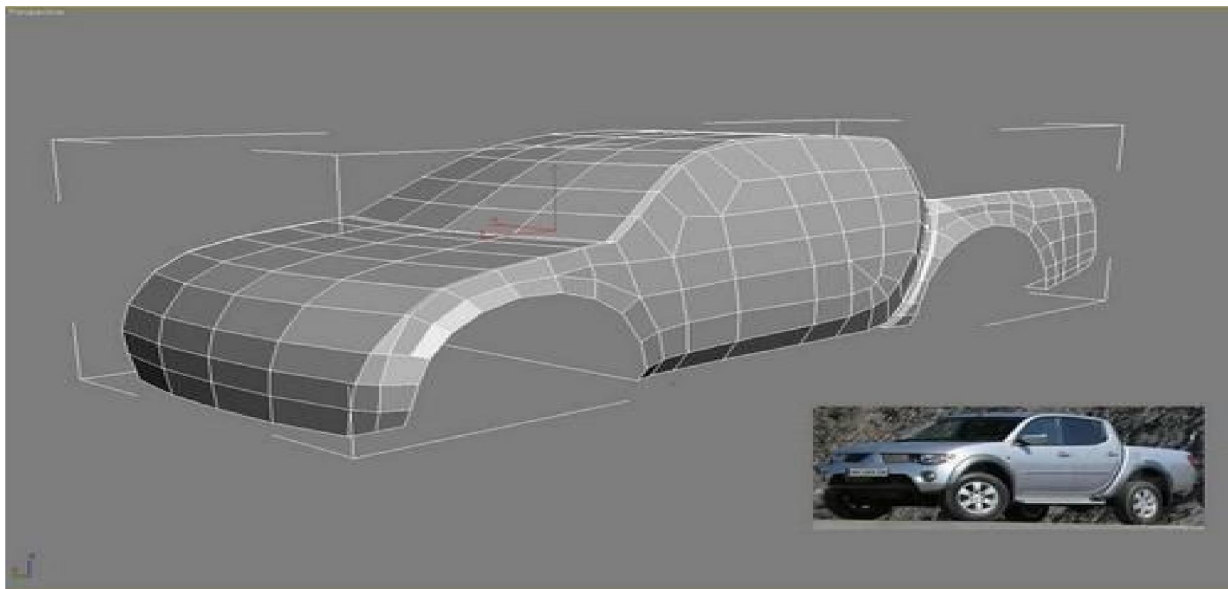


Рисунок 23. Распознавание типа кузова автомобиля.

Для работы с корпусом используется полигональная сетка, которая помогает определить параметры плоскости, округления, выпуклости/вогнутости и фактуру автотранспорта (рис. 24).

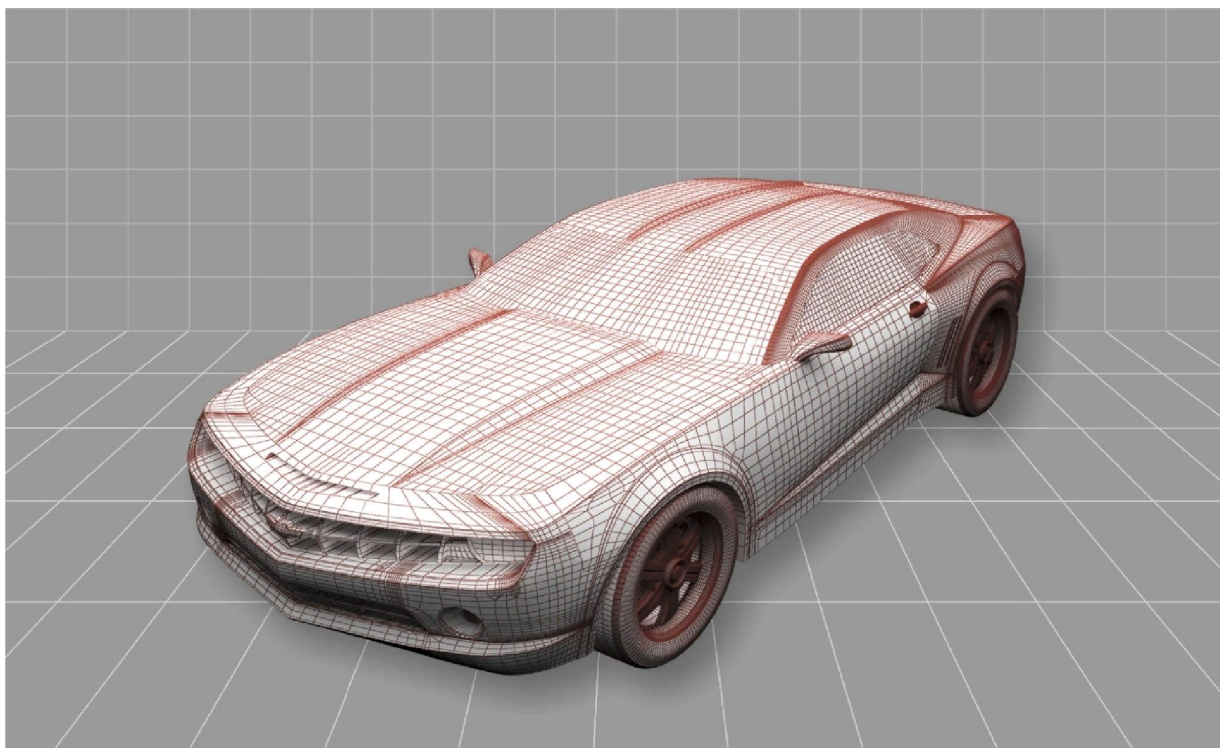


Рисунок 24. Полигональная сетка корпуса автомобиля.

Камера видеофиксации может работать с одной стороной автомобиля, а затем воспользоваться функцией симметричного отображения для получения полного образа кузова автомобиля, который проходит процедуру идентификации при въезде на территорию предприятия или закрытого охраняемого объекта.

Существует необходимость написания дополнительного алгоритма для уменьшения вероятности идентификационного сбоя. Техническая литература и прочие ресурсы по аналогичным разрабатываемой системам указывают на то, что сбой любой системы управления и контроля доступом невозможен, либо его вероятность составляет такой процент, что им можно пренебречь. Тем не менее, если рассматривать актуальные примеры из области устройств, чья функциональность является достижением наукоемкого производства, то стоит обратить внимание на компанию Samsung. Северокорейский производитель техники и умных устройств и смартфонов на базе операционной системы Android был одной из первых компаний, чьи флагманские смартфоны получили дактилоскопический сканнер, расположенный под дисплеем. Это решение и по сей день является конкурентным, сейчас его применяют не только фирмы-гиганты индустрии. Срабатывание подэкранного сканнера отпечатка пальца отличается от уже ставшего стандартным дактилоскопического тем, что в последнем применяется технология оптического анализа поверхности. Направленный маломощный поток фотонов направляется из передающей части датчика в объект на экране, приемная часть фиксирует по комплексным показателям рельеф отраженной поверхности и составляет аналитический портрет поверхности с высокой точностью. В основе работы подэкранных дактилоскопических датчиков заложена технология использования ультразвуковых волн. Электромагнитные волны указанной природы обладают интерференцией, вследствие чего сканируемая поверхность может

быть проанализирована не только в пятне контакта, но и в участках за его пределами. Аналитический эскиз поверхности на экране датчика теоретически работает быстрее и точнее, чем аналог, что повышает его надежность и безопасность. По заявлениям производителя, ультразвуковой дактилоскопический датчик способен работать через стеклопластик толщиной до 800 микрон.

Несмотря на описанные в спецификациях характеристики, крупным компаниям на рынке мобильных устройств было необходимо провести тщательные практические испытания и тесты, чтобы изучить возможность обойти блокировку такой системы контроля доступом. Тесты завершились положительно, ложное срабатывание ультразвукового подэкранного сканнера отпечатка пальца по результатам исследований не выявлено или их процент бесконечно мал. Этот вывод можно сделать на основе того, что смартфоны с таким типом считывателя поступили в продажу и производятся до сих пор.

Репутацию же компании Samsung испортил просчет практического тестирования и посредственный анализ целевой аудитории. Вероятность ложного срабатывания ультразвукового отпечатка пальца возростала до критического значения из-за использования владельцами китайских пленок для защиты экрана устройства от царапин. Частное лицо, настроившее аутентификацию по отпечатку пальца и производшее ее один и более раз создает постоянный отпечаток пальца на клеевом слое пленки посредственного качества. Точность ультразвукового датчика работает в данном случае не в угоду безопасности, так как при активации токопроводящей поверхностью датчика, ультразвуковые волны отражаются от клеевого слоя. Таким образом потенциальный злоумышленник получает доступ к смартфону, к личным данным и банковским счетам владельца.

Это отступление было необходимо для того, чтобы подчеркнуть важность анализа модели поведения злоумышленника, так как система, разрабатываемая в рамках данной работы, является передовым продуктом, и высокая точность и обработка исключительных ситуаций для нее является ключом и главной идеей наряду с гибкостью и практичностью.

В работе распознавания типа кузова автомобиля могут возникнуть некоторые проблемы определения автотранспорта, связанные с его цветом и фактурой, а именно черным цветом и зеркальной гладкой поверхностью. Необходимо также рассмотреть вариант, при котором злоумышленник, пытаясь подделать объемную модель транспортного средства, использует подручные средства, либо подготовленную 3D модель из какого-либо материала. Необходимо предусмотреть алгоритм, сообщающий о посторонних предметах в шлюзе идентификации транспортного средства, так как датчик объема может воспринять их за элемент автомобиля, что приведет к некорректным данным, а также посторонние предметы могут быть использованы злоумышленниками для влияния на результат идентификации. В случае кризисной ситуации СКУД подает сигнал на центральный сервер, после чего администратор обязан в ручном режиме принять решение о разрешении или запрещении доступа. При положительном результате администратор подает сигнал на разрешение проезда на территорию предприятия или закрытого охранного объекта.

3.3 Выводы к разделу 3

В результате проведенного исследования был разработан алгоритм работы СКУД. На данном этапе достигнуты основные цели, поставленные перед магистерской диссертацией. Алгоритм считывания автомобильного номера и определения типа кузова автотранспорта является достаточно точным, что позволяет использовать автомобильный номер и модель кузова

в качестве уникального идентификатора транспортного средства. Существует необходимость в доработке алгоритма как для увеличения устойчивости и безопасности системы, так и уменьшения вероятности ложного срабатывания последней. Для создания алгоритмов, реализующих защитный протокол, необходимо провести практическое тестирование системы, так как теоретический анализ не позволит с достаточной точностью установить недостатки и просчеты алгоритма.

4 ЗАКЛЮЧЕНИЕ

В ходе выполнения магистерской диссертации был разработан алгоритм системы контроля и управления доступом. Разработанная система может быть внедрена на предприятиях, так как она проста во внедрении, эксплуатации и отличается низкой стоимостью.

Описываемый в этой работе алгоритм является технологичной платформой. По данному шаблону может быть построена система на передовых технологиях, которые предлагают разработчики аппаратных платформ. Использование стандартной для подобных систем топологии сетей позволяет пройти проверку соответствия требованиям текущих ГОСТ, и как следствие сертифицировать систему для внедрения на объекты государственного уровня.

В магистерской диссертации приведены общие описания технологий, а также алгоритм работы системы. Существует возможность конфигурировать продукт на основе описанного решения, так как у описанного алгоритма в свою очередь заложен огромный запас гибкости. При обновлении входных условий и составления технического задания, как аппаратная, так и программная платформы могут подвергнуться модернизации, они будут сконфигурированы в соответствии с требованиями технического задания и особенностями структуры, в которую данная система может быть внедрена. В достижении этой особенности хочется отметить технологию Feather, которая позволяет подстраиваться под задачи средствами «горячей» замены компонентов, развернутый функционал которых описан в разделах данной работы.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Т. Шарфельд. Системы RFID низкой стоимости. М.: Москва, 2006 с. 6-11.
2. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.
3. ГОСТ Р 54831-2011 Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний.
4. «Машинное зрение. Что это и как им пользоваться? Обработка изображений оптического источника» - Хабр, электронный научно-популярный журнал. URL: <https://habr.com/ru/post/350918/> (дата обращения: 30.05.2020).
5. «Регистрация транспорта в СКУД» - Биометрические системы BIO5. URL: <http://www.bio5.ru/articles/kontrol-dostupa/registratsiya-transporta-v-skud.html> (дата обращения: 29.05.2020).
6. «UHF vs. HF RFID: новый взгляд на старую полемику» - электронный журнал Secutech. URL: http://lib.secuteck.ru/articles2/sys_ogr_dost/uhf-vs-hf-rfid-novy-vzglyad-na-staruyu-polemiku (дата обращения: 29.05.2020).
7. Электронный ресурс просмотра статистики поисковых запросов «Подбор слов. Яндекс». URL: <https://wordstat.yandex.ru/> (дата обращения: 14.05.2020).
8. Ракутин, А.Н. Учет автотранспорта в СКУД / А.Н. Ракутин // Каталог СКУД. Антитерроризм, 2010.
9. Лахири. С. RFID. Руководство по внедрению. М.: КУДИЦ-ПРЕСС. – 2007. – 312с.

10. Умнов, А.В. RFID-технология в автомобильных СКУД / А.В. Умнов // Каталог СКУД. Антитерроризм, 2004.
11. Катренко А.В. Беспроводные СКУД: еще раз про технологии, терминологию и заблуждения / А.В. Катренко // Журнал «Системы безопасности», 2014 стр. 104-106
12. «Система контроля и управления доступом» - Википедия, свободная электронная энциклопедия. URL: https://ru.wikipedia.org/wiki/Система_контроля_и_управления_доступом (дата обращения: 15.05.2020).
13. Выбор и применение систем контроля и управления доступом. Рекомендации: Документ № Р 78.36.005-99 [Министерство внутренних дел, от 31 марта 1998г.]
14. Particle Argon: Wi-Fi + Bluetooth specification – электронный ресурс, документация на изделие. URL: <https://docs.particle.io/argon/> (дата обращения: 20.05.2020)

Приложение А Презентация