МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»
Институт космической инженерии и телекоммуникаций
Кафедра электроники и робототехники

«ДОПУЩЕН К ЗАЩИТЕ»
Зав.кафедрой доц., Чигамбаев Т.О.
_____ «___» _____20__г.
(подпись)

ДИПЛОМНАЯ РАБОТА

На тему: «Промышленный прибор для контроля доступа с применением технологии биометрической идентификации»
Специальность «5В071600 – Приборостроение»
Выполнил Жангаскиев А.Ж.
Научный руководитель доцент Юсупова С.А.

_____ «___» _____20__г.
(подпись)

Консультанты:
по экономической части: ст.преп., Боканова Г.Ш.

_____ «___» _____20__г.
(подпись)

по безопасности жизнедеятельности: к.т.н., доц., Приходько Н.Г.

_____ «___» _____20__г.
(подпись)

Нормоконтролер: ст. преп., Фазылова А.Р.

_____ «___» _____20__г.
(подпись)

Рецензент: к.т.н., профессор Пя Д.Р.
_____ «___» _____20__г.
(подпись)

Алматы 2020

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»

Институт космической инженерии и телекоммуникаций
Специальность «5В071600 –Приборостроение»
Кафедра «Электроника и робототехника»

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Жангаскиеву А.Ж.

Тема работы «Промышленный прибор для контроля доступа с применением технологии биометрической идентификации» утверждена приказом ректора № ___ от ___ сентября 2020 г.

Срок сдачи законченной работы «__» мая 2020г.

Исходные данные к проекту (требуемые параметры результатов проектирования) и исходные данные:

а) Система управления (СУ) системы контроля и управления доступом (СКУД).

б) Программно-техническая платформа (ПТП) Arduino.

Требуется:

Разработать техническое предложение по реализации заданной СУ СКУД на базе функций, предоставляемых ПТП Arduino, обеспечивающую требуемую эффективность по показателям, определенным в соответствии с предложенной системой критериев.

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

1) инженерный анализ (общие сведения об имеющихся биометрических системах управления и контроля доступа, обоснование сферы применения разрабатываемой системы);

2) обзор СКУД с биометрической идентификацией;

3) моделирование прибора;

4) программное обеспечение;

5) бизнес-план;

6) безопасность жизнедеятельности (расчет защиты от электромагнитных полей и излучений).

Перечень графического материала (с точным указанием обязательных чертежей): в данной работе содержится 22 рисунка и 16 таблиц.

Рекомендуемая основная литература:

1) Сайт: https://www.arduino.cc/ «Официальный сайт Arduino»

2) Сайт: https://www.c-cpp.ru/ «Программирование на С и С++»

3) Г.Ш. Боканова. Методические указания к выполнению экономической части дипломных работ для студентов специальности 5В071900 – Радиотехника, электроника и телекоммуникаций. – Алматы: АУЭС, 2020 – 26 с.

4) М.К. Дюсебаев, Ж.С. Абдимуратов. Безопасность жизнедеятель-ности. Учебное пособие для студентов всех форм обучения специальности 050718 – Электроэнергетика – Алматы: АУЭС, 2010 – 81 с.

Консультанты по проекту с указанием относящихся к ним разделов работы.

Раздел	Консультант	Сроки	Подпись
Инженерный анализ	Юсупова С.А.	29.03.20	
Обзор систем контроля и управления доступа	Юсупова С.А.	03.04.20	
Конструирование прибора	Юсупова С.А.	23.04.20	
Описание опытного образца	Юсупова С.А.	15.05.20	
Экономическая часть	Боканова Г.Ш.	10.04.20	
Безопасность жизнедеятельности	Приходько Н.Г.	11.04.20	

ГРАФИК
подготовки дипломного проекта

№ п/п	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления руководителю	Примечание
1	2	3	4
1	Инженерный анализ	29.03.20	
2	Обзор систем контроля и управления доступа	03.04.20	
3	Конструирование прибора	11.05.20	
4	Программное обеспечение	11.05.20	
5	Экономическая часть	25.04.20	
6	Безопасность жизнедеятельности	26.04.20	

Дата выдачи задания «___» _____ 2020 г.

Заведующий кафедрой _____ Чигамбаев Т.О.

Руководитель _____ Юсупова С.А.

Задание принял к исполнению
студент _____ Жангаскиев А.Ж.
(подпись)

Аңдатпа

Бұл дипломдық жұмыста бақылау және деректерді басқаруға арналған биометриялық жүйенің, сәйкестендіру құрылғыларының әзірлеуін қарастырады, сонымен қатар биометриялық сәйкестендірумен қол жеткізетін басқару жүйелерінің даму кезеңдері қарастырылады. Зерттеу объектісі Arduino Uno контроллері зерттелді. Әзірлеу және модельдеуге арналған жабдық таңдалды. Салыстырмалы талдау негізінде тапсырманы орындау үшін таңдау негізделді. Жұмыста алақан тамырларының суретін қолдана отырып, деректерді оқитын биометриялық авторизациясы бар өнімді құру арқылы мәселенің шешімі көрсетілген. Процесс барысында келесі бағдарламалау орталары қолданылды: C / C ++, Arduino, Proteus (электронды схемаларды автоматтандырылған жобалауға арналған бағдарламалық пакет).

Аннотация

В данной дипломной работе исследованы вопросы разработки биометрической системы для контроля и управления данными, устройств идентификации, также рассмотрены этапы развития СКУД с биометрической идентификацией. Изучен объект исследования контроллера Arduino Uno. Выбрано оборудование для разработки и моделирования. Основываясь на сравнительный анализ обоснован выбор для решения поставленной задачи. В работе показано решение задачи посредством создания продукта с биометрической авторизацией, который считывает данные при помощи рисунка вен ладони. В процессе работы использовались следующие среды программирования: C/C++, Arduino, Proteus (пакет программ для автоматизированного проектирования электронных схем).

Annotation

This diploma project examines the development of a biometric system for monitoring and data management, identification devices, and also discusses the stages of development of access control systems with biometric identification. Arduino Uno controller research object studied. Equipment for development and modeling was selected. Based on a comparative analysis, the choice is justified for solving the task. The work shows the solution of the problem by creating a product with biometric authorization, which reads data using a drawing of the veins of the palm. In the process, the following programming environments were used: C/C++, Arduino, Proteus (software package for the automated design of electronic circuits).

Содержание

Введение 7
1 Анализ технологий биометрической идентификации СКУД 11
1.1 Современные представления о технологиях биометрической идентификации для контроля и управления доступом 11
1.2 Технологии биометрической идентификации 11
1.3 Критерии биометрической идентификации 12
1.4 Сравнительный анализ основных методов биометрической идентификации 13
1.5 Анализ биометрической идентификации по рисунку вен 21
1.6 Идентификация в облаке: Morpho Cloud 23
1.7 Биометрическая аутентификация на мобильных устройствах 23
2 Обзор существующих СКУД с технологиями биометрии 25
2.1 Терминал BioSmart PV-WTC 25
2.2 Технологии распознавания по рисунку вен Fujitsu Palm Secure, терминал FPS ID Access 33
3 Конструирование и моделирование прибора 36
3.1 Выбор оборудования 36
3.2 Структурная схема 42
3.3 Разработка электрической принципиальной схемы на основе платформы Arduino 47
4 Бизнес – план 50
4.1 Резюме 50
4.2 Характеристика предлагаемого продукта 50
4.3 Анализ рынка сбыта 51
4.4 Организационный план 52
4.5 Расчет капитальных затрат 52
4.6 Годовые эксплуатационные расходы 53
4.7 Расчет доходов, прибыли и чистой прибыли 56
4.8 Оценка срока окупаемости проекта с учетом фактора времени 57
4.9 Выводы 61
5 Безопасность жизнедеятельности 62
5.1 Анализ потенциально опасных и вредных факторов, воздействующих на персонал при работе с персональным компьютером (ПК) 62
5.2 Расчетная часть 66
5.3 Выводы 70
Заключение 72
Список литературы 73
Приложение А 75

Введение

В течение долгих лет разработки были созданы информационные системы для биометрической идентификации людей (далее именуемые информационными биометрическими системами), которые широко распространены сегодня и контролируют физический доступ и доступ к конфиденциальной информации. Области, в которых сложно переоценить степень надежности биометрических информационных систем, пограничного контроля, воздушного транспорта и доступа к информации, содержащей государственные секреты. Одним из важных применений информационных биометрических систем является идентификация читателей публичных библиотек (включая онлайн-читателей) с целью обеспечения надежного контроля и учета доступа к различным публикациям, особенно ценным. В качестве биометрического идентификатора используются человеческий голос, почерк, радужная оболочка, отпечатки пальцев. В условиях высокого развития информационных и технических средств современного мира исследуемая тема является очень актуальной. В работе представлены основной принцип действия биометрических систем контроля и управления доступом, их классификация, преимущества и сфера применения. Объектом – выступают указанные системы.

Исследования биометрических информационных систем показали, что при существующих технологиях биометрической идентификации невозможно гарантировать правильную идентификацию с вероятностью 100%. В то же время расширяющаяся область применения технологий биометрического распознавания предъявляет все более строгие требования к показателям качества информационных биометрических систем. Результаты испытаний этих систем показывают, что ни одна из них не может обеспечить достаточную точность для идентификации человека в больших объемах данных в автоматическом режиме. Сегодня метки радиочастотной идентификации (RFID – Radio Frequency Identification - радиочастотная идентификация) активно используются для идентификации читателей библиотек и фондовых фондов, но в случаях контроля доступа к ценным публикациям (рукописи, редкие книги) более надежными средствами идентификации читателей являются биометрические идентификаторы. [1]

В настоящее время повышение точности биометрических информационных систем является актуальной научной и практической проблемой.

Необходимо учитывать тот факт, что решение этой проблемы осложняется действиями (атаками) злоумышленников, которые распространились в контексте расширения области применения биометрических информационных систем. Поэтому сегодня важно разработать методы и средства для повышения точности, которые повышают устойчивость биометрических информационных систем к атакам.

Степень разработанности проблемы. Значительный вклад в развитие биометрических информационных систем связан с именами известных исследователей биометрии А. Джейн, Р. Болла, Д. Веймана, А. Росса, В. Улудага, Д. Рейсмана, С. Панканти, Н. Рата (США), Д. Мал-Тони, Д. Майо, Р. Капелли (Италия), Л. Хонг (Китай), С. Ли (Япония), В. Дикманн (Германия) и др. В работе этих авторов были заложены основы современных технологий биометрической идентификации, разработаны стандарты и алгоритмы для применения соответствующих технологий.

Во всех исследованиях проблемы, связанные с повышением точности биометрических информационных систем, работающих в условиях атаки, а также проблемы, связанные со стабильностью инструментов и методов, разработанных для повышения точности против атак, были не полностью изучены.

Биометрия – понятие комплексное. Она охватывает набор различных технологий и методов, благодаря которым возможно провести идентификацию конкретной личности. В основу этого комплекса положены биологические данные человека. Человек обладает сугубо индивидуальными характеристиками, в т. ч. и физиологическими. Биометрические системы контроля доступа сегодня приобретают огромную популярность. Это связано с прогрессирующим усовершенствованием техники, позволяющей исследовать природные данные человека. Конечно, биометрические системы имеют свои преимущества и недостатки. Неоспоримым преимуществом является способ идентификации. Во-первых, физиологические параметры достаточно уникальны. Во-вторых, их невозможно утерять, в отличие от электронных ключей доступа.

Объектом исследования дипломной работы являются контроль доступа с применением биометрических технологий идентификации по рисунку вен. Выбор объекта исследования обусловлен высокой степенью надежности, огромным потенциалом в этой отрасли и специфическими индивидуальными свойствами используемых идентификаторов (венозные паттерны).

Предметом данной работы являются методы и средства повышения точности биометрических информационных систем для выявления закономерностей вен на основе классических алгоритмов идентификации.

Целью работы является исследование возможностей повышения точности идентификации информационных биометрических систем, основанных на классических алгоритмах идентификации отпечатков пальцев, используя методы интеграции биометрической информации. Для достижения поставленной цели необходимо решить следующие задачи:

а) провести сравнительный анализ известных методов биометрической идентификации, их «точностных» возможностей;

б) провести анализ ошибок, возникающих при работе информационных биометрических систем, и их влияния на точность идентификации;

в) разработать новый метод (алгоритм) повышения точности идентификации. Выполнить практическую проверку эффективности предложенного метода (алгоритма);

г) разработать алгоритмы и программную реализацию информационной биометрической системы, обеспечивающей повышение точности;

д) провести моделирование разработанной информационной биометрической системы, в том числе в условиях атаки злоумышленников, и оценить ее эффективность.

В данной работе используются методы теории вероятностей и математической статистики, методы распознавания образов, компьютерное программирование и моделирование.

Изучение возможностей повышения точности идентификации информационных биометрических систем на основе венозного рисунка.

Метод был разработан для повышения точности идентификации биометрической информационной системы на основе традиционных алгоритмов идентификации в соответствии с венозной схемой и использованием интеграции измерений того же типа. Этот метод доказал свою инвариантность по отношению к сканирующим устройствам и конкретной реализации классического алгоритма идентификации.

Были изучены проблемы уязвимости биометрических информационных систем к атакам, и были внесены предложения по компенсации несанкционированных воздействий.

Разработанный метод повышения точности идентификации биометрических информационных систем дает возможность получать, накапливать, обрабатывать полученную информацию измерений и принимать решения относительно представленных идентификаторов.

Разработаны структурные и функциональные схемы информационной биометрической системы и модуля атаки, алгоритмов и программного обеспечения, которые могут быть использованы как при проектировании новых информационных биометрических систем, так и для установки в существующих системах на основе классических алгоритмов для определения структуры вен. Разработанный метод является инвариантным по отношению к сканирующему устройству и программной реализации классического алгоритма сравнения венозных моделей.

Положения, выносимые на защиту:

а) метод, разработанный в результате исследования и основанный на классических алгоритмах для определения структуры вен и интеграции той же информации, может повысить точность идентификации;

б) предложенная функциональная схема и алгоритмы работы, комбинированной биометрической информационной системы устойчивы к возможным атакам на канал передачи изображений;

в) предложенный алгоритм атаки на канал передачи изображения

позволяет тестировать информационные системы биометрической идентификации на предмет уязвимости к атакам независимо от конкретной реализации классического алгоритма для определения рисунка вен и используемых сканирующих устройств.

1 Анализ технологий биометрической идентификации СКУД

1.1 Современные представления о технологиях биометрической идентификации для контроля и управления доступом

Система контроля и управления доступом (СКУД) – это совокупность специализированного оборудования и программного обеспечения, предназначенного для организации на заданной территории системы ограничения, регистрации и контроля доступа людей и транспорта через «точки прохода» (двери, ворота, КПП и др.).

Биометрическая система контроля и управления доступом позволяет распознавать людей по их физическим индивидуальным особенностям (отпечатки пальцев либо ладони, сетчатке радужной оболочки глаз, голосу, чертам лица, форме кисти руки, ДНК и др.). Таким образом, качество контроля и безопасности системы значительно повышается, снижается риск несанкционированного проникновения и обмана системы.

В настоящее время биометрические системы контроля доступа очень востребованы покупателями, что повлияло на готовность производителей развивать отрасль и технологии, расширять номенклатуру и характеристики оборудования. Современные технологии позволяют интегрировать его практически в любую систему действующего СКУД. Само оборудование стало функциональней, легче, компактней, удобней в эксплуатации и доступней по стоимости. Несколько лет назад установку такой системы могли себе позволить только крупные предприятия, сейчас спектр заказов расширился от локальных систем (на одну дверь), до крупных сетевых структур территориально-распределенных объектов. Оборудование стало широко применяться не только в банках и особо охраняемых учреждениях, но и в обычных офисах, школах, больницах, санаториях, жилых домах (частных и многоквартирных) и др.

Биометрическая идентификация - это представление пользователем его уникального биометрического параметра и процесс его сравнения со всей базой доступных данных. Биометрические считыватели используются для извлечения, такого типа персональных данных.

Биометрические системы контроля доступа удобны для пользователей, так как носители данных всегда с ними, их нельзя потерять или украсть. Биометрический контроль доступа считается более надежным, поскольку идентификаторы не могут быть переданы третьим лицам, скопированы.

1.2 Технологии биометрической идентификации

Методы биометрической идентификации:

а) статические, основанные на физиологических признаках человека, присутствующих с ним на протяжении всей его жизни:

1) идентификация по отпечатку пальца;
2) идентификация по лицу;
3) идентификация по радужной оболочке глаза;

4) идентификация по геометрии руки;
5) идентификация по термограмме лица;
6) идентификация по ДНК;
7) идентификация на основе акустических характеристик уха;
8) идентификация по рисунку вен;

б) динамические берут за основу поведенческие характеристики людей, а именно подсознательные движения в процессе повторения какого-либо обыденного действия: почерк, голос, походка:

1) идентификация по голосу;
2) идентификация по рукописному почерку;
3) идентификация по клавиатурному почерку;
4) и др.

Одним из главных типов поведенческой биометрии является стиль набора на клавиатуре. При ее определении скорость печати, нажатие на клавиши, продолжительность нажатия клавиши, интервалы времени между нажатиями фиксированы.

Отдельным биометрическим фактором может быть способ использования мыши. Кроме того, поведенческая биометрия охватывает большое количество факторов, не связанных именно с компьютером, особенностью является, что фактором может стать, даже то, как человек поднимается по лестнице.

Существуют также системы идентификации, объединенные с использованием различных биометрических характеристик, которые могут удовлетворить самые строгие требования к надежности и безопасности систем контроля доступа. [2]

1.3 Критерии биометрической идентификации

Для определения эффективности СКУД на основе биометрической идентификации используют следующие показатели:

– FAR - коэффициент ложного пропуска;

– FMR - вероятность, что система неверно сравнивает входной образец с несоответствующим шаблоном в базе данных;

– FRR - коэффициент ложного отказа;

– FNMR - вероятность того, что система ошибётся в определении совпадений между входным образцом и соответствующим шаблоном из базы данных;

– график ROC - визуализация компромисса между характеристиками FAR и FRR;

– коэффициент отказа в регистрации (FTE или FER) – коэффициент безуспешных попыток создать шаблон из входных данных (при низком качестве последних);

– коэффициент ошибочного удержания (FTC) - вероятность того, что автоматизированная система не способна определить биометрические входные данные, когда они представлены корректно;

– емкость шаблона - максимальное количество наборов данных, которые могут храниться в системе.

В Республике Казахстан использование персональных данных преследуется Статьей 14 Конституционного закона «Использование персональных данных» № 94-V от 21.05.2013 г. (с изменениями и дополнениями по состоянию на 28.12.2017 г.). [3]

1.4 Сравнительный анализ основных методов биометрической идентификации

1.4.1 Сравнение методов биометрической аутентификации с использованием математической статистики (FAR и FRR)

Главными, для оценки любой биометрической системы, являются два параметра:

FAR (False Acceptance Rate) - коэффициент ложного пропуска, т.е. процент возникновения ситуаций, когда система разрешает доступ пользователю, незарегистрированному в системе.

FRR (False Rejection Rate) - коэффициент ложного отказа, т.е. отказ в доступе настоящему пользователю системы.

Обе характеристики получены расчетным путем на основе методов математической статистики. Чем ниже эти показатели, тем точнее распознавание объекта.

Для самых популярных сегодня методов биометрической идентификации средние значения FAR и FRR представлены в таблице 1.1 и имеют следующий вид:

Таблица 1.1 – Средние значение FAR и FRR

Биометрическая СКУД использует:	FAR	FRR
Отпечаток пальца	0,001%	0,6%
Распознавание лица 2D	0,1%	2,5%
Распознавание лица 3D	0,0005%	0,001%
Радужная оболочка глаза	0,00001%	0,016%
Сетчатка глаза	0,0001%	0,4%
Рисунок вен	0,0008%	0,01%

Но для создания эффективной системы контроля доступа FAR и FRR параметры недостаточно совершенны. Например, сложно представить СКУД на основе анализа ДНК, хотя при этом методе аутентификации эти факторы

стремятся к нулю. Но время идентификации увеличивается, увеличивается влияние человеческого фактора, неоправданно увеличиваются затраты на систему.

Поэтому для качественного анализа биометрической системы контроля доступа необходимо использовать другие данные, которые иногда можно получить только экспериментально.

Прежде всего, такие данные должны включать возможность фальсификации биометрических данных для идентификации в системе и способы повышения уровня безопасности.

Во-вторых, стабильность биометрических факторов: их неизменность во времени и независимость от условий окружающей среды.

Как логическое следствие, скорость аутентификации, возможность быстрого получения бесконтактных биометрических данных для идентификации.

И, конечно, затраты на внедрение биометрической системы управления доступом на основе рассматриваемого метода аутентификации и доступности компонентов.

1.4.2 Сравнение биометрических методов по устойчивости к фальсификации данных

Фальсификация биометрических данных в любом случае является довольно сложным процессом, часто требующим специальной подготовки и технической поддержки. Но если вы можете смоделировать отпечаток пальца в домашних условиях, успешная подделка радужной оболочки еще не известна. А для биометрических систем аутентификации на сетчатке создать фальшивку просто невозможно (таблица 1.2).

Таблица 1.2 – Сравнение биометрических методов по устойчивости к фальсификации данных

Биометрическая СКУД использует:	Фальсификация
Отпечаток пальца	Возможна
Распознавание лица 2D	Возможна
Распознавание лица 3D	Проблематична
Радужная оболочка глаза	Безуспешна
Сетчатка глаза	Невозможна
Рисунок вен	Невозможна

1.4.3 Сравнение биометрических методов по возможности строгой аутентификации

Повышение уровня безопасности биометрической системы контроля доступа обычно достигается с помощью программных и аппаратных методов. Например, технология «живой палец» для отпечатков пальцев, анализ непроизвольного тряски глаз. Чтобы повысить уровень безопасности, биометрический метод может быть одним из компонентов системы многофакторной аутентификации (таблица 1.3).

Включение дополнительных программ безопасности в программно-аппаратный комплекс обычно довольно значительно увеличивает его стоимость. Однако для некоторых методов возможна строгая аутентификация на основе стандартных компонентов: использование нескольких шаблонов для идентификации пользователя (например, рисунок вен).

Таблица 1.3 – Сравнение биометрических методов по возможности строгой аутентификации

Биометрическая СКУД использует:	Строгая аутентификация (один фактор)
Отпечаток пальца	Возможна
Распознавание лица 2D	Нет
Распознавание лица 3D	Нет
Радужная оболочка глаза	Возможна
Сетчатка глаза	Возможна
Рисунок вен	Возможна

1.4.4 Сравнение методов аутентификации по неизменности биометрических характеристик

Постоянные биометрические характеристики с течением времени также являются условными: все биометрические параметры могут изменяться в результате медицинской операции или травмы. Но если обычная домашний порез, который может затруднить проверку пользователя по отпечатку пальца, является нормальной ситуацией, то операция, которая меняет рисунок радужной оболочки, является редкостью (таблица 1.4).

Таблица 1.4 – Сравнение методов аутентификации по неизменности биометрических характеристик

Биометрическая СКУД использует:	Неизменность характеристики
Отпечаток пальца	Низкая
Распознавание лица 2D	Низкая

Продолжение таблицы 1.4

Распознавание лица 3D	Высокая
Радужная оболочка глаза	Высокая
Сетчатка глаза	Средняя
Рисунок вен	Средняя

1.4.5 Сравнение по чувствительности к внешним факторам

Влияние параметров окружающей среды на производительность систем контроля доступа зависит от алгоритмов и технологий работы, применяемых производителем оборудования, и может значительно различаться даже в рамках одного биометрического метода. Ярким примером таких различий могут служить считыватели отпечатков пальцев, которые, как правило, достаточно чувствительны к воздействию внешних факторов (таблица 1.5).

Таблица 1.5 – Сравнение по чувствительности к внешним факторам

Биометрическая СКУД использует:	Чувствительность к влиянию внешних факторов
Отпечаток пальца	Высокая
Распознавание лица 2D	Высокая
Распознавание лица 3D	Низкая
Радужная оболочка глаза	Средняя
Сетчатка глаза	Высокая
Рисунок вен	Средняя

Если мы сравним другие методы биометрической идентификации, наиболее чувствительным будет распознавание лица в 2D: здесь, наличие очков, шляпы, новой прически или заросшей бороды может стать критическим.

Системы, использующие метод аутентификации сетчатки, требуют довольно жесткого положения глаза относительно сканера, неподвижности пользователя и фокусировки самого глаза.

Методы идентификации пользователя, основанные на рисунках вен и радужных оболочках, относительно стабильны в работе, если вы не пытаетесь использовать их в экстремальных условиях работы (например, бесконтактная аутентификация на большом расстоянии во время "грибного" дождя).

Трехмерная идентификация лица наименее чувствительна к влиянию внешних факторов. Единственный параметр, который может повлиять на работу такой СКУД, - это чрезмерное освещение.

1.4.6 Сравнение по скорости аутентификации

Скорость аутентификации зависит от времени захвата данных, размера модели и количества ресурсов, выделенных для ее обработки, а также от основных программных алгоритмов, используемых для реализации конкретного биометрического метода (таблица 1.6).

Таблица 1.6 – Сравнение по скорости аутентификации

Биометрическая СКУД использует:	Скорость аутентификации
Отпечаток пальца	Высокая
Распознавание лица 2D	Средняя
Распознавание лица 3D	Низкая
Радужная оболочка глаза	Высокая
Сетчатка глаза	Низкая
Рисунок вен	Высокая

1.4.7 Сравнение по возможности бесконтактной аутентификации

Бесконтактная аутентификация предлагает много преимуществ использования биометрических методов в системах физической безопасности в учреждениях с высокими гигиеническими и санитарными требованиями (медицина, пищевая промышленность, научно-исследовательские институты и лаборатории). Кроме того, идентификация удаленного объекта ускоряет процесс проверки, что важно для больших систем контроля доступа с высокой скоростью потока. Кроме того, правоохранительные органы могут использовать бесконтактную идентификацию в целях нац. безопасности. Вот почему ученые пытаются разработать системы бесконтактной аутентификации на основе отпечатков пальцев, но пока не достигли

стабильных результатов. Особенно эффективны методы, которые фиксируют биометрические характеристики объекта на большом расстоянии и во время движения. С распространением камер наблюдения с высоким качеством изображения, реализация этого принципа работы становится все проще (таблица 1.7).

Таблица 1.7 – Сравнение по возможности бесконтактной аутентификации

Биометрическая СКУД использует:	Бесконтактная аутентификация во время движения
Отпечаток пальца	Безуспешна
Распознавание лица 2D	На большом расстоянии
Распознавание лица 3D	На среднем расстоянии
Радужная оболочка глаза	На большом расстоянии
Сетчатка глаза	Невозможна
Рисунок вен	На маленьком расстоянии

1.4.8 Сравнение биометрических методов по психологическому комфорту пользователя

Психологический комфорт пользователей также является достаточно актуальным показателем при выборе системы безопасности. Если в случае двумерного распознавания лица или радужной оболочки - это происходит незаметно, сканирование сетчатки является довольно неприятным процессом. И идентификация отпечатков пальцев, хотя и удобная, может вызвать негативные ассоциации с судебными процессами (таблица 1.8).

Таблица 1.8 – Сравнение биометрических методов по психологическому комфорту пользователя

Биометрическая СКУД использует:	Комфорт пользователя
Отпечаток пальца	Средний
Распознавание лица 2D	Высокий
Распознавание лица 3D	Средний

Радужная оболочка глаза	Высокий
Сетчатка глаза	Низкий
Рисунок вен	Средний

1.4.9 Сравнение по стоимости реализации биометрических методов в СКУД

Ценообразование систем контроля доступа и учета, в зависимости от используемых методов биометрической идентификации, чрезвычайно различно. Тем не менее, разница может быть ощутимой в рамках одного и того же метода, в зависимости от назначения системы (функциональности), производственных технологий, методов, которые повышают защиту от несанкционированного доступа и т.д. (таблица 1.9).

Таблица 1.9 – Сравнение по стоимости реализации биометрических методов в СКУД

Биометрическая СКУД использует:	Стоимость
Отпечаток пальца	Низкая
Распознавание лица 2D	Средняя
Распознавание лица 3D	Высокая
Радужная оболочка глаза	Высокая
Сетчатка глаза	Высокая
Рисунок вен	Средняя

1.4.10 Сравнение доступности методов биометрической идентификации в Казахстане

Доступность систем контроля доступа, использующих тот или иной метод биометрической аутентификации, зависит от их использования в целом. И конечно же, особенности отечественного рынка накладывают свои ограничения (таблица 1.10).

Учитывая сложные экономические условия, цена выходит на первый план. Кроме того, для Казахстана играет роль не только сравнительная оценка стоимости внедрения различных методов, но и наличие отечественного оборудования, использующего назначенный метод для биометрической идентификации. Прежде всего, присутствие наших собственных

производителей снижает стоимость оборудования на порядок. Кроме того, наличие оборудования позволяет рассчитывать на быструю замену или ремонт компонентов при необходимости.

Таблица 1.10 – Сравнение доступности методов биометрической идентификации в Казахстане

Биометрическая СКУД использует:	Доступность на казахстанском рынке
Отпечаток пальца	Высокая
Распознавание лица 2D	Средняя
Распознавание лица 3D	Средняя
Радужная оболочка глаза	Низкая
Сетчатка глаза	Низкая
Рисунок вен	Высокая

Нету проблем с распознаванием отпечатков пальцев: у потребителя имеется широкий ассортимент устройств, доступных как для импортного, так и для казахстанского производства. Последний, конечно, дешевле и популярен среди клиентов и установщиков. В том числе для реализации систем многофакторной аутентификации.

Примерно такая же картина, как у метода распознавания вен: наличие оборудования на рынке делает эту технологию очень популярной.

Двумерная идентификация лица недостаточно эффективна для построения системы безопасности на ее основе. Скорее, этот метод используется для видео-аналитики или в качестве одного из компонентов для систем многофакторной аутентификации. При необходимости можно найти отечественных производителей для решения этой проблемы.

Трехмерная аутентификация обходится дорого, даже при простом сравнении методов биометрической идентификации. Стоит учитывать тот факт, что выбор казахстанских производителей ограничен.

Метод аутентификации Retina настолько узок, а объекты, для которых он был разработан, настолько секретны, что лучше не думать и не говорить вслух об их доступности.

Метод идентификации радужной оболочки глаза является одним из наиболее перспективных и эффективных на протяжении многих лет, и его доля на мировом рынке, естественно, растет. В то же время высокая стоимость и сложная ситуация с технологическими патентами являются ограничениями на мировой арене. Для казахстанского рынка, учитывая обменный курс тенге

к иностранной валюте, стоимость технологии огромна, и оборудование, произведенное за границей, по этой причине доступно только по заказу. Что касается казахстанских производителей, то им, помимо всего прочего, придется преодолевать юридические преграды на родине. Поэтому, несмотря на все перспективы метода, на нашем рынке нет чисто казахстанского производственного оборудования.

1.4.11 Сравнение биометрических методов по совокупности факторов

Конечно, выбор метода биометрической аутентификации для системы контроля доступа зависит главным образом от ее требований. Тем не менее, сравнение биометрических методов по совокупности факторов наглядно демонстрирует их преимущества в целом.

И если рост систем, основанных на распознавании радужной оболочки, ограничен его высокой стоимостью и низкой доступностью для казахстанского потребителя, потенциал метода биометрической аутентификации по венному рисунку очевиден. [4]

1.5 Анализ биометрической идентификации по рисунку вен

1.5.1 Аутентификация по рисунку вен (мировой рынок)

Аутентификация по рисунку вен относительно новый биометрический метод, занимающий все более значительный сегмент на рынке СКУД. Флагманом внедрения решений является Япония, где васкулярное сканирование уже широко распространено в банковской сфере и в медицинских учреждениях.

1.5.2 Аутентификация по рисунку вен (рынок Казахстана)

Аутентификация по рисунку вен одно из наиболее перспективных направлений на казахстанском рынке СКУД. Кроме основных преимуществ метода, сказывается доступность устройств отечественного производства, коррелирующая со стоимостью готовых решений, что делает системы васкулярной идентификации одним из приоритетных средств защиты.

1.5.3 Преимущества идентификации по рисунку вен

Высокая надежность. Использование рисунка вен в качестве идентификатора для биометрической системы демонстрирует высокий уровень надежности при небольшом количестве отказов: FAR - 0,0008% при FRR - 0.01%.

Отличная защищенность. Рисунок вен является биометрической характеристикой, которую практически невозможно «украсть» - поскольку, в отличие от отпечатка пальца или радужной оболочки глаза, она скрыта от стороннего наблюдателя и определяется только сканированием в ИК-освещении. Даже при наличии шаблона – муляж создать крайне сложно. Кроме того, производители стремятся активизировать и другие защитные механизмы.

Комментарии экспертов:

"Излучение датчика реагирует на ток крови. А это значит, что никакую "отрубленную руку" к сканеру не приложишь - в венах должен быть кровоток, следовательно, ни муляж, ни мертвая рука не годятся,"- утверждает Джозеф Регер, руководитель СТО EMEA Fujitsu.

Бесконтактное сканирование. Аутентификация по рисунку вен является бесконтактной технологией, которые сейчас в тренде на мировом рынке СКУД. Применение этой технологии отлично подходит для мест с массовым потоком людей, объектов сферы питания и здравоохранения.

Комментарии экспертов:

"Бесконтактные биометрические датчики помогают предотвратить распространение бактерий и инфекций, передающихся, в основном, через грязные руки. Это более гигиенично," - считает Йорг Хартманн, вице-президент Global Client Computing Devices Fujitsu.

Удобство интеграции. Технология распознавания рисунка вен сравнительно проста в реализации и, зачастую, использует ту же аппаратную базу, что и оптические сканеры отпечатков пальца. Таким образом, интеграция этой биометрической характеристики в комбинированные устройства и схемы, для создания мультифакторных или мультибиометрических систем – является несложной задачей, реализация которой значительно повышает уровень защищенности СКУД в целом.

Доступная цена. Стоимость систем, использующих в качестве идентификатора, рисунок вен несколько выше, чем для систем с дактилоскопическими идентификаторами. Однако, васкулярное сканирование значительно дешевле аутентификации по радужной оболочке глаза при почти идентичном уровне надежности.

1.5.4 Недостатки метода идентификации по рисунку вен

Считыватели рисунка вен чувствительны к засветке галогеновыми лампами или попаданию прямого солнечного света, что создает особые требования к условиям освещения в месте установки сканера.

Некоторые болезни человека могут затруднять работу считывателя. Например, это касается некоторых форм анемии.

Сопоставляя метод распознавания рисунка вен с остальными биометрическими методами идентификации сложно назвать это недостатками. Скорее – технологические особенности.

1.5.5 Принцип работы сканеров рисунка вен

Принцип работы считывателей рисунка вен, основывается на способности гемоглобина крови поглощать инфракрасное излучение.

Сканирующее оборудование может работать «на просвет» (Transmission), когда объект сканирования (чаще всего ладонь или палец) помещается между источником излучения и считывающей поверхностью. Но, значительно чаще, используется технология считывания отраженного ИК-

света (Reflection). Она позволяет получить более компактную конструкцию считывателя, за счет размещения всех аппаратных компонентов в одном месте. И, кроме того, избежать лишних психологических барьеров у пользователя, которому не приходится помещать свой биометрический идентификатор (например, руку) внутрь сканирующего устройства.

В результате ИК-сканирования получается изображение объекта, где вены представлены более темным, фактически черным, цветом. Картинка проходит дополнительную программную обработку, после чего полученная схема расположения вен проходит верификацию. [5]

1.6 Идентификация в облаке: Morpho Cloud

О принятии Облачных сервисов в качестве удобного и безопасного решения, говорит первое развертывание автоматизированной системы биометрической идентификации для государственных правоохранительных органов в коммерческой облачной среде, завершившееся в сентябре 2016 гола: MorphoTrak, дочерняя компания Safran Identity & Security, и Департамент полиции Альбукерке успешно развернули MorphoBIS в облаке MorphoCloud. Полицейские уже отметили значительное увеличение скорости обработки, а также возможность распознавания отпечатков значительно худшего качества.

Служба, разработанная MorphoTrak) базируется на Microsoft Azure Government и включает в себя несколько биометрические механизмов идентификации: дактилоскопическая биометрия, биометрия лица и радужной оболочки глаза. Кроме того, возможно распознавание татуировок, голоса, услуги видеоаналитики (VSaaS).

Кибербезопасность системы отчасти гарантируется размещением на правительственном сервере уголовного правосудия Criminal Justice Information Services (CJIS), а отчасти совокупным опытом работы в области безопасности компаний Morpho и Microsoft.

"Мы разработали наше решение, чтобы помочь правоохранительным органам добиться экономии времени и увеличения эффективности. Безопасность, конечно, является ключевым элементом. Мы хотели, чтобы облачное решение отвечало бы жесткой политике безопасности правительства CJIS и нашли Microsoft идеальным партнером, чтобы обеспечить жесткий контроль над уголовными и национальными данными по безопасности, в рамках территориально-распределенной среды центров обработки данных." - говорит Франк Баррет, директор Cloud Services в MorphoTrak, LLC.

В результате Morpho Cloud является выдающимся примером аутсорсингового управления идентификацией, которая может обеспечить эффективность и экономичность улучшений в системах безопасности правоохранительных органов. Идентификация как сервис предоставляет преимущества, недоступные для большинства учреждений. Например, гео-распределенное аварийное восстановление данных, как правило, не целесообразно с точки зрения высокой стоимости проекта, и повышение

уровня безопасности таким образом возможно только благодаря масштабу Microsoft Azure и Morpho Cloud. [6]

1.7 Биометрическая аутентификация на мобильных устройствах

1.7.1 Аутентификация по отпечатку пальца на мобильных устройствах

Исследование Biometrics Research Group, Inc. посвящено анализу и прогнозу развития рынка биометрической аутентификации в мобильных устройствах. Исследование спонсировано ведущими производителями рынка биометрии Cognitec, VoicePIN и Applied Recognition.

1.7.2 Рынок мобильной биометрии в цифрах

По данным исследования объем сегмента мобильной биометрии оценивается в 9 млрд. долл. к 2018 г. и 45 млрд. долл. к 2020 году по всему миру. При этом использование биометрических характеристик для аутентификации будет применяться не только для разблокировки мобильных устройств, а также для организации многофакторной аутентификации и мгновенного подтверждения электронных платежей.

Развитие сегмента рынка мобильной биометрии связано с активным использованием смартфонов с предустановленными сенсорами. Отмечается, что к концу 2015 года, мобильные устройства с биометрией будут использовать не менее 650 млн человек. Число пользователей мобильных с биометрическими датчиками согласно прогнозам, будет расти на 20.1% в год и к 2020 году составит не менее 2 млрд. человек. [7]

2 Обзор существующих СКУД с технологиями биометрии

2.1 Терминал BioSmart PV-WTC

2.1.1 Описание терминала

Терминал «BioSmart PV-WTC» предназначен для работы в составе биометрической системы контроля и управления доступом BioSmart.

Терминал позволяет организовать учет рабочего времени посредством идентификации пользователей по уникальным биометрическим особенностям сосудистого русла вен ладоней человека и бесконтактным RFID-меткам (картам), а также, в зависимости от исполнения, может применяться для организации контроля и управления доступом. [8]

Описание лицевой панели терминала.

Внешний вид терминала представлен на рисунке 2.1:

Рисунок 2.1 – Внешний вид терминала BioSmart PV-WTC

а) поле для считывания пластиковых карт;
б) ЖК экран;
в) клавиатура;
г) сканер вен ладони.

Навигация по экранному меню осуществляется с помощью кнопок клавиатуры (рисунок 2.2):

а) 2 – переход вверх по списку;

б) 6 – переход вправо или переход от списка к функциональным кнопкам. В меню «Пользователи» используется для постраничной навигации;

в) 4 – переход влево или переход от функциональных кнопок к списку, в меню «Пользователи» используется для постраничной навигации;

г) 5 – переход для подтверждения в меню «сотрудники»;

д) 8 – переход вниз по списку;

Рисунок 2.2 – Клавиатура терминала

Описание индикации и перемычек на плате терминала.

Расположение контактов, разъёмов, перемычек и индикаторов на печатной плате терминала представлено на рисунке 2.3.

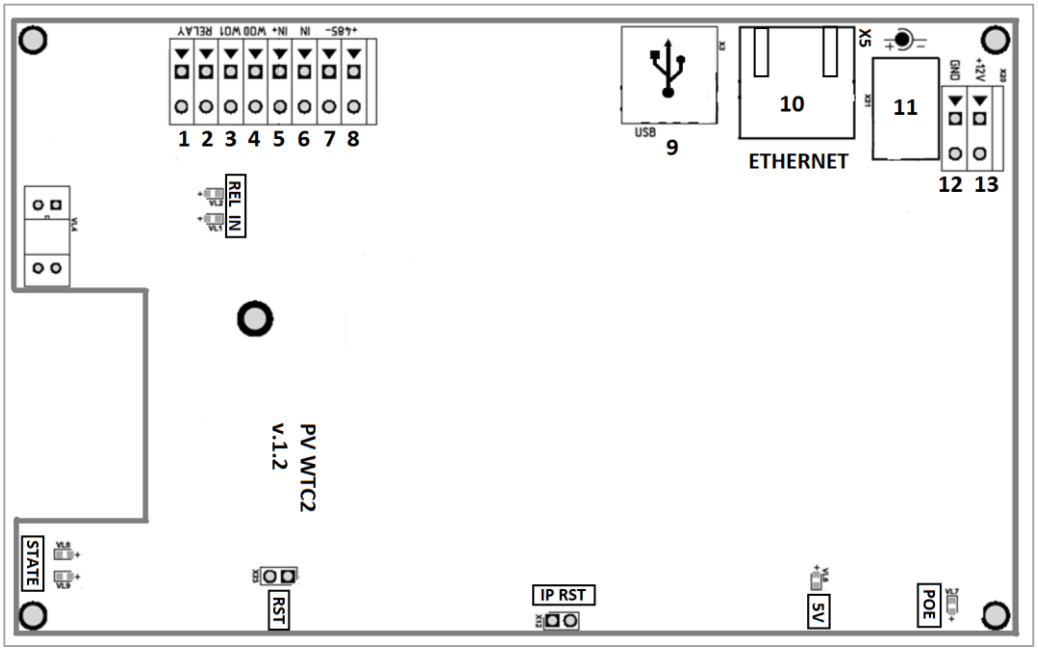

Рисунок 2.3 – Расположение контактов, разъёмов, перемычек и индикаторов на печатной плате терминала

а) светодиоды, размещенные на разъеме X5 (Ethernet), отображают состояние физического подключения (Link, зеленый) и активности обмена по сети (Activity, красный);

б) светодиод REL загорается при включении бортового реле. При включении бортового реле замыкаются выходы RELAY;

в) светодиод IN загорается при поступлении +12В на вход IN терминала;

г) светодиод PoE загорается при наличии питания терминала по стандарту PoE;

д) светодиод 5V загорается при наличии питания микросхем +5В, что говорит об исправности источника питания терминала;

е) светодиоды STATE отображают информацию о работе системы (для служебного пользования);

ж) перемычка IPRST предназначена для сброса сетевых настроек на заводские.

Перемычка RST предназначена для перезагрузки терминала. Для перезагрузки терминала при включенном питании необходимо замкнуть контакты перемычки на 1 секунду.

Для сброса сетевых настроек при включенном питании необходимо замкнуть контакты перемычки IPRST и дождаться, пока светодиоды Link и Activity на разъеме Ethernet погаснут.

2.1.2 Технические характеристики

1) тип сканера вен ладоней: Оптический, инфракрасный;
2) максимальное количество пользователей*: 1 000 000;
3) максимальное количество кодов карт: 1 000 000;
4) максимальное количество ладоней: 300 000;
5) максимальное количество событий в памяти терминала: 10 000 000;
6) время идентификации по венам ладони: 1:1000 Не более 2 с;
7) вероятность ошибочного предоставления доступа FAR**: 0.00008%;
8) встроенный считыватель RFID-карт: Да;
9) дальность считывания карт, мм: До 100;
10) дисплей: TFT 3.5” 320x240 мм;
11) клавиатура: Сенсорная, 12 кнопок;
12) поддержка БУР Biosmart: Да;
13) интерфейс связи с управляющим компьютером: Ethernet (IEEE 802.3, 10BASE-T, IEEE 802.3u, 100BASE-TX);
14) интерфейс USB для конфигурации: USB2.0 Full Speed;
15) WEB-интерфейс для конфигурации: Да;
16) выходной интерфейс Wiegand 26-40 бит: Да;
17) бортовое реле: 12VDC, 1A;
18) количество дискретных входов: 1;
19) параметры электропитания: 12VDC±15%, 1A;
20) поддержка PoE: IEEE802.3af class 3;
21) габаритные размеры (L x W x H): 220x155x140 мм;
22) масса нетто: 840 г;
23) масса брутто: 1230 г;

24) температурный диапазон эксплуатации: От 0 до плюс 50 °С;
25) относительная влажность воздуха эксплуатации: Не более 90%;
26) степень защиты: IP54;
27) исполнение: Накладной пластиковый корпус.

2.1.3 Режим ожидания и доступ к основному меню

В режиме ожидания экран терминала имеет вид, соответствующий установленному на нем режиму работы. Один из вариантов вида приведен на рисунке 2.4. На экране, как правило, выводится тип действия, которое ожидается терминалом («Нажмите кнопку», «Приложите ладонь» и т.д.).

Рисунок 2.4 – Экран терминала в режиме ожидания

Основное меню терминала позволяет пользователю получить доступ к настройкам терминала, данным о сотрудниках, информацию об ошибках.

а) для входа в основное меню нажмите клавишу «Ввод»;
б) введите пароль администратора в появившемся поле.

После первого входа рекомендуется установить новый пароль, в целях исключения в дальнейшем несанкционированного доступа к настройкам терминала.

Вид основного меню представлен на рисунке 2.5.

Рисунок 2.5 – Экран терминала в режиме доступа к основному меню

2.1.4 Принцип действия СКУД BioSmart

СКУД BioSmart - это сетевая распределенная система с разграничением прав доступа пользователей, при необходимости расширяемая, открытая для интеграции с оборудованием других производителей. В точках прохода устанавливаются контроллеры, которые подключаются к управляющему ПК или серверу через интерфейс RS485 или локальную сеть Ethernet. Путь RS485 организован с использованием преобразователей (USB-RS485, LAN-RS485, GPRS-RS485). Регистрация пользователя осуществляется в программе BioSmart-Studio. Для регистрации отпечатков пальцев используется контрольный считыватель, подключенный через порт USB персонального компьютера. Для каждого пользователя вы можете зарегистрировать до пяти отпечатков пальцев и один код бесконтактной карты Em-Marine, Mifare или HID. Математические модели отпечатков пальцев записываются в базу данных, что делает невозможным воссоздание их графического изображения. Затем пользователю назначаются права доступа к конкретным точкам доступа, пользовательская информация передается на контроллер или на сервер аутентификации безопасным способом. Когда пользователь кладет на сканер палец или пластиковую карточку, в базе данных зарегистрированных моделей производится поиск. В режиме аутентификации сервера поиск и сравнение моделей выполняется на внешнем сервере, что увеличивает скорость обработки больших баз данных. В случае правильной идентификации контроллер генерирует управляющий сигнал для приводов (электромагнитный блок, турникет и т.д.). Блок релейного управления (БУР) устанавливается внутри помещения, что исключает возможность несанкционированного доступа в помещение из-за короткого замыкания в проводах или имитации управляющего сигнала. После успешной идентификации соответствующая информация записывается в журнал событий, который затем используется для записи рабочего времени и создания различных отчетов. В режиме мониторинга можно отображать все события в режиме реального времени. События неуспешной идентификации или попытки несанкционированного доступа пользователей фиксируются в системе. СКУД BioSmart может работать с внешними датчиками. Система предлагает дискретные входы для подключения кнопки дистанционного вывода, датчика открытия двери, датчика турникета и пожарной сигнализации. Все события, вызванные внешними датчиками, записываются в журнал. [9]

2.1.5 СКУД BioSmart на малом предприятии (численность до 100 человек)

Для организации контроля доступа и учета времени на малом производстве возможно использование системы BioSmart в базовой комплектации (рисунок 2.6). Персональный компьютер (ПК) может использоваться для регистрации пользователей в системе, а также для ведения журнала событий и создания отчетов о рабочем времени. Контроллеры

подключены к компьютеру через преобразователь USB-RS485, до 32 контроллеров могут работать одновременно на одной линии RS485.

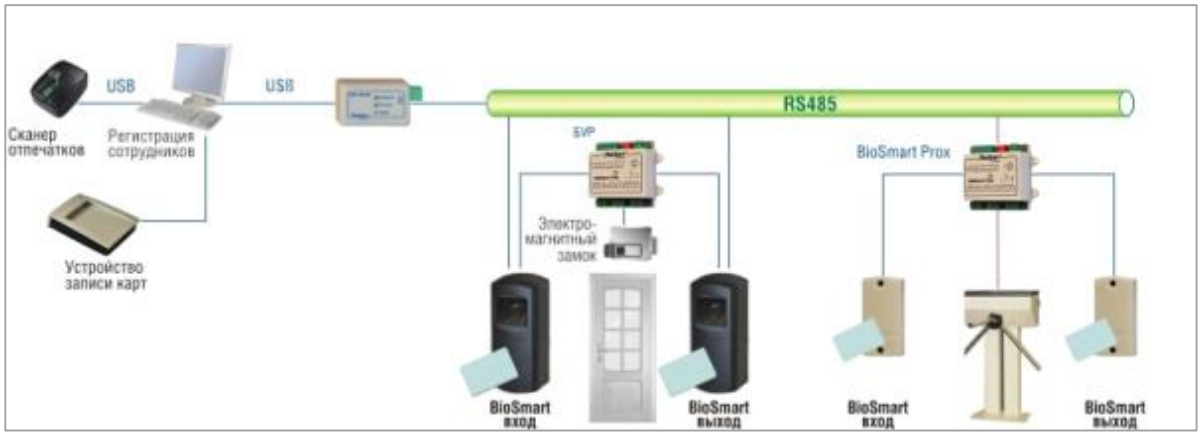

Рисунок 2.6 – Конфигурация системы для малого предприятия

2.1.6 СКУД BioSmart на среднем предприятии (численность до 500 человек)

Отличительной чертой использования системы BioSmart на среднем предприятии является факт применения магистрали RS485 и локальной, промышленной сети Ethernet (рисунок 2.7). К сети контроллеры подключаются через преобразователь LAN-485 или напрямую, при использовании BioSmart со встроенным патчем Ethernet. Биометрический терминал BioSmart управляет турникетом, установленным на входе организации, а использование терминала со встроенными считывателями бесконтактных карт позволяет организовать проход сотрудников по отпечаткам пальцев, и гостям или посетителям с помощью пластиковой карты. В зависимости от уровня доступа отдельные помещения могут быть оснащены биометрическими контроллерами BioSmart и контроллерами BioSmart-Prox для работы с бесконтактными картами. Программное обеспечение BioSmart Net-Work и Work-Time позволяет организовать отдельные рабочие станции для регистрации пользователей, мониторинга событий в системе (шаг за шагом) и получения отчетов о рабочем времени.

2.1.7 СКУД BioSmart на крупном предприятии (численность до 3000 человек)

В крупной организации с большой базой данных отпечатков пальцев сотрудников (до 30 тысяч моделей) требуется идентификация на основе сервера, т.е. использование вычислительной мощности сервера для быстрого поиска отпечатков пальцев в базе данных (рисунок 2.8). Стабильная скорость аутентификации 10 тысяч отпечатков на сервере обычно составляет одну секунду. Обязательно нужно использовать соединительные линии Ethernet и контроллеры BioSmart со встроенным портом Ethernet. Для режимно-работающих предприятий можно организовать доступ по карте или по карте +

отпечаток пальца. Программное обеспечение «Центр Синхронизации» позволяет организовать работу нескольких автономных серверов в рамках одной системы контроля доступа BioSmart. [10]

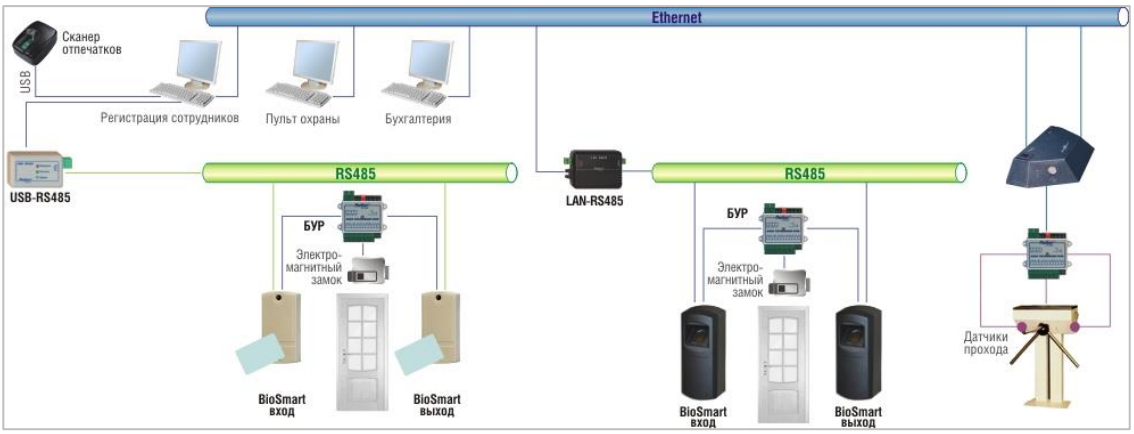

Рисунок 2.7 – Конфигурация системы для среднего предприятия

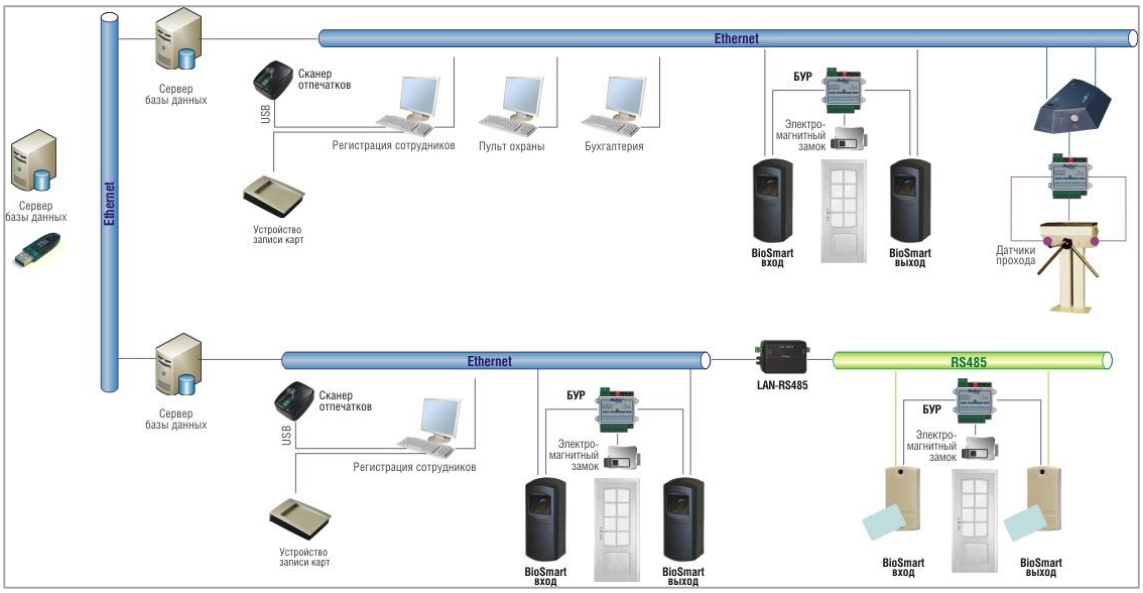

Рисунок 2.8 – Конфигурация системы для крупного предприятия

2.1.8 Идентификация по карте и отпечатку пальца (неограниченное количество пользователей)

Неограниченные возможности емкости базы данных отпечатков в СКУД BioSmart возможны при использовании пластиковых карт формата Mifare или HID iClass с внутренней памятью 1 или 4 кБ (рисунок 2.9). При этом шаблоны отпечатков записываются на пластиковую карту. При идентификации пользователь прикладывает карту к считывателю контроллера, передавая шаблон отпечатка в память контроллера. Контроллер переходит в режим ожидания отпечатка, затем пользователь прикладывает палец к считывателю, происходит сравнение шаблона, хранящегося на карте с приложенным

отпечатком. Такой способ идентификации не предусматривает ограничений по емкости базы данных отпечатков.

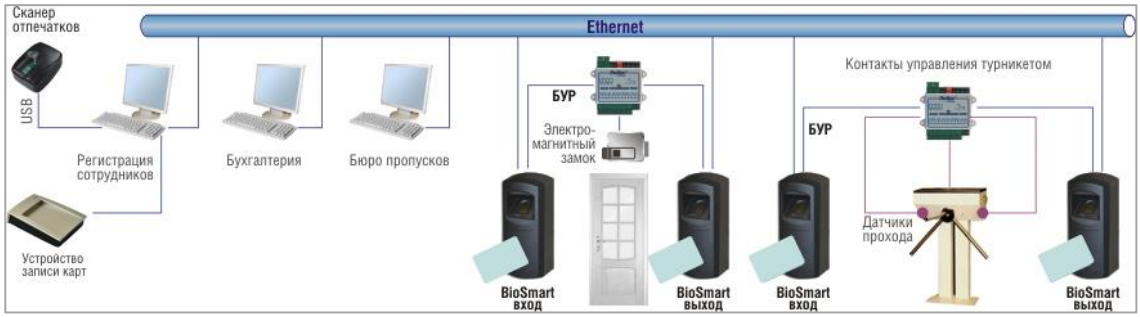

Рисунок 2.9 – Конфигурация системы для идентификации по карте

2.1.9 Контроль доступа и учет рабочего времени для удаленных объектов

При организации контроля доступа и учета рабочего времени при значительной удаленности управляющего ПК или сервера от точек прохода, где применение локальной сети Ethernet или сети Интернет становиться невозможным, можно воспользоваться каналом связи GRPS сотовой сети (рисунок 2.10). Контроллеры Biosmart подключаются при помощи преобразователя GRPS-485, загрузка данных отпечатков и журналов событий производится по GRPS каналу обеспечивая быструю и недорогую передачу данных на сервер. Количество удаленных точек может быть не ограниченным. Для организации контроля за сохранностью оборудования предусмотрены датчики вскрытия корпуса и датчики разряда аккумулятора, при срабатывании которых незамедлительно высылается SMS сообщение на любые 5 телефонных номеров. [11]

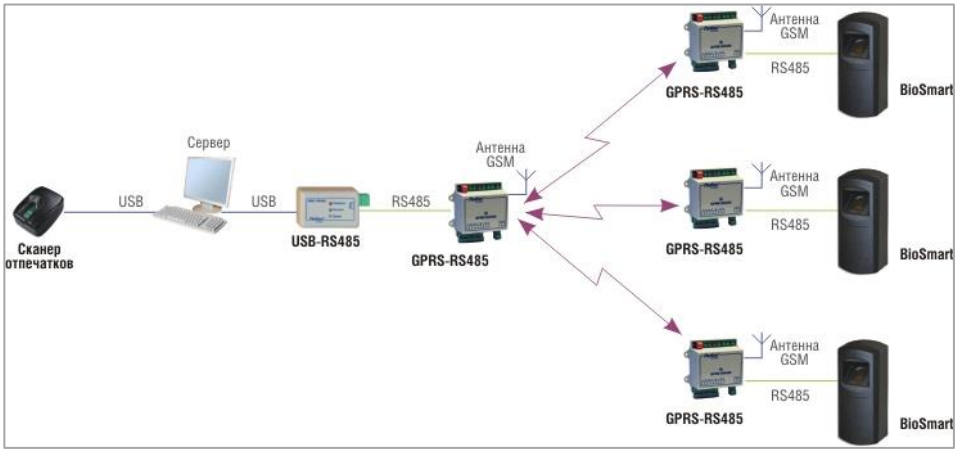

Рисунок 2.10 – Конфигурация удаленного контроля доступа

2.1.10 Преимущества системы Biosmart HandVein:

а) бесконтактная идентификация;

б) невозможность фальсификации (рисунок вен ладони не видим в видимом спектре);

в) идентификация не зависит от сухости/влажности и загрязненности ладоней;

г) низкий процент ошибок;

д) высокая надежность;

е) удобство использования.

2.2 Технология распознавания по рисунку вен Fujitsu PalmSecure, терминал FPS ID Access

2.2.1 Описание технологии PalmSecure

Сегодня существует довольно много способов идентифицировать человека по биометрическим параметрам - по лицу, голосу, почерку, отпечаткам пальцев, сетчатке, но чаще всего это обязанность охранника пропускать важных лиц, а для запуска программы требуется пароль. Более того, каждый из этих методов имеет ряд других недостатков. Процедура идентификации отпечатка пальца не так удобна, как хотелось бы, и распознавание лица работает относительно некомфортно. Возможно, только распознавание сетчатки имеет оптимальное отношение к пользователю, ложные ограничения доступа для авторизованного пользователя и возможность фальсифицировать его биометрические характеристики (рисунок 2.11).

Рисунок 2.11 – Внешний вид терминала ID Access

Считается, что жест «открытой ладони» восходит к каменному веку, потому встреча с представителями разных племен показывала, что у них не было камня в руке, и они не будут сражаться. Этот же жест послужил основой технологии, разработанной японскими инженерами Fujitsu: чтобы войти в здание, запустить программу или оборудование, достаточно поднять ладонь

руки и удерживать ее на датчике Fujitsu PalmSecure в течение нескольких секунд. Метод идентификации вены ладони так же надежен, как и метод идентификации по отпечатку пальца, но с меньшей вероятностью «забудет» владельца, обеспечив самый высокий процент правильных допусков. [12]

2.2.2 Описание терминала PalmSecure ID Access

Fujitsu представила PalmSecure ID Access — полностью готовое к использованию устройство, с помощью которого крупные корпорации и компании малого и среднего бизнеса могут модернизировать свои системы контроля доступа.

Новинка представляет собой компактный терминал с датчиком PalmSecure и сенсорным экраном, предназначенный для аутентификации личности с помощью технологии бесконтактного сканирования рисунка вен ладони. PalmSecure ID Access можно легко интегрировать в существующие системы контроля доступа.

Технология биометрической аутентификации обеспечивает высокий уровень точности по сравнению с системами безопасности на базе пин-кодов, паролей, ключей или карт доступа. Она отличается исключительным удобством использования и гигиеничностью. Кроме того, отсутствуют какие-либо элементы, которые можно потерять, передать другом лицу, скопировать или украсть. У компаний-заказчиков появляется возможность индивидуально предоставлять права доступа отдельным лицам, при этом исключив риски, связанного с утерей паролей.

Устройство PalmSecure ID Access (модель PSN900) создана на базе, отмеченной наградами, биометрической технологии сканирования рисунка вен ладоней компании Fujitsu. PalmSecure ID Access доступно в различных вариантах конфигурации для мультифакторной аутентификации. Также предусмотрена установка считывателей карт Mifare или бесконтактных карт HID. Существует вариант поставки устройства только с одним датчиком PalmSecure.

2.2.3 Принцип работы технологии

Сканер облучает руку в ближнем инфракрасном диапазоне и считывает рисунок вен, которые теплее окружающих их тканей за счет крови, приходящей из сердца. Изображение венозного рисунка на ладони записывается в 5-Мбайт образ, содержащий температуру в 5 млн. точках. Этот образ шифруется по алгоритму AES с разрядностью 128 или 256 бит. Через USB-интерфейс зашифрованный файл передается на ПК, сервер, ноутбук или индустриальный ПК, где формируется биометрический шаблон (хэш, иными словами) размером 1 – 3 Кбайт. Биометрический шаблон вторично шифруется по алгоритму AES и используется во всех последующих операциях. Такой механизм не требует применения дополнительных устройств для хранения данных, что обеспечивает полную сохранность информации (разве что сам сканер украдут).

Для регистрации производится двухкратное сканирование ладони пользователя и создается биометрический шаблон (рисунок 2.12). Эта операция единовременная и самая длительная – она занимает 10 – 30 секунды. Процесс опознавания пользователя длится 1 – 2 секунды. [13]

Каждая фирма-девелопер, использующая комплект PalmSecure получает от разработчика – компании Fujitsu – свой шифровальный ключ. Этим ключом кодируется биометрический шаблон, который имеется только у интегратора. При этом шифр, используемый для кодировки информации, доступен только компании, эксплуатирующей сенсор. Такой подход предотвращает риск потенциальной подделки шаблонов фирмой-разработчиком или интегратором.

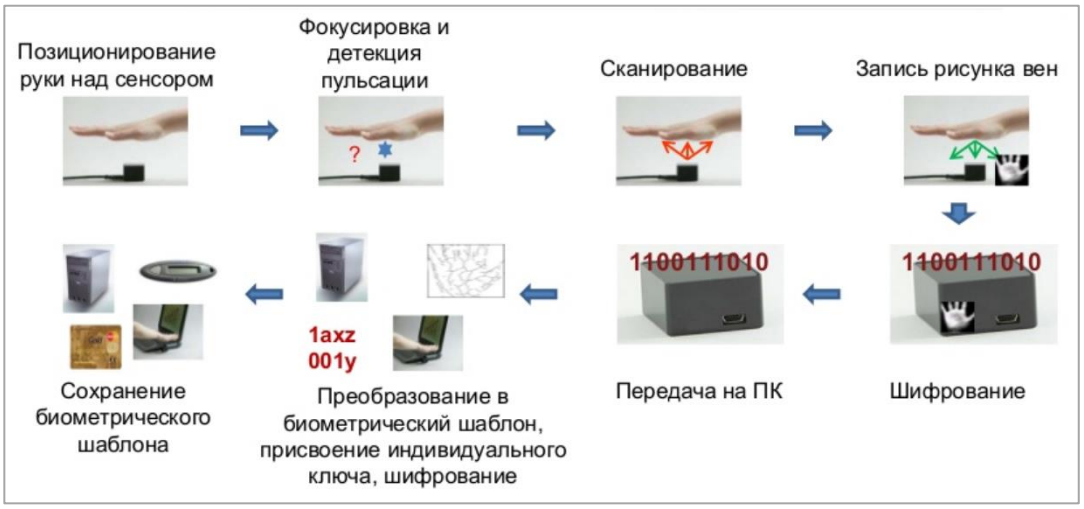

Рисунок 2.12 – Цикл действий для создания биометрического шаблона

3 Конструирование и моделирование прибора

3.1 Выбор оборудования

3.1.1 Выбор микроконтроллера

а) при проектировании системы необходимо учесть следующие требования;

б) платформа должна иметь необходимое количество портов ввода-вывода;

в) должны иметься порты для подключения аналоговых и цифровых датчиков и модулей;

г) сам контроллер должен автоматически управлять датчиками;

д) контроллер обязательно должен быть правильно подобран к техническим условиям, в которых он планируется эксплуатироваться.

Платформа Nano, построенная на микроконтроллере ATmega328 (Arduino Nano 3.0) или ATmega168 (Arduino Nano 2.3), имеет небольшие размеры и может использоваться в лабораторных работах. Она имеет схожую с Arduino Duemilanove функциональность, однако отличается сборкой. Отличие заключается в отсутствии силового разъема постоянного тока и работе через кабель Mini-B USB. Nano разработана и продается компанией Gravitech. [14]

Далее приведены только те характеристики микроконтроллера, которые являются наиболее важными для данного проекта. Итак, Arduino Nano 2.3 является законченным устройством, в основе которого лежит микроконтроллер ATMega 168. Имеет 14 цифровых входа/выхода (6 из которых могут использоваться как выходы ШИМ), что достаточно для представленного дипломного проекта. Также имеется 8 аналоговых входов, разъем питания, разъем USB, который используется для связи ПК и микроконтроллера и кнопка для сброса параметров. Рабочее напряжение – 5В, рекомендованное напряжение питания– 7-12В, предельное питание – 20В, память 16 КБ, ток вывода – максимум 40мА. Также в приложении А приведена принципиальная схема микроконтроллера.

Arduino Nano может получать питание через подключение Mini-B USB, или от нерегулируемого 6-20 В (вывод 30), или регулируемого 5 В (вывод 27), внешнего источника питания. Автоматически выбирается источник с самым высоким напряжением.

Микросхема FTDI FT232RL получает питание, только если сама платформа запитана от USB. Таким образом при работе от внешнего источника (не USB), будет отсутствовать напряжение 3.3 В, генерируемое микросхемой FTDI, при этом светодиоды RX и TX мигаю только при наличии сигнала высокого уровня на выводах 0 и 1.

На рисунке 3.1 показан внешний вид платы:

Рисунок 3.1 – Внешний вид устройства

Каждый из 14 цифровых выводов Nano, используя функции pinMode(), digitalWrite(), и digitalRead(), может настраиваться как вход или выход. Выводы работают при напряжении 5 В. Каждый вывод имеет нагрузочный резистор (стандартно отключен) 20-50 кОм и может пропускать до 40 мА. Некоторые выводы имеют особые функции:

а) последовательная шина: 0 (RX) и 1 (TX). Выводы используются для получения (RX) и передачи (TX) данных TTL. Данные выводы подключены к соответствующим выводам микросхемы последовательной шины FTDI USB-to-TTL;

б) внешнее прерывание: 2 и 3. Данные выводы могут быть сконфигурированы на вызов прерывания либо на младшем значении, либо на переднем или заднем фронте, или при изменении значения. Подробная информация находится в описании функции attachInterrupt();

в) ШИМ: 3, 5, 6, 9, 10, и 11. Любой из выводов обеспечивает ШИМ с разрешением 8 бит при помощи функции analogWrite();

г) SPI: 10 (SS), 11 (MOSI), 12 (MISO), 13 (SCK). Посредством данных выводов осуществляется связь SPI, которая, хотя и поддерживается аппаратной частью, не включена в язык Arduino;

д) LED: 13. Встроенный светодиод, подключенный к цифровому выводу 13. Если значение на выводе имеет высокий потенциал, то светодиод горит.

На платформе Nano установлены 8 аналоговых входов, каждый разрешением 10 бит (т.е. может принимать 1024 различных значения). Стандартно выводы имеют диапазон измерения до 5 В относительно земли, тем не менее имеется возможность изменить верхний предел посредством

функции analogReference(). Некоторые выводы имеют дополнительные функции:

I2C: A4 (SDA) и A5 (SCL). Посредством выводов осуществляется связь I2C (TWI). Для создания используется библиотека Wire (информация на сайте Wiring).

Дополнительная пара выводов платформы:

а) AREF. Опорное напряжение для аналоговых входов. Используется с функцией analogReference();

б) Reset. Низкий уровень сигнала на выводе перезагружает микроконтроллер. Обычно применяется для подключения кнопки перезагрузки на плате расширения, закрывающей доступ к кнопке на самой плате Arduino.

Достоинства. Функциональная маленькая плата Arduino Nano, ничуть не уступающая по функциям большой UNO, – дешевле, удобнее для монтажа и сборки миниатюрных устройств.

3.1.2 Выбор ИК – термометра

Большинство методов измерения температуры требуют некий физический контакт температурного датчика с объектом, температура которого должна быть измерена.

Но по мере развития технологий меняется и способ измерения температуры. Как быть если нам необходимо измерить температуру объекта без физического контакта с ним? В этом нам окажет помощь инфракрасный термометр.

Принцип работы инфракрасных термометров прост — все тела при температуре выше 0° Кельвина (абсолютный ноль) в той или иной степени излучают инфракрасную энергию, которая может быть обнаружена датчиком инфракрасного термометра.

Конструкция инфракрасного термометра имеет оптическую систему, которая фокусирует инфракрасную энергию, излучаемую объектом. Далее инфракрасный датчик преобразует энергию в электрический сигнал, который затем может быть передан в микроконтроллер для интерпретации и отображения в единицах температуры.

Melexis MLX90614ESF-BAA - инфракрасный термометр для бесконтактного замера температуры (рисунок 3.2). Внутри - 17-битный АЦП и мощный DSP, поэтому термометр точный и имеет высокое разрешение. Он имеет широкий диапазон применения, например, измерение температуры тела, и даже измерение количества движения.

MLX90614 имеет два метода вывода: PWM и SMBus (то есть TWI, I2C). 10-битный PWM имеет разрешение 0.14°C, в то время как интерфейс TWI имеет разрешение 0.02°C. Сенсор откалиброван на заводе и имеет диапазон: -40 -- 85°C температуру воздуха и -70 -- 382.2°C температура объектов. Измеренное значение представляет собой усредненное значение температуры

в поле зрения сенсора. При комнатной температуре термометр имеет стандартную точность 0.5°C.

Рисунок 3.2 – Внешний вид термометра

Основные функции и свойства данного термометра:

- компактность, низкая стоимость;
- легкость интеграции;
- откалиброван на заводе;
- диапазон: -40 - +85°C температура воздуха;
- диапазон: -70 - +380°C температура объектов;
- цифровой интерфейс SMBus;
- настраиваемый PWM-выход для непрерывного считывания;
- точность в пределах 0,5C по всему диапазону 0-50C;
- разрешение 0,02C;
- есть версии с одной и двойной зонами считывания;
- простая адаптация для напряжений от 8 до 16V;
- режим экономии энергии;
- различные опции корпусов;
- подходит для автомобилей.

3.1.3 Выбор ИК – датчика расстояния

Для измерения расстояния до объекта существуют оптические датчики, работающие на методе триангуляции. Самые распространенные из них – это работающие на длине волны, инфракрасные (на английском языке infra-red, сокращенно ИК) датчики расстояния с выходным аналоговым напряжением, производимые фирмой Sharp. У датчиков Sharp имеется IR LED с линзой, который излучает узкий световой луч. Отраженный от объекта луч направляется через другую линзу на позиционно-чувствительный фотоэлемент (на английском языке position-sensitive detector, сокращенно PSD). От местоположения луча падающего на PSD, зависит его проводимость.

Проводимость преобразуется в напряжение и, к примеру, диджитализируя его аналого-цифровым преобразователем микроконтроллера, можно вычислить расстояние.

Выход датчика расстояния Sharp обратно пропорциональный - с увеличением расстояния это уменьшается и растет медленно. Точный график между расстоянием и выходом приведен в спецификации датчика. У датчиков, в соответствии с типом, имеется граница измерения, в пределах которой выход датчика является надежным. Измерение максимально реального расстояния ограничивают два аспекта: уменьшение интенсивности отражающегося света и невозможность PSD регистрировать изменение местоположения отображенного маленького луча. При измерении сильно отдаленных объектов, выход датчика остается приблизительно таким же, как и при измерении максимально отдаленных расстояний. Минимально измеряемое расстояние ограничено особенностями датчика Sharp, а именно - выходное напряжение на определённом расстоянии (в зависимости от датчика: 4-20 см) начинает резко падать при уменьшении расстояния. По существу, это означает, что одному значению выходного напряжения соответствует два расстояния. Для предотвращения проблемы нужно избегать слишком близкого приближения объектов к датчику.

Рисунок 3.3 – Внешний вид датчика Sharp GP2Y0A21YK

В комплекте датчика есть инфракрасный измеритель расстояния Sharp GP2Y0A21YK с границей измерения 10-80 см (рисунок 3.3). Выходное напряжение датчика до 3 V в зависимости от измеряемого расстояния. Датчик подключается на модуль «Датчики» и его выходное напряжение направляется на канал 0 аналого-цифрового преобразователя AVR. На базе предыдущего задания датчиков, можно просто сделать программу, которая измеряет выходное напряжение измерителя расстояния, но вдобавок к этому целью данного задания является так же ознакомление с процессом перевода напряжения в расстояние.

В спецификации датчика GP2Y0A21YK приведен график зависимости между выходным напряжением и измеренным расстоянием. Этот график не является линейным, однако график обратной величины выходного напряжения и расстояния почти линейный, и с помощью него довольно просто найти формулу для преобразования напряжения в расстояние. Для нахождения формулы необходимо точки этого графика ввести в какую-либо программу обработки табличных данных и из них создать новый график. В программе обработки табличных данных на основе точек графика возможно автоматически вычислить линию тренда. Далее приведен график связи исправленной обратной величины между выходным напряжением GP2Y0A21YK и расстоянием вместе с линейной линией тренда. Выходное напряжение для упрощения формулы уже переведено в 10-битное значение аналогово-дигитального преобразователя с опорным напряжением +5 V.

3.1.4 Выбор камеры

В качестве камеры остановился на веб-камере Logitech B910 (рисунок 3.4). Испытания моделей устройства, а их было аж 4, выявили недостатки трех предыдущих камер. Первая модель была с камерой LinkSprite JPEG Color Camera TTL Interface. Процесс передачи изображения на ПК ограничивался скоростью порта, пришлось от нее отказаться. Также были проверены еще 2 noname веб-камеры, но получаемые изображения были очень плохого качества. Далее буду описывать только последнюю модель.

Рисунок 3.4 – Logitech HD Webcam B910

Веб-камера Logitech HD Webcam B910 для профессионального проведения видеоконференций характеризуется дополнительными функциями, обеспечивающими комфорт ведения деловых переговоров. Трансляция ведется в видеоформате стабильного высокого качества HD 1280x720. Угол обзора объектива составляет 78 градусов, а формат экрана

16:9 – это оснащает видеочат эффектом присутствия. Защитная шторка закрывается и открывается, обеспечивая дополнительную безопасность личного пространства. Широкополосный чистый звук обеспечивают 2 стереомикрофона. Камера самостоятельно подстраивается под уровень освещения в комнате благодаря системе Logitech RightLight 2 и автофокусировке.

Технология Plug-and-play обеспечивает работу камеры без дополнительных драйверов. Крепление позволяет установить Logitech HD Webcam B910 на LCD-монитор. Стеклянный фирменный объектив ZEISS четко передает мелкие детали изображения. Поддержка автоматической установки и командной строки позволяет использовать камеры целой компанией.

Основные характеристики:

а) веб-камера с матрицей 5 МП;
б) разрешение видео 1280x720;
в) подключение через USB 2.0;
г) встроенный микрофон;
д) автоматическая фокусировка;
е) совместима с Windows.

3.1.5 Выбор других комплектующих компонентов

а) Arduino Project Enclosure;
б) USB Hub;
в) 2 транзистора;
г) 2 резистора 4.7кОм, 6-470Ом;
д) 6 ИК-диодов 850нм;
е) фототранзистор;
ж) USB B разъем и USB кабель.

3.2 Структурная схема

3.2.1 Структурная схема СКУД

Системы контроля и управления доступом (СКУД), являются одной из важных составных частей безопасности предприятия, организации.

Здесь будут рассмотрены состав и основная структурная схема этой системы. Назначение оборудования контроля доступа явствует из самого названия. Структурная схема его соединения приведена на рисунке 3.5, где

а) СРВ – сервер;
б) АРМ - автоматизированное рабочее место;
в) СК - системный контроллер СКУД;
г) К - контроллер замков и считывателей;
д) СЧ – считыватель;
е) ИУ - исполнительное устройство;
ж) ПИ - преобразователь интерфейса.

Далее - составные части СКУД, их функциональное назначение.

Сервер СКУД - место хранения базы данных, базового программного обеспечения (ПО), его дополнительных модулей. АРМ позволяет осуществлять работу с базами данных, программами и модулями различным пользователям в соответствии с предоставленными им правами доступа.

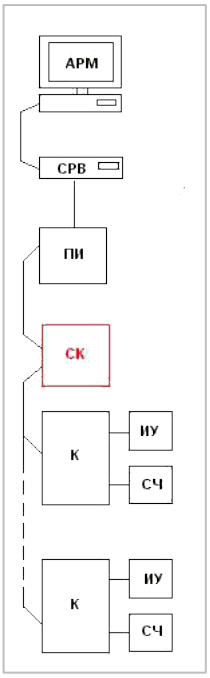

Рисунок 3.5 – Структурная схема СКУД

Следует отметить, что иногда для управления и работой со всеми устройствами бывает достаточно одного компьютера, одновременно выполняющего функции сервера и рабочего места. [15]

Системные требования к серверу, как правило, невысоки, они определяются технической документацией производителя.

Базовое программное обеспечение в большинстве случаев позволяет осуществлять:

а) автоматическое определение аппаратного состава системы, настройку параметров работы подключенных устройств;

б) операции с базами данных, создание новых баз, резервных копий и архивов, восстановление утерянных данных;

в) создание шаблонов оформления карты доступа в виде пропуска с фотографией;

г) ведение базы данных персонала с фотографиями, должностями, графиками работы и личными данными сотрудников;

д) получение отчетов о времени присутствия сотрудников, о нарушениях (опозданиях, преждевременных уходах, прогулах), как по отдельным сотрудникам, так и по подразделениям в целом.

Дополнительные модули ПО значительно расширяют возможности оборудования, позволяют интегрировать ее данные с бухгалтерскими и иными программами, используемыми на предприятии (организации).

Системный контроллер осуществляет общее управление устройствами. В некоторых, как правило, небольших системах он может отсутствовать. Вообще, одной из основных характеристик является количество поддерживаемой системой устройств управления. Для больших (по емкости) СКУД системный контроллер является своего рода расширителем, позволяет создавать разветвленную архитектуру.

Контроллер замков и считывателей основной задачей имеет идентификацию посетителя (сотрудника) на основании предъявленного идентификатора (как правило карта proximity, ключ Touch Memory), управления исполнительным устройством (замок, турникет, пр.).

Есть устройства, выполняющие дополнительные функции, в частности - охранные). Основной технической характеристикой рассматриваемого оборудования является объем памяти для хранения информации о количестве идентификаторов (карт доступа), системных событиях.

Считыватель предназначен для передачи данных об идентификаторе СКУД контроллеру. Может быть специализированным (считыватель proximity карт), комбинированным (считыватель proximity, Touch Memory).

Исполнительное устройство - это замки, турникеты, шлагбаумы и т.д.).

Преобразователь интерфейса - устройство, осуществляющее сопряжение интерфейса контроллеров и сервера контроля доступа.

3.2.2 Разработка структурной схемы

Исходя из предложенного состава аппаратных компонентов контроллера СКУД на основе платформы Arduino, в работе была разработана структурная схема контроллера, представляющая собой набор программных модулей микроконтроллера Arduino и их взаимосвязи между собой, а также с встроенными датчиками и интерфейсными модулями.

Кроме того, предложенная структурная схема определяет набор информационных структур, участвующих в процессе функционирования контроллера СКУД.

Разработка структурной схемы контроллера СКУД велась, исходя из предположения, что разрабатываемый контроллер будет автономным, однако, при этом будет иметь возможность подключения к локальной сети для обеспечения взаимодействия с централизованным сервером СКУД.

Автономность разрабатываемого контроллера СКУД предлагается обеспечивать путем хранения базы данных пользователей СКУД на flash-накопителе, устанавливаемом в слот SD-карт на интерфейсном модуле Ethernet Shield. Такое решение позволяет обеспечить сокращение времени выработки сигнала управления для исполнительного устройства.

Параллельно информация об идентификаторе пользователя будет дублироваться по сети в базу аудита сервера СКУД, позволяющую сохранять сведения о процессе функционирования множества автономных контроллеров СКУД.

Особенности функционирования каждого конкретного контроллера в составе СКУД предлагается конфигурировать с использованием специального конфигурационного файла, также хранящегося на flash-накопителе.

Поскольку информация базы данных СКУД и конфигурационного файла, хранимая на flash-карте, а также данные между контроллером и сервером СКУД потенциально доступна для непреднамеренной или злонамеренной модификации, одним из вариантов защиты этих данных является их шифрование.

Исходя из представленных выше особенностей, была разработана структурная схема исполнительного устройства (контроллера) СКУД на основе платформы Arduino. Разработанная схема представлена на рисунке 3.6.

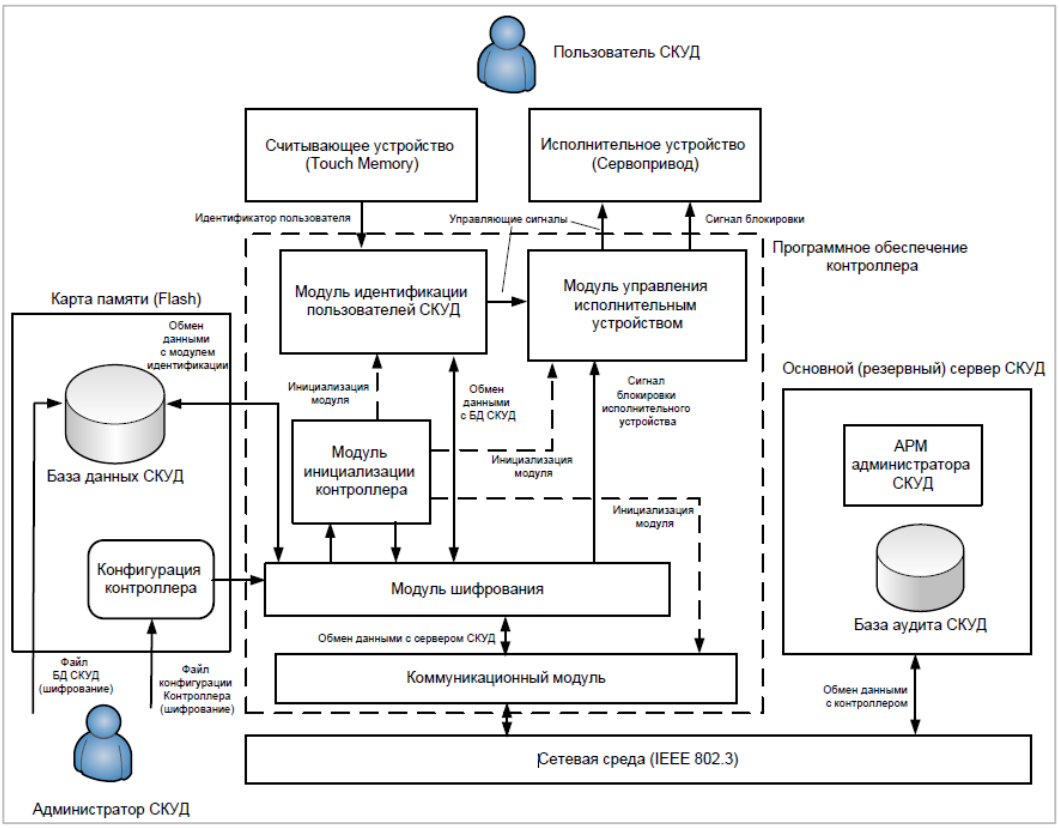

Рисунок 3.6 – Структурная схема контроллера СКУД на основе платформы Arduino

Из рисунка 3.6 видно, что структурно контроллер СКУД на основе платформы Arduino состоит из следующих модулей:

а) модуль шифрования – в зависимости от начальной конфигурации контроллера обеспечивает шифрование/дешифрование следующих данных:

1) хранящихся на flash-накопителе контроллера (интерфейсный модуль Ethernet Shield);

2) поступающих из/в локальной сети (интерфейсный модуль Ethernet Shield);

3) взаимодействия остальных модулей контроллера в процессе функционирования;

б) модуль инициализации контроллера – реализует функции запуска модулей идентификации пользователей СКУД и управления исполнительным устройством на основе данных из конфигурационного файла;

в) модуль идентификации пользователей СКУД – получает и декодирует сигнал со считывающего устройства Touch Probe, преобразуя его в идентификационный номер пользователя СКУД;

г) модуль управления исполнительным устройством – получает управляющий или блокирующий сигналы, обеспечивающие срабатывание;

д) блокировку работы исполнительного устройства (интерфейсный модуль Motor Shield);

е) коммуникационный модуль – обеспечивает преобразование индентификационной информации в формат ethernet-кадров для передачи ее по локальной сети (интерфейсный модуль Ethernet Shield).

Базовыми информационными структурами, необходимыми для функционирования перечисленных выше модулей, являются:

а) база данных СКУД – информация о соответствии уникального идентификатора пользователя СКУД и возможности его прохождения, через заградительное устройство, оборудованное данным контроллером;

б) файл конфигурации контроллера – текстовый файл определенной структуры, на основании данных которого модуль инициализации контроллера производит его начальную конфигурацию.

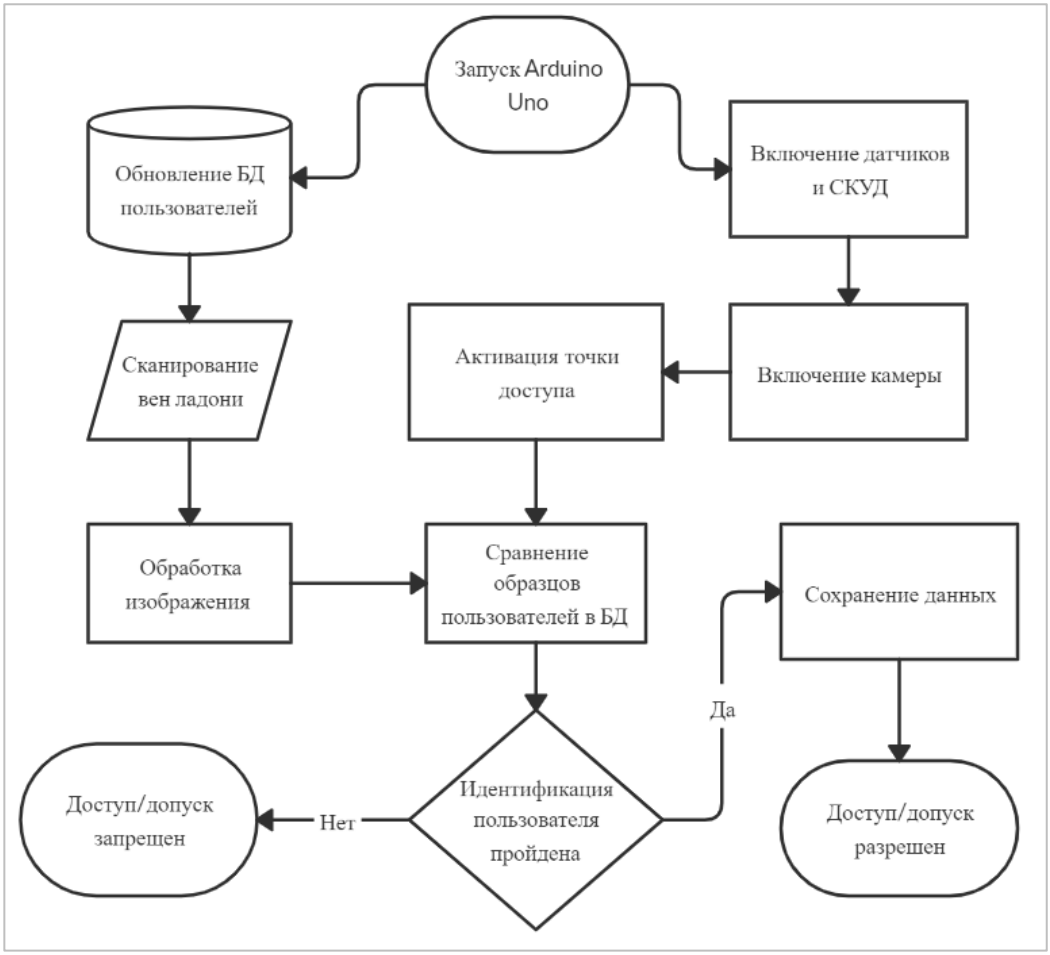

Рисунок 3.7 – Блок-схема

Разработанная структурная схема позволила определить базовые функциональные модули разрабатываемого контроллера СКУД, реализующие процесс его функционирования.

Разрабатываемое в рамках дипломной работы исполнительное устройство (контроллер) ориентировано применение в рамках сетевых СКУД с гибридной структурой, в которой имеется централизованный сервер, обеспечивающий решение задач управления множеством пользователей СКУД и их разрешений, а также управление базой данных аудита активности пользователей СКУД и множество контроллеров, способных функционировать, как в автономном режиме (с применением локальной базы данных пользователей СКУД), так и к сетевом режиме обмена данными с централизованным сервером (рисунок 3.7).

В соответствии с этим важной задачей является разработка схемы функциональной структуры процесса функционирование такого исполнительного устройства.

В качестве формальной основы для разработки схемы функциональной структуры была выбрана методология IDEF0.

3.3 Разработка электрической принципиальной схемы на основе платформы Arduino

Исполнительное устройство на основе платформы Arduino состоит из следующих элементов:

а) микроконтроллерная плата Arduino Uno;

б) 2 резистора 4,7 КОм, 6 резисторов 470 Ом;

в) 2 транзистора КТ940А;

г) ИК-термометр MLX90614;

д) ИК-датчик расстояния Sharp GP2Y0A21YK;

е) 6 ИК-диодов 850 нм;

ж) фототранзистор.

ИК-диоды D1-D6 выполняют роль электрических замков, загораются зеленым или красным цветом, что соответствует открываю дверей.

Резисторы R7 и R8 обеспечивают ограничение тока в цепях считывания пользовательской информации с ключевых носителей.

Транзисторы обеспечивает функцию перезагрузки микроконтроллера в случае сбоя в работе.

Датчики обеспечивают считывание и анализ информации.

Фототранзистор использовался для измерения засветки прибора посторонним светом.

Схема электрическая принципиальная компонентов исполнительного устройства на основе платформы Arduino приведена на рисунке 3.8.

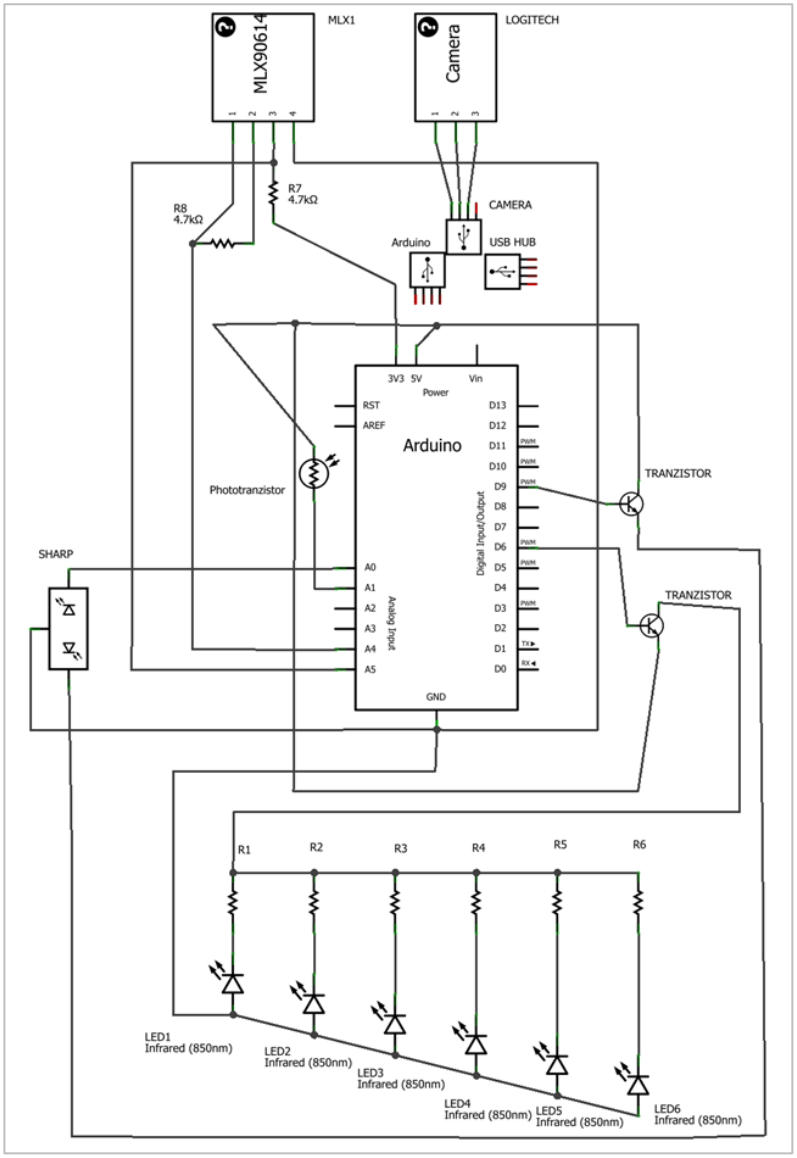

Рисунок 3.8 – Электрическая схема

Учитывая условия, при которых не довелось сконструировать модель данного устройства, было решено смоделировать данную часть работы в программной среде Proteus 8.7 Professional используя все доступные в этой программе библиотеки (рисунок 3.9). ПО для данного продукта было написано на языке программирования Arduino, который в свою очередь основан на языках C/C++. Он очень просто в усвоении, и на данный момент Arduino – это, пожалуй, один из самых удобных способов программирования устройств на микроконтроллерах. Также в приложении А приведен листинг программы для данного продукта.

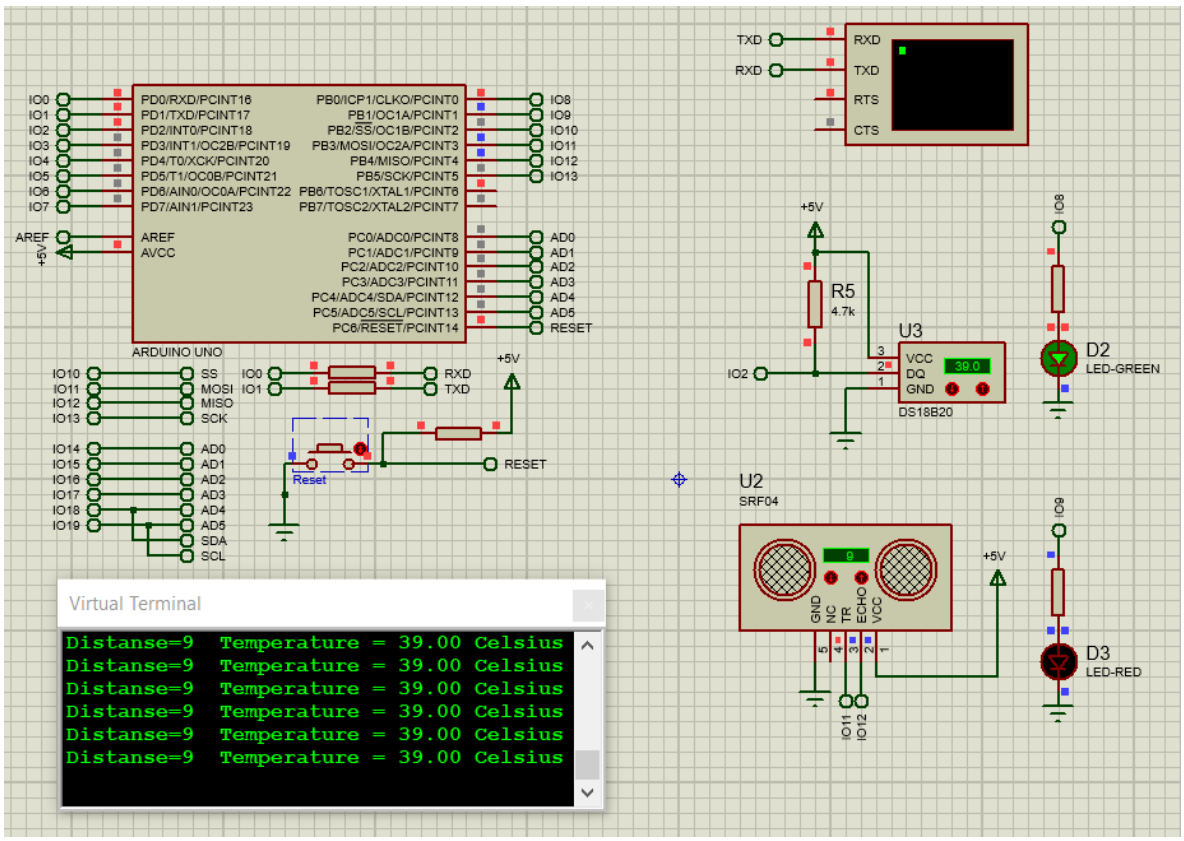

Рисунок 3.9 – Модель устройства на Proteus

4 Бизнес – план

4.1 Резюме

Биометрия — это наука, основанная на описании и измерении характеристик тела живых существ.

В применении к системам автоматической идентификации под биометрическими понимают те системы и методы, которые основаны на использовании для идентификации или аутентификации каких-либо уникальных характеристик человеческого организма.

Наша жизнь наполнена ситуациями, когда нам нужно доказать, кто мы. Такими ситуациями наполнена как личная, так и профессиональная сфера.

Нетрудно перечислить широкий спектр отраслей, которые требуют быстрой, надежной и удобной аутентификации пользователя: доступ к персональному компьютеру или смартфону, доступ к электронной почте, банковские транзакции, открытие дверей и запуск двигателя вашего автомобиля, контроль доступа в помещения, пересечение государственных границ, и вообще, как правило любое взаимодействие с государственными органами власти требует идентификации.

Таким образом, идентификация и аутентификация нашей личности стали краеугольным камнем в современном обществе, обеспечивая безопасное взаимодействие, предотвращая мошенничество и преступность.

Главной задачей данного проекта является создание датчика биометрической идентификации, в дальнейшем совершенной системы, для определения личности человека и его данных. Используя при этом микроконтроллер и базу данных, с их помощью будет возможно считывание, хранение и анализ полученных данных. Для реализации проекта будут применены: Arduino Uno, ИК термометр модели MLX90614, ИК датчик расстояния модели Sharp GP2Y0A21YK и камера Logitech HD Webcam B910.

Разработанная система будет снимать рисунок вен ладони человека, сканировать его, обрабатывать и сравнивать с рисунками в базе данных. Далее, выдавать разрешение или запрет на пропуск, доступ данному человеку. Возможности системы имеют огромный потенциал, так как данный метод биометрической идентификации освоен не полностью.

4.2 Характеристика предлагаемого продукта

Система контроля доступа представляет собой биометрическую систему, располагаемую на пропускных пунктах предприятий или компаний в целях контроля и ограничения доступа, отслеживания времени, в которое был произведен доступ, а также кем, то есть в целях учета посещаемости. В проекте задействованы базы данных для организаций, требуемые для бесконтактной идентификации личности при помощи основополагающего компонента системы – микроконтроллера Arduino Uno.

4.3 Анализ рынка сбыта

J’son & Partners Consulting представляет краткие результаты исследования мирового рынка биометрических систем. Уже сейчас системы биометрической идентификации стали зрелым технологическим направлением развития с большим количеством успешно реализованных проектов по всему миру. В связи с этим анализ как общих тенденций и перспектив, так и детальной информации о динамике развития ключевых сегментов в разрезе, отраслей применения и регионов, представляется актуальным.

Согласно, оценкам J’son & Partners Consulting, объем мирового рынка биометрических систем достигнет более $14 млрд. на конец 2016 года. На ближайшие 6 лет средние темпы роста CAGR для биометрического рынка составит 18,6%, а прогнозируемый объем рынка к 2022 году вырастет до $40 млрд.

Приведенные оценки объема биометрического рынка основаны на показателях выручки ключевых игроков в зависимости от сегментов и учитывают оборудование, программное обеспечение и интеграцию, при этом не учитывались расходы, связанные с дальнейшим обслуживанием систем, если таковое предполагается проектом.

Мировой рынок биометрических решений вступил в фазу активных инноваций и интенсификации применения как в правительственных, силовых, правоохранительных и оборонных структурах, так и в коммерческом сегменте, высокими темпами интегрируясь в банковский сектор, ритейл, мобильные приложения, Интернет вещей, здравоохранение, образование и т.д. Банки, платежные системы, торговые сети, кафе и другие сервисы активно внедряют биометрические технологии. С одной стороны, это помогает защитить клиентов от мошенников –преодолеть шифры двойной, а то и тройной биометрической идентификации гораздо сложнее, чем подобрать ПИН-код. С другой — это упрощает финансовые операции: покупки, денежные переводы и оплата услуг становятся легкими и быстрыми.

Кроме того, биометрия — это защита на случай экстренных ситуаций. В Японии после разрушительного землетрясения и цунами в марте 2011 года множество людей лишись не только своих банковских карт, но и документов. Они вынуждены были проходить через долгие и утомительные процедуры идентификации личности, чтобы снять деньги со своих счетов. После этого в стране создали единую биометрическую систему, которая исключает такую проблему в будущем.

Наиболее активными странами по реализации биометрических проектов в 2015-2016 гг. были США, Великобритания, Канада, Индия, Япония, Китай, Бразилия, Франция, Южная Корея и Германия, Нидерланды, а также ЮАР, Саудовская Аравия, ОАЭ, Нигерия и Мексика. Рынок биометрических систем Северной Америки, являясь в настоящее время самым крупным, к 2022 году

потеряет в своей доле, а наиболее перспективными регионами для внедрения биометрии выглядят Латинская Америка, Азия и Ближний Восток.

По мнению J'son & Partners Consulting, Россия, Индия, Мексика — это три страны, в которых прогнозируются высокие темпы роста рынка биометрических технологий в ближайшие 5-7 лет.

4.4 Организационный план

Для того, чтобы осуществить данный проект требуется финансирование на:

а) закупку технических средств с целью сбора устройства;

б) оплату труда специалистам.

Для установления общего числа инвестиций при создании интегрированной системы необходимо суммировать затраты.

4.5 Расчёт капитальных затрат

Инвестиционный капитал (IC – Invest Capital) или капитальные вложения включают в себя стоимость оборудования, монтажных работ и транспортных услуг, т.о определяется величина капитальных затрат. Для этой цели составляются сметы на приобретение оборудования. Кроме того, учитываются затраты на строительство здания, сооружения и т.д. Общие капитальные вложения (IC – инвестиционный капитал) [16]:

$$\Sigma IC = К_о + К_м + К_{тр} + К_{ус} \quad (4.1)$$

где $К_о$ – капитальные вложения на приобретение оборудования (линейных, стационарных и др.);

$К_м$ – капитальные вложения на монтажные работы;

$К_{тр}$ – капитальные вложения на транспортные расходы (5-10% от стоимости оборудования);

$К_{ус}$– затраты для доставки и установки оборудования.

Таблица 4.1 – Стоимость оборудования для реализации проекта [17]

Наименование	Количество штук	Цена за единицу, тг.	Итого, тг.
Arduino Uno	1	5.000	5.000
ИК термометр MLX90614	1	12.400	12.400
Соединительные провода (комплект)	1	500	500
ИК датчик Sharp GP2Y0A21YK	1	5.800	5.800
Logitech B910 HD Webcam	1	10.200	10.200
ИК-диод 850 нм	6	80	480

Резистор 4.7 кОм	2	50	100

Продолжение таблицы 4.2

Транзистор	2	120	240
Фототранзистор	1	280	280
Итого:			35.000

Капитальные вложения на монтажные работы составляют 5% от стоимости оборудования. Исходя из этого, получим:

$$К_м = 0.05 \cdot К_о, \quad (4.2)$$

$$К_м = 0.05 \cdot 35.000 = 1.750 \text{ (тенге)}.$$

Транспортные расходы составляют 5% от стоимости оборудования Исходя из этого, получим, взята из [18]:

$$К_{тр} = 0.05 \cdot К_о, \quad (4.3)$$

$$К_{тр} = 0.05 \cdot 35.000 = 1.750 \text{ (тенге)}.$$

Применяя полученные параметры, общие капитальные вложения по формуле (4.1) составят:

$$\Sigma IC = 35.000 + 1750 + 1750 = 38.500 \text{ (тенге)}.$$

4.6 Годовые эксплуатационные расходы

В состав эксплуатационных расходов относятся следующие виды затрат: заработная плата работников, социальный налог, электроэнергия, амортизационные отчисления и накладные расходы.

4.6.1 Расчет заработной платы труда

По закону Республики Казахстан на 2020 год минимальная заработная плата составляет 42.500 тенге, в зависимости от стажа и опыта работы средняя заработная плата одного работника варьируется.

Таблица 4.2 – Данные о количестве людей, заработной плате обслуживающего персонала новой системы управления. [19]

№	Должность	Количество	Месячный оклад, тенге	Общая сумма, тг.год
1	Программист	1	80.000	960.000

Дополнительная заработная плата (складывается из количества заявок):

$$ЗП_{доп} = N_{ср} \cdot 2500 \text{ (тенге)}, \quad (4.4)$$

$$ЗП_{доп} = 100 \cdot 10000 = 1000000 \text{ (тенге)}.$$

где N – среднее количество заявок на доставку и установку оборудования.

Расходы по заработной плате (фонд оплаты труда) определяются по формуле 4.5:

$$ФОТ = ЗП_{12} + ЗП_{доп}, \quad (4.5)$$

$$ФОТ = 960.000 + 1.000.000 = 1.960.000 \text{ (тенге)}.$$

4.6.2 Расчет расходов на социальный налог

Социальный налог составляет 9,5% от ФОТ, после отчисления 10% от ФОТ в пенсионный фонд.

Рассчитаем по формуле:

$$С_н = 0{,}095 \cdot (ФОТ - 0{,}1 \cdot ФОТ), \quad (4.6)$$

$$С_н = 0.095 \cdot (1.960.000 - 0.1 \cdot 1.960.000) = 167.580 \text{ (тенге)}.$$

4.6.3 Расчет амортизационных отчислений

Годовая норма амортизации выражается в процентном соотношении к первичной (восстановительной) стоимости имущества и рассчитывается по формуле:

$$К = (1 : n) \cdot 100\%, \quad (4.7)$$

$$К = (1 : 5) \cdot 100\% = 20\%,$$

где К – годовая норма амортизации;

n – срок эксплуатации в годах (в данном случае – 5 лет).

Амортизационные отчисления равны:

$$А = 0.2 \cdot К, \quad (4.8)$$

$$А = 0.2 \cdot 38.500 = 7700 \text{ (тенге)},$$

где К – сумма капитальных затрат, тенге.

4.6.4 Расчет расхода на материалы и запасные части

Расходы на материалы и запасные части составляют 0,5% в год от суммы капитальных затрат:

$$Р_м = 0.005 \cdot К, \quad (4.9)$$

$$Р_м = 0.005 \cdot 38.500 = 192{,}5 \text{ (тенге)}.$$

4.6.5 Расчет расходов на электроэнергию для производственных нужд

Расходы на электроэнергию рассчитываются по следующей формуле:

$$Р_{эл} = 8760 \cdot Ц_{кВт} \cdot W, \quad (4.10)$$

где $Ц_{кВт}$ – цена одного киловатта электроэнергии, договорная, составляющая на данный момент в среднем по Казахстану 15,15 тенге за 1 кВт/ч.

Общая потребляемая мощность оборудования, включая все устройства – 1 кВт [20].

$$Р_{эл} = 8760 \cdot 15.15 \cdot 1 = 132.714 \text{ (тенге)}. \quad (4.10)$$

4.6.6 Накладные расходы

Определим по формуле:

$$Р_{накл} = 0.4 \cdot (ФОТ + С_н + А + Р_м + Р_{эл}), \quad (4.11)$$

$Р_{накл}$= 0.4 · (1.960.000+167.580+7.700+192,5+132.714) = 907.274,6 (тенге).

4.6.7 Годовые эксплуатационные расходы

Эксплуатационные расходы:

$$Э_{год} = Р_{накл} + ФОТ + С_н + А + Р_м + Р_{эл}, \quad (4.12)$$

$Э_{год}$ = 907274.6+1960000+167580+7700+192.5+132714 = 3175461.1 (тенге).

Эксплуатационные расходы предприятий включают текущие затраты, амортизационные отчисления, налоговые выплаты изображено в таблице 4.3.

Таблица 4.3 – Эксплуатационные расходы

Статьи затрат	Сумма затрат, тенге
Фонд оплаты труда	1960000
Социальный налог	167580
Амортизационные отчисления	7700

Расходы на запасные части и материалы	192.5
Расходы на электроэнергию	132714

Продолжение таблицы 4.3

Накладные расходы	907274.6
Итого:	3175461.1

К текущим эксплуатационным расходам относят затраты, связанные с использованием в процессе производства энергии, материалов, труда, а также затраты на реализацию продукции. Выраженные в денежной форме текущие затраты предприятия на производство и сбыт продукции представляют собой себестоимость.

4.6.8 Себестоимость продукта:

$$С_п = \frac{ΣIC+Э_{год}}{n}, \quad (4.13)$$

$С_П$ = (38500+3175461.1)/100=32139.6 (тенге).

4.7 Расчет доходов, прибыли и чистой прибыли

Доходы от реализаций услуг представляют собой выручку от реализации пользователям услуг по установленным тарифам и определяются умножением тарифа на количество реализованных услуг:

$$Д_{ру} = Σp_i \cdot q_i, \quad (4.14)$$

где q_i – количество услуг связи i-го вида;
p_i – тариф на услугу i-го вида.

$$Д_{ру} = 100 \cdot 4000 + 200 \cdot 2000 = 800000 \text{ (тенге)}.$$

Доходы предприятия – это денежные средства, получаемые за реализацию продукции и предоставляемые услуги. Планируется реализовывать в среднем 100 устройств год, и предоставлять техобслуживание раз в полгода. Предварительная цена за продукт формируется из себестоимости (4.13) и наценкой на нее в данном случае наценка составляет 24,4% и стоимость продукта составит 40000 тенге.

$$Д = 100 \cdot 40000 = 4000000 \text{ (тенге)}.$$

Прибыль от реализации услуг исчисляют как разницу между доходами от реализации услуг (или собственными для предприятий где применяется

этот показатель) и затратами. Прибыль облагается корпоративным 20% налогом. После налогообложения прибыль называется чистой прибылью.

$$П_{реал} = (Д_{ру} + Д) - \sum Э_р, \quad (4.15)$$

$П_{реал}$ = (800000+4000000)-(38500+3175461.1) = 1586038.9 (тенге).

Подоходный налог:

$$П_н = 0.2 \cdot П_{реал}, \quad (4.16)$$

$$П_н = 0.2 \cdot 1586038.9 = 317207.8 \text{ (тенге)}.$$

Чистая прибыль:

$$ЧП = П_{реал} - П_н, \quad (4.17)$$

$$ЧП = 1586038.9 - 317207.8 = 1268831.1 \text{ (тенге)}.$$

Коэффициент экономической эффективности рассчитывается по формуле:

$$E = ЧП/IC, \quad (4.18)$$

$$E = 1268831.1/3850000 = 0.33.$$

Срок окупаемости рассчитываем по формуле:

$$T = 1/E, \quad (4.19)$$

$$T = 1/0.33 = 3 \text{ (года)}.$$

4.8 Оценка срока окупаемости проекта с учетом фактора времени

При принятии долгосрочных инвестиционных решений в бизнесе следует прогнозировать их эффективность. Для этого рассчитываются следующие показатели:

– чистая приведенная стоимость - NPV (Net Present Value);

– индекс рентабельности инвестиций - PI (Profitability Index);

– дисконтированный срок окупаемости инвестиций - DPB (Discounted Payback Period).

Международная практика оценки эффективности проектов основана на концепции временной стоимости денег. Оценка эффективности использования вложенного капитала производится путем сравнения денежных потоков (денежных потоков), возникающих в ходе реализации инвестиционного проекта и первоначальных инвестиций. Проект считается

эффективным, если он обеспечивает возврат первоначальной суммы инвестиций и требуемый доход для инвесторов, предоставивших капитал.

Вложенный капитал, а также денежные потоки вводятся за текущий год или в определенный отчетный год (который обычно предшествует началу проекта).

Дисконтирование – это процесс приведения (корректировки) будущей стоимости денег к их текущей стоимости (текущей стоимости).

Процесс дисконтирования капитальных вложений и денежных потоков осуществляется по различным ставкам дисконтирования, которые определяются в соответствии с характеристиками инвестиционных проектов. Ставки дисконтирования могут быть установлены инвестором на основе годового процента прибыли, которую он хочет или может иметь на вложенный капитал.

Коэффициент дисконтирования рассчитывается по формуле:

$$\alpha_t = \frac{1}{(1+r)^t}, \tag{4.20}$$

где α_t - коэффициент дисконтирования;

r - норма дисконта;

t - номер шага расчета.

$$\alpha_1 = \frac{1}{(1+0.2)^1} = 0.83,$$
$$\alpha_2 = \frac{1}{(1+0.2)^2} = 0.69,$$
$$\alpha_3 = \frac{1}{(1+0.2)^3} = 0.58,$$
$$\alpha_4 = \frac{1}{(1+0.2)^4} = 0.48,$$
$$\alpha_5 = \frac{1}{(1+0.2)^5} = 0.4.$$

Чистая приведенная стоимость (Net Present Value – NPV) относится к группе методов дисконтирования денежных потоков или методов DFC.

Пусть I_0 — сумма первоначальных затрат, т.е. сумма инвестиций на начало проекта;

PV — современная стоимость денежного потока на протяжении экономической жизни проекта.

Общая накопленная стоимость дисконтированной выручки рассчитывается по формуле:

$$PV = \sum_{t=1}^{n} \frac{P_t}{(1+r)^t} \tag{4.21}$$

где r - норма дисконта;

n — число периодов реализации проекта;

P_t — чистый поток платежей в периоде t.

$$PV = \frac{1268831.1}{(1+0.2)} + \frac{1522597.3}{(1+0.2)^2} + \frac{1776363.5}{(1+0.2)^3} + \frac{2030129.8}{(1+0.2)^4} + \frac{2283896.0}{(1+0.2)^5} =$$

$$= 5039589.6 \text{ (тенге).}$$

Текущая стоимость затрат (I_0) сравнивается с текущей стоимостью доходов (PV). Разность между ними составляет чистую текущую стоимость проекта (NPV):

$$NPV = \sum_{t=1}^{n} \frac{CF_t}{(1+r)^t} - I_O; \qquad (4.22)$$

$$\text{NPV} = 5039589.6 - 3850000 = 1189589.6 \text{ (тенге).}$$

Если вычисленная таким образом чистая текущая стоимость потока платежей имеет положительный знак (NPV > 0), это означает, что в течение своей экономической жизни проект возместит первоначальные затраты Io, обеспечит получение прибыли согласно заданному стандарту г, а также ее некоторый резерв, равный NPV. Если NPV < 0, то проект имеет доходность ниже рыночной и поэтому проект следует отвергнуть. Если NPV=0, то проект не является ни прибыльным, ни убыточным.

Индекс рентабельности (доходности) инвестиций (PI). Индекс рентабельности – это отношение суммы вышеуказанных эффектов к стоимости инвестиционных затрат. Индекс рентабельности (PI) рассчитывается по формуле:

$$PI = \sum_{k} \frac{P_k}{(1+r)^k} \Big/ I, \qquad (4.23)$$

$$\text{PI} = 5039589.6/3850000 = 1.31.$$

Очевидно, что если:

а) PI > 1, то проект должен быть принят;

б) PI< 1, тогда проект должен быть отклонен;

в) PI =1, тогда проект ни прибыльный, ни убыточный.

Логика критерия PI заключается в следующем: он характеризует доход на единицу стоимости.

В отличие от чистого приведенного эффекта индекс рентабельности является относительным показателем.

Внутренняя норма доходности инвестиций (IRR) представляет собой ту норму дисконта (r вн.) при которой дисконтированные доходы от проекта равны инвестиционным затратам. IRR = r, при котором NPV = f(r) = 0.

Внутренняя норма доходности определяет максимально приемлемую ставку дисконта, при которой можно инвестировать средства без каких-либо потерь для собственника. Её значения находят исходя из следующего уравнения.

$$NPV = \sum_{t=1}^{n} \frac{CF_t}{(1+IRR)^t} - I_O = 0. \qquad (4.24)$$

Современные табличные процессоры позволяют быстро и эффективно определить этот показатель путем использования специальных функций, или применяется метод последовательных итераций с использованием табулированных значений дисконтирующих множителей. Для этого с помощью таблиц в Microsoft Excel (рисунок 4.1), выбираются два значения коэффициента дисконтирования r1<r2 таким образом, чтобы в интервале (r1, r2) функция *NPV=f(r)* меняла свое значение с "+" на "-" или с "-" на "+". Далее применяют формулу для расчета.

Ниже приведены расчеты для определения максимальной приемлемой ставки дисконта, производится это методом подбора ставки дисконтирования.

$$IRR = r_1 + \frac{NPV(r_1)}{NPV(r_1) - NPV(r_2)}(r_2 - r_1), \qquad (4.25)$$

$$IRR = 0.3 + \frac{161434.06}{161434.06 - (-566379.6)} \cdot (0.4 - 0.3) = 0.3221.$$

		Значения дисконтированных доходов		
Норма дисконта	0,2	0,30	0,4	0,5
Год				
1	1057359,3	976023,9231	906307,9286	845887,4
2	1057359,25	900945,1598	776835,3673	676709,92
3	1027988,16	808540,528	647362,8061	526329,938
4	979036,3426	710804,8598	528459,4336	401013,286
5	917846,5712	615119,5902	424654,902	300759,964
PV	5039589,623	4011434,061	3283620,438	2750700,51
NPV	1189589,623	161434,0608	-566379,5624	-1099299,49

Рисунок 4.1 – Подбор значении коэффициента дисконтирования

Таким образом, можно поднять ставку дисконта до 32,21%, но тогда проект не будет приносить прибыль, но и не будет затратным.

Срок окупаемости является одним из самых простых и распространенных в мировой практике; это не подразумевает временную рационализацию притока денежных средств.

Он состоит в расчете количества лет, необходимых для полного возмещения первоначальных затрат, то есть момент определяется, когда денежный поток дохода равен сумме денежного потока расходов (расчет чистая приведенная стоимость с накопленной суммой). Если прибыль распределяется неравномерно, период восстановления рассчитывается путем прямого подсчета количества лет, в течение которых инвестиции будут возмещены накопленным доходом.

$$\mathrm{DPP} = \mathrm{t} + \frac{\mathrm{IC} - (\mathrm{PV}_1 + \mathrm{PV}_2 + \cdots + \mathrm{PV}_\mathrm{t})}{\mathrm{PV}_{\mathrm{t}+1}}, \tag{4.26}$$

$$\mathrm{DPP} = 3 + \frac{3850000 - 3142706.8}{979036{,}34} = 3.7 \text{ (года)}.$$

4.9 Выводы

В этой части дипломной работы были рассчитаны необходимые затраты по капитальным вложениям, эксплуатационные расходы, расходы на электроэнергию, материальные расходы, фонд оплаты труда работников, амортизационные отчисления, накладные расходы, доходы и расчет показателей экономической эффективности. Произведен перерасчет расходов и подсчитана экономическая прибыль с этих операций.

По полученным значениям можно увидеть, данная система экономически себя оправдывает, и теоретический расчетный срок окупаемости этой системы равен 3.7 годам.

В настоящее время инвестиции считают привлекательными при сроке окупаемости $\leq$ 5 лет. Следовательно, можно сделать вывод, что проектирование систем биометрической аутентификации для контроля доступа является экономически оправданным, и может быть принято к реализации. Данная система имеет преимущества на рынке в виде возможности усовершенствования и сведения эксплуатационных затрат к минимуму.

5 Безопасность жизнедеятельности

5.1 Анализ потенциально опасных и вредных факторов, воздействующих на персонал при работе с персональным компьютером (ПК)

В последние годы большое внимание уделяется улучшению условий труда пользователей электронно-вычислительных машин (ПЭВМ) и видеодисплейных терминалов (ВДТ), учитывая, что качество и безопасность самых ПЭВМ и ВДТ постоянно улучшаются. В развитых странах, в том числе в США, Германии, Швеции, вопрос об опасности работы за дисплеями поднялся до уровня национальной проблемы, а в Германии работа за дисплеями входит в список 40 наиболее вредных и опасных профессий.

Работа с персональным компьютером — это воспроизведение визуальной информации на дисплее, которая должна быстро и точно восприниматься пользователем. [21]

Основным фактором, влияющим на производительность труда людей, работающих с ПЭВМ и ВДТ, являются комфортные и безопасные условия труда.

Условия труда пользователя, работающего с персональным компьютером, определяются:

а) особенностями организации рабочего места;

б) условиями производственной среды (освещением, микроклиматом, шумом, электромагнитными и электростатическими полями, визуальными эргономическими параметрами дисплея и т. д.);
характеристиками информационного взаимодействия человека и персональных электронно-вычислительных машин.

5.1.1 Классификация опасных и вредных факторов при выполнении работ на ПК

При выполнении работ на персональном компьютере (ПК) согласно ГОСТу 12.0.003-74 “ССБТ. Опасные и вредные производственные факторы. Классификация” могут иметь место следующие факторы:

1) повышенная температура поверхностей ПК;
2) повышенная или пониженная температура воздуха рабочей зоны;
3) выделение в воздух рабочей зоны ряда химических веществ;
4) повышенная или пониженная влажность воздуха;
5) повышенный или пониженный уровень отрицательных и положительных аэроионов;
6) повышенное значение напряжения в электрической цепи, замыкание;
7) повышенный уровень статического электричества;
8) повышенный уровень электромагнитных излучений;
9) повышенная напряженность электрического поля;
10) отсутствие или недостаток естественного света;

11) недостаточная искусственная освещенность рабочей зоны;
12) повышенная яркость света;
13) повышенная контрастность;
14) прямая и отраженная блесткость;
15) зрительное напряжение;
16) монотонность трудового процесса;
17) нервно-эмоциональные перегрузки.

Работа на компьютере сопровождается постоянным и значительным напряжением функции визуального анализатора. Одной из основных особенностей является другой принцип чтения информации, чем обычное чтение. Во время обычного чтения текст на бумаге, размещенной горизонтально на столе, читается рабочим, опустившим голову, когда на него падает поток света. При работе на ПК работник читает текст практически не наклоняя головы, его глаза выглядят прямыми или почти прямыми, текст (источником является люминесцентное вещество экрана) формируется на другой стороне экрана, так что пользователь не читает отраженный текст, а смотрит прямо на источник света. Заставив глаза и органы зрения в целом работать в стрессовом режиме, который долгое время был для него необычным.

Нарушения зрения резко возрастают при работе более четырех часов в день. Всемирная организация здравоохранения (ВОЗ) представила концепцию «Компьютерного Зрительного Синдрома» (КЗС), типичными симптомами которой являются жжение в глазах, покраснение век и конъюнктивы, ощущение инородного тела или песка под веками, боль в глазах и лбу, помутнение зрения, медленная фокусировка от объектов вблизи к дальним.

Нейро-эмоциональный стресс при работе на ПК возникает из-за нехватки времени, большого объема и плотности информации, особенностей коммуникационного диалога между человеком и ПК, ответственности за достоверность информации. Длительная работа на экране, особенно в интерактивном режиме, может привести к нервно-эмоциональной перегрузке, нарушениям сна, ухудшению состояния, снижению концентрации внимания и работоспособности, хронической головной боли, повышенной возбудимости нервной системы, депрессия. [22]

Кроме того, с ростом нервно-психических стрессов в сочетании с другими вредными факторами витамины и минералы «выбрасываются» из организма. При работе в условиях повышенного нервно-эмоционального и физического напряжения, гиповитаминоз, недостаток микроэлементов и минералов (особенно железа, магния, селена) ускоряют и ухудшают чувствительность к воздействию факторов, экологические и производственные воздействия, нарушают обмен веществ, приводят к износу и старению организма. Поэтому, при постоянной работе на ПК для повышения эффективности и поддержания здоровья, меры безопасности включают защиту организма с помощью витаминно-минеральных

комплексов, которые рекомендуются всем пользователям ПК, даже в добром здравии.

Увеличение статических и динамических нагрузок среди пользователей компьютеров приводит к болям в спине, шейному отделу позвоночника и плечам. Из всех недугов, вызванных работой на компьютерах, чаще встречаются те, которые связаны с использованием клавиатуры. Во время операций ввода данных, число небольших стереотипных движений рук и пальцев за смену может превышать 60 тысяч, что согласно медицинской классификации труда, классифицируется как вредное и опасное. Поскольку каждое нажатие клавиши связано с сокращением мышц, сухожилия непрерывно скользят вдоль костей и вступают в контакт с тканями, в результате чего могут развиваться болезненные воспалительные процессы. Воспалительные процессы сухожильных тканей («тендинит») в совокупности называют «повторяющимся стрессовым повреждением».

Большинство работающих рано или поздно начинают предъявлять жалобы на боли в шее и спине. Эти недомогания накапливаются постепенно и получили название «синдром длительных статических нагрузок» (СДСН).

Другой причиной возникновения СДСН может быть длительное пребывание в положении “сидя”, которое приводит к сильному перенапряжению мышц спины и ног, в результате чего возникают боли и неприятные ощущения в нижней части спины. Основной причиной перенапряжения мышц спины и ног являются нерациональная высота рабочей поверхности стола и сидения, отсутствие опорной спинки и подлокотников, неудобное размещение монитора, клавиатуры и документов, отсутствие подставки для ног.

Для существенного уменьшения боли и неприятных ощущений, возникающих у пользователей ПК, необходимы частые перерывы в работе и эргономические усовершенствования, в том числе оборудование рабочего места так, чтобы исключать неудобные позы и длительные напряжения.

К числу факторов, ухудшающих состояние здоровья пользователей компьютерной техники, относятся электромагнитное и электростатическое поля, акустический шум, изменение ионного состава воздуха и параметров микроклимата в помещении. Немаловажную роль играют эргономические параметры расположения экрана монитора (дисплея), состояние освещенности на рабочем месте, параметры мебели и характеристики помещения, где расположена компьютерная техника.

5.1.2 Физически вредные и опасные факторы

К физическим вредным и опасным факторам относятся: повышенные уровни электромагнитного, рентгеновского, ультрафиолетового и инфракрасного излучения; повышенный уровень статического электричества и запыленности воздуха рабочей зоны; повышенное содержание положительных аэроионов и пониженное содержание отрицательных аэроионов в воздухе рабочей зоны; повышенный уровень блесткости и

ослепленности; неравномерность распределения яркости в поле зрения; повышенная яркость светового изображения; повышенное значение напряжения в электрической цепи, замыкание которое может произойти через тело человека. [23]

5.1.3 Психофизические вредные и опасные факторы

Психо-физиологически вредные и опасные факторы: напряжение зрения и внимания; интеллектуальные, эмоциональные и длительные статические нагрузки; монотонность труда; большой объем информации, обрабатываемый в единицу времени; нерациональная организация рабочего места.

Типичными ощущениями, которые испытывают к концу рабочего дня операторы ПЭВМ, являются: переутомление глаз, головная боль, тянущие боли в мышцах шеи, рук и спины, снижение концентрации внимания.

Уже в первые годы компьютеризации было отмечено специфическое зрительное утомление у пользователей дисплеев, получившее общее название «компьютерный зрительный синдром». Одной из причин служит то, что сформировавшаяся за миллионы лет эволюции зрительная система человека приспособлена для восприятия объектов в отраженном свете (печатные тексты, рисунки и т.п.), а не для работы за дисплеем. Изображение на дисплее принципиально отличается от привычных глазу, объектов наблюдения — оно светится, мерцает, состоит из дискретных точек, а цветное компьютерное изображение не соответствует естественным цветам. Но не только особенности изображения на экране вызывают зрительное утомление. Большую нагрузку орган зрения испытывает при вводе информации, так как пользователь вынужден часто переводить взгляд с экрана на текст и клавиатуру, находящиеся на разном расстоянии и по-разному освещенные. Зрительное утомление проявляется жалобами на затуманивание зрения, трудности при переносе взгляда с ближних предметов на дальние и с дальних на ближние, кажущиеся изменения окраски предметов, их двоение, чувство жжения, «песка» в глазах, покраснение век, боли при движении глаз.

Длительная и интенсивная работа на компьютере может стать источником тяжелых профессиональных заболеваний, таких, как травма повторяющихся нагрузок (ТПН), представляющая собой постепенно накапливающиеся недомогания, переходящие в заболевания нервов, мышц и сухожилий руки.

5.1.4 Профессиональные заболевания у пользователей ПК

К профессиональным заболеваниям, связанным с ТПН, относятся:

а) тендовагинит – воспаление сухожилий кисти, запястья, плеча;

б) тендосиновит – воспаление синовиальной оболочки сухожильного основания кисти и запястья;

в) синдром запястного канала (СЗК) – вызывается ущемлением срединного нерва в запястном канале. Накапливающаяся травма вызывает

образование продуктов распада в области запястного канала, в результате чего вначале возникает отек, а затем СЗК.

Появляются жалобы на жгучую боль и покалывание в запястье, ладони, а также пальцах, кроме мизинца. Наблюдается болезненность и онемение, ослабление мышц, обеспечивающих движение большого пальца.

Эти заболевания обычно наступают в результате непрерывной работы на неправильно организованном рабочем месте.

Механизм нарушений, происходящих в организме под влиянием электромагнитных полей, обусловлен их специфическим (нетепловым) и тепловым действием. [24]

Специфическое воздействие ЭМП отражает биохимические изменения, происходящие в клетках и тканях. Наиболее чувствительными являются центральная и сердечно-сосудистая системы. Возможны отклонения со стороны эндокринной системы.

В начальном периоде воздействия может повышаться возбудимость нервной системы, проявляющаяся раздражительностью, нарушением сна, эмоциональной неустойчивостью. В последующем развиваются астенические состояния, т.е. физическая и нервно-психическая слабость. Поэтому для хронического воздействия ЭМП характерны: головная боль, утомляемость, ухудшение самочувствия, гипотония (снижение артериального давления), брадикардия (урежение пульса), боли в сердце. Указанные симптомы могут быть выражены в разной степени.

Тепловое воздействие ЭМП характеризуется повышением температуры тела, локальным избирательным нагревом клеток, тканей и органов вследствие перехода ЭМП в тепловую энергию. Интенсивность нагрева зависит от количества поглощенной энергии и скорости оттока тепла от облучаемых участков тела. Отток тепла затруднен в органах и тканях с плохим кровоснабжением. К ним в первую очередь относится хрусталик глаза, вследствие чего возможно развитие катаракты. Тепловому воздействию ЭМП подвергаются также паренхиматозные органы (печень, поджелудочная железа) и полые органы, содержащие жидкость (мочевой пузырь, желудок). Нагревание их может вызвать обострение хронических заболеваний. [25]

5.2 Расчетная часть

5.2.1 Расчет защиты от электромагнитных полей и излучений

Провести оценку эффективности защитного экрана, представляющего собой камеру размерами 2х1,5х1 м из сетки, изготовленной из медной проволоки диаметром 0,1 мм, шаг сетки - 10 мм, длина волны излучения $\lambda = 6.5 \times 10^6$ м. Работа в условиях поля напряженности 200 кВ/м производится не более трех часов в сутки.

Решение:

По формуле (5.1) определяем частоту излучения:

$$\lambda = \frac{c}{f}, \tag{5.1}$$

$$f = \frac{3 \cdot 10^8}{6.5 \cdot 10^6} = 46{,}2 \text{ (Гц)}.$$

Следовательно, поле промышленной частоты, и нормировать уровень напряженности следует по выражению (5.2):

$$T = \frac{50}{E} - 2, \tag{5.2}$$

$$\text{Е}_{\text{норм}} = \frac{50}{\text{Т} + 2} = \frac{50}{3 + 2} = 10 \left(\frac{\text{кВ}}{\text{м}}\right).$$

т.е. допустимое значение напряженности электрического поля при трехчасовой работе составляет 10 кВ/м.

По формуле (5.3) определяется требуемая эффективность экранирующего устройства:

$$\Delta_{\text{ТР}} = 20\, lg \frac{\text{Е}}{\text{Е}_{\text{норм}}}, \tag{5.3}$$

$$\Delta_{\text{ТР}} = 20\, lg \frac{\text{Е}}{\text{Е}_{\text{норм}}} = 20\, lg \frac{200}{10} = 20\, lg\, 20 = 26 \text{ (дБ)}.$$

По формуле (5.4) находится эквивалентный радиус экрана:

$$R = \sqrt[3]{\frac{3V}{4\pi}}, \tag{5.4}$$

$$R = \sqrt[3]{\frac{3 \cdot 2 \cdot 1{,}5 \cdot 1}{4\pi}} = 0.37 \text{ (м)}.$$

По формуле (5.5) определяем границы зоны индукции (ближней зоны):

$$r = \frac{\lambda}{2\pi}, \tag{5.5}$$

$$r = \frac{6.5 \cdot 10^6}{2\pi} = 1035 \text{ (км)}.$$

т.е. рабочее место находится в зоне индукции.

По выражению (5.6) находится параметр экранирования:

$$\gamma = \frac{d}{2\pi R} (\ln \frac{d}{r_0} - 1{,}25), \tag{5.6}$$

$$\gamma = \frac{10 \cdot 10^{-3}}{2\pi \cdot 0{,}37}(\ln \frac{10 \cdot 10^{-3}}{0{,}5 \cdot 10^{-3}} - 1{,}25) = 0{,}0075 .$$

По выражению (5.7) находим проницаемость экрана:

$$\eta = \frac{3\gamma}{1 + 3\gamma} , \tag{5.7}$$

$$\eta = \frac{3 \cdot 0{,}0075}{1 + 3 \cdot 0{,}0075} = 0{,}022 .$$

По формуле (5.8) определяется фактическая эффективность экрана:

$$\Delta = 20 \lg\left(\frac{1}{\eta}\right), \tag{5.8}$$

$$\Delta = 20 \lg\left(\frac{1}{0{,}022}\right) = 33.15(\partial Б).$$

Проверим выполнения условия формулы (5.9):

$$\Delta_{TP} \le \Delta , \tag{5.9}$$

26дБ < 33.15 (дБ).

Выбранное экранирующее устройство обеспечивает ослабление электрического поля в рабочей зоне.

5.2.2 Расчет электромагнитных полей, часто используемых в рабочих помещениях

Оценка уровня воздействия электростатического поля (ЭСП).

Находим предельно допустимый уровень напряженность электростатического поля при воздействии на персонал более одного часа за смену по формуле:

$$\text{Е}_{\text{ПДУ}} = \frac{60}{\sqrt{t}} = \frac{60}{\sqrt{8}} = 22{,}21 \left(\frac{\text{кВ}}{\text{м}}\right), \tag{5.10}$$

где $\text{Е}_{\text{ПДУ}}$ – предельно допустимый уровень напряженности поля, кВ/м;

t – время воздействия, ч.

ЭМП промышленной частоты предельно допустимый уровень напряженности ЭП на рабочем месте в течение всей смены устанавливается равным 60 кВ/м.

Оценка и нормирование ЭМП промышленной частоты на рабочих местах персонала проводится дифференцированно в зависимости от времени пребывания в электромагнитном поле.

Находим допустимое время пребывания персонала в ЭП при напряженности 5 кВ/м по формуле:

$$\mathrm{T} = \frac{50}{\mathrm{E}} - 2, \tag{5.11}$$

$$T = \frac{50}{\mathrm{E}} = \frac{50}{5} - 2 = 8 \text{ (ч)}.$$

где Т – допустимое время пребывания в ЭП при соответствующем уровне напряженности, ч.

При напряженности ЭП от 20 до 25 кВ/м допустимое время пребывания составляет 10 мин. Пребывание в ЭП с напряженностью более 25 кВ/м без средств защиты не допускается.

Оценка и нормирование ЭМП.

ЭМП диапазона частот 30 кГц – 300 ГГц оценка и нормирование ЭМП осуществляется по величине энергетической экспозиции (ЭЭ). Энергетическая экспозиция ЭМП определяется как произведение квадрата напряженности электрического или магнитного поля на время воздействия на человека. [26]

Находим энергетическую экспозицию в диапазоне частот 30 кГц – 300 МГц по формулам:

$$\text{ЭЭ}_{\mathrm{E}} = \mathrm{E}^2\mathrm{T}, \tag{5.12}$$

$$\text{ЭЭ}_{\mathrm{H}} = \mathrm{H}^2\mathrm{T}, \tag{5.13}$$

где Е – напряженность электрического поля, В/м;

Н – напряженность магнитного поля, А/м;

Т – время воздействия на рабочем месте за смену, ч.

Напряженность магнитного поля подбирается по таблице 5.1.

Таблица 5.1 Воздействие ЭМП на персонал

Время воздействия, мин	Напряженность МП
0-10	24
11-60	16
61-480	8

$$\text{ЭЭ}_{\mathrm{E}} = 5^2 \cdot 8 = 200 \text{ (В/м)}^2 \cdot \text{ч},$$

$$ЭЭ_{Н} = 8^2 \cdot 8 = 72\ (А/м)^2 \cdot ч.$$

Определим энергетическую экспозицию по плотности потока энергии в диапазоне частот 300 МГц – 300 ГГц по формуле:

$$ЭЭ_{ППЭ} = ППЭ^2 Т = 1{,}2^2 \cdot 8 = 11{,}52\ мкВт/см^2, \quad (5.14)$$

где ППЭ – плотность потока энергии (мкВт/см^2).

Предельно допустимые уровни энергетических экспозиций (ЭЭПДУ) на рабочих местах персонала за смену приведены в таблице 5.2.

Таблица 5.2 ПДУ энергетических экспозиций ЭМП диапазона частот 30 кГц – 300 ГГц

Параметр	$ЭЭ_{ПДУ}$ в диапазонах частот, МГц				
	0,03–3,0	3,0–30,0	30,0–50,0	50,0–300,0	300,0-300000,0
$ЭЭ_{Е}(В/м)^2 \cdot ч$	20000	7000	800	800	–
$ЭЭ_{Н}(А/м)^2 \cdot ч$	200	–	0,72	–	–
$ЭЭ_{ППЭ}$мкВт/см^2	–	–	–	–	200

Максимальные допустимые уровни напряженности электрического и магнитного полей, плотности потока энергии ЭМП не должны превышать значений, представленных в таблице 5.3.

Таблица 5.3 Максимальные ПДУ напряженности и плотности потока энергии ЭМП диапазона частот 30 кГц – 300 ГГц

Параметр	$ЭЭ_{ПДУ}$ в диапазонах частот, МГц				
	0,03–3,0	3,0–30,0	30,0–50,0	50,0–300,0	300,0-300000,0
$Е, (В/м)^2$	2500	295	80	80	–
$Н, (А/м)^2$	250	–	3,0	–	–
ППЭ, мкВт/см^2	–	–	–	1000	5000

5.3 Выводы

Важным моментом в комплексе мероприятий направленных на совершенствование условий труда являются мероприятия по охране труда. Этим вопросам с каждым годом уделяется все большее внимание, т.к. забота о здоровье человека стала не только делом государственной важности, но и элементом конкуренции работодателей в вопросе привлечения кадров. Для успешного воплощения в жизнь всех мероприятий по охране труда необходимы знания в области физиологии труда, которые позволяют правильно организовать процесс трудовой деятельности человека.

Имеющийся в настоящее время комплекс разработанных организационных мероприятий и технических средств защиты, накопленный опыт работы ряда вычислительных центров показывает, что имеется

возможность добиться значительно больших успехов в деле устранения воздействия на работающих опасных и вредных производственных факторов.

В разделе безопасности жизнедеятельности проведен анализ опасных и вредных факторов, влияющих на персонал. Уровень условий труда признан допустимым, и показания, взятые из расчетов, полностью подходят под предписание стандартов безопасности жизнедеятельности. Также были определены значения уровня воздействия электромагнитных и электростатических полей на персонал в офисном помещении.

Заключение

В данной дипломной работе была разработана система биометрической идентификации для контроля и управления доступом в промышленных целях на основе микроконтроллера Arduino Uno. Основным объектом предполагаемого внедрения стала промышленная отрасль в нашей стране, которой необходимо вести контроль и учет персонала. Посредством сравнительного анализа, для получения стабильной работы устройства и конкурентоспособного товара на рынке были выбраны следующие средства: микроконтроллер Arduino Uno, ИК-датчики для измерения температуры и расстояния. Основаниями для использования являлись следующие факторы: технические характеристики, удобство использования, цены, преимущества и т.д. В технической части работы указано полное объяснение работы данной системы.

Также было произведено моделирование работы системы. В результате, которой была произведена проверка работы системы в программной среде Proteus.

Произведен расчет защиты от электромагнитных волн и излучений. В результате, которого был определен ослабляющий эффект экранирующего устройства от электрического поля, сделаны соответствующие выводы.

Произведен экономический расчет капитальных вложений, прибыли, экономических затрат, заработной платы рабочих, рассчитана себестоимость и цена товара, рентабельность производства, коэффициент экономической эффективности и сроки окупаемости проекта. Произведен прогноз доходности проекта, в итоге срок окупаемости составит 3,7 года.

Все поставленные задачи дипломной работы были выполнены успешно и внедрение подобной технологии в промышленность принесет выгоду как производителю, так и потребителю.

Список литературы

1. RFID. Статья. // [https://ru.wikipedia.org/wiki/RFID]/ «Radio Frequency Identification» [дата обращения –23.03.2020]
2. RFID. Статья // [https://ru.wikipedia.org/wiki/RFID]/ «Radio Frequency Identification» [дата обращения – 25.03.2020]
3. Техпортал // [http://www.techportal.ru/glossary/biometricheskaya_iden-tifikaciya.html] / «Биометрическая идентификация» [дата обращения – 02.04.2020]
4. Интемс // [https://securityrussia.com/blog/biometriya.html] / «Биометрия от А до Я полное руководство биометрической идентификации и аутентификации» [дата обращения – 07.04.2020]
5. Википедия – свободная энциклопедия // [https://ru.wikipedia.org/wiki/Биометрия] / «История биометрии» [дата обращения – 25.03.2020]
6. Техпортал // [http://www.techportal.ru/glossary/kontrol-dostupa-po-risunku-ven.html] / «Контроль доступа по рисунку вен» [дата обращения – 04.04.2020]
7. NovaInfo // [https://novainfo.ru/article/4909] / «Эффективность биометрических СКУД» [дата обращения – 07.04.2020]
8. Прудников И.В. Исследование возможностей повышения точности идентификации информационных биометрических систем. Москва, 2012. - 190 с.
9. АО ГК Искандер // [https://gciskander.ru/biosmart1/] / «BioSmart — биометрическая система контроля доступа и рабочего времени» [дата обращения – 11.04.2020]
10. Копесбаева А.А. Микропроцессорные комплексы в системах управления. Учебное пособие для всех форм обучения специальности 5В070200 – Автоматизация и управление. - Алматы: АИЭС, 2010. - 124с.
11. Петров И.В. Программируемые контроллеры. Стандартные языки и приемы прикладного проектирования - СОЛОМОН – Пресс,2004. – 256 с.
12. Контроль доступа СКУД // [https://vashtvmir.ru/biometricheskaya-sistema-kontrolya-i-upravleniya-dostupom-skud/] / «Биометрическая система контроля и управления доступом (СКУД)» [дата обращения –13.04.2020]
13. Fujitsu // [https://habr.com/ru/company/fujitsu/blog/166787/] / «Технология распознавания Fujitsu PalmSecure» [дата обращения –15.04.2020]
14. Unimax // [https://www.umx.ru/about-company/article/biometricheskie-tekhnologii-identifikacii/] / «Биометрические технологии в СКД» [дата обращения – 18.04.2020]
15. Arduino Nano // [http://arduino.ru/Hardware/ArduinoBoardNano] / «Общие сведения Arduino Nano» [дата обращения –20.04.2020]
16. Оборудование и системы безопасности // [https://labofbiznes.ru/skud1.html] / «Структурная схема СКУД» [дата обращения –22.04.2020]

17. Г.Ш. Боканова. Методические указания к выполнению экономической части дипломных работ для студентов специальности 5В071900 – Радиотехника, электроника и телекоммуникаций. – Алматы: АУЭС, 2020 – 26 с.

18. AliExpress // [https://aliexpress.ru] / «Торговая платформа» [дата обращения –28.04.2020]

19. АлматыЭнергоСбыт // [https://esalmaty.kz/ru/?region=almaty] «Тарифы для юридических лиц»

20. HeadHunter // [https://hh.kz] / «Поиск и подбор персонала» [дата обращения –01.05.2020]

21. З.Д. Еркешева, Г.Ш. Боканова. Методические указания к выполнению расчетно-графических работ для студентов специальности 5В070400 – «Вычислительная техника и программное обеспечение». – Алматы: АУЭС, 2012. – 36 с.

22. М.К. Дюсебаев, Ж.С. Абдимуратов. Безопасность жизнедеятельности. Учебное пособие для студентов всех форм обучения специальности 050718 –Электроэнергетика – Алматы: АУЭС, 2010 – 81 с.

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

24. Охрана труда: учебник для вузов/ Ф.Р. Жандаулетова, Т.Е. Хакимжанов, Т.С. Санатова; МОН РК, НАО АУЭС. - Алматы : АУЭС, 2019. - 399 с.

25. Санитарные правила и нормы. СанПиН 2.1.8/2.24.1383-03. Электромагнитные излучения радиочастотного диапазона (ЭМИ РЧ). Госкомсанэпиднадзор России. – М.,2003.

26. Т.С. Санатова, Т.Е. Хакимжанов. Охрана труда и основы безопасности жизнедеятельности. Защита от воздействия электромагнитных полей радиочастотного диапазона. Методические указания и задания к расчетно-графической работе для студентов специалистов 5В071900 - Алматы: АИЭС, 2010 - 33 с.

27. Безопасность жизнедеятельности: Учебник для студентов средних спец. учеб. Заведений / С. В. Белов, В.А. Девисилов, А.Ф. Козьяков и др.; Под общ. ред. С.В. Белова.— 3-е изд., испр. и доп.— М.: Высш. шк., 2003.— стр. 144-227.

Приложение А

Листинг программы

```
#include <OneWire.h>

OneWire  ds(2);  // on pin 10 (a 4.7K resistor is necessary)

  byte i;
  byte present = 0;
  byte type_s;
  byte data[12];
  byte addr[8];
  float celsius;

  unsigned long previousDS = 0;
  unsigned long currentDS = 0;
  boolean j=LOW;

int trigPin = 11;    //Триггер – зеленый проводник
int echoPin = 12;    //Эхо – желтый проводник
unsigned long duration, cm;
float tempC;
void setup()
{
  Serial.begin(9600);
  pinMode(8,OUTPUT);
  pinMode(9,OUTPUT);
  pinMode(trigPin, OUTPUT);
  pinMode(echoPin, INPUT);
   if ( !ds.search(addr))
{
    Serial.println("No more addresses.");
    Serial.println();
    ds.reset_search();
    delay(250);
    return;
  }

  if (OneWire::crc8(addr, 7) != addr[7])
{
      Serial.println("CRC is not valid!");
      return;
  }
```

```
  Serial.println();

  // the first ROM byte indicates which chip
  switch (addr[0]) {
    case 0x10:
      Serial.println("  Chip = DS18S20");  // or old DS1820
      type_s = 1;
      break;
    case 0x28:
      Serial.println("  Chip = DS18B20");
      type_s = 0;
      break;
    case 0x22:
      Serial.println("  Chip = DS1822");
      type_s = 0;
      break;
    default:
      Serial.println("Device is not a DS18x20 family device.");
      return;
  }
  Serial.print("Adress=");
   for (uint8_t i = 0; i < 8; i++)
  {
    if (addr[i] < 16) Serial.print("0");
    Serial.print(addr[i], HEX);
  }
  Serial.println();
}
void loop()
 {
  if (j == HIGH) {ds.reset();
  ds.select(addr);
  ds.write(0x44, 1); }

 // start conversion, with parasite power on at the end
  //delay(1000);     // maybe 750ms is enough, maybe not
  // we might do a ds.depower() here, but the reset will take care of it.

  currentDS = millis();
  if(currentDS - previousDS > 1000)
{
  previousDS = millis();
  j=HIGH;
```

```
present = ds.reset();
ds.select(addr);
ds.write(0xBE);         // Read Scratchpad

  for ( i = 0; i < 9; i++) {data[i] = ds.read();} // we need 9 bytes

int16_t raw = (data[1] << 8) | data[0];
if (type_s) {
  raw = raw << 3; // 9 bit resolution default
  if (data[7] == 0x10) {raw = (raw & 0xFFF0) + 12 - data[6];} // "count
remain" gives full 12 bit resolution
        } else {byte cfg = (data[4] & 0x60);
  // at lower res, the low bits are undefined, so let's zero them
  if (cfg == 0x00) raw = raw & ~7;  // 9 bit resolution, 93.75 ms
  else if (cfg == 0x20) raw = raw & ~3; // 10 bit res, 187.5 ms
  else if (cfg == 0x40) raw = raw & ~1; // 11 bit res, 375 ms
  //// default is 12 bit resolution, 750 ms conversion time
}
celsius = (float)raw / 16.0;

  digitalWrite(trigPin, LOW);
  delayMicroseconds(5);
  digitalWrite(trigPin, HIGH);
  delayMicroseconds(10);
  digitalWrite(trigPin, LOW);
  // Считываем данные с ультразвукового датчика: значение HIGH,
которое
  // зависит от длительности (в микросекундах) между отправкой
  // акустической волны и ее обратном приеме на эхолокаторе.
  pinMode(echoPin, INPUT);
  duration = pulseIn(echoPin, HIGH);
  cm = (duration/2) / 29.1; //Растояние в сантиметрах
  Serial.print("Distanse=");Serial.print(cm);

if (cm<10 && celsius>=35 && celsius<=40)
{digitalWrite(9,LOW);digitalWrite(8,HIGH);}                    else
{digitalWrite(8,LOW);digitalWrite(9,HIGH);}
Serial.print("  Temperature = ");
Serial.print(celsius);
Serial.print(" Celsius");
Serial.println();}
 else {j=LOW;}
```

```
        //float tempC = sensors.getTempC(deviceAddress);

        //Serial.print(" Temperature=");Serial.println(sensors.getTempCByIndex(0));

        //j=millis()-prev;
        //prev=millis();
        //Serial.print(j);
        //Serial.print(" ");
      }
```