МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт энергетики и электротехники
(наименование института полностью)
Кафедра «Промышленная электроника»
(наименование кафедры)
27.03.04 Управление в технических системах
(код и наименование направления подготовки, специальности)
Системы и технические средства автоматизации и управления
(направленность (профиль)/специализация)

БАКАЛАВРСКАЯ РАБОТА

на тему Электронный замок с управлением через Wi-Fi

Студент Федин Олег Юрьевич _____
(И.О. Фамилия) (личная подпись)

Руководитель Глибин Евгений Сергеевич _____
(И.О. Фамилия) (личная подпись)

Консультанты _____ _____
(И.О. Фамилия) (личная подпись)

_____ _____
(И.О. Фамилия) (личная подпись)

Допустить к защите

Заведующий кафедрой к.т.н., доцент А.А. Шевцов _____

« » июня 2017 г.

Тольятти 2017

АННОТАЦИЯ

Общий объем выпускной квалификационной работы - 66 стр., рисунки – 39 шт.

В работе представлена система управления электромеханическим замком с помощью беспроводной технологии WI-FI.

Структура работы представлена одиннадцатью разделами, заключением и списком литературы.

Определены актуальность темы , задачи. В заключение сделаны выводы о проделанной работе.

Объект работ – система, позволяющая пользователю управлять режимом работы электромеханического замка, устройствами светового и звукового оповещения с помощью смартфона или иного электронного устройства посредством связи Wi-Fi, используя символьный идентификатор. Источником питания в данной системе служит солнечные панели.

Цель – разработать устройство более дешевое, не требующее постоянного наличия у пользователя стандартных носителей идентификатора и осуществляющее работу за счет энергии солнечных панелей.

В работе предложена структурная схема электронного устройства. Обоснованно выбраны все элементы электрической схемы. Рассмотрен алгоритм работы управляющей программы.

Представлена принципиальная схема, структурная, схема соединений и описан весь порядок разработки устройства.

Выполнен подсчет стоимости всех комплектующих для создания одного устройства. В приложении приведены перечень элементов и спецификация.

ANNOTATION

The total volume of the final qualifying work is 66 pages, Figures - 39 pcs.

Interaction with wireless networks WI-FI.

The structure of the work section eleven sections, conclusion and list of literature.

The urgency of the topic is determined. In conclusion, conclusions are drawn about the work done.

The object of work is a system that allows you to own the mode of operation of an electromechanical lock, control light and sound notification using a smartphone or other device through Wi-Fi communications using a symbolic identifier. The source of power in this system is the solar panels.

The goal is to develop a cheaper device that does not require the constant availability of standard storage media and means for providing energy to solar panels.

A block diagram of the electronic device is proposed. All elements of the electrical circuit are selected in a valid way. The considered algorithm for working program.

A schematic diagram, a structural diagram of the connections is presented and the whole order of device development is described.

Performs the calculation of the cost of all components to create one device. The annex contains a list and a specification

СОДЕРЖАНИЕ

Введение

В современном мире, в данный момент происходит быстрое развитие мобильных технологий. Техника становится все более универсальной, компактной, более производительной. Параллельно развиваются средства беспроводной связи, позволяя передавать данные быстрее и надежнее. Развитие технологий оказывает влияние на другие сферы, такие как сфера безопасности, давая ей новые оборудование и удобства.

В сфере безопасности, под мобильным доступом понимают систему, в которой для получения доступа к данным и иным ресурсам , в качестве устройства-идентификатора используется мобильное устройство. Для примера, , мобильные телефоны с беспроводным интерфейсом передачи данных NFC (near field communication, связь ближнего действия).

Основным отличием данного способа доступа является то, что тут используется мобильное устройство, а не ключи и карты доступа. Устройства с NFC позволяют расширить возможности доступа. К примеру, телефон может иметь несколько различных виртуальных карт доступа, что позволит владельцу устройства получить доступ к нескольким местам. Связь с интернетом позволяет реализовывать оперативную выдачу или отзыв карт доступа и пропусков. Это позволяет избавиться от необходимости носить с собой ключи, карты и другие средства доступа в необходимые места. Таким образом, телефон становится эффективной и удобной заменой другим устройствам.

Попытки реализовать мобильный доступ с использованием технологий NFC начались еще в 2009 году. В начале развития NFC, для хранения данных использовался защищенный элемент (Secure Element, SE), который находился в самом телефоне (мобильном устройстве) или в SIM-карте, но из-за обширной разновидности и различий спецификаций чипов, самих мобильных устройств и операторов связи было сложно найти подходящее для всех случаев решение проблемы. Появились различные промежуточные решения, но они не получили развития. Возможность реше-

ния проблемы появилась лишь в 2013 году, при проявлении Bluetooth Smart и режим эмуляции карты HCE на уровне процессора (без аппаратного чипа SE). Благодаря этим инновациям, удалось уйти от необходимости прямого взаимодействия с производителями телефонов и операторами сотовой связи и найти новое решение. Появилась система мобильного доступа от HID. Получилось эффективное, удобное, безопасное, гибкое, инновационное решение. Конечно, такая система мобильного доступа не является полной заменой классических карт доступа. Но, это может быть удобным дополнение для систем СКУД, совершенствуя ее.

СКУД – система контроля и управления доступом – это средство защиты от неправомерного доступа посторонних лиц на какую-либо территорию (предприятие), разграничения уровня доступа сотрудников во внутренние помещения. Также СКУД является эффективным средством повышения эффективности управления персоналом.

1 Актуальность систем контроля и управления доступом

По данным исследований компании HIS (американская технологическая компания по предоставлению критически важных данных, бизнес отчетов и аналитики.) годовой объем продаж СКУД в 2014 году на мировом рынке (кроме Китая) вырос на 6.3% относительно 2013 года.(Рисунок 1.1)

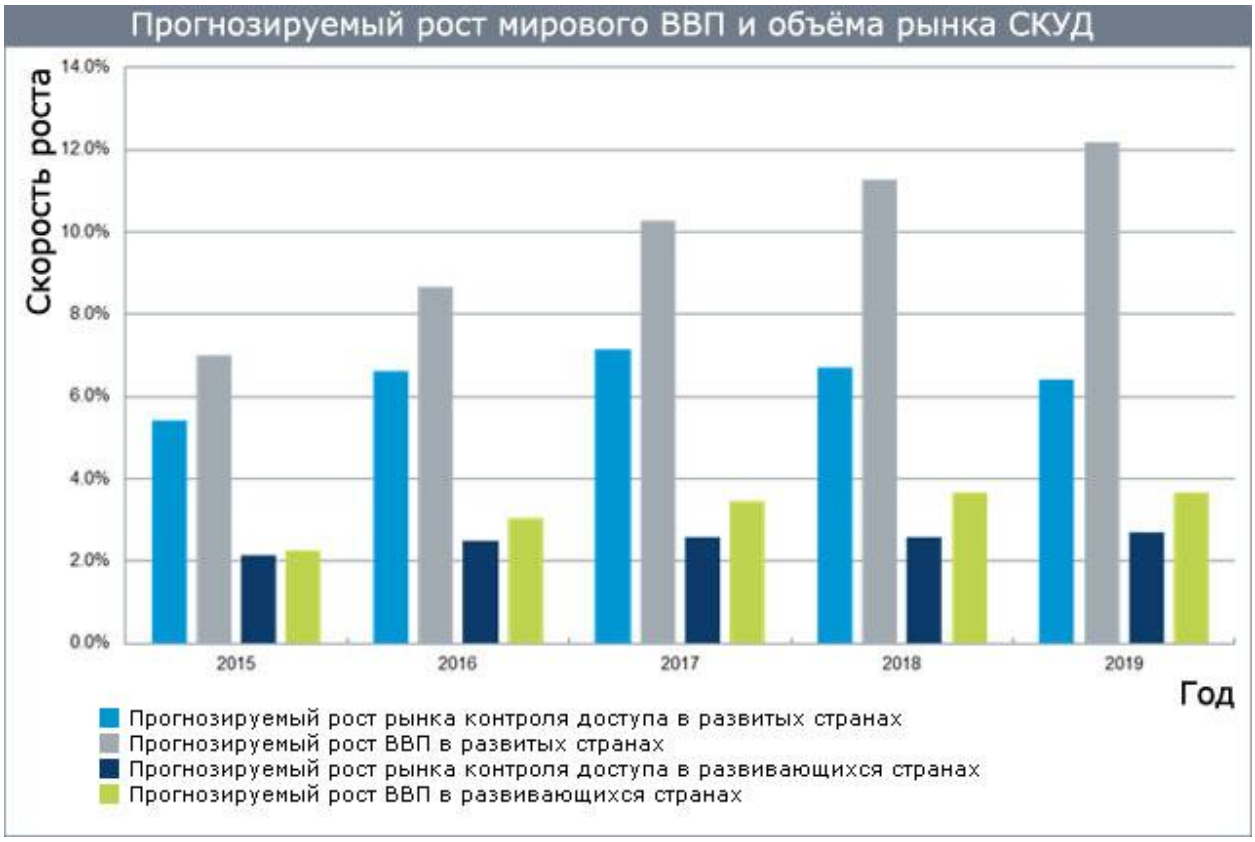

Рисунок 1.1 – Статистика роста объема рынка СКУД в мире

Российский рынок СКУД на данный момент предоставляет довольно широкий спектр продукции, при этом он постоянно обновляется и пополняется новыми технологиями. На мировом рынке доля СКУД российских производителей занимает более 50%.

СКУД выполняют не только задачи сферы безопасности, но также они могут взаимодействовать с другими системами, использующимися для обеспечения жизнедеятельности зданий и более эффективного управления компанией в других сферах деятельности. Например, система управления персоналом, коммерческие систе-

мы. Таким образом, данные об уходе и приходе сотрудником позволят более точно регулировать время работы освещения на рабочем месте, обогрева помещения, микроклимата и т.д., что, в свою очередь позволяет сэкономить до 15% ресурсов предприятия. В другом случае, те же данные могут быть использованы в кадровых и бухгалтерских службах для автоматизации расчета заработной платы сотрудника, составления графиков отпусков и смен, статистики посещаемости.

Стоит отметить активное внедрение IP технологий в данную сферу. Уже более 10 лет используются локальные вычислительные сети для передачи информации в некоторых системах контроля и управления доступом. В таких случаях часто используются интерфейсы RS-485 для объединения контроллеров в общую сеть по каналам Ethernet. С точки зрения компонентов СКУД Wi-Fi каналы могут быть отличной заменой проводного Ethernet, ведь подключенные к беспроводным точкам доступа устройства не отличат одну среду передачи от другой. При этом, данный способ передачи данных позволяет избежать трудностей с осуществлением коммуникации между компонентами системы, в отличии от использования стандартного интерфейса RS-485. По мере развития сетей Wi-Fi популярность такого способа коммуникации в системах контроля и управления доступом будет только расти, ведь данный способ по финансовым затратам заметно выигрывает у стандартных методов в связи с отсутствием необходимости прокладки проводного канала связи длиной в несколько десятков метров.

2 Основные технологии СКУД в мире

Существует несколько технологий, на которых реализованы большинство СКУД в мире:

- Технологии, основанные на бесконтактном считывании данных
- Технологии, требующие контакта носителя данных и считывателя
- Биометрические технологии

Бесконтактные карты доступа

Это особый тип карт которые используются в системах контроля и управления доступом. Особенность таких карт заключается в том, что они работают удалено от считывателя данных и их не требуется позиционировать каким либо образом, а достаточно просто иметь при себе. На рисунке 2.1 изображены части, из которых состоит карта. Карты состоят из антенны для приема сигнала и чипа. Принцип действия таков: Устройство для считывания данных с карты постоянно генерирует электромагнитный сигнал определенной частоты. Если в поле распространения данного сигнала появляется карта, то, под действием сигнала антенна создает ЭДС, силы которой достаточно чтобы запитать чип в карте. В данном чипе находится определенный код доступа. Далее, с карты на считыватель приходит электромагнитный сигнал определенной формы и частоты с самой карты , который несет идентификационный код .

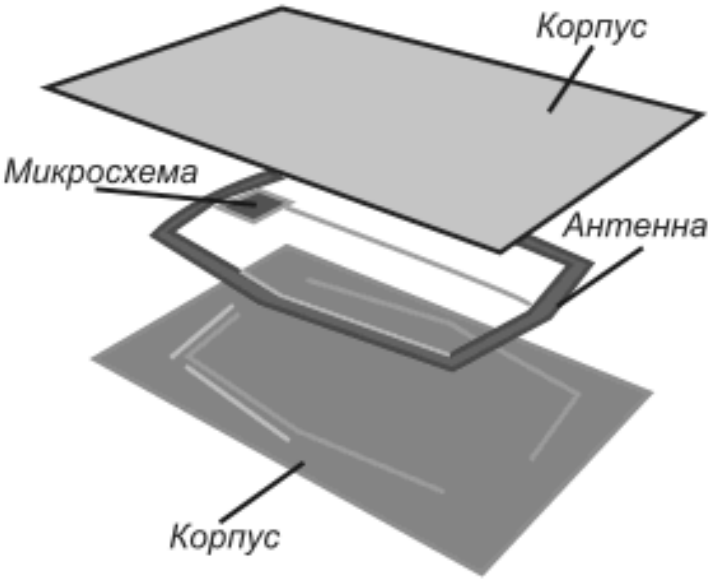

Рисунок 2.1 – Строение бесконтактных карт

В качестве носителя (передачи) данных могут служить не только электромагнитные волны , но и инфракрасное излучение и ультразвук. Устройство для считывания может находиться на стене с дверью, на самой двери, в помещении. Расстояние, на котором происходит считывание данных может быть в пределах от нескольких сантиметров , да нескольких метров. Следовательно, нет необходимости доставать карту, позиционировать каким либо образом у считывателя и тд. Ее можно носить под одеждой или в сумке, ведь сигнал будет проникать через ткань и кожу.

Очень распространены бесконтактные жетоны и метки. Это электронные карты со встроенной схемой. В схеме записан личный код владельца, который забит в базе данных. Другое название этих карт- **proximity (RFID)** карты. Они бывают активные и пассивные.

Пассивные эл. карты не имеют источника питания и их срок службы практически не имеет конца. Но у них малый радиус действия. От десяти до пятидесяти сантиметров. В активных картах присутствует элемент питания, и радиус действия карт 1-3 метра, но элемент питания необходимо периодически менять и контролиро-

вать уровень заряда. Также, они более хорошо защищены, по сравнению с пассивными.

Когда говорят про защищенность и уязвимость данных с бесконтактных карт доступа, определяют три направления.

- Незащищенность конфиденциальных данных
- Повторное воспроизведение
- Копирование карт.

Незащищенность конфиденциальных данных подразумевает, что данных с карты могут быть считаны злоумышленниками и тем самым получить не только данные для доступа, но и всю информацию о владельце карты.

Повторное воспроизведение означает, что при очередном запросе доступа, данные с носителя могут быть скопированы и, в будущем, быть использованы злоумышленниками для доступа. В качестве защиты поможет проверка подлинности считывателем данных с карты.

Копирование данных – в случае, если данные с карты хранятся в незащищённой базе, то они могут быть скопированы. Таким образом, появится клон карты. Также, на современном рынке легко приобрести такой прибор как “дубликатор”. С его помощью можно быстро и просто считать информацию с карты. Для этого надо приблизиться к карте, далее, прибор имитирует сигнал со считывателя и получает ответный сигнал, содержащий нужный идентификатор.

Бесконтактные Smart-карты

Существуют **бесконтактные Smart-карты.** Это относительно новая технология, тем не менее, завоевала большую популярность у автолюбителей. Эта технология отличается от proximity карт следующими признаками:

- Большим объемом памяти, для доступа к которой требуется ключ.

- Для защиты от клонирования карты, у каждой карты есть свой индивидуальный номер.
- Более надежный способ аутентификации между картой и считывателем.

Самый существенный минус данной технологии перед Proximity картами- это более высокая стоимость smart карт. Скорее всего, данная технология в будущем заменит Proximity карты. На рисунке 2.2 изображена структурная схема smart карт

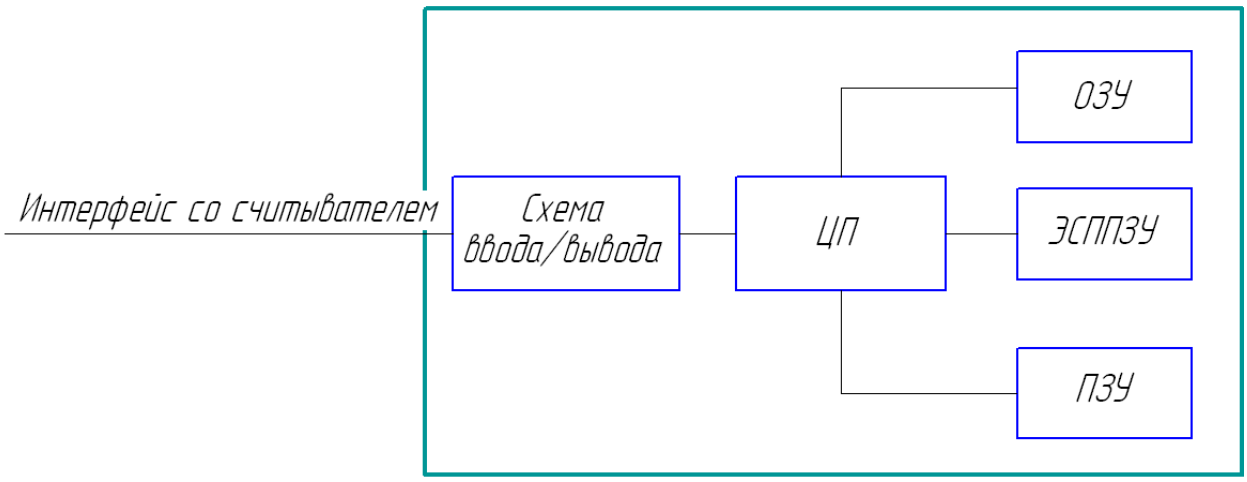

Рисунок 2.2 – Структурная схема Smart карт

Магнитные карты

Данные карты очень распространены в финансовой сфере, нежели в охранной. Считывание информации происходит путем проведения карты через считыватель. Причина, по которой данная технология не получила распространения в Системах контроля и управления доступом- это то, что информация при данной технологии легко стирается и перезаписывается. Это не допустимо в СКУД. Рисунок 2.3 показывает общее изображение магнитных карт.

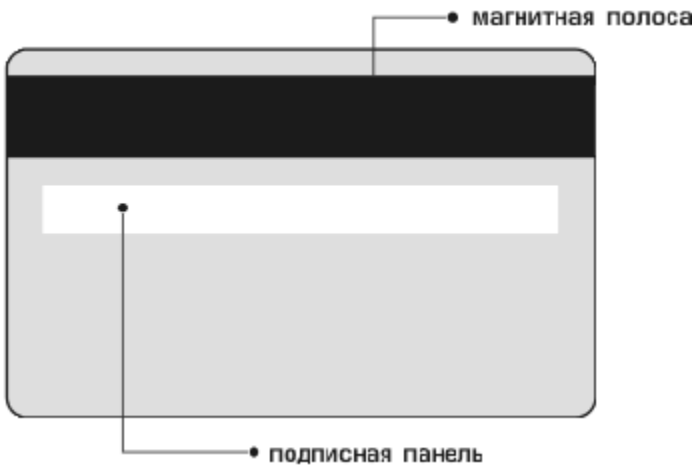

Рисунок 2.3 – Пример магнитной карты

Штрихкодовая технология

Существует также и штрихкодовая технология. Данная технология получила широкое распространение в сфере торговли. В системах контроля и управления доступом данная технология применяется редко из за возможности легко скопировать сам штрих код. Данная технология не поддерживает возможность перезаписи и стирания данных.

Wiegand – технология

Промежуточным звеном между штриховой и магнитными технологиями, и бесконтактными, стала Wiegand – технология. В наше время она очень распространена повсеместно. От магнитных карт она отличается тем, что у Wiegand отсутствует магнитная полоса. Вместо этого карта передает сигнал посредством электромагнитного поля, в ответ на сигнал считывателя (необходимо поднести карту очень близко к считывателю). Отсюда следует, что нет необходимости непосредственного физического контакта со считывателем, поэтому карта будет меньше изнашиваться и дольше служить. Данные карты могут стабильно работать при температурах от минус сорока до плюс семидесяти градусов. Также, носителем идентификатора может быть не только карта, но и брелок или ключ. Данная технология имеет доста-

точно низкую стоимость, устойчивость к помехам, долговечность и достаточно высокий уровень защищенности данных.

Биометрические технология

Данная технология подразумевает считывание индивидуальных биометрических параметров человека. На данный момент на рынке присутствуют данная технология, идентифицирующая человека по отпечаткам пальцев, чертам лица, радужке глаза, голосу, ладони и тд. Данные системы используют статические средства, имеющие вероятностный характер. Следовательно, каждое считывание параметра может каждый раз изменяться и, возможно, допускать ошибки. Из достоинств таких систем можно выделить довольно сложные алгоритмы идентификации. Соединив несколько таких систем в единую систему, можно создать СКУД, которая удовлетворит строжайшие требования защиты. На рисунке 2.4 показаны основные элементы биометрической СКУД

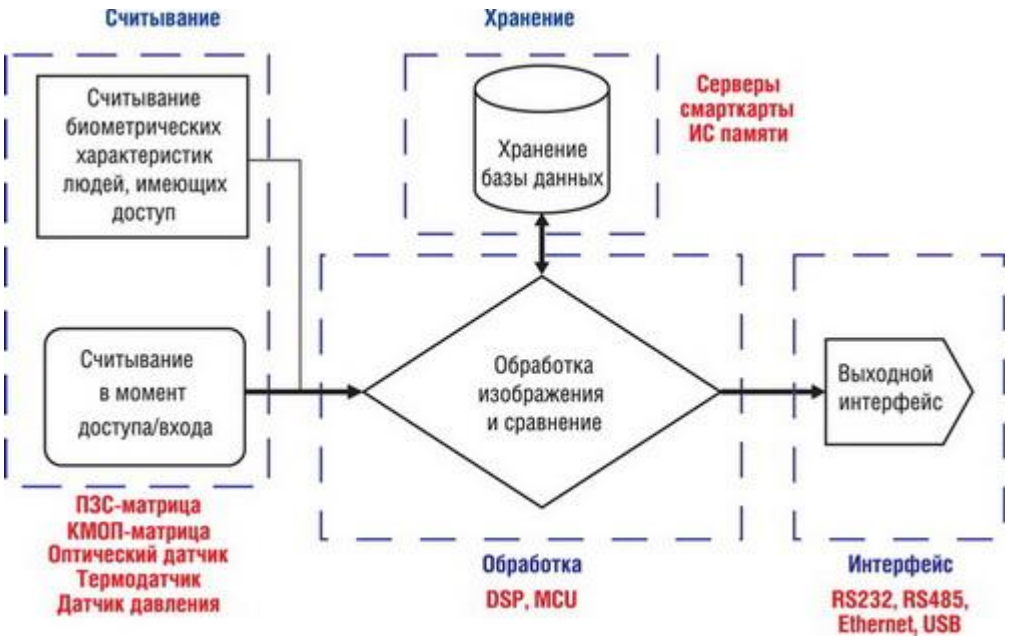

Рисунок 2.4 - Основные элементы биометрической СКУД

2.1 Обзор систем контроля и управления доступом на рынке РФ

Система контроля и управления доступом (СКУД) от компании PERCo

Компания **PERCo** производит СКУД для решения широкого спектра задач: локальные СКУД (для одного помещения), сетевые (СКУД, рассчитанные на несколько помещений). СКУД включает в себя большой спектр оборудования. Контроллеры управления доступом, считыватели, турникеты, калитки, замки.Для прохода мимо СКУД, чаще всего используются карты доступа. При опознании карты контроллеры либо запрещают, либо разрешают вход/выход.

Электронные кабинеты **PERCo** - это пример локальной СКУД. Данная система позволяет владельцам какого либо помещения (кабинет, квартира) удаленно осуществлять контроль доступа на территорию. Например, принятие посетителей в кабинете.

Электронные проходные - это готовые решения, которые сделают организацию системы контроля доступа на проходных предприятия максимально быстрой и удобной. Данная система представляет собой турникеты, с уже установленной СКУД внутри. На рисунке 2.1.1 изображена электронная **проходная** КТ08.3А**.**

Рисунок 2.1.1 - Электронная проходная КТ08.3А

К сетевым системам относится СКУД S-20. Это система, которая позволяет контролировать и управлять доступом на всем предприятии. Данная система удовлетворяет всем требованиям безопасности**.** На рисунке 2.1.2 представлен структурный состав системы S-20.

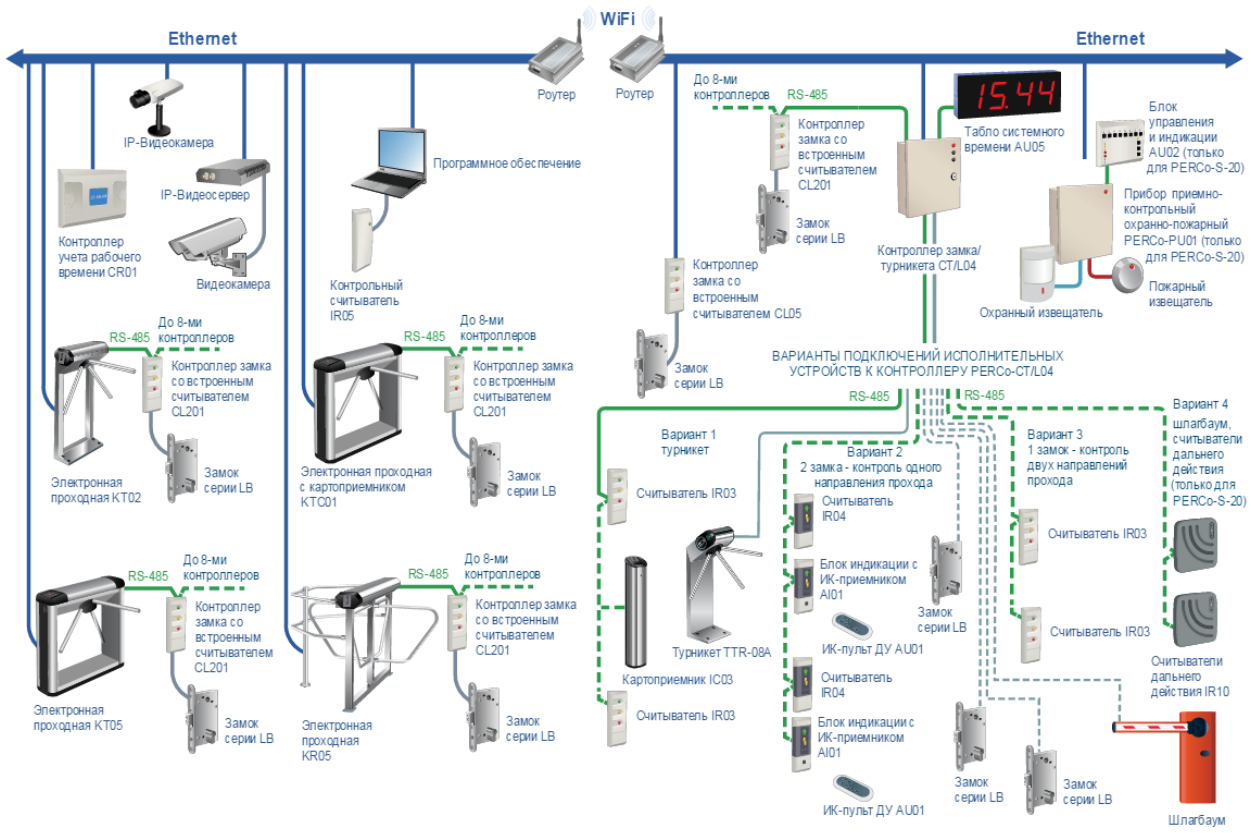

Рисунок 2.1.2 – Структурный состав системы S-20

Преимущества СКУД S-20:

- Возможность работы в автономном режиме без постоянной связи с ПК.
- Не зависящее от питания хранение данных для доступа и данных событий в контроллерах системы.
- Возможность разделения уровней доступа в зависимости от помещений, времени.
- Наличие поддержки сменных графиков.
- Наличие защиты от передачи карты

Система контроля и управления доступом S-20 включает в себя сеть контроллеров и компьютеров. ПК и контроллеры поддерживают связь через Ethernet.

Использование IP-технологий в системах контроля и управления доступом позволяет воспользоваться огромным выбором типовых решений, сформированным в компьютерных сетях, обеспечивает надежность самой системы.

Основным же преимуществом системы контроля и управления доступом S-20 является то, что можно использовать одно и тоже оборудование для решения широкого спектра задач. Так, у примеру, информация, которая поступает в системы доступа может в дальнейшем использоваться в других системах, не связанных с охранной сферой. Например, Данные о том, что сотрудники прошли систему контроля и времени данного события сохраняются в памяти контроллеров, которые, в свою очередь находятся в самом турникете. Эти данные могут в дальнейшем использоваться при составлении отчетов по труд. дисциплине и табеля учета рабочего времени. На основании табеля начисляется заработная плата сотруднику. Существуют системы контроля и управления доступом, которые разрабатываются, ориентируясь на особенности здания предприятия.

Примером таких систем может служить **PERCo S-20 “Школа”**. Эта система была создана для обеспечения безопасности в школах и других учебных заведениях. Данная система контроля и управления доступом, помимо предотвращения проникновения и присутствия на территории учреждения посторонних лиц, оповещает родителей о приходе и уходе из школы или другого учебного учреждения учащегося через SMS оповещение. В системе контроля и управления доступом “Школа” могут использоваться электронные проходные от компании **PERCo,** либо любые другие турникеты с устройствами для считывания данных с карт доступа.

Возможность размещения системы контроля и управления доступом **PERCo S-20 “Школа”** в школах и других учебных заведениях подтверждена Противопожарной службой МЧС России. Система контроля и управления доступом транспорта “Автотранспортная проходная ”- это система для контроля проезда транспорта (личного и общественного) на территории предприятий.

Терминал учета рабочего времени- это система автоматизации учета рабочего времени и дисциплины труда. Данная система может быть установлена в зданиях компаний, предприятиях и местах, где места работы сотрудников находятся на удалении от проходной. Также, для обеспечения безопасности работы граждан с банкоматами, существует система контроля и управления доступом «Система ограничения доступа к банкомату». Данная система обеспечивает безопасность осуществления различных операций с наличностью в банкоматах, от негативно настроенных и различных потенциально опасных личностей.

Данная система контроля доступа состоит из кабины, в которую помещается банкомат и электромагнитного замка для данной кабины. Для того, что бы открыть или закрыть дверь кабины используется банковская карта. Сигнал поступает на контроллер, который, в свою очередь, принимает решение для открытия и закрытия замка. Также, контроллер управляет тало с информацией и сигналом тревоги.

Системы контроля и управления доступом в помещении используются для осуществления доступа определенного круга лиц (сотрудников, гостей) в какое-либо помещение и для предотвращения доступа туда посторонних лиц. Для этого применяется электромагнитный замок, который устанавливается на дверь. Со внешней стороны двери размещается устройство для считывания информации с носителя (карты). Внутри помещения устанавливается контроллер. Используя различное программное обеспечение для данной системы контроля и управления доступом можно использовать данную систему и в других направлениях, отличных от сферы безопасности. Как пример, использовать данные о проходе тех или иных лиц для учёта рабочего времени и повышения дисциплины труда. Примечательно, что в этом случае нет необходимости использовать другое оборудование, либо закупать дополнительное.

Если организация имеет несколько помещений, то система контроля и управления доступом в помещения может контролировать сразу несколько дверей, тем самым обеспечивая безопасность доступа сразу в несколько помещений. На пред-

приятии возможно построение Единой системы S 20. В неё, помимо систем доступа, могут входить система видеонаблюдения, противопожарная сигнализация и система повышения эффективности предприятия. Все элементы Единой системы S 20 взаимодействуют посредством связи Ethernet. Помимо оптимального подхода к стоимости монтажа и прокладке кабеля, это обеспечивает бесперебойность работы оборудования и связи, что в свою очередь, положительно отражается на стабильности работы всей Единой системы. Системы контроля и управления доступом PERCo созданы для автоматизации как можно большего количества процессов на предприятии в сфере труда и охраны.

Средняя цена каждой из систем на 10.02.2017 составляет **213060** руб.

Система контроля и управления доступом «Сфинкс»

СКУД «Сфинкс» для офиса позволит покупателям контролировать доступ в помещение при небольших затратах. Контроль доступа осуществляется по бесконтактным картам.

Основные функции данной системы:

- Контроль доступа по времени
- Учет рабочего времени
- Совместимость с 1С-Предприятие
- Фотоидентификация (всплывающая фотография сотрудника на экран)
- Редактор граф. оформления пропусков
- Возможность отправки SMS уведомления о событиях

На рисунке 2.1.3 представлена структурная схема системы

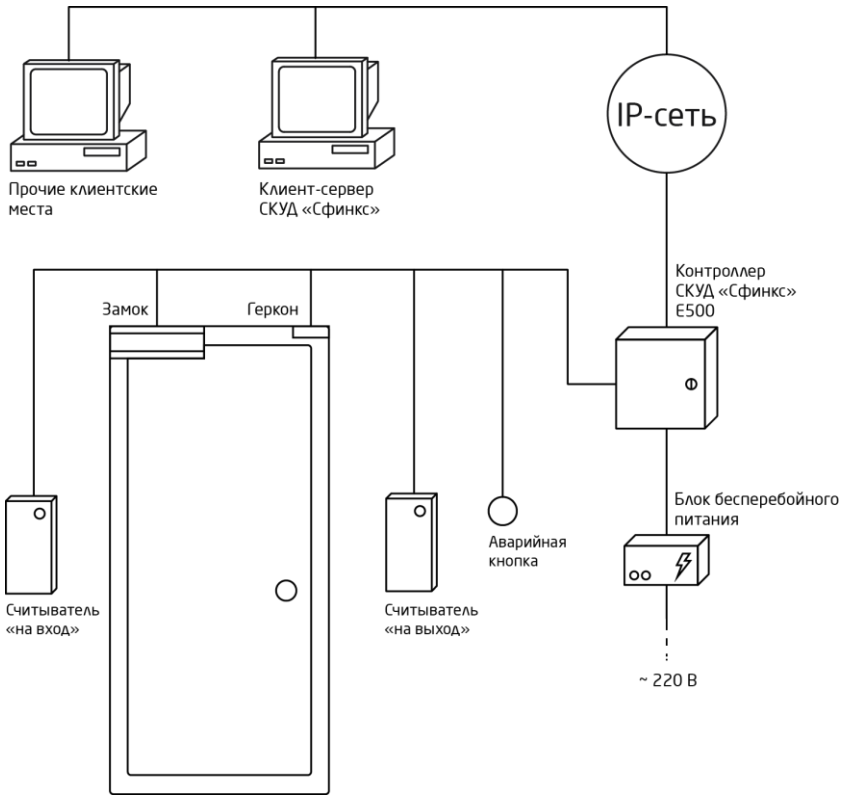

Рисунок 2.1.3 - Структурная схема СКУД «Сфинкс»

Данная система имеет следующий набор комплектующих:

- Сетевой контроллер «Sphinx E500».
  Интерфейс связи Ethernet
- Считыватель карт EM-Marine
- Блок питания бесперебойный 12В, 2А (ББП-20)
- Аккумулятор CSB 12В, 7 а*ч
- Замок электромагнитный М1-300,
  усилие удержания 300 кг
- Датчик магнито-контактный скрытой установки
- Кнопка аварийной разблокировки
- ПО Сфинкс «Малый Офис»,
  ограничение до 50 карт доступа

Стоимость данной системы на 10.02.2017 составляет **24350** руб.

СКУД разработанная в университете Чосон в Южной Кореи

Описанная ниже система была разработана в Университете Чосон в городе Кванжоу, Южной Корее. Автор статьи: Sadeque Reza Khan.

В университете Чосон в Южной Кореи разработали гибкую и недорогую модульную систему, основанную на интеграции клавиатуры, магнитного замка и контроллера и 8-и разрядного контроллера PIC 16F876A, который является главным контроллером в этой системе. Усовершенствованное моделирование на компиляторе Flowcode V4 использовано для разработки программной части этого проекта.

Основная цель системы управления доступом в офисе является обеспечение доступа к контролируемой зоне только тем лицам, которым разрешен доступ. Контролируемая дверь- это не единственный (самостоятельный) элемент в системе , а комплекс технического обеспечения, который обычно включает в себя выходы управления, такие как: замок, держатель двери, звуковой оповеститель и т.д. А также, входы под наблюдением, такие как: контакты, запросы на выход, детекторы движения и т.д. Система контроля доступа играет роль проверки и посредника попыток пользователей получить доступ к ресурсам системы. Система контроля доступа отображает деятельность и ресурсы для законных пользователей. Главная цель данной работы- это разработать автоматизированную и недорогую офисную систему контроля и управления доступом с помощью микроконтроллера. Автоматизация- это использование систем контроля и информационных технологий для уменьшения потребности в человеческом труде для производства товаров и сервисе. Клавиатура используется для ограничения доступа лицам, а соответствующий пароль предусмотрен для каждого индивидуально. Таким образом, правильный пароль гарантирует проход через дверь, запертую на электромагнитный замок. В противном случае, система сворачивается и звучит сигнал тревоги. LCD экран соединен с главным контроллером. Он показывает статус, когда пользователь вводит соответствующий пароль.

На рисунке 2.1.4 обобщенно показана предложенная система , где главный контроллер получает пользовательский пароль, введенный с клавиатуры. Если пароль верен, то система разрешит доступ этого пользователя к контролируемой электро замком двери. Для неправильного пароля система оповестит защитной сиреной.

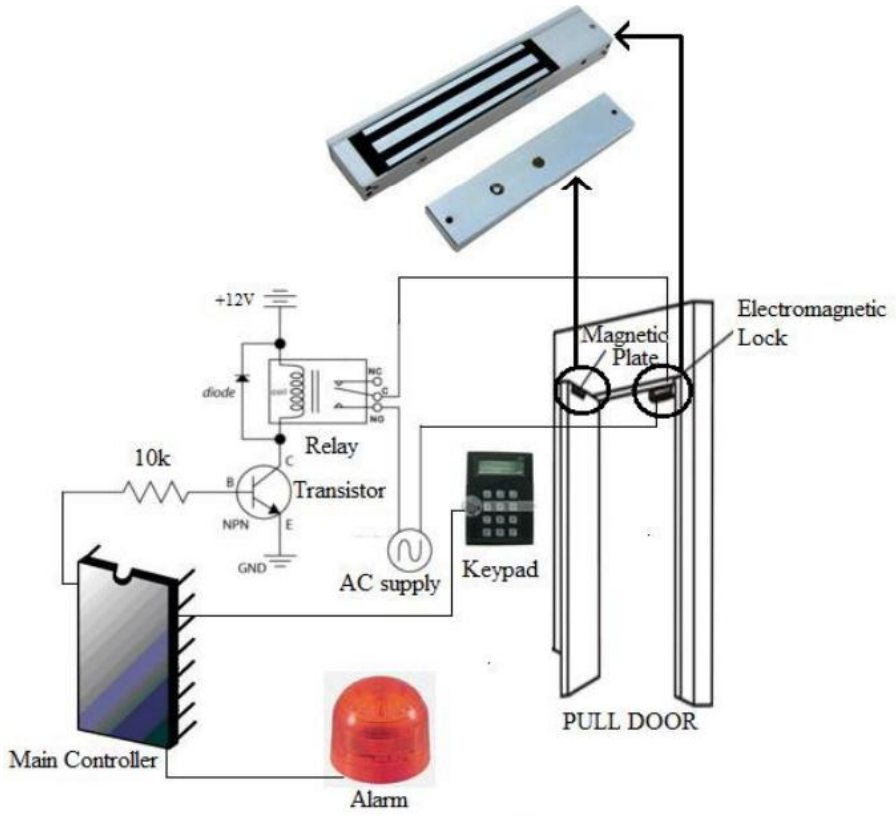

Figure 1. Proposed System.

Рисунок 2.1.4 - Структурная схема системы

Техническое обеспечение

Главный контроллер

Модуль управления построен на основе микроконтроллера MC. Центральный контроллер это микрочип PIC16F876A, который является 8-битным контроллером с пятью встроенными каналами и 22 портами входа/выхода. Этот контроллер управляет всеми операциями. Он принимает пароль с клавиатуры, обрабатывает его и решает, является ли он рабочим или нет. Одним из преимуществ микроконтроллеров

является низкое потребление энергии, благодаря технологии CMOS, что делает их гибкими для выбора источника питания, а также обеспечивает широкий диапазон рабочего напряжения. Например, PIC16F876A работает в диапазоне напряжений 2-2.5 вольт.

Дисплей

Блок дисплей использует двустрочный, 16-и символьный алфавитно-цифровой жидкокристаллический экран (LCD), который может быть сопряжен с 4-8 битным микроконтроллером или микропроцессором.

Клавиатура

В этом проекте используется клавиатура 4x3. Клавиатура - просто массив кнопок, соединенных в строки и столбцы, так что каждый может быть протестирован на замыкание с минимальным количеством соединений. Ключевое нажатие сканируется путем последовательного уменьшения каждой строки X и определения столбца Y с низким уровнем, чтобы идентифицировать каждую клавишу в матрице.

Электромагнитный замок

Магнитный замок использует электрический ток для создания электромагнитной силы. Когда ток пропускается через катушку, магнитный замок становится намагниченным. Дверь надежно закрепляется, когда электромагнит запитан, держась за пластину якоря. Магнитный замок представляет собой простое запирающее устройство, которое состоит из магнитного замка и пластины якоря без движущихся частей, и оно чисто работает из-за магнитного поля.

Сигнализация

Электрическая сирена подключается к выходу микроконтроллера PIC через реле для генерирования сигнала тревоги при вводе трех последовательных ошибочных введенных паролей.

Система контроля и управления доступом основанная на RFID технологии

Данная система разработана в Университете Пенджаба, город Лахор, совместно с Университетом Гуджрата, в городе Гуджрат и Университета Пенджаба, город Пенджаб. Пакистан. Авторы статьи: Umar Farooq, Usman Asad, Athar Hanif.

Далее представлена система контроля доступа, основанная на RFID защите для использования в хостелах, находящихся на территории Университета Пенджаба**.** Система сочетает в себе RFID и биометрическую технологию для выполнения требуемой задачи. Когда считыватель RFID меток, установленный на входе в хостел обнаруживает номер (идентификатор), система захватывает изображение пользователя и сканирует базы данных какое-то время. Если оба: номер метки и захваченное изображение, принадлежит зарегистрированному пользователю, то вход разрешается. В противном случае включается сигнал тревоги и делается тревожный сигнал охране через GSM модем. В этом случае подозрительная персона может быть поймана.

Автоматическая идентификация и системы контроля доступа возникли в связи с необходимостью преодоления угроз для безопасности, с которыми сталкиваются многие организации в Пакистане. Установка систем на входе позволит проходить через них только определенным лицам, относящихся к организации. Система также имеет возможность установки точек внутри организации, для отслеживания перемещения людей и запрещать их доступ в определенные места в организации. В таком случае подозрительные лица могут быть пойманы, что в свою очередь повысит уровень безопасности организации.

Радиочастотная идентификация- это технология беспроводной передачи, которая может быть использована для развития систем контроля доступа. В литературе показано использование этой технологии для различных процессов начиная от производственного сектора, до управления домом. Бо Ян сообщил об использовании

RFID технологии для автоматизации системы управления выдачи отслеживающих карт. Аппаратные средства системы состоят из: карты с RFID меткой, считывателя RFID, компьютерного терминала, оптоволоконного кабеля, сервера, и контроллера. Электронный носитель (билет, карта) содержит SDES зашифрованную форму данных, которая включает номер научного региона, номер носителя, дату носителя, серийный номер и номер проверки. RFID считыватель читает данные внутри электронного носителя и передает в компьютерный терминал и сервера через оптоволоконную сеть. Данные расшифровываются в самом терминале и там же проверяется их подлинность. Затем контроллер дает разрешение на вход. Эта система идентификационных и аутентификационных процессов осуществляет три подуровня (подсистемы), а именно: подсистема продажи, подсистема принятия решения и подсистему управления. Все эти системы осуществляют связь друг с другом через информационную базу данных. G. Ostojic разработал систему контроля автоматической парковки автомобиля, основанную на RFID технологии для города Нови-Сад, Республики Сербия. Техническое оснащение системы состоит из RFID метки и считывателя, работающих на частоте 13.56 Мгц для аутентификации, металлодетекторной арки, ёмкостного датчика подсчета транспортных средств, модема Siemens MC 39i GPRS для осуществления связи между воротами входа и выхода, а также программируемого логического контроллера (ПЛК) FEC FC440, который является сердцем всей системы. Когда автомобиль останавливается на металлодетекторной арке, RFID считыватель читает метку. Данные на метке включают в себя уникальный идентификационный номер, период действия метки и проверочный бит для проверки статуса парковки. Эта информация используется в ПЛК и доступ предоставляется для парковки автомобилей если информация с метки содержит правильный идентификационный код, период действия и парковочный статус. После того, как автомобиль поступил на парковочное место, его RFID статус будет изменен для чтения/записи, чтобы не допустить проезд другого транспортного средства с такой же картой. Аналогичная процедура повторяется когда автомобиль покидает парковочное средство.

Нова Ахмед описала систему управления и мониторинга в помещениях, основанную на RFID технологии, известную как GuardianAngel в повсеместной среде. Красота системы заключается в том, что она может генерировать динамические запросы в режиме реального времени через пользовательский интерфейс. Среда в системе оснащена RFID-метками и разделена на различные зоны. Промежуточное программное обеспечение системы разделено на два уровня: уровень руководства и уровень контроля. Уровень контроля представляет из себя карманный считыватель RFID, чтобы периодически предоставлять информацию о местоположении на уровне мониторинга. Таким образом, уровень мониторинга имеет информацию о всей среде. Экспериментальные результаты показали, что система почти на 100% точна в обеспечении зональной информации, что позволяет создавать очень надежные средства управления и мониторинга. Kuo-shien Huang описал подход на основе бизнес-модели для использования технологии RFID в автоматизации процесса в соответствии с стратегическим видением и целями предприятия. Автор разработал бизнес-модель системы проката велосипедов и использовал технологию RFID для внедрения системы. Обычный способ получения велосипеда в аренду, который включает запись данных о клиенте пером, а затем ввод данных на компьютер заменяется предоставлением клиенту RFID-карты и фиксацией метки RFID на велосипеде. Велосипед помечается, чтобы отслеживать его местоположение от арендованного магазина до магазина возврата. Информация делится между магазинами через веб-интерфейс. Таким образом, построена и внедрена успешная стратегия RFID.

Из всего вышенаписанного можно сделать вывод о том, что практически все предлагаемые на сегодняшний день решения для создания систем контроля и управления доступом, вне зависимости от сфер их применения и возложенных на них функций, подразумевают:

- Постоянного наличия у пользователя переносного идентификатора (карты, брелоки, метки и т.д.)

- Необходимость наличия какого-либо стационарного источника питания. В основном это электрическая сеть 220В, а следовательно, наличие трудностей при монтаже данных систем в местах, где электрическая сеть отсутствует.

В данном проекте спроектирована система контроля и управления доступом, основанная на управлении электромеханическим замком, а так же световым и звуковым устройствами оповещения с помощью WI-FI сигнала, с использованием в качестве устройства доступа смартфон пользователя.

Также, питание данной системы осуществляется с помощью солнечных панелей, что снимает потребность в наличии электрической сети в месте монтажа.

3 Разработка структурной схемы устройства

На рисунке 3.1 представлена структурная схема электронного замка с управлением через WI-FI.

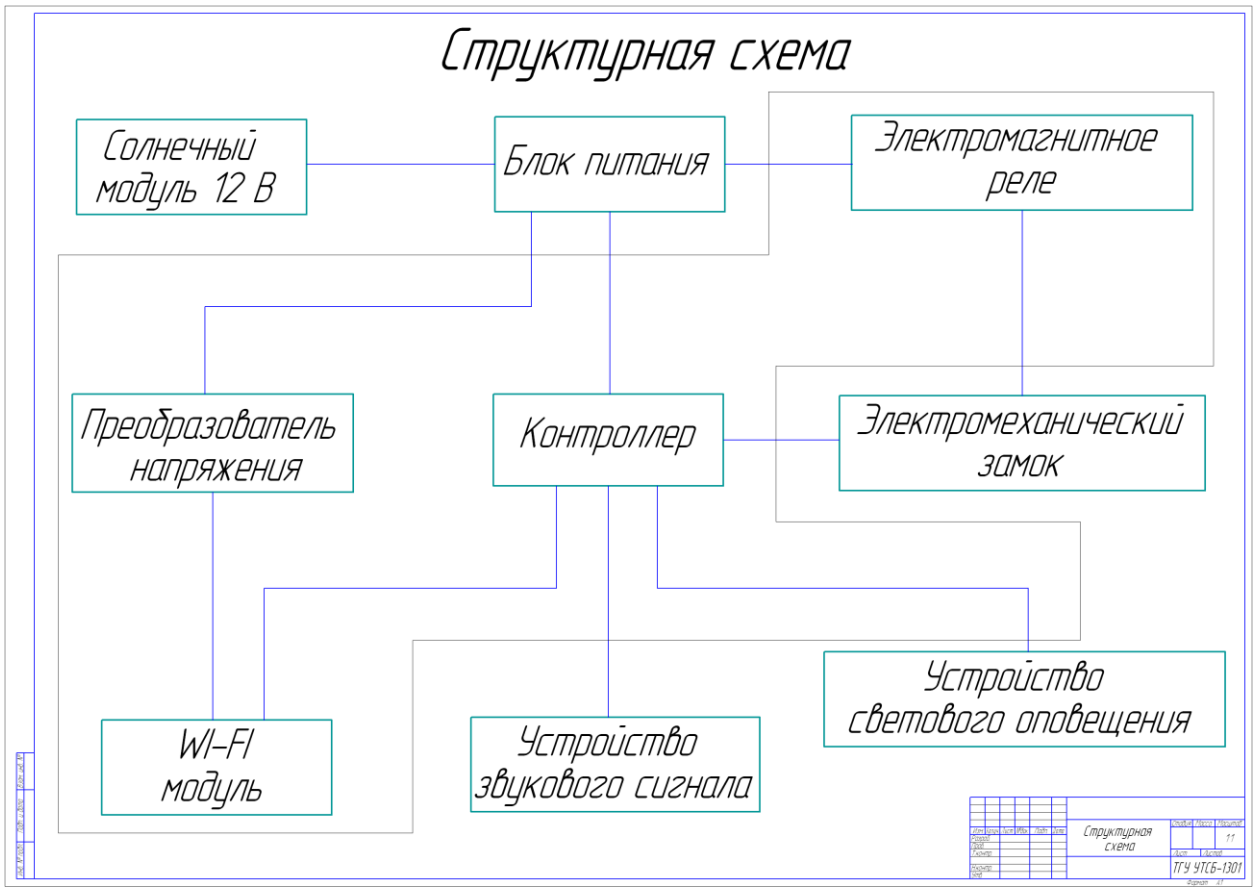

Рисунок 3.1 –Структурная схема электронного замка с управлением через WI-FI

Питание системы осуществляется от 10 солнечных модулей, которые должны быть установлены на месте, доступном для солнечного света. Данные модули в свою очередь заряжают блок питания, который состоит из 8 литиевых аккумуляторов. Для осуществления беспроводной связи устройства ввода данных пользователя и системы управления и контроля доступом будет использоваться WI-FI модуль. Так как WI-FI модуль работает с напряжением 3.3 Вольта, то будет использоваться преобразователь напряжения 12-3.3 Вольт, для преобразования 12 Вольт блока питания в 3.3 Вольт для питания модуля. Также, выводы модуля подключаются к выходам

RX и TX контроллера через делитель напряжения. Для воспроизведения звукового и светового сигналов будут использоваться пьезодинамик и светодиоды, подключенные непосредственно к рабочим выходам контроллера. Объектом управления данной системы является электромеханический замок. Для управления электромеханическим замком потребуется электромагнитное реле, замыкающее цепь из замка и блока питания, т.к. выходного напряжения контроллера не хватит для управления замком.

4 Выбор электронных компонентов

- Arduino UNO на базе процессора ATmega328
- Wi-Fi модуль ESP8266-01
- Электромагнитное реле srd-05vdc-sl-c
- Солнечный модуль 6В, 1 Ватт фирмы ANBES – 10 шт.
- Литиевые аккумуляторы 18650 3.7В, 2600 мАч – 8 шт.
- Электромеханический замок «ШЕРИФ-3В.У»
- Пьезоизлучатель звука HPA17A 5 5В, 25мА
- Светодиод зеленый 510PG2C 3В, 20мА
- Светодиод красный 510HR3C 2.6В, 20мА
- С1-4 резистор 0,25 Вт, 5%, 430 Ом
- С1-4 резистор 0,25 Вт, 5%, 150 Ом
- С1-4 резистор 0,25 Вт, 5%, 220 Ом
- С1-4 резистор 0,25 Вт, 5%, 100 Ом
- Диод 1N4007 1А, 1000 В.
- Преобразователь напряжения AMS1117
- Батарейный кейс для аккумуляторов 18650 – 4 шт.
- Макетная плата 200X150

В данной системе контроля и управления доступом в роли устройства принимающего решение, относительно разрешения или запрета доступа в помещение, используется Arduino UNO на базе микроконтроллера ATmega 328 (рисунок 4.1).

Выбор именно микроконтроллера, а не одноплатного компьютера обосновывается поставленной перед системой задачей, а именно управлением электромагнитным замком. Так как микроконтроллеры могут выполнять только одну задачу, заданную программой пользователя, в нашем случае это управление замком, а одноплатные компьютеры исполняют несколько программ в рамках операционной системы, то нет необходимости использовать данные более сложные, мощные и доро-

гостоящие платформы. Поэтому в данном проекте будет использоваться микро-контроллер Arduino UNO. Также, платформа Arduino имеет очень удобную среду программирования Arduino IDE, которая имеет монитор порта, с помощью которого можно управлять WI-FI модулем посредством АТ-команд.

От контроллера нам потребуется четыре цифровых выхода. Три выхода- для подачи сигнала 5 Вольт на устройства светового и звукового оповещения и один- для подачи сигнала на электромагнитное реле. Для обмена данными с WI-FI модулем будут использоваться RX-TX выходы. Также, необходим выход GND. Сама плата должна питаться от напряжения 12 Вольт. Исходя из вышенаписанного, лучшим выбором будет плата Arduino Uno. Конкурентом ей может стать плата Arduino Due, но данная плата проигрывает Uno по цене, при этом имеет дополнительные функции, не востребованные в нашем проекте. На рисунке 4.1 изображена плата Arduino Uno.

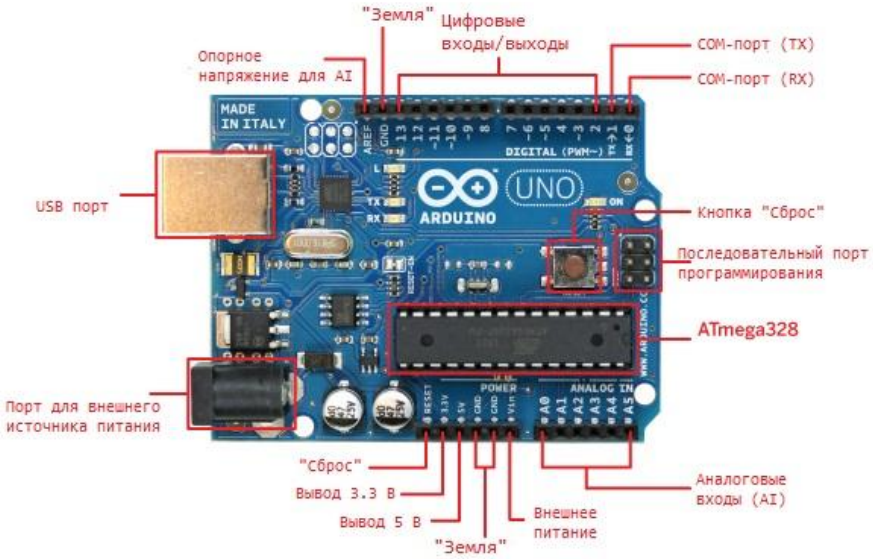

Рисунок 4.1- Плата Arduino Uno

Максимальный ток на выходах Arduino Uno составляет 40мА. Этого недостаточно для управления WI-FI модулем ESP8266-01, который может потреблять от 62 до 215 мА, в зависимости от режима работы. Следовательно, его нельзя подключить для питания к выходу 3,3 Вольт контроллера. Но, можно подключить данный модуль к

блоку питания системы, предварительно понизив напряжение до 3,3 Вольт, необходимых для питания модуля. Для решения этой проблемы можно воспользоваться преобразователем напряжения AMS1117 он преобразует напряжение 12 Вольт в 3.3 Вольт. Данный модуль может выдавать при 3,3 Вольтах ток до 1 А. При этом, максимальное входное напряжение может достигать 18 Вольт. На рисунке 4.2 изображен преобразователь AMS1117.

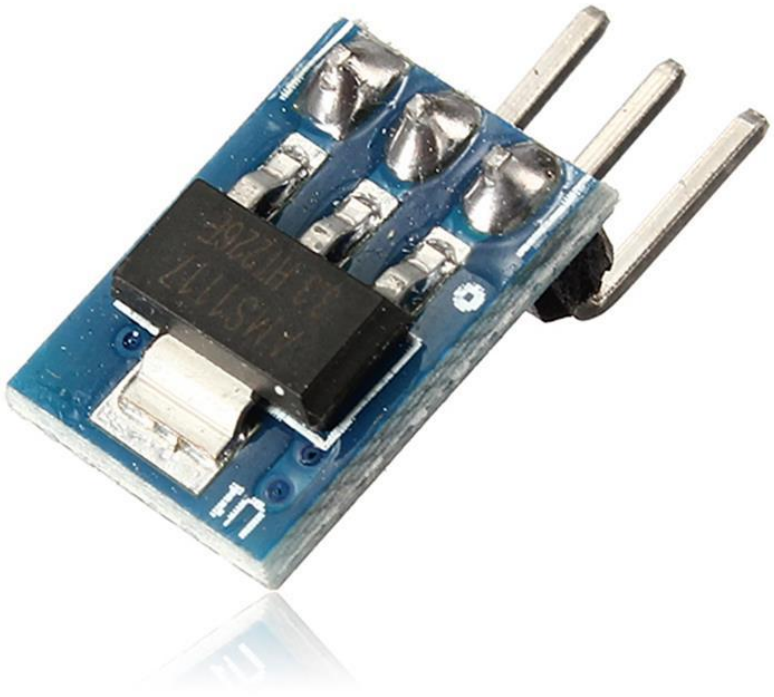

Рисунок 4.2- Преобразователь напряжения AMS1117

С помощью WI-FI модуля esp8266-01 в нашей системе контроля и управления доступом осуществляется связь между пользовательским устройством ввода данных для открытия замка и контроллером Arduino Uno. На рисунке 4.3 представлен внешний вид модуля ESP8266-01. На современном рыке существуют аналоги данного

модуля, например, MediaTek MT7681. Из его плюсов можно выделить его сравнительно маленькие габариты (5 х 5 мм), и наличие UART, SPI, GPIO портов. Однако его использование затрудняется его высокой, относительно аналогов, ценой и практически отсутствием какой либо технической и справочной документации о модуле. Esp8266 подключается к последовательному порту Arduino UNO, который представлен выходами RX TX. Модуль esp8266-01 питается от напряжения 3.3 Вольта, которые подаются на выход VCC модуля через преобразователь напряжения. Выход GND –это земля (минус питания). RST- выход для перезагрузки модуля. При подаче на него напряжения модуль перезагружается. Обмен данными между модулем и контроллером осуществляется через выхода RX (прием данных) и TX (передача данных). У платы Arduino Uno на выходе TX значение напряжения при единице равно 5 В. Такое напряжение, поданное на вход RX модуля, может вывести его из строя. Чтобы этого не произошло можно использовать делитель напряжения, состоящий из двух резисторов: 110 КОм и 200 КОм, который будет преобразовывать 5 Вольт в 3,3 Вольта, которые будут подаваться на выход RX модуля. Максимальная дистанция связи 100 метров.

Рисунок 4.3 – Модуль ESP8266-01

Объектом управления разрабатываемой системы контроля и управления доступом является электромеханический замок «ШЕРИФ-3В.У». На рисунке 4.4

представлены габаритные размеры замка. Он является нормально открытым, то есть, он открывается при снятии с него напряжения. Это является очень полезной характеристикой, так как в случае какой либо поломки системы, люди в помещении не окажутся заблокированы закрытыми дверьми. Замок может выдерживать усилие удержания не менее 300 кг. Напряжение питания данного замка составляет 12 Вольт. Так как Arduino UNO не может обеспечить такое значение напряжения на своих выходах, то замок необходимо подключить к блоку питания 12 Вольт.

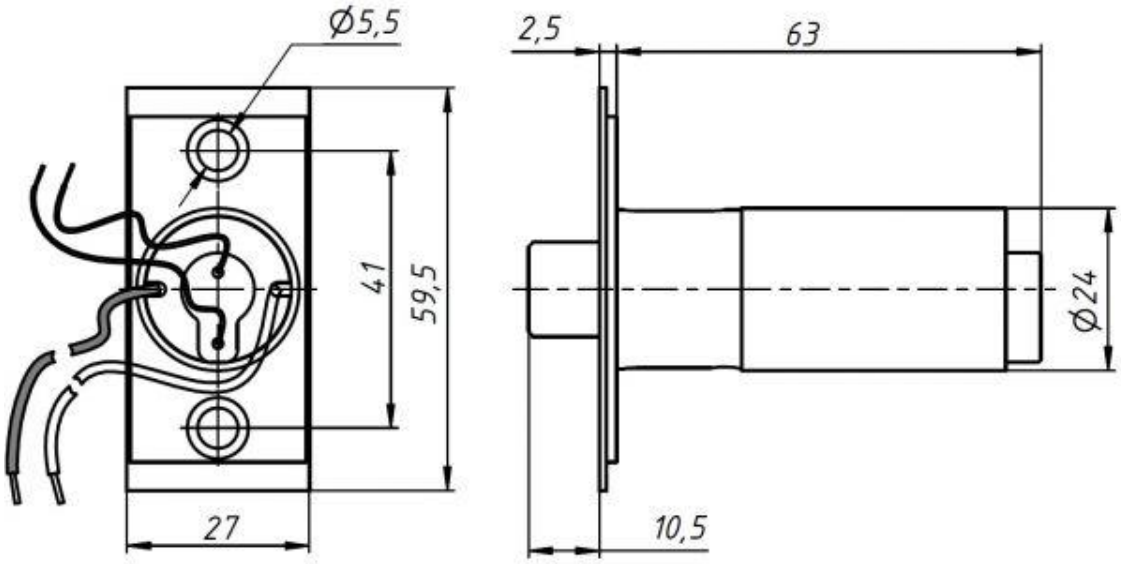

Рисунок 4.4- Габаритные размеры замка

Питание системы будут осуществлять десять солнечных модуля фирмы ANBES (рисунок 4.5). Напряжение на выходе каждого модуля составляет 6 Вольт, мощность- 1 Ватт. Для обеспечения 12 вольт модули будут разделены на пять пар, в которых мо-

дули будут соединены последовательно. Затем, пять пары модулей будут соединены параллельно. Таким образом, мы получим источник питания 12 Вольт мощностью 10 Ватт.

Так как вся наша система потребляет примерно 4 Ватта (так как в разные режимы работы для работоспособности системы необходим разный ток), то для работы системы в течение 12 часов нам необходим блок питания емкостью минимум 4800 а*час.

Рисунок 4.5 – Солнечный модуль ANBES 6 Вольт, 0.6 Ватт

Для того, чтобы разрабатываемая система не зависела от степени освещенности окружающей среды, необходимо наличие устройства, которое бы принимало заряд от солнечных модулей, накапливало его и отдавало его для питания системы. Данное устройство - блок питания и состоит из последовательно и параллельно соединенных 8 литиевых аккумуляторов 18650 3.7В 2600 мАч (Рисунок 4.6). Таким образом, мы получим блок питания который обеспечит нашу систему необходимыми 7 Ваттами на 12 часов работы в течение темного времени суток. Максимальный ток разрядки данных аккумуляторов может достигать 4,6 А. Для того, чтобы в отсут-

ствии освещения, когда на солнечных модулях напряжение может опускаться ниже 12 В, ток не был направлен от блока питания к солнечным модулям, будет использован диод 1N4007. Его максимальное обратное напряжение = 1000 В. Прямой ток 1А.

Рисунок 4.6 - Литиевые аккумуляторы 18650 3.7В

Данные аккумуляторы будет располагаться в четырех, последовательно соединенных кейсах, изображенных на рисунке 4.6.1

Рисунок 4.6.1 - Кейс для аккумуляторов 18650 3.7В

Помимо подачи напряжения на WI-FI модуль и контроллер, напряжение будет подаваться и на электромеханический замок через реле srd-05vdc-sl-c, изображенный на рисунке 4.7.

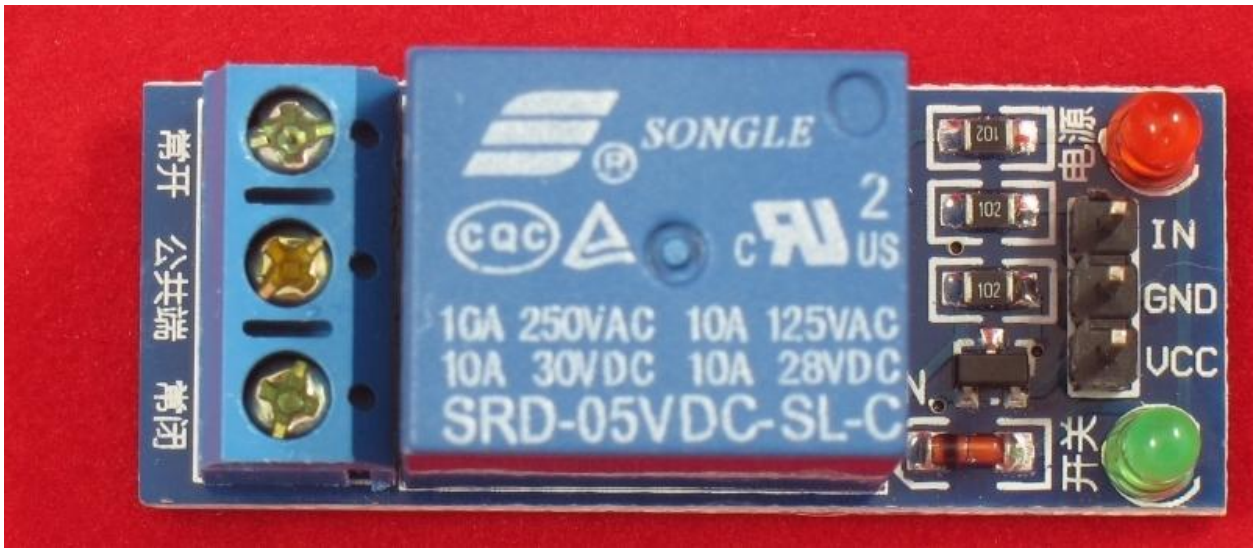

Рисунок 4.7 - Модуль реле srd-05vdc-sl-c

Данный модуль реле имеет три вывода - IN, DC+, DC-. На вывод IN подается управляющий сигнал с контроллера. DC- вывод для земли, он подключается к выходу GND котроллера. К выводу DC+ подключается вывод 5 V контроллера. Также, реле имеет еще три вывода: NO, COM и NC. COM вывод – это общий контакт, к нему будет подключен один из контактов цепи “блок-замок”. NO - это нормально-разомкнутый контакт. NC - нормально-закрытый. Наш электромеханический замок является нормально открытым, то есть, он открывается при снятии с него напряжения. Следовательно, второй контакт цепи “блок-замок” необходимо подключить к выводу NC. Таким образом, управляющий сигнал на выходе IN реле отсутствует, то цепь, состоящая из блока питания замка будет замкнут контактами COM и NC. Следовательно, на него будет поступать необходимое напряжение чтобы замок был закрыт. При подаче управляющего сигнала с контроллера на вход IN реле, цепь, из блока питания и замка будет размыкаться, и замок будет открыт.

Для того, чтобы пользователь узнал, открылся замок или нет будут использоваться светодиоды (Рисунок 4.8). В случае, если идентификатор, введенный пользователем правильный, то замок откроется и загорится зеленый светодиод. Во всех остальных случаях будет гореть красный светодиод.

Рисунок 4.8 – Светодиоды 510PG2C и 510HR3C

Данные светодиоды потребляют ток, равный 20 мА. Светодиоды имеют две ножки. Одна короткая- катод. Длинная – анод. Для ограничения тока, проходящего через

них от выходов контроллера, каждый будет подключен через резистор. Красный светодиод потребляет ток 20 мА при напряжении 2-2.6 Вольта. Он будет подключен к выводу контроллера через резистор 150 Ом. Рассеиваемая мощность на резисторе составит 0.06 Вт. Зеленый светодиод подключается к следующему выводу контроллера и потребляет ток 20 мА при напряжении 3 Вольта. Он подключается через резистор 100 Ом и рассеиваемая мощность на нем составит 0,04 Вт.

Для звукового оповещения об открытии замка будет использоваться пьезоизлучатель звука HPA17A 5 5B, 25мА. Он изображен на рисунке 4.9. Так как ток, который он потребляет равен 25 мА, то он будет напрямую подключен к выходам контроллера. Диаметр корпуса излучателя составляет всего 9,6 мм, что делает его очень компактным. Уровень звука составляет 78дБ. Был выбран именно пьезоизлучатель, а не электромагнитный излучатель, так как он обладает большей износостойкостью. Также, ни имеет посторонних шумов и потребляет меньший ток, по сравнению с электромагнитным излучателем.

Рисунок 4.9 – Пьезоизлучатель звука HPA17A

Все элементы системы, кроме солнечных панелей и электромеханического замка будут располагаться односторонней макетной плате 200мм на 150 мм (Рисунок 4.10).

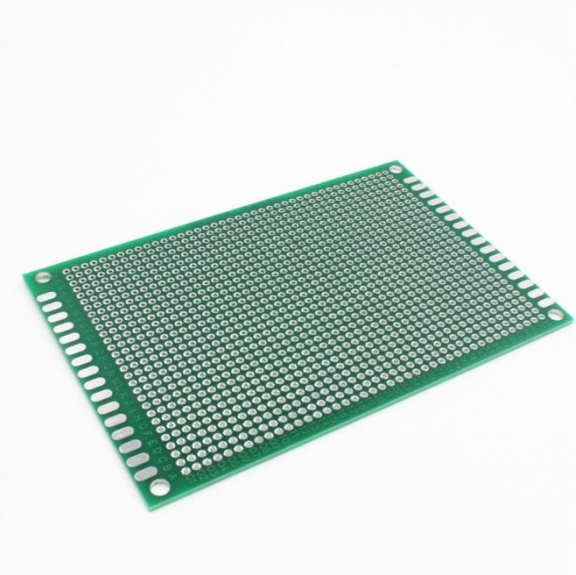

Рисунок 4.10 – Стеклотекстолит FR4

Его размеры соответствуют необходимым размерам для размещения на нем всех необходимых элементов системы контроля и управления доступом.

5 Подключение компонентов

5.1 Подключение WI-FI модуля

В данном проекте используется микроконтроллер ESP8266 с интерфейсом WI-FI и UART. Существуют различные варианты исполнения плат с данным контроллером. Все они различаются только размерами, вариантами антенн и выходами. Поэтому в данной работе используется Wi-Fi модуль ESP8266 01, изображенный на рисунке 5.1.1

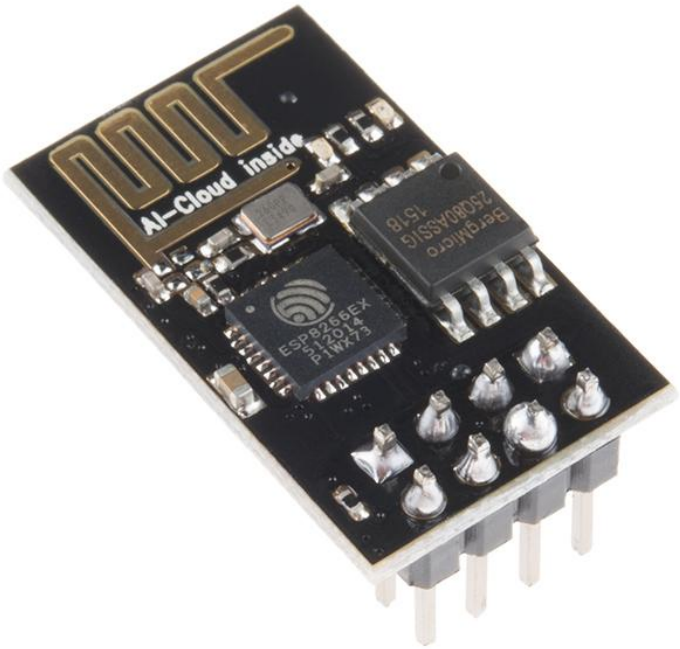

Рисунок 5.1.1 – Wi-Fi модуль ESP8266 01

Данный модуль поддерживает протокол передачи данных UART. UART- это асинхронный последовательный протокол, который передает и принимает данные в виде 0 и 1. Синхронизация осуществляется по времени, которая определяется до начала передачи данных. Поэтому принимающее устройство и передающее должно работать на одной скорости передачи данных, иначе данные могут быть либо частично, либо полностью утеряны.

В начале передачи предающее устройство посылает логический ноль. Это- стартовый бит. Принимающая сторона, получив стартовый бит, выжидает определенное время и начинает считывать 2,3,4 и т.д. биты через одинаковые интервалы времени. Последний бит является стоп битом, который сигнализирует о конце передачи данных. Для передачи данных используются 8 бит плюс бит старта и бит окончания передачи.

Работать с ESP8266 можно двумя способами:

1. Для управления модулем использовать переходник USB- UART. Тогда, модуль можно подключить через переходник к USB порту компьютера и управлять им с помощью АТ – команд.
2. Подключить модуль через интерфейс UART к последовательному интерфейсу UART Arduino UNO. А arduino UNO, в свою очередь, подключить к UAB порту компьютера, так как сама плата контроллера уже имеет преобразователь USB-UART TTL CH340G. Управление модулем будет осуществляться с помощью АТ - команд при помощи среды программирования Arduino IDE.

В данном проекте используется второй вариант.

Модуль ESP8266 01 имеет 8 выводов рисунок 5.1.2:

- VCC
- CH_PD
- GND
- RX
- TX
- RESET
- GPIO0
- GPIO2

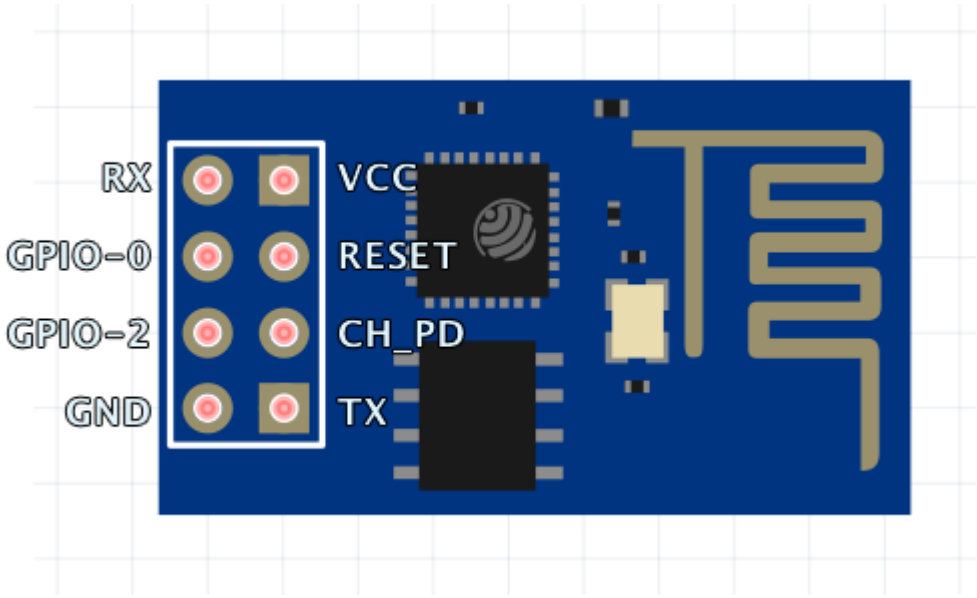

Рисунок 5.1.2 – Обозначения выводов Wi-Fi модуля ESP8266 01

На вывод **VCC** подается напряжение для питания модуля. Для его работы необходимо напряжение 3,3 Вольта. На плате Arduino UNO присутствует вывод 3,3 Вольта, но он не подойдет для питания модуля, так как максимальный ток, который может потреблять ESP8266 01 составляет 250 мА, в то время, как максимальный ток, который может обеспечить Arduino UNO составляет 40 мА. Поэтому для питания модуля используется блок питания на 12 Вольт, напряжение которого преобразуется с помощью преобразователя напряжения AMS1117 в 3.3 вольта, и который может обеспечить максимальный ток 1 А. Вывод **GND** модуля подключается к земле преобразователя AMS1117. Вывод **CH_PD** нужен для включения модуля. Для этого на него необходимо подать напряжение, как и на вывод VCC. Он также подключается к контакту 3,3 Вольт преобразователя AMS1117. Выводы **RX** и **TX** представляют из себя передающую (TX) и принимающую (RX) линии UART. Они используются для последовательной передачи данных между модулем и платой Arduino. Вывод TX модуля необходимо подключить к выводу RX контролера. Вывод же TX контроллера нельзя подключать непосредственно к выводу RX модуля. Arduino UNO работает на TTL логике (0-5 Вольт) в то время как ESP8266 работает с 3,3 Вольтами. Следовательно, напряжение на выводе TX контроллера может ока-

заться слишком большим для модуля и вывести его из строя. Для решения этой проблемы используется делитель напряжения из резисторов 220 Ом и 430 Ом, изображенный на рисунке 5.1.3 Земля делителя - это земля контроллера. Выводы RESET, GPIO0, GPIO2 не используются, так как нужны только во время перепрошивки модуля.

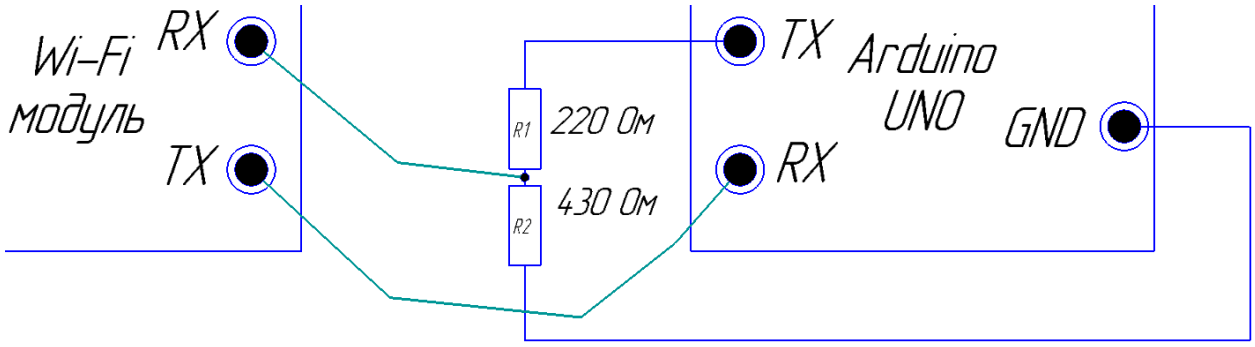

Рисунок 5.1.3 – Делитель напряжения для передачи данных по интерфейсу UART

$$\varepsilon = U_1 + U_2$$

$$\varepsilon = I(R_1 + R_2)$$

$$I = \frac{\varepsilon}{R_1 + R_2}$$

$$U_2 = \frac{\varepsilon * R_2}{R_1 + R_2}$$

$$U_1 = \frac{5 * 430\ \text{Ом}}{220\ \text{Ом} + 430\ \text{Ом}} \approx 3.3\ \text{В}$$

В конечном итоге схема подключения Wi-Fi модуля к Arduino Uno будет выглядеть так, как показано на рисунке 5.1.4.

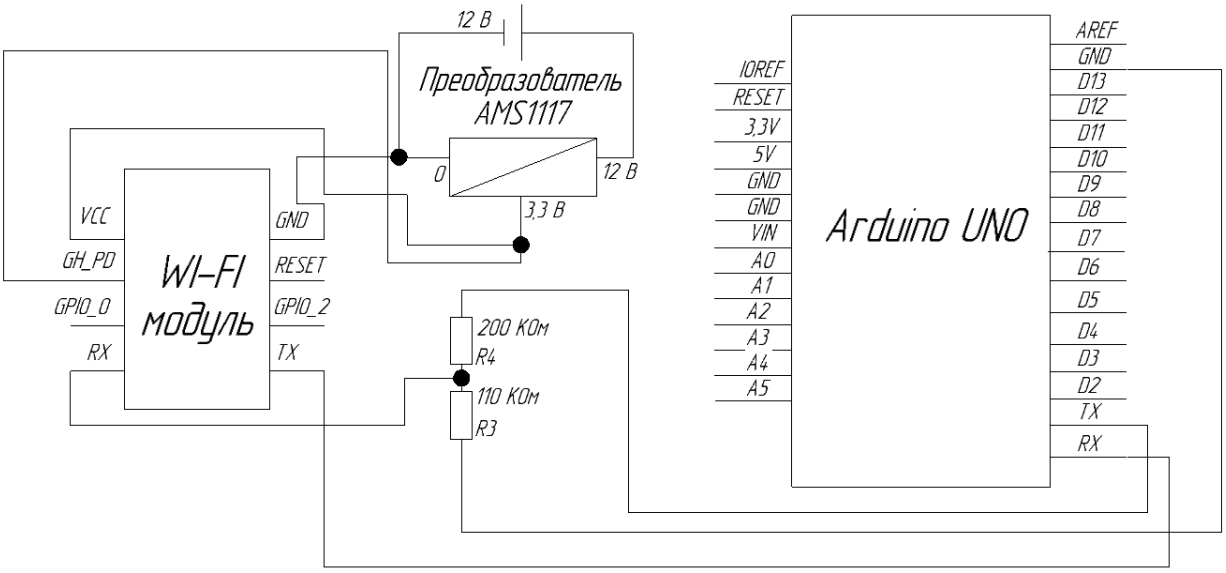

Рисунок 5.1.4 – Принципиальная схема подключения модуля Wi-Fi

5.2 Подключение реле

Так как максимальный ток и напряжение, которые может выдать Arduino UNO недостаточны для питания электромеханического замка, то в данном проекте используется электромагнитное реле srd-05vdc-sl-c.

Данный модуль будет управляться с помощью управляющего сигнала с Arduino UNO. Напряжение для работы самого замка будет поступать с блока питания 12 Вольт, после замыкания необходимых контактов реле.

Данный модуль реле имеет три вывода - IN, DC+, DC-. На вывод IN подается управляющий сигнал с контроллера. DC- вывод для земли, он подключается к выходу GND котроллера. К выводу DC+ подключается вывод 5 V контроллера. Также, реле имеет еще три вывода: NO, COM и NC. COM вывод – это общий контакт, к нему будет подключен один из контактов цепи “блок-замок”. NO - это нормально-разомкнутый контакт. NC - нормально-закрытый.

Наш электромеханический замок является нормально открытым, то есть, он открывается при снятии с него напряжения. Следовательно, второй контакт цепи “блок-замок” необходимо подключить к выводу NC. Таким образом, управляющий

сигнал на выходе IN реле отсутствует, то цепь, состоящая из блока питания замка будет замкнут контактами COM и NC. Следовательно, на него будет поступать необходимое напряжение чтобы замок был закрыт. При подаче управляющего сигнала с контроллера на вход IN реле, цепь, из блока питания и замка будет размыкаться, и замок будет открыт.

Принципиальная схема подключения реле показана на рисунке 5.2.1

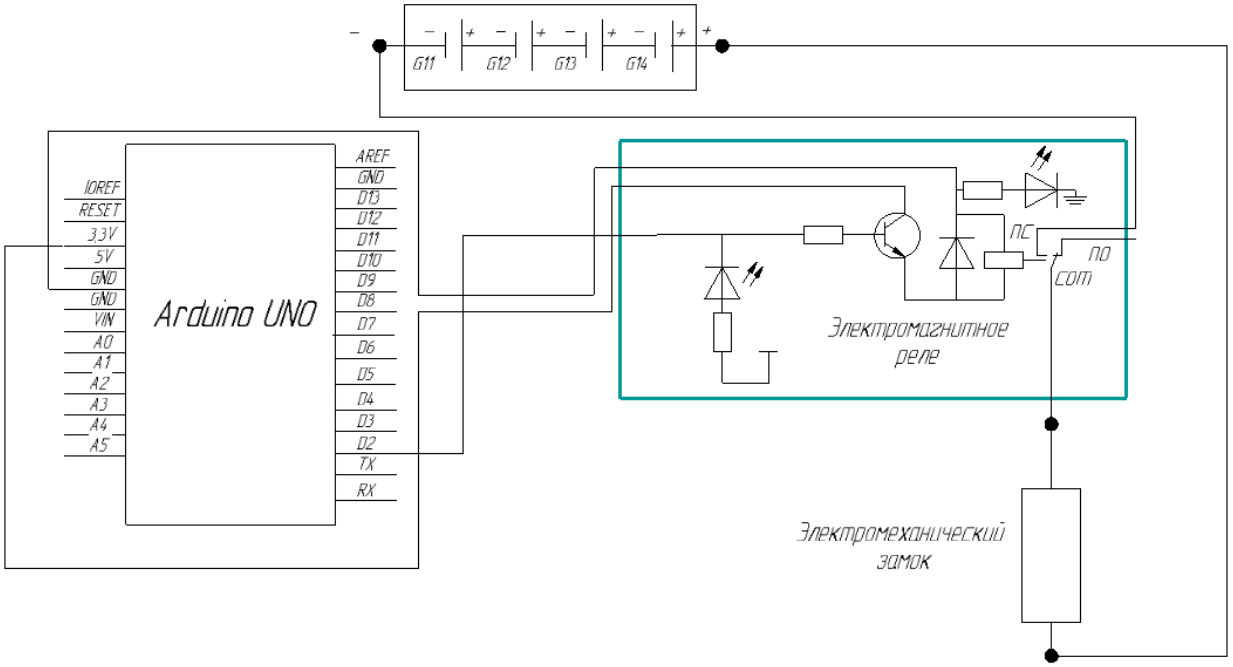

Рисунок 5.2.1 – Принципиальная схема подключения реле

5.3 Подключение светодиодов и излучателя звуков

В качестве устройств звукового и светового оповещения о режиме работы замка в данном проекте используются:

- Светодиод зеленый 510PG2C 3В, 20мА
- Светодиод красный 510HR3C 2.6В, 20мА
- Пьезоизлучатель звука HPA17A 5 5В, 25мА
- С1-4 резистор 0,25 Вт, 5%, 150 Ом

- С1-4 резистор 0,25 Вт, 5%, 100 Ом

Так как пьезоизлучатель звука HPA17A рассчитан на напряжение 5 Вольт, а именно такое напряжение на выводах контроллера Arduino UNO, то данный пьезоизлучатель подключается к любому выводу контроллера выводом + и на вывод GND котроллера выводом - напрямую.

Светодиоды так подключать нельзя, так как при рабочем токе 20 мА они в среднем требуют напряжение 2.6-3.3 Вольта, в зависимости от светодиода. Поэтому, данные светодиоды подключаются к выводам контроллера каждый через резистор. Красный светодиод при токе 25 мА требует в среднем 2.6 Вольт. В среднем, так как светодиод имеет нелинейную ВАХ, поэтому у каждого производителя требования по напряжению для каждого вида светодиодов разные. Светодиоды имеют по две ножки. Одна- короче, другая длиннее. Длиная ножка – это анод. Он подключается к выводу контроллера, на котором будет высокое значение напряжения. Короткая ножка- катод она подключается к GND контроллера. Красный светодиод подключается к выводу контроллера последовательно через резистор 150 Ом. Зеленый требует в среднем напряжение 3 Вольта. Он подключается к выводу контроллера последовательно через резистор 100 Ом. Принципиальная схема подключения пьезодинамика и светодиодов показана на рисунке 5.3.1

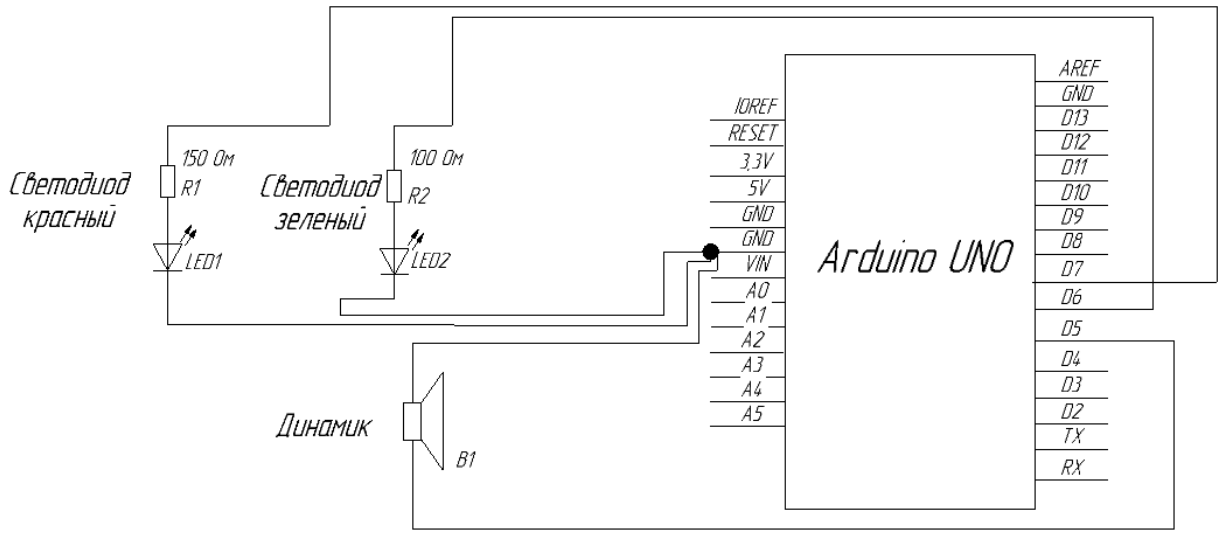

Рисунок 5.3.1 – Принципиальная схема подключения светодиодов и пьезодинамика

5.4 Подключение солнечных модулей и блоков питания

Для работы всей разрабатываемой системы , необходим какой либо источник питания. В данном проекте используются 10 солнечных панелей, которые совокупно имеют мощность 10 Ватт. Одна солнечная панель может обеспечить уровень напряжения 6 вольт и 160 мА тока. Если мы подключим две такие панели последовательно, то мы получим панель, которая может обеспечить 12 Вольт при 160 мА тока. Далее, если соединить две панели по 12 Вольт и 160 мА тока параллельно, то мы получим панель, которая обеспечивает 12 Вольт напряжения и 320 мА тока. Таким образом если соединить панели так как показано на рисунке 5.4.1. то мы получим на выводах солнечной панели 12 Вольт напряжения и примерно 1 Ампер тока.

Емкость аккумулятора в А*час = мощность нагрузки в кВт x время в часах x 100

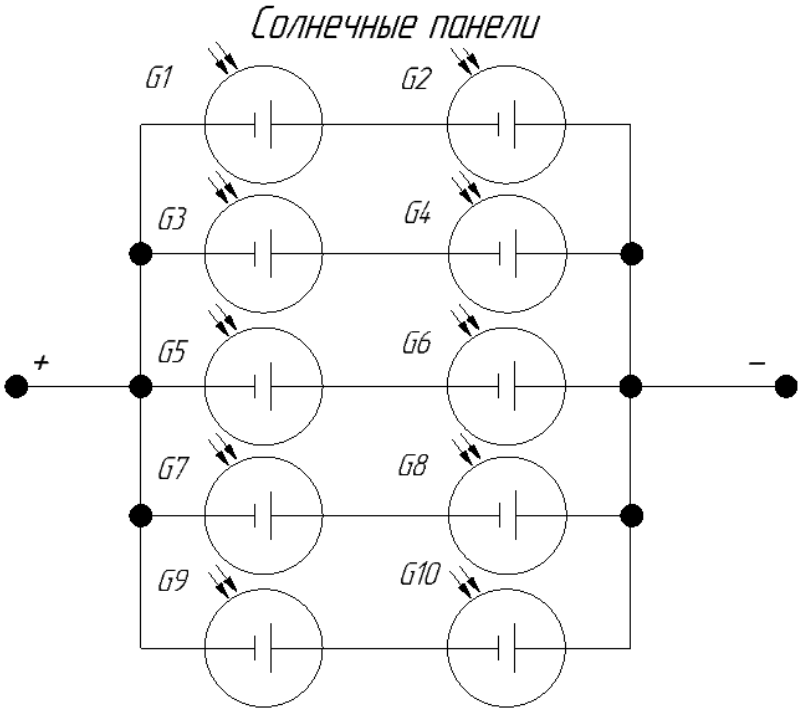

Рисунок 5.4.1 – Принципиальная схема соединения солнечных панелей

Для обеспечения питания разрабатываемой системы в течение 12 часов работы темного времени суток требуется аккумулятор, емкостью минимум 4800 мА/ч и

обеспечивающий 12 Вольт постоянного напряжения , так как усреднено (в зависимости от режима работы) потребляемая мощность делится так:

- ESP 8266 – 0,825 Вт
- Arduino UNO – 0,48 Вт
- Два светодиода и резисторы- 0,3 Вт
- Пьезодинамик- 0,02
- Реле-0,96 Вт
- Электромеханический замок- 0,96
- ИТОГ – 3,5Вт (4Вт)

Для этого необходимо 8 аккумуляторов 18650 3.7В, 2600 мА/ч. Каждый аккумулятор обеспечивает напряжение 3,7 Вольт. Если соединить аккумуляторы последовательно по 4 штуки, (**предварительно разрядив все аккумуляторы до 0)** то мы получим блок питания 12 Вольт (EMS1117 способен выдержать напряжение до 18 вольт) емкостью 2600 мА/ч. Следовательно, нам необходимо соединить два таких блока для получения блока питания 12 Вольт и 5200мА/ч чего более чем хватит для бесперебойного питания нашей системы. Схема подключения показана на рисунке 5.4.2

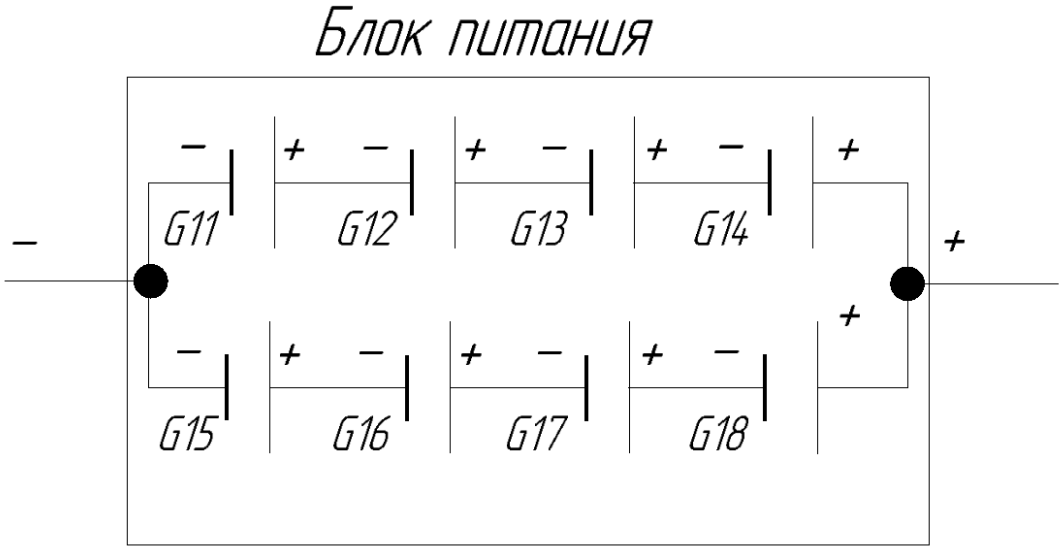

Рисунок 5.4.2 – Принципиальная схема соединения аккумуляторов в один блок питания

Так как могут быть случаи, когда на солнечных панелях напряжение может быть меньше 12 Вольт, например, когда панели плохо освещаются, то для предотвращения движения тока от блока питания, к солнечным панелям последовательно с панелями подключим диод 1N4007 1A, 1000 В.

Схема подключения солнечных панелей к блоку питания показана на рисунке 5.4.3

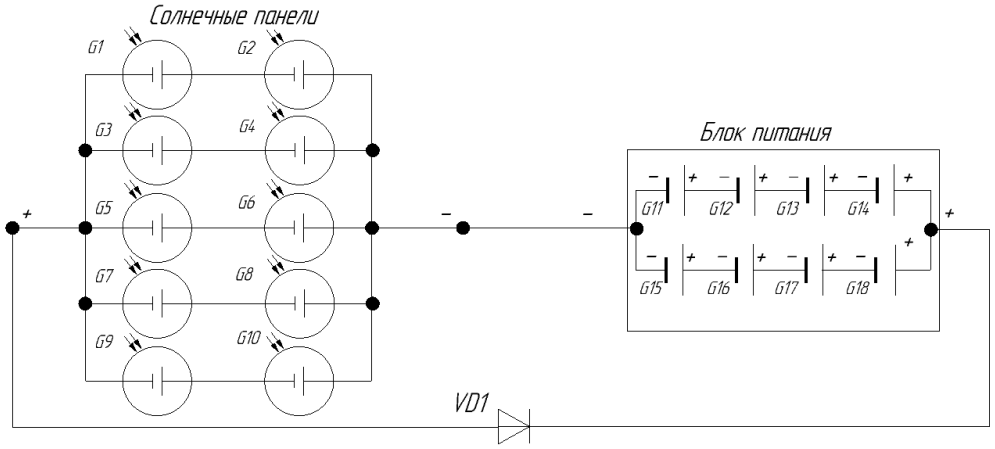

Рисунок 5.4.3 – Принципиальная схема подключения солнечных панелей и блоков питания

В нашей системе есть элемент, который для питания требует строго 3,3 Вольт. Для преобразования 12 вольт блока питания используется преобразователь напряжения EMS1117. Он имеет три вывода: 0 В – земля, 3.3 В и 12 В.

Полная схема подключения элементов питания к преобразователю показана на рисунке 5.4.4

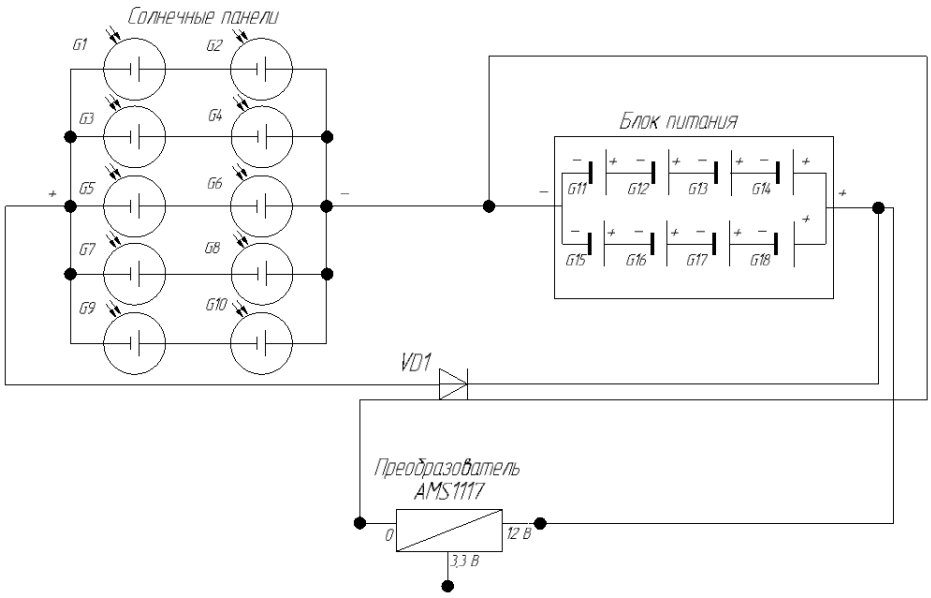

Рисунок 5.4.4 – Принципиальная схема подключения солнечных панелей и блоков питания к преобразователю

6 Создание управляющей программы

Программа, управляющая работой системы, будет состоять из двух частей

- Создание сервера
- Создание программы, управляемой ответом сервера на запрос клиента

Алгоритм работы системы: Пользователь, которому требуется открыть замок, подключается к точке доступа Wi-Fi, которая создается Wi-Fi модулем. Затем, пользователь вводит пароль (идентификатор) и, если пароль верен, пользователь подключается к модулю, заходит в браузер телефона по ссылке 192.168.4.1 (ip адрес модуля).Далее, замок открывается и звучит звуковой сигнал. Через 5 секунд замок закрывается.

Для программирования используется интегрированная среда разработки Arduino –Arduino IDE.

Управлять модем ESP8266 01 можно посредством отправки ему АТ-команд.

АТ-команды – это набор команд, изначально разработанных в 1997 году компанией Hayes для собственной продукции. Все АТ команды начинаются с букв АТ.

Сначала необходимо, чтобы модуль Wi-Fi создал сервер, при обращении к которому открывался замок. Для этого сначала необходимо воспользоваться следующими командами:

- AT (Это команда для проверки модуля. Ожидаемый ответ от него- OK.)
- AT+CWMODE = 3 (Команда для определения режима работы модуля. 1-клиент, 2- точка доступа, 3- совмещенный)
- AT+RST (перезагрузка модуля. Необходимо для CWMODE)
- AT+CWSAP= "ARDUINOUNO","123456789",1,4 (настройка “имени”, “пароля”, номера канала и типа шифрования данных)
- AT+CIPMUX=1 (включение режима множественных подключений)
- AT+ AT+CIPSERVER=1,80 (задание запуска сервера и порта)

Константа 1 указывает на то, что сервер будет запущен. Порт номер 80 используется протоколом передачи гипертекста HTTP. Следовательно, что бы сервер зарегистрировал подключение к нему устройства пользователя, необходимо, чтобы пользователь воспользовался браузером телефона и ввести в адресную строку ip сервера.

- AT+CIFSR (отображение IP адреса сервера.)

При подключении к серверу, модуль отправит на контроллер информацию о подключаемом устройстве. Выглядеть она может так как на рисунке 6.1

```
0,CONNECT

+IPD,0,495:GET / HTTP/1.1
Host: 192.168.4.1
Connection: keep-alive
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
x-wap-profile: http://www.zte.com.cn/mobile/uaprof/ZTE
V880H.xml
X-Requested-With: com.android.browser
User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.1; ru-ru; ZTE V880H
Build/JOP40D) AppleWebKit/534.30 (KHTML, like Gecko)
Version/4.0 Mobile Safari/534.30
Accept-Encoding: gzip,deflate
Accept-Language: ru-RU, en-US
Accept-Charset: utf-8, utf-16, *;q=0.7
```

Рисунок 6.1 – Информация о клиенте

Подача напряжения на реле, и остальные устройства будет осуществляться в случае, если в присланном от сервера ответе будет найдено какое либо определенный набор символов. В описанной ниже программе таким набором символов является слово Accept:. Но при желании, можно указать любую другую последовательность символов.

Ниже представлены рисунки 6.2 и 6.3 с управляющей программой написанной в Arduino IDE

ARDUINO_WIFI §

```
char answer[1500];
void setup()
{
  Serial.begin (115200); // задание скорости работы порта передачи данных 115200
  pinMode (5,OUTPUT); // 5 выход управляющего сигнала для электромагнитного реле
  pinMode (8,OUTPUT); // 8 выход для зеленого светодиода
  pinMode (9,OUTPUT); // 9 выход красного светодиода
  pinMode (10,OUTPUT);// 10 выход пьезодинамика
  digitalWrite(5, LOW); // установка низкого логического сигнала на выходе 5
  digitalWrite(8, LOW); // установка низкого логического сигнала на выходе 8
  digitalWrite(9, HIGH); // установка высокого логического сигнала на выходе 9
  digitalWrite(10, LOW); // установка низкого логического сигнала на выходе 10
  Serial.println("AT"); // отправка команды проверки готовности модуля по интерфейсу UART от контроллера к модулю
  delay(2000); // ожидание 2 секунды
  Serial.println("AT+RST"); // отправка команды  перезагрузки модуля
  delay(2000);// ожидание 2 секунды
  Serial.println("AT+CWMODE=3"); // отправка команды совмещенного режима работы модуля
  delay(2000);// ожидание 2 секунды
  Serial.println("AT+CIPMUX=1"); // отправка команды множественных подключений
  delay(2000);// ожидание 2 секунды
  Serial.println("AT+CIPSERVER=1,80");// отправка команды запуска сервера и использование 80 порта
  delay(2000);// ожидание 2 секунды


}

void loop()
{
```

Рисунок 6.2 – Первая часть управляющей программы

ARDUINO_WIFI §

```
}

void loop()
{
  int i; // инициализация переменной i
  if (Serial.available()) // если arduino получает какие - либо данные, начинается цикл записи данных в массив
  {
    for (i=0; i<1501-1; ++i) // учловия цикла
        {
      if (!Serial.available()) // если передачи нет, то выход из цикла
      break;
      answer[i]= Serial.read(); // запись полученных данных в каждую ячейку массива
        }
  answer[i]=0; // нет данных в массиве

    if (strchr(answer,'Accept:') !=NULL) // функция поиска символов Accept в массиве answer. если найдены, то выполнение функций ниже
    {
   digitalWrite(5, HIGH);// подача высокого логического сигнала на выход реле
   digitalWrite(8, HIGH);//подача высокого логического сигнала на зеленый светодиод
   digitalWrite(9, LOW);//подача низкого логического сигнала на красный светодиод
   tone (10,15000,5000); // включение пьезодинамика для звук.сигнала частотой 15кГц длительностью 5 секунд.
   delay(5000); // ожидание 5 секунд
   digitalWrite(5, LOW);//подача низкого логического сигнала на реле
   digitalWrite(8, LOW);//подача низкого логического сигнала зеленый светодиод
   digitalWrite(9, HIGH);//подача высокого логического сигнала на красный светодиод

      }


  }
}
```

Рисунок 6.3 –Вторая часть управляющей программы

7 Разработка схемы электрической соединений

На рисунке 7.1 представлена электрическая схема соединений. На ней представлены:

- Arduino UNO на базе процессора ATmega328
- Wi-Fi модуль ESP8266-01
- Электромагнитное реле srd-05vdc-sl-c
- Солнечный модуль 6В, 1 Ватт фирмы ANBES – 10 шт.
- Литиевые аккумуляторы 18650 3.7В, 2600 мАч – 8 шт.
- Электромеханический замок «ШЕРИФ-3В.У»
- Пьезоизлучатель звука HPA17A 5 5В, 25мА
- Светодиод зеленый 510PG2C 3В, 20мА
- Светодиод красный 510HR3C 2.6В, 20мА
- С1-4 резистор 0,25 Вт, 5%, 430 Ом
- С1-4 резистор 0,25 Вт, 5%, 150 Ом
- С1-4 резистор 0,25 Вт, 5%, 220 Ом
- С1-4 резистор 0,25 Вт, 5%, 100 Ом
- Диод 1N4007 1А, 1000 В.
- Преобразователь напряжения AMS1117

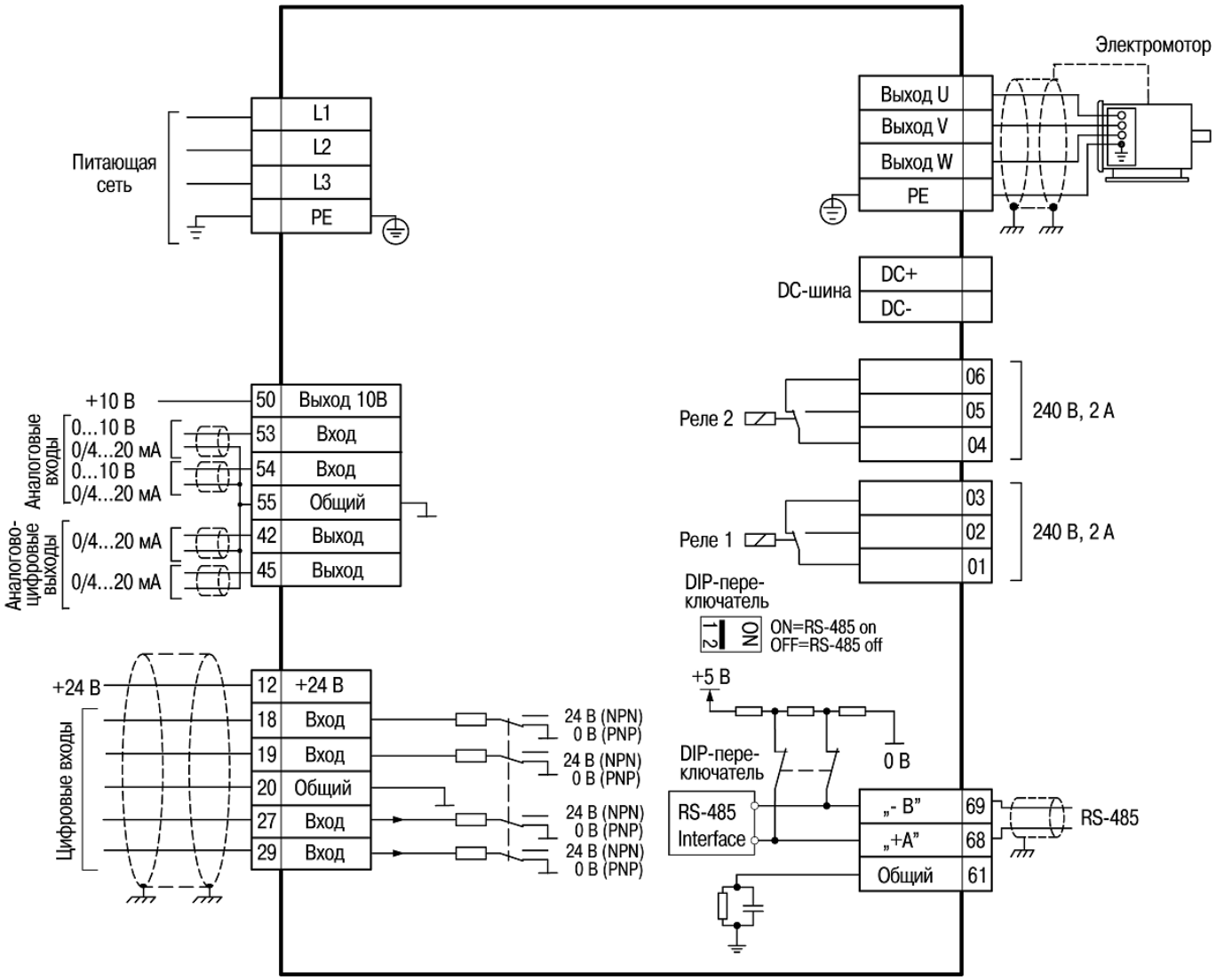

Рисунок 7.1 – Схема электрическая соединений

8 Разработка принципиальной схемы

Принципиальная схема системы контроля и управления доступом включает следующие элементы:

- Arduino UNO на базе процессора ATmega328
- Wi-Fi модуль ESP8266-01
- Электромагнитное реле srd-05vdc-sl-c
- Солнечный модуль 6В, 1 Ватт фирмы ANBES – 10 шт.
- Литиевые аккумуляторы 18650 3.7В, 2600 мАч – 8 шт.
- Электромеханический замок «ШЕРИФ-3В.У»
- Пьезоизлучатель звука HPA17A 5 5В, 25мА
- Светодиод зеленый 510PG2C 3В, 20мА
- Светодиод красный 510HR3C 2.6В, 20мА
- С1-4 резистор 0,25 Вт, 5%, 430 Ом
- С1-4 резистор 0,25 Вт, 5%, 150 Ом
- С1-4 резистор 0,25 Вт, 5%, 220 Ом
- С1-4 резистор 0,25 Вт, 5%, 100 Ом
- Диод 1N4007 1А, 1000 В.
- Преобразователь напряжения AMS1117

Сама принципиальная схема изображена на рисунке 8. Данная схема была спроектирована в системе автоматизированного проектирования (САПР) КОМПАС 3D фирмы Аскон. Система «Компас-3D» предназначена для создания трёхмерных ассоциативных моделей отдельных деталей и сборочных единиц, содержащих как оригинальные, так и стандартизованные конструктивные элементы. Система «Компас-3D» включает следующие компоненты: система трёхмерного твердотельного моделирования, универсальная система автоматизированного проектирования «Компас-График» и модуль формирования спецификаций. Ключевой особенностью

«Компас-3D» является использование собственного математического ядра и параметрических технологий.

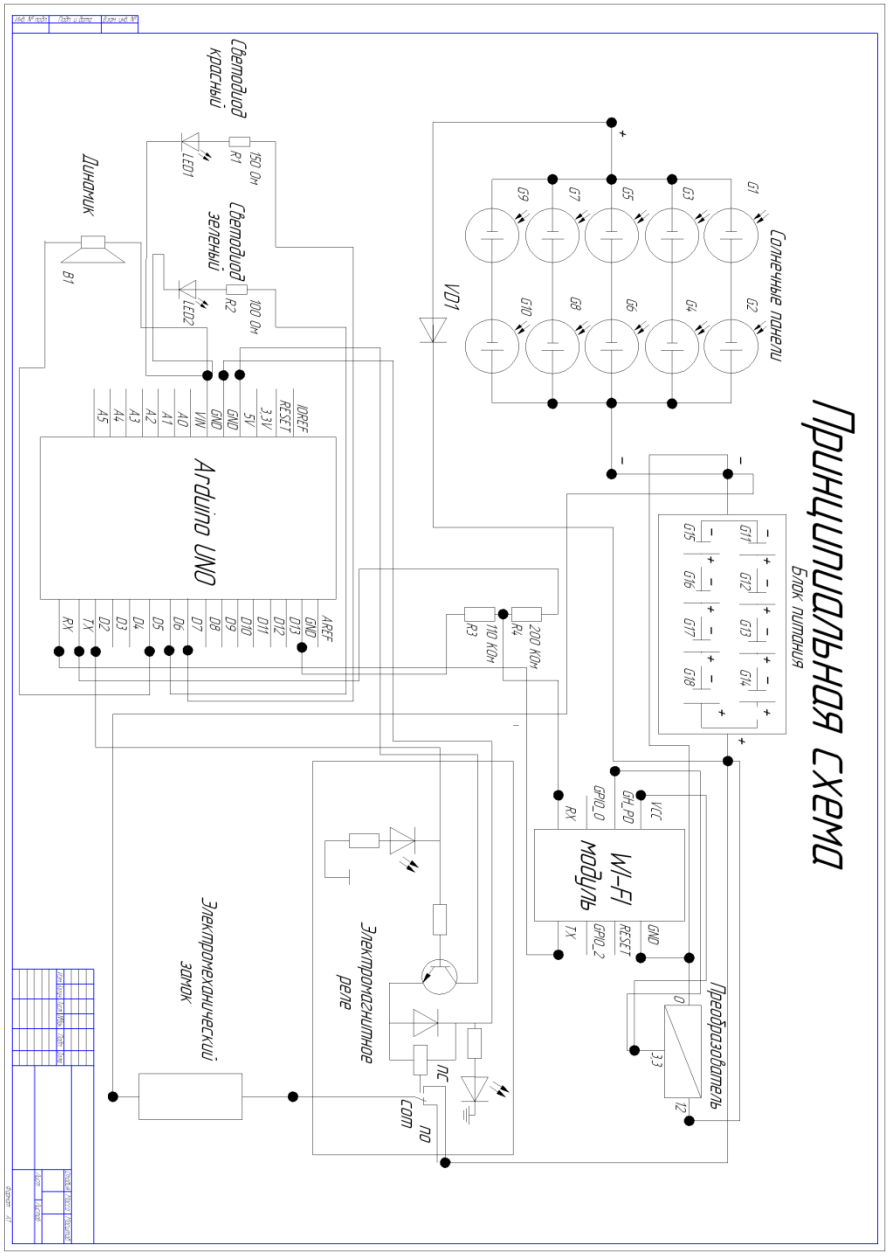

Рисунок 8 – Принципиальная схема

9 Разработка сборочного чертежа

На рисунке 9.1 представлен сборочный чертеж платы, на которой присутствуют следующие элементы.

- Arduino UNO на базе процессора ATmega328
- Wi-Fi модуль ESP8266-01
- Электромагнитное реле srd-05vdc-sl-
- Литиевые аккумуляторы 18650 3.7В, 2600 мАч – 8 шт.
- Пьезоизлучатель звука HPA17A 5 5В, 25мА
- Светодиод зеленый 510PG2C 3В, 20мА
- Светодиод красный 510HR3C 2.6В, 20мА
- С1-4 резистор 0,25 Вт, 5%, 430 Ом
- С1-4 резистор 0,25 Вт, 5%, 150 Ом
- С1-4 резистор 0,25 Вт, 5%, 220 Ом
- С1-4 резистор 0,25 Вт, 5%, 100 Ом
- Диод 1N4007 1А, 1000 В.
- Преобразователь напряжения AMS1117
- Макетная плата 200X150

На данной плате отсутствуют солнечные модули и электромеханический замок из за их габаритов, конструкторских особенностей и способа их применения.

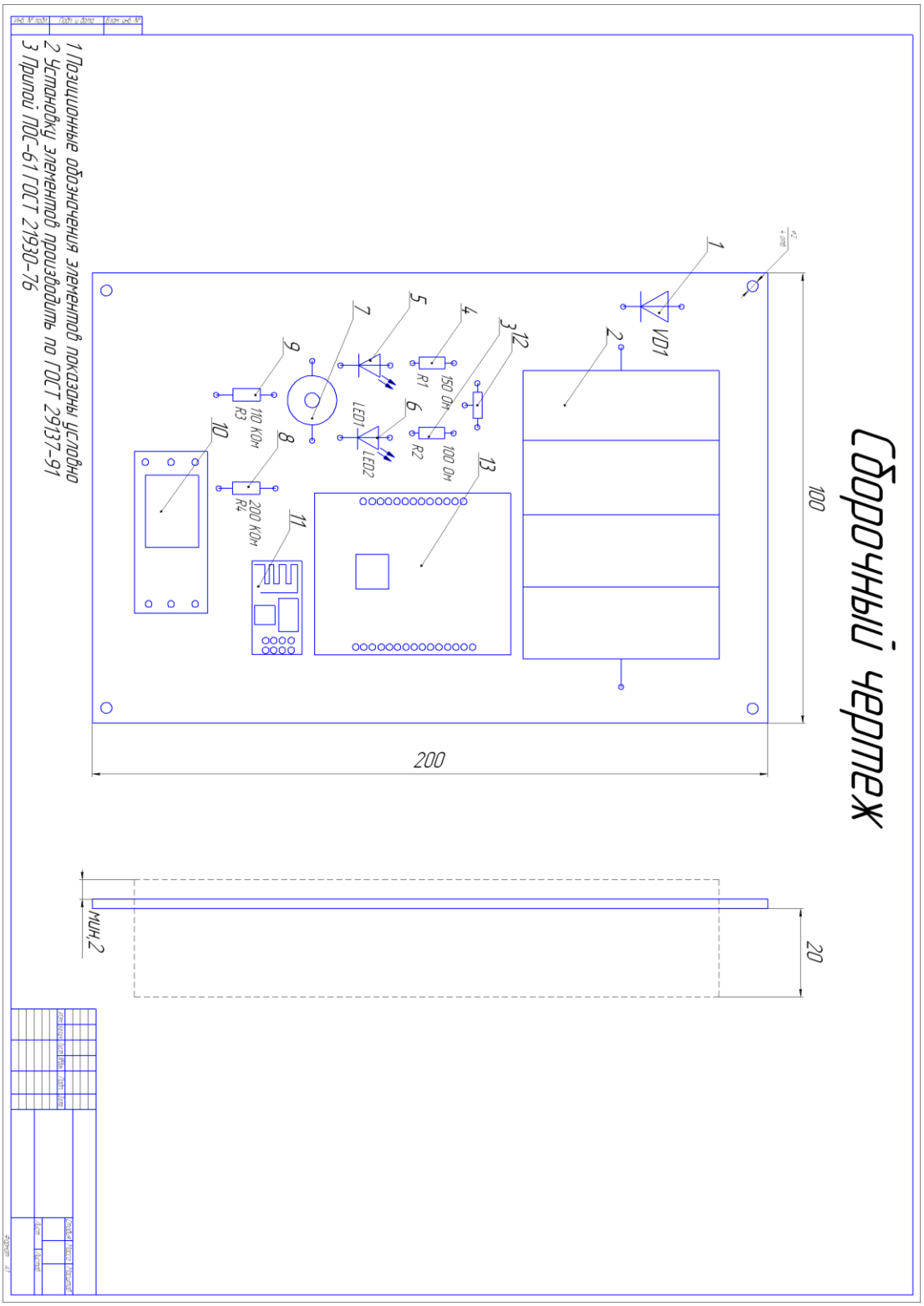

Рисунок 9.1 – Сборочный чертеж

10 Блок-схема алгоритма работы программы

На рисунке 10.1 представлена блок-схема алгоритма управляющей работы программы проекта.

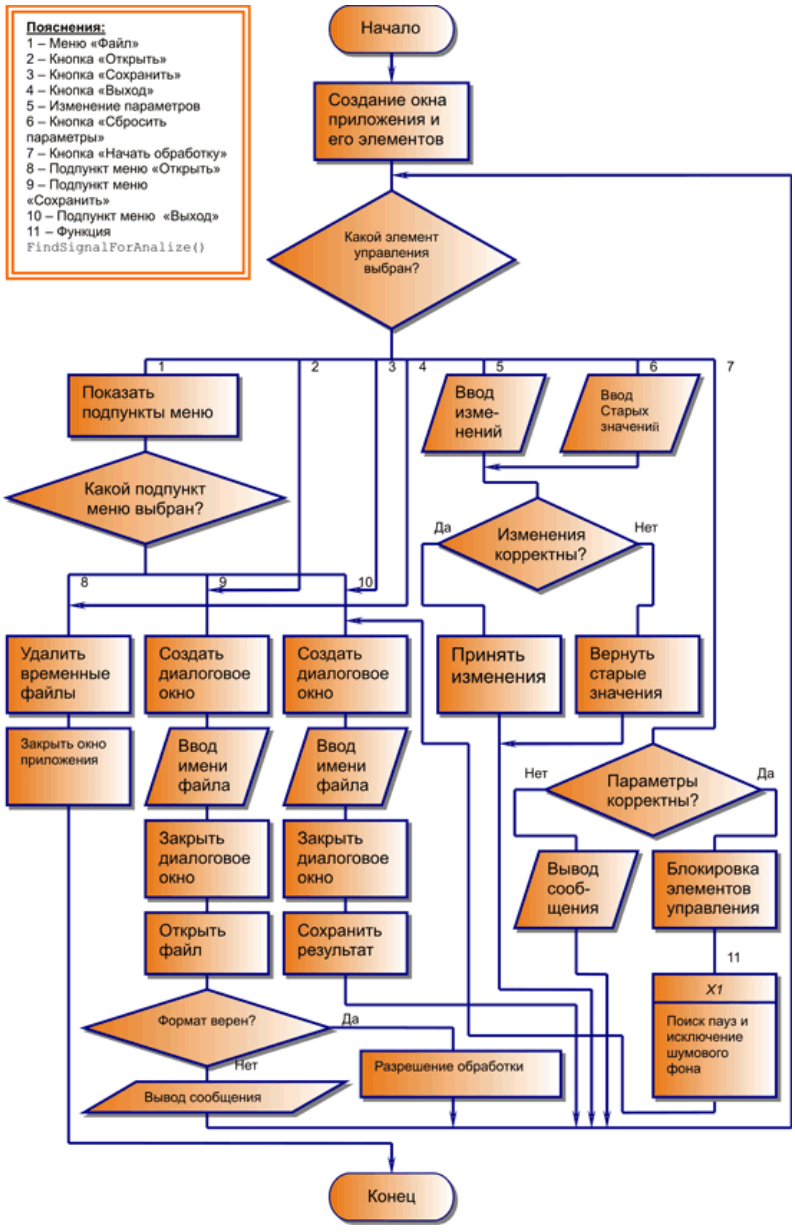

Рисунок 10.1 – Блок-схема алгоритма управляющей программы

11 Экономический расчет проекта

На рисунке 11.1 изображена таблица, содержащая наименования комплектующих системы, их количество и стоимость. В конце таблицы подсчитана общая стоимость всех комплектующих, использовавшихся в разработке проекта.

Цены комплектующих контроллера гидропонной теплицы

№	Обозначение	Наименование	Кол.	Цена, р.
1	C1, C2	Конд.тант. 10 мкФ х 25 В тип С 10% выводной	2	29
2	C3, C4	(К50-35) 4.7мкф 16В 105 гр, серия SH, 5х11 электролит.конденсатор	2	8
3	C5, C6	К 10-17Б имп. 100 пф NP0 5% ,RPE5C1H101J2K1A03B	2	7
4	DA1, DA3	CA3140	2	33
5	DA2	LM1117DT-3.3	1	140
6	DA4, DA5	К293КП13П	2	200
7	L1	RLB0914-101KL индукт. 100 мкГн	1	32
8	R1 R4, R6, R8	С1-4 резистор 0.25 Вт, 5%, 100 кОм	4	0,54
9	R2	С1-4 резистор 0.25 Вт, 5%, 68 кОм	1	0,54
10	R3	С1-4 резистор 0.25 Вт, 5%, 8,2 кОм	1	0,54
11	R5	С1-4 резистор 0.25 Вт, 5%, 300 кОм	1	0,54
12	R7	С1-4 резистор 0.25 Вт, 5%, 1 кОм	1	0,54
13	R9	С1-4 резистор 0.25 Вт, 5%, 4,7 кОм	1	0,54
14	R10, R15-R18	С1-4 резистор 0.25 Вт, 5%, 10 кОм	5	0,54
15	R11, R12	С1-4 резистор 0.25 Вт, 5%, 130 Ом	2	0,54
16	R13, R14	С1-4 резистор 0.25 Вт, 5%, 100 Ом	2	0,54
17	XS1	BNC-144 гнездо на плату пласт, GB-142R	1	61
18	XS2	3-151, Разъем питания 3.5х1.3мм "гн" пластик на плату	1	23
19	XS3-XS5	15EDGK-3.81-02P клеммник винтовой разъемный	3	29
20	XS6	PBD-8 гнездо на плату 2х4 прям	1	12
21		Стеклотекстолит	1	60

Итого: 978 р.

Рисунок 11.1 – Расчет стоимости комплектующих системы.

Заключение

В рамках данной выпускной квалификационной работы была показана актуальность развития систем контроля и управления доступом. Разработана система, позволяющая управлять электромеханическим замком и устройствами звукового и светового оповещения при помощи Wi-Fi связи. Была разработана структурная схема системы. Обоснован выбор комплектующих, использовавшихся в проекте. Разработана принципиальная схема и схема соединений. Показан алгоритм работы управляющей программы. Также, пошагово описан процесс подключения всех компонентов системы. Данная система является системой контроля и управления доступом с помощью беспроводной Wi-Fi связи. Для получения доступа пользователю необходимо , с помощью смартфона, подключиться к точке доступа системы и ввести личный идентификатор. Идентификатор верен, система открывает замок, вмонтированный в какую – либо дверь. Также, о режиме работы системы сообщает звуковой и световой сигналы. В завершении выполнен анализ экономичности проекта.

Список использованной литературы

1. Хоровиц, Хилл : Искусство схемотехники. М.: Издательство БИНОМ 2014. - 704 с., ил.
2. Кузин А.В, Жаворонков М.А.: Микропроцессорная техника. М.: Издательский центр «Академия», 2007.- 304 с.
3. Джонс М.Х.: Электроника – практический курс. Москва: Постмаркет, 1999. - 528 с.
4. Титце У., Шенк К. Полупроводниковая схемотехника. 12-е изд. Том I: Пер. с нем. – М.: ДМК Пресс, 2008. – 832 с.: ил.
5. Москатов Е. А. Электронная техника. Начало. – 3-е изд., перераб. и доп. – Таганрог, 204 с., ил
6. Шилдт, Герберт: C++: Базовый курс, 3 - е издание.: Пер. с англ. – М.: Издательский дом «Вильямс», 2010. – 624 с.: ил.
7. [Электронный ресурс] – Электрон. дан. – М.: Интернет-портал «ESP8266- сообщество разработчиков», 2017. – Режим доступа: http:// esp8266.ru/, свободный. – Загл. с экрана.
8. [Электронный ресурс] – Электрон. дан. – М.: Интернет-портал «Амперка», 2017. – Режим доступа: http://amperka.ru/, свободный. – Загл. с экрана.
9. [Электронный ресурс] – Электрон. дан. – М.: Интернет-портал «Технология защиты», 2017. – Режим доступа: http://tzmagazine.ru/, свободный. – Загл. с экрана.
10. [Электронный ресурс] – Электрон. дан. – М.: Интернет-портал «Security News», 2017. – Режим доступа: http://secnews.ru/, свободный. – Загл. с экрана.
11. [Электронный ресурс] – Электрон. дан. – М.: Интернет-портал «Хабрахабр», 2017. – Режим доступа: https://habrahabr.ru, свободный. – Загл. с экрана.
12. Афанасьева Н.А., Булат Л.П. Электротехника и электроника: Учеб. пособие. – СПб.: СПбГУНиПТ, 2009. – 181 с.
13. В. Л. Бройдо. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. — СПб.: Питер, 2004. — 703 с.: ил.

14. Щербаков А. К. Wi#Fi: Все, что Вы хотели знать, но боялись спросить. Неофициальное пособие по глобальной системе местоопределения, 2005. - 352 с.
15. Руденков Н.А., Долинер Л.И. Основы сетевых технологий: Учебник для вузов. Екатеринбург: Изд-во Уральского. Федерального ун-та, 2011. – 300 с.
16. Sadeque Reza Khan. Development of Low Cost Private Office Access Control System [Электронный ресурс]: https://www.researchgate.net
17. Umar Farooq, Athar Hanif, Usman Asad, Mahmood ul Hasan, Muhammad Amar. RFID Based Security and Access Control System [Электронный ресурс]: https://www.researchgate.net
18. Hussaini Habibu, Adamu Murtala Zungeru, Ajagun Abimbola Susan, Ijemaru Gerald Kelechi, Oresanya Babajide. Design of a GSM-Based Biometric Access Control System [Электронный ресурс]: https://www.researchgate.net
19. Qasim Hasan Mezher Al-shebani. Embedded door access control systems based on face recognition [Электронный ресурс]: https://www.researchgate.net
20. Matjaž Gams and Tea Tušar. Intelligent High-Security Access Control [Электронный ресурс]: https://www.researchgate.net