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

ИНСТИТУТ ЭНЕРГЕТИКИ И ЭЛЕКТРОТЕХНИКИ
(институт)
Промышленная электроника
(кафедра)
11.03.04 Электроника и наноэлектроника
(код и наименование направления подготовки, специальности)
Промышленная электроника
(профиль)

БАКАЛАВРСКАЯ РАБОТА

на тему Система безопасности «Умного дома» на основе микроконтроллера

Студент(ка)	А.И. Сидоренко		
	(И.О. Фамилия)		(личная подпись)
Руководитель	А.В. Прядилов		
	(И.О. Фамилия)		(личная подпись)
Консультанты	Н.В. Андрюхина		
	(И.О. Фамилия)		(личная подпись)

Допустить к защите

Заведующий кафедрой, к.т.н., доцент А.А. Шевцов _____
(ученая степень, звание, И.О. Фамилия) (личная подпись)
«_____»_____20_____г.

Тольятти 2018

АННОТАЦИЯ

Ключевые слова: УМНЫЙ ДОМ, СИСТЕМА БЕЗОПАСНОСТИ, МИКРОКОНТРОЛЛЕР, ARDUINO.

Целью данной бакалаврской работы является разработка системы безопасности «Умного дома» на основе микроконтроллера, которая должна фиксировать и в некоторых случаях предотвращать аварийные события, представляющие угрозу безопасности дому, находящемуся в нем имуществу, а также самим домовладельцам.

Работа состоит из четырех основных разделов: состояние вопроса, проектный раздел, конструктивно-экспериментальный раздел, экономический раздел. Для достижения поставленной в рамках данной работы цели решен ряд задач, а именно: рассмотрены существующие решения в области «умных» систем безопасности; разработана структурная схема системы, разработан алгоритм работы системы, выбрано необходимое аппаратное обеспечение и разработано соответствующее программное обеспечение; собрана рабочая модель спроектированной системы для проверки ее работоспособности и функциональности.

Степень внедрения: на основе спроектированной системы безопасности «Умного дома» возможна реализация полномасштабной системы, которую можно будет устанавливать в квартирах и частных домах. Рабочую модель спроектированной системы можно использовать для демонстрации ее возможностей.

ABSTRACT

The title of this bachelor's thesis is *Smart home security system based on microcontroller*.

Keywords: Smart home, security system, microcontroller, Arduino platform.

The popularity of Smart homes has been increasing vastly in recent years. One of the most useful and important applications of home automation is a home security, because safety is a really important part of our life.

The aim of this bachelor`s work is the development of the security system based on microcontroller that can protect homeowners and their property from different risks.

This work consists of four parts. The goal and targets of this final qualifying work were stated. The existing solutions were considered. The required electronic components were selected and the software part of the system was developed

The hardware of the proposed system contains Arduino open-source microcontroller, fire sensor, gas sensor to detect the harmful gas or the gas leakage, water sensor to detect the water leakage, reed switch to monitor invasions. The system uses relays and actuators to respond automatically to some events, such as a gas or water leakage. The system contains RFID access control system, so the homeowner can open a power door lock using RFID card. The system also contains Bluetooth module, so the user can control an Arduino board using his Android smartphone.

As a result of the bachelor's thesis, the working model of the proposed system was created using the same hardware and software parts to show the efficiency of the developed system.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Информационные технологии наряду с разработками в области электроники развиваются быстрыми темпами и значительно меняют образ жизни людей. Появляется возможность создания сложных сетей, состоящих из физических объектов и исполнительных механизмов, бытовых приборов и других электронных устройств, способных взаимодействовать друг с другом с помощью различных средств коммуникации. На основе таких сетей реализуется автоматизация процессов в самых разных областях, например: при производстве товаров и их транспортировке, в инженерных сетях зданий и сооружений, при охране и защите различных объектов. Грамотная автоматизация позволяет снизить влияние человеческого фактора, тем самым повышая эффективность и надежность системы, в которой она применяется.

Идеи межмашинного взаимодействия и создания различных «умных» сетей объединены в рамках парадигмы Интернета вещей. Одним из частных случаев данной парадигмы является технология домашней автоматизации, а жилой дом, в котором она используется, принято называть «Умным домом». Существует множество реализаций «Умного дома» на основе разных аппаратных и программных платформ, однако принято считать, что такой дом помимо управляющих устройств содержит в себе нескольких подсистем: систему освещения; систему тепло- и газоснабжения, а также вентиляции и кондиционирования; систему видеонаблюдения, систему электроснабжения; систему управления коммуникациями; систему безопасности.

В настоящее время широкое распространение получила так называемая распределенная архитектура «Умного дома», при которой каждая из его систем управляется своим контроллером и решает свои локальные задачи. Зачастую эти системы выпускаются различными производителями, используют для передачи данных разные протоколы и поэтому не связаны друг с другом. Иногда осуществление некоторых процессов в доме и вовсе доверяется отдельным «умным» устройствам: термостатам, лампочкам,

дверным замкам, бытовым приборам. Такая ситуация на рынке способствует быстрому росту популярности технологии домашней автоматизации, а потребитель может в любой момент масштабировать свой модульный «Умный дом», имея простор в выборе и установке понравившихся ему решений.

Конечно, «Умный дом» может создать для своих домовладельцев уютную и комфортную среду проживания: плавно включая свет, регулируя температуру и влажность воздуха, автоматически открывая жалюзи по утрам и в нужный момент поливая комнатные растения. Однако во все времена человек был в первую очередь заинтересован вопросами безопасности своего жилища и стремился сделать его максимально надежным и защищенным от разного рода угроз, исходящих как от природы, так и от других людей. По этой причине даже сегодня домовладельцы начинают превращение своих домов в «умные» зачастую именно с установки различных систем безопасности, а сами эти системы и «умные» охранные приборы занимают значительную долю на рынке домашней автоматизации, что доказывает *актуальность темы* данной бакалаврской работы.

Целью данной бакалаврской работы является разработка системы безопасности «Умного дома» на основе микроконтроллера, которая должна фиксировать и в некоторых случаях предотвращать аварийные события, представляющие угрозу безопасности дому, находящемуся в нем имуществу, а также самим домовладельцам.

1 СОСТОЯНИЕ ВОПРОСА

1.1 Формулирование актуальности, цели и задач работы

«Умный дом» является примером использования глобальной технологической парадигмы, получившей название Интернет вещей.

Годом зарождения данной парадигмы принято считать 1999 год, когда в Массачусетском технологическом институте было создано подразделение, занимающееся разработкой технологии радиочастотной идентификации RFID (Radio Frequency Identification) [1].

В настоящее время Интернет вещей позволяет объединить электронные устройства и связанные с ними с помощью беспроводных, а иногда проводных технологий физические объекты в масштабные сети, принцип действия которых основан сборе информации, ее хранении, обработке и, как результат, принятии определенных решений (рисунок 1).

Рисунок 1 — Составляющие Интернета вещей.

Сбор данных в Интернете вещей происходит в первую очередь с помощью датчиков — электронных устройств, способных обнаруживать изменение определенных параметров внешней физической среды и генерировать соответствующий электрический сигнал. Все собираемые «умной» системой данные с помощью специального программного обеспечения обрабатывает некое управляющее устройство, в качестве которого в большинстве случаев выступает микроконтроллер. После обработки информации микроконтроллер может задействовать различные исполнительные механизмы.

Датчики в большинстве современных систем являются беспроводными и для передачи данных используют специальные протоколы, например Bluetooth, ZigBee, Z-Wave. Беспроводные технологии с малым радиусом действия, такие как RFID и NFC (Near Field Communication), широко применяются для идентификации объектов, а протокол Wi-Fi и GSM-связь (Global System for Mobile Communications) в основном используются для удаленного обмена данными с пользователем (рисунок 2).

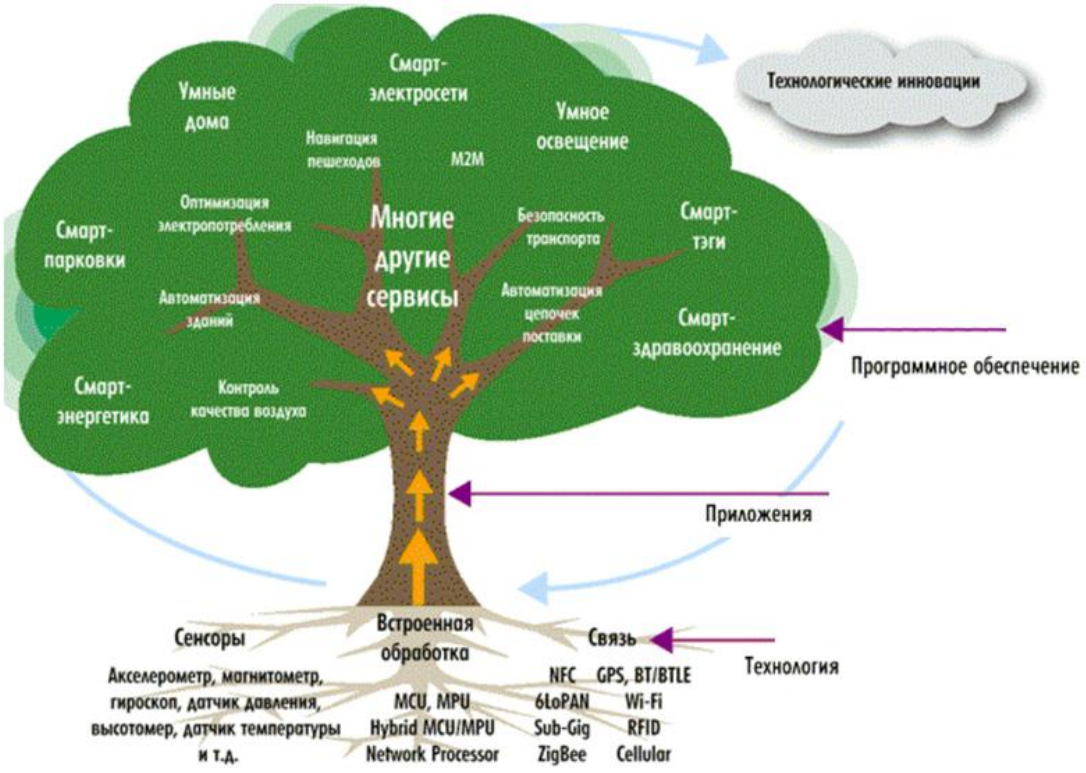

Рисунок 2 — «Экосистема» Интернета вещей.

Интернет вещей важен не только для таких корпораций как Google, Amazon, Microsoft, Samsung, но и обсуждается на правительственном уровне во многих странах. Так, в США (Соединенные Штаты Америки) Интернет вещей включен в список прорывных технологий, способных существенно повлиять на все области деятельности человека [2].

Численность электронных устройств, подключенных к сети Интернет, существенно превышает население планеты Земля, и с каждым годом эта разница только увеличивается. Ожидается, что к 2020 году более 50 миллиардов электронных устройств будут объединены между собой [3]. К уже существующим областям применения Интернета вещей будут добавляться многочисленные новые (рисунок 3).

Рисунок 3 — Этапы развития технологии Интернета вещей.

Однако стоит признать, что многие возможности Интернета вещей все еще не находят широкого применения. И еще меньшее количество его возможностей доступно для понимания конечному пользователю, который не всегда обладает нужными техническими знаниями. Как итог, в лидирующих позициях применения Интернета вещей находится именно домашняя

автоматизация, так ее возможности могут быть полезны многим домовладельцам, методы и способы ее реализации хорошо известны и постоянно совершенствуются, а конечному пользователю не составляет труда понять логику ее работы.

Согласно данным исследовательской компании TechNavio, на данный момент в мире насчитывается примерно 50 млн «Умных домов», при этом их количество постоянно увеличивается [4]. Статистика роста «Умных домов» на рынке приведена на рисунке 4.

Рисунок 4 — Прогноз количества «Умных домов» в мире.

В России темпы развития данной технологии не так велики: количество «Умных домов» на отечественном рынке жилья составляет всего 3% от общего объема всех жилых домов в стране. В то же время по результатам опроса, проведенного Высшей школой экономики, около 42% россиян выразили желание опробовать системы «Умных домов» [5].

При этом важно отметить, что, согласно консалтинговой компании PwC, устройства, относящиеся к системам безопасности «Умного дома», имеют высокий потенциал роста [6]. Сравнение потенциалов роста различных «Умных устройств» приведено на рисунке 5.

Рисунок 5 — Потенциал роста различных устройств «Умных домов».

Такому направлению потребительского спроса есть объяснение: надежное и защищенное жилище позволяет человеку добиться собственной безопасности, а также безопасности своих близких и своего имущества. Так было во все времена, однако с появлением новых технологий методы и средства защиты своего дома изменились: теперь люди устанавливают современные датчики, камеры видеонаблюдения, системы контроля и управления доступом, различные средства удаленного мониторинга и управления [7].

Таким образом, существующий на рынке «Умных домов» высокий спрос на системы безопасности является подтверждением *актуальности темы* данной бакалаврской работы.

Целью данной бакалаврской работы является разработка системы безопасности «Умного дома» на основе микроконтроллера, которая должна фиксировать и в некоторых случаях предотвращать аварийные события, представляющие угрозу безопасности дому, находящемуся в нем имуществу, а также самим домовладельцам.

Задачи, которые необходимо решить в рамках данной работы для достижения поставленной цели: провести анализ существующих решений в области систем безопасности «Умного дома»; выбрать подходящее аппаратное обеспечение; разработать необходимое программное обеспечение; собрать рабочую модель спроектированной системы для проверки ее работоспособности и функциональности.

1.2 Обзор известных решений

Домашние охранные системы, по своим функциональным возможностям близкие к технологиям «Умных домов», начали активно применяться еще до начала широкого распространения домашней автоматизации.

Например, примерно с 2000-х гг. начали появляться так называемые домашние GSM-сигнализации, состоящие в общем случае из контроллера, связанного с ним GSM-модуля и набора датчиков [8]. При возникновении какой-либо аварийной ситуации домовладелец может получить от GSM-сигнализации тревожный сигнал на свой мобильный телефон посредством GSM-связи в виде SMS-сообщений (Short Message Service) и посредством этой же связи может управлять настройками системы (рисунок 6).

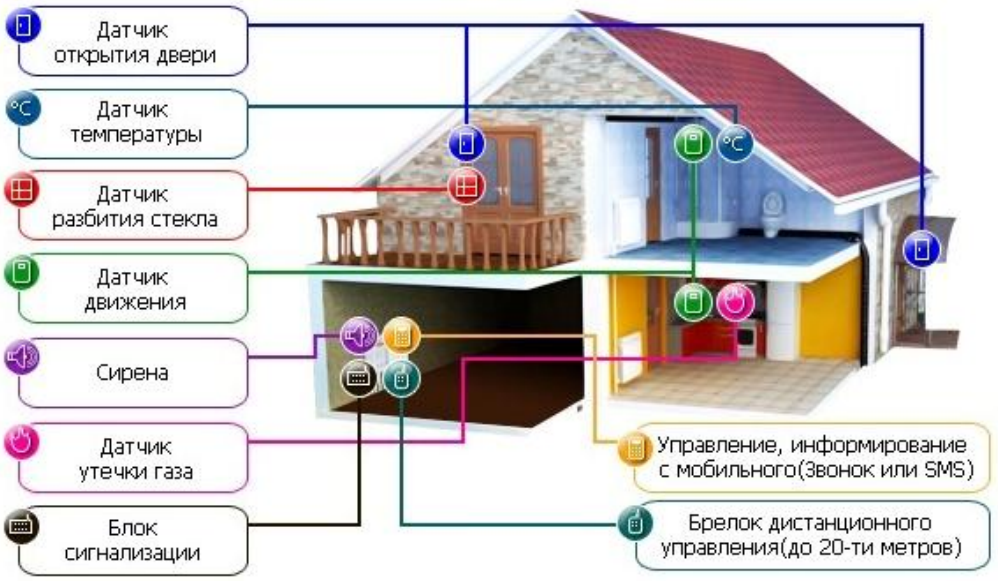

Рисунок 6 — Пример построения домашней GSM-сигнализации.

Недостаток GSM-сигнализации заключается в том, что в большинстве случаев она «пассивная», то есть не имеет в своем составе исполнительных механизмов: при протечке воды или утечке газа она не сможет перекрыть их подачу, а только будет генерировать соответствующие тревожные сигналы для уведомления пользователя или профессиональной службы охраны.

Примерно в 2010-х гг. в качестве способа дистанционного обмена информацией между системой безопасности и пользователем или охранной службой начал использоваться Интернет. Система подключается к Интернету с помощью протокола Wi-Fi, а пользователь «общается» с ней через специальное приложение на своем мобильном телефоне, который также должен иметь доступ к Интернету. Кроме того, Интернет обладает возможностью передачи больших пакетов данных, которые невозможно передать с помощью GSM-связи, благодаря чему через приложение на мобильном телефоне становится возможным в режиме реального времени просматривать получаемое с установленных в доме Wi-Fi видеокамер изображение. Таким образом, домашние системы безопасности с подключением к Интернету являются наиболее популярными на сегодняшний день решениями, но, стоит заметить, в них в качестве

резервного канала часто используется и GSM-связь [9]. Пример такой системы представлен на рисунке 7.

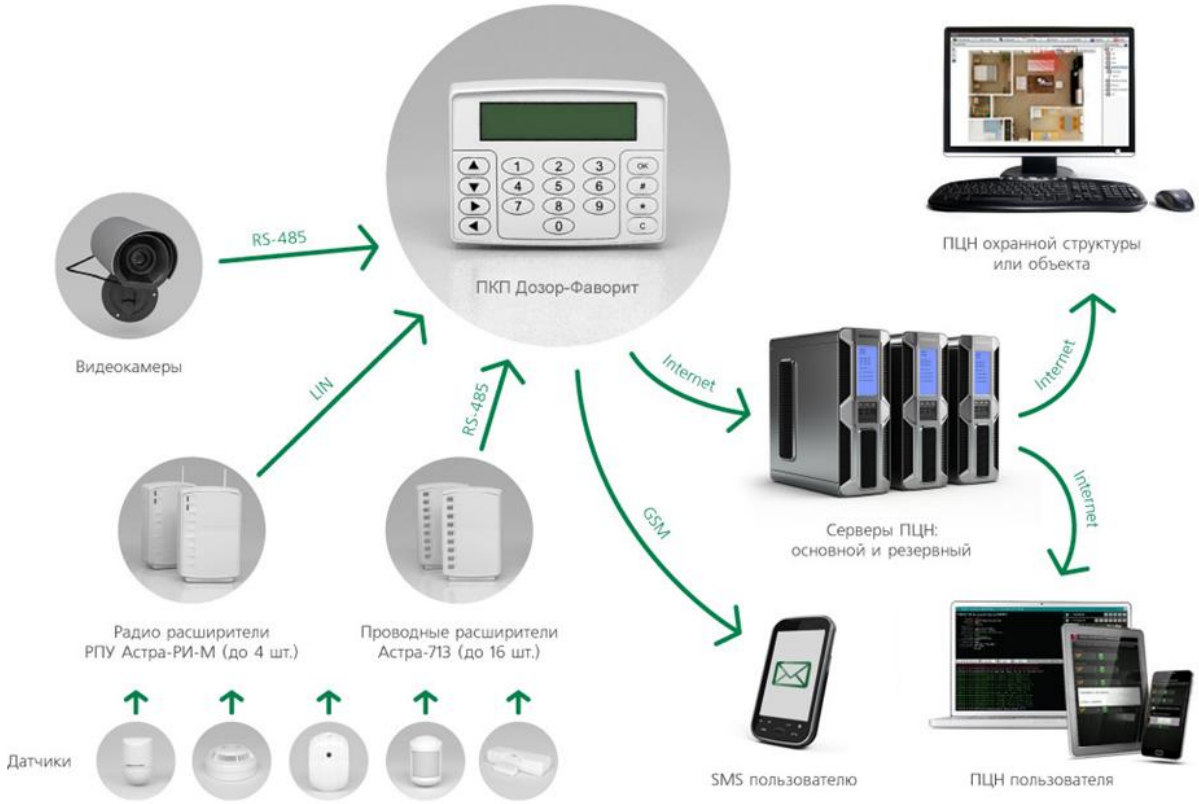

Рисунок 7 — Пример построения домашней системы безопасности с подключением к сети Интернет.

Все домашние системы безопасности делятся на две большие группы: проводные и беспроводные, то есть устройства, составляющие эти системы, для передачи данных используют либо провода, либо, соответственно, протоколы беспроводной передачи данных [10].

В настоящее время широкую популярность получили именно беспроводные технологии передачи данных. Во-первых, происходит существенное снижение затрат на установку и обслуживание системы, поскольку нет необходимости в покупке кабелей и их профессиональной укладке. Во-вторых, мобильность системы: в силу отсутствия проводов пользователь может часто менять расположение датчиков по своему усмотрению. В-третьих, благодаря беспроводным сетям в систему «Умного

дома» можно интегрировать мобильный телефон домовладельца, используя для этого, например, Wi-Fi, Bluetooth или GSM-связь [11].

Однако системы с беспроводной передачей данных имеют ряд недостатков. Во-первых, электромагнитные волны, используемые при беспроводной передаче данных, могут быть «заглушены» злоумышленником или подвергнуты различным наводкам и помехам со стороны других источников электромагнитного излучения, что может привести к ошибкам при передаче данных и случайным срабатываниям устройств. Во-вторых, большинство беспроводных протоколов передачи данных имеют относительно большой радиус действия, что означает возможность подключения к сети злоумышленника, находящегося вне пределов охраняемой территории, но в пределах действия сети [12]. В-третьих, беспроводные датчики в большинстве работают от батареек, что вынуждает пользователя периодически делать их замену, а к самим датчикам предъявляются жесткие требования в плане энергетический эффективности работы, на что существенно влияет используемый в системе протокол передачи данных [13].

Таким образом, окончательный выбор способа передачи данных между устройствами системы безопасности «Умного дома» остается за домовладельцем, так как оба способа имеют свои преимущества и недостатки. При этом стоит отметить, что возможны комбинированные способы: датчики и исполнительные механизмы имеют проводное подключение к центральному контроллеру, но для связи с пользователем или службой охраны центральный контроллер может использовать беспроводные технологии.

Таким образом, на сегодняшний день на рынке домашней автоматизации существует большой выбор как комплексных систем безопасности, так и отдельных «умных» устройств, однако большинство существующих решений можно разделить на три основные категории:

пожарно-охранные системы; *системы защиты от протечек воды и утечек газа*; *системы контроля и управления доступом (СКУД)*.

Рассмотрели каждую из данных категорий отдельно.

Пожарно-охранные системы в общем случае состоят из следующих датчиков: открытия двери/окна, движения, дыма [14]. В таких системах могут иметься, в том числе, и датчики протечки воды и утечки газа, однако решения с непосредственной защитой от данных аварийных ситуаций принято относить к отдельной категории. Пример построения типовой пожарно-охранной системы представлен на рисунке 8.

Рисунок 8 — Типовая домашняя пожарно-охранная сигнализация.

Панель управления системой рекомендуется устанавливать в местах, трудно заметных для потенциального злоумышленника. Постановка системы в режим охраны и отключение этого режима обычно осуществляется «скрытой кнопкой», расположение которой должен знать только домовладелец.

Типовой алгоритм работы такой системы следующий: перед выходом из дома пользователь ставит систему в режим охраны. Если в момент его отсутствия срабатывает какой-то из датчиков, то включается звуковая и световая сигнализация, а на мобильный телефон пользователя приходит соответствующее уведомление. Однако систему нужно настроить так, чтобы при возвращении домовладельца домой она не включала сигнализацию при обнаружении присутствия самого домовладельца. Когда пользователь вернулся домой, на снятие системы с режима охраны отводится некоторый установленный промежуток времени. Пользователь знает расположение «скрытой кнопки», управляющей режимами работы системы, и поэтому вовремя снимает систему с охраны, но при этом сигнализация может сработать на потенциального злоумышленника, не знающего о задержке на выключение и о расположении этой кнопки,

В *системах защиты от протечек воды и утечек газа* ключевую роль играют исполнительные механизмы, которые отсекают подачу, соответственно, воды или газа. Кроме того, если системы защиты от данных аварийных ситуаций связаны с системой электроснабжения дома, то в случае возникновения аварийной ситуации имеется возможность отключить подачу электричества на все бытовые приборы в доме, а системы защиты от протечки воды или утечки газа продолжат работу от встроенных аккумуляторов.

Типовой пример построения системы защиты от протечек воды представлен на рисунке 9.

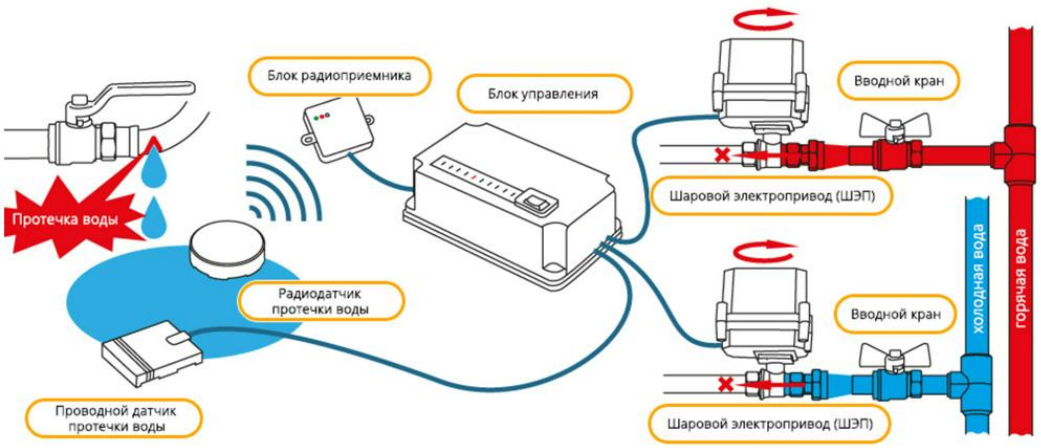

Рисунок 9 — Пример построения системы защиты от протечек воды.

Датчик протечки воды размещается в тех помещениях и местах, в которых возможна протечка воды: под ванной, рядом со стиральной машиной и так далее. При попадании воды на контактную поверхность датчика сигнал от датчика поступает на блок управления, который задействует шаровые клапаны с электроприводом, установленные на водопроводных трубах для холодной и горячей воды, тем самым перекрывая подачу воды до тех пор, пока домовладелец самостоятельно не перезагрузит систему или вручную не откроет клапаны. Некоторые функции, которые могут иметь системы защиты от протечек воды: звуковое и световое оповещение при обнаружении протечки, дистанционное уведомление пользователя посредством SMS-сообщений или через Интернет, работа от встроенных аккумуляторов в случае отключения основного источника электроэнергии.

Система защиты от утечек газа работает по принципу, схожему с системой защиты от протечек воды и устанавливается в помещениях с газовым оборудованием: котельные, кухонные комнаты. Газоанализатор, то есть датчик газа, фиксирует утечку газа, если его концентрация в воздухе превышает некоторое пороговое значение. Далее газоанализатор подает соответствующий сигнал на контроллер, а тот, в свою очередь, задействует электромагнитный клапан, перекрывающий подачу газа (рисунок 10).

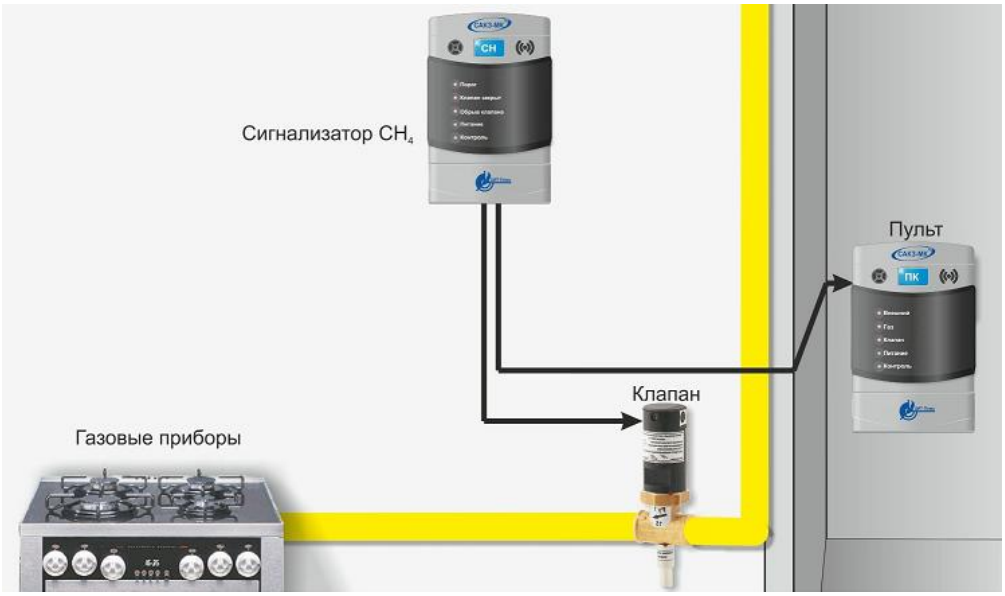

Рисунок 10 — Общее устройство системы защиты от утечки газа.

Использование *СКУД* в «Умных домах» в большинстве случаев сводится к установке «умных» дверных замков. Такие замки имеют несколько способов для идентификации пользователя: ввод пароля на наборной панели, использование технологии RFID или NFC, с помощью биометрических данных пользователя, а также комбинацией этих способов.

В качестве примера для рассмотрения выбрали модель дверного замка SHS-P718 от компании Samsung (рисунок 11).

Рисунок 11 — «Умный» дверной замок от Samsung.

Благодаря встроенному в корпус замка инфракрасному датчику движения, замок активируется, когда человек вплотную подходит к двери. Имеется возможность активации тревожного сигнала в случае, если кто-то стоит рядом с дверью в течение одной минуты без попыток открыть замок. Возможные способы идентификации пользователя: ввод кода на наборной панели, считывание RFID-карты, считывание отпечатка пальца, а также комбинированные способы. При попытке нанести замку механические повреждения активируется звуковая сигнализация. От попыток взлома программного кода замок защищен специальными методами шифрования. Кроме того, в замок встроен датчик дыма и при его срабатывании также активируется сигнал тревоги. Замок работает от батареек и при низком уровне их заряда начинает с помощью специальных звуковых сигналов уведомлять об этом пользователя. Если батарейки все же разрядились, то в корпусе замка предусмотрена личинка для обычного механического ключа, а также разъем для подключения батарейки «Крона». «Умные» замки от Samsung могут быть объединены в единую сеть с другими «умными» устройствами компании: телевизорами, холодильниками, стиральными машинами, духовыми шкафами. Управление всеми устройствами осуществляется с помощью мобильного телефона домовладельца.

На российском рынке «Умных домов» одним из лидеров является компания Rubetek. Она предлагает как отдельные «умные» устройства, так и готовые комплекты, один из которых называется «Управление и безопасность». В его состав входят: модуль управления, датчик протечки, датчик открытия, датчик дыма. Однако пользователь может собрать свою собственную систему из любых понравившихся ему устройств от данного производителя: центр управления, поворотные Wi-Fi камеры, датчик утечки газа, датчик открытия, датчик протечки, датчик движения, датчик дыма, а также «умные» розетки и многоканальные реле (рисунок 12).

Рисунок 12 — Система безопасности «Умного дома» от Rubetek.

Все датчики работают от батареек и являются беспроводными: обмен данными осуществляется на частоте 433 МГц по протоколу EV 1527. Пользователь управляет системой и получает от нее уведомления через Интернет с помощью специального приложения для мобильного телефона. Пример построения системы «Умного дома» на основе устройств от данной компании представлен на рисунке 13.

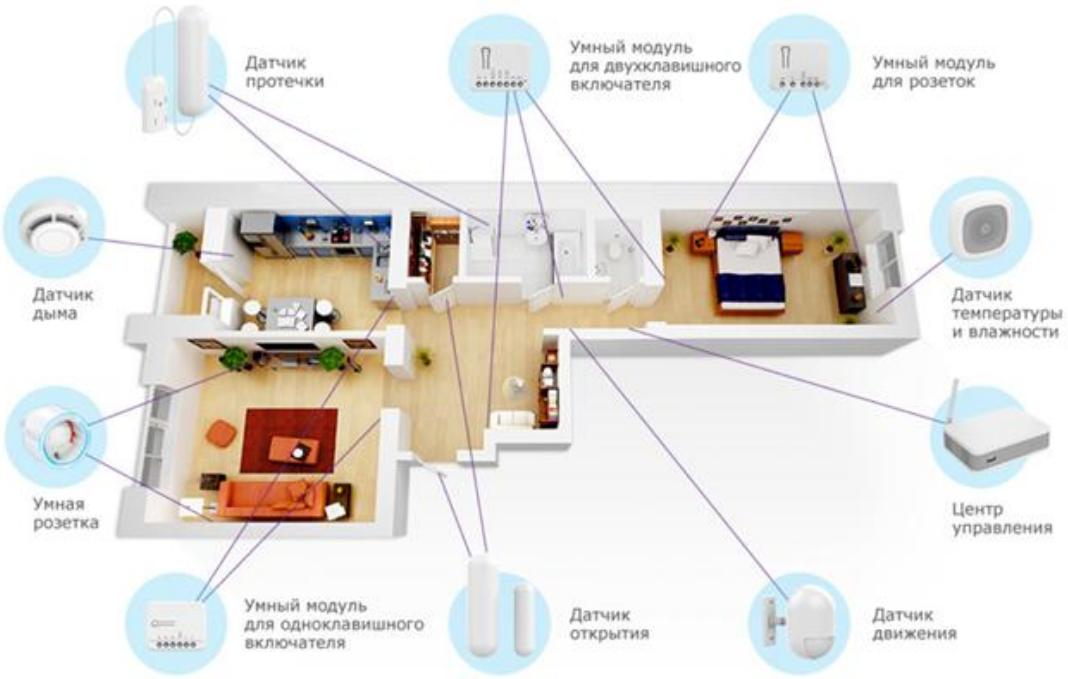

Рисунок 13 — Пример расположения элементов «Умного дома» от компании Rubetek.

Широкое признание на рынке охранных систем получила «умная» сигнализация Ajax украинского производства. Данная охранная система состоит из управляющего устройства и набора датчиков. Управление настройками системы осуществляется с помощью приложения для мобильного телефона. Для обмена данными между устройствами компания разработала собственный протокол передачи данных Jeweller, использующий для работы одну из нескольких радиочастот: если злоумышленник решит «заглушить» систему, то она автоматически переключится на другую частоту и продолжит функционировать. При попытке вскрытия корпуса любого из устройств система активирует сигнализацию, так как сработают встроенные в корпусы устройств датчики вскрытия.

Перечень предлагаемых производителем датчиков: датчик движения, датчик разбития стекла, датчик детектирования дыма, датчик обнаружения затопления, датчик открытия двери/окна (рисунок 14).

Рисунок 14 — «Умная» охранная система Ajax.

Таким образом, большинство существующих на сегодняшний день систем безопасности, применяемых в «Умных домах», фиксируют возникновение следующих аварийных ситуаций: возникновение очага возгорания, протечку воды, утечку бытового газа, проникновение посторонних лиц. Для этого они имеют в своем составе: датчик огня, датчик протечки воды, датчик утечки газа, датчики проникновения (датчик открытия двери или окна, датчик разбития оконного стекла, датчик движения). Для уведомления пользователя используется звуковое или световое оповещение, а для дистанционного уведомления и управления системой: GSM-связь, Интернет, Bluetooth.

2 ПРОЕКТНЫЙ РАЗДЕЛ

2.1 Разработка структурной схемы

На основе анализа существующих решений определили, какие именно аварийные ситуации должна фиксировать проектируемая система безопасности «Умного дома», а именно: протечку воды, утечку бытового газа, возникновение очага возгорания, проникновение посторонних лиц. Из данных аварийных ситуаций система должна уметь предотвращать протечку воды и утечку бытового газа. В случае возникновения какой-либо аварийной ситуации система должна оповещать пользователя с помощью сигнального устройства, а сам пользователь должен иметь возможность дистанционно управлять системой. Должна иметься подсистема контроля и управления доступом.

Таким образом, проектируемая система должна содержать в себе несколько основных структурных блоков (рисунок 15).

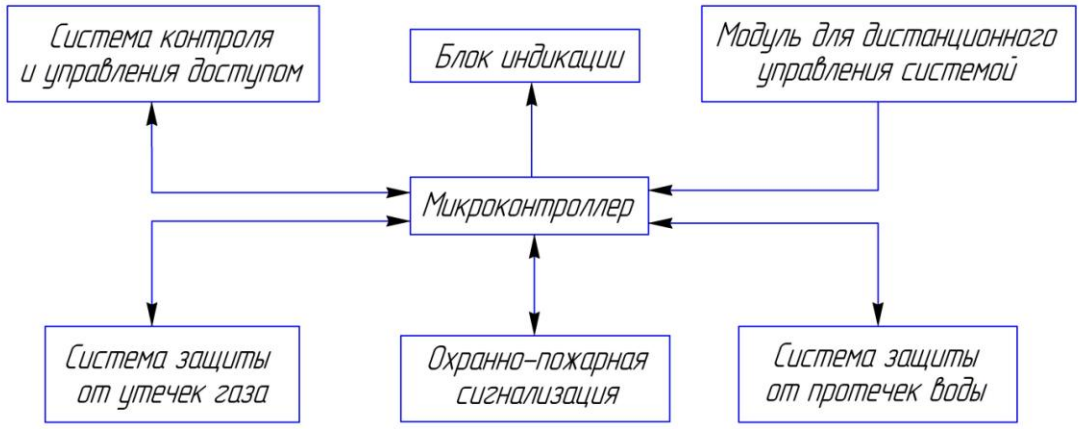

Рисунок 15 — Структурная схема проектируемой системы безопасности «Умного дома» на основе микроконтроллера.

Управляющим устройством проектируемой системы является *микроконтроллер*. Его преимущества по сравнению с одноплатными компьютерами или промышленными контроллерами заключаются в низкой

стоимости, малом потреблении электроэнергии, а также малых габаритах, при этом микроконтроллеры обладают достаточными возможностями для создания гибких и функциональных систем.

Блок индикации содержит в себе устройства для оповещения пользователя в заранее определенных случаях, а именно: дисплей для вывода информации, а также сигнальное устройство.

Охрано-пожарная сигнализация обнаруживает проникновение посторонних лиц, а также возникновение очага возгорания. В своем составе она имеет: датчик открытия входной двери и датчик огня.

Система защиты от протечек воды состоит из соответствующего датчика протечки воды, а также исполнительного механизма, перекрывающего подачу воды. *Система защиты от утечек газа* состоит из соответствующего датчика утечки газа, а также исполнительного механизма, перекрывающего подачу газа.

Система контроля и управления доступом состоит из устройства для идентификации пользователя, а также электромагнитного замка.

Возможность дистанционного управления системой осуществляется с помощью соответствующего модуля, работающего по одной из беспроводных технологий.

Однако на рынке домашних систем безопасности существует большой выбор не только различных датчиков, но и исполнительных механизмов: различные устройства для перекрытия подачи воды; устройства для перекрытия подачи газа, а также принудительной вентиляции помещения в случае его утечки; электромагнитные замки в системах контроля и управления доступом. Выбор таких исполнительных механизмов зависит от множества разных факторов, например: при выборе механизма для перекрытия подачи воды надо учитывать давление в соответствующем трубопроводе, при выборе механизма для принудительной вентиляции воздуха в помещении надо учитывать площадь этого помещения. Сигнальные звуковые и световые устройства, срабатывающие в случае

возникновения какой-либо аварийной ситуации, также требуют тщательного выбора. В связи с этим в рамках данной работы при проектировании системы безопасности «Умного дома» не производится выбор непосредственно исполнительных механизмов. Для разработки структурной схемы и последующих этапов проектирования приняли, что при возникновении аварийной ситуации микроконтроллер должен задействовать только сами коммутирующие устройства, например реле. С помощью коммутирующих устройств можно напрямую управлять работой исполнительных механизмов, конечный выбор которых остается за пользователем и никак не влияет не алгоритм работы системы.

Таким образом, более подробная структурная схема проектируемой системы безопасности представлена на рисунке 16.

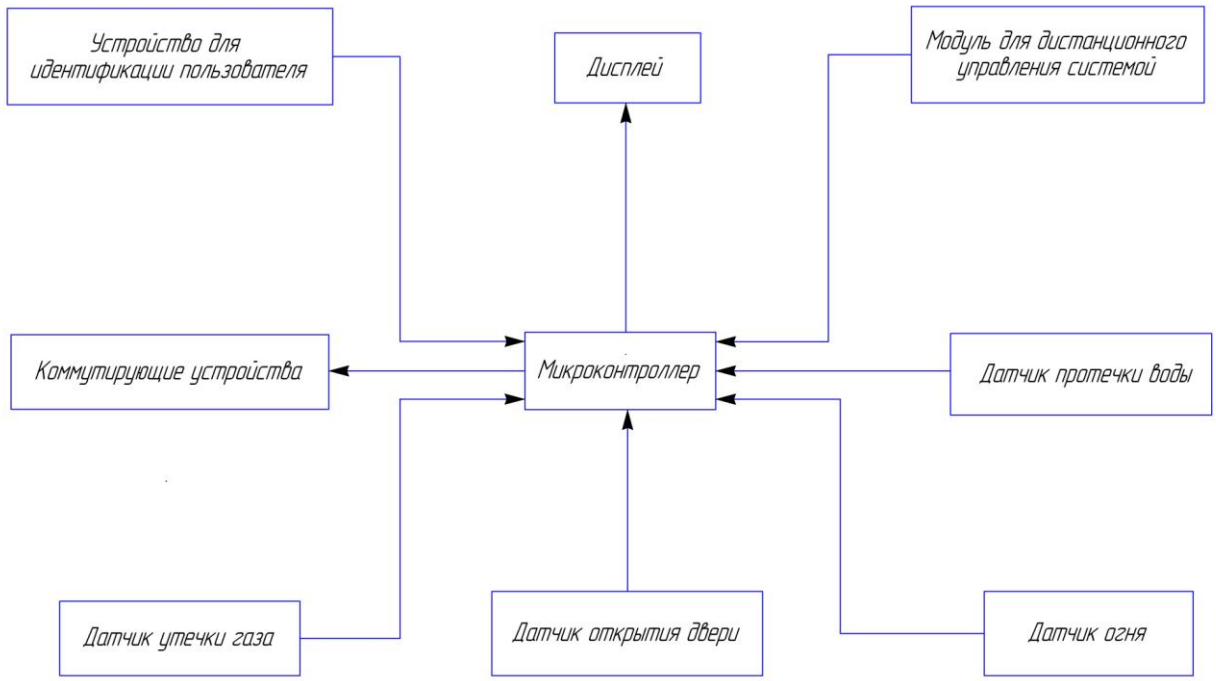

Рисунок 16 — Структурная схема проектируемой системы безопасности «Умного дома».

2.2 Разработка алгоритма работы

Проектируемая система безопасности «Умного дома» должна иметь два режима работы: «охрана отключена» и «охрана включена».

В режиме «охрана отключена», который является исходным и активируется сразу после подачи питания на систему, опрашиваются только датчики протечки воды, утечки газа, огня. Эти датчики отслеживают возникновение наиболее опасных аварийных ситуаций и поэтому при наличии питающего напряжения должны работать постоянно в целях защиты от их случайного отключения. При срабатывании любого из данных датчиков задействуется блок индикации: срабатывает сигнальное устройство, выводится соответствующая информация на дисплей. При обнаружении протечки воды должен срабатывать исполнительный механизм, перекрывающий ее подачу до тех пор, пока пользователь самостоятельно не отключит данный механизм (рисунок 17).

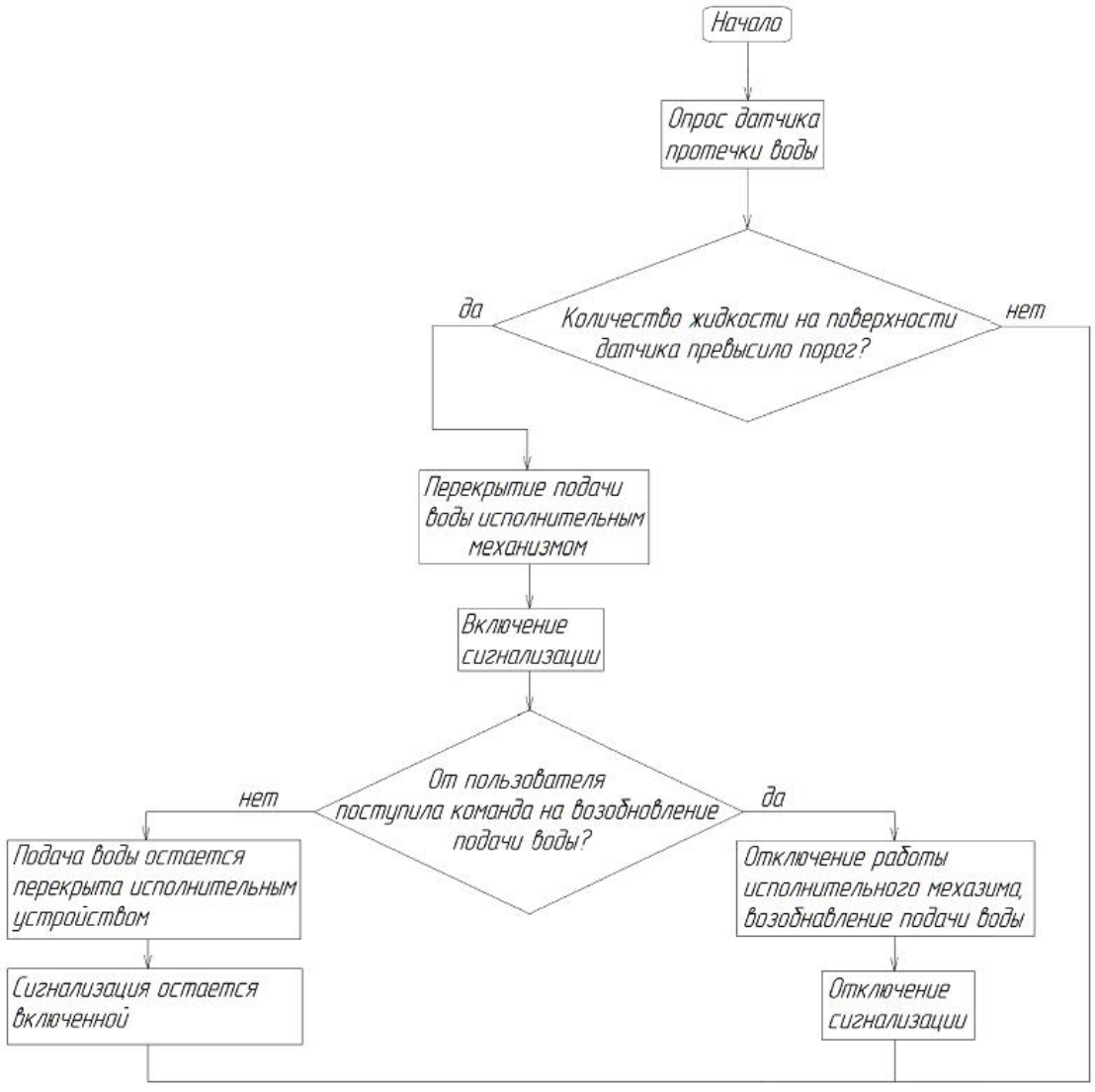

Рисунок 17 — Блок-схема алгоритма работы системы защиты от протечек воды.

Аналогично для системы защиты от утечек газа: при утечке газа исполнительный механизм перекрывает его подачу до тех пор, пока пользователь самостоятельно не отключит данный исполнительный механизм (рисунок 18).

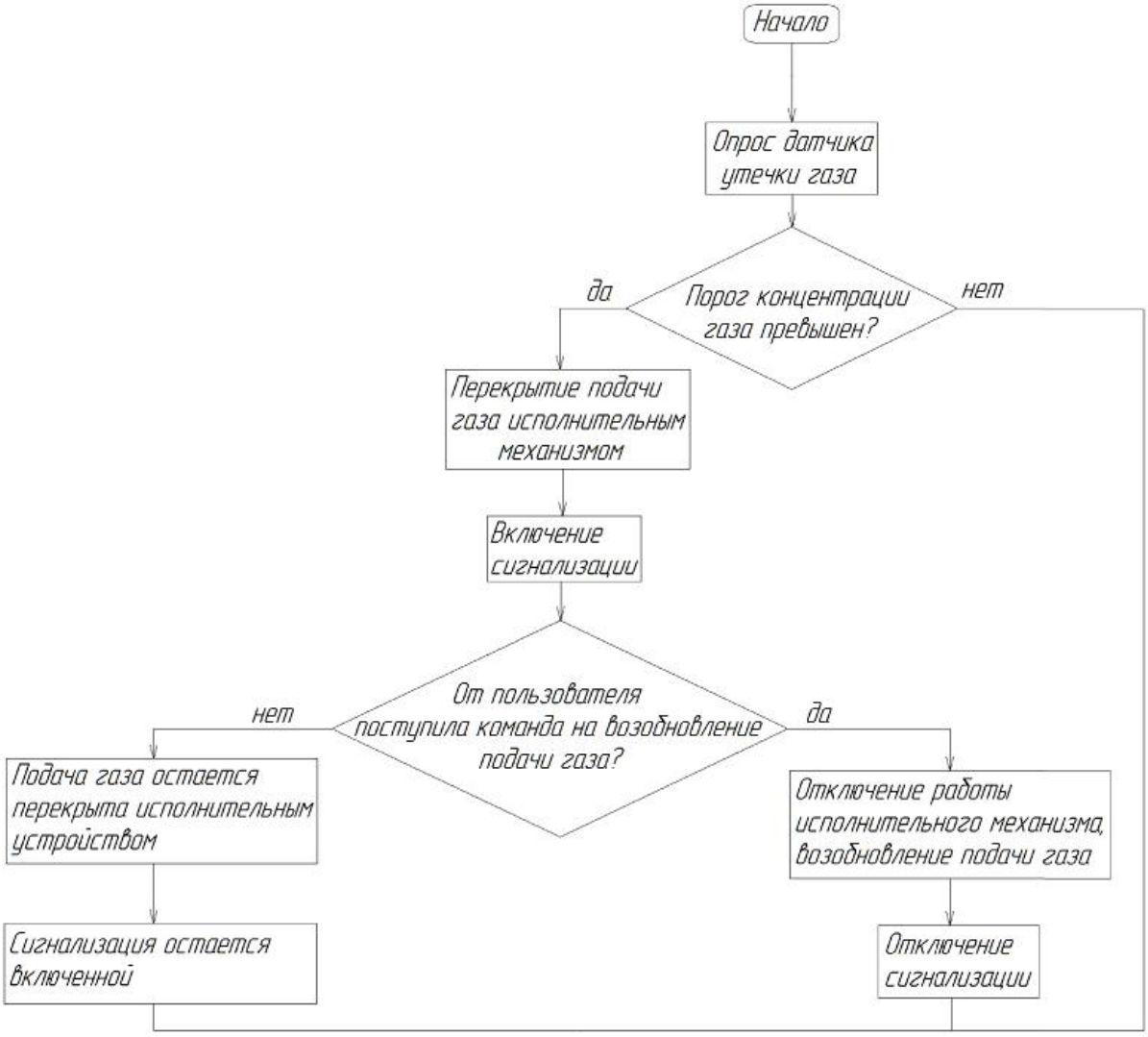

Рисунок 18 — Блок-схема алгоритма работы системы защиты от утечек газа.

Алгоритм работы системы при обнаружении возгорания: при возникновении очага возгорания соответствующий датчик огня фиксирует данную аварийную ситуацию и включается сигнализация. Сигнализация остается включенной, даже если источник пламени потушен или не фиксируется датчиком по какой-либо иной причине. Отключение сигнализации так же производится пользователем.

В обоих режимах работы проектируемой системы управление и контроль доступом осуществляется с помощью RFID-технологии и исполнительного механизма, в качестве которого выступает электромагнитный дверной замок. В микроконтроллере хранится уникальный идентификационный номер RFID-метки пользователя и при поднесении метки к RFID-считывателю последний осуществляет чтение номера метки и на основе сравнения полученного номера с номером, хранящимся в памяти микроконтроллера, разрешает или запрещает доступ (рисунок 19).

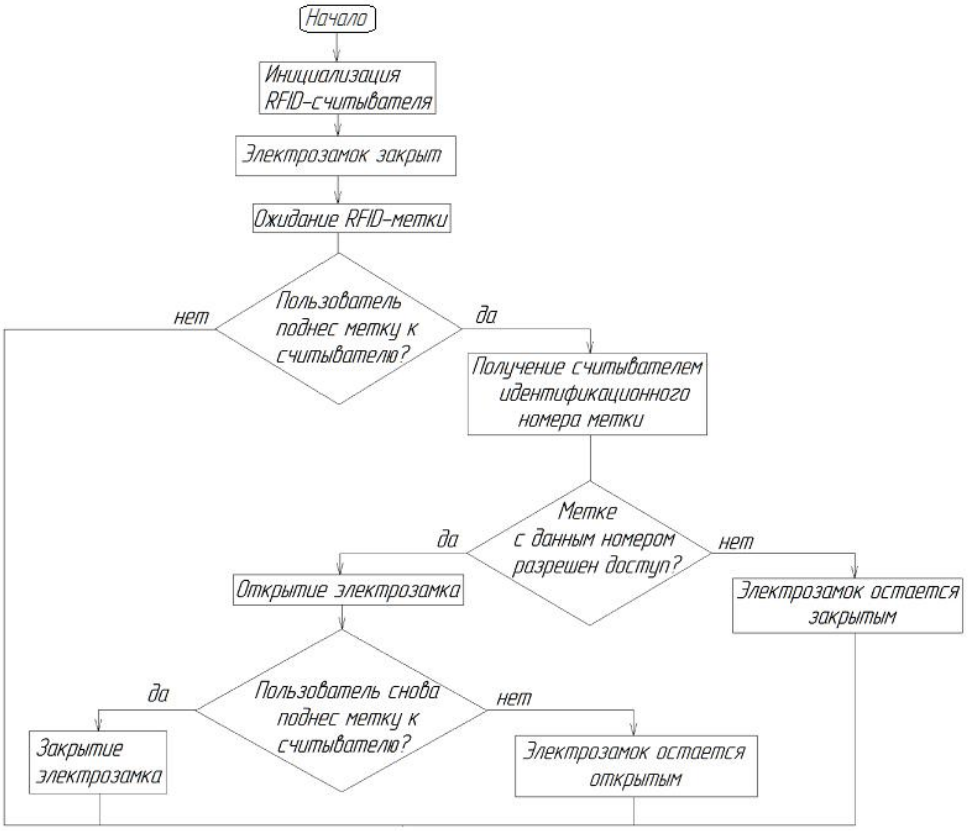

Рисунок 18 — Блок-схема алгоритма контроля доступа в проектируемой системе безопасности «Умного дома».

Открытие и закрытие дверного замка осуществляется с помощью одной метки и одного считывателя: сначала пользователь подносит свою RFID-метку, находясь снаружи входной двери, а затем, войдя внутрь своего дома или квартиры, он подносит метку к считывателю снова, чтобы закрыть за собой замок. Считыватель должен монтироваться в дверной замок таким

образом, чтобы была возможность считывания метки, когда пользователь находится с любой из сторон двери.

В режиме «охрана включена» опрашиваются не только датчики протечки воды, утечки газа, огня, но и датчик открытия входной двери. Режим «охрана включена» активируется пользователем, когда он уже вышел из дома или квартиры, то есть находится за входной дверью. Снятие системы с режима охраны также происходит за пределами дома или квартиры пользователя. В противном случае, если пользователь забыл снять систему с охраны и открыл входную дверь, активируется сигнализация — тогда пользователю нужно снять систему с охраны и сигнализация автоматически отключится (рисунок 20).

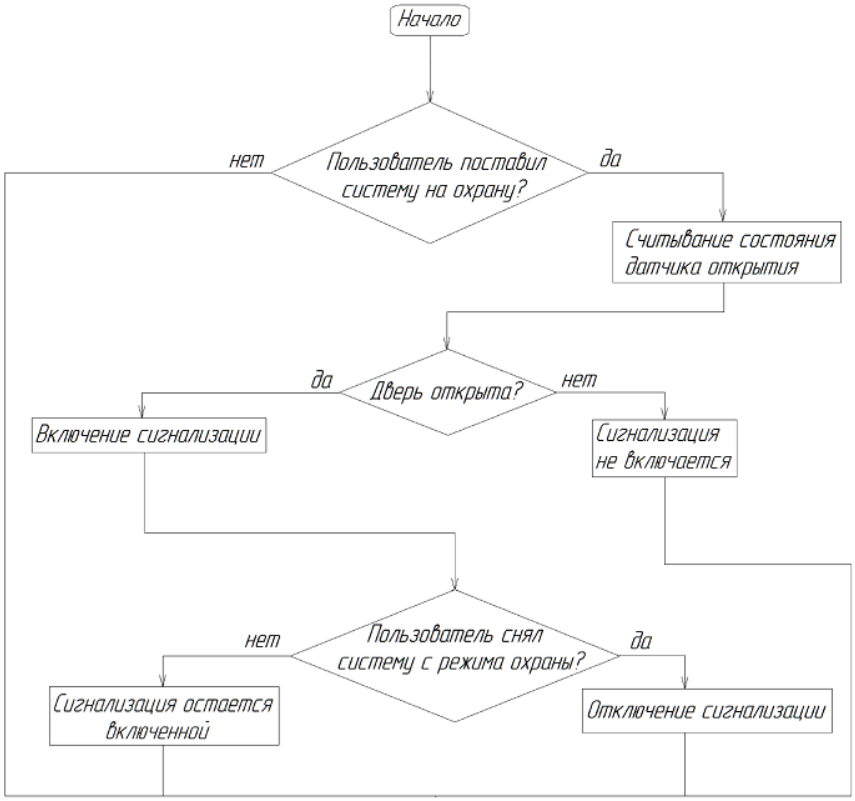

Рисунок 20 — Блок-схема алгоритма постановки системы в режим охраны и снятие системы с данного режима с помощью кнопки.

Отключение исполнительных устройств и сигнализации осуществляется без использования кнопок и других физических переключателей, но с использованием беспроводной технологии передачи

данных, например с помощью мобильного телефона пользователя и специальной установленной на нем программы.

2.3 Выбор необходимых компонентов

2.3.1 Проектируемая система безопасности «Умного дома» для работы согласно разработанному алгоритму должна иметь в своем составе ряд электронных элементов: микроконтроллер, датчики для фиксации аварийных событий, коммутирующие устройства для подключения исполнительных механизмов, дисплей для вывода различной информации, модуль для дистанционного управления системой пользователем.

В качестве аппаратно-программной платформы проектируемой системы была выбрана Arduino. Данная платформа с открытым исходным кодом включает в себя серию плат на основе 8-битных микроконтроллеров ATmega, совместимые с платами модули для решения различных задач (рисунок 21), а также среду разработки и отладки программ Arduino IDE (Integrated Development Environment).

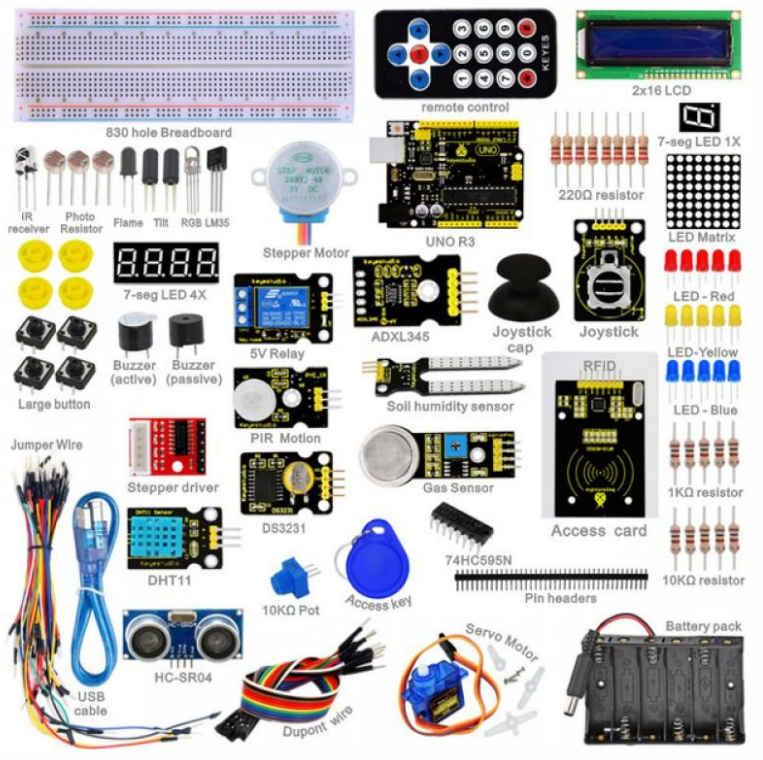

Рисунок 21 — Часть аппаратного обеспечения платформы Arduino.

Пример некоторых модулей, совместимых с платами Arduino: дисплеи, индикаторы, шаговые двигатели и сервоприводы, датчики, кнопки, реле, а кроме того, имеются модули и платы расширения, с помощью которых платформа может работать с современными технологиями Wi-Fi, Bluetooth, GSM, ZigBee, Ethernet, RFID, NFC

Платы Arduino помимо самого микроконтроллера содержат в своей конструкции различные компоненты: аналоговые и цифровые порты ввода-вывода информации, разъемы для питания и подключения к компьютеру, стабилизатор входного напряжения, интерфейс UART (Universal Asynchronous Receiver-Transmitter) и многое другое (рисунок 22).

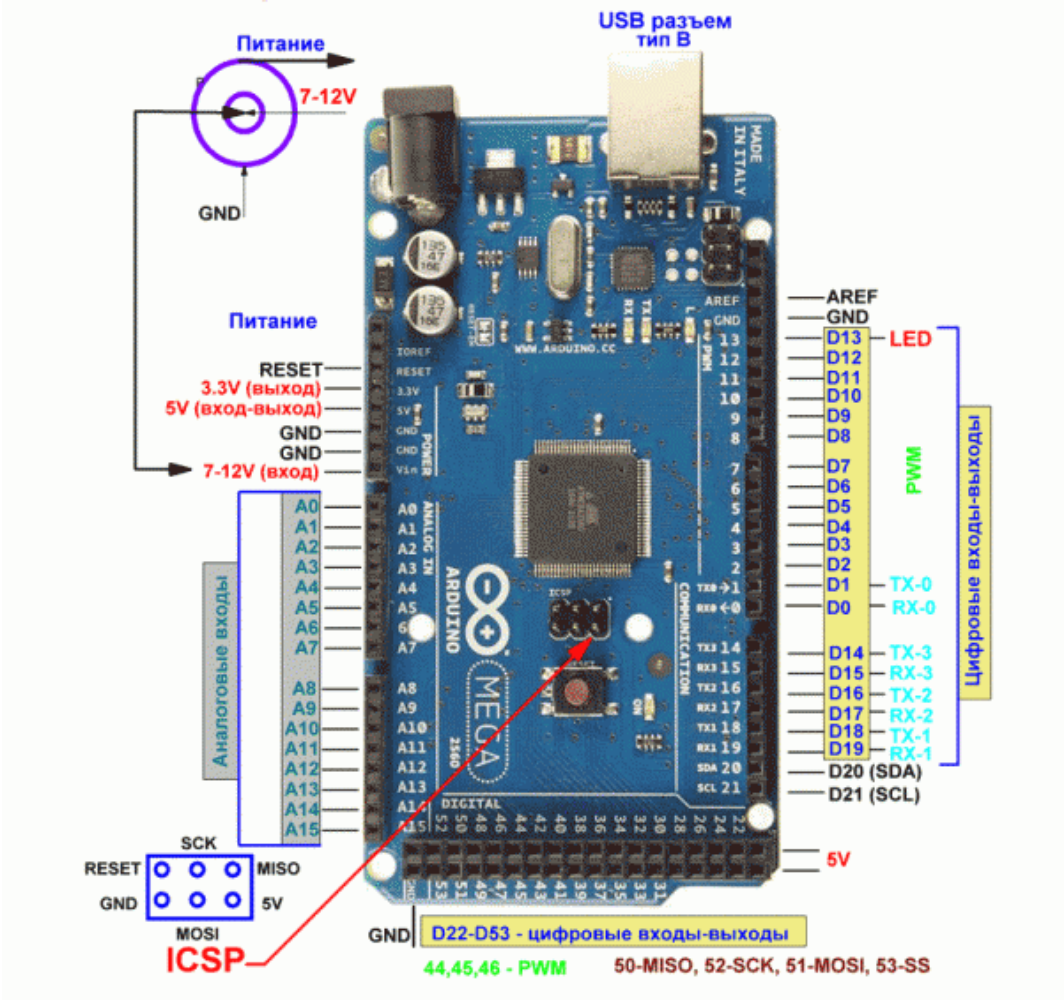

Рисунок 22 — Плата Arduino Mega 2560.

Из линейки плат Arduino стоит выделить две платы, наиболее часто встречающиеся в сложных электронных проектах и обеспечивающие

подключение относительно большого числа различных внешних устройств, а именно: плата Arduino Uno и плата Arduino Mega 2560. На основе сравнительного анализа этих двух плат в качестве центрального управляющего устройства проектируемой системы была выбрана плата Arduino Mega 2560 [15]. Данная плата оснащена «мощным» микроконтроллером и имеет наибольшее число портов ввода-вывода информации среди всех плат Arduino, что обеспечивает гибкость проектируемой системы в плане возможности ее дальнейшего масштабирования [16].

2.3.2 В проектируемой для вывода различной полезной информации необходим дисплей. С его помощью пользователь может получать информацию о фиксации того или иного аварийного события, о режиме работы схемы, о факте считывания незарегистрированной в памяти микроконтроллера RFID-метки, о включении коммутирующих устройств.

В качестве дисплей выбрали дисплей LCD-1602 HD44780 (рисунок 23).

Рисунок 23 — LCD-дисплей 16x2.

Данный дисплей можно подключить к плате Arduino с помощью интерфейса I2C (Inter-Integrated Circuit) с использованием всего четырех проводов: двух для питания и двух для обмена информацией [17].

Напряжение питания дисплея составляет от 3,3 до 5 В, яркость изображения регулируется потенциометром на I2C-модуле.

2.3.3 Для фиксации возникновения очага возгорания необходим датчик огня. Выбрали модель KY-026 (рисунок 24).

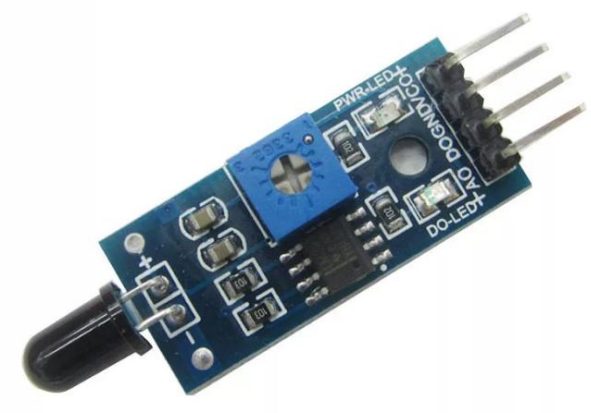

Рисунок 24 — Датчик огня KY-026.

Данный датчик реагирует электромагнитные волны, лежащие в области инфракрасного излучения, благодаря чему он может обнаруживать открытый огонь [18]. Однако при определенных условиях он может сработать и на яркий солнечный свет, исправить этот недостаток можно регулировкой чувствительности датчика. Рабочая дистанция датчика составляет до 4 м. Рабочее напряжение датчика находится в пределах от 3,3 до 5 В, максимальный ток потребления составляет 10 мА.

2.3.4 Для системы защиты от утечек газа выбрали модуль MQ-2 на основе полупроводникового газоанализатора MQ-2 (рисунок 25).

Рисунок 25 — Датчик газа MQ-2.

Данный модуль способен обнаруживать различные горючие и воспламеняющиеся газы, в том числе природный газ (метан, бутан, пропан) [19].

В своей конструкции газоанализатор имеет трубку из керамики, покрытую чувствительным слоем из диоксида олова. Внутри трубки находится специальный нагревательный элемент, обеспечивающий правильную работу датчика: нагретый чувствительный слой начинает реагировать на молекулы газа, концентрацию которого необходимо отслеживать. Концентрацию отслеживаемого газа можно контролировать с помощью аналогового сигнала, снимаемого с выхода датчика: чем выше концентрация этого газа, тем больше по величине выходное напряжение, и наоборот. Рабочее напряжение датчика находится в пределах от 3,3 до 5 В, ток потребления составляет 160 мА. Датчик, при подаче на него питания, требует несколько минут на нагрев чувствительного элемента, поэтому иногда возможны ложные срабатывания.

2.3.5 Для системы защиты от протечек воды выбрали модуль FC-37 [20]. Контактная поверхность датчика состоит из двух не связанных друг с другом токопроводящих дорожек: вода, при попадании одновременно на обе дорожки, замыкает их, тем самым вызывая срабатывание датчика (рисунок 26).

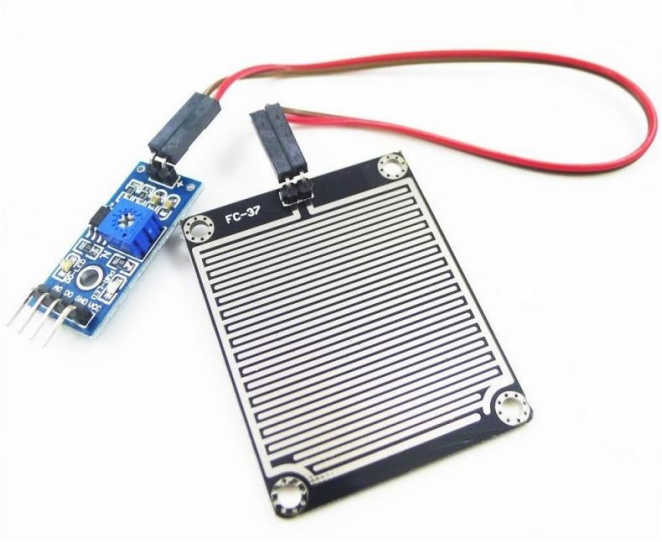

Рисунок 26 — Датчик протечки воды FC-37.

2.3.6 Для фиксации открытия входной двери выбрали датчик открытия KY-025. Данный модуль содержит в своей конструкции геркон (рисунок 27).

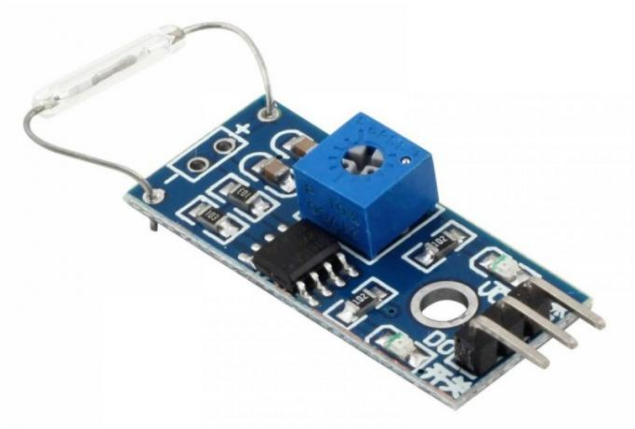

Рисунок 27 — Датчик открытия двери KY-025.

При отсутствии магнитного поля геркон нормально открыт, а при его появлении контакты геркона замыкаются. Сам датчик должен располагаться на неподвижной части конструкции (дверной раме), а магнит, создающий нужное магнитное поле, должен крепиться к подвижной части конструкции, то есть непосредственно к самой двери.

Данный модуль имеет рабочее напряжение от 3,3 до 5 В, способен выдержать протекание тока величиной до 1,2 А и имеет рабочее расстояние до 1,5 м [21].

2.3.8 Для контроля доступа выбрали модуль RC522 [22]. Для RFID-считывателя нужна RFID-метка, например RFID-карта (рисунок 28).

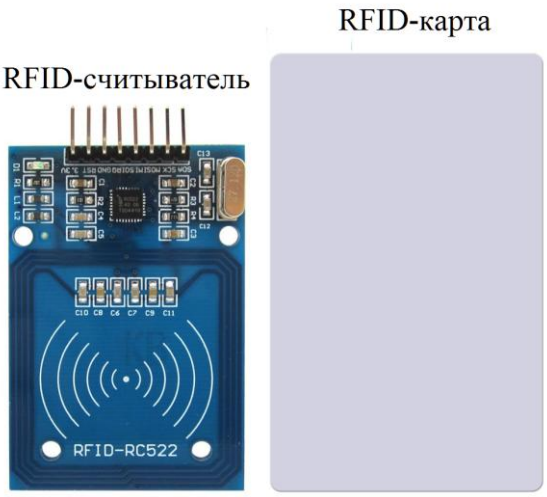

Рисунок 28 — RFID-система для платформы Arduino.

Рабочее напряжение RFID-считывателя RC522 составляет 3,3 В, а максимальный рабочий ток достигает 26 мА.

Технология RFID (радиочастотная идентификация) является надежной и экономичной технологией, созданной с целью автоматического распознавания объектов с использованием электромагнитных полей (рисунок 29).

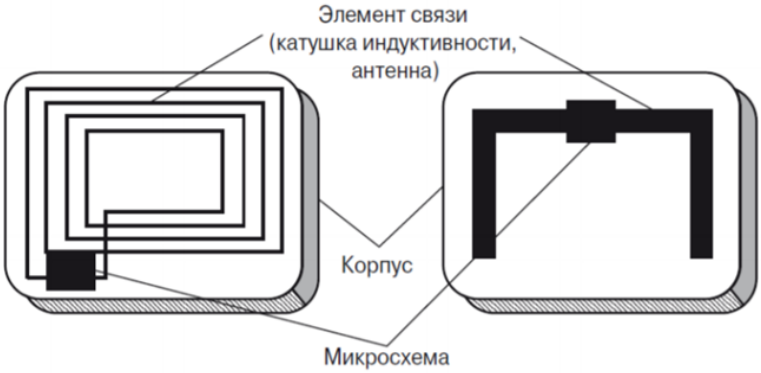

Рисунок 29 — Строение RFID-метки.

Система работает следующим образом. Внутри RFID-карты находится чип, хранящий в себе уникальный идентификационный номер в виде цифрового кода. Также в корпусе карты находится специальная антенна, принимающая и излучающая радиоволны. Считыватель генерирует радиоволну — антенна RFID-карты принимает ее, получая нужную для своей работы энергию. RFID-карта с помощью антенны излучает радиоволну той же частоты, что и пришедшая от считывателя волна, модулировав ее содержимым памяти чипа. Наконец, RFID-считыватель получает эту радиоволну от карты и декодирует ее, получая доступ к цифровому идентификационному номера именно данной RFID-карты [23].

2.3.9 Для подключения к плате Arduino различных исполнительных механизмов необходимы коммутирующие устройства. Выбрали модуль четырехканального реле (рисунок 30).

Рисунок 30 — Модуль четырехканального реле для Arduino.

Модуль работает от напряжения 5 В, ток потребления каждого из четырех реле составляет 70 мА. В данном модуле имеются обратные диоды, защищающие контакты реле, а также гальваническая развязка, защищающая выводы непосредственно самого микроконтроллера [24].

2.3.10 Для возможности дистанционного управления платой Arduino Mega 2560 выбрали Bluetooth-модуль HC-05 [25]. Конечно, технология Bluetooth не может обеспечить передачу данных на большие расстояния, в отличие от GSM-связи или же сети Интернет. Однако к важным преимуществам протокола Bluetooth следует отнести низкое энергопотребление, хорошую защищенность передаваемых данных, локализованный радиус действия.

Выбранный Bluetooth-модуль обменивается данными с платой Arduino по интерфейсу UART через выводы TX и RX (рисунок 31).

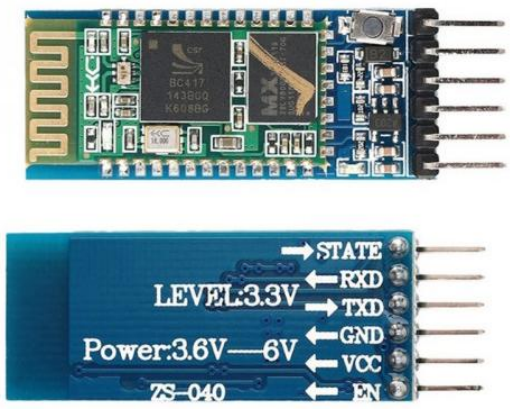

Рисунок 31 — Bluetooth модуль HC-05.

2.3.11 Составили принципиальную электрическую схему проектируемой системы безопасности «Умного дома» (рисунок 32).

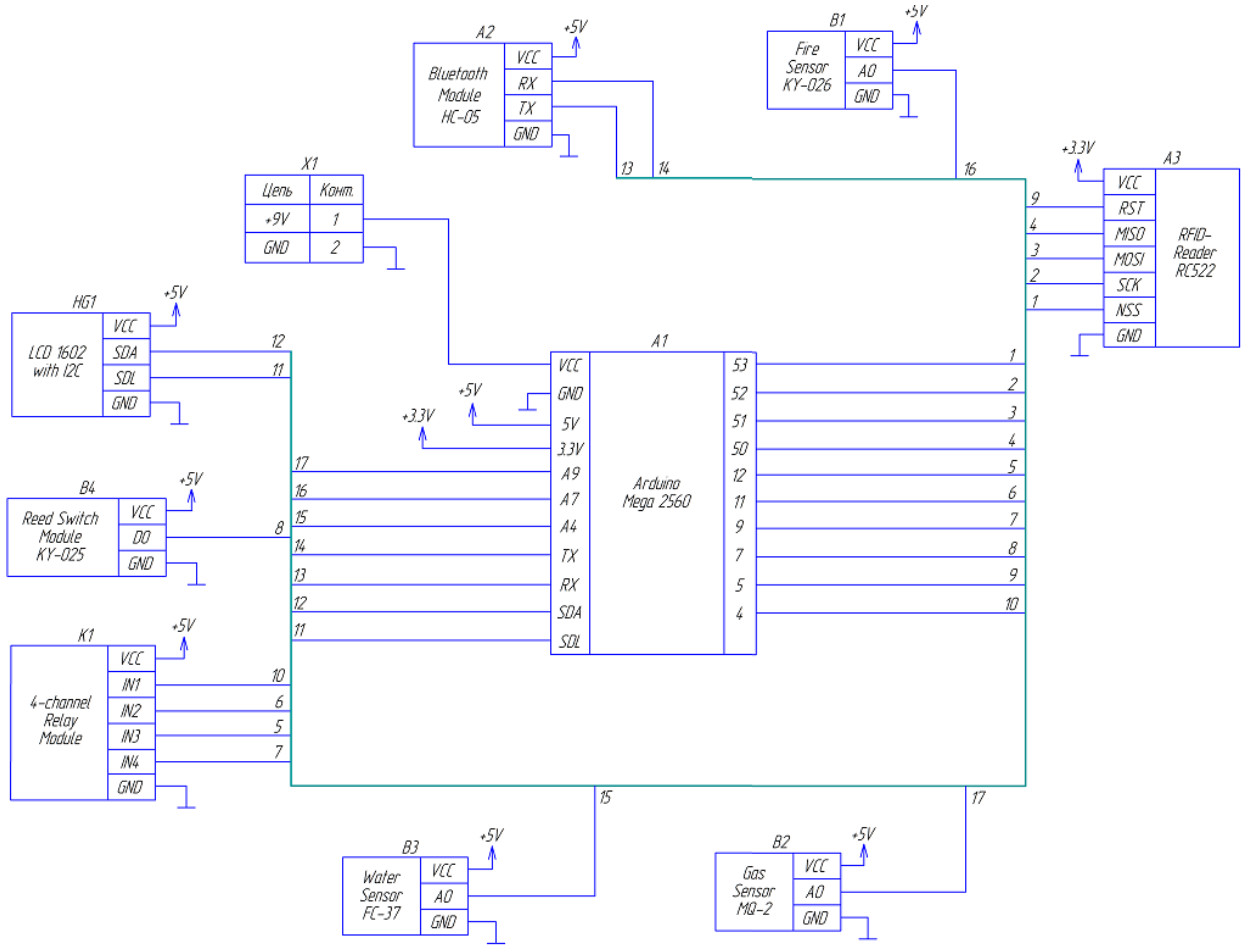

Рисунок 32 — Принципиальная схема проектируемой системы.

2.4 Программная часть

В среде разработки Arduino IDE составили программный код, реализующий разработанный ранее алгоритм работы проектируемой системы (смотреть ПРИЛОЖЕНИЕ А).

Программа составлена на языке C/C++. При написании программы использовались специальные готовые библиотеки для Arduino IDE: библиотека для работы с RFID-считывателем, библиотека для работы с LCD-дисплеем и библиотека для работы с I2C-интерфейсом.

Для возможности управления платой Arduino посредством протокола Bluetooth выбрали приложение Bluetooth Terminal для мобильной операционной платформы Android. С помощью этого приложения пользователь может как отправлять команды на плату Arduino, так и принимать от нее данные. Основное окно программы и пример обмена данными представлены на рисунке 33.

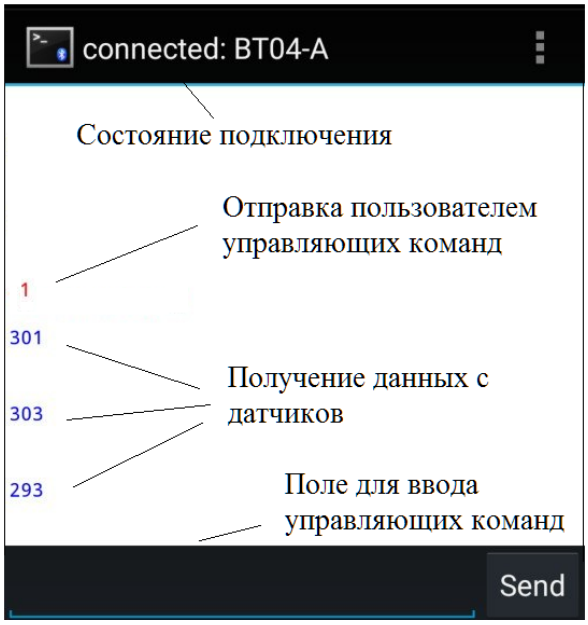

Рисунок 33 — Окно программы Bluetooth Terminal для обмена данными между устройством пользователя и модулем HC-05 по протоколу Bluetooth.

С помощью Bluetooth-модуля и данного приложения возможно подключение мобильного телефона пользователя к последовательному порту Arduino, который инициализируется функцией Serial.begin(). В скобках данной функции указывается скорость обмена данными по порту, зачастую это 9600 бит/с. Подключившись к последовательному порту, пользователь может видеть данные, которые Arduino выводит в последовательный порт, например данные с датчиков. И в обратную сторону: пользователь может сам отправить данные по последовательному порту, а Arduino их считает и, в зависимости, от пришедшей информации выполнит то или иное действие.

Реализация управления платой Arduino по Bluetooth в функции Void loop() выглядит следующим образом:

```
if (Serial.available() > 0) //Если в последовательный порт что-то пришло
{
val = Serial.read(); //Считываем пришедшие в порту данные и записываем их в переменную
if (val == '1') //Если пришла цифра 1
{
digitalWrite(Relay, LOW); //Срабатывает реле
}
```

Стоит отметить, что отправка управляющих команд осуществляется путем отправки одной из цифр от 0 до 10. Для проектируемой системы установили следующие соотношения: «1» — задействовать реле 1 (отключить подачу газа); «2» — задействовать реле 1,4 (возобновить подачу газа, отключить сигнализацию); «3» — задействовать реле 3 (отключить подачу воды); «4» — задействовать реле 3,4 (возобновить подачу воды, отключить сигнализацию); «5» — задействовать реле 4 (отключить сигнализацию при обнаружении возгорания); «6» — поставить систему на охрану (включить сигнализацию путем задействования реле 4 в случае срабатывания датчика открытия); «7» — снять систему с охраны и/или отключить сигнализацию путем задействования реле 4.

Номера реле совпадают с соответствующими выводами IN1, IN2, IN3, IN4 на выбранном модуле четырехканального реле.

3 КОНСТРУКТИВНО-ЭКСПЕРИМЕНТАЛЬНЫЙ РАЗДЕЛ

Используя ранее выбранное аппаратное обеспечение, собрали модель спроектированной системы безопасности «Умного дома» (рисунок 34).

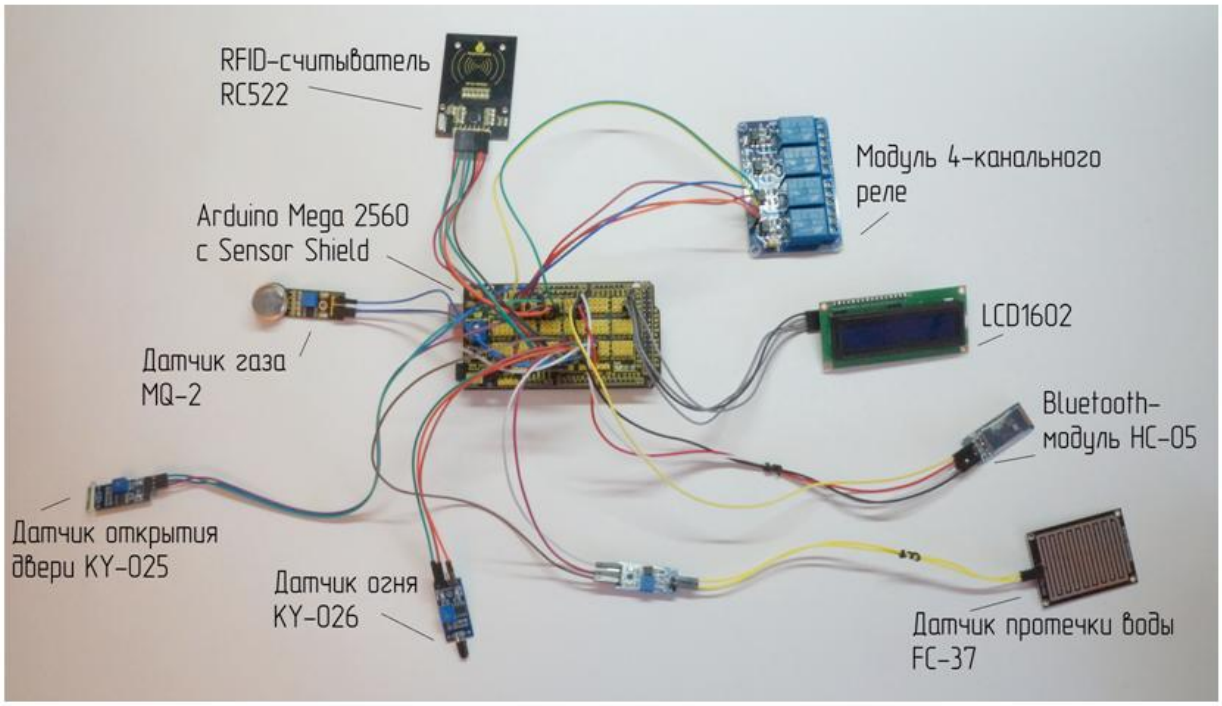

Рисунок 34 — Собранная модель проектируемой системы.

Для удобства сборки использовали расширение для платы Arduino Mega 2560, называемое Sensor Shield. Данное расширение позволяет упростить процесс подключения к плате большого количество датчиков и других электронных модулей, не используя макетную плату (рисунок 35).

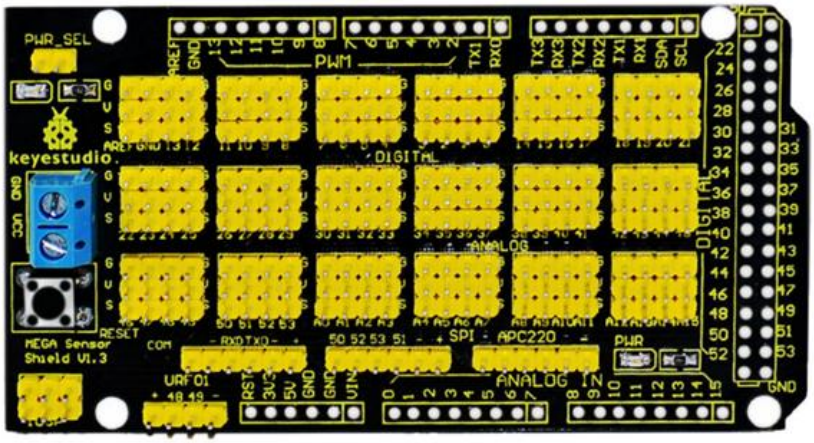

Рисунок 35 — Расширение Sensor Shield для платы Arduino.

В качестве исполнительных механизмов для демонстрации работы спроектированной системы были выбраны следующие устройства (рисунок 36): электромагнитный замок для системы контроля и управления доступом, электромагнитный клапан для системы защиты от протечек воды.

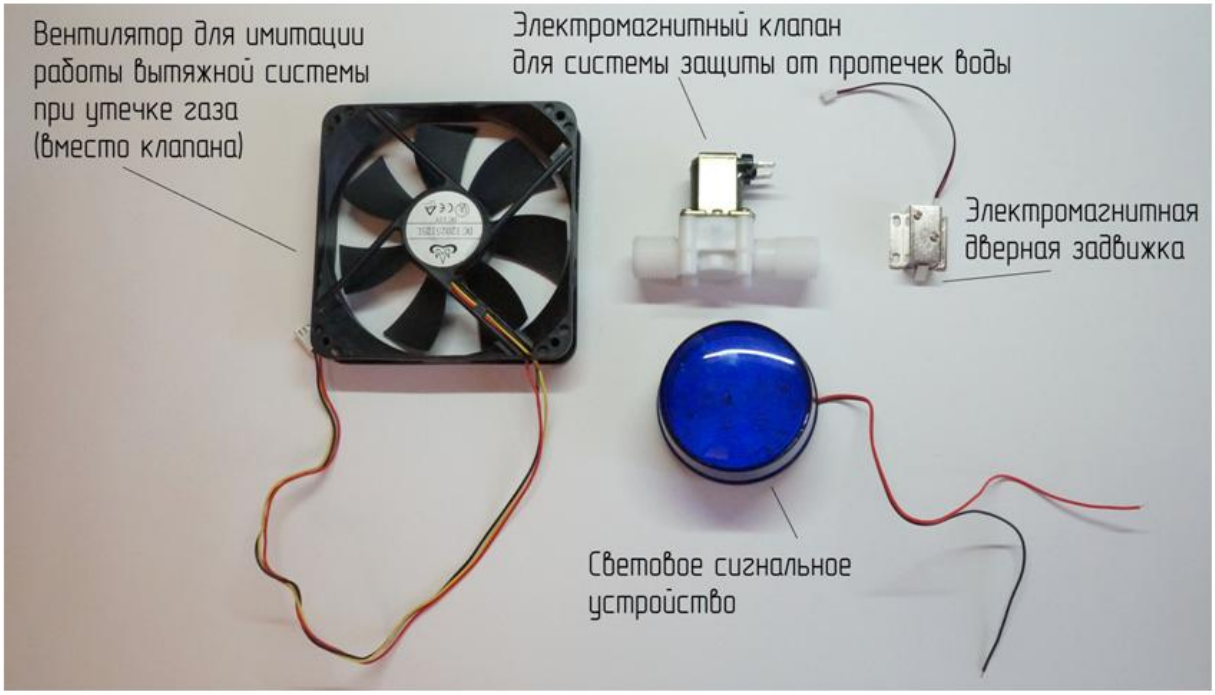

Рисунок 36 — Исполнительные механизмы для демонстрации работоспособности спроектированной системы.

Для демонстрации системы защиты от утечек газа выбрали вентилятор из системного блока компьютера, чтобы показать другой возможный вариант работы системы: включение вытяжной вентиляции при скоплении опасного объема газа в помещении. Все выбранные исполнительные устройства работают от напряжения от 9 до 12 В, а их работа управляется блоком 4-х канального реле.

На рисунке 37 представлена реализация вывода информационных сообщений при каком-либо событии в системе, а именно: при фиксации какого-либо аварийного события, при считывании незарегистрированной RFID-метки, при включении пользователем какого-либо реле, при активации режима охраны, при открытии входной двери в режиме охраны.

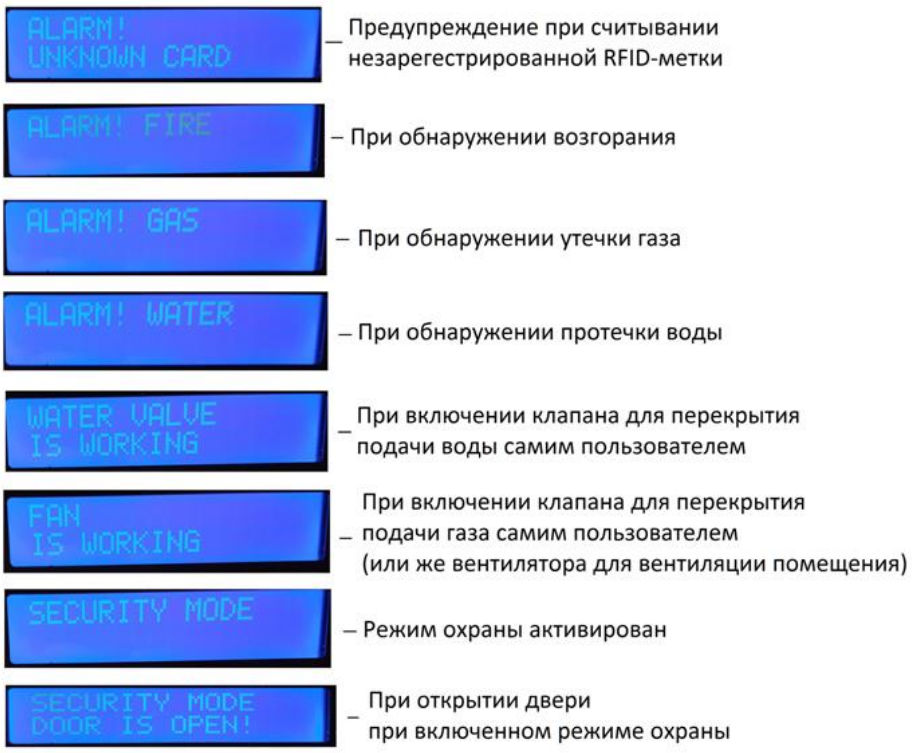

Рисунок 37 — Вывод информационных сообщений на LCD-дисплей.

4 ЭКОНОМИЧЕСКИЙ РАЗДЕЛ

Составили таблицу стоимости всех электронных компонентов, входящих в состав спроектированной системы безопасности «Умного дома» и купленных для сборки ее рабочей модели (таблица 1).

Таблица 1 — Стоимость электронных компонентов системы

Наименование компонента	Кол-во, ед.	Стоимость, руб.
Плата Arduino Mega 2560	1	840
RFID-считыватель RC522	1	356
Bluetooth-модуль HC-05	1	343
Экран LCD1602	1	136
Модуль 4-х канального реле	1	107
Датчик воды FC-37	1	76
Датчик газа MQ-2	1	61
Датчик огня KY-026	1	45
Модуль геркона KY-025	1	25

ЗАКЛЮЧЕНИЕ

В рамках данной бакалаврской работы спроектирована система безопасности «Умного дома» на основе микроконтроллера.

Доказана актуальность рассматриваемой темы. Проанализированы существующие решения в области систем безопасности «Умного дома». Составлена структурная схема. Разработан алгоритм работы системы. Подобраны необходимые электронные компоненты, а также написано нужное программное обеспечение для достижение поставленной цели.

Собрана рабочая модель системы для демонстрации ее функциональности и работоспособности.

На основе спроектированной системы безопасности «Умного дома» возможна реализация полномасштабной системы, которую можно устанавливать в квартиры и частные дома. Рабочую модель спроектированной системы можно использовать для демонстрации ее возможностей.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1 Интернет вещей: учебное пособие [текст] / А.В. Росляков, С.В. Ваняшин, А.Ю. Гребешков. – Самара: ПГУТИ, 2015. – 200 с.

2 Arduino и Raspberry Pi в проектах Internet of Things. — СПб.: БХВ-Петербург, 2016. – 320 с.

3 Объем рынка интернета вещей удвоится [Электронный ресурс]. URL: http://www.vestifinance.ru/articles/92629 (дата обращения: 18.02.2018).

4 Умный дом по-русски: комфорт против энергоэффективности [Электронный ресурс]. URL: https://iot.ru/gorodskaya-sreda/umnyy-dom-po-russki-komfort-protiv-energoeffektivnosti (дата обращения: 21.02.2018).

5 42% россиян хотели бы протестировать технологию умного дома [Электронный ресурс]. URL: https://hightech.fm/2017/10/12/sourvey (дата обращения: 24.02.2018).

6 «Интернет вещей» (IoT) в России. Технология будущего, доступная уже сейчас // PricewaterhouseCoopers URL: https://www.pwc.ru/ru/publications/iot/IoT-inRussia-research_rus.pdf

7 Chitnis, S., Deshpande, N. and Shaligram, A. (2016) An Investigative Study for Smart Home Security: Issues, Challenges and Countermeasures. Wireless Sensor Network, 8, 61-68. doi: 10.4236/wsn.2016.84006.

8 Budijono S., Andrianto J., Axis Novradin M. Design and implementation of modular home security system with short messaging system [Text] / EPJ Web of Conferences. — 2014, Vol. 68. doi: 10.1051/epjconf/20146800025.

9 Bangali, J. and Shaligram, A. Design and Implementation of Security Systems for Smart Home Based on GSM Technology. International Journal of Smart Home, Vol.7, No.6 (2013), pp.201-208.

10 Shirisha Tadoju, J. Mahesh. “Bluetooth Remote Home Automation System using Android Application”, International Journal Of Advanced

Technology and Innovative Research, ISSN 23 48–2370 Vol.07, Issue.10, August 2015, PP.1815-1818.

11 Krishna M., V. Narasimaha N., K. Ravi Kishore Reddy, B. Rakesh, 2015, “Bluetooth Base Wireless Home Automation System Using FPGA”, Journal of Theoretical and Applied Information Technology, Vol.77. No.3, PP. 1992-8645.

12 Choudhary V., Parab A., Bhapkar S., Jha N., Kulkarni Ms. Medha. Design and Implementation of Wi-Fi based Smart Home System, International Journal Of Engineering And Computer Science. - 2016, Vol.5 - PP.15852-15855.

13 Kumar A., Tiwari N., 2015, “Energy Efficient Smart Home Automation System” , International Journal of Scientific Engineering and Research (IJSER), Vol. 3 Issue 1 - PP. 2347-3878.

14 Роберт К. Элсенпитер, Тоби Дж. Велт, Умный дом строим сами / Пер. с англ. – М.: КУДИЦ-ОБРАЗ, 2005. – 384 с.

15 Arduino Mega 2560 Datasheet [Электронный ресурс] URL: https://www.robotshop.com/media/files/pdf/arduinomega2560datasheet.pdf (дата обращения: 14.03.2018).

16 Блум Д., Изучаем Arduino: инструменты и методы технического волшебства: Пер. с англ. – СПб.: БХВ-Петербург, 2015. — 336 с.

17 Specification for LCD Module 1602A-1 (V1.2) [Электронный ресурс] URL: https://www.openhacks.com/uploadsproductos/eone-1602a1.pdf (дата обращения: 17.03.2018).

18 Модуль датчика огня [Электронный ресурс] URL: http://arduino-kit.ru/catalog/id/modul-datchika-ognya (дата обращения: 20.03.2018)

19 Датчик широкого спектра газов MQ-2 [Электронный ресурс] URL: https://static.chipdip.ru/lib/497/DOC001497434.pdf (дата обращения: 10.04.2018).

20 FC-37 Аналогово-цифровой датчик [Электронный ресурс] URL: https://imrad.com.ua/userdata/modules/wproducts/wprod_products/151678/FC-37.pdf (дата обращения: 26.04.2018).

21 Модуль магнитный датчик с герконом [Электронный ресурс] URL: http://arduino-kit.ru/catalog/id/modul-magnitnyiy-datchik-s-gerkonom (дата обращения: 29.04.2018).

22 MRFC522 [Электронный ресурс] URL: https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf (дата обращения: 06.05.2018).

23 Петин В., Создание умного дома на базе Arduino. – М.: ДМК Пресс, 2018. – 180 с.

24 4 Channel 5V Optical Isolated Relay Module [Электронный ресурс] URL: http://www.handsontec.com/dataspecs/4Ch-relay.pdf (дата обращения: 18.05.2018).

25 HC-05-Bluetooth to Serial Port Module [Электронный ресурс] URL: http://www.electronicaestudio.com/docs/istd016A.pdf (дата обращения: 18.05.2018)

ПРИЛОЖЕНИЕ А

```
//Подключения LCD-дисплея
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
LiquidCrystal_I2C lcd(0x27,16,2);

//Подключение RFID-СКУД
#include <SPI.h>
#include <MFRC522.h>
#define SS_PIN 53
#define RST_PIN 5
MFRC522 mfrc522(SS_PIN, RST_PIN);
unsigned long uidDec, uidDecTemp; //Для хранения номера метки в десятичном формате
int countRFID = 0; //Счетчик числа считываний RFID-карты
int relayDoor = 11; //Реле для управления эл.задвижкой (далее - замком)
bool d = false; //Для реализации смены состояния замка
int countUNKNOWN; //Счетчик числа считываний незарегистрированной RFID-карты

//Для сигнализации
int relayAlarm = 9; //Реле для подключения сирены

//Для управления по Bluetooth
int val = 0; //Переменная для записи данных из порта

//Для системы защиты от утечек газа
int gasPin = A9; //Пин для датчика газа
int gasValue = 0; //Переменная для хранения данных с датчика газа
int relayGas = 4; //Реле для подключения вентилятора или эл.клапана (в данном случае - вентилятора)
bool a = true; //Включить сигнализацию даже при одном срабатывании датчика газа
int countGas = 0; //Количество срабатываний датчика газа

//Для системы защиты от протечек воды
int waterPin = A4; //Пин для датчика воды
int waterValue = 0; //Переменная для хранения данных с датчика воды
int relayWater = 12; //Реле для подключения эл.клапана
bool b = true; //Включить сигнализацию даже при одном срабатывании датчика воды
int countWater = 0; //Количество срабатываний датчика воды
```

```
//Для датчика огня
int firePin = A7; //Пин для датчика огня
int fireValue = 0; //Переменная для хранения данных с датчика огня
bool c = true; //Включить сигнализацию даже при одном срабатывании датчика огня
int countFire = 0; //Количество срабатываний датчика огня

//Для охраны входной двери
int gerkon = 7; //Пин датчика открытия
int gerkonState = 0; //Переменная для хранения данных с датчика открытия
int countDoor = 0; //Переменная для постановки системы на охрану

void setup()
{
//Примечание: любое реле отключено при уровне сигнала HIGH
Serial.begin(9600); //Скорость обмена данными по com-порту
pinMode(relayAlarm, OUTPUT); //Подключение сирены
digitalWrite(relayAlarm, HIGH); //Изначально сирена отключена
pinMode(gerkon, INPUT); //Подключение датчика открытия

//Подключение дисплея
lcd.begin(); //Инициализация
lcd.noBacklight(); //Отключить подсветку

//Подключение системы защиты от утечек газа
pinMode(relayGas, OUTPUT);
digitalWrite(relayGas, HIGH);

//Подключение системы защиты от протечек воды
pinMode(relayWater, OUTPUT);
digitalWrite(relayWater, HIGH);

//Подключение СКУД
SPI.begin(); //Инициализация
mfrc522.PCD_Init();
pinMode(relayDoor, OUTPUT);
digitalWrite(relayDoor, HIGH); //Изначально замок закрыт
}

void loop()
{
//УПРАВЛЕНИЕ ПО BLUETOOTH
if (Serial.available() > 0) //Если в com-порт что-то пришло
{
val = Serial.read(); //Записываем в переменную val, считав данные из порта
```

```
//Для системы защиты от утечек газа
if (val == '1') //Если пришла “1”
{
lcd.clear(); //Вывод надписи на дисплей
lcd.backlight();
lcd.setCursor(0,0);
lcd.print("FAN");
lcd.setCursor(0,1);
lcd.print("IS WORKING");
digitalWrite(relayGas, LOW); //Включить вентиляцию
}
if(val == '2') //Если пришла “2”
{
digitalWrite(relayGas, HIGH); //Отключить вентиляцию
digitalWrite(relayAlarm, HIGH); //Отключить сигнализацию
lcd.clear();
lcd.noBacklight();
countGas = 0;
}

//Для системы защиты от протечек воды
if (val == '3') //Если пришла “3”
{
lcd.clear(); //Вывод надписи на дисплей
lcd.backlight();
lcd.setCursor(0,0);
lcd.print("WATER VALVE");
lcd.setCursor(0,1);
lcd.print("IS WORKING");
digitalWrite(relayWater, LOW); //Включить эл.клапан
}
if(val == '4')
{
digitalWrite(relayWater, HIGH); //Отключить эл.клапан
digitalWrite(relayAlarm, HIGH); //Отключить сигнализацию
lcd.clear();
lcd.noBacklight();
countWater = 0;
}

//Для датчика огня
if (val == '5')
{
digitalWrite(relayAlarm, HIGH); //Отключить сигнализацию
lcd.clear();
```

```
lcd.noBacklight();
countFire = 0;
}

//Для постановки на охрану (контроль входной двери)
if (val == '6')
{
lcd.clear(); //Вывод надписи
lcd.backlight();
lcd.setCursor(0,0);
lcd.print("SECURITY MODE");
countDoor++; //Переменная для постановки системы на охрану
}

//Для снятия с охраны
if (val == '7')
{
countDoor = 0; //Обнуление переменной
lcd.clear(); //Отключение сигнализации, если включена
lcd.noBacklight();
digitalWrite(relayAlarm, HIGH);
}
}

if (countDoor > 0 && a == true) //Если система в режиме охраны
{
a = false;
gerkonState = digitalRead(gerkon); //Считываем данные с датчика открытия
if(gerkonState == HIGH) // Если дверь открыта
{
lcd.clear(); //Вывод надписи
lcd.backlight();
lcd.setCursor(0,0);
lcd.print("SECURITY MODE");
lcd.setCursor(0,1);
lcd.print("DOOR IS OPEN!");
digitalWrite(relayAlarm, LOW); //Включение сигнализации
}
}

//СИСТЕМА ЗАЩИТЫ ОТ ПРОТЕЧЕК ВОДЫ
waterValue = analogRead(waterPin); //Считываем данные с датчика воды
if (waterValue <= 500 && b == true) //Если обнаружена протечка
{
b = false;
```

```
countWater = 1; //Увеличиваем счетчик срабатывания датчика
}
if (waterValue > 500 && b == false) //Если не сработал
{
countWater = 0; //Обнуляем
b = true;
}
if (countWater == 1) //При срабатывании датчика делается:
{
lcd.backlight(); //Вывод надписи
lcd.clear();
lcd.setCursor(0,0);
lcd.print("ALARM! WATER");
lcd.setCursor(0,1);
lcd.print("               ");
digitalWrite(relayWater, LOW); //Включение эл.клапана
digitalWrite(relayAlarm, LOW); //Включение сигнализации
}

//СИСТЕМА ЗАЩИТЫ ОТ УТЕЧЕК ГАЗА
gasValue = analogRead(gasPin); //Считываем данные с датчика газа
if (gasValue > 400 && a == true) //Если обнаружена утечка
{
a = false;
countGas = 1; //Увеличиваем счетчик срабатывания датчика
}
if (gasValue < 400 && a == false) //Если не сработал
{
countGas = 0; //Обнуляем
a = true;
}
if (countGas == 1) //При срабатывании датчика делается:
{
lcd.backlight(); //Вывод надписи
lcd.clear();
lcd.setCursor(0,0);
lcd.print("ALARM! GAS");
lcd.setCursor(0,1);
lcd.print("               ");
digitalWrite(relayGas, LOW); //Включение эл.клапана
digitalWrite(relayAlarm, LOW); //Включение сигнализации
}

//ДАТЧИК ОГНЯ
fireValue = analogRead(firePin); //Считываем данные с датчика огня
```

```
if (fireValue < 30 && c == true) //Если обнаружен огонь
{
c = false; //Увеличиваем счетчик срабатывания датчика
countFire = 1;
}
if (fireValue > 100 && c == false) //Если не сработал
{
countFire = 0; //Обнуляем
c = true;
}
if (countFire == 1) //При срабатывании датчика делается:
{
lcd.backlight(); //Вывод надписи
lcd.clear();
lcd.setCursor(0,0);
lcd.print("ALARM! FIRE");
lcd.setCursor(0,1);
lcd.print("                ");
digitalWrite(relayAlarm, LOW); //Включение сигнализации
}

//СКУД
if (!mfrc522.PICC_IsNewCardPresent()) { //Поиск новой метки
return;
}
if (!mfrc522.PICC_ReadCardSerial()) { //Выбор метки
return;
}
uidDec = 0;
for (byte i = 0; i < mfrc522.uid.size; i++) { //Выдача серийного номера метки
uidDecTemp = mfrc522.uid.uidByte[i]; //В десятичном формате
uidDec = uidDec * 256 + uidDecTemp;
}
if (uidDec == 16909060) { //Сравнивание номера метки с заданным, если номера равны,то
d = !d; //Меняем состояние замка
delay(1000);
}
if (d) {
digitalWrite(relayDoor, LOW); //"дверь открыта"
}
else
{
digitalWrite(relayDoor, HIGH); //"дверь закрыта"
}
```

```
if (uidDec != 16909060) { //Если номера не равны
delay(1000);
countUNKNOWN++;
if(countUNKNOWN = 1) { //Кол-во считываний незарегистрированной карты
lcd.clear(); //Вывод надписи
lcd.backlight();
lcd.setCursor(0,0);
lcd.print("ALARM!");
lcd.setCursor(0,1);
lcd.print("UNKNOWN CARD");
digitalWrite(relayAlarm, LOW); //Включение сигнализации
}
}
}
```