МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»
Институт Систем Управления и Информационных Технологий
Кафедра «Системы информационной безопасности»

«ДОПУЩЕН К ЗАЩИТЕ»
Зав.кафедрой _____
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: «Реализация схемотехнического решения защиты на базе двухфакторной аутентификации»

«Екі факторлы аутентификацияға негізделген қорғаудың схемотехникалық шешімін іске асыру»

«Implementation of schematic solution of protection based on two-factor authentication»_____

Специальность: Системы Информационной Безопасности_____

Выполнил(а): Әділ Алтынай Жанарбекқызы_____ Группа СИБ-16-2___
(Ф.И.О.)

Научный руководитель: к.т.н., профессор Маргаров Г.И.
(ученая степень, звание, Ф.И.О.)

Консультанты:
по специальной части:
старший преподаватель Дмитриева Маргарита Валерьевна_____

_____ «_____» _____20____г.
(подпись)

по безопасности жизнедеятельности:
к.т.н. доцент Приходько Николай Георгиевич_____

_____ «_____» _____20____г.
(подпись)

Нормоконтролер: старший преподаватель Дмитриева Маргарита Валерьевна
(ученая степень, звание, Ф.И.О.)

_____ «_____» _____20____г.
(подпись)

Рецензент: ___к.т.н., доцент Айтхожаева Евгения Жамалхановна_____
(ученая степень, звание, Ф.И.О.)

_____ «_____» _____20____г.
(подпись)

Алматы 2020

Задание на выполнение дипломного проекта

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»

Институт Систем Управления и Информационных Технологий_____

Кафедра «Системы Информационной Безопасности»_____

Специальность «Системы Информационной Безопасности»_____

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Әділ Алтынай Жанарбекқызы _____
(Ф.И.О.)

Тема проекта «Реализация схемотехнического решения защиты на базе двухфакторной аутентификации»

«Екі факторлы аутентификацияға негізделген қорғаудың схемотехникалық шешімін іске асыру»

«Implementation of schematic solution of protection based on two-factor authentication»_____

Утверждена приказом по университету № _146_ от «11»_ноября__2020 г.

Срок сдачи законченного проекта «__12__» __июня_____ 2020 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): Исходные материалы для выполнения задания дипломного проекта – сканер отпечатков пальцев ZFM60 V1.4, набор RFID модуля 13.56Mhz с карточкой и ключем, модуль датчика наклона, MP3-плеер DFPlayer Mini, Arduino Mega 2560 (CH340), блок питания 220/12V 5A, преобразователь DC-DC понижающий 12В / 5, модуль транзистора IRF520 для Ардуино, провода, резисторы, замок-защелка, USB провод, металлические ящики для сейфа, ПО ARDUINO, ПО Delphi 10.

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта: Цель работы - создание модели сейфа с доступом по двухфакторной аутентификации: сканеру отпечатка пальцев и RFID карте. Задачами дипломного проекта являются внедрение биометрического сканера в систему защиты сейфа, внедрение модуля RFID в систему защиты сейфа, разработка программного обеспечения для реализации разграничения доступа.

Перечень графического материала (с точным указанием обязательных чертежей): структурная схема программы, биометрического модуля и модуля RFID, схема соединения устройств конструкции.

Основная рекомендуемая литература: В.В. Вихман, А.А. Якименко Биометрические системы контроля и управления доступом в задачах защиты информации: учебно-метод. Пособие /. – Новосибирск: НГТУ, 2016. – 54 с. ; Антти Суомалайнен Биометрическая защита: обзор технологии – М.: ДМК Пресс, 2019. – 104 с.

Консультации по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Анализ рисков информационной безопасности	старший преподаватель Дмитриева Маргарита Валерьевна	17.02.2020 – 09.05.2020	
Безопасность жизнедеятельности	к.т.н. доцент Приходько Николай Георгиевич	17.02.2020 – 09.05.2020	

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Изучение деталей конструкции дипломного проекта	17.02.2020 – 20.02.2020	
Подключение сканера отпечатков пальцев к плате ARDUINO	21.02.2020 – 28.02.2020	
Подключение сканера RFID к плате ARDUINO	01.03.2020 – 08.03.2020	
Создание взаимодействия между биометрическим сканером и модуля RFID	09.03.2020 - 18.03.2020	
Настройка звукового оповещения, датчиков наклона	19.03.2020 – 27.03.2020	
Написание кода для платы ARDUINO	28.03.2020 - 07.04.2020	
Написание программного обеспечения на Delphi 10 для организации разграничения доступа к сейфу	08.04.2020 - 18.04.2020	
Поиск уязвимостей конструкции	19.04.2020 - 30.04.2020	

Анализ рисков ИБ. БЖД	01.05.2020 - 09.05.2020	

Дата выдачи задания «_7__» _____ноября_____ 2019 г.
Заведующий кафедрой _____ (Бердибаев Р.Ш.)
(подпись)

Научный руководитель проекта _____ (Маргаров Г.И.)
(подпись)

Задание приял к исполнению студент _____ (Әділ А.Ж.)
(подпись)

Аннотация

Бұл дипломдық жұмыстың мақсаты екі факторлы аутентификация қатынасы бар қауіпсіз үлгіні құру: саусақ ізі сканері және RFID картасы арқылы.

Бұл жұмыста басты назар схемотехникалық бөлігіне аударылды. Дипломдық жұмысты орындау үшін негізгі компонент ретінде Arduino тақтасы пайдаланылды. Қауіпсіздікті сақтау үшін саусақ ізі сканері мен RFID модулі тақтаға қосылған. Бұл схемаға арналған бағдарламалық жасақтамасы Delphi 10 Seattle программасында іске асырылды.

Дипломдық жұмыстың нәтижелері:

- қауіпсіз қорғау жүйесіне биометриялық сканерді енгізу;
- RFID модулін сейфтің қауіпсіздік жүйесіне енгізу;
- қауіпсіз үшін бағдарламалық жасақтама жасау.

Аннотация

Целью данной работы является создание модели сейфа с доступом по двухфакторной аутентификации: сканеру отпечатка пальцев и RFID карте.

Акцент в данной работе делался на схемотехнический части работы. Для реализации дипломной работы была использована плата Arduino как базовый компонент. Сканер отпечатков пальца и модуль RFID подключены к плате для обеспечения защиты сейфа. Программное обеспечение интерфейса для данного схемотехнического решения реализовано в среде Delphi 10 Seattle.

Итогами дипломной работы станут:

- внедрение биометрического сканера в систему защиты сейфа;
- внедрение модуля RFID в систему защиты сейфа;
- разработка программного обеспечения для реализации разграничения доступа.

Annotation

The aim of this work is to create a safe model with two-factor authentication access: a fingerprint scanner and an RFID card.

The emphasis in this work was on the circuitry part of the work. To implement the thesis, the Arduino board was used as a basic component. The fingerprint scanner and the RFID module are connected to the board to protect the safe. The interface software for this circuitry is implemented in the Delphi 10 Seattle environment.

The results of the thesis will be:

- introduction of a biometric scanner into the security system of the safe;
- implementation of the RFID module in the security system of the safe;
- software development for the implementation of access control.

Содержание

Введение

Вопросы, касающиеся биометрической защиты информации, являются очень актуальными. С расширением сферы применения биометрические технологии трансформировались из просто заместителя паролей в полноценный компонент систем безопасности, интеграция которого требует продуманного подхода. В связи с этим при внедрении биометрических технологий сегодня необходимо принимать во внимание многие характеристики, такие, как точность распознавания, общая стоимость владения, скорость получения образцов и обработки данных, внутренняя и системная безопасность, конфиденциальность информации, удобство интерфейса и одобрение пользователей.

Целью данной дипломной работы является создание модели сейфа с доступом по двухфакторной аутентификации: сканеру отпечатка пальцев и RFID карте. Задачами дипломного проекта являются внедрение биометрического сканера в систему защиты сейфа, внедрение модуля RFID в систему защиты сейфа, разработка программного обеспечения для реализации разграничения доступа.

Биометрия является широкой областью исследований, включающей в себя многие аспекты, в том числе правовые и социальные проблемы, а также вопросы эргономики, безопасности, поддержания целостности данных и применения крупномасштабных систем (включая меры обеспечения отказоустойчивости и процедуры восстановления в случае сбоев). Причины популярноости биометрических технологий очевидны: это их надежность, безопасность, эффективность, комфортность. В отличие от других технологий биометрия работает с людьми и выделяет их индивидуальность, иначе биометрические решения не смогли бы действовать. В широком смысле под биометрией понимается измерение уникальных физических и/или поведенческих характеристик человека. Примерами физиологических характеристик являются отпечатки пальцев, форма руки, характеристики лица, радужная оболочка глаза. К поведенческим характеристикам относятся особенности или характерные черты либо приобретенные, либо появившиеся со временем, т.е. динамика подписи, идентификация голоса, динамика нажатия на клавиши. В узком смысле в это понятие включают технологии и системы автоматической идентификации человека и/или подтверждения его личности, основанные на анализе уникальных биометрических параметров.

Биометрия тесно связана с теорией распознавания паттернов. Так как биометрия включает в себя элементы теории распознавания паттернов, она использует методы статистики и теорию вероятности в разработке биометрических мэтчеров, а также при анализе точности систем, потому что, ни одна биометрическая система не может гарантировать полного отсутствия ошибок. Но необходимо признать, что в области биометрии ведется серьезная теоретическая работа, проводятся тесты и статистический анализ результатов. Это привлекает внимание специалистов в области защиты информации.

1 Теоретическая часть

1.1 Методы реализации биометрической аутентификации

Применение для аутентификации разных подходов представляет свои преимущества: признаки, по которым происходит идентификация, нельзя потерять или забыть, передать третьим лицам, в отличие от обычных бесконтактных карт, практически невозможно подделать или украсть. Но существуют также и недостатки, к которым относятся отсутствие возможности 100%-ной достоверности идентификации, относительно высокая стоимость считывателей и зачастую слишком продолжительное время процесса идентификации. В этой главе рассмотрим популярные и развивающиеся методы считывания информации электронным способом, отличительные особенности и перспективы разных методов.

Принцип работы систем опознавания основан на получении изображения со сканера биометрического считывателя и его преобразовании в шаблон в электронной форме, который затем сравнивается с заранее составленным электронным банком данных. Шаблоны могут храниться как в базе данных СКУД, так и во встроенной памяти считывающего устройства или в памяти карты доступа.

Для идентификации живого объекта (человека) в биометрических системах контроля доступа используются параметры, уникальные для каждого человека. Наиболее распространенными являются системы, идентифицирующие граждан по следующим признакам:

- отпечатки пальцев;
- рисунок вен или геометрии руки;
- радужная оболочка или сетчатка глаза;
- геометрия или термограмма лица.

Рассмотрим каждый метод геометрического считывания информации. Геометрия лица человека. Биометрическая идентификация лиц в плане технической реализации представляет собой более сложную и дорогую задачу и базируется на построении двухмерных или трехмерных моделей лица на основании снимков, сделанных видеокамерой. Она является самой комфортной и не всегда заметной для пользователя, не требует физического контакта с устройством.

При построении двухмерной модели получается плоское изображение, такие системы более требовательны к освещению и положению лица при сканировании, в связи с чем происходит довольно много ошибок.

При построении трехмерной модели получается объемное изображение, что позволяет добиться большей точности распознавания за счет минимизации влияния таких факторов, как изменение цвета кожи (в том числе и с помощью косметики), ношение бороды или усов, изменение поверхности лица при болезни и др., обеспечивая при этом достаточную скорость построения 3D-модели лица.

На рисунке 1.1 представлена иллюстрация сканирования по геометрии лица человека.

Рисунок 1.1 – Иллюстрация сканирования по геометрии лица человека

Для повышения достоверности распознавания лиц дополнительно может использоваться термограмма лица (сканирование лица в инфракрасном диапазоне), которая компенсирует наличие очков, шляпы или накладных элементов.

Радужная оболочка и сетчатка глаза. Идентификация по радужной оболочке – одна из самых надежных, но дорогих технологий биометрической идентификации. Радужная оболочка уникальна, наиболее защищена от повреждений и не изменяется во времени. Очки и контактные линзы не влияют на получение изображения, даже слепой человек может быть идентифицирован таким способом.

На рисунке 1.2 представлена иллюстрация этого метода.

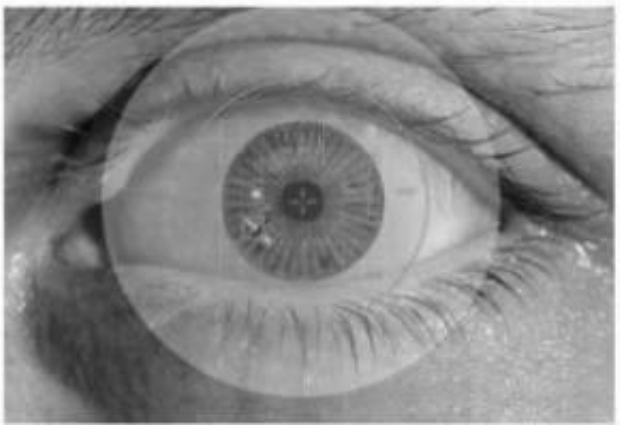


Рисунок 1.2 – Иллюстрация метода сканирования по оболочке и сетчатке глаза

После получения изображения происходит выделение частотных или других данных о рисунке радужной оболочки глаза, которые сохраняются в шаблон. Такой метод достаточно комфортен, поскольку не требует физического контакта с устройством и при этом отсутствует поток яркого света, направленный в глаз. При использовании камеры, разрешение которой превышает 3 Мп, можно захватывать 2 глаза на одном кадре, что заметно повышает уровень достоверности распознавания.

Этот принцип является быстрым и комфортным, по сравнению с идентификацией по сетчатке глаза, и может использоваться на объектах численностью в несколько десятков тысяч человек. В настоящее время активно развивается благодаря своей перспективности.

При идентификации по сетчатке глаза используется узор кровеносных сосудов, расположенных на поверхности глазного дна (сетчатке), получаемый путем просвечивания кровеносных сосудов на задней стенке глаза лазерным лучом мягкого излучения. Сетчатка – один из наиболее стабильных физиологических признаков организма, однако этот метод очень дорог, имеет невысокую пропускную способность и не является комфортным, так как пользователю приходится неподвижно сидеть и смотреть в окуляр в течение нескольких секунд. В настоящее время идентификация по сетчатке глаза в СКУД используется редко.

Идентификация по рисунку вен ладони и ее геометрии. Идентификация по рисунку вен ладони основана на получении шаблона при фотографировании внешней или внутренней стороны руки инфракрасной камерой. Из-за бесконтактной составляющей этот метод является достаточно комфортным для пользователя, при этом практически отсутствует возможность подделки, но болезни вен могут затруднять или искажать результат идентификации.

На рисунке 1.3 представлена иллюстрация сканирования ладони по ее геометрии и рисунку вен.

Рисунок 1.3 – Иллюстрация сканирования ладони по ее геометрии и рисунку вен

Степень достоверности распознавания сравнима с идентификацией по радужной оболочке глаза, хотя стоимость оборудования гораздо ниже.

Метод идентификации по геометрии ладони основан на измерении отдельных параметров формы руки, таких как ширина ладони, радиус окружности, вписанной в центр ладони, длина пальцев и высота кисти руки, учитываются также пять основных линий, существующих на любой ладони.

Надежность этого метода сравнима с идентификацией по отпечатку пальца и тоже сильно зависит от состояния объекта, поскольку распухание тканей или ушибы руки могут исказить исходную структуру, руки могут изменяться с возрастом.

К плюсам использования можно отнести отсутствие влияния на процесс сканирования температуры, влажности и загрязненности, хотя в настоящее время идентификации по геометрии руки в СКУД используется редко.

Отпечаток пальца. Идентификация по отпечаткам пальцев — самая распространенная, надежная и эффективная биометрическая технология. Благодаря универсальности этой технологии она может применяться практически в любой сфере и для решения любой задачи, где необходима достоверная идентификация пользователей. Отпечатки всех пальцев каждого человека уникальны по рисунку папиллярных линий и различаются даже у близнецов. Отпечатки пальцев не меняются в течение всей жизни взрослого человека, они легко и просто предъявляются при идентификации. Если один из пальцев поврежден, для идентификации можно воспользоваться «резервным» отпечатком (отпечатками), сведения о которых, как правило, также вносятся в биометрическую систему при регистрации пользователя.

Дополнительная идентификация по штрих-коду. Штрих-код представляет собой набор закодированных цифровых или алфавитно-цифровых символов в виде геометрических фигур, например последовательность черных и белых полос. Штрих-коды бывают разных видов, отличающихся тем, какой объем и какой тип информации можно с их помощью закодировать.

В системах контроля доступа обычно применяются самые простейшие

штрих-коды, поскольку, как правило, не стоит задача передавать через идентификатор большое количество данных. Среди таких:

- Code 39;
- Code 128;
- EAN‑13.

Штрих-код может наноситься практически на любую поверхность, например распечатываться обычным принтером на листе бумаги или вовсе отображаться в электронном виде на экране смартфона. Кроме этого, штрих-код может быть легко передан по электронным каналам связи, к примеру по электронной почте или факсу. Это делает использование штрих-кодов в СКУД очень дешевым. С другой стороны, такие идентификаторы никак не защищены от копирования, а также имеют низкую износостойкость. Исходя

из данных особенностей, штрих-коды в СКУД обычно используются в качестве разовых пропусков для посетителей.

1.2 Сравнительный анализ основных методов биометрической аутентификации

Для определения эффективности СКУД на основе биометрической аутентификации 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;
- ёмкость шаблона - максимальное количество наборов данных, которые могут храниться в системе.

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

В таблице 1.1 представлены статистические данные сравнения методов биометрической аутентификации с использованием математической статистики (FAR и FRR).

Таблица 1.1 - Сравнение методов биометрической аутентификации с использованием математической статистики (FAR и FRR)

Биометрическая СКУД использует:	Коэффициент пропуска, FAR	Коэффициент ложного отказа, FRR
Отпечаток пальца	0,001%	0,6%
Распознавание лица 2D	0,1%	2,5%

Продолжение таблицы 1.1

Распознавание лица 3D	0,0005%	0,1%
Радужная оболочка глаза	0,00001%	0,016%
Сетчатка глаза	0,0001%	0,4%
Рисунок вен	0,0008%	0,01%

Но для построения эффективной системы контроля доступа недостаточно отличных показателей FAR и FRR. Например, сложно представить СКУД на основе анализа ДНК, хотя при таком методе аутентификации указанные коэффициенты стремятся к нулю. Зато растет время идентификации, увеличивается влияние человеческого фактора, неоправданно возрастает стоимость системы. Таким образом, для качественного анализа биометрической системы контроля доступа необходимо использовать и другие данные, получить которые, порой, возможно только опытным путем.

В первую очередь, к таким данным нужно отнести возможность подделки биометрических данных для идентификации в системе и способы повышения уровня безопасности. Во- вторых, стабильность биометрических факторов: их неизменность со временем и независимость от условий окружающей среды. Как логичное следствие, - скорость аутентификации, возможность быстрого бесконтактного снятия биометрических данных для идентификации. И, конечно, стоимость реализации биометрической СКУД на основе рассматриваемого метода аутентификации и доступность составляющих.

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

Фальсификация биометрических данных это в любом случае достаточно сложный процесс, зачастую требующий специальной подготовки и технического сопровождения. Но если подделать отпечаток пальца можно и в домашних условиях, то об успешной фальсификации радужной оболочки - пока не известно. А для систем биометрической аутентификации по сетчатке глаза создать подделку попросту невозможно.

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

Повышение уровня безопасности биометрической системы контроля доступа, как правило, достигается программно-аппаратными методами. Например, технологии «живого пальца» для отпечатков, анализ непроизвольных подрагиваний – для глаз. Для увеличения уровня безопасности биометрический метод может являться одной из составляющих многофакторной системы аутентификации.

Включение в программно-аппаратный комплекс дополнительных средств защиты обычно довольно ощутимо увеличивает его стоимость. Однако, для некоторых методов возможна строгая аутентификация на основе стандартных составляющих: использование нескольких шаблонов для идентификации пользователя (например, отпечатки нескольких пальцев).

Таблица 1.4 - Сравнение методов аутентификации по неизменности биометрических характеристик

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

Неизменность биометрической характеристики с течением времени понятие также условное: все биометрические параметры могут измениться вследствие медицинской операции или полученной травмы. Но если обычный бытовой порез, который может затруднить верификацию пользователя по отпечатку пальца, - ситуация обычная, то операция, изменяющая рисунок радужной оболочки глаза – редкость.

Таблица 1.5 - Сравнение по чувствительности к внешним факторам

Биометрическая СКУД использует:	Чувствительность к влиянию внешних факторов

Отпечаток пальца	Высокая

Продолжение таблицы 1.5

Распознавание лица 2D	Высокая
Распознавание лица 3D	Низкая
Радужная оболочка глаза	Средняя
Сетчатка глаза	Высокая
Рисунок вен	Средняя

Влияние параметров окружающей среды на эффективность работы СКУД зависит от алгоритмов и технологий работы, реализованных производителем оборудования, и может значительно отличаться даже в рамках одного биометрического метода. Ярким примером подобных различий могут послужить считыватели отпечатков пальцев, которые в целом довольно чувствительны к влиянию внешних факторов.

Если сравнивать остальные методы биометрической идентификации – самым чувствительным окажется распознавание лиц 2D: здесь критичным может стать наличие очков, шляпы, новой прически или отросшей бороды. Системы, использующие метод аутентификации по сетчатке, требуют довольно жесткого положения глаза относительно сканера, неподвижности пользователя и фокусировки самого глаза. Методы идентификации пользователя по рисунку вен и радужной оболочке глаза сравнительно стабильны в работе, если не пытаться использовать их в экстремальных условиях работы (например, бесконтактная аутентификация на большом расстоянии во время «грибного» дождя). Наименее чувствительна к влиянию внешних факторов трехмерная идентификация по лицу. Единственным параметром, который может повлиять на работу подобной СКУД, является чрезмерная освещенность.

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

Скорость аутентификации зависит от времени захвата данных, размеров шаблона и объема ресурсов, отведенных на его обработку, и основных программных алгоритмов, применяемых для реализации конкретного биометрического метода.

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

Бесконтактная аутентификация дает массу преимуществ использования биометрических методов в системах физической безопасности на объектах с высокими санитарно-гигиеническими требованиями (медицина, пищевая промышленность, научно-исследовательские институты и лаборатории). Кроме того, возможность идентификации удаленного объекта ускоряет процедуру проверки, что актуально для крупных СКУД с высокой поточностью. А также, бесконтактная идентификация может использоваться правоохранительными органами в служебных целях. Именно поэтому ученые стремятся разработать бесконтактные системы аутентификации по отпечатку пальца, но еще не достигли устойчивых результатов. Особенно эффективны методы, позволяющие захватывать биометрические характеристики объекта на большом расстоянии и во время движения. С распространением мегапиксельных камер видеонаблюдения реализация подобного принципа работы становится все более легкой.

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

Психологический комфорт пользователей – также достаточно актуальный показатель при выборе системы безопасности. Если в случае с двухмерным распознаванием лиц или радужной оболочкой – оно происходит незаметно, то сканирование сетчатки глаза – довольно неприятный процесс. А идентификация по отпечатку пальца, хоть и не приносит неприятных ощущений, может вызывать негативные ассоциации с методами криминалистической экспертизы.

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

Стоимость систем контроля и учета доступа в зависимости от используемых методов биометрической идентификации крайне различается между собой. Впрочем, разница может быть ощутимой и внутри одного метода, в зависимости от назначения системы (функциональности), технологий производства, способов, повышающих защиту от несанкционированного доступа и т.п.

Таблица 1.10 - Сравнение доступности методов биометрической идентификации в Казахстане [6]

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

Доступность СКУД, использующих тот или иной метод биометрической аутентификации, зависит от распространенности их в целом. И, конечно, специфика казахстанского рынка накладывает свои ограничения.

При учете сложных экономических условий на передний план выходит цена. При чем, для Казахстана играет роль не только сравнительная оценка стоимости реализации различных методов, но и наличие оборудования отечественного производства, использующего для биометрической идентификации обозначенный метод. В первую очередь, наличие собственных производителей на порядок снижает стоимость оборудования. Кроме того, доступность оборудования позволяет рассчитывать на быструю замену или ремонт комплектующих в случае необходимости.

С распознаванием отпечатков пальцев проблем не возникает: потребителю доступен широкий ассортимент оборудования. Двухмерная идентификация по лицу недостаточно эффективна для построения системы безопасности на ее основе. Скорее этот метод используется для задач видеоаналитики или в качестве одной из составляющих для мультифакторных

систем аутентификации. При необходимости, можно найти отечественных производителей для решения этих задач. Трехмерная аутентификация – дорогое удовольствие, даже при простом сравнении методов биометрической идентификации. Метод аутентификации по сетчатке глаза настолько узкоспециализирован, а объекты, для которых он предназначен, настолько секретны, что лучше о его доступности даже не думать и не говорить вслух. Метод идентификации по радужной оболочке глаза уже много лет считается одним из самых перспективных и эффективных, и его доля на мировом рынке, конечно, растет. При этом высокая стоимость и сложная ситуация с патентами на технологию – являются ограничителями и на мировой арене. Для казахстанского рынка, с учетом курса тенге к иностранным валютам, стоимость технологии огромна и оборудование иностранного производства, по этой причине, доступно только под заказ.

1.3 Обоснование выбора метода для реализации

Был выбран отпечаток пальца как метод считывания информации и реализации биометрической защиты. Этот вид идентификации наиболее изучен, он основан на получении изображения рисунка папиллярных узоров пальцев людей, которые обладают свойствами индивидуальности, относительной устойчивости и восстанавливаемости.

Существуют два основных алгоритма распознавания отпечатков пальцев: по отдельным деталям (характерным точкам) и по рельефу всей поверхности пальца, причем по получаемому в результате обработки цифровому коду нельзя воссоздать первоначальный отпечаток.

Разнообразие биометрических считывателей отпечатков пальцев обусловлено широким спектром сенсоров (сканеров), использующихся для получения изображения. Среди инновационных решений есть бесконтактные считыватели, которые не требуют прикосновения, и считыватели 10 пальцев одновременно, но они довольно дороги при своей точности и комфортности для пользователя.

«Минусом» такой идентификации является зависимость качества распознавания отпечатка от состояния поверхности пальца и внешних условий
(температура, влажность, пыль), нежелание некоторых людей оставлять свои отпечатки, а также наличие людей (порядка 2 % от общего количества) с врожденными плохо выделяющимися отпечатками пальцев.

Среди методов идентификации рисунка линий на пальце человеческой руки наиболее популярны следующие.

Оптический метод. Для получения оптического изображения отпечатка пальца может быть использовано устройство, подобное цифровой камере. Кончик пальца прикладывается к стеклянной пластине, освещенной должным образом. Необходим только объектив, способный работать в непосредственной близости от объекта съемки. Изображение захватывается при помощи матрицы элементов с зарядовой связью (CCD) или элементов

нужного разрешения (CMOS) и преобразуется в изображение в оттенках серого цвета (от 2 до 16 оттенков обычно вполне достаточно). Недостаток этой технологии заключается в том, что незаметный отпечаток пальца остается на поверхности стекла и может быть использован повторно. Другая сложность состоит в том, чтобы отличить настоящий палец от хорошо выполненной имитации.

Емкостный метод. Когда кончик пальца прикладывается к матрице элементов, чувствительных к электрическому заряду, разница в электропроводности выступов (содержащих много воды) и впадин (содержащих воздух) приводит к локальному изменению емкости элементов. Это позволяет определить положение выступов и впадин и построить изображение отпечатка. Несмотря на подверженность этого метода электростатическим разрядам и прочим паразитным электрическим полям, он остается одним из наиболее популярных для получения изображений отпечатков пальцев. Однако такие сканеры сравнительно легко обмануть имитированным отпечатком или скрытым отпечатком на поверхности сканера.

Радиометод. Если облучить кончик пальца радиоволнами низкой интенсивности, то разницу в расстоянии между поверхностью выступов и впадин можно определить с помощью матрицы правильно настроенных антенных элементов. При этом требуется, чтобы кончик пальца контактировал с излучающим элементом датчика (обычно по периферии). Поскольку метод основан на физиологических свойствах кожи, его трудно обмануть имитацией пальца. Слабым местом метода является необходимость качественного контакта пальца и кольца передатчика, которое может быть весьма горячим.

Нажимной метод. Для получения узора отпечатка прикладываемого пальца может применяться и матрица пьезоэлектрических элементов, чувствительных к нажатию. Несмотря на многие недостатки этого метода (низкая чувствительность, неспособность отличить настоящий палец от имитации, подверженность повреждениям из-за чрезмерных прилагаемых усилий и т. п.), некоторые компании продолжают придерживаться этого метода в прототипах своей продукции.

Микроэлектромеханический метод. Микроэлектромеханический метод (MEMS) по состоянию на начало 2019 года – в промежуточной стадии между научно-исследовательскими разработками и внедрением. Для определения выступов и впадин отпечатка пальца в лабораториях разработана матрица микромеханических датчиков, но пока еще нет уверенности в их устойчивости. Таким методом также невозможно отличить настоящий палец от имитации.

Более эффективным способом защиты информации является использование биометрической защиты вместе с другими устройствами считывания информации. В данной дипломной работе используется оптический датчик отпечатка пальца, а также бесконтактные карты.

1.4 Идентификация по бесконтактным картам

Среди идентификаторов, применяющихся в системах контроля доступа, распространение получили бесконтактные карты. Они удобны в использовании, бывают выполнены в разных формах и видах, а использование криптоалгоритмов в некоторых форматах карт существенно снижает риск их копирования и подделки.

Ниже рассмотрены основные особенности такого типа идентификаторов.

Физическое исполнение. Кроме представленных ниже, также существуют и другие исполнения идентификаторов (метки, наклейки, болты, колбы, ярлыки), однако в качестве отдельных элементов в системах контроля доступа они используются нечасто. В таблице 1.12 представлены сведения по различным идентификаторам.

Таблица 1.12 - Различные современные идентификаторы и их особенности

Вид идентификатора	Особенность
Толстые карты (Clamshell card)	Бесконтактные карты стандартных размеров толщиной 1,6 мм. Самые недорогие идентификаторы, дальность считывания – самая высокая из представленных (для формата EM Marine имеется исполнение повышенной дальности считывания – до 1,5 м). Для персонализации могут использоваться специальные наклейки
Брелки	Брелки обычно дороже карт, при этом имеют меньшую дальность чтения. Могут иметь фирменный дизайн исполнения, однако возможность персонализации таких идентификаторов практически отсутствует. По сравнению с картами, брелки более устойчивы к физическому воздействию – меньше ломаются, могут прикрепляться к ключам
Браслеты	Стоимость немного выше, чем у брелков, дальность считывания примерно одинаковая. Могут закрепляться на теле человека, иметь

	фирменный дизайн. Из-за удобства ношения, как правило, применяются в различных фитнес-центрах, бассейнах, аквапарках и прочих спортивных учреждениях
Тонкие карты (ISO card)	Бесконтактные карты стандартных размеров толщиной 0,76 мм.

Продолжение таблицы 1.12

	Стоимость немного выше, чем у толстых карт, однако дальность считывания ниже. Идеально подходят для персонализации посредством прямой печати на самих картах (сублимационной либо ретрансферной)

Протокол взаимодействия (формат). Правильный выбор формата имеет непосредственное влияние на уровень безопасности системы. Получило распространение несколько форматов, отличающихся рядом параметров, они сведены в таблице 1.13.

Таблица 1.13 - Особенности различных форматов и их параметров

Формат	Внутренняя перезаписываемая память	Защита от копирования	Механизм антиколлизии	Цена	Диапазон выбора считывателей
EM Marine	нет	нет	нет	низкая	высокий
HID ProxCard II, HID ISO Prox	нет	нет	нет	средняя	средний
HID iClass	да	да	да	высокая	средний
Mifare	да	да	да	средняя	высокий

Кроме перечисленных форматов, есть и другие, к примеру Legic или Indala, однако они мало распространены в Казахстане.

Возможна поддержка сразу нескольких форматов одним идентификатором. Наиболее дешевым и имеющим самый широкий диапазон выбора считывателей является формат EM Marine, однако он никак не защищен от копирования. В отличие от него, идентификаторы Mifare ненамного дороже, но имеют внутреннюю перезаписываемую память, правильное использование которой в совокупности со специально настроенными считывателями позволяет организовать защищенную идентификацию.

При организации СКУД следует подбирать оборудование и использующиеся идентификаторы, исходя из требований, предъявляемых к безопасности системы. Выбор считывателя обусловливается несколькими основными параметрами. Считыватели могут поддерживать как один, так и несколько форматов одновременно. При выборе идентификатора Mifare считывателям необходимо поддерживать работу с ним в защищенном режиме. Используется для исключения влияния считывателей друг на друга при установке на близком расстоянии, к примеру при монтаже на тонких стенах. Стандартная дальность составляет не более 10 см, но бывают считыватели повышенной дальности до 1,5 м. За счет большей дальности и помехоустойчивости самым предпочтительным является Wiegand. Интерфейс связи Dallas Touch Memory (iButton) имеет более низкие характеристики, а OSDP пока редок в использовании. Встречаются считыватели с проприетарным интерфейсом, которые работают с контроллерами только этого же производителя. Для подключения к ПК и заведения карт в систему могут использоваться считыватели с USB-интерфейсом. Считыватели могут использоваться как в помещении, так и на улице, поэтому производятся с различными значениями рабочей температуры, влагоустойчивости и вандалостойкости. Для работы были выбраны тонкие смарт-карты.

Вывод по разделу: в данном разделе были рассмотрены методы реализации биометрической аутентификации и произведен анализ основных методов биометрической аутентификации. На основе сравнительного анализа был выбран отпечаток пальца как метод считывания информации и реализации биометрической защиты. Также в данном разделе дипломной работы быаи рассмотрена идентификация по RFID картам.

2 Практическая часть

2.1 Описание деталей конструкции и схемы

На рисунке 2.1 изображена обобщенная структурная схема программы. При включении сейфа к питанию происходит автопоиск порта, далее приложение подключается к сейфу посредством USB шнура. После подключения необходимо выбрать один из модулей либо модуль карт, либо биометрический модуль. В зависимости от выбранного модуля можно произвести различные действия. Например, при выборе модуля FRID карточек (рисунок 2.2) возможно добавить, удалить или отредактировать базу данных карт. Таким же образом при выборе биометрического модуля (рисунок 2.3) возможно добавить новый отпечаток пальца в базу данных либо удалить существующий отпечаток пальца. Детальная структурная схема конструкции изображена на рисунке 2.5. В детальной структурной схеме изображена последовательность каждого действия. Например, при добавлении новой карты в базу данных модуля FRID карточек в начале необходимо ввести имя пользователя в приложение. Далее происходит сравнение введенного имени пользователя с существующими именами в БД, если

данные совпадают происходит перезапись. После сравнения данных необходимо выбрать права доступа к ящикам (A, B, AB), далее сканируется карта и определяется идентификационный номер карты. После этого номер карты прикрепляется к имени пользователя и данные сохраняются. На рисунке 2.7 изображена схема подключения всех устройств в реальности.

Модуль RFID-RC522 (рисунок 2.11) подключен к плате через интерфейсы SDA (выбор ведомого), SCK (сигнал синхронизации), MOSI (передача от master к slave), MISO (передача от slave к master), GND (земля), RST (вывод для сброса), 3.3V (питание 3.3 В) к пинам 48, 53, 51, 50, 49, 3.3V соответственно. Для защиты сейфа от несанкционированного доступа, кражи к сейфу подключен датчик наклона (рисунок 2.12) через цифровые пины 6,7. Для ограничения тока в цепи к датчику наклона присоединен резистор на 10КОм. К плате также через пины 2,3 подключены лампочки синяя и красная. К ним подсоединены резисторы на 220Ом. Синяя лампа загорается при положительном сканировании отпечатка пальца или RFID карты, красная лампочка горит при закрытом состоянии дверей сейфа.

К плате Arduino подключен сканер отпечатков пальцев ZFM60 V1.4 через цифровые пины 10,11. Чтобы начать сканирование пальца в начале необходимо нажать на тактовую кнопку (рисунок 2.20), которая подключена к 33 пину платы. Кнопка соединена с плеером и получает питание от платы. Для воспроизведения голосового оповещения «Доступ разрешен», «Доступ запрещен» после сканирования отпечатка пальца к датчику отпечатков пальцев подключен MP3 DFPlayer (рисунок 2.14) через пины VCC, GND для питания (+/-). На плеере расположена карта памяти формата microSD с заготовленными записями. Плеер подключен к плате через входы RX, TX (UART прием и предача), также к плееру подключена колонка ко входу SPK1 (громкоговоритель «+»). Для подключения датчиков и модуля RFID карт используется плата Arduino Mega 2560 (рисунок 2.15). Питание плеер и сканер отпечатков пальцев получает посредством платы Arduino, которая получает питание от блока питания (рисунок 2.17). Так как плата работает на 5В, а замки на 12В для преобразования напряжения к плате через пины VIN, GND подключен DC-DC преобразователь 12-5V (рисунок 2.18). Для преобразования тока к DC-DC преобразователь подключено два IRF-520 транзистора (рисунок 2.19), к которому подключены замки. Замоки-защелки прикреплены к дверцам металлических ящиков (рисунок 2.21). Для подключения платы Arduino к приложению, расположенному на ноутбуке, используется USB шнур (рисунок 2.22). Замок-защелка работает на 12В (рисунок 2.23). Помимо структурных схем конструкции имеются также принципиальная схема Arduino Mega, распиновка Arduino Mega принципиальная схема подключения RFID-RC522 к Arduino Mega2560 (Приложение Б).

Рисунок 2.1 – Обобщенная структурная схема программы

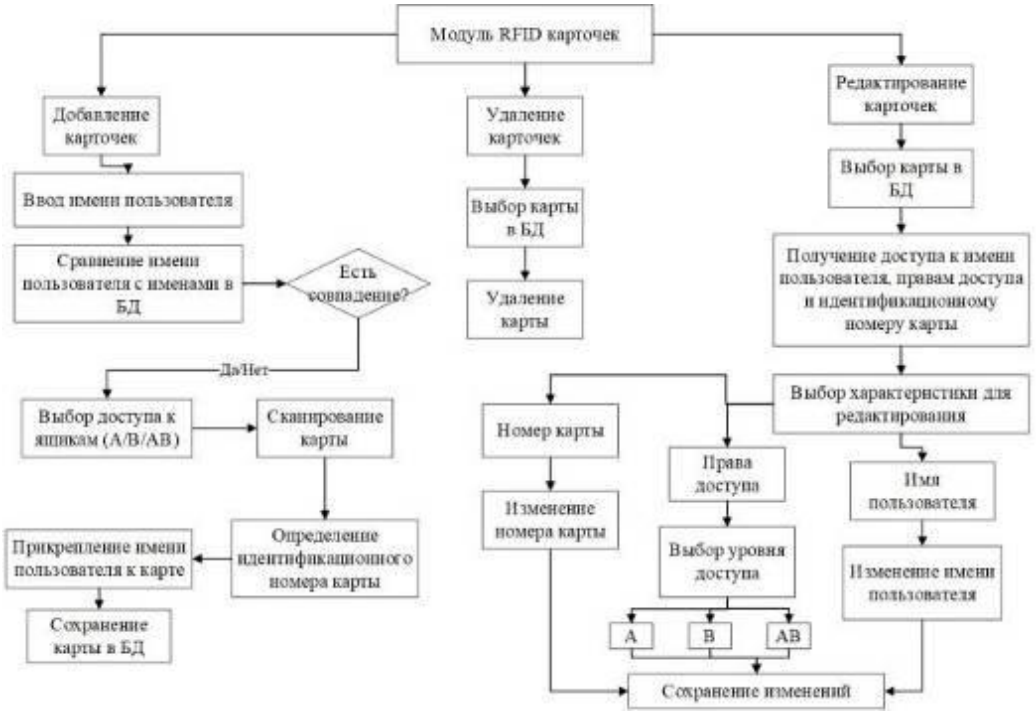


Рисунок 2.2 – Структурная схема модуля FRID карточек

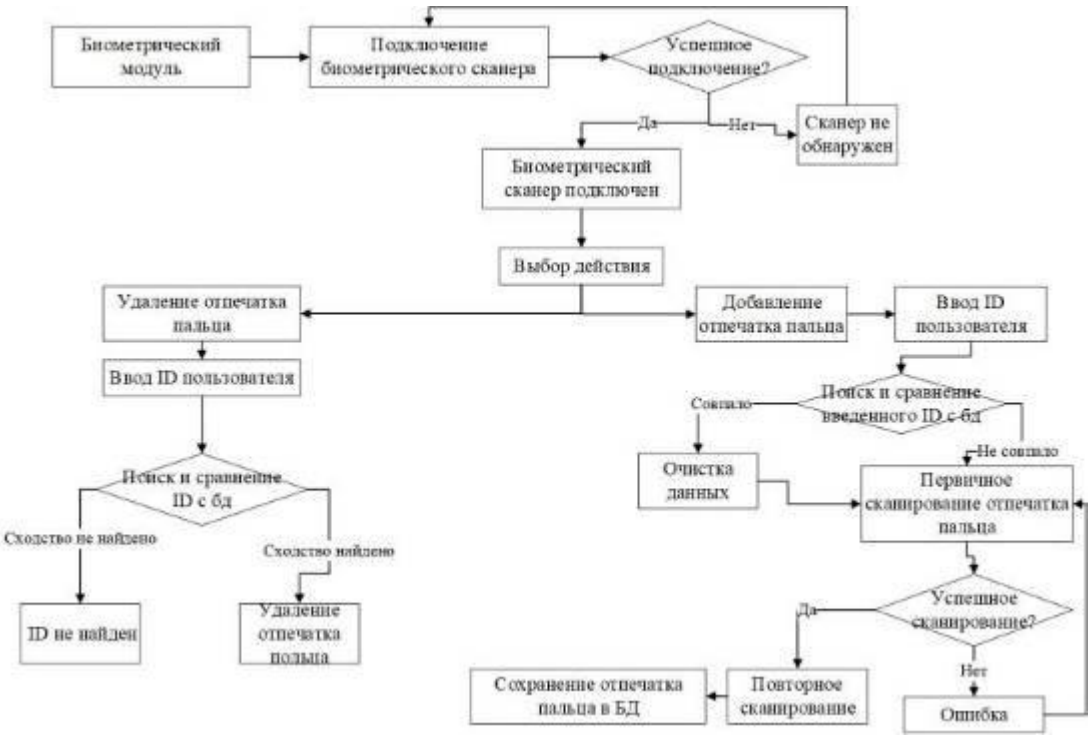


Рисунок 2.3 – Структурная схема биометрического модуля

На рисунке 2.4 представлена схема соединения вех устройств.

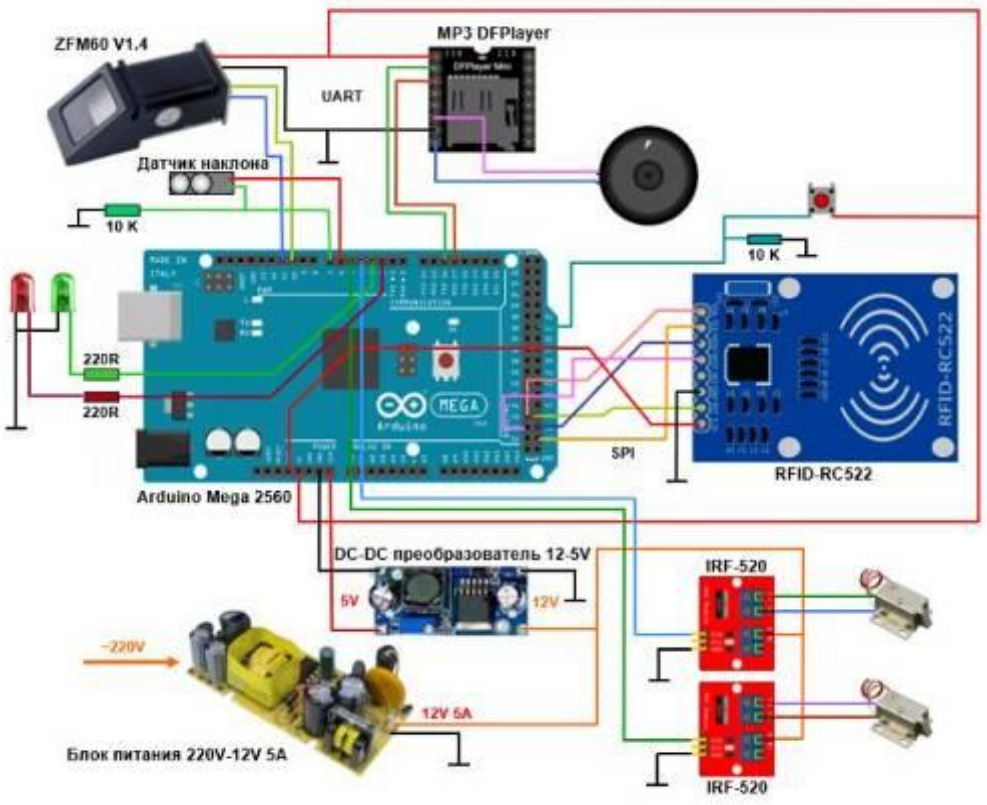


Рисунок 2.4 – Схема соединения устройств

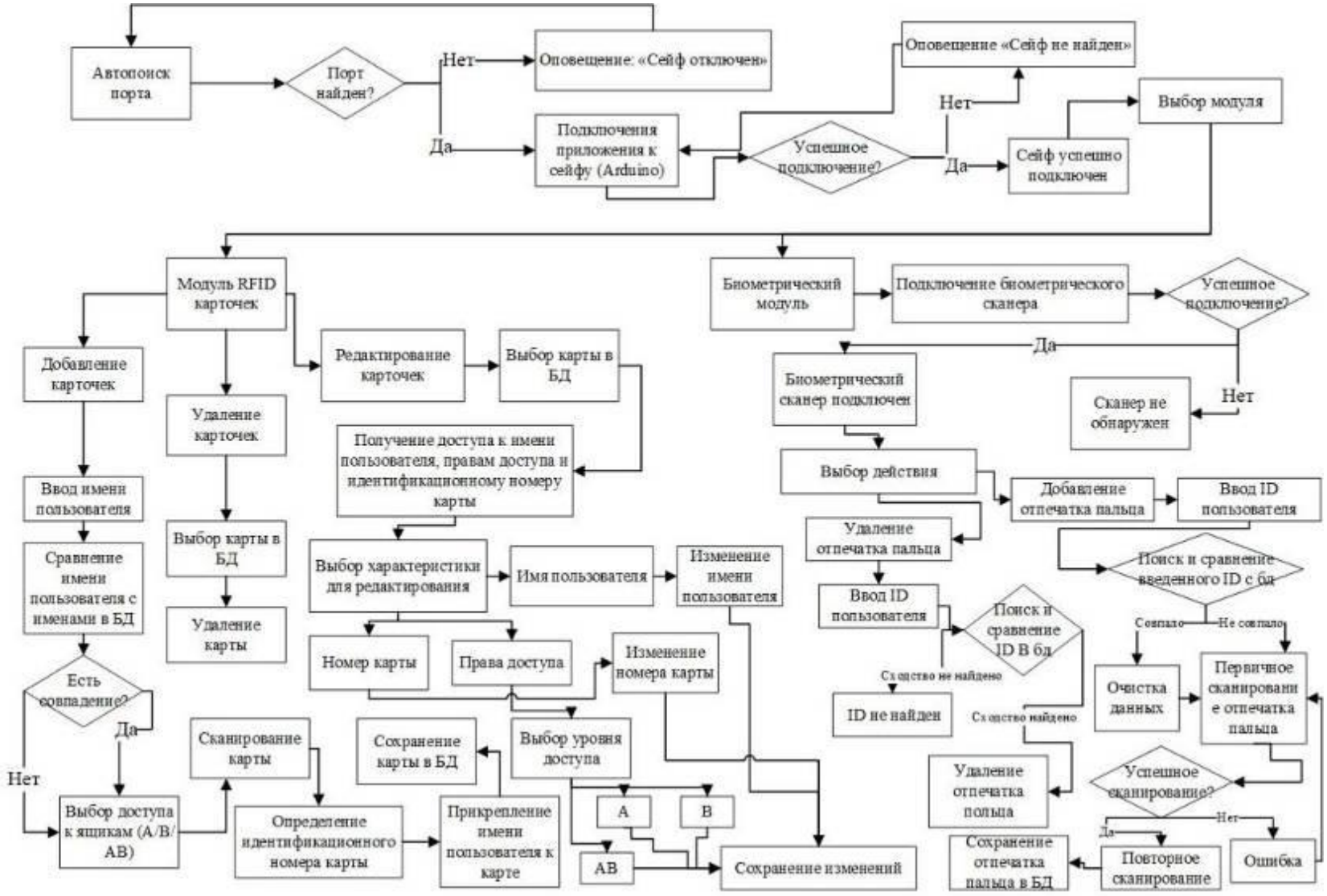


Рисунок 2.5 - Структурная схема

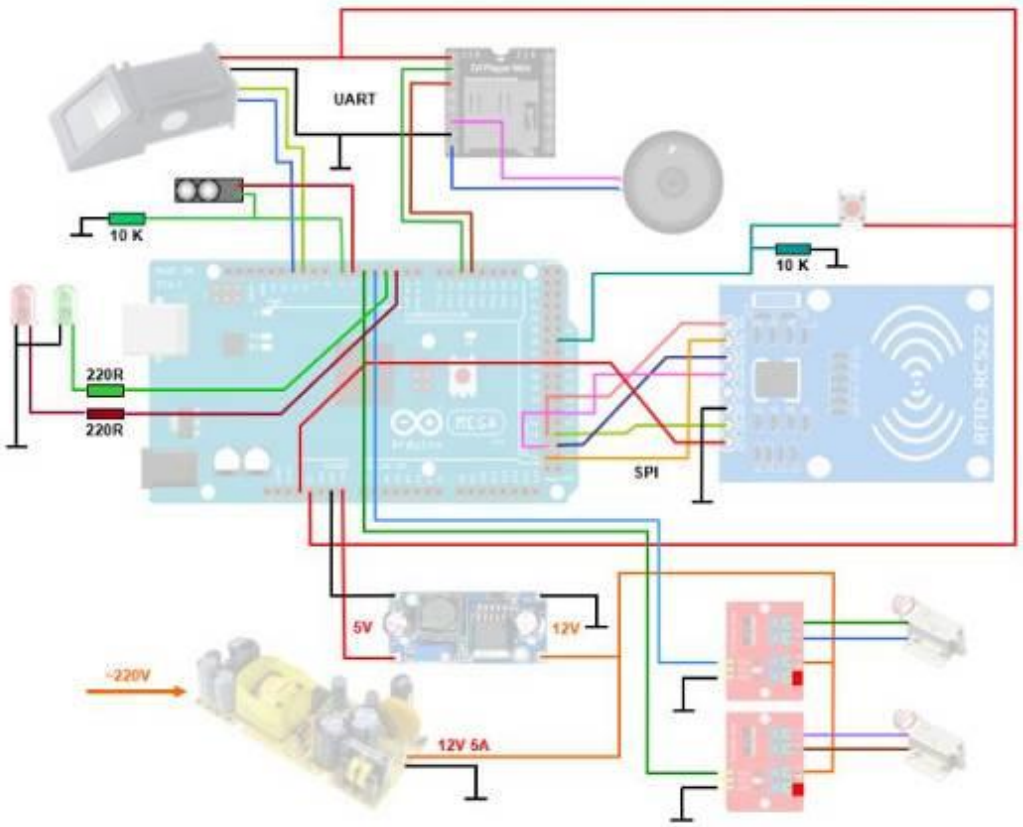


Рисунок 2.6 – Схема соединения устройств

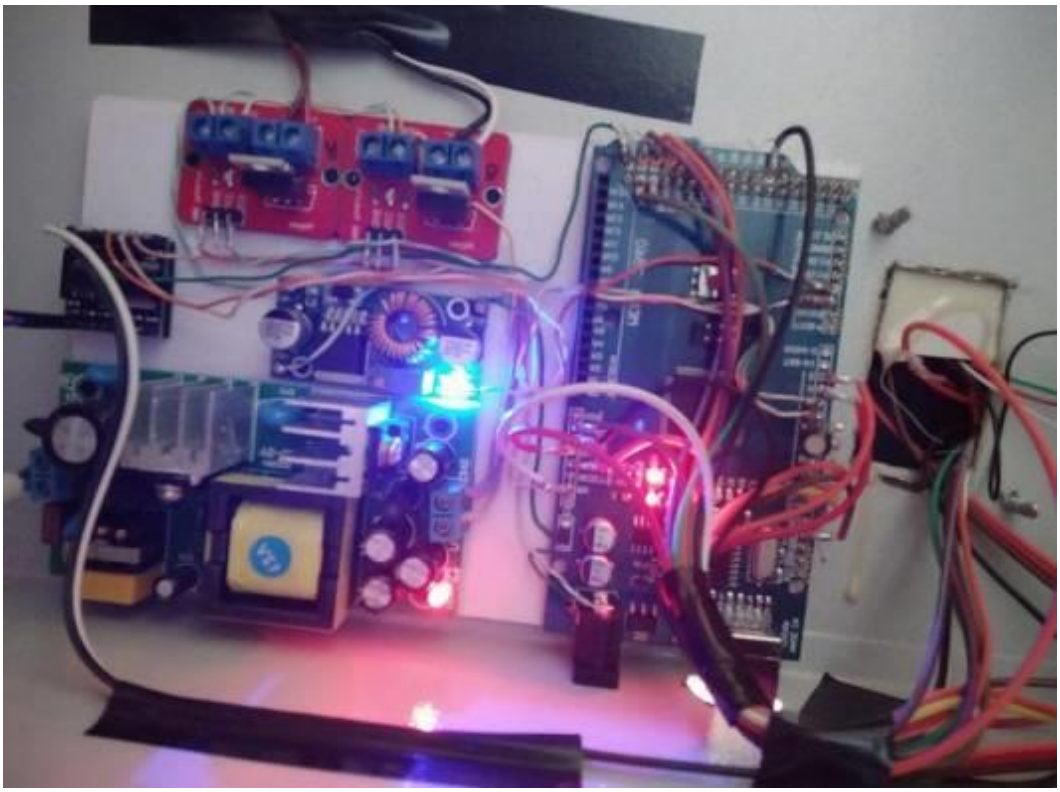


Рисунок 2.7 – Подключение устройств

Таблица 2.1 – Расчет стоимости оборудования

Оборудование	Количество, шт	Стоимость, тенге
Сканер отпечатков пальцев ZFM60 V1.4	1	15500
Набор RFID модуля 13.56Mhz с карточкой и ключем	1	800
Модуль датчика наклона	1	500
MP3-плеер DFPlayer Mini	1	1780
Arduino Mega 2560 (CH340)	1	4600
Блок питания 220/12V 5A	1	3000
Преобразователь DC-DC понижающий 12В / 5	1	900
Модуль транзистора IRF520 для Ардуино	2	600
Кнопка	1	200
Провода, резисторы	20	500
Замок-защелка	2	4400
USB провод	1	700
Металлические ящики для сейфа	2	15000

Общая стоимость оборудования: 48480 тенге.

Рассмотрим каждое устройство в отдельности.

Сканер отпечатков пальцев ZFM60 V1.4 (рисунок 2.8), с подключением по последовательному интерфейсу (UART), скорость передачи данных 57600bps, напряжение питания 5В. К сканеру прилагалась инструкция (рисунок 2.9) и ПО (demo версия). Приложенное ПО (рисунок 2.10) к сканеру в работе не использовалось.

Рисунок 2.8 - Сканер отпечатков пальцев ZFM60 V1.4

Рисунок 2.9 – Инструкция к сканеру

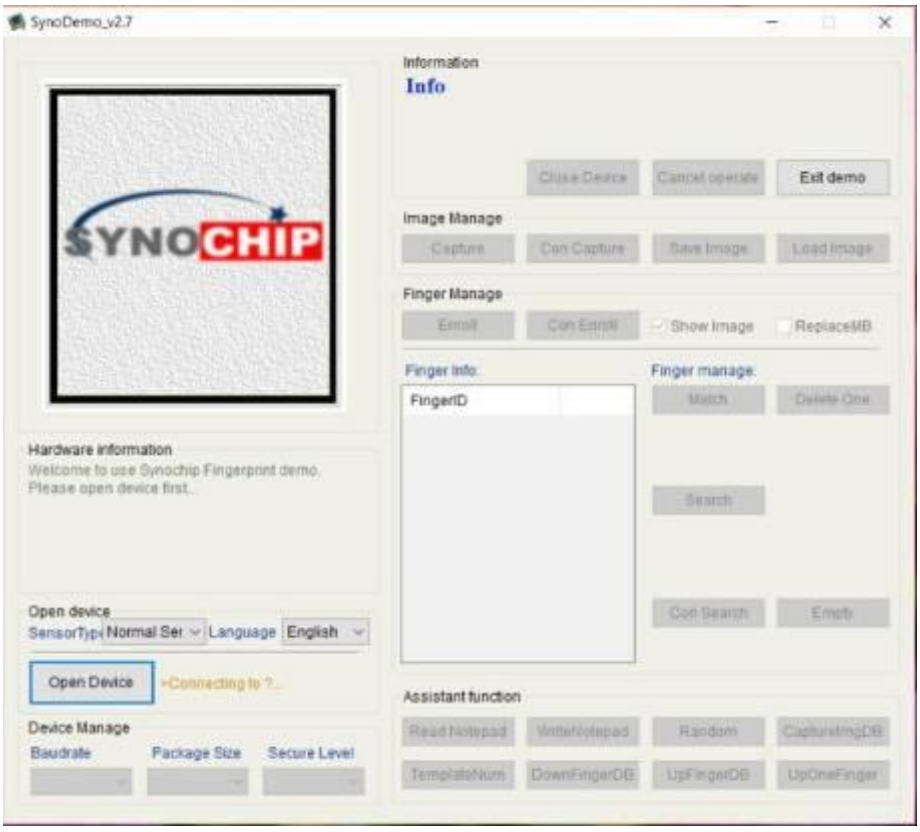


Рисунок 2.10 – ПО приложенное к сканеру

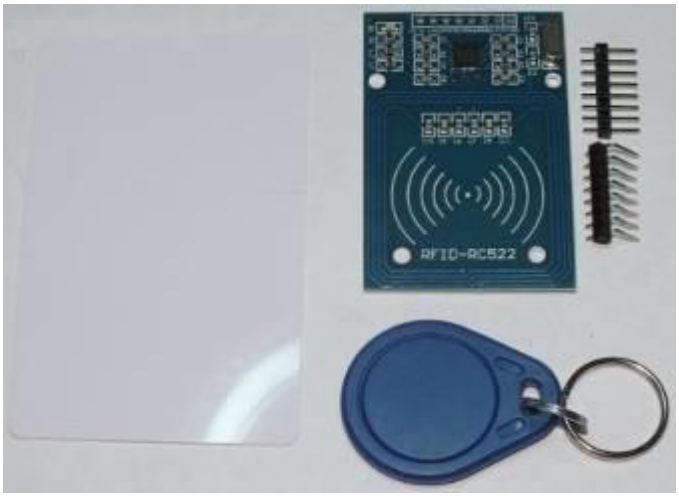


Рисунок 2.11 - Набор RFID модуля 13.56Mhz с карточкой и ключом

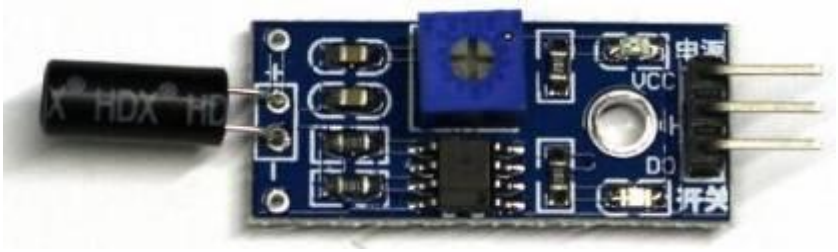
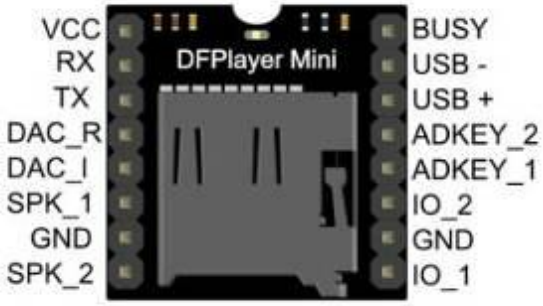


Рисунок 2.12 - Модуль датчика наклона

Риснуок 2.13 - MP3-плеер DFPlayer Mini

MP3-плеер DFPlayer Mini (рисунок 2.13) позволяет воспроизводить аудиофайлы, записанные на карту памяти формата microSD. С помощью данного плеера возможны также приостановка и возобновление воспроизведения, выбор одного из 30-ти уровней громкости и одного из 6-ти режимов эквалайзера. Для работы с DFPlayer Mini подойдет любая карта microSD с файловой системой FAT16 или FAT32 и объемом до 32 Гб.



Риснуок 2.14 – Пины MP3-плеера DFPlayer Mini

Таблица 2.2 – Характеристики MP3-плеер DFPlayer Mini

Название	Значение
Напряжение питания	3,3–5 В
Количество каналов	1 (моно, 3 Вт) + 2 (стерео, без усилителя)
Поддерживаемые частоты дискретизации	8, 11,025, 12, 16, 22,05, 24, 32, 44,1, 48 кГц
Разрядность ЦАП	24 бита
Отношение сигнал/шум	до 85 дБ
Поддерживаемые файловые системы	FAT16, FAT32
Максимальный объём карты памяти	32 ГБ
Количество каталогов композиций	до 100
Количество композиций в каталоге	до 255
Форматы аудиофайлов	MP3, WAV, WMA
Кол-во уровней громкости	30
Режимов эквалайзера	6 (Normal/Pop/Rock/Jazz/Classic/Base)

Рисунок 2.15 - Arduino Mega 2560 (CH340)

Таблица 2.3 – Характеристики Arduino Mega 2560

Название	Значение
Микроконтроллер	ATmega2560
Рабочее напряжение	5В
Входное напряжение (рекомендуемое)	7-12В
Входное напряжение (предельное)	6-20В
Цифровые Входы/Выходы	54 (14 из которых могут работат также как выходы ШИМ)
Аналоговые входы	16
Постоянный ток через вход/выход	40 mA
Постоянный ток для вывода 3.3 В	50 mA
Флеш-память	256 KB (из которых 8 KB используются для загрузчика)
ОЗУ	8 KB
Энергонезависимая память	4 KB
Тактовая частота	16 MHz

Принципиальная схема платы представлена в приложении А. Для правильной работы платы необходимо установить драйвер ch340 (рисунок 2.16).

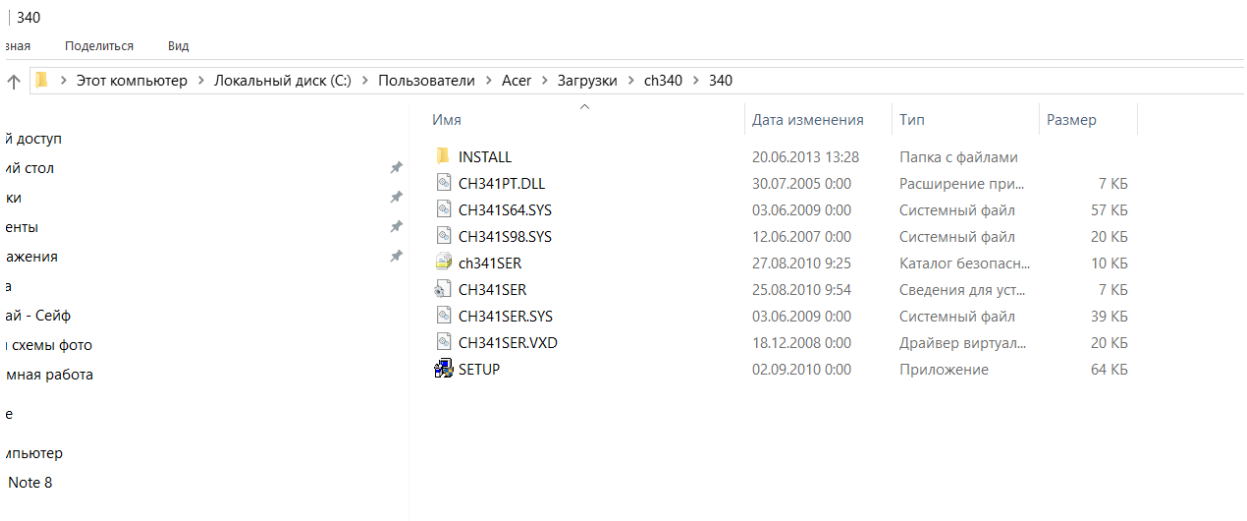


Рисунок 2.16 – Исходные файлы для установки драйвера

Рисунок 2.17 - Блок питания 220/12V 5A

Рисунок 2.18 - Преобразователь DC-DC понижающий 12В / 5

Рисунок 2.19 - Модуль транзистора IRF520 для Ардуино

Таблица 2.4 – Характеристики транзистора IRF520

Название	Значение
Транзистор	IRF520
Напряжение	до 24V DC
Рабочее напряжение	5V
Выходное напряжение на нагрузку	0—24V
Максимальный рабочий ток	5A
Сопротивление	Rds=0.23R@10V,5A

Рисунок 2.20 - Тактовая кнопка

Рисунок 2.21 – Металлические ящики

Рисунок 2.22 – USB шнур

Рисунок 2.23 – Замок-защелка

2.2 ПО на Delhi 10 Seattle

Embarcadero Delphi — интегрированная среда разработки ПО для Microsoft Windows, Mac OS, iOS и Android на языке Delphi (ранее носившем

название Object Pascal), созданная первоначально фирмой Borland и на данный момент принадлежащая и разрабатываемая Embarcadero Technologies.

Версия Delhi RAD Studio 10 Seattle — это законченное средство для быстрой разработки кроссплатформенных приложений с помощью Object Pascal и C++.

Основные возможности Delphi 10 Seattle:

- поддержка параллельной компиляции C++;
- отладка iOS 64x приложений;
- поддерживается iOS 8.4;
- поддерживается Android 5.1.1;
- поддержка служб Android;
- поддержка модульного тестирования DUnitX для Android и iOS;
- поддержка DirectX 12;
- поддержка вызова API WinRT;
- поддержка FireDAC для базы данных NoSQL MongoDB
- новое поведение MultiView;
- новые компоненты VCL;
- новые компоненты для работы с Beacon;
- улучшен механизм стилей;
- улучшен диспетчер библиотек GetIt;
- улучшены возможности IDE.

Система программирования Delphi рассчитана на программирование различных приложений и предоставляет большое количество компонентов для этого. К тому же работодателей интересует, прежде всего, скорость и качество создания программ, а эти характеристики может обеспечить только среда визуального проектирования, способная взять на себя значительные объемы рутинной работы по подготовке приложений, а также согласовать деятельность группы постановщиков, кодировщиков, тестеров и технических писателей. Возможности Delphi полностью отвечают подобным требованиям и подходят для создания систем любой сложности.

Основным конкурентом Delhi 10 Seattle является Lazarus. Для того чтобы обосновать, почему выбор остановился на Delhi 10 Seattle, достаточно провести сравнительный анализ двух сред разработки.

Таблица 2.5 - Сравнительный Delhi 10 Seattle и Lazarus.

Технические различия	Delhi 10 Seattle	Lazarus
Установка дополнительных компонент	удобнее. Не надо компилировать весь пакет, надо скомпилировать только модули компонента.	Для того, чтобы установить дополнительный компонент Lazarus, нужно полностью перекомпилировать всю визуальную систему программирования,

Продолжение таблицы 2.5

		компонент интегрируется в среду и становится непосредственной ее частью.
Время компилирования	Процесс компилирования в среде Delphi занимает более короткое время.	Процесс компилирования в среде Lazarus занимает более длительное время по сравнении с Delphi и зависит от мощности компьютера и объема проекта.
Удобство в работе	В Delphi работать с компонентами труднее.	В Lazarus работать с компонентами намного удобнее. При добавлении новых элементов на поле формы появляются линии, помогающие выровнять этот элемент с другими.
Интерфейс	У Delphi больше вкладок с компонентами.	Code Editor у Lazarus отличается от Delphi только тем, что у него нет субокна Explore. Это субокно в Lazarus является отдельным окном и может быть вызвано через «Вид/Обозреватель кода».
Сохранение проектов	В Delphi сохранение проекта происходит в Файл> Сохранить Проект.	Lazarus автоматически сохраняет проект при компиляции.
Работа с несколькими проектами одновременно	в Delphi необходимо сохранить запущенный проект и закрыть его, после этого можно будет открыть другой проект.	В Lazarus можно запускать несколько проектов одновременно.
Исполнимые файлы	Delphi, использует	Lazarus подключает для

при компиляции	собственный отладчик, поэтому при компиляции нет необходимости включать в исполнимые	отладки внешнюю программу gdb (GNU Debugger) и вынужден включать в компилируемые
	файлы дополнительную информацию, что уменьшает размер компилируемых исполнимых файлов и соответственно уменьшает время компиляции	исполнимые файлы информацию, помогающую этому отладчику в работе. Объём такой информации в несколько раз превышать объём кода.

Таблица 2.6 – Сравнительный анализ Delhi 10 Seattle и Visual Studio

Среда разработки	Delhi 10 Seattle	Visual Studio
Плюсы	1) Быстрая и простая разработка настольных приложений. 2) Быстрая компиляция проектов. 3) Возможность разрабатывать мобильные приложения. 4) Простота использования форм.	1) IDE имеет более современный интерфейс, например, для темы темного цвета. 2) Модульное тестирование легко и интегрировано в IDE, что облегчает запуск тестов во время разработки. 3) Отладка сервисов легче, чем в Delphi.
Минусы	1) Некоторые области IDE выглядят устаревшими	1) Медленный запуск среды разработки. 2) Частое зависание ПО.

Таблица 2.7 – Сравнение VS и Delphi в компиляции и отладке

Свойство	Visual Studio	Delphi
Удаление неиспользуемых переменных Linker’ом	нет	да
Создание Release и Debug версий	да	нет
Наличие break-point’ов	да	да
Пошаговый проход	да	да
Возврат вверх по коду во время отладки	да	да

Продолжение таблицы 2.7

Изменение кода во время отладки	да	да
Завершение работы приложение при исключительном событии	да	нет
Оптимизация приложения	да	да
Раздельная компиляция	да	нет
Скорость выполнения приложения	высокая	средняя
Автоматическое сохранение проекта	да	нет

В результате сравнительного анализа для дипломного проекта была выбрана среда разработки Delhi 10 Seattle, так как данная среда разработки по таким критериям как цена, доступность компонентов, легкость в разработке более подходит для данного проекта. Преимущества Delphi по сравнению с аналогичными программными продуктами:

- быстрота разработки приложения (RAD);
- высокая производительность разработанного приложения;
- низкие требования разработанного приложения к ресурсам компьютера; - наращиваемость за счет встраивания новых компонент и инструментов в среду Delphi;
- возможность разработки новых компонентов и инструментов собственными средствами Delphi (существующие компоненты и инструменты доступны в исходных кодах);
- удачная проработка иерархии объектов.

Работа в программе Delphi изображена на рисунке 2.24. После создания формы для приложения и добавления компонентов необходимо настроить свойства компонентов (рисунок 2.25). На рисунке 2.26 изображено редактирование свойств компонента CommPortDriver1. Этот компонент необходим для взаимодействия приложения с платой. После написания кода программы (рисунок 2.27) необходимо проверить работоспособность приложения (рисунок 2.28) посредством компиляции (рисунок 2.29). На рисунке 2.30 изображен интерфейс приложения.

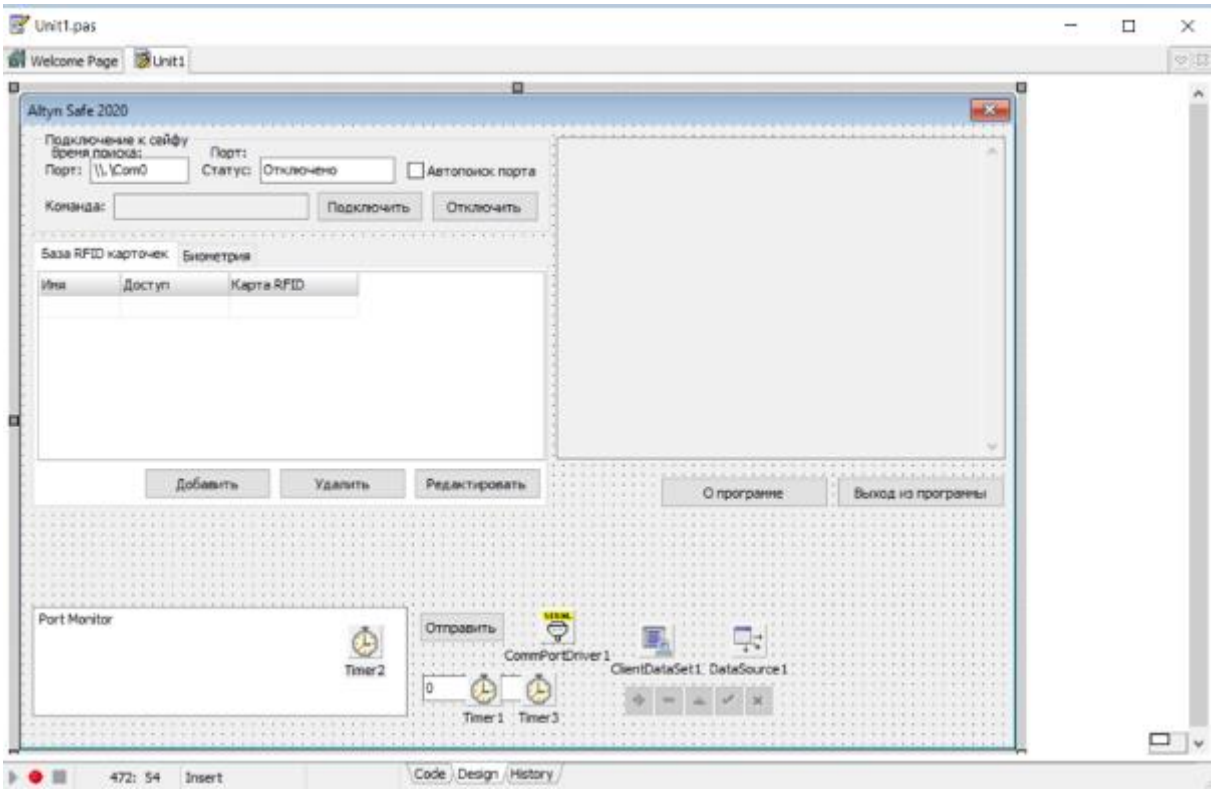


Рисунок 2.24 – Создание формы для приложения, добавление компонентов

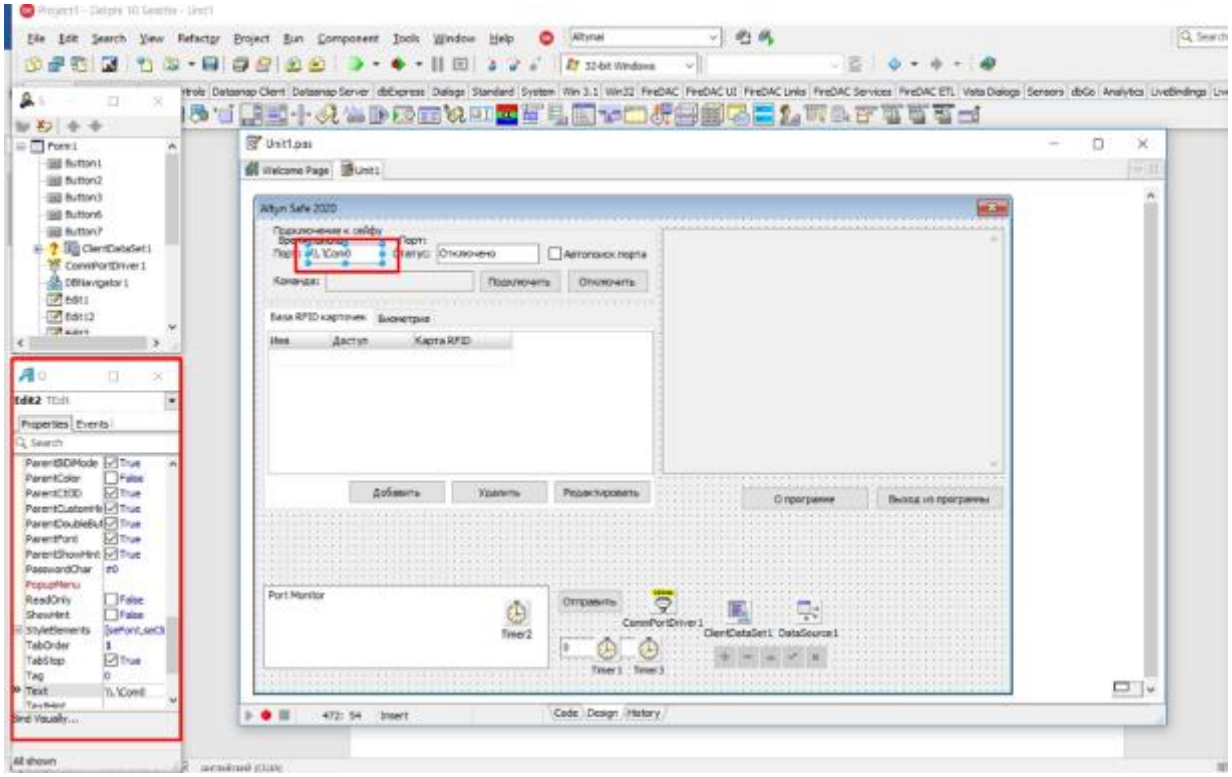


Рисунок 2.25 – Редактирование свойств компонента «Текстовое поле»

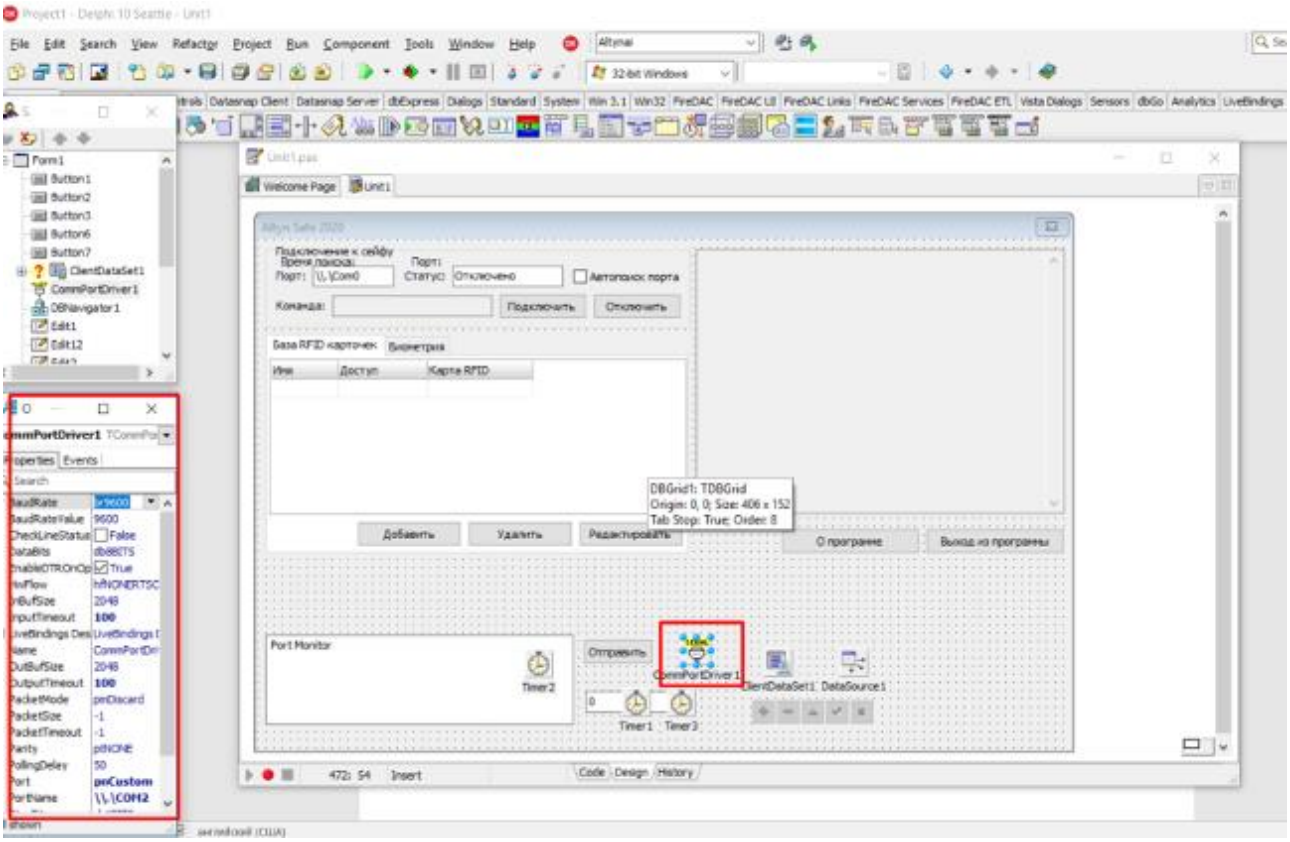


Рисунок 2.26 – Редактирование свойств компонента CommPortDriver1

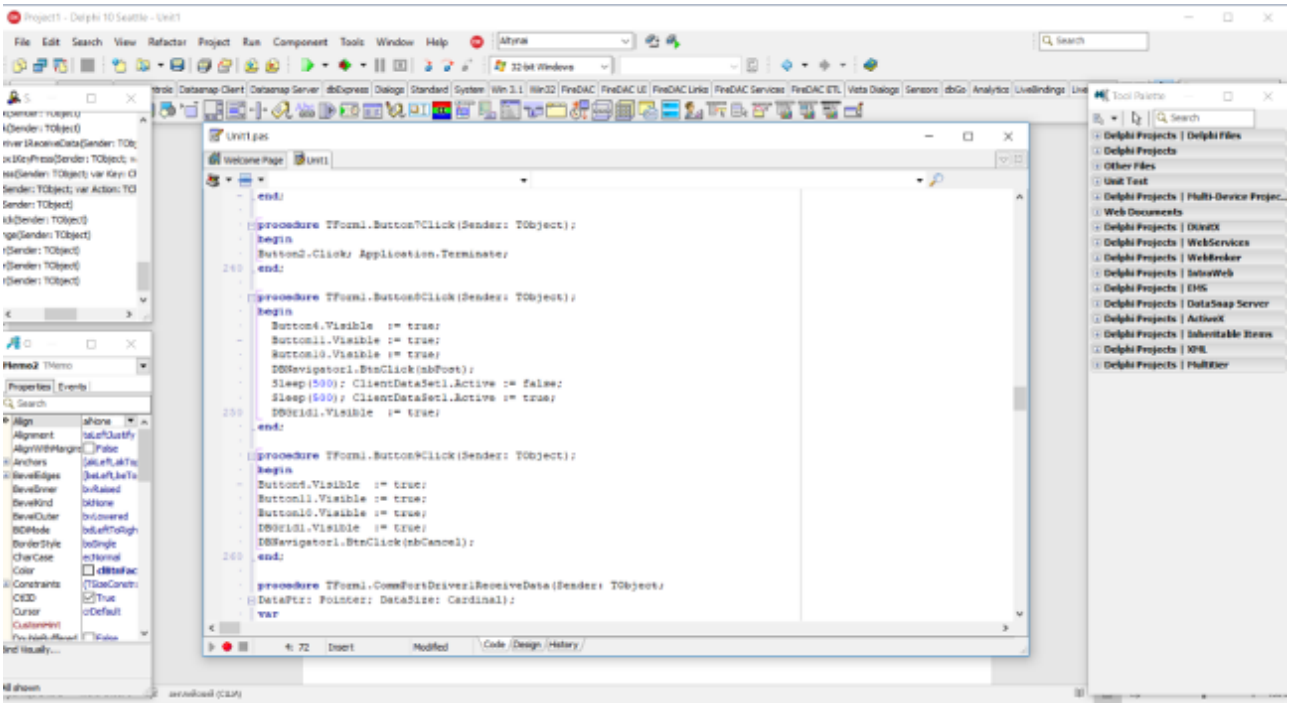


Рисунок 2.27 – Код программы (Приложение А)

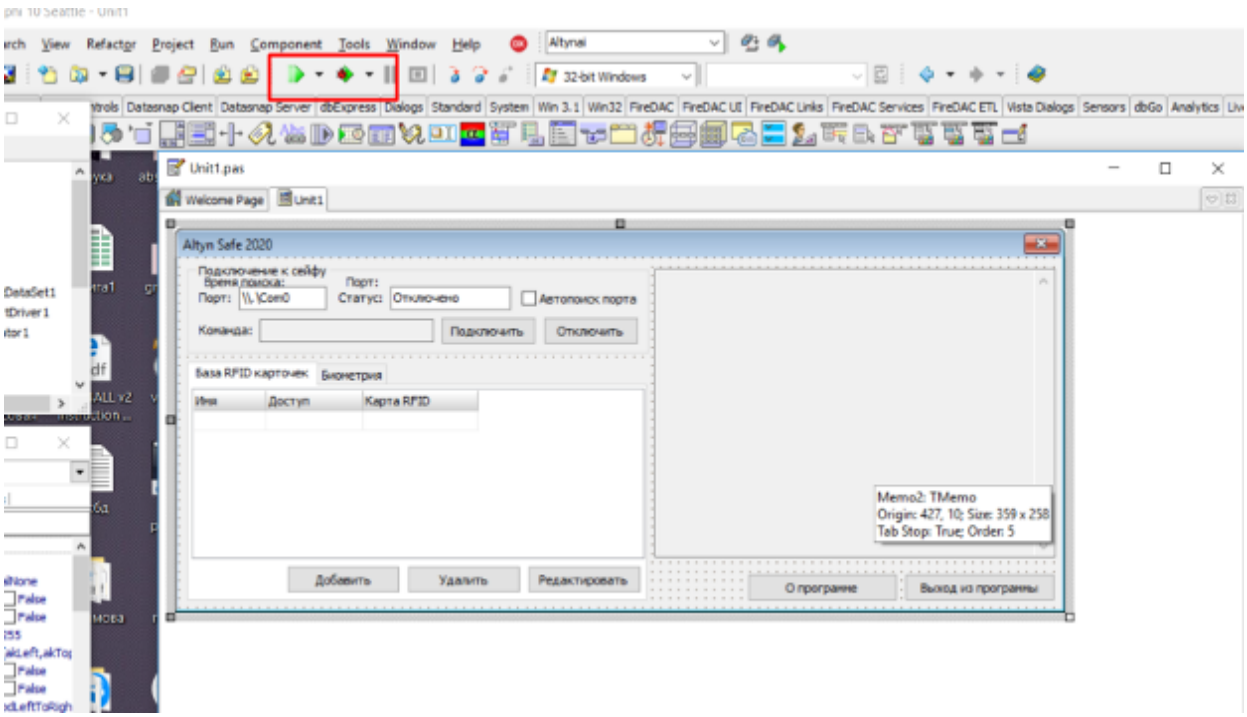


Рисунок 2.28 – Проверка работоспособности приложения

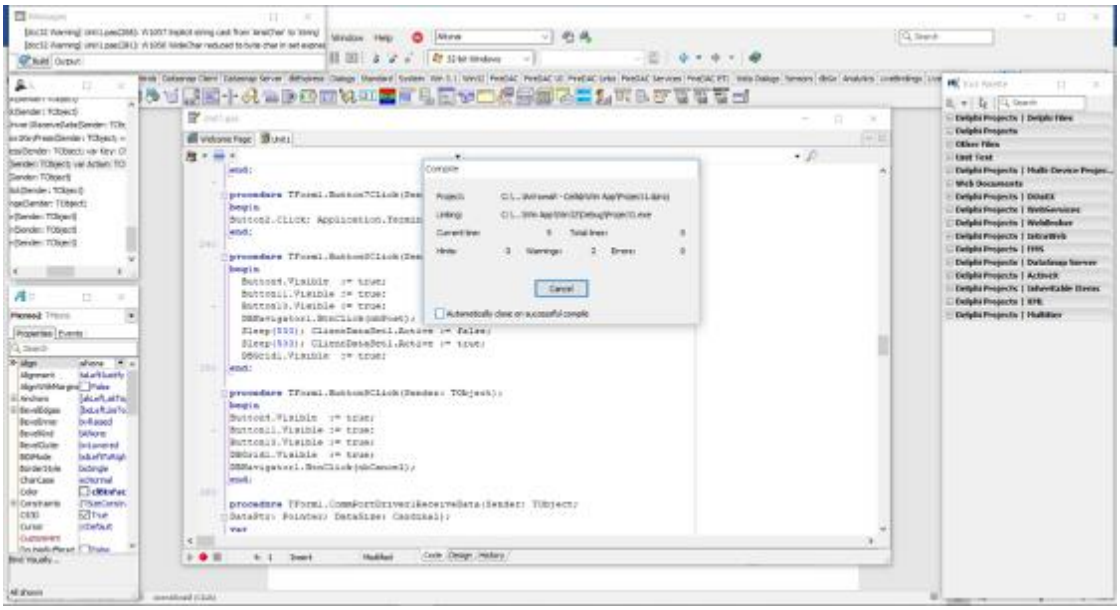


Рисунок 2.29 – Процесс компиляции

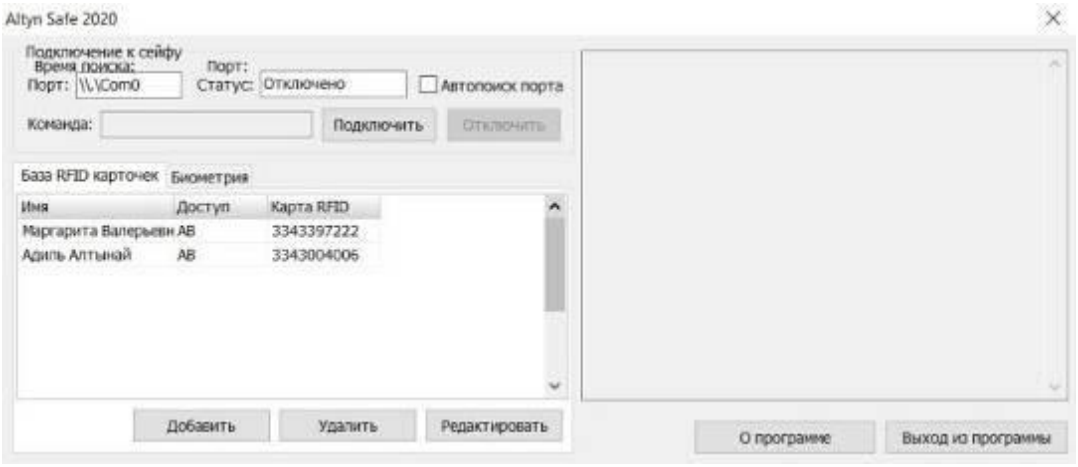


Рисунок 2.30 – Результат компиляции

2.3 Код программы на Arduino

Arduino — это простая для освоения платформа с открытым кодом на основе встроенного микроконтроллера и среды разработки с программным интерфейсом API для микроконтроллеров. Для взаимодействия между человеком и микроконтроллером могут присоединяться различные аналоговые и цифровые датчики, которые регистрируют состояние окружающей среды и передают данные в микроконтроллер. Микроконтроллер обрабатывает входящие данные, а программа выдает новые данные в виде аналоговых или цифровых значений. Как платформу для разработки помимо Arduino используют одноплатные компьютеры, типичным представителем является Raspberry Pi.

Таблица 2.6 – Сравнительный анализ микроконтроллера Arduino и одноплатного компьютера Raspberry Pi

Характеристика	Микроконтроллер	Одноплатный компьютер
Производительность	1 ядро, десятки-сотни МГц, десятки КБ оперативки, десятки-сотни КБ постоянной памяти.	1 или более ядер, сотни-тысячи МГц, сотни МБ оперативки, гигабайты постоянной памяти.
Многозадачность	Нет. Но можно эмулировать.	Да. Управляется ОС.
Удобство работы с интернетом	Обычно нужны дополнительные модули и глубокое знание протоколов.	Легко подключается из коробки, сетевой модуль обычно уже на борту.

Продолжение таблицы 2.6

Длительность работы от батареек	Потребляет единицы-десятки мА. Возможны недели работы от батареек.	Потребляет сотни-тысячи мА. Заряда большого аккумулятора хватит от силы на десяток часов.
Скорость реакции в проектах критичных к времени	100% контроль над временем и длительностью подачи сигналов.	Из-за многозадачности критический процесс может проспать своё время.
Выбор языков программирования	Ограниченный. Чаще C/C++.	Python, JavaScript, Bash и десяткии других: любые доступные в ОС.
Возможности для работы с видео, компьютерным зрением	Не хватит мощности.	OpenCV, аппаратные видеокодеки, HDMI-выход.
Возможности для работы со звуком	На мощных микроконтроллерах возможен синтез звука. Для работы с MP3/OGG/WAV нужны дополнительные модули.	Поддержка MP3/OGG/WAV на уровне ОС. Аудиовыход HDMI и/или разъём 3,5 мм.

В результате сравнительного анализа для реализации задач проекта был выбран микроконтроллер Arduino. Преимущества:

- Arduino IDE основан на AVRGCC. Если отсутствует конкретная высокоуровневая команда или библиотека для Arduino, ее всегда можно заменить на аналогичную C++;

- возможность питать, программировать и обмениваться сообщениями с Arduino при помощи одного USB кабеля (или FTDI кабеля для некоторых клонов);

- возможность сделать простой проект за несколько минут, используя стандартные библиотеки;

- последовательные и SPI интерфейсы связи сделаны превосходно.

На сегодняшний день существует большое количество видов плат Arduino, начиная с классических Arduino UNO, Leonardo, Mini, Micro и Nano и заканчивая специфическими Industrial 101, Tian и MKR1000. И все эти платы имеют какие-либо характерные отличия и различные области применения. Платы отличаются друг от друга своими формами, характеристиками и возможностями. Для облегчения выбора платы для проекта ниже приводится сравнительная таблица большинства выпущенных на сегодняшний день плат Arduino.

Таблица 2.7 – Сравнительный анализ плат Arduino

Плата Arduino	Микроконтроллер	Рабочее напряжение (В)	Цифровые входы/выходы	Выходы с ШИМ
Uno	Atmega328	5	14	6
Leonardo	Atmega32u4	5	20	7
Nano	Atmega328	5	14	6
Mega	Atmega2560	5	54	14
Due	Atmel SAM3X8E ARM Cortex-M3 CPU	3.3	54	12
Mini	Atmega328	5	14	6
Micro	Atmega32u4	5	20	7
MO	Atmel SAMD21	3.3	20	12
LilyPad	Atmega328p	2.7-5.5	20	6
Uno	Atmega328	6	40	32
Leonardo	Atmega32u4	12	40	32
Nano	Atmega328	8	40	32
Mega	Atmega2560	16	40	256
Due	Atmel SAM3X8E ARM Cortex-M3 CPU	12	800	512
Mini	Atmega328	6	40	32
Micro	Atmega32u4	12	40	32
MO	Atmel SAMD21	6	7	256
LilyPad	Atmega328p	6	40	32

В результате сравнительного анализа была выбрана плата Arduino Mega2560. При установке ПО Arduino программа запрашивает разрешение на установку дополнительного программного обеспечения, для корректной работы Arduino необходимо установить все дополнительные ПО в процессе установки.

После написания кода программы необходимо загрузить код на плату Arduino (рисунок 2.31).

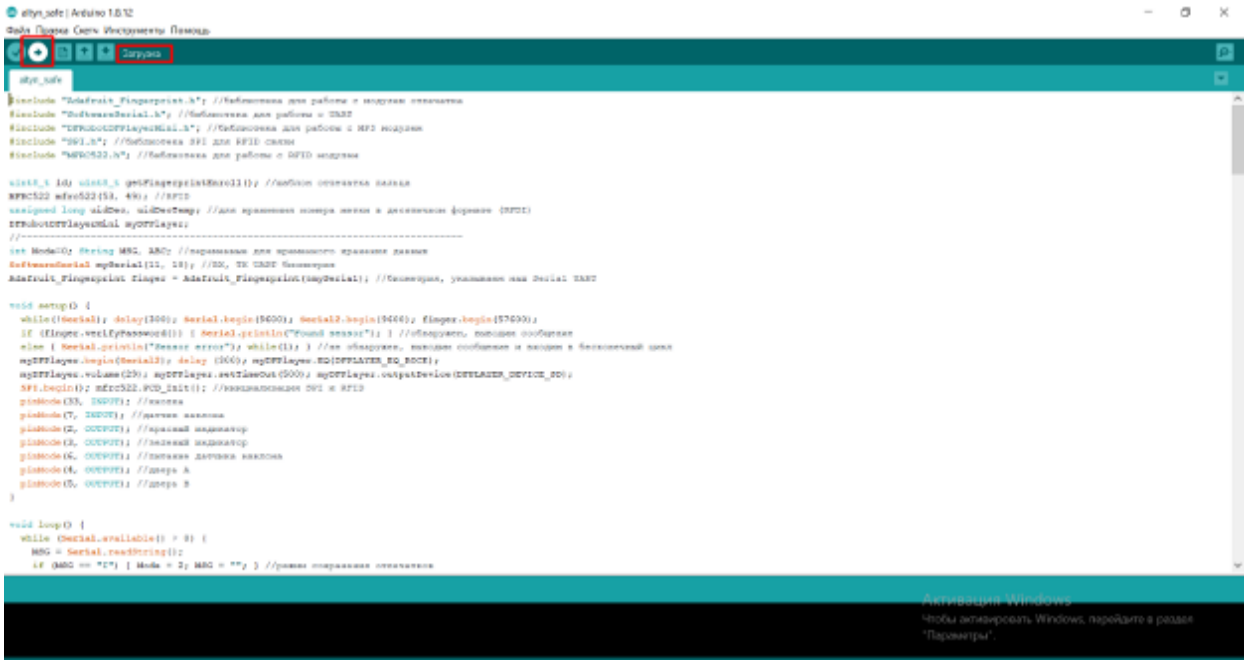


Рисунок 2.31 – Загрузка кода программы

При загрузке кода программы видим сообщение об ошибке «Adafruit_Fingerprint. No such file or directory» (рисунок 2.32). Для исправления данной ошибки необходимо дополнительно подключить библиотеку (рисунок 2.33).

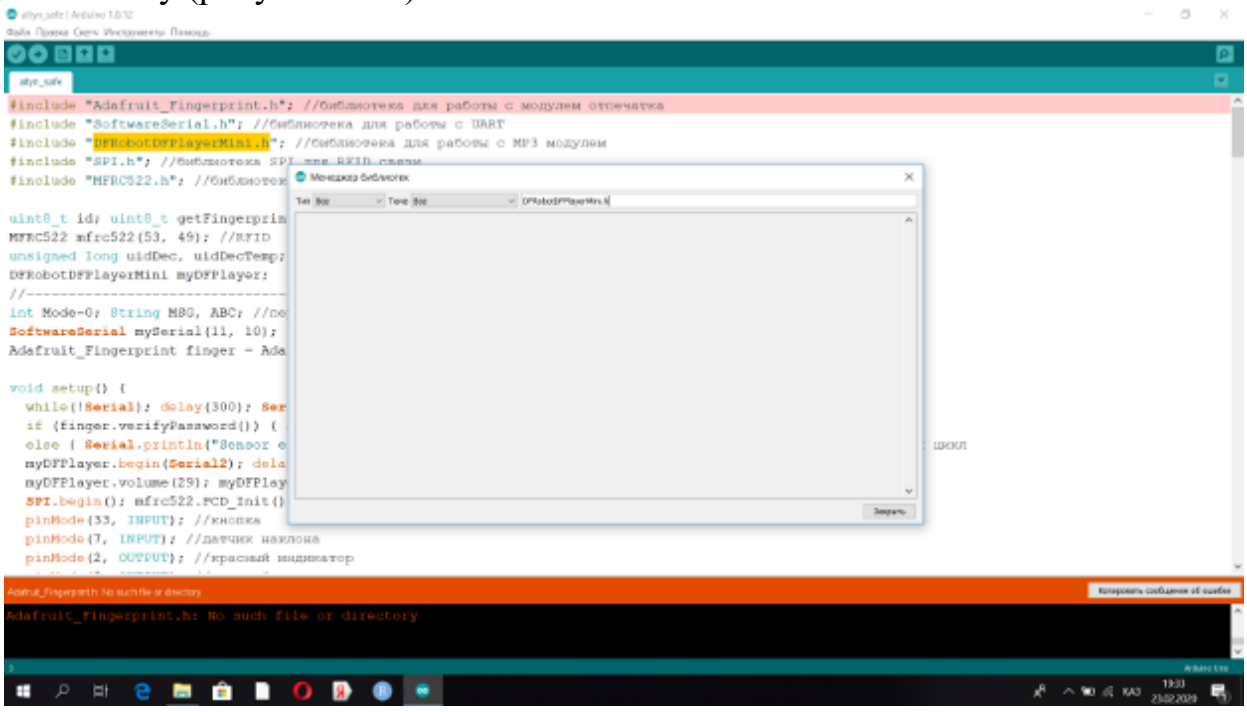


Рисунок 2.32 – Сообщение об ошибке

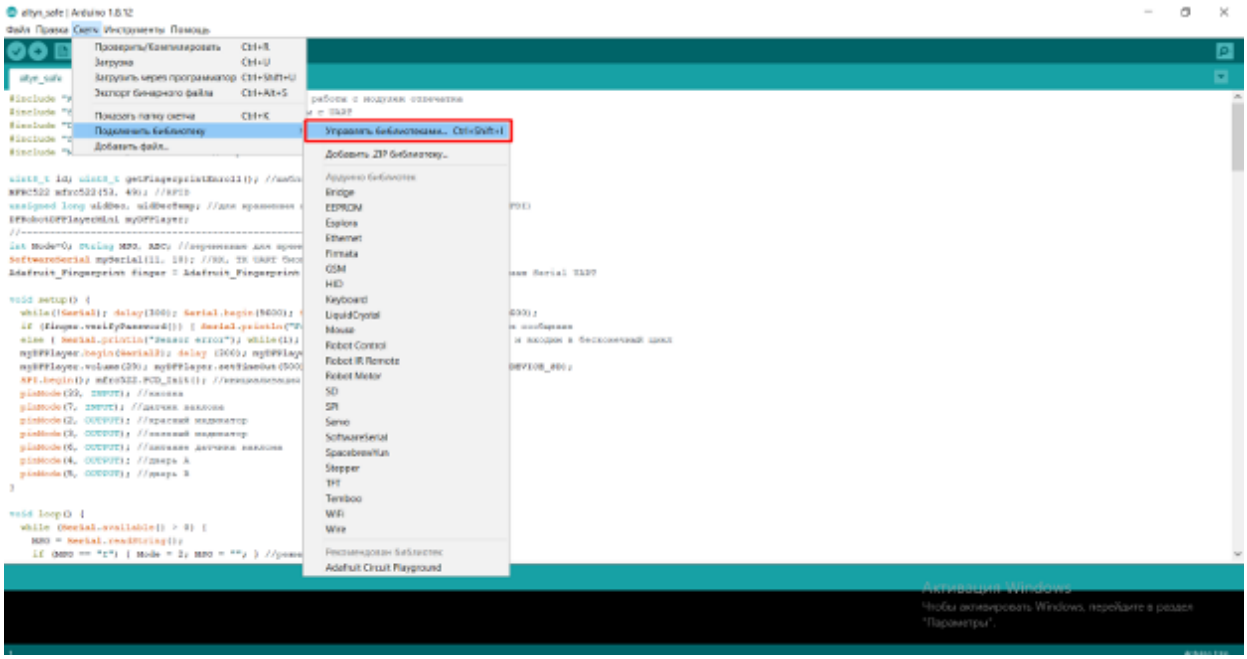


Рисунок 2.33 – Подключение библиотеки

В менеджере библиотек необходимо найти библиотеки (рисунок 2.34) и произвести установку (рисунок 2.35).

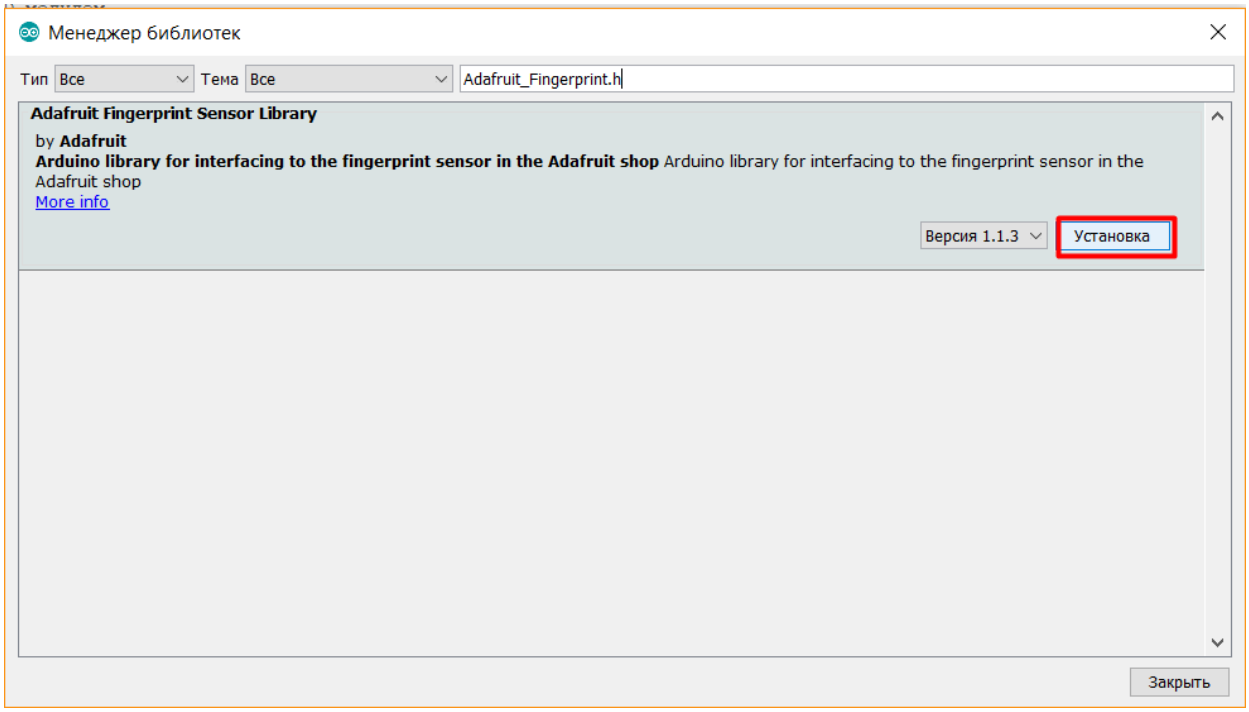


Рисунок 2.34 – Поиск библиотеки

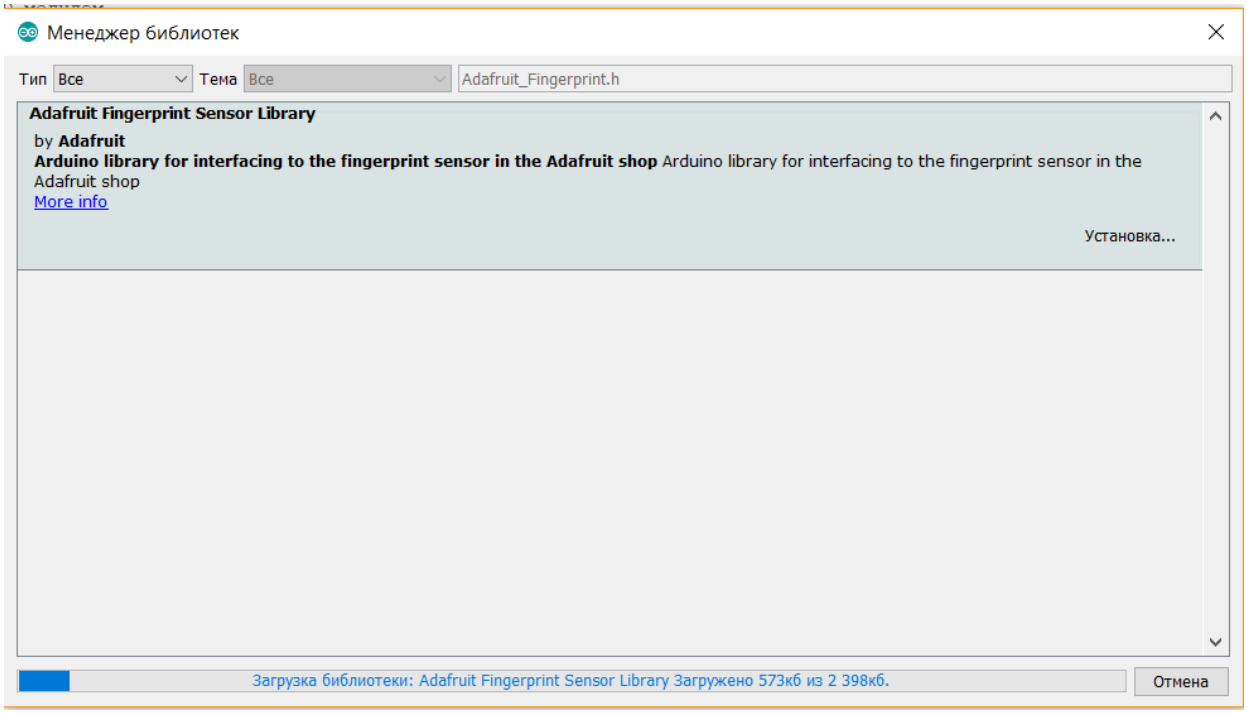


Рисунок 2.35 – Процесс установки библиотеки

Таким образом добавляем все необходимые библиотеки. Далее при попытке загрузки кода видим ошибку «Serial2 was not declared in this scope». Для исправления данной ошибки меняем плату «Arduino Uno» в настройках на «Arduino Mega or Mega 250" (рисунок 2.36). После изменения настроек платы проверяем подключение порта (рисунок 2.37), при успешном подключении порта загружаем код на плату (рисунок 2.38).

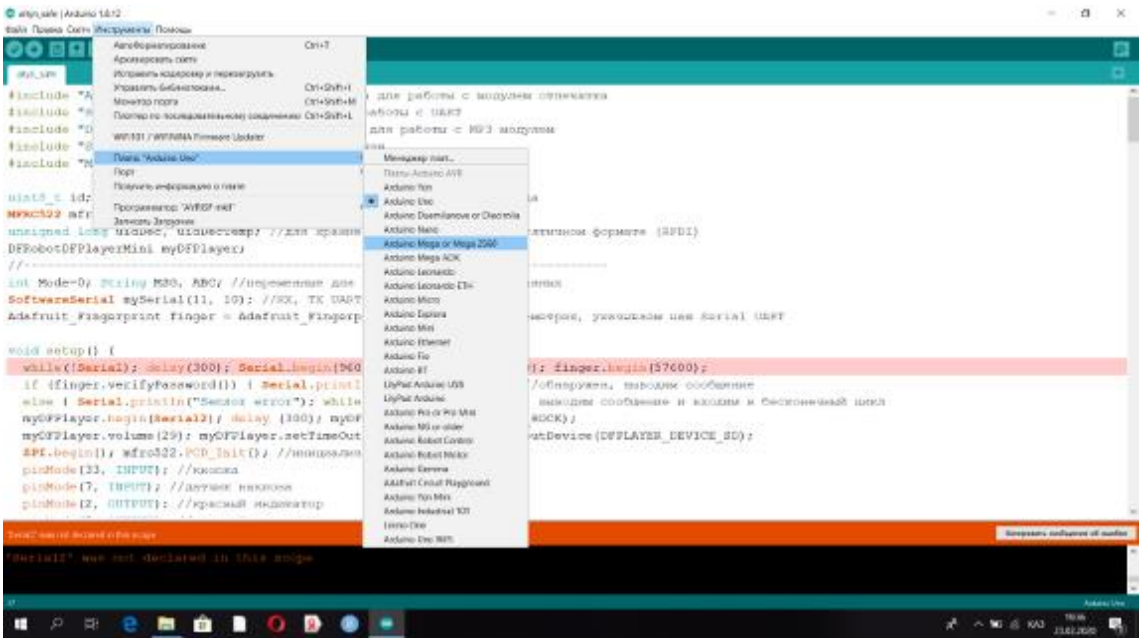


Рисунок 2.36 – Изменение настроек платы

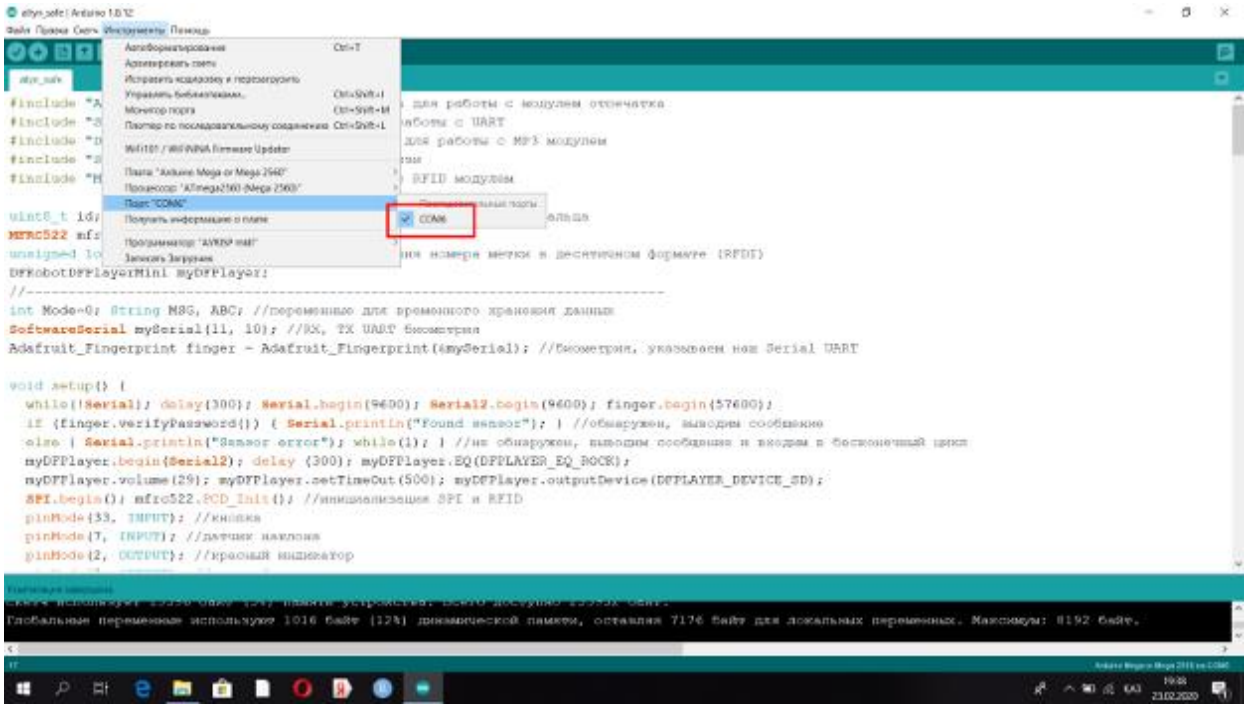


Рисунок 2.37 – Проверка подключения порта

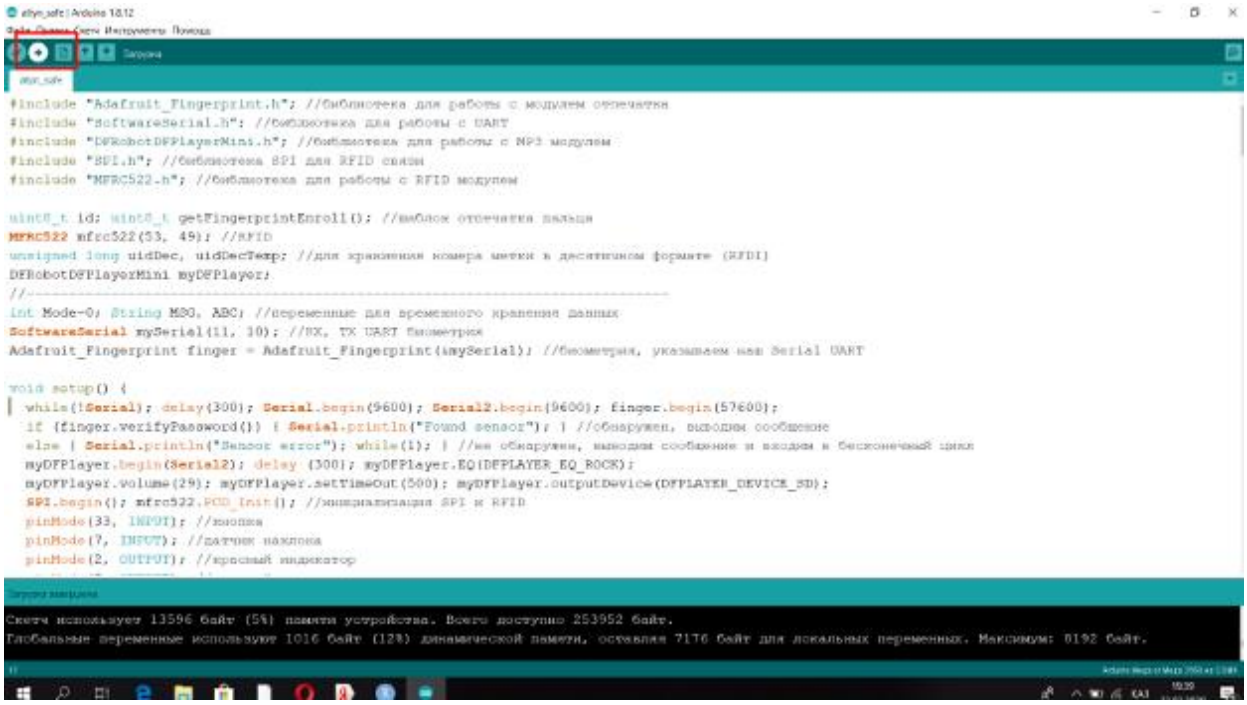


Рисунок 2.38 – Успешная загрузка кода на плату

2.4 Результат работы

Всего смарт карт шесть (рисунок 2.39). Самая большая смарт карта открывает обе дверцы сейфа вне зависимости от настроек программы. Доступ к дверцам сейфа следующих пяти мини карт настраивается в приложении.

Рисунок 2.39 – Смарт карты

Рисунок 2.40 – Открытие сейфа большой картой

При открытии сейфа большой картой (рисунок 2.40) открываются обе дверцы сейфа (рисунок 2.41).

Рисунок 2.41 – Открытие двух дверей

Рисунок 2.42 – Открытие сейфа картой под номером 1

Далее открываем дверь картой под номером 1 (рисунок 2.42). В приложении видим, что карта 1 принадлежит Адиль Алтынай (рисунок 2.43), и доступ разрешен к обоим дверцам (рисунок 2.44).

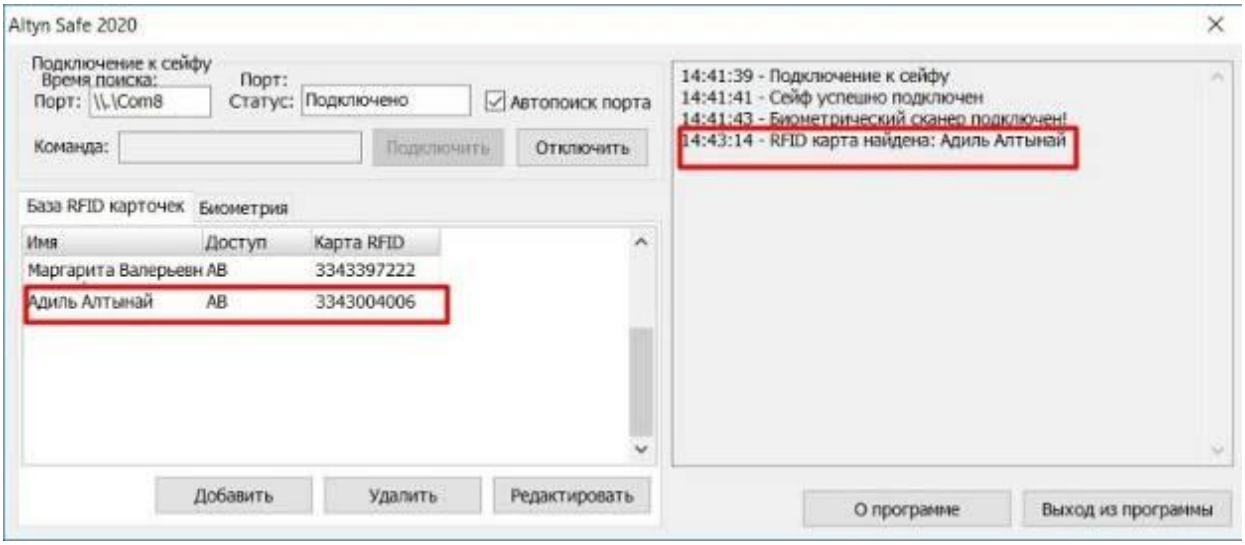


Рисунок 2.43 – Нахождение карты

Рисунок 2.44 – Результат

Базу карточек в приложении можно редактировать, удалять, добавлять новые карты. Для редактирования базы данных карточек (рисунок 2.45) необходимо выбрать имя держателя карты и выбрать кнопку редактировать. Во вкладке «редактировать» возможно изменить имя держателя карты, идентификационный номер карты, а также изменить доступ к дверцам сейфа (рисунок 2.46). Для удаления карты из базы данных необходимо выбрать карту и выбрать кнопку «удалить» (рисунок 2.47). При добавлении карты

необходимо ввести имя держателя карты, выбрать доступ и идентификационный номер карты (рисунок 2.48).

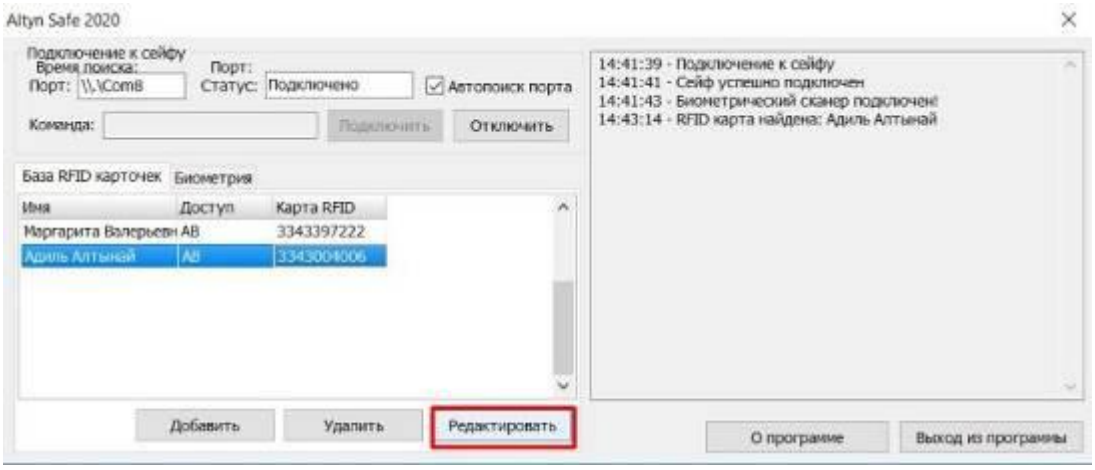


Рисунок 2.45 – Редактирование базы карточек

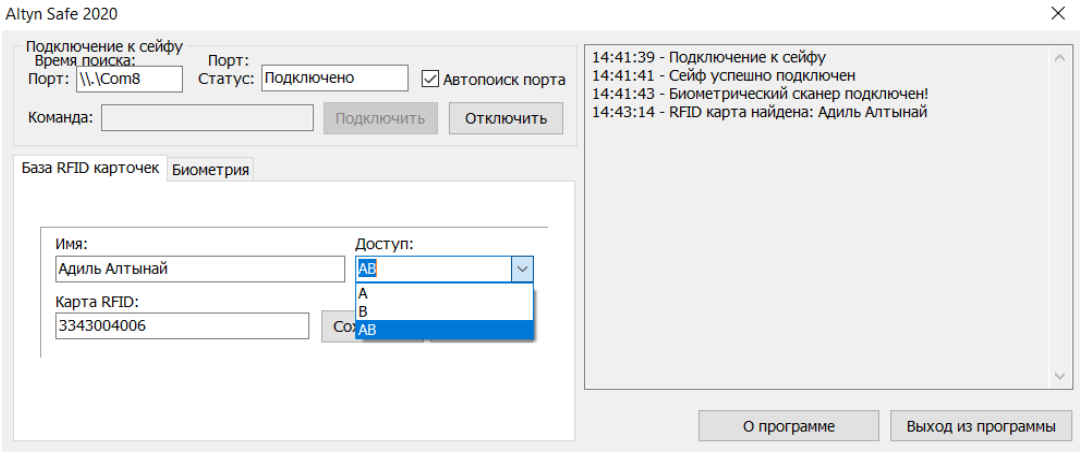


Рисунок 2.46 – Редактирование карты Адиль Алтынай

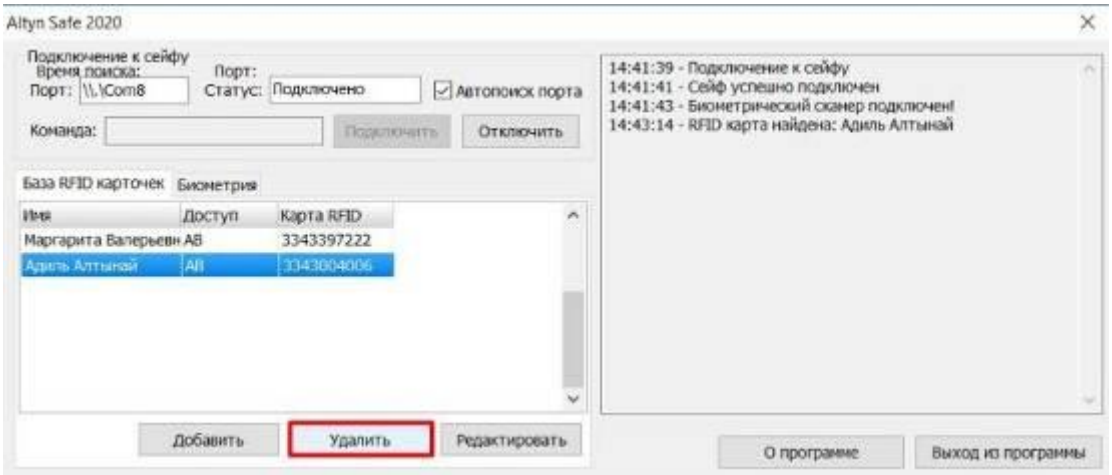


Рисунок 2.47 – Удаление карты

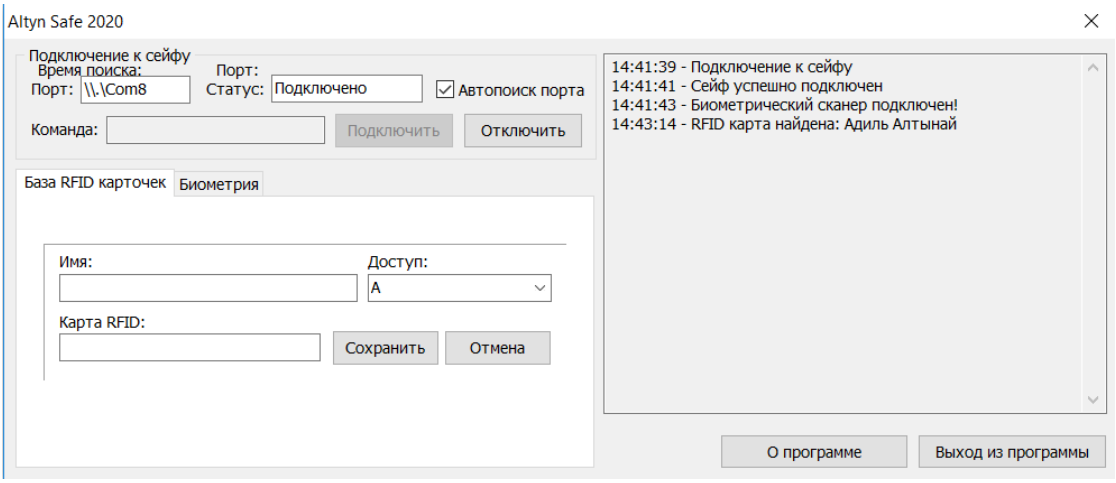


Рисунок 2.48 – Добавление карты

Далее добавляем отпечаток пальца в приложение для открытия двери при помощи биометрического сканера (рисунок 2.49).

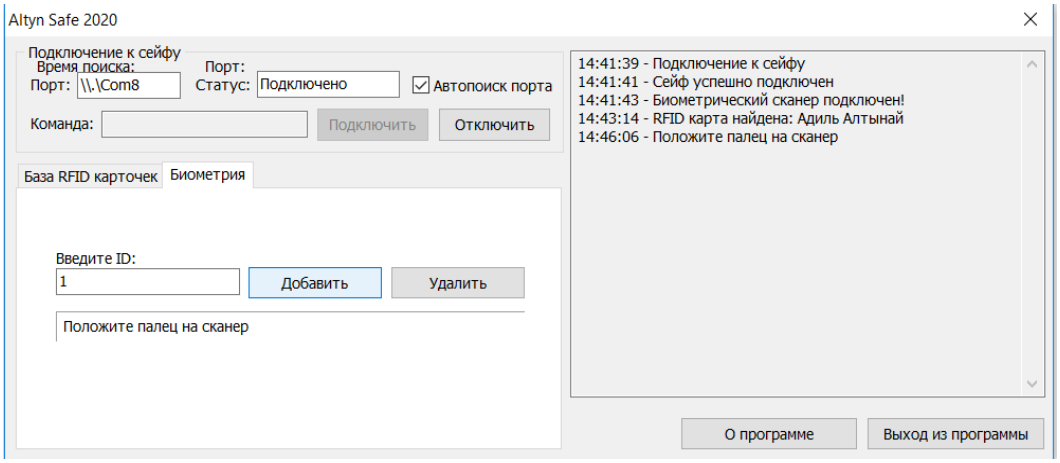


Рисунок 2.49 – Добавление отпечатка пальца

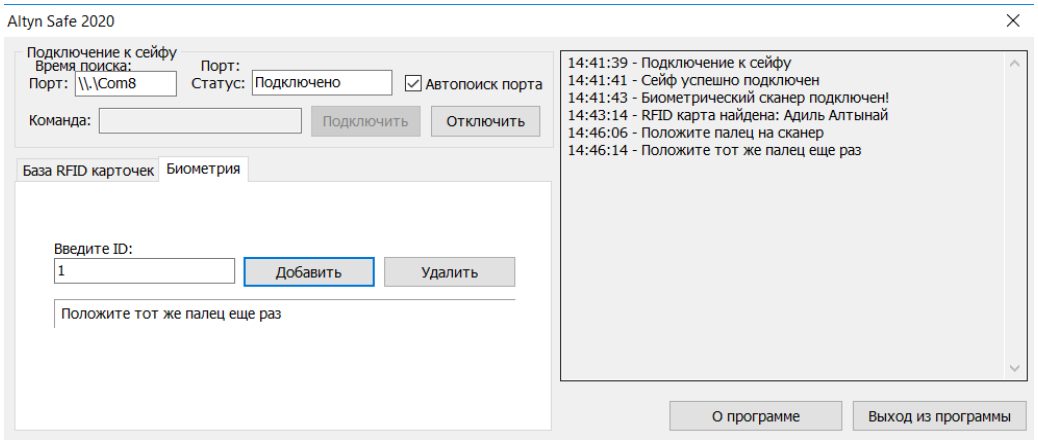


Рисунок 2.50 – Сканирование отпечатка пальца

При добавлении отпечатка пальца приложение выдает сообщение «Положите палец на сканер» (рисунок 2.50), после того как прикладывается нужный палец на сканер необходимо повторно его просканировать. После сканирования отпечатка пальца видим сообщение «Модель отпечатка пальца сохранена» (рисунок 2.51). Также, как и смарт карты отпечатки пальцев можно удалять (рисунок 2.52) и добавлять в приложении. Сканер отпечатков пальцев запоминает до 100 пальцев.

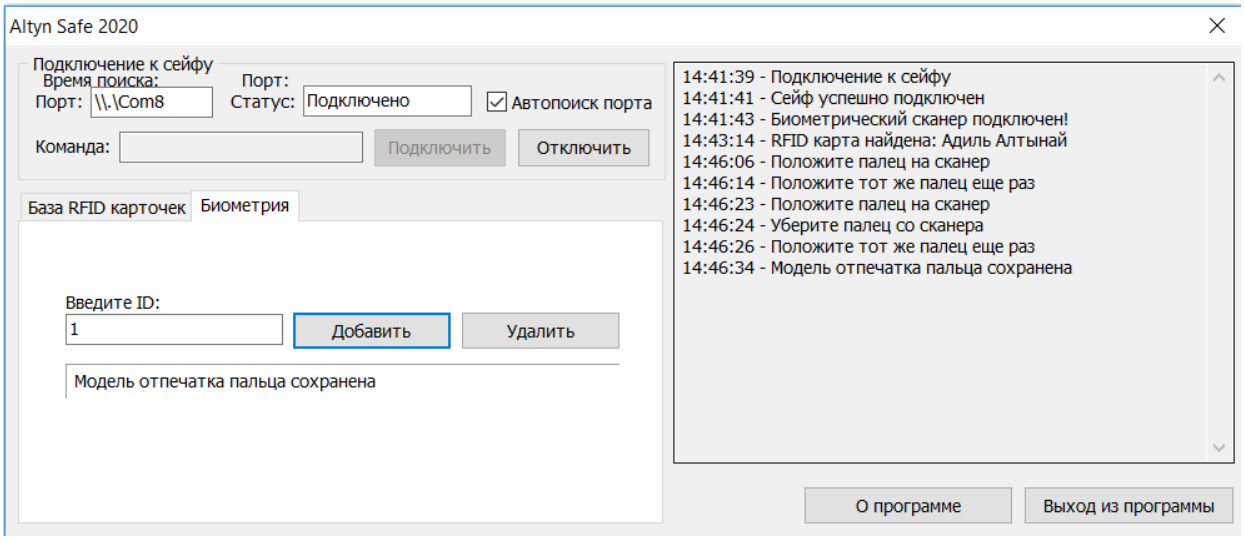


Рисунок 2.51 – Сохранение модели отпечатка пальца

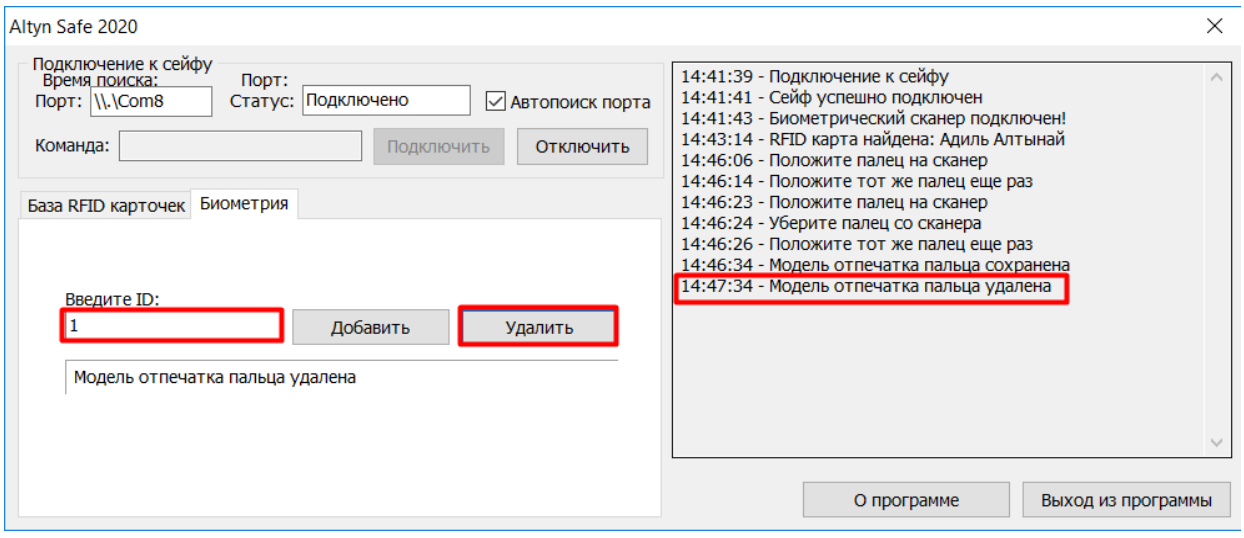


Рисунок 2.52 – Удаление модели отпечатка пальца

Вывод по разделу: в данном разделе были описаны структурные схемы, детали конструкции, схемы подключения всех устройств. Также была описана последовательность создания приложения на ПО Arduino, Delphi 10 и сборка конструкции. В результате данного раздела были показаны работа биометрического и карточного модулей.

3 Оценка рисков

3.1 Расчёт рисков

В данной дипломной работе в качестве актива был выбран сейф как сложный актив. Сейф состоит из простых активов: биометрический сканер, считыватель RFID меток, программное обеспечение, дверцы сейфа, карточки, датчики наклона, замки, плата ARDUINO. Далее риски просчитываются для каждого простого актива.

Уровень риска рассчитывается по формуле:

$$\lambda=\tau*\eta, \quad (3.1)$$

где λ - уровень риска, тг;

τ - шкала вероятности возникновения, тг;

η - ценность актива, тг.

После расчета рисков указываются необходимые меры по обработке и уменьшению рисков. Далее рассчитываются остаточные риски также по формуле (3.1). В таблице 3.1 описаны простые активы. Ценность актива определяется по таблице 3.2.

Таблица 3.1 – Перечень активов

Наименование простого актива	Кол-во	Ответственный	Ценность	Приоритет	Код актива
Биометрический сканер	1	Служба безопасности	1	2	А
Считыватель RFID меток	1	Служба безопасности	1	3	Б
ПО	1	Администратор	2	4	В
Дверцы сейфа	2	Служба безопасности	1	5	Г
Карточки	6	Сотрудники	1	6	Д
Датчики наклона	1	Служба безопасности	1	8	Е
Замки	2	Служба безопасности	1	7	Ж
Плата ARDUINO	1	Служба безопасности	1	1	З

Таблица 3.2 – Ценность актива

Ценность актива	Значение
1	до 50 000 тг
2	до 100 000 тг
3	до 200 000 тг

Продолжение таблицы 3.2

4	до 400 000 тг

5	от 600 000 тг

Таблица 3.3 – Шкала вероятности возникновения рисков

Значение	Описание
0 - очень низкий	раз в несколько лет
1 - низкий	один раз в 3 года
2 - средний	несколько раз в год
3 - высокий	один раз в месяц

Таблица 3.4 – Шкала приемлемости рисков

Значение	Потери	Описание
от 0 до 3	стоимость до 150 000 тг	приемлемый риск (п)
от 4 до 7	стоимость до 500 000 тг	средне-приемлемый риск (сп)
от 7	стоимость выше 500 000 тг	неприемлемый риск (н)

Таблица 3.5 – Расчет рисков (итоговая таблица)

Угрозы	Уязвимости	Максимальный уровень риска	Меры по обработке риска	Остаточный уровень риска	Дата	Ответственный за выполнение, комментарии
Обработка рисков сейфа (сложный актив)						
1) Биометрический сканер						
1.1 Остановка функционирования сканера отпечатков пальцев	Отключение питания	1	Обеспечение бесперебойного питания	0	18.04.20	Служба безопасности
1.2 Взлом датчика	Отсутствие шифрования	2	Шифрование	1	18.04.20	Служба безопасности
1.3 Атака подделки	Нарушение соблюдения конфиденциальности	1	Дополнительная верификация физических характеристик	0	18.04.20	Служба безопасности
2) Считыватель RFID меток						
2.1 Подмена содержимого памяти RFID меток	Отсутствие шифрования	1	Шифрование	0	18.04.20	Служба безопасности
2.2 Атаки RFID-Zapper (уничтожение меток)	Слабый защитный слой меток	2	Обеспечение защитного слоя меток, устойчивого к электромагнитному полю	1	18.04.20	Служба безопасности
2.3 Клонирование меток	Отсутствие шифрования	3	Шифрование	2	18.04.20	Служба безопасности
3) ПО						
3.1 Заражение вирусом	Отсутствие шифрования	2	Шифрование	0	18.04.20	Служба безопасности
3.2 Захват ресурсов ПО	Не обновлённый антивирус	2	Антивирусная система	0	18.04.20	Служба безопасности

3.3 Модификация данных, находящихся в ПО	Нарушение соблюдения конфиденциальности	4	Разграничение доступа	2	18.04.20	Служба безопасности
4) Дверцы сейфа						
4.1 Кража данных	Нарушение соблюдения конфиденциальности	2	Разграничение доступа	1	18.04.20	Служба безопасности

Продолжение таблицы 3.5

4.2 Модификация содержимого сейфа	Отсутствие или неверное организация парольной защиты	3	Организация парольной защиты	2	18.04.20	Служба безопасности
4.3 Физический взлом	Слабая система защиты от физического доступа, неправильная организация доступа	1	Использование прочных материалов	0	18.04.20	Служба безопасности
5) Карточки						
5.1 Утеря карточки	Нарушение соблюдения конфиденциальности	2	Удаленная блокировка карт	1	18.04.20	Служба безопасности
5.2 Доступ к данным	Отсутствие шифрования	2	Шифрование	1	18.04.20	Служба безопасности
5.3 Атака ROCA	Отсутствие шифрования	3	Шифрование	2	18.04.20	Служба безопасности
6) Датчики наклона						
6.1 Обход датчиков	Слабая система защиты	3	Использование нескольких датчиков	2	18.04.20	Служба безопасности
6.2 Отключение питания	Отключение питания	1	Обеспечение бесперебойного питания	0	18.04.20	Служба безопасности

Продолжение таблицы 3.5

6.3 Кражда данных	Слабая система защиты	2	Использование различных датчиков	1	18.04.20	Служба безопасности
8) Плата ARDUINO						
8.1 Физический взлом	Слабая система	1	7) Замки	0	18.04.20	Служба безопасности
7.1 Физический взлом	Слабая система защиты от физического доступа, неправильная организация доступа	2	Использование средств защиты	1	18.04.20	Служба безопасности
8.2 Перехват данных	Слабая система	2	Шифрование	1	18.04.20	Служба безопасности
7.2 Утеря данных	Отсутствие шифрования	3	Разграничение доступа	2	18.04.20	Служба безопасности
8.3 Модификация кода	Слабая система	1	Использование	0	18.04.20	Служба безопасности
7.3 Вскрытие замка	Отсутствие или неверное организация физического доступа, парольной защиты неправильная организация доступа	1	Организация дополнительных мер защиты	0	18.04.20	Служба безопасности

Вывод: был исследован сейф как сложный актив, состоящий из простых активов. К каждому активу были рассмотрены риски, состоящие из угроз и уязвимостей. По таблице 3.7 можно заметить, что до принятия мер по обработке рисков уровень риска был выше, соответственно финансовые потери организации также увеличивались. После принятия мер по уменьшению рисков можно заметить, что уровень рисков стал ниже.

3.2 Исследование рисков методологией Coras

Метод CORAS позволяет осуществлять анализ рисков путем их моделирования. Его суть состоит в адаптации, уточнении и комбинировании таких методов проведения анализа рисков, как Event-Tree-Analysis, цепи Маркова, HazOp и FMECA. CORAS использует технологию UML и базируется на австралийском/новозеландском стандарте AS/NZS 4360: 1999 Risk Management и ISO/IEC 17799-1: 2000 Code of Practice for Information Security Management. В соответствии с подходом CORAS информационные системы рассматриваются не только с точки зрения используемых технологий, а как сложный комплекс, в котором учитывается и человеческий фактор.

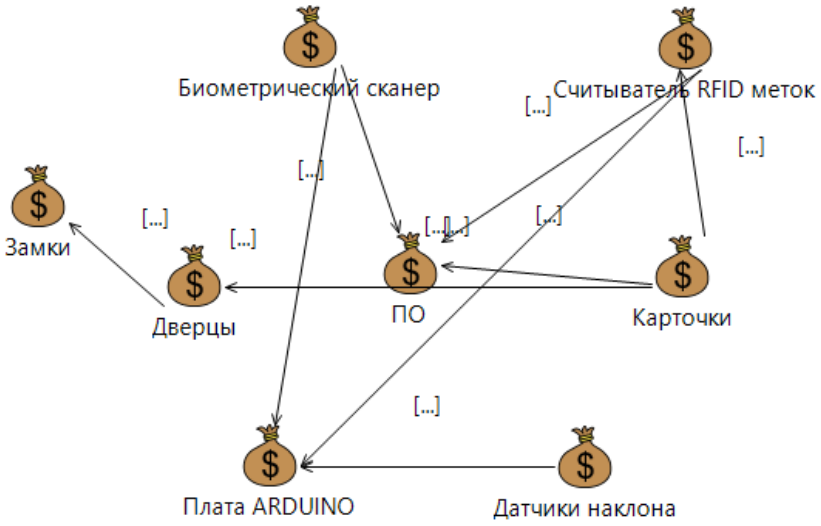


Рисунок 3.1 – Диаграмма активов

Описание схем Coras: на рисунке 3.1 изображена схема взаимодействия активов. Биометрический сканер подключен к плате ARDUINO и ПО, считыватель RFID меток также подключен к плате ARDUINO и ПО. Карточки необходимы для открытия дверцей сейфа, редактируются при помощи ПО и взаимодействуют со считывателем RFID меток. Замки необходимы для обеспечения защиты дверцей сейфа и содержимого сейфа. Датчики наклона используются как дополнительная защита от кражи данных, хранящихся в сейфе. Датчики наклона подключены к плате ARDUINO. На рисунке 3.2 изображена схема модели угроз. В качестве актива был рассмотрен сейф как сложный актив. На рисунке изображены источники угроз:

- злоумышленники;

- администратор;
- сама система биометрического модуля и модуля RFID.

Также изображены возможные риски, которые состоят из угроз и уязвимостей и зависимость актива от рисков. На рисунке 3.3 изображена модель угроз с вероятностными характеристиками до принятия мер по уменьшению рисков. После добавления мер по обработке рисков показатели вероятностных характеристик улучшились. Это можно наблюдать на рисунке 3.5. На рисунке 3.6 изображены отдельно неприемлемые риски, на которые необходимо обратить внимание и принять соответствующие меры по уменьшению рисков. По рисунку 3.4 можно заметить риски с характеристикой последствий осуществления угрозы. Например, отсутствие шифрования данных считается неприемлемым риском. Так как при отсутствии шифрования данных может произойти атака RFID-Zapper, что может привести ко взлому сейфа, краже данных злоумышленником.

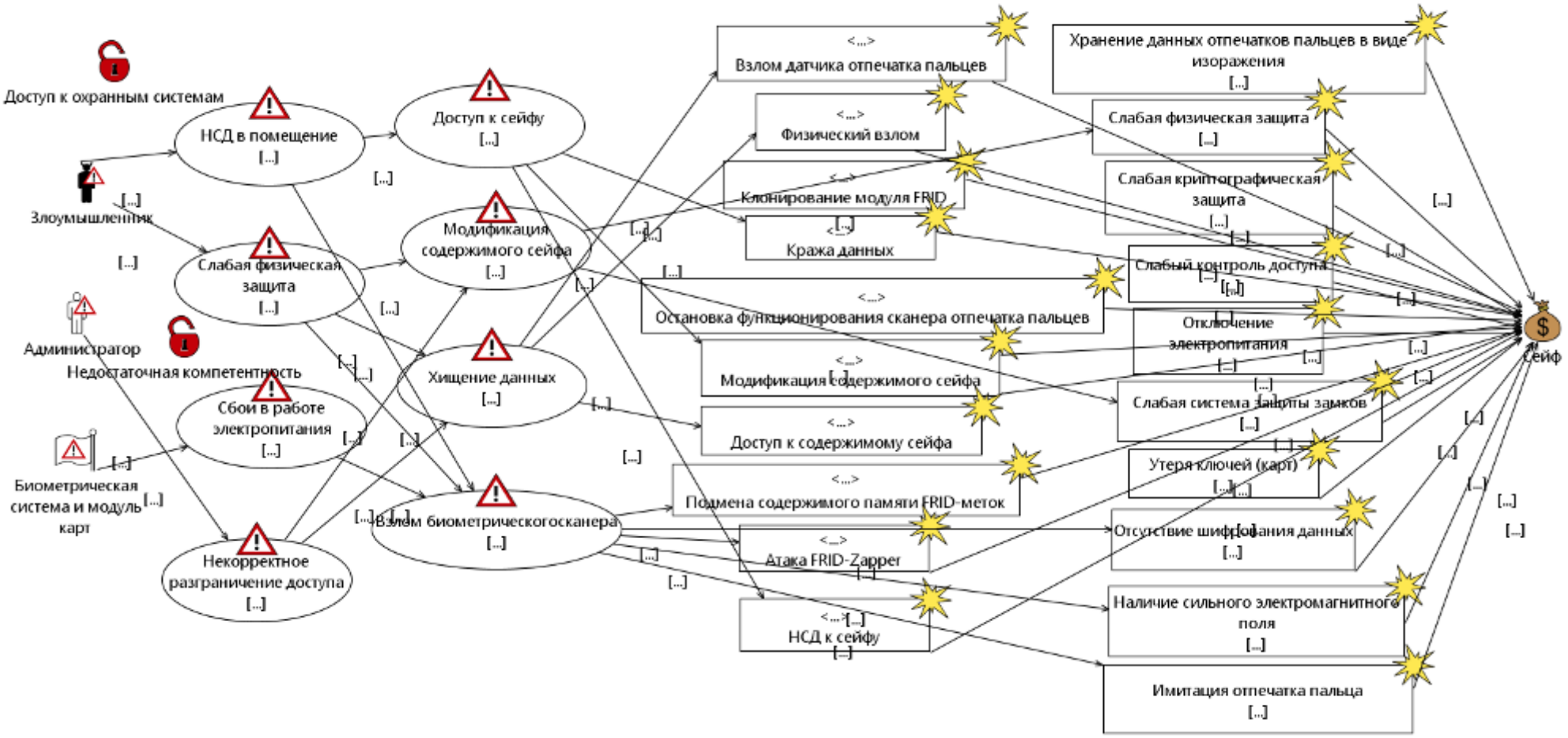


Рисунок 3.2 - Модель угроз

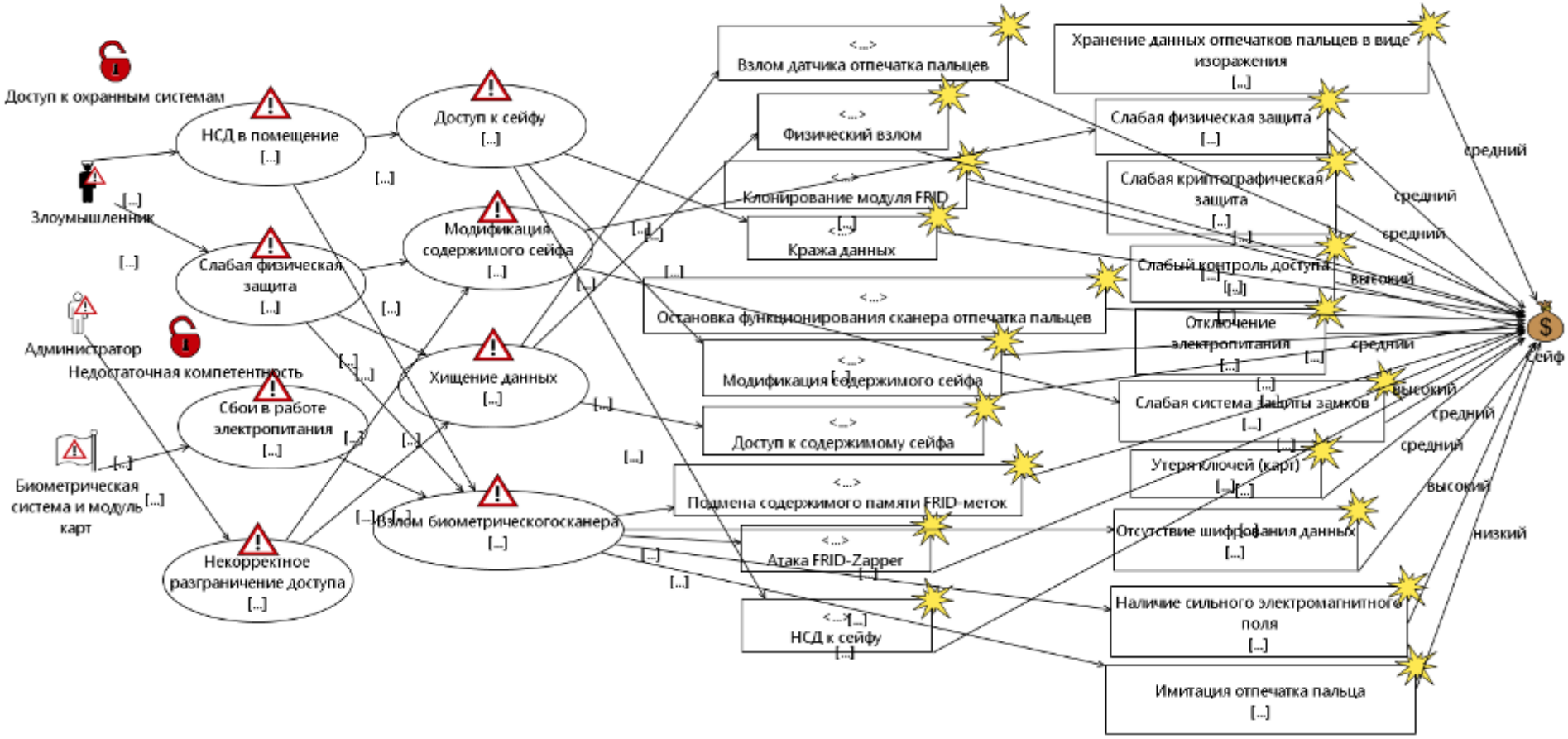


Рисунок 3.3 - Модель угроз с вероятностными характеристиками

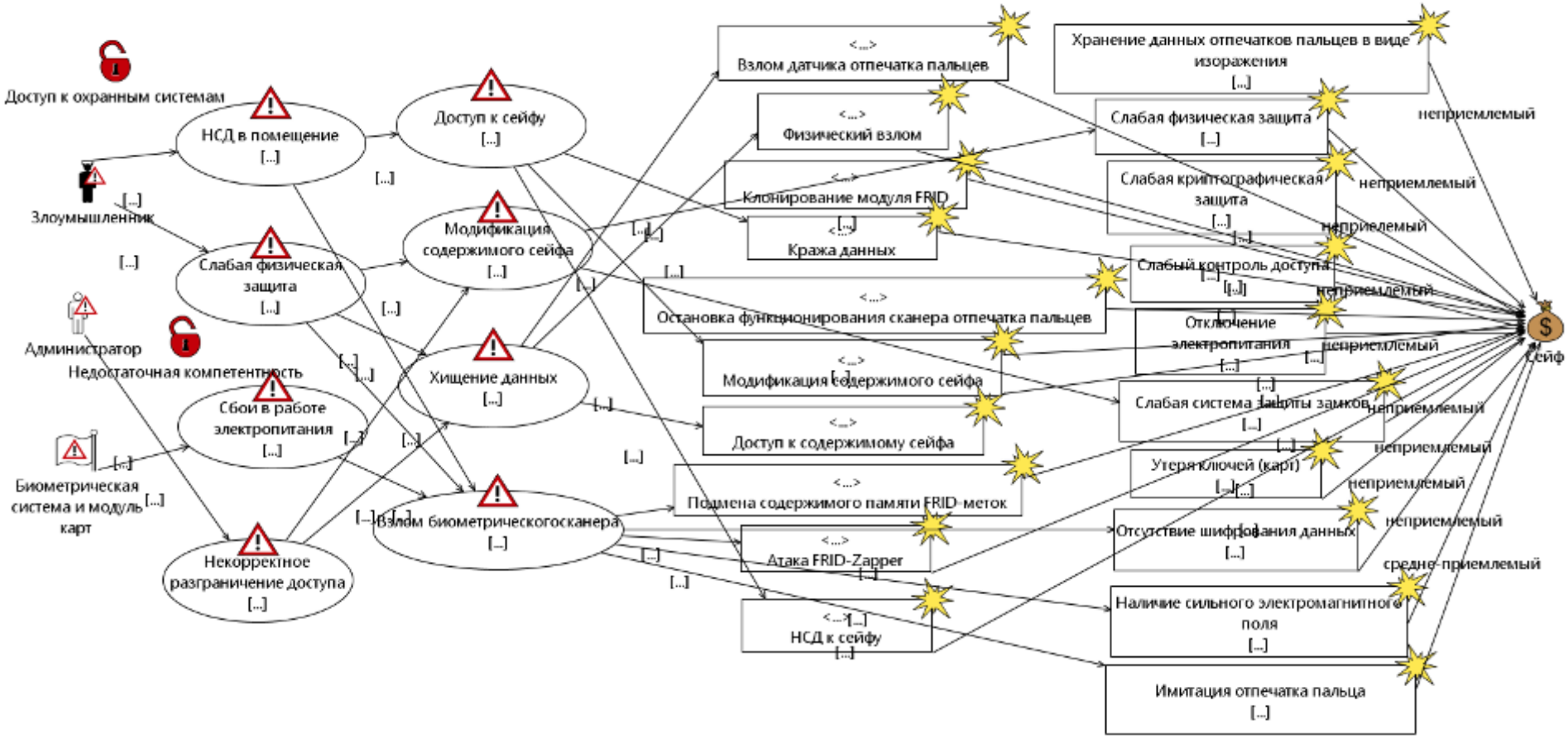


Рисунок 3.4 - Диаграмма рисков с характеристикой последствий осуществления угрозы

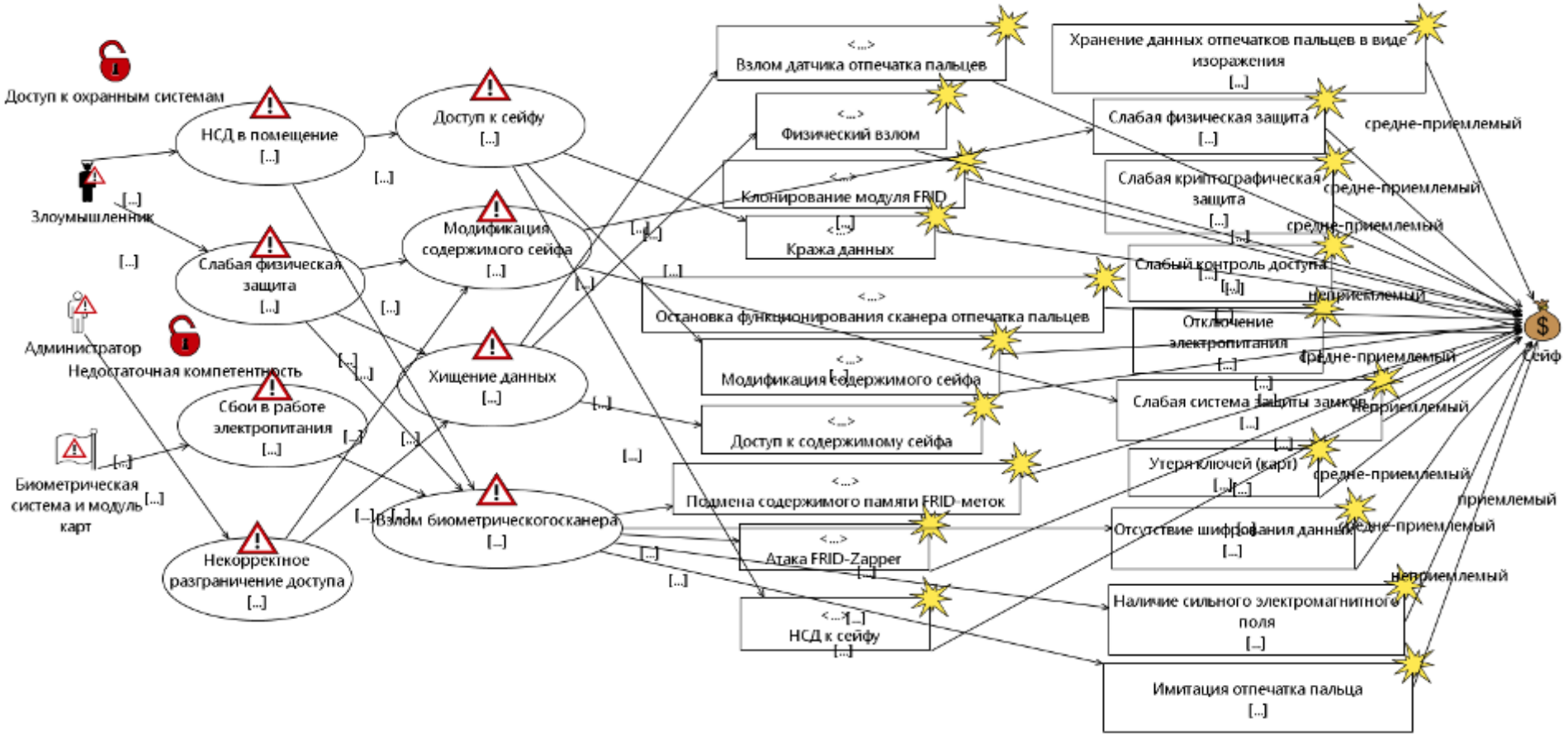


Рисунок 3.5 - Диаграмма угроз после добавления противодействий

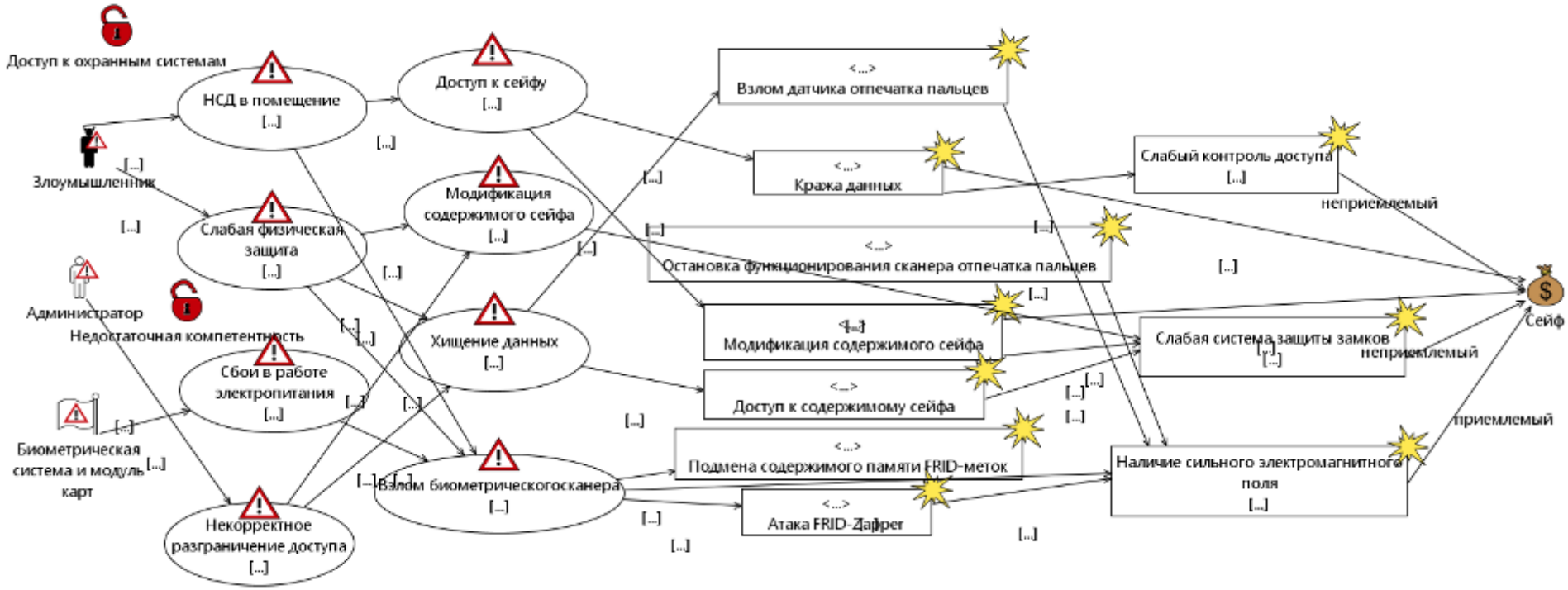


Рисунок 3.6 - Диаграмма неприемлемых рисков

Вывод по разделу: был произведен расчет уровня рисков по формуле (3.1). Также были исследованы риски по методологии Coras и проиллюстрированы в программном обеспечении Coras. Для каждой диаграммы было произведено описание схемы.

4 Безопасность жизнедеятельности

4.1 Анализ потенциально опасных и вредных факторов в офисе, воздействующих на персонал

Основным фактором, влияющим на производительность труда людей, работающих с персональными электронно-вычислительными машинами (ПЭВМ) и видео дисплейными терминалами (ВДТ), являются комфортные и безопасные условия труда. Условия труда пользователя, работающего с персональным компьютером (ПК), определяются:

- особенностями организации рабочего места;
- 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.

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

- повышенная температура поверхностей персонального компьютера;
- повышенная или пониженная температура воздуха рабочей зоны;
- выделение в воздух рабочей зоны ряда химических веществ;
- повышенная или пониженная влажность воздуха;
- повышенный или пониженный уровень отрицательных и положительных аэроионов;
- повышенное значение напряжения в электрической цепи, замыкание;
- повышенный уровень статического электричества;
- повышенный уровень электромагнитных излучений;
- повышенная напряженность электрического поля;
- отсутствие или недостаток естественного света;
- недостаточная искусственная освещенность рабочей зоны;
- повышенная яркость света;
- повышенная контрастность;
- зрительное напряжение;
- монотонность трудового процесса;
- нервно-эмоциональные перегрузки [12].

Работа на персональном компьютере сопровождается постоянным и значительным напряжением функций зрительного анализатора. Одной из основных особенностей является иной принцип чтения информации, чем при обычном чтении. При обычном чтении текст на бумаге, расположенный горизонтально на столе, считывается работником с наклоненной головой при падении светового потока на текст. При работе на персональном компьютере оператор считывает текст, почти не наклоняя голову, глаза смотрят прямо или почти прямо вперед, текст (источник — люминесцирующее вещество экрана) формируется по другую сторону экрана, поэтому пользователь не считывает

отраженный текст, а смотрит непосредственно на источник света, что вынуждает глаза и орган зрения в целом работать в несвойственном ему стрессовом режиме длительное время.

Расстройство органов зрения резко увеличивается при работе более четырех часов в день. Всемирная организация здравоохранения (ВОЗ) ввела понятие “компьютерный зрительный синдром” (КЗС), типовыми симптомами которого являются жжение в глазах, покраснение век, чувство инородного тела или песка под веками, боли в области глазниц и лба, затуманивание зрения, замедленная фокусировка с ближних объектов на дальние [8].

Нервно-эмоциональное напряжение при работе на ПК возникает вследствие дефицита времени, большого объема и плотности информации, особенностей диалогового режима общения человека и ПК, ответственности за безошибочность информации. Продолжительная работа на дисплее, особенно в диалоговом режиме, может привести к нервно-эмоциональному перенапряжению, нарушению сна, ухудшению состояния, снижению концентрации внимания и работоспособности, хронической головной боли, повышенной возбудимости нервной системы, депрессии.

Кроме того, при повышенных нервно-психических нагрузках в сочетании с другими вредными факторами происходит “выброс” из организма витаминов и минеральных веществ. При работе в условиях повышенных нервно-эмоциональных и физических нагрузок гиповитаминоз, недостаток микроэлементов и минеральных веществ (особенно железа, магния, селена) ускоряет и обостряет восприимчивость к воздействию вредных факторов окружающей и производственной среды, нарушает обмен веществ, ведет к изнашиванию и старению организма. Поэтому при постоянной работе на ПК для повышения работоспособности и сохранения здоровья к мерам безопасности относится защита организма с помощью витаминно-минеральных комплексов, которые рекомендуется применять всем, даже практически здоровым пользователям ПК [8].

Повышенные статические и динамические нагрузки у пользователей ПК приводят к жалобам на боли в спине, шейном отделе позвоночника и руках. Из всех недомоганий, обусловленных работой на компьютерах, чаще встречаются те, которые связаны с использованием клавиатуры. В период выполнения операций ввода данных количество мелких стереотипных движений кистей и пальцев рук за смену может превысить 60 тыс., что в соответствии с гигиенической классификацией труда относится к категории вредных и опасных. Поскольку каждое нажатие на клавишу сопряжено с сокращением мышц, сухожилия непрерывно скользят вдоль костей и соприкасаются с тканями, вследствие чего могут развиться болезненные воспалительные процессы. Воспалительные процессы тканей сухожилий получили общее название “травма повторяющихся нагрузок”.

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 [8].

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 аэронов и пониженное содержание отрицательных аэронов в воздухе рабочей зоны; неравномерность распределения яркости в поле зрения; повышенная яркость светового изображения; повышенное значение напряжения в электрической цепи, замыкание которой может произойти через тело человека.

Химически вредные и опасные факторы. Химические вредные и опасные факторы, следующие: повышенное содержание в воздухе рабочей зоны двуокиси углерода, озона, аммиака, фенола и формальдегида.

Психофизические вредные и опасные факторы. Психофизиологические 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 [8].

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.

К профессиональным заболеваниям, связанным с ТПН, относятся:

- тендовагинит, воспаление сухожилий кисти, запястья, плеча;
- тендосиновит, воспаление синовиальной оболочки сухожильного основания кисти и запястья;
- 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. 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.

Воздействие электромагнитных полей (ЭМП) на организм человека.

Степень вредного воздействия ЭМП на человека зависит от напряженности электрического и магнитного полей, интенсивности потока энергии, продолжительности действия, длины волны источника, а также от индивидуальных особенностей организма.

Систематическое воздействие на человека ЭМП низкой частоты может вызвать изменения деятельности нервной и сердечно-сосудистой систем, а также некоторые изменения в составе крови, особенно выраженные при высокой их напряженности [9].

Биологическое действие таких полей более высоких частот связано в основном с их тепловым и аритмическим эффектом. Поля ВЧ и УВЧ создают в тканях высокочастотные ионные потоки, нагревающие их. Такое явление наблюдается также при очень интенсивном облучении электромагнитными волнами СВЧ. Тепловое действие характеризуется общим повышением температуры тела или местным нагревом тканей, что особенно опасно для органов со слабой терморегуляцией (мозг, глаза, почки). Облучение глаз сантиметровыми волнами (от 1 до 20 см) может повысить температуру в задней части хрусталика, что вызывает его помутнение (катаракту).

Постоянное воздействие ЭМП умеренной интенсивности влияет на биофизические процессы в клетках и тканях, поражает центральную нервную и сердечно-сосудистую системы. Человек чувствует себя уставшим, появляются необоснованная раздражительность, периодические головные боли, нарушается сон. Нередки жалобы на потливость, ослабление памяти, боли в области сердца, одышку. Функциональные изменения, вызванные биологическим воздействием электромагнитных полей, обратимы. Если исключить воздействие излучения, болезненные явления исчезают [9].

К работе на высокочастотных установках допускаются лица не моложе 18 лет. Не реже одного раза в год они должны проходить медицинский осмотр. Люди с органическими заболеваниями центральной нервной системы, заболеваниями нервно-психической формы и эндокринно-вегетативными сердечно-сосудистыми заболеваниями, а также заболеваниями легких к работе на таких установках не допускаются.

В зависимости от диапазона частот в основу гигиенического нормирования электромагнитных излучений положены разные принципы.

Критерием безопасности для человека, находящегося в электрическом поле промышленной частоты, является напряженность этого поля, а гигиенические нормы установлены ГОСТ 12.1.002-84ГОСТ 12.1.002-84 ССБТ. «Электрические поля промышленной частоты. Допустимые уровни напряженности и требования к проведению контроля на рабочих местах». Нормируется время пребывания человека в электрическом поле в зависимости от напряженности (табл. 4.1) [9].

Таблица 4.1 - Допустимая напряженность и продолжительность пребывания человека в электрическом поле без средств защиты [11]

Напряженность электрического поля, кВ/м	Время пребывания человека в электрическом поле в течение одних суток, мин
Менее 5	Без ограничений
От 5 до 10	Не более 180
Свыше 10 до 15	Не более 90
Свыше 15 до 20	Не более 10
Свыше 20 до 25	Не более 5

Эти нормы обеспечивают безопасность при условии, что в остальное время суток человек не подвергается воздействию ЭП напряженностью больше 5 кВ/м, а также исключена возможность воздействия на организм человека электрических разрядов.

В диапазоне частот 60 КГц - 300 МГц нормируются напряженности магнитной и электрической составляющих электромагнитного поля. Они установлены ГОСТ 12.1.006-84 «ССБТ. Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля». Интенсивность электромагнитного поля на рабочих местах и в местах возможного нахождения персонала, связанного с воздействием электромагнитного поля, не должны превышать следующих значений:

по электрической составляющей (В/м):

- 50 — для частот 60 КГц — 3 МГц;
- 20 — для частот 3 МГц — 30 МГц;
- 10 — для частот 30 КГц — 50 МГц;
- 5 — для частот 50 КГц — 300 МГц;

по магнитной составляющей (А/м):

- 5 — для частот 60 КГц — 1,5 МГц;
- 0,3 — для частот 30 МГц — 50 МГц.

Интенсивность электромагнитного поля в диапазоне частот 300 МГц - 300 ГГц на рабочих местах и в местах возможного нахождения персонала, связанного с воздействием ЭМП, оценивается плотностью потока энергии. В этом случае предельно допустимую плотность потока энергии ЭМП устанавливают, исходя из допустимого значения энергетической нагрузки на организм человека и продолжительности пребывания его в зоне облучения.

Однако во всех случаях она не должна превышать 10 Вт/м^2, а при наличии рентгеновского излучения или высокой температуры воздуха в рабочих помещениях (выше 28 ^{0}С) - 1 Вт/м^2 [9].

Соблюдение предельно допустимых значений ЭМП контролируют измерением напряженности и плотности потока энергии ЭМП на рабочих местах и в местах возможного нахождения персонала, подвергающегося в условиях производства воздействию ЭМП.

Контроль следует проводить периодически не реже одного раза в год, а также при приеме в эксплуатацию новых и при внесении изменений в конструкцию действующих установок, после ремонта, перестройки схемы и при организации новых рабочих мест. Измерения делают при наибольшей используемой мощности источника ЭМП.

Воздействие лазерного излучения на организм человека.

В зависимости от технических параметров конструкции лазера и условий его эксплуатации, на работающих могут воздействовать различные опасные и вредные факторы. Основную опасность представляют прямое, рассеянное, зеркально и диффузно отраженные лазерные излучения.

При эксплуатации лазеров возникает опасность не только воздействия лазерного излучения, но и ряда сопутствующих производственных факторов: повышенное напряжение в цепях управления и источниках электропитания лазеров; повышенные запыленность и загазованность воздуха рабочей зоны продуктами взаимодействия лазерного излучения с материалом мишени и воздухом (озон, окислы азота и др.); ультрафиолетовое излучение импульсных ламп накачки или кварцевых газоразрядных трубок в рабочей зоне; свет высокой яркости от ламп накачки и зоны взаимодействия лазерного излучения с материалом мишени; повышенный уровень ионизирующих и электромагнитных излучений ВЧ- и СВЧ-диапазонов от генераторов накачки, а также инфракрасное излучение и тепловыделение в рабочей зоне.

По степени опасности генерируемого излучения лазеры подразделяются на четыре класса:

- 1 класс - выходное излучение не представляет опасности для глаз и кожи;

- 2 класс - выходное излучение представляет опасность при облучении глаз прямым или зеркально отраженным излучением;

- 3 класс - выходное излучение представляет опасность при облучении глаз прямым, зеркально отраженным, а также диффузно отраженным излучением на расстоянии 10 см от диффузно отражающей поверхности и (или) при облучении кожи прямым и зеркально отраженным излучением;

- 4 класс - выходное излучение представляет опасность при облучении кожи диффузно отраженным излучением на расстоянии 10 см от диффузно отражающей поверхности.

Лазерное излучение воздействует на весь организм человека. Биологические эффекты, возникающие при этом, делятся на две группы: первичные эффекты - органические изменения, возникающие

непосредственно в облучаемых тканях; вторичные эффекты - неспецифические изменения, возникающие в организме как реакция на облучение [10].

При взаимодействии лазерного излучения с биологическими тканями человека возможны ожоги. Наиболее опасно это излучение для глаз, так как роговица и хрусталик фокусируют излучение на сетчатке и концентрируют его. В зависимости от падающей энергии лазерное излучение может вызвать временное ослепление или необратимую потерю зрения из-за сильного ожога сетчатки.

При большой интенсивности излучения возможно поражение не только глаз, но кожи, внутренних органов и мозга.

Предельно допустимые уровни лазерного облучения установлены ГОСТ 12.1.040-83ГОСТ 12.1.040-83 ССБТ. «Лазерная безопасность. Общие положения». «ССБТ. Лазерная безопасность. Общие положения». Предельно допустимые уровни выражаются в энергетических экспозициях.

Предельно допустимые уровни облучения моноимпульсного и непрерывного лазерного излучения выбирают из расчета наименьшей энергетической экспозиции, не вызывающей первичных и вторичных биологических эффектов. При этом следует учитывать длину волны излучения и длительность его воздействия.

Так, для непрерывного лазерного излучения с длиной волны λ = 0,308 мкм при облучении глаз и кожи в течение рабочего дня предельно допустимый уровень будет $H_{пду} = 10^{-4}$ ДЖ/см^2 [10].

При одновременном воздействии лазерного излучения с различными параметрами на один и тот же участок тела возможно суммирование биологических эффектов.

Таблица 4.2 - Опасные и вредные производственные факторы [10]

Опасные и вредные производственные факторы	Класс лазера			
	1	2	3	4
Лазерное излучение:				
прямое, зеркальное, отраженное		+	+	+
прямое, зеркальное, отраженное	-	-	+	+
Повышенная напряженность электрического поля	-(+)	+	+	+
Повышенная запыленность и загазованность воздуха рабочей зоны	-	-	-(+)	+
Повышенный уровень ультрафиолетовой радиации	-	-	-(+)	+
Повышенная яркость света	-	-	-(+)	+

Продолжение таблицы 4.2

Повышенные уровни шума и вибрации	-	-	-(+)	+
Повышенный уровень ионизирующих излучений	-	-	-	+
Повышенный уровень электромагнитных излучений ВЧ- и СВЧ-диапазонов	-	-	-	-(+)
Повышенный уровень инфракрасной радиации	-	-	-(+)	+
Повышенная температура поверхностей оборудования	-	-	-(+)	+
Химические опасные и вредные производственные факторы	При работе с токсичными веществами			
П р и м е ч а н и я 1 «+» означает имеют место всегда. 2 «-» - опасные и вредные производственные факторы отсутствуют. 3 «-(+)» - наличие вредных факторов зависит от конкретных технических характеристик, лазера и условий его эксплуатации.				

Ультрафиолетовое излучение. УФ-излучение необходимо для нормальной деятельности человека. При длительном его отсутствии в организме развиваются неблагоприятные явления, получившие название «светового голодания» или «ультрафиолетовой недостаточности». В то же время длительное воздействие больших доз УФ-излучения может привести к серьезным поражениям глаз и кожи. Острые поражения глаз обычно проявляются в виде кератитов.

Для профилактики неблагоприятных последствий, используют как солнечное излучение (инсоляция помещений, устройство соляриев), так и применение искусственных источников УФ-излучения. Искусственное облучение проводится в соответствии с действующими «Рекомендациями по профилактике ультрафиолетовой недостаточности».

В зависимости от степени УФ-дефицита и контингента населения рекомендуются дозы в пределах 0,125-0,75 эритемной дозы (10-60 $_{(мэр*ч)/м^2}$).

Для защиты от избытка УФ-излучения применяют противосолнечные экраны, жалюзи, оконные стекла со специальным покрытием. Для защиты глаз в производственных условиях используют очки с защитными стеклами. При устройстве помещений необходимо учитывать, что отражающая способность различных отделочных материалов для УФ-излучения иная, чем для видимого света. Хорошо отражают УФ-излучения полированный

алюминий и меловая побелка, в то время как оксиды цинка и титана на масляной основе - плохо.

4.2 Расчетный раздел. Расчет естественного освещения и расчет уровня шума на рабочем месте

Расчет естественного освещения для помещения со следующими характеристиками: длина - 5,83 м, ширина - 3,9 м, высота от уровня условной рабочей поверхности до верха окна - 1,5 м, стены окрашены в белый цвет, пол - в коричневый цвет, на потолке побелка. Оконный проем имеет ширину 2,6м, высоту 1,5м.

Предварительный расчет площади световых проемов при боковом освещении проводится по следующей формуле [7]:

$$S_o = 0{,}01 \cdot \frac{S \cdot e_н \cdot \eta_o \cdot K_з \cdot K_{зд}}{\tau_o \cdot r_1} \quad (4.1)$$

где S_0 - площадь окон, м^2;

S - площадь пола помещения, м^2;

$e_н$ - нормированное значение коэффициента естественной освещенности (КЕО), % (определяется из СНиП 23.05-95 - естественное освещение должно осуществляться через светопроемы, ориентированные преимущественно на север и северо-восток и обеспечивать коэффициент естественной освещенности (КЕО) не ниже 1,2%, для зрительной работы высокой точности, когда наименьший размер объекта различения равен 0.3 - 0.5 мм;

η_0 - световая характеристика окна, %;

$К_з$ - коэффициент запаса, %;

$К_{зд}$ - коэффициент, учитывающий затемнение окон противостоящими зданиями, %;

τ_0 - общий коэффициент светопропускания, в данном случае зависит от коэффициента светопропускания материала и коэффициента, учитывающего потери света в переплетах светопроема, %;

r_1- коэффициент, учитывающий повышение КЕО за счет отражения света от поверхностей помещения, зависит от ряда параметров, в том числе от средневзвешенного коэффициента отражения Rср, который рассчитывается по формуле [7]:

$$R_{ср} = \frac{R_{ст} \cdot S_{ст} + R_{пт} \cdot S_{пт} + R_{пл} \cdot S}{S_{ст} + S_{пт} + S} \quad (4.2)$$

где $R_{ст}$, $R_{пт}$, $R_{пл}$ - коэффициенты отражения от стен, потолка и пола, %;

$S_{ст}$, $S_{пт}$, S - площади стен, потолка и пола, м^2.

Учитывая характеристики помещения, значения коэффициентов примем равными: 0,53; 0,5; 0,23.

Рассчитаем средневзвешенный коэффициент отражения $R_{ср}$ по формуле (4.2):

$$R_{ср} = \frac{0.53 * 28.18 + 0.5 * 22.7 + 0.23 * 22.7}{22.7 + 28.18 + 22.7} = 0{,}43 \text{ м}^2$$

Определим значение требуемой площади светового проема:

$$S_0 = 0.01 * \frac{22.7 * 1.2 * 15 * 1.3 * 1}{0.52 * 1.37} = 7.45 \text{ м}^2$$

Площадь оконных проемов в помещении должна быть не менее 7,45м2, тогда как площадь окна составляет 3,9м2. Расчет показывает, что естественного освещения будет недостаточно, поэтому, для постоянной работы в течение всего рабочего дня, во все времена года, используют искусственное освещение, которое повышает уровень освещенности до допустимой нормы.

Расчет уровня шума на рабочем месте.

Шум ухудшает условия труда, оказывая вредное действие на организм человека. В табл. 4.1 указаны предельные уровни звука в зависимости от категории тяжести и напряженности труда, являющиеся безопасными в отношении сохранения здоровья и работоспособности.

Таблица 4.3 - Предельные уровни звука, дБ, на рабочих местах

Категории напряженности труда	Категория тяжести труда		
I. Легкая	II. Средняя	III. Тяжелая	IV. Очень тяжелая
I. Мало напряженный	80	80	75
II. Умеренно напряженный	70	70	65
III. Напряженный	60	60	-
IV. Очень напряженный	50	50	-

Уровень шума на рабочем месте делопроизводителя-оператора ЭВМ не должен превышать 50дБА. Источниками шума на рабочем месте являются компьютер, оргтехника и кондиционер. Рассчитаем уровень шума на рабочем месте от всех возможных источников. Уровень шума, возникающий от нескольких некогерентных источников, работающих одновременно, подсчитывается на основании принципа энергетического суммирования излучений отдельных источников i=n, i=1:

$$L = 10 \lg 100{,}1Li \quad (4.3)$$

где Li - уровень звукового давления i-го источника шума; n - количество источников шума [13].

Для расчета возьмем стандартные табличные значения уровней шума, создаваемых всеми видами оборудования на рабочем месте. Уровни звукового давления источников шума, действующих на оператора на его рабочем месте, представлены в табл. 4.2.

Таблица 4.4 - Уровни звукового давления различных источников

Источник шума	Уровень шума, дБ
Жесткий диск	40
Вентилятор	45
Монитор	17
Клавиатура	10
Принтер	44
Сканер	43
Кондиционер	40

Рабочее место оператора оснащено следующим оборудованием: винчестер в системном блоке, вентилятор(ы) систем охлаждения ПК, монитор, клавиатура, принтер и сканер. Подставив значения уровня звукового давления для каждого вида оборудования в формулу, получим следующие данные расчета:

L=10*lg(1000+31622,78+50,12+10+25118,86+19952,62+10000)=
=10*lg(96754,38) = 49,85671 Дб

Таким образом, уровень шума на рабочем месте составляет 49,86Дб, что не превышает допустимого значения.

Заключение

Были проведены исследования в сфере методологии реализации защиты на базе многофакторной аутентификации с практическим применения методов исследования. В результате данной дипломной работы реализован сейф с двойной аутентификацией - биометрический замок и смарт карта. Также было разработано пользовательское приложение для управления правами доступа к дверцам сейфа. Дверцы сейфа управляются замком-защелкой, которые подключены к запрограммированной плате Arduino.

В разделе расчета рисков были рассмотрены следующие риски: взлом датчика отпечатка пальцев, физический взлом, клонирование модуля RFID, кража данных, остановка функционирования сканера отпечатка пальцев, модификация содержимого сейфа, доступ к содержимому сейфа, подмена содержимого памяти RFID-меток, атака RFID-Zapper (уничтожение метки RFID), НСД к сейфу и др. В роли актива был рассмотрен сейф как сложный актив, состоящий из восьми простых активов. Был также произведен расчет уровня рисков до и после принятия мер по обработке рисков. Также были исследованы риски по методологии Coras и проиллюстрированы в программном обеспечении Coras. Для каждой диаграммы было произведено описание схемы.

В разделе безопасности жизнедеятельности был описан анализ потенциально опасных и вредных факторов в офисе, воздействующих на персонал. Произвела анализ наиболее характерных опасных и вредных факторов для работающего в офисе (электромагнитное излучение от компьютера, влияние компьютера на работающего — сидячая длительная поза и др., шум, запыленность, хим. вещества — озон от лазерного принтера, требования по микроклимату, пожаробезопасность, электробезопасность), описала их негативное действие на организм человека и привести допустимые параметры в соответствии с нормами. Также произвела два расчетных вопроса, обеспечивающие комфортные условия труда: расчет шума на рабочем месте, расчет освещенности (офиса). В результате расчетов выявлено, что площадь оконных проемов в помещении должна быть не менее 7,45м2, тогда как площадь окна составляет 3,9м2. Расчет показывает, что естественного освещения будет недостаточно, поэтому, для постоянной работы в течение всего рабочего дня, во все времена года, используют искусственное освещение, которое повышает уровень освещенности до допустимой нормы. В результате второго расчета выявлено, что уровень шума на рабочем месте составляет 49,86Дб, что не превышает допустимого значения.

Список литературы

1. В.В. Вихман, А.А. Якименко Биометрические системы контроля и управления доступом в задачах защиты информации: учебно-метод. Пособие /. – Новосибирск: НГТУ, 2016. – 54 с.

2. Антти Суомалайнен Биометрическая защита: обзор технологии – М.: ДМК Пресс, 2019. – 104 с.

3. Р. М. Болл, Дж. Х. Коннел, Ш. Панканти, Н. К. Ратха, Э. У. Сеньор Руководство по биометрии – М.: Техносфера, 2007. — 370 с.

4. Биометрические системы BioLink // Идентификация по отпечаткам пальцев / URL: https://www.biolink.ru/technology/fingerprint.php

5. Инструкция по использованию биометрического сканера ZFM-60 / URL: http://ba3ar.kz/documents/lettore_impronte_zfm60.pdf

6. Биометрическая идентификация // Технологии биометрической идентификации / URL: http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html

7. М. И. Краснов, Я. Я. Киреев, Г. А, Тищенко, М. Я. Марусова Пособие по расчету и проектированию естественного и совмещенного освещения (к СНиП II-4-79) – М.: 1985г.

8. http://www.grandars.ru/shkola/bezopasnost-zhiznedeyatelnosti/vrednye-faktory-pri-rabote-na-pk.html

9. http://www.hi-edu.ru/e-books/xbook908/01/part-009.htm

10. ГОСТ 12.1.040-83ГОСТ 12.1.040-83 ССБТ. «Лазерная безопасность. Общие положения». «ССБТ. Лазерная безопасность. Общие положения».

11. ГОСТ 12.1.002-84 Система стандартов безопасности труда (ССБТ). Электрические поля промышленной частоты. Допустимые уровни напряженности и требования к проведению контроля на рабочих местах.

12. ГОСТ 12.0.003-2015 Система стандартов безопасности труда (ССБТ). Опасные и вредные производственные факторы.

13. ГОСТ 30530-97 Методы расчета предельно допустимых шумовых характеристик стационарных машин.

Приложение А

Листинг программы на Delphi

```
unit Unit1;
interface
uses
  Winapi.Windows, Winapi.Messages, System.SysUtils, System.Variants, System.Classes,
Vcl.Graphics,
  Vcl.Controls, Vcl.Forms, Vcl.Dialogs, Vcl.StdCtrls, Vcl.ComCtrls, CPDrv,
  Vcl.ExtCtrls, Data.DB, Vcl.DBCtrls, Vcl.Grids, Vcl.DBGrids, Datasnap.DBClient,
  Vcl.Mask, MMSYSTEM;
type
  TForm1 = class(TForm)
    CommPortDriver1: TCommPortDriver;
    Timer1: TTimer;
    Timer2: TTimer;
    Label2: TLabel;
    Edit1: TEdit;
    Label3: TLabel;
    Edit2: TEdit;
    Button1: TButton;
    Button2: TButton;
    GroupBox5: TGroupBox;
    CheckBox1: TCheckBox;
    Label1: TLabel;
    Memo2: TMemo;
    Edit12: TEdit;
    Button3: TButton;
    Memo1: TMemo;
    Label4: TLabel;
    ClientDataSet1: TClientDataSet;
    DataSource1: TDataSource;
    DBNavigator1: TDBNavigator;
    Label5: TLabel;
    Edit3: TEdit;
    Timer3: TTimer;
    PageControl1: TPageControl;
    TabSheet1: TTabSheet;
    Button4: TButton;
    Button11: TButton;
    Button10: TButton;
    Bevel1: TBevel;
    DBEdit2: TDBEdit;
    Label8: TLabel;
    DBEdit1: TDBEdit;
    Label6: TLabel;
    Label7: TLabel;
    DBComboBox1: TDBComboBox;
    Button8: TButton;
```

```
    Button9: TButton;
    TabSheet2: TTabSheet;
    Edit4: TEdit;
    Button5: TButton;
    Label9: TLabel;
    Button12: TButton;
    Label10: TLabel;
    Bevel2: TBevel;
    Button6: TButton;
    Button7: TButton;
    DBGrid1: TDBGrid;
    procedure Button1Click(Sender: TObject);
    procedure Timer1Timer(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure Timer2Timer(Sender: TObject);
    procedure Button3Click(Sender: TObject);
    procedure CommPortDriver1ReceiveData(Sender: TObject; DataPtr: Pointer;
      DataSize: Cardinal);
    procedure Button4Click(Sender: TObject);
    procedure Button10Click(Sender: TObject);
    procedure Button8Click(Sender: TObject);
    procedure Button9Click(Sender: TObject);
    procedure Button11Click(Sender: TObject);
    procedure FormShow(Sender: TObject);
    procedure Label9DblClick(Sender: TObject);
    procedure Timer3Timer(Sender: TObject);
    procedure Button5Click(Sender: TObject);
    procedure Button12Click(Sender: TObject);
    procedure DBComboBox1KeyPress(Sender: TObject; var Key: Char);
    procedure FormClose(Sender: TObject; var Action: TCloseAction);
    procedure Edit4KeyPress(Sender: TObject; var Key: Char);
    procedure Button7Click(Sender: TObject);
    procedure Button6Click(Sender: TObject);
    procedure Memo2Change(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }
  end;
var
  Form1: TForm1;
implementation
{$R *.dfm}
procedure TForm1.Button10Click(Sender: TObject);
begin
Button4.Visible  := false;
Button11.Visible := false;
Button10.Visible := false;
DBGrid1.Visible  := false;
DBEdit2.Color := clWhite;
DBNavigator1.BtnClick(nbEdit);
```

```
end;
procedure TForm1.Button11Click(Sender: TObject);
begin
DBNavigator1.BtnClick(nbDelete);
end;
procedure TForm1.Button12Click(Sender: TObject);
var
Str: string;
Ach: PWideChar;
begin
  Edit4.Color := clWhite;
  if Edit3.Text = 'Подключено'
  then Label10.Caption := 'Идет передача данных...'
  else begin
  Str := ExtractFilePath(Application.ExeName) + 'ringout.wav';
  Ach := PWideChar(Str); sndPlaySound(Ach, 1);
  Memo2.Lines.Add(TimeToStr(Time)+' - Подключите сейф к компьютеру!');
  Label10.Caption := 'Подключите сейф к компьютеру!';
  end;
  if Edit4.GetTextLen > 0
  then begin
    Edit12.Text := 'D';
    Button3.Click;
  end else begin
    Edit4.Color := $00CECEFF;
    Str := ExtractFilePath(Application.ExeName) + 'ringout.wav';
    Ach := PWideChar(Str); sndPlaySound(Ach, 1);
    Memo2.Lines.Add(TimeToStr(Time)+' - Введите удаляемый ID номер!');
    Label10.Caption := 'Введите удаляемый ID номер!';
  end;
end;
procedure TForm1.Button1Click(Sender: TObject);
begin
  Edit3.Text := 'Отключено';
  Timer2.Enabled := false;
  Memo2.Lines.Add(TimeToStr(Time)+' - Подключение к сейфу');
  Edit1.Text := '0';
  if CheckBox1.Checked = true
  then Timer1.Enabled := true
  else begin
    CommPortDriver1.BaudRateValue := 9600;
    CommPortDriver1.PortName := Edit2.Text;
    CommPortDriver1.DataBits := db8BITS;
    CommPortDriver1.PollingDelay := 50; //время ожидания
    CommPortDriver1.Connect;
    if CommPortDriver1.Connect = true
    then begin
      Button1.Enabled := false;
      Button2.Enabled := true;
      Timer2.Enabled := true;
```

```
    Memo2.Lines.Add(TimeToStr(Time)+' - Сейф успешно подключен');
    Edit3.Text := 'Подключено';
   end else
    Memo2.Lines.Add(TimeToStr(Time)+' - ОШИБКА! сейф не найден!');
  end;
end;
procedure TForm1.Button2Click(Sender: TObject);
begin
  Timer1.Enabled := false;
  CommPortDriver1.Disconnect;
  Memo2.Lines.Add(TimeToStr(Time)+' - Отключено');
  Button1.Enabled := true;
  Button2.Enabled := false;
  Timer2.Enabled := false;
  Edit3.Text := 'Отключено';
end;
procedure TForm1.Button3Click(Sender: TObject);
begin
CommPortDriver1.SendString(Edit12.Text);
CommPortDriver1.SendString('');
Edit12.Clear;
end;
procedure TForm1.Button4Click(Sender: TObject);
begin
Button4.Visible  := false;
Button11.Visible := false;
Button10.Visible := false;
DBGrid1.Visible  := false;
DBEdit2.Color := clWhite;
DBNavigator1.BtnClick(nbInsert);
DBComboBox1.Text := 'A';
end;
procedure TForm1.Button5Click(Sender: TObject);
var
Str: string;
Ach: PWideChar;
begin
  Edit4.Color := clWhite;
  if Edit3.Text = 'Подключено'
  then Label10.Caption := 'Идет передача данных...'
  else begin
  Str := ExtractFilePath(Application.ExeName) + 'ringout.wav';
  Ach := PWideChar(Str); sndPlaySound(Ach, 1);
  Memo2.Lines.Add(TimeToStr(Time)+' - Подключите сейф к компьютеру!');
  Label10.Caption := 'Подключите сейф к компьютеру!';
  end;
  if Edit4.GetTextLen > 0
  then begin
    Edit12.Text := 'I';
    Button3.Click;
```

```
  end else begin
    Edit4.Color := $00CECEFF;
    Str := ExtractFilePath(Application.ExeName) + 'ringout.wav';
    Ach := PWideChar(Str); sndPlaySound(Ach, 1);
    Memo2.Lines.Add(TimeToStr(Time)+' - Введите новый ID номер!');
    Label10.Caption := 'Введите новый ID номер!';
  end;
end;
procedure TForm1.Button6Click(Sender: TObject);
var
  Str: string;
  Ach: PWideChar;
begin
  Str := ExtractFilePath(Application.ExeName) + 'ringout.wav';
  Ach := PWideChar(Str); sndPlaySound(Ach, 1);
  Memo2.Lines.Add('-----------------------------------------');
  Memo2.Lines.Add('Программа "Altyn Safe 2020" БД');
  Memo2.Lines.Add('Адиль Алтынай, группа Сиб-16-2');
  Memo2.Lines.Add('НАО "АУЭС" г. Алматы, 2020 год');
  Memo2.Lines.Add('-----------------------------------------');
end;
procedure TForm1.Button7Click(Sender: TObject);
begin
Button2.Click; Application.Terminate;
end;
procedure TForm1.Button8Click(Sender: TObject);
begin
  Button4.Visible  := true;
  Button11.Visible := true;
  Button10.Visible := true;
  DBNavigator1.BtnClick(nbPost);
  Sleep(500); ClientDataSet1.Active := false;
  Sleep(500); ClientDataSet1.Active := true;
  DBGrid1.Visible  := true;
end;
procedure TForm1.Button9Click(Sender: TObject);
begin
Button4.Visible  := true;
Button11.Visible := true;
Button10.Visible := true;
DBGrid1.Visible  := true;
DBNavigator1.BtnClick(nbCancel);
end;
procedure TForm1.CommPortDriver1ReceiveData(Sender: TObject;
DataPtr: Pointer; DataSize: Cardinal);
var
  i: integer;
  s: string;
begin
  s := '';
  for i := 0 to DataSize + 1 do s := s + (PAnsiChar(DataPtr)[i]);
```

```
  begin
    Memo1.Lines.Add(s);
  end;
end;
procedure TForm1.DBComboBox1KeyPress(Sender: TObject; var Key: Char);
begin
  Key:=#0;
end;
procedure TForm1.Edit4KeyPress(Sender: TObject; var Key: Char);
begin
if not (Key in ['0'..'9', #8]) then Key:=#0;
end;
procedure TForm1.FormClose(Sender: TObject; var Action: TCloseAction);
begin
Button2.Click;
end;
procedure TForm1.FormShow(Sender: TObject);
var
Dir: string;
begin
 Dir := ExtractFilePath(Application.ExeName) + 'my_data.cds';
 ClientDataSet1.FileName := Dir;
 ClientDataSet1.Active := true;
 DBGrid1.Columns[0].Width := 142;
 TabSheet1.Show;
end;
procedure TForm1.Label9DblClick(Sender: TObject);
begin
  Edit12.Text := 'L';
  Button3.Click;
end;
procedure TForm1.Memo2Change(Sender: TObject);
begin
end;
procedure TForm1.Timer1Timer(Sender: TObject);
begin
  if Edit1.Text = '20'
  then begin
    Edit1.Text := '0';
    Memo2.Lines.Add(TimeToStr(Time)+' - ОШИБКА! сейф не найден!');
    Timer1.Enabled := false;
  end else begin
    if Button1.Enabled = true
    then begin
      Edit2.Text := '\\.\Com'+Edit1.Text; //порт
      CommPortDriver1.BaudRateValue := 9600;
      CommPortDriver1.PortName := Edit2.Text;
      CommPortDriver1.DataBits := db8BITS;
      CommPortDriver1.PollingDelay := 50; // время ожидания
      CommPortDriver1.Connect;
      if CommPortDriver1.Connect = true
```

```
        then begin
          Button1.Enabled := false;
          Button2.Enabled := true;
          Timer2.Enabled := true;
          Timer1.Enabled := false;
          Memo2.Lines.Add(TimeToStr(Time)+' - Сейф успешно подключен');
          Edit3.Text := 'Подключено';
        end;
        Edit1.Text := IntToStr(StrToInt(Edit1.Text)+1);
        end else begin
          Edit1.Text := '0';
          Timer1.Enabled := false;
        end;
    end;
  end;
  procedure TForm1.Timer2Timer(Sender: TObject);
  var
    Find: String;
    i: Integer;
    Str: string;
    Ach: PWideChar;
  begin
    find := 'Found sensor';
    for i := 0 to Memo1.Lines.Count-1 do
    If Pos(FIND, Memo1.Lines.Text)<> 0
    then begin
      Memo2.Lines.Add(TimeToStr(Time)+' - Биометрический сканер подключен!');
      Memo1.Lines.Clear;
      Sleep(2000);
      Edit12.Text := 'O';
      Button3.Click;
    end;
    find := 'Sensor error';
    for i := 0 to Memo1.Lines.Count-1 do
    If Pos(FIND, Memo1.Lines.Text)<> 0
    then begin
      Memo2.Lines.Add(TimeToStr(Time)+' - ОШИБКА! Биометрический сканер - не
обнаружен!');
      Memo1.Lines.Clear;
    end;
    find := 'Enter ID';
    for i := 0 to Memo1.Lines.Count-1 do
    If Pos(FIND, Memo1.Lines.Text)<> 0
    then begin
      Edit12.Text := Edit4.Text;
      Button3.Click;
      Memo1.Lines.Clear;
    end;
    find := 'put your finger';
    for i := 0 to Memo1.Lines.Count-1 do
    If Pos(FIND, Memo1.Lines.Text)<> 0
```

```
then begin
  Memo2.Lines.Add(TimeToStr(Time)+' - Положите палец на сканер');
  Label10.Caption := 'Положите палец на сканер';
  Str := ExtractFilePath(Application.ExeName) + 'ringout.wav';
  Ach := PWideChar(Str); sndPlaySound(Ach, 1);
  Memo1.Lines.Clear;
end;
find := 'remove finger';
for i := 0 to Memo1.Lines.Count-1 do
If Pos(FIND, Memo1.Lines.Text)<> 0
then begin
  Memo2.Lines.Add(TimeToStr(Time)+' - Уберите палец со сканера');
  Label10.Caption := 'Уберите палец со сканера';
  Str := ExtractFilePath(Application.ExeName) + 'ringout.wav';
  Ach := PWideChar(Str); sndPlaySound(Ach, 1);
  Memo1.Lines.Clear;
end;
find := 'put finger again';
for i := 0 to Memo1.Lines.Count-1 do
If Pos(FIND, Memo1.Lines.Text)<> 0
then begin
  Memo2.Lines.Add(TimeToStr(Time)+' - Положите тот же палец еще раз');
  Label10.Caption := 'Положите тот же палец еще раз';
  Str := ExtractFilePath(Application.ExeName) + 'ringout.wav';
  Ach := PWideChar(Str); sndPlaySound(Ach, 1);
  Memo1.Lines.Clear;
end;
find := 'ID saving OK';
for i := 0 to Memo1.Lines.Count-1 do
If Pos(FIND, Memo1.Lines.Text)<> 0
then begin
  Memo2.Lines.Add(TimeToStr(Time)+' - Модель отпечатка пальца сохранена');
  Label10.Caption := 'Модель отпечатка пальца сохранена';
  Str := ExtractFilePath(Application.ExeName) + 'ringout.wav';
  Ach := PWideChar(Str); sndPlaySound(Ach, 1);
  Memo1.Lines.Clear;
end;
find := 'ID Deleted';
for i := 0 to Memo1.Lines.Count-1 do
If Pos(FIND, Memo1.Lines.Text)<> 0
then begin
  Memo2.Lines.Add(TimeToStr(Time)+' - Модель отпечатка пальца удалена');
  Label10.Caption := 'Модель отпечатка пальца удалена';
  Str := ExtractFilePath(Application.ExeName) + 'ringout.wav';
  Ach := PWideChar(Str); sndPlaySound(Ach, 1);
  Memo1.Lines.Clear;
end;
find := 'Unknown error';
for i := 0 to Memo1.Lines.Count-1 do
If Pos(FIND, Memo1.Lines.Text)<> 0
```

```
  then begin
    Memo2.Lines.Add(TimeToStr(Time)+' - Неизвестная ошибка модуля!');
    Label10.Caption := 'Неизвестная ошибка модуля!';
    Str := ExtractFilePath(Application.ExeName) + 'ringout.wav';
    Ach := PWideChar(Str); sndPlaySound(Ach, 1);
    Memo1.Lines.Clear;
  end;
  find := 'RFID UID';
  for i := 0 to Memo1.Lines.Count-1 do
  If Pos(FIND, Memo1.Lines.Text)<> 0
  then begin
    Timer3.Enabled := true;
    Memo1.Lines.Clear;
  end;
end;
procedure TForm1.Timer3Timer(Sender: TObject);
var
  Str: string;
  Ach: PWideChar;
begin
  Edit1.Text := Memo1.Lines.Text;
  if Edit1.GetTextLen > 5
  then begin
    Timer3.Enabled := false;
    if Button4.Visible = false then DBEdit2.Text := Edit1.Text
    else begin
      if not ClientDataSet1.Locate('RFID', Edit1.Text, [loCaseInsensitive, loPartialKey])
      then begin
        Memo2.Lines.Add(TimeToStr(Time)+' - RFID карта НЕ найдена!');
        Str := ExtractFilePath(Application.ExeName) + 'ringout.wav';
        Ach := PWideChar(Str); sndPlaySound(Ach, 1);
        Edit12.Text := 'N'; Button3.Click;
      end else begin
        if DBComboBox1.Text = 'A' then begin Edit12.Text := 'A'; Button3.Click; end;
        if DBComboBox1.Text = 'B' then begin Edit12.Text := 'B'; Button3.Click; end;
        if DBComboBox1.Text = 'AB' then begin Edit12.Text := 'C'; Button3.Click; end;
        Memo2.Lines.Add(TimeToStr(Time)+' - RFID карта найдена: ' + DBEdit1.Text);
        Str := ExtractFilePath(Application.ExeName) + 'ringout.wav';
        Ach := PWideChar(Str); sndPlaySound(Ach, 1);
      end;
    end;
  end;
end;
end.
```

Листинг программы на Arduino:

```
#include "Adafruit_Fingerprint.h"; //библиотека для работы с модулем отпечатка
#include "SoftwareSerial.h"; //библиотека для работы с UART
#include "DFRobotDFPlayerMini.h"; //библиотека для работы с MP3 модулем
#include "SPI.h"; //библиотека SPI для RFID связи
```

```
#include "MFRC522.h"; //библиотека для работы с RFID модулем
uint8_t id; uint8_t getFingerprintEnroll(); //шаблон отпечатка пальца
MFRC522 mfrc522(53, 49); //RFID
unsigned long uidDec, uidDecTemp; //для хранениия номера метки в десятичном формате (RFDI)
DFRobotDFPlayerMini myDFPlayer;
//--------------------------------------------------------------------------
int Mode=0; String MSG, ABC; //переменные для временного хранения данных
SoftwareSerial mySerial(11, 10); //RX, TX UART биометрия
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial); //биометрия, указываем наш Serial UART
void setup() {
  while(!Serial); delay(300); Serial.begin(9600); Serial2.begin(9600); finger.begin(57600);
  if (finger.verifyPassword()) { Serial.println("Found sensor"); } //обнаружен, выводим сообщение
  else { Serial.println("Sensor error"); while(1); } //не обнаружен, выводим сообщение и входим в бесконечный цикл
  myDFPlayer.begin(Serial2); delay (300); myDFPlayer.EQ(DFPLAYER_EQ_ROCK);
  myDFPlayer.volume(29);  myDFPlayer.setTimeOut(500); myDFPlayer.outputDevice(DFPLAYER_DEVICE_SD);
  SPI.begin(); mfrc522.PCD_Init(); //инициализация SPI и RFID
  pinMode(33, INPUT); //кнопка
  pinMode(7, INPUT); //датчик наклона
  pinMode(2, OUTPUT); //красный индикатор
  pinMode(3, OUTPUT); //зеленый индикатор
  pinMode(6, OUTPUT); //питание датчика наклона
  pinMode(4, OUTPUT); //дверь A
  pinMode(5, OUTPUT); //дверь B
}

void loop() {
  while (Serial.available() > 0) {
    MSG = Serial.readString();
    if (MSG == "I") { Mode = 2; MSG = ""; } //режим сохранения отпечатков
    if (MSG == "D") { Mode = 4; MSG = ""; } //режим удаления отпечатков
    if (MSG == "A") { Mode = 1; MSG = ""; ABC = "A"; }
    if (MSG == "B") { Mode = 1; MSG = ""; ABC = "B"; }
    if (MSG == "C") { Mode = 1; MSG = ""; ABC = "C"; }
    if (MSG == "N") { Mode = 0; MSG = ""; myDFPlayer.play(2); } //получен отказ от компьютера
    if (MSG == "O") { MSG = ""; myDFPlayer.play(4); } //есть связь с компьютером
  }
  if (digitalRead(33) == HIGH) { delay (100); if (digitalRead(33) == HIGH) {
    Mode = 3; myDFPlayer.play(5); //если нажали кнопку сканера
  }}
  if (digitalRead(7) == HIGH) {
    myDFPlayer.play(3); delay (8000); Mode = 0; //если обнаружили взлом
  }
```

```
        //============================================================
Режим охраны (читаем карту)
          if (Mode == 0) {
            digitalWrite(3, LOW); //зеленый индикатор
            digitalWrite(2, HIGH); //красный индикатор
            digitalWrite(6, HIGH); //питание датчика наклона
            digitalWrite(4, LOW); //дверь A
            digitalWrite(5, LOW); //дверь B
            if (!mfrc522.PICC_IsNewCardPresent()) { return; } //поиск метки
            if (!mfrc522.PICC_ReadCardSerial()) { return; } //чтение метки
               uidDec = 0; for (byte i = 0; i < mfrc522.uid.size; i++) { //выдача серийного номера
метки
            uidDecTemp = mfrc522.uid.uidByte[i]; uidDec = uidDec * 256 + uidDecTemp; }
            int Boss = 392524386; int RFID = uidDec;
            if (RFID == Boss) { Mode = 1; ABC = "C"; } else {
              Serial.println("RFID UID"); Serial.println(); delay(1000);
              Serial.println(uidDec); Serial.println();
            }
            delay(1000);
          }

        //============================================================
Режим успешной авторизации (открывание дверей)
          if (Mode == 1) {
            if (ABC == "A") {
              myDFPlayer.play(1);
              delay(2000);
              digitalWrite(3, HIGH); //зеленый индикатор
              digitalWrite(2, LOW); //красный индикатор
              digitalWrite(4, HIGH); //дверь A
              digitalWrite(5, LOW); //дверь B
            }
            if (ABC == "B") {
              myDFPlayer.play(1);
              delay(2000);
              digitalWrite(3, HIGH); //зеленый индикатор
              digitalWrite(2, LOW); //красный индикатор
              digitalWrite(4, LOW); //дверь A
              digitalWrite(5, HIGH); //дверь B
            }
            if (ABC == "C") {
              myDFPlayer.play(1);
              delay(2000);
              digitalWrite(3, HIGH); //зеленый индикатор
              digitalWrite(2, LOW); //красный индикатор
              digitalWrite(4, HIGH); //дверь A
              digitalWrite(5, HIGH); //дверь B
            }
            delay(500); digitalWrite(3, LOW); delay(500); digitalWrite(3, HIGH);
```

```
    delay(500); digitalWrite(3, LOW); delay(500); digitalWrite(3, HIGH);
    delay(500); digitalWrite(3, LOW); delay(500); digitalWrite(3, HIGH);
    delay(500); digitalWrite(3, LOW); delay(500); digitalWrite(3, HIGH);
    delay(500); digitalWrite(3, LOW); delay(500); digitalWrite(3, HIGH);
    myDFPlayer.play(6); delay(2000); ABC = ""; Mode = 0;
   }
  //=============================================================
Режим сохранения отпечатков
   if (Mode == 2) {
    Serial.print("Enter ID"); //введите идентификационный номер
    id = readnumber(); //ожидание получения цифры, введённой с COM-порта
    Serial.print("OK, ID = "); Serial.println(id); //введён идентификационный номер
    while(!getFingerprintEnroll()); //вызываем функцию сохранения шаблона по его ID
   }
  //=============================================================
Режим биометрического доступа
   if (Mode == 3) {
    if(finger.getImage() == FINGERPRINT_OK) { //если корректная загрузка
изображения, то идем дальше
    if(finger.image2Tz() == FINGERPRINT_OK) { //если изображение
сконвертировано, то идем дальше
    if(finger.fingerFastSearch() == FINGERPRINT_OK) { //если найдено соответствие,
то идем дальше
     ABC = "C";
     Mode = 1;
    } else {
     myDFPlayer.play(2);
     Mode = 0;
    }}}
   }
  //=============================================================
Режим удаления отпечатков
   if (Mode == 4) {
    Serial.print("Enter ID"); //введите идентификационный номер
    id = readnumber(); //получения цифры с COM-порта
    Serial.print("OK, ID = "); Serial.println(id); //введён идентификационный номер
    deleteFingerprint(id); //вызываем функцию удаления шаблона по его ID
   }
  } //конец LOOP-a, снизу у нас функции ------------------------------------------------------------
-----------------------------------
  uint8_t readnumber(void) { //функция возвращает номер, введённый с COM-порта
   int num = -1;
   while(num<0) {
    while(!Serial.available()); while(Serial.available()) {
     char c = Serial.read(); //присваиваем очередной символ из COM-порта в
переменную
     if(isdigit(c)) {
      if(num<0){num=0;}else{num *= 10;}
```

```
        num += c - '0';
       } delay(5);
      }
     } return num;
    }
    uint8_t getFingerprintEnroll() { //загрузка первого изображения отпечатка пальца
     int p; //переменная результатов
     p = -1; Serial.print ("put your finger"); //положите Ваш палец на сканер
     while(p != FINGERPRINT_OK){
      p = finger.getImage();
      switch(p) {
       case FINGERPRINT_OK: Serial.println("Finger img OK"); break; //отпечатка корректно загрузилось
       case FINGERPRINT_NOFINGER: Serial.print  ("Finger no img"); break; //сканер не обнаружил отпечаток пальца
       case FINGERPRINT_PACKETRECIEVEERR: Serial.println("Communication error"); break; //ошибка соединения
       case FINGERPRINT_IMAGEFAIL: Serial.println("Imaging error"); break; //ошибка изображения
       default: Serial.println("Unknown error"); break; //неизвестная ошибка
      }
     }
      p = finger.image2Tz(1); Serial.print("Image converting"); //конвертируем первое изображение
     switch(p) {
      case FINGERPRINT_OK: Serial.println("Converting OK"); break; //изображение сконвертировано
      case FINGERPRINT_IMAGEMESS: Serial.println("Image too messy"); return p; //изображение слишком нечеткое
      case FINGERPRINT_PACKETRECIEVEERR: Serial.println("Communication error"); return p; //ошибка соединения
      case FINGERPRINT_FEATUREFAIL: Serial.println("No fingerprint on image"); return p; //ошибка конвертирования
      case FINGERPRINT_INVALIDIMAGE: Serial.println("No fingerprint on image"); return p; //ошибка изображения
      default: Serial.println("Unknown error"); return p; //неизвестная ошибка
     }
      p = 0; Serial.print("remove finger"); delay(2000); //уберите Ваш палец со сканера
     while(p != FINGERPRINT_NOFINGER){
      p=finger.getImage();
     } Serial.println("Image OK");
     p = -1; Serial.print ("put finger again"); //положите тот же палец еще раз
     while(p != FINGERPRINT_OK){
      p = finger.getImage();
      switch(p){
       case FINGERPRINT_OK: Serial.println("Finger img OK"); break; //отпечатка пальца корректно загрузилось
```

```
            case FINGERPRINT_NOFINGER: Serial.print  ("Finger no img"); break; //сканер не обнаружил отпечаток пальца
            case FINGERPRINT_PACKETRECIEVEERR: Serial.println("Communication error"); break; //ошибка соединения
            case FINGERPRINT_IMAGEFAIL: Serial.println("Imaging error"); break; //ошибка изображения
            default: Serial.println("Unknown error"); break; //неизвестная ошибка
           }
          }
          p = finger.image2Tz(2); Serial.print("Image converting"); //конвертируем второе изображение
          switch(p){
           case FINGERPRINT_OK: Serial.println("Converting OK"); break; //изображение сконвертировано
           case FINGERPRINT_IMAGEMESS: Serial.println("Image too messy"); return p; //изображение слишком нечеткое
           case FINGERPRINT_PACKETRECIEVEERR: Serial.println("Communication error"); return p; //ошибка соединения
           case FINGERPRINT_FEATUREFAIL: Serial.println("No fingerprint on image"); return p; //ошибка конвертирования
           case FINGERPRINT_INVALIDIMAGE: Serial.println("No fingerprint on image"); return p; //ошибка изображения
           default: Serial.println("Unknown error"); return p; //неизвестная ошибка
          }
          p = finger.createModel(); Serial.print("Creating model"); //создание модели по двум изображениям
          if(p == FINGERPRINT_OK){ Serial.println("Creating OK"); } else //модель (шаблон) отпечатка пальца создана
          if(p == FINGERPRINT_PACKETRECIEVEERR){ Serial.println("Communication error"); return p; } else //ошибка соединения
          if(p == FINGERPRINT_ENROLLMISMATCH){ Serial.println("Did not match"); return p; } else //отпечатки пальцев не совпадают
          { Serial.println("Unknown error"); return p; } //неизвестная ошибка
          p = finger.storeModel(id); Serial.print("Saving model ID = "); Serial.print(id); Serial.print(": "); //сохранение
          if(p == FINGERPRINT_OK){ Serial.println("ID saving OK"); Mode = 0; } else //модель отпечатка пальца сохранена
          if(p == FINGERPRINT_PACKETRECIEVEERR){ Serial.println("Communication error"); return p; } else //ошибка соединения
          if(p == FINGERPRINT_BADLOCATION){ Serial.println("Not store location"); return p; } else //не удалось сохранить в этом месте
          if(p == FINGERPRINT_FLASHERR){ Serial.println("Error flash"); return p; } else //ошибка записи в flash память
          { Serial.println("Unknown error"); return p; } //неизвестная ошибка
         }
        uint8_t deleteFingerprint(uint8_t id) { //функция удаляет отпечаток пальца по указанному ID
          int p = -1; //переменная для получения результатов
```

```
        p = finger.deleteModel(id); //удаляем шаблон отпечатка пальца
        switch(p){
          case FINGERPRINT_OK: Serial.println("ID Deleted"); Mode = 0; break; //шаблон отпечатка пальца корректно удалён
          case FINGERPRINT_PACKETRECIEVEERR: Serial.println("Communication error"); break; //ошибка соединения
          case FINGERPRINT_BADLOCATION: Serial.println("Could not delete"); break; //не удалось
          case FINGERPRINT_FLASHERR: Serial.println("Error flash"); break; //ошибка в flash память
          default: Serial.println("Unknown error"); break; //неизвестная ошибка
        }
      }
```

Приложение Б

Принципиальные схемы конструкции

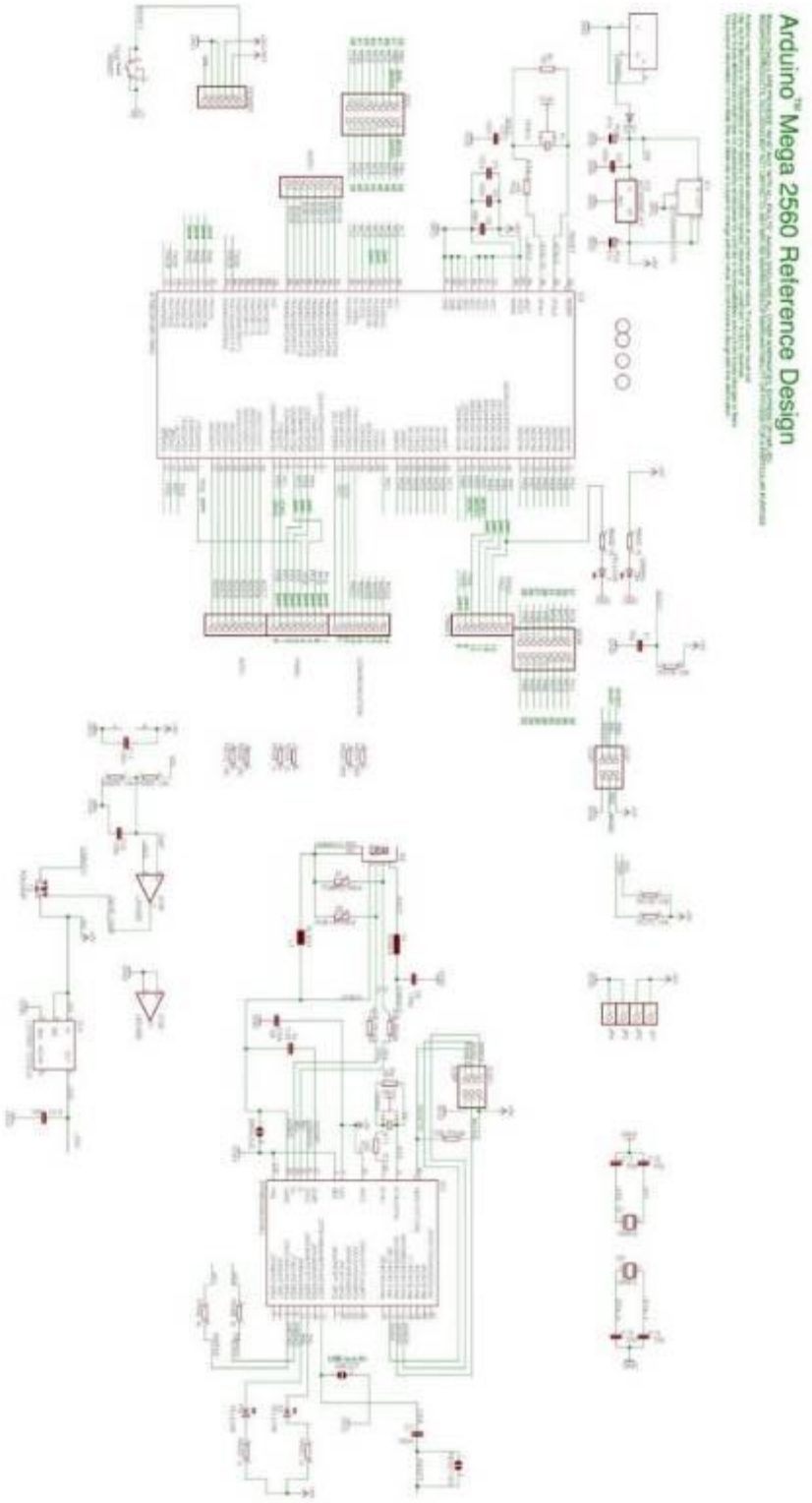


Рисунок Б.1 - Принципиальная схема Arduino Mega

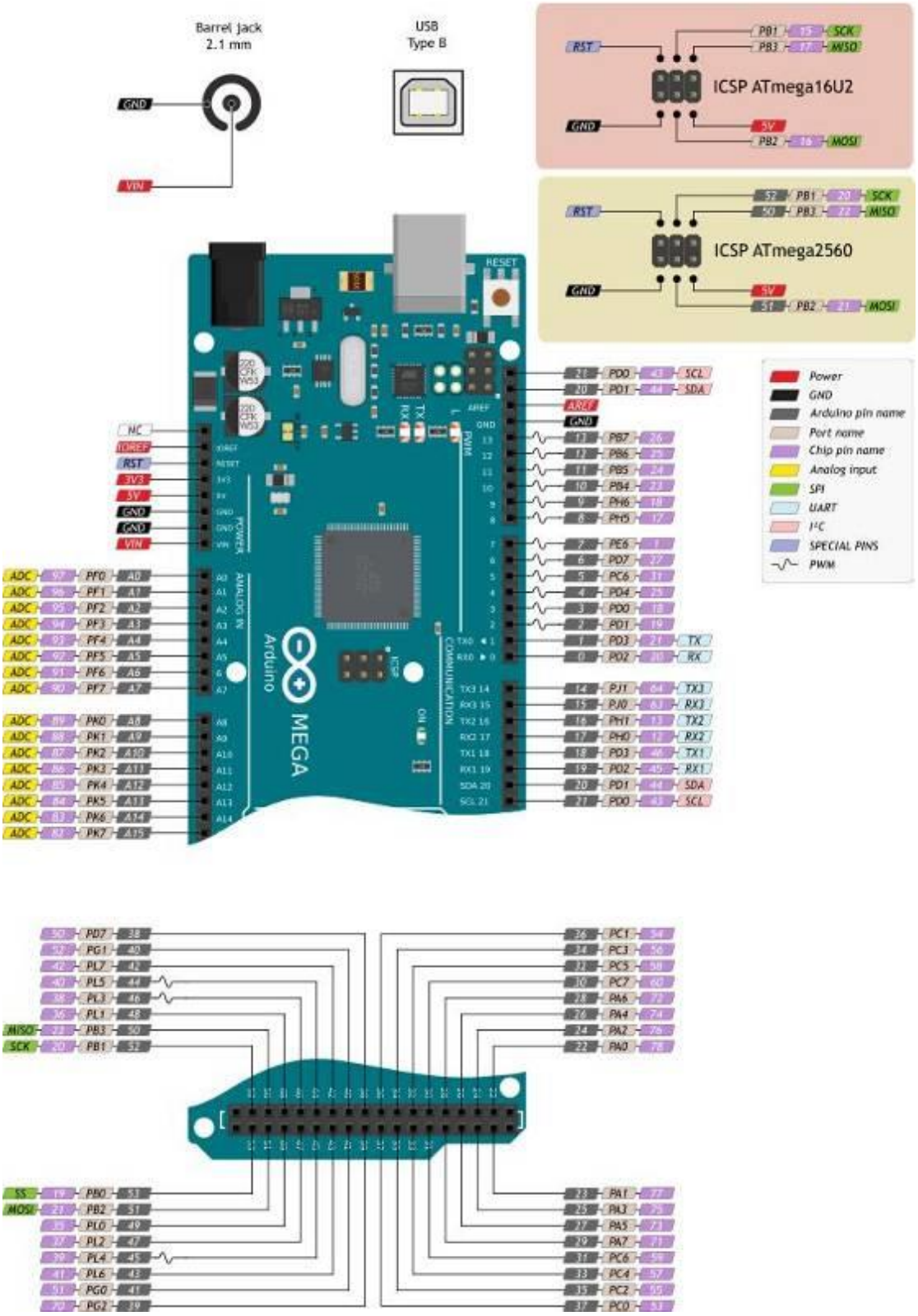


Рисунок Б.2 – Распиновка Arduino Mega

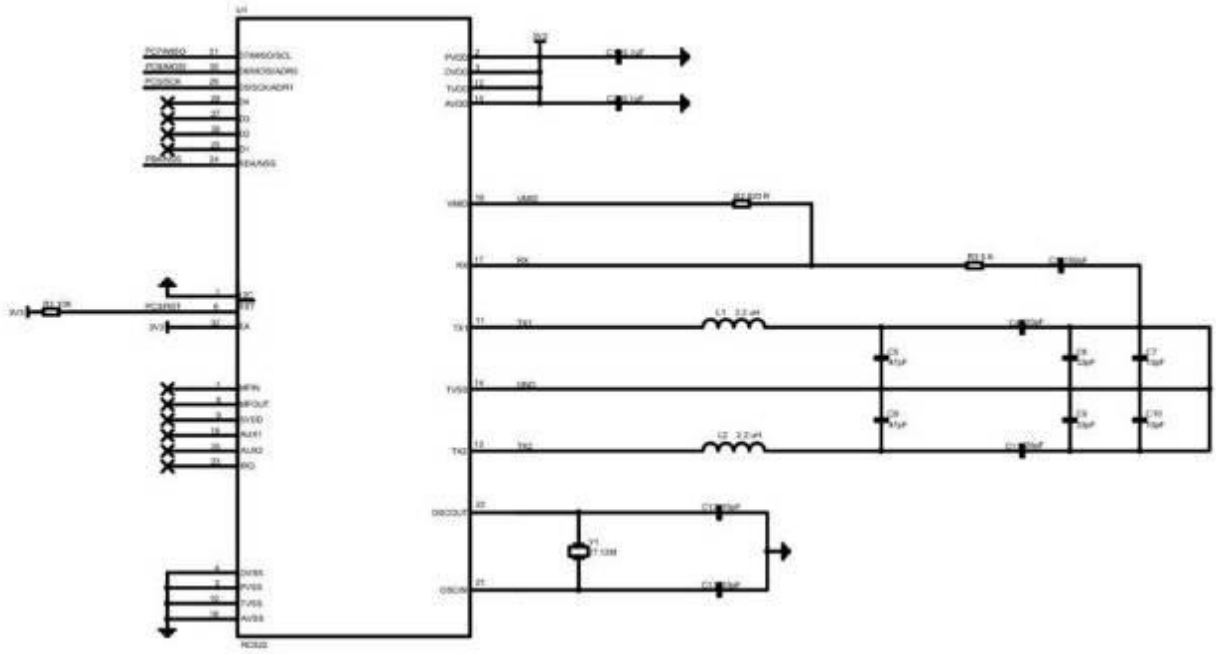


Рисунок Б.3 – Принципиальная схема RFID модуля

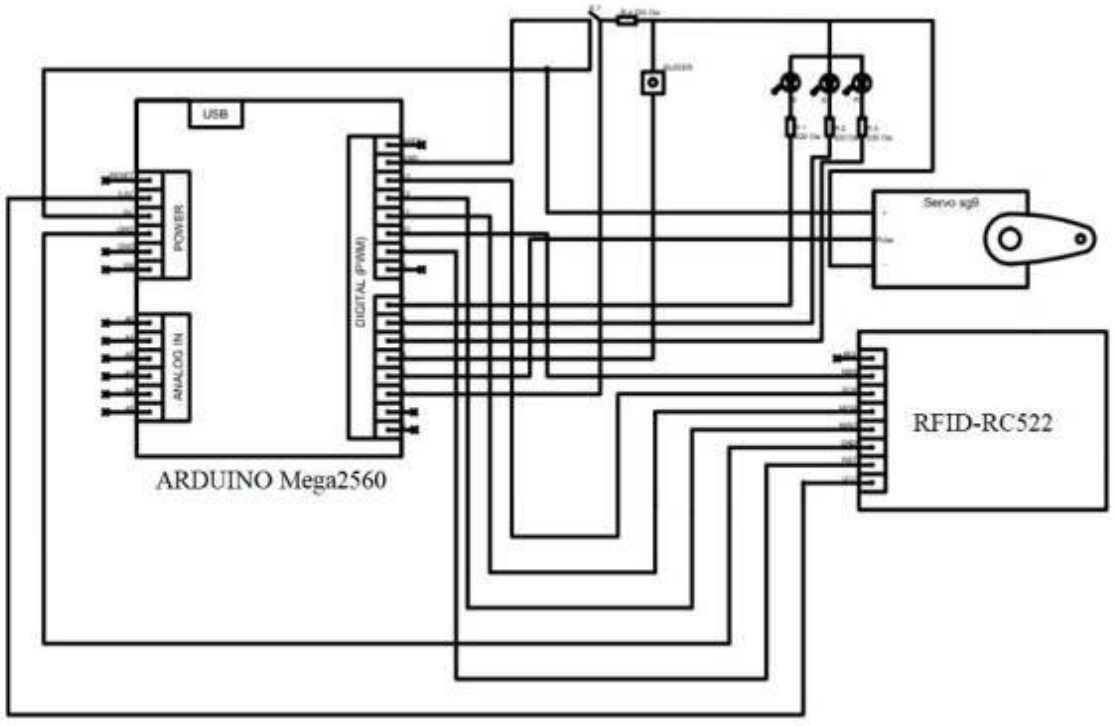


Рисунок Б.4 – Принципиальная схема подключения RFID-RC522 к Arduino Mega2560