**Оглавление**

[1. Литературный обзор 2](#_Toc70587601)

[2. Анализ исходных данных и основных технических требований к разрабатываемому устройству. 4](#_Toc70587602)

[2.1 Выбор и обоснование элементной базы, унифицированных узлов, установочных изделий и материалов конструкции. 5](#_Toc70587603)

[2.1.1 Разбиение системы на функциональные модули 6](#_Toc70587604)

[2.1.2 Выбор соотношения между аппаратными и программными средствами. 8](#_Toc70587605)

[2.1.3 Выбор элементной базы 9](#_Toc70587606)

[2.2 Выбор и обоснование компоновочной схемы и метода конструирования. 15](#_Toc70587607)

[2.3 Выбор и обоснование способов и средств обеспечения теплового режима, герметизации, виброзащиты и электромагнитной совместимости. 17](#_Toc70587608)

# Литературный обзор

В данном дипломном проекте требуется разработать систему управления кодовым замком на микроконтроллере со сканером отпечатка пальца.

Электронный замок — электронное устройство, предназначенное для того, чтобы предотвратить доступ в помещение посторонних лиц, или наоборот, ограничить выход из помещения. Решение о доступе лиц в помещение принимается на основе сигналов от различных датчиков: считывателей магнитных карт, штрих-кодов, датчиков контактной памяти, биометрических датчиков, наборной клавиатуры, комбинаторных флуоресцентных молекулярных датчиков, дистанционного управления и т. д. Часто является частью сложной электронной системы контроля доступа, иногда неотделим от неё. В качестве исполнительных механизмов используются электромеханические и электромагнитные запорные устройства [1].

Надежность и простота использования системы, компактные габариты и низкое энергопотребление определяют эффективность системы.

У данных устройств, к сожалению, есть и свои минусы:

1. Код можно забыть. Код обычно забывается после того, как он длительное время не использовался. Тем не менее, его можно записать, но тогда увеличивается вероятность, что код узнает посторонний;
2. Код могут подсмотреть при вводе. Поэтому при вводе кода необходимо сохранять скрытность.
3. Часто в качестве кодов используются даты (рождения), адреса, общеизвестные числа (3.141592653, 2,718281828), что упрощает подбор кода.
4. Если код долгое время не меняется, то часто используемые кнопки замка начинают изнашиваться и таким образом показывают код.

Для нивелирования данных недостатков, как разработчик, предоставляю следующие решения:

1. При первом включении пользователь сам инициализирует пароль
2. Для повышения защиты в устройстве будет использован сканер отпечатка пальца как замена вводу пароля с помощью клавиатуры.
3. У пользователя будет возможность менять пароль, используя привилегию «Супер-пользователя». Период смены пароля определяется самим клиентом.

Сейчас развивается сфера распознавания и анализа биометрических данных человека, поэтому было принято решение использовать сканер отпечатка пальца.

В основе многих биометрических систем лежит сканер отпечатков пальцев.

При всем многообразии биометрических систем их возможно упрощённо разделить на три типа:

1. преобразование отпечатка в цифровой код при помощи оптического сенсора;
2. преобразование отпечатка посредством линейного теплового датчика;
3. преобразование отпечатка с помощью ёмкостного датчика.

Для конечного пользователя разница состоит лишь в том, какие манипуляции необходимо производить со сканером: прикладывать палец (оптический и ёмкостной) или проводить им по сенсору (тепловой).

У обеих систем имеются как преимущества, так и недостатки:

Прозрачное окно оптического сенсора сканирования необходимо содержать в чистоте. Многократное прикладывание пальцев к нему загрязняет стеклянное покрытие.

Оптический сенсор обеспечивает сканирование чёткой картинки, которая впоследствии будет сравниваться.

Линейный тепловой сенсор не оставляет возможности воспользоваться имитацией пальца (например, пальцем или фрагментом кожного покрова, отделённым от трупа; трёхмерной силиконовой имитацией на кончике носа или на гениталиях; латексной псевдотрёхмерной имитацией; трёхмерной травленой имитацией и другими жульническими приёмами, либо уже существующими, либо пока не изобретёнными злоумышленниками, но уже предусмотренными производителем)

Линейный тепловой сканер, по утверждению его разработчика и производителя, очищается с каждым проведением пальца.

В ёмкостном датчике используется разница в электрической ёмкости между гребнем и канавкой (система более экономична, но с меньшей точностью распознавания).

Надёжность сканирования зависит не только от сенсора. Дальнейшая обработка полученных данных — ключ к успешному распознаванию отпечатка.

В сканере отпечатков пальцев с оптическим чувствительным элементом, по сути монохромной матрицей, изображение поступает в виде фотографии.

В простейших сканерах изображение просто сравнивается с эталоном. Часто дальнейшая обработка базируется на работе с несколькими шаблонами.

Цифровой код, полученный от сканера, в системе с линейным тепловым датчиком — это всегда разный шаблон. Скан отпечатка пальца всегда разный, качество распознавания зависит от угла, под которым проводился палец, от влажности пальца или поверхности сканера. Данные, поставляемые таким сканером — фактически набор точек. Не важно, как лег палец на поверхность сканера, эти точки всегда будут иметь одинаковый изгиб линий.

Необходимо заметить, что при распознавании отпечатков любым типом сенсоров и алгоритмов неизбежны ошибки. Ошибки обычно разделяют на 2 типа — нераспознавание правильного отпечатка и распознавание неправильного отпечатка как правильного.

Производители сканеров начали производить компактные сканеры, подключаемые к порту USB. Сканеры вмонтированы в ноутбуки бизнес-класса, в отдельные модели клавиатур, компьютерных мышей и смартфонов.

Сканеры, совместно с соответствующим программным обеспечением, широко применяются в больших корпорациях в дополнение к паролям.

Сканерами отпечатков пальцев в Британии планируется заменить билеты пассажиров, чтобы решить проблему загруженности железнодорожных станций, сэкономить время на покупку билетов и увеличить пропускную способность турникетов. С помощью отпечатка пальца сумма за проезд будет автоматически сниматься со счетов пассажиров.

В лондонском музыкальном баре ‘Proud’ тестируется новая технология FingoPay. Данная система биометрических платежей изобретена компанией Sthaler Limited. Устройство сканирует на пальце вены, расположение которых уникально у каждого человека. Эта идея уже завоевала себе поклонников среди клиентов заведения. Главный исполнительный директор компании заявил, что вскоре на подобный шаг решатся кинотеатры, супермаркеты и музыкальные фестивали.

Таким образом, интеграция сканеров отпечатков пальцев и прочих биометрических сканеров имеет плюсы, одними из которых является упрощение повседневных действий и повышение защиты в местах, где это необходимо.

# Анализ исходных данных и основных технических требований к разрабатываемому устройству.

Для открытия и закрытия двери требуется, чтобы система имела способность подавать высокое(открытие) и низкое(закрытие) напряжение на исполнительное устройство электромагнитного замка или на серво привод.

Согласно требованиям, устройство должно обеспечивать подсветку при приближении к двери. Это может быть реализовано с помощью датчика приближения или движения. Когда сотрудник подходит на заранее определенное расстояние к замку, загорается подсветка клавиатуры. После ввода верного пароля пользователь должен быть извещен о том, что замок открыт, то есть необходима индикация при открытии замка с помощью дисплея и звукового сопровождения.

Следующим требованием является оперативная смена секретной кодовой комбинации. Для этого после 3 неудачных попыток ввода срабатывает защита и требуется сменить кодовую комбинацию. Для этого надо ввести заранее закрепленную последовательность, затем старый пароль. После успешного ввода следует ввести новый код.

Функциональная спецификация определяет, какие функции должны выполняться системой и как выглядит интерфейс между системой и окружением. Таким образом, функциональная спецификация включает в себя два основных компонента:

1. Список функций, выполняемых системой;
2. Описание интерфейса между системой и пользователем.

Для составления корректной функциональной спецификации составлен список вопросов:

* Что является триггерным моментом для включения подсветки клавиатуры?
* Каким образом сконфигурирован ввод и вывод информации?
* Каким образом происходит оповещение пользователя об открытии двери?
* Какой алгоритм для сброса и ввода введенной пользователем информации?
* Каким образом система будет способна открыть замок?

После анализа данных составлен список аспектов, требуемых для рассмотрения:

* Будет установлен датчик приближения для определения расстояния до пользователя. При приближении до кодового замка на расстояние вытянутой руки подсветка загорается.
* Для ввода информации будет предусмотрена матричная клавиатура, а для вывода информации – LCD-дисплей.
* Оповещение пользователя об открытии двери будет многопоточный: вывод фразы на дисплей и звуковое оповещение.
* Для открытия двери отводится 3 попытки. В случае 3 неправильных попыток требуется ввести закрепленную последовательность с подтверждением старого пароля.
* Для открытия двери системой контроля кодовым замком было принято решение использовать сервопривод.

## Выбор и обоснование элементной базы, унифицированных узлов, установочных изделий и материалов конструкции.

### Разбиение системы на функциональные модули

На основе функциональной спецификации определим набор модулей реализации функций в системе. Следующим шагом будет разбиение модулей на аппаратные и программные.

В результате получим модульную структуру аппаратных средств устройства.

Основу аппаратных средств системы составляет управляющая микро-ЭВМ, которая включает в себя:

* Процессорный модуль, предназначенный для обработки информации;
* Модель генератора тактовых импульсов, предназначенный для синхронизации работы системы;
* Модуль памяти, предназначенный для хранения информации;
* Модуль интерфейса ввода и модуль интерфейса вывода, содержащие интерфейсные компоненты, необходимые для связи процессорного модуля с другими модулями системы
* Модуль таймера;
* Модуль преобразования входного сигнала;
* Модуль преобразования входного сигнала, которые содержат компоненты, необходимые для обмена входными и выходными сигналами с внешним окружением.

На рисунке 2.1 представлена структура аппаратных средств системы управления кодовым замком.

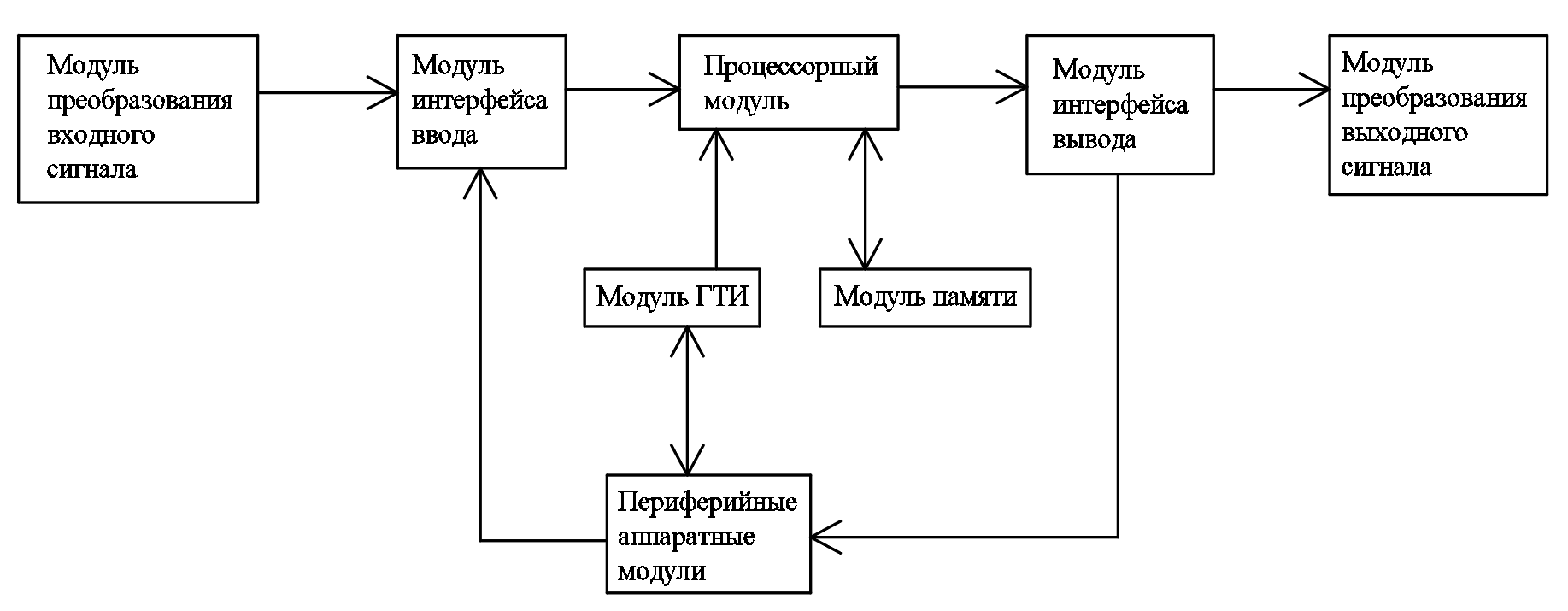


Рисунок 2.1 – Модульная структура аппаратных средств микропроцессорной системы

Разобьем систему на функциональные модули. Система состоит из 3 основных частей: вход, выход и обработка информации.

Входной модуль является матричной клавиатурой для считывания информации.

Выходной модуль состоит из сервопривода, пьезодинамика и дисплея.

Модуль обработки информации состоит из подмодулей:

1. Модуль проверки состояния датчика движения;
2. Модуль считывания информации с клавиатуры;
3. Модуль проверки на нажатие клавиши «\*»;
4. Модуль вывода информации на дисплей;
5. Модуль проверки на совпадение введенного кода с верным;
6. Модуль проверки на совпадение введенной информации с закрепленной последовательностью;
7. Модуль смены пароля;
8. Модуль открытия/закрытия замка;
9. Модуль проверки количества неверных попыток ввода пароля;
10. Модуль сигнализации.

Сканер отпечатка пальца является полноценным устройством, которое состоит из модулей ввода, вывода и обработки данных. Но из-за направленности устройства он будет входить во входной модуль.

Функционально-модульная структура, разбитая на слои по иерархии представлена на рисунке 2.2. Верхний уровень представлен исполнительным модулем, который имеет средства, необходимые для реализации управляющей функции. На среднем уровне располагаются модули считывания, смены пароля и проверки. Дальше расположились модуль открытия замка, блокировки и сигнализации. А на нижнем находятся входной и выходной модуль.



Рисунок 2.2 – Функционально-модульная структура системы управления кодовым замком

Распределение функций по модулям системы управления кодовым замком выглядит следующим образом:

1. Исполнительный модуль:
   1. Управление системой;
2. Входной модуль:
   1. Считывание матричной клавиатуры;
   2. Считывание опечатка пальца;
   3. Считывания состояния датчика движения;
3. Выходной модуль:
   1. Включение/выключение дисплея;
   2. Воспроизведение звукового предупреждения;
4. Модуль ожидания выполнения действия:
   1. Ожидание сигнала активности с датчика движения;
5. Модуль считывания:
   1. Считывание значений с клавиатуры:
6. Модуль проверки действия:
   1. Проверка на нажатие клавиши «\*»;
   2. Проверка на совпадение введенного кода с верным;
   3. Проверка на совпадение введенной информации с закрепленной последовательностью;
   4. Проверка количества последовательно неверно введенных кодовых комбинаций;
7. Модуль смены пароля:
   1. Смена секретной кодовой комбинации;
8. Модуль открытия/закрытия замка:
   1. Поворот сервопривода;
9. Модуль сигнализации:
   1. Включение сигнализации;

### Выбор соотношения между аппаратными и программными средствами.

Функция управления системы реализуется управляющей микро-ЭВМ (микроконтроллер) в результате выполнения основной (управляющей) программы путем последовательного вызова функций соответствующих программных модулей системы.

Связь между программными и аппаратными модулями представлена на рисунке 2.3.

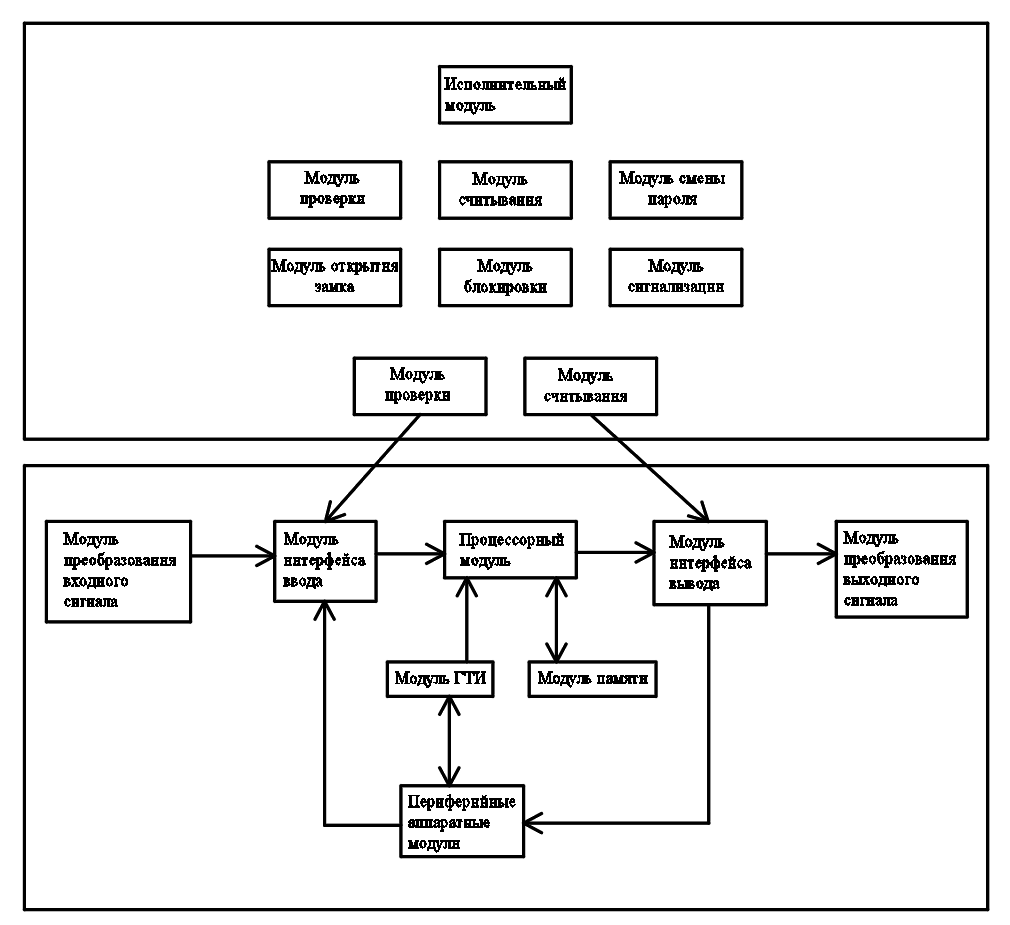


Рисунок 2.3 – Связь между аппаратными и программными средствами

### Выбор элементной базы

#### Выбор микроконтроллера

Проанализировав сложность поставленной задачи было принято решение использовать микроконтроллер ATmega328 в составе платформы Arduino Uno 3.0 (рисунок 2.1.1). Данный микроконтроллер является представителем семейства 8-ми разрядных CMOS микроконтроллеров с низким энергопотреблением, основанным на усовершенствованной AVR RISC архитектуре в корпусе TQFP32 [2].



Рисунок 2.1.1 – Внешний вид Arduino Uno 3.0

Следует рассказать про Atmel Corporation и AVR RISC архитектуре.

Atmel Corporation — компания производитель полупроводниковых электронных компонентов, основана в 1984 году. Один из лидеров производства микроконтроллеров (MCS-51, ARM, AVR, AVR32). Также разрабатывает и производит небольшие модули энергонезависимой памяти для электронных изделий, ПЛИС, цифровые микросхемы-радиоприёмники и передатчики, сканеры отпечатков пальцев. Компания для своих клиентов может предложить систему на кристалле, объединяющую затребованные компоненты. Продукция Atmel широко применяется в компьютерных сетях, промышленности, медицине, связи, автомобилях, космосе, военных устройствах, а также кредитных картах [3].

Идея разработки нового RISC-ядра принадлежит двум студентам Norwegian University of Science and Technology (NTNU) из норвежского города Тронхейма — Альфу Богену (Alf-Egil Bogen) и Вегарду Воллену (Vegard Wollen). В 1995 году Боген и Воллен решили предложить американской корпорации Atmel, которая была известна своими чипами с Flash-памятью, выпускать новый 8-битный RISC-микроконтроллер и снабдить его Flash-памятью для программ на одном кристалле с вычислительным ядром.

Идея была одобрена Atmel Corp., и было принято решение незамедлительно инвестировать в данную разработку. В конце 1996 года был выпущен опытный микроконтроллер AT90S1200, а во второй половине 1997 г. корпорация Atmel приступила к серийному производству нового семейства микроконтроллеров, к их рекламной и технической поддержке.

Микроконтроллеры AVR имеют гарвардскую архитектуру (программа и данные находятся в разных адресных пространствах) и систему команд, близкую к идеологии RISC. Процессор AVR имеет 32 8-битных регистра общего назначения, объединённых в регистровый файл.

Arduino получило широкое применение в отрасли создания электронных средств. Основными достоинствами платформы Arduino являются следующие показатели:

1. Низкая стоимость;
2. Кросс-платформенность;
3. Простая и понятная среда программирования;
4. Программное обеспечение с открытым исходным кодом;
5. Аппаратные средства с возможностью модернизации.

Согласно документации платформа имеет следующие характеристики:

1. 14 цифровых входов/выходов (6 из которых могут использоваться как выходы ШИМ);
2. 6 аналоговых входов;
3. 2 последовательных порта UART;
4. Кварцевый генератор 16 МГц;
5. USB коннектор;
6. Разъем питания;
7. Разъем ISCP;
8. Кнопку перезагрузки;
9. Флеш-память объемов 32 КБ;
10. ОЗУ объемом 2 КБ;
11. ПЗУ 1 КБ.

#### Выбор пьезодинамика

Источником звука в проектируемой схеме будет пьезодимакик.

Пьезоэлемент — электромеханический преобразователь, одним из разновидностей которого является пьезоизлучатель звука, который также называют пьезодинамиком, просто звонком или английским buzzer. Пьезодинамик переводит электричеcкое напряжение в колебание мембраны. Эти колебания и создают звук (звуковую волну) [5].

В схеме будет использоваться пьезодинамик KPR-G1750 (рисунок 2.1.2).



Рисунок 2.1.2 – Пьезодинамик KPR-G1750

#### Выбор LCD-дисплея

За вывод информации в проектируемой схеме будет отвечать LCD-дисплей. Для подключения дисплея будет использоваться конвертер в I2C.

I2C – последовательная асимметричная шина для связи между интегральными схемами внутри электронных приборов. Использует две двунаправленные линии связи (SDA и SCL), применяется для соединения низкоскоростных периферийных компонентов с процессорами и микроконтроллерами (например, на материнских платах, во встраиваемых системах, в мобильных телефонах). Подключение дисплея к микроконтроллеру будет представлено позже.

В схеме будет использоваться модель YJD1602A-1 (рисунок 2.1.3).

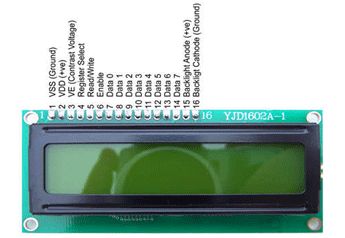


Рисунок 2.1.3 – Дисплей YJD1602A-1

Для более удобного управления подключается библиотека “LiquidCrystal\_I2C”.

Управление проецируемым текстом можно задать программным образом с помощью следующих функций:

1. init() – для инициализации дисплея в программе;
2. backlight() – для включения подсветки дисплея;
3. setCursor() – для установления координат курсора;
4. clear() – для отчистки дисплея от данных;
5. print(someString) – для отображения заданной информации, начиная с координат курсора;

#### Выбор сервопривода

За открытие/закрытие двери отвечает в проектируемой схеме сервопривод.

Сервопривод – это механический привод с автоматической коррекцией состояния через внутреннюю отрицательную обратную связь, в соответствии с параметрами, заданными извне.

В схеме используется цифровой сервопривод Power HD D25-V2 (рисунок 2.1.4).



Рисунок 2.1.4 - Сервопривод Power HD D25-V2

Для более удобного управления подключается библиотека “Servo”.

Управление состоянием привода можно задать программным образом с помощью следующих функций:

1. attach() – для закрепления пина для передачи информации для привода;
2. write() – для передачи угла отклонения привода;

#### Выбор матричной клавиатуры

За ввод данных предусмотрена матричная клавиатура. Для подключения клавиатуры используются порты ввода и вывода. Для уменьшения количества выводов кнопки объединяют в столбцы и строки. Подавая низкий уровень напряжения последовательно на каждую строку, мы опрашиваем столбцы на предмет присутствия на них низкого уровня. Зная на какую строку подан низкий уровень напряжения, и на каком столбце оно появилось, можно определить, какая именно клавиша нажата.

В схеме используется матричная клавиатура KB207-PNW.



Рисунок 2.1.5 – Матричная клавиатура KB207-PNW

Для управления клавиатурой подключается библиотека “Keypad”. Данный пакет определяет набор функций, который используется для программной задачи поведения клавиатуры:

1. makeKeymap(keys) – присвоение маски символов клавиатуре;
2. waitForKey() – остановка работы программы, пока не поступит сигнал с клавиатуры;

#### Выбор датчика приближения

Ультразвуковой датчик приближения является распространенным методом обнаружения движения. Базовой идеей является измерение времени между импульсами, а зная скорость распространения световой волны можно определить расстояние до объекта.

В данной схеме буде использоваться датчик HC-SR04.



Рисунок 2.1.6 – ультразвуковой датчик HC-SR04

Для управления используются стандартные функции:

1. digitalWrite(pinNumber, HIGH/LOW) – подача на заданный пин высокий/низкий уровень напряжения;
2. delayMicroseconds(seconds) – задержка системы на заданное количество миллисекунд;
3. pulseIn(pinNumber, HIGH/LOW) – считывает длину сигнала высокого/низкого напряжения на заданном порту;

#### Выбор сканера отпечатка пальца

На рынке почти нет выбора сканером отпечатков пальцев, так как это является новшеством. В процессе исследования ресурсов выбор пал на Adafruit Optical Fingerprint Sensor. Это решение является привлекательным еще и с той стороны, что компания предоставляет собственное API для управления этим средством. Устройство представлено на рисунке 2.1.7.

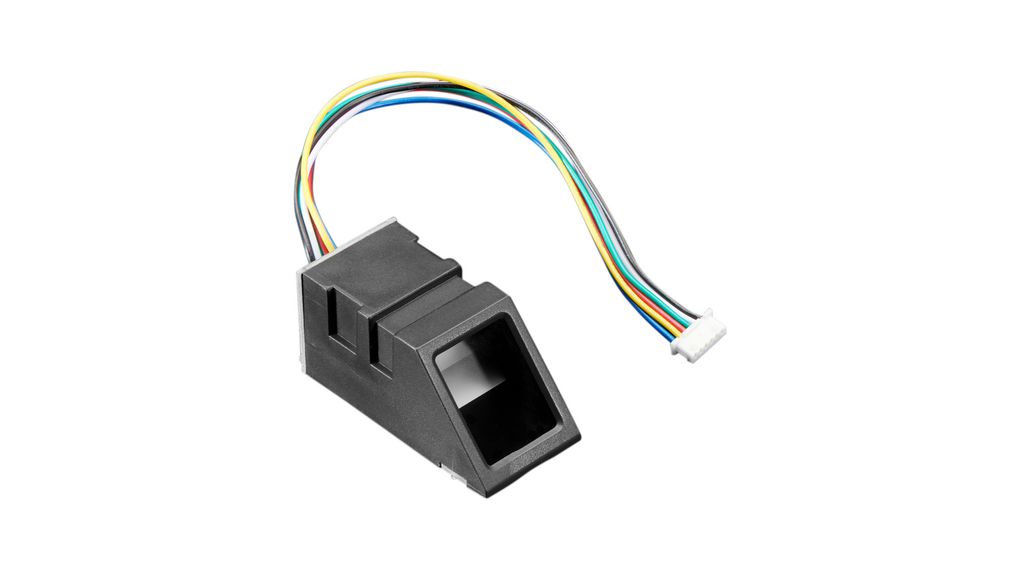


Рисунок 2.1.7 – Сканер отпечатка пальца

## Выбор и обоснование компоновочной схемы и метода конструирования.

Компоновочная схема блоков определяется количеством, видом составляющих элементов и их расположением.

Все компоновочные схемы делятся на два вида:

- централизованная;

- децентрализованная.

Децентрализованная компоновочная схема устройства принимается для электронных средств, обладающих мощными выходными модулями, источниками помех и т.д., тогда электронное средство разносится по нескольким корпусам.

В данном случае будем использовать централизованную компоновочную схему устройства, т. е. все его элементы располагаются в одном корпусе.

На компоновочные схемы электронных средств значительное влияние оказывают вспомогательные элементы. Это различные индикаторы, ручки управления, кнопки, экраны. В зависимости от их количества необходимо выбирать порядок их размещения на передней панели, что влияет на форму самого средства.

Предварительная компоновка электронных средств осуществляется уже на этапе технического предложения, поскольку необходимо учесть требования по габаритам и массе, которые определены в техническом задании на проектирование. На последующих стадиях проектирования происходит корректировка и уточнение компоновочных параметров. Как правило, при компоновке необходимо определить площадь и объем, массу конструкции. В том случае, если результаты расчетов не будут соответствовать требованиям технического задания, то по согласованию с заказчиком в технически обоснованных случаях в техническое задание могут быть внесены соответствующие корректировки.

При компоновке системы кодового замка со сканером отпечатка пальца должны быть учтены следующие основные требования:

- оптимальность, устойчивость и стабильность функциональных межблочных связей;

- требования по жесткости и прочности;

- отсутствие помех;

- эргономика, удобство ремонта;

- оптимальное размещение комплектующих элементов в модулях всех уровней с учетом коэффициента заполнения по объему и удобству для осмотра и ремонта;

- сосредоточение центра тяжести ближе у опорной поверхности;

- наличие достаточного пространства для межблочных соединений.

В первом случае помехи имеют один и тот же характер. Это позволяет относительно легко выявить их причину. Однако могут возникнуть трудности при ее устранении, но если она устранена, то окончательно. Во втором случае, помехи появляются время от времени. Такой характер помех сильно затрудняет выявление их источника.

Проблемы возникновения помех и наводок можно свести к минимуму, изолируя чувствительные части схемы от источника помех, устраняя паразитные индуктивные и емкостные связи. Для этого необходимо:

- располагать маломощные (чувствительные) схемы поблизости от источника сигнала;

- размещать мощные схемы (в которых велика вероятность возникновения помех) вблизи нагрузок;

- располагать маломощные и мощные схемы как можно дальше друг от друга;

- стараться свести к минимуму длину проводников;

- использовать максимально короткие контуры прохождения тока.

## Выбор и обоснование способов и средств обеспечения теплового режима, герметизации, виброзащиты и электромагнитной совместимости.

Вопрос охлаждения изделий электронной техники является одним из важных этапов конструирования электронных средств в связи с широким использованием в электронных средств элементов, выделяющих при работе тепло. Проблема отвода тепла от изделий электронной техники в первую очередь должна решаться на этапе разработки электронных средств. Выделяемое изделиями тепло может быть отведено от поверхности прибора и передано за пределы аппаратуры несколькими методами, применяемыми отдельно или в сочетании друг с другом. В зависимости от характера и назначения электронных средств применяют следующие методы отвода тепла от индивидуальных изделий электронной техники или групп изделий []:

- естественное охлаждение (воздушное);

- принудительное воздушное охлаждение;

- принудительное жидкостное (без кипения или с поверхностным кипением);

- охлаждение, основанное на изменении агрегатного состояния вещества;

- термоэлектрическое охлаждение.

Эффективность того или иного метода охлаждения определяется значением коэффициента теплоотдачи, то есть интенсивностью протекающих процессов теплоотдачи.

Выбор метода охлаждения определяется следующими факторами интенсивностью (плотностью) теплового потока, условиями теплообмена с окружающей средой, условиями эксплуатации (возможностью демонтажа или замены элементов), нормами эксплуатации (уровень шума, токсичностью хладагентов), специальными условиями работы (стационарными или кратковременными режимами, работой против сил тяготения и так далее), затратами электроэнергии на привод нагнетателей и другими [].

Анализируя схему электрическую принципиальную системы кодового замка со сканером отпечатка пальца, тип корпуса устройства и техническое задание, можно сделать предположение о возможности применения естественного воздушного охлаждения.

При естественном охлаждении отвод тепла происходит за счет теплопроводности, естественной конвекции окружающего воздуха и излучения.

Герметизация – это обеспечения полной непроницаемости для газов и жидкостей (герметичности) стен и поверхностей, ограничивающих внутренние части и объёмы аппаратов и машин, помещений и сооружений, а также их стыков и соединений. Следует различать понятия герметизации и герметичности. Герметизация широко применяется в науке и технике. Способ герметизации выбирается в зависимости от конкретных целей и условий. Для герметизации используют пайку, сварку и холодное газодинамическое напыление соединений и течей металлических деталей и изделий, специальные герметизирующие материалы (герметики), составы и уплотнения.

Воздействие влаги на материал корпуса системы кодового замка со сканером отпечатка пальца и изоляционные материалы имеет разную природу, но одинаковый конечный результат – разрушение исходной структуры материала. В фенопласте это происходит за счет разрушение структурной решетки, в изоляционных материалах – за счет влагопоглощения.

Наличие влаги – причина электрохимической коррозии, реакции которой идут при низких температурах.

Разрушение структурной может быть равномерной (по всей поверхности изделия), и неравномерной (например, за счет механического повреждения поверхности алюминия и затем образования отверстий в нем).

Влияние влаги на материалы, входящие в состав системы кодового замка со сканером отпечатка пальца, может быть очень значительным из-за отсутствия изоляционных материалов. Но разрабатываемое устройство относится к классу аппаратуры, которая будет эксплуатироваться в закрытом помещении.

Исходя вышеперечисленных факторов можно сделать вывод, что окружающая среда помещения, где будет использоваться устройство, не повлияет на него.

В данном разделе решается вопрос о необходимости виброзащиты устройства и выборе, при необходимости, способа ее осуществления.

В процессе эксплуатации и транспортировки устройство подвергается различным видам механических воздействий в виде вибраций (основные параметры: частота вибраций *f*, и возникающее при этом ускорение *g*), ударов (основные параметры: ускорение и длительность) и линейных ускорений.

Под вибропрочностью понимают способность электронных средств противостоять разрушающему действию вибрации в заданных диапазонах частот и при возникающих ускорениях в течение срока службы, а под виброустойчивостью аппаратуры - способность выполнения всех функций в условиях вибрации в заданных диапазонах частот и возникающих при этом ускорений.

Известно, что в приборах, не защищенных от вибрации и ударов, узлы, чувствительные к механическим перегрузкам, выходят из строя. Делать такие узлы настолько прочными, чтобы они выдерживали максимальные (действующие) динамические перегрузки, нецелесообразно, так как увеличение прочности в конечном счете приводит к увеличению массы, а вследствие этого и к неизбежному возрастанию динамических перегрузок. Поэтому считают более целесообразным использовать другие средства для снижения воздействия перегрузок [].

При проектировании электронных средств прежде всего следует выяснить, нужны ли вообще защитные мероприятия. С этой целью сравнивают оговоренные в технических условиях причины допустимых механических воздействий для предназначенных к использованию элементов (микросхем, резисторов и так далее) с величинами механических действий на объекте установки радиоэлектронных средств. При этом величины воздействующих механических факторов следует скорректировать с учетом возможного резонансного усиления колебаний по пути их распространения с места установки блока до конкретного рассматриваемого элемента. В случае, если уровни воздействующих механических факторов превышают допустимые, предусматривают защитные мероприятия с оценкой их эффективности [].

Защитные системы от наиболее распространенных видов механических помех, к которым относятся вибрации и удары, могут быть пассивными и активными. Пассивные виброзащитные системы, по сравнению с активными, более просты в исполнении и не требуют для выполнение своих функций затрат дополнительной энергии.

Существуют три пассивных способа виброзащиты аппаратуры:

- увеличение жесткости конструкции;

- демпфирование;

- использование виброизоляторов.

Плату системы кодового замка со сканером отпечатка пальца можно представить, как колебательную систему с равномерно распределенной нагрузкой. Она характеризуется собственной частотой. Поведение колебательной системы при воздействии на нее извне вибраций зависит от отношения частоты этих вибраций к резонансной частоте. Собственная частота колебаний плат зависит от формы, размеров, характера материала и условий закрепления.

Для обеспечения электромагнитной совместимости необходимы ликвидация или максимальное ослабление влияния помех, источников нежелательных сигналов на элементы конструкции. Помехой является непредусмотренный при проектировании электронных средств сигнал, способный вызвать нежелательное воздействие, выраженное в виде нарушения функционирования, искажения передаваемой информации. Помехами могут быть напряжения, токи, электрические заряды, напряженность поля и др. Источники помех весьма многообразны по физической природе и подразделяются на внутренние и внешние.

Внутренние помехи возникают внутри электронных средств. Источниками электрических помех являются блоки питания, цепи распределения электроэнергии, термопары, потенциалы, возникающие при трении.

Источниками магнитных помех являются трансформаторы и дроссели. При наличии пульсаций выходного напряжения вторичных источников электропитания цепи распределения электроэнергии, тактирующие и синхронизирующие цепи следует рассматривать как источники электромагнитных помех. Значительные помехи создают электромагниты, электрические двигатели, реле и электромеханические исполнительные механизмы устройств ввода и вывода информации электронных средств. Внутренними помехами являются помехи от рассогласования волновых сопротивлений линий связи с входными и выходными сопротивлениями модулей, которые эти линии соединяют, а также помехи, возникающие по земле.

Внешними помехами являются помехи сети электропитания, сварочных аппаратов, щеточных двигателей, передающей радиоэлектронной аппаратурой и пр., а также помехи, вызванные разрядами статического электричества, атмосферными и космическими явлениями, ядерными взрывами. Действие на аппаратуру внешних помех по физической природе аналогично действию внутренних помех.

Приемниками помех являются высокочувствительные усилители, линии связи, магнитные элементы, характеристики которых изменяются под действием полей рассеивания источников помех. Помехи могут проникать в ЭС непосредственно по проводам или проводникам (гальваническая помеха), через электрическое (емкостная помеха), магнитное (индуктивная помеха) или электромагнитное поле. Многочисленные проводники, входящие в состав любой аппаратуры, можно рассматривать как приемопередающие антенные устройства, принимающие или излучающие электромагнитные поля.

Гальваническая связь возникает в результате протекания токов и падения напряжений на электрических соединениях конструкций. Радикальным способом устранения гальванической помехи является устранение цепей, по которым проходят совместные токи питания и земли как чувствительных к помехам схем, так и сравнительно не чувствительных мощных схем. Таким образом, по проводам, связывающим модули в систему, пере­даются как полезные сигналы, так и сигналы помехи. Эффективным схемным средством селективного ослабления помехи при отсутствии ослабления и искажения сигнала является использование помехоподавляющих фильтров [].

Экраны включаются в конструкцию для ослабления нежелательного возмущающего поля в некотором ограниченном объеме до приемлемого уровня. Возможны два варианта защиты. В первом случае экранируемые средства размещается внутри экрана, а источник помех - вне его, во втором - экранируется источник помех, а защищаемая от помех аппаратура располагается вне экрана. Первый вариант используют при защите от внешних помех, второй - внутренних. В обоих вариантах в качестве экранов используются металлические оболочки [].

При выполнении линий передачи схемы печатным способом вводятся экранирующие трассы, коммутируемые с шиной нулевого потенциалаи выполняющие функции экранов проводов. Если источник помехи расположен на соседней плате, то защита схемы экранирующей трассой невозможна

В проектируемой системе кодового замка со сканером отпечатка пальца, учитывая используемую элементную базу, значительных внутренних помех, оказывающих влияние на работоспособность устройства, не должно возникать. Внешние помехи так же не должны возникать. Следовательно, дополнительных средств, снижающих количество помех, не нужно устанавливать на печатную плату.

ы