Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Кафедра «Информационные системы»
Специальность 6М0703000 «Информационные системы»

ДОПУЩЕН К ЗАЩИТЕ
Зав. Кафедрой
к.т.н., доцент Имангалиев Ш.И.
(ученая степень, звание, Ф.И.О.)

_____
(подпись)
«____» _____2017 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ
пояснительная записка

на тему: «Исследование и разработка корпоративной безопасности системы телекоммуникационной компании (на базе микроконтроллеров «AT mega»)»

Магистрант МИСнп 15-1 _____ Рыбалов Н.Б.
(группа) (подпись) (Ф.И.О.)

Руководитель д.х.н., доцент _____ Жаксибаев М.Ж.
(ученая степень) (подпись) (Ф.И.О.)

Рецензент _____
(ученая степень) (подпись) (Ф.И.О.)

Рекомендуемая основная литература

1. Зайцев А.П. – "Технические средства защиты информации / Машиностроение" 2009
2. Программирование микроконтроллерных плат Arduino/Freeduino – Ч.III Соммер

ГРАФИК
подготовки магистерской диссертации

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
1. Информационный обзор согласно теме	05.10.2017	
	14.01.2018	
2) Основные направления развития и проблемы современных систем безопасности		
3) Внешние факторы влияющих на качество и возможность детектирования нарушителей.	02.02.2018	
4) Проектирование опытного образца системы безопасности.	18.03.2017	
5) Анализ полученных данных	01.05.2017	

Дата выдачи задания

Заведующий кафедрой _____ (_____)
(подпись) (Ф.И.О.)

Руководитель диссертации _____ (_____)
(подпись) (Ф.И.О.)

Задание принял к исполнению магистрант
_____ (Рябовалъ Н.Б)
(подпись) (Ф.И.О.)

Алматы 2017

Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Факультет «Аэрокосмические и информационные технологии»
Кафедра «Информационные системы»
Специальность 6М0703000 «Информационные системы»

ЗАДАНИЕ
На выполнение магистерской диссертации

Магистранту Рыбалову Николаю Борисовичу
(Ф.И.О.)

Тема дисертации Исследование и разработка периметральной безопасности системы телекоммуникационной полиции
утверждена Ученым советом университета №__ от «___»_____
Срок сдачи законченной диссертации «___»_____
Цель исследования состоит в экспериментальном исследовании возможности улучшения принципов детектирования проникновений на особо охраняемые телекоммуникационные объекты.

Перечень подлежащих разработке в магистерской диссертации вопросов или краткое содержание магистерской диссертации:
1) Основные направления развития систем безопасности
2) Изучение параметров применяемых сенсоров
3) Решение проблем взаимодействия сенсоров с программной частью.

Перечень графического материала (с точным указанием обязательных чертежей)
Рисунок 26 – структурная схема системы
Рисунок 23 – графический интерфейс. Java

Аңдатпа

Диссертациялық жұмыс қазіргі заманғы қауіпсіздік жүйелерінің мәселелеріне арналған. Бұл сала бүгінгі қоғамдағы криминогендік жағдайдың нашарлауына байланысты өзекті мәселе болып табылады. Осы жұмыста ұсынылған қауіпсіздік жүйесінің модульді болуы, оның даусыз артықшылығы болып табылады. Күрделі жүйелердің модульді болуы техникалық қолдаудың мүлдем жаңа саласының белсенді дамуына мүмкіндік берді, сондай-ақ еркін бағдарламалық қамтамасыздандырудың болуы бір мезгілде соңғы жаңартуларды шығаруға мүмкіндік береді.

Бірыңғай периферияльық датчиктер жиынтығымен жабдықталған лазерлік жүйесінің потенциялын белсенді пайдаланылуы, рұқсатсыз кірудің барлық түрлеріне қарсы тиімділігін айтарлықтай арттыруға мүмкіндік береді. Жанама анықтау әдісі ретінде және тұтас игерілген жуйенің тиімділігін арттыру мақсатында температура функциясының туындысы қолданылған.

Аннотация

Диссертационная работа направлена на рассмотрение проблем безопасности современных датацентров. Неоспоримым преимуществом в представленной работе является её модульность и открытость ПО. Именно модульность таких сложных систем позволила положить начало активному развитию совершенно новой сфере технической поддержки, а так же наличие программного обеспечения, носящего характер свободное ПО позволяет единовременно выпускать актуальные обновления. Активное внедрение потенциала сенсоров , дающих дифференциальную результирующую позволяет значительно повысить эффективность схемы ко всем видам несанкционированных проникновений. В качестве косвенного метода обнаружения и повышения продуктивности разработанной системы в целом была применена производная функция температуры.

Abstract

The thesis is devoted to the problems of modern security systems. This area remains a topical effect worsening crime situation in today's society. The undeniable advantage presented in this paper, the security system is its modularity. This modularity of complex systems has allowed to initiate active development of an entirely new field of technical support, as well as the availability of software in the nature of free software allows you to simultaneously release the latest updates.

The active use of the potential of the laser system with a set of unified peripheral sensors can significantly increase the efficiency of the scheme to all types of infiltrations.

Содержание

Введение 8

1 Основные понятия систем безопасности 11

1.1 Основы построения систем безопасности 11

1.2 Механизмы взаимодействия аппаратных модулей системы 23

Выводы по первой главе 25

2 Подбор аппаратной и программной части, необходимой для реализации системы безопасности 26

2.1 Подбор программных модулей для построения комплексной системы 26

2.2 Основные аспекты выбора оборудования для построения распределённой вычислительной системы 27

Выводы по второй главе 49

3 Разработка и исследование системы безопасности 49

3.1 Разработка принципов взаимодействия модулей аппаратной части 50

3.2 Разработка принципов взаимодействия модулей программной части .. 51

Выводы по третьей главе 55

Заключение 56

Перечень сокращений 57

Список литературы 58

Приложение А 59

Введение

Общая характеристика работы.

Диссертационная работа посвящена рассмотрению проблемы современных систем безопасности. Данное направление остаётся актуальным в силу обострения криминогенной обстановки в современном обществе. Неоспоримым преимуществом представленной в данной работе системы безопасности является её модульность. Именно модульность таких сложных систем позволила положить начало активному развитию совершенно новой сфере технической поддержки, а так же наличие программного обеспечения, носящего характер свободное ПО позволяет единовременно выпускать актуальные обновления.

В магистерской диссертации представлена концепция реализации принципов построения современных систем безопасности, продемонстрированы способы взаимодействия их модулей между собой, а так же описаны программные и аппаратные рекомендации, которые следует учитывать при разработке подобных систем.

Постановка проблемы и её актуальность.

На сегодняшний день в области организации активной безопасности стремительно развиваются и внедряются модульные концепции. Данное направление было актуальным и раннее, однако настоящее развитие получило лишь в недавнее время. Связано это с выпуском большого числа сенсоров с открытыми интерфейсами. Модульность конструкции позволяет масштабировать и расширять функционал конечного устройства без полной замены аппаратной части, что может полностью покрыть спектр запросов потенциальных заказчиков. Согласно аналитическим данным, в будущем наиболее динамично будут развиваться те сервисы, которые полностью отвечают потребностям современных компаний. Они должны быстро и просто внедряться, не требовать больших инвестиций, иметь постоянную доступность.

Необходимо определить критерии системы, которые следует учесть при разработке модели. При этом система должна обеспечивать сочетание нескольких важных характеристик:

-управляемость;

-поддержка и сопровождение;

-масштабируемость;

-надёжность;

-высокая готовность;

-работоспособность.

Целью работы является решение части существующих проблем:

1 Организация протокола взаимодействия между аппаратной и программной частью;

3 Рассмотрение вариантов построения модульной конструкции;

4 Улучшение эффективности действия лазерных сенсоров;

5 Тестирование и анализ результатов исследования системы.

Объектом исследования является технология построения и взаимодействия элементов системы безопасности и улучшения функционирования сенсоров проникновения. Внедрение принципиально нового подхода к детектированию.

Методы исследования.

Исследование проводилось на самостоятельно разработанной модели. За время работы над диссертацией было изучено множество материалов, представленных на специализированных интернет - порталах. Все базовые понятия и теория были выделены из литературы, указанной авторами статей, в том числе представленные в трудах зарубежных научных исследователей.

Необходимые практические навыки исследования были получены во время прохождения обязательной научной стажировки.

Над аппаратной частью системы проводились эксперименты путём симуляции всех возможных сценариев организации проникновения, программная часть разрабатывалась в открытой среде разработки Arduino IDE. В дальнейшем поведение системы исследовалось да полноценном физическом макете.

Научную новизну представляет разработка протокола взаимодействия между аппаратной частью и программным обработчиком, логированием данных в MySQL и исследованием возможности обнаружения проникновения в охраняемую зону базируясь на производной функции температуры и температурной карты.

Практическая значимость результатов исследований представляет собой возможность дальнейшего активного развития данного направления и открывает перспективы выпуска на рынок конечного продукта в виде охранного комплекса. По результатам опросов, на сегодняшний день в Казахстане нет компаний, занимающихся разработкой подобных систем безопасности, в связи, с чем все основные исследования проходят только в рамках университетов.

Личный вклад автора присутствует во всех звеньях работы, а именно: в проведении литературного обзора по теме диссертации, постановке проблемы, постановке и проведении экспериментов, разработку виртуальной модели системы на базе компьютера с применением систем автоматизированного проектирования, анализе результатов решения задач, создания рабочего прототипа.

Апробация

Рыбалов Н.Б Разработка системы безопасности телекоммуникационной компании//Сборник научных трудов магистрантов специальностей “Информационные системы”.

Рыбалов Н.Б Аренбаева Ж.Г Программа кодирования-декодирования RSA//Гжельский государственный университет

Структура и объем диссертации. Диссертационная работа содержит список обозначений и сокращений, введение, основная часть из пяти разделов, заключения, приложения и списка использованных источников. Объем диссертации составляет 59 страницы машинописи, включая 30 рисунков.

1 Основные понятия систем безопасности

1.1 Основы построения систем безопасности

Интенсивное развитие современных технических средств безопасности, постоянное расширение выполняемых ими функций позволяет эффективно использовать их в различных сферах деятельности. На современном рынке гостеприимства существует довольно широкий спектр предложений таких средств, и растеряться при выборе необходимого оборудования проще простого. Поэтому сегодня мы рассмотрим основы основ, самые необходимые технические средства безопасности, которыми можно минимизировать факторы, способные привести к дополнительным финансовым потерям для владельца

Автоматизация является качественно новым этапом в совершенствовании производства. Основные обязанности человека в этом случае – наблюдение за параметрами процесса и выполнение внештатных операций. Применение средств автоматизации позволяет увеличить число агрегатов и механизмов, обслуживаемых одним человеком. Основные операции, которые выполняет человек в этом процессе – включение и отключение агрегатов, а в случае возникновения нештатных ситуаций – отключение регулятора и принятия на себя функции регулирования. Для этого он пользуется средствами дистанционного управления механизированными приводами различных регулирующих органов применение средств технологической защиты, блокировки и автоматического включение резервных механизмов позволяет автоматизировать и сам процесс ликвидации аварийных положений.

Автоматизация производственных процессов развилась по пути замены тяжелого физического труда человека работой механизмов. Механизация ручных операций на производственных предприятиях создала предпосылки для передачи технологическим регуляторам операций по управлению производственными процессами.

При автоматизации одной области промышленности возникает потребность в перенастройке технологии, аппаратуры и организации в смежной области. Автоматизация приносит наибольший эффект в тех случаях, когда технологи, конструкторы, специалисты по организации и планированию работают в тесном контакте со специалистами по автоматизации. Такая совместная работа предполагает их взаимопонимание, которое может быть достигнуто лишь в том случае, если специалисты различных профессий будут иметь общие представления автоматизации производственных процессов.

Таким образом, автоматизация работы оборудования включает: механизацию тяжелых работ и трудоемких процессов, дистанционное

управление, автоматизацию непрерывных процессов, автоматическое регулирование по заданной программе.

К функциям контроля за состоянием объектов относят: технологическая защита, блокировка, автоматическое включение резерва, технологическая сигнализация.

Сигнализация автоматически подает сигнал при срабатывании защиты, блокировки, а так же при включении резерва и служит для привлечения внимания дежурного персонала к месту возникновения неисправности.

Контролем над состоянием объекта управления называется процесс получения информации. Основной задачей системы автоматического контроля является измерение параметров объекта управления и сравнения текущих значений с допустимыми, регистрация значений параметров и их текущих отклонений от заданных , сигнализация возникновения нештатных ситуаций. По расстоянию от объекта до средств автоматического контроля системы бывают сосредоточенного, дистанционного и телемеханического контроля. Системы сосредоточенного контроля размещают в непосредственной близости от объекта управления. Системы дистанционного контроля размещают на определенном расстоянии от объекта управления, они содержат специальные средства предварительной обработки для передачи контролируемых параметров по линиям связи. Системы телемеханического контроля позволяют осуществить беспроводную связь с объектом управления.

Применение отдельных видов автоматизации не освобождает персонал от выполнения ряда ручных операций и не позволяет сократить численность персонала до возможного минимума. Поэтому полный эффект от автоматизации достигается лишь при комплексном использовании всех ее средств в умеренном сочетании.

Выбор конкретных типов систем охранной сигнализации производится в зависимости от нижеперечисленных факторов:

наличия и вида ограждения (кирпичный забор, сетка Рабина и т.п.);

наличия полосы отчуждения и её ширины;

протяженности периметра;

рельефа местности.

Для защиты периметров объектов рекомендуется использовать следующие виды периметральных систем охранной сигнализации, выполненные на основе:

1) Радио-лучевых извещателей, представляющих собой двухблочные технические средства с разнесенными друг относительно друга передатчиком и приемником СВЧ-излучения.

2) Радиоволновых извещателей, представляющих собой специальную систему параллельных проводов, по которым осуществляется приемопередача излучения в определенном диапазоне волн.

3) Радиоволновых доплеровских извещателей.

4) Вибрационных извещателей.

5) Вибросейсмических извещателей.

6) Активных оптико-электронных инфракрасных извещателей.

7) Емкостных извещателей.

9) Проводно-обрывных извещателей.

10) Пассивных оптико-электронных инфракрасных извещателей.

11) Индуктивных извещателей, представляющих собой систему натянутых между опорами ограждения проводов, образующих индуктивную петлю.

В зависимости от принципа действия периметральные системы охранной сигнализации могут блокировать:

- только периметры, имеющие заграждение (заборы): проводно-обрывные, емкостные, индуктивные, вибрационные;
- только периметры, не имеющие заграждения (заборов): пассивные и активные инфракрасные, вибросейсмические, радиолучевые;
- периметры, имеющие и не имеющие заграждения (заборов): проводно-обрывные, радиоволновые, магнитометрические, линии вытекающей волны.

Периметральные системы охранной сигнализации, блокирующие периметры без ограждения целесообразно использовать для охраны особо важных объектов подгрупп AII (хранилищ с взрывчатыми материалами, денежных хранилищ и т.п.) и AI (ядерных реакторов, электростанций и т.п.) путем установки их перед основным ограждением для упреждения возможного проникновения на охраняемый объект (территорию). Наиболее эффективным из периметральных систем является применение магнитометрической системы, которая может применяться в условиях лесистой местности за счет того, что не реагирует на перемещение животных или людей, не имеющих металлических предметов (холодного или огнестрельного оружия, металлизированных элементов одежды).

Проводно-обрывные системы охраны имеют слабую защищенность от саботажа и как правило являются системами одноразового действия, поэтому их целесообразно применять только в комплексе с другими периметральными системами охранной сигнализации.

При оснащении объектов, имеющих ограждения (заборы), в качестве периметральных систем охранной сигнализации рекомендуется использовать в основном емкостные, радиолучевые, радиоволновые, вибрационные, вибросейсмические и пассивные или активные оптико-электронные инфракрасные извещатели.

На выбор типа периметральной сигнализации в первую очередь влияет её устойчивость к воздействию внешних климатических факторов, которые могут присутствовать на охраняемом объекте. Например, в условиях Беларуси применение активных инфракрасных извещателей связано со многими трудностями, поскольку снежные заносы, растительность, туман вызывают или ложные срабатывания, или отказ

системы. Дальность действия пассивных оптикоэлектронных инфракрасных извещателей в условиях тумана или сильного снегопада уменьшается на 25-30%. Поэтому на местности, где возможно появление туманов, расстояние между извещателями необходимо уменьшать, а в местах поворота периметра либо направлять извещатели встречно друг на друга, либо устанавливать сплошные щиты из досок, изготавливать другие преграды, чтобы компенсировать излишнюю дальность действия извещателей в ясную погоду.

Для дополнительного, визуального контроля, с целью повышения надежности и оперативности службы охраны по выявлению места и характера нарушения, целесообразно применять системы видеонаблюдения. При этом периметр должен оборудоваться охранным освещением с дистанционным управлением из помещения охраны и с автоматическим включением при регистрации тревожных сигналов.

С целью оперативного оповещения о нарушении на участках периметра и отдачи распоряжений по его пресечению, рекомендуется предусматривать громкоговорящую и телефонную связь из расчета одна точка на каждом блок-участке.

На крупных объектах (большой площади, сложной конфигурации, со свободным доступом посторонних, например, магазинах, универмагах), а также для повышения надежности блокировки музеев, выставок и других объектов с особо ценными товарами, экспонатами и т.п. устанавливаются "ловушки" на основе магнитоконтактных и активных и пассивных оптико-электронных извещателей на переходных дверях, дверях, ведущих в подвалы, чердаки, на подступах к ценностям и т.п.

ПКП, подключенные к системе передачи извещений (СПИ), должны эксплуатироваться в режиме "без права отключения", то есть программироваться таким образом, чтобы могли сдаваться под охрану только при исправности всех задействованных шлейфов сигнализации.

Системы охранной сигнализации, устанавливаемые на объектах, должны быть максимально защищены от саботажа:

ПКП, сдающиеся под охрану на СПИ, должны в обязательном порядке эксплуатироваться с задействованными антисаботажными контактами ("Tamper"-контактами).

При программировании ПКП в обязательном порядке должны заменяться коды доступа к программированию, установленные заводом-изготовителем (коды установщика), на коды, присваиваемые конкретному объекту. Программирование ПКП должно осуществляться таким образом, чтобы исключалась возможность возврата ПКП к заводским кодам доступа (кодам установщика) при обесточивании ПКП.

Организацией, обслуживающей систему сигнализации, и заказчиком системы должны быть проведены организационные мероприятия по обеспечению сохранности кодов доступа к программированию ПКП и исключению к ним доступа посторонних лиц.

Прокладка проводов и кабелей шлейфов и соединительных линий систем охранной сигнализации по коридорам и через помещения, которые не подлежат блокировке системами охранной сигнализации, должна производиться с учетом обеспечения их максимальной защиты от саботажа. Способ прокладки выбирается с учетом категорийности помещения и определяется в задании на проектирование. В зависимости от категорийности объекта защита шлейфов сигнализации и соединительных линий должна осуществляться одним из способов:

- прокладкой кабелей и проводов скрытым способом;
- прокладкой кабелей и проводов в металлических или пластмассовых трубах, металлорукавах;
- прокладкой кабелей за подшивными потолками непосредственно по стенам, потолкам или в трубах;
- использования для прокладки многожильных телефонных кабелей.

Способ прокладки проводов и кабелей должен быть согласован при разработке технического задания на проектирование и основных технических решений.

Для повышения надежности срабатывания при блокировке двери на открытие могут устанавливаться по два магнитоконтактных извещателя.

Технические средства охранной сигнализации, устанавливаемые для блокировки объектов, должны выбираться с учетом наихудших неблагоприятных факторов, которые могут возникнуть в местах их установки (низких температур, повышенной влажности, воздействия осадков, наличия тумана, люминисцентного освещения, тепловых воздушных потоков, неровности грунта, снежных заносов и т.п.).

Выходное напряжение источников питания должно соответствовать требованиям ГОСТ 26342, электромагнитная совместимость - ГОСТ 30379. Аккумуляторные батареи ПКП и внешних источников питания должны обеспечивать бесперебойное электропитания всей системы охранной сигнализации в течение 24 часов.

Установка технических средств охранной сигнализации, не имеющих резервного электропитания, запрещена на всех объектах независимо от ведомственной принадлежности и способа охраны.

На объектах, охраняемых подразделениями Департамента охраны МВД Республики Беларусь, должны применяться только технические средства охранной сигнализации, включенные в Перечень технических средств, разрешенных к применению на охраняемых объектах.

Структура системы охранной сигнализации объекта должна строиться таким образом, чтобы была обеспечена её максимальная информативность, позволяющая лицам, осуществляющим охрану объекта принимать правильные меры реагирования. Для чего максимально, где это возможно периметр объекта должен разбиваться на отдельные шлейфы сигнализации, подключаемые к ПКП (шлейф тыла, фасада, левой стороны тыла 1 этажа, правой стороны 2 этажа и т.п.). В обязательном порядке подключаются на

ПКП разными шлейфами извещатели, устанавливаемые на разных уровнях здания (1 этаж, второй, подвал и т.п.), тыл и фасад магазинов и других крупных объектов, а также "ловушки" и извещатели, блокирующие наиболее уязвимые места.

Система охранной сигнализации должна обеспечивать максимальное удобство для пользователей.

При охране объектов с помощью ПКП, устанавливаемых на посту охраны без вывода сигнала на СПИ, удаленные от поста охраны помещения и объекты должны блокироваться с установкой на них отдельного ПКП со световой индикацией.

Тревожная сигнализация

Тревожной сигнализацией в обязательном порядке оснащаются объекты подгруппы AI, обменные пункты, крупные (головные) кассы, ювелирные магазины, ломбарды, ювелирные мастерские.

Учреждения банков, почтовые отделения, объекты с хранением наркотических средств и психотропных веществ, бланков строгой отчетности в соответствии с требованиями нормативных документов согласованных с МВД Республики Беларусь и Департаментом охраны МВД Республики Беларусь.

Необходимость оснащения тревожной сигнализацией других объектов определяется комиссией, принимающей объекты под охрану.

Тревожная сигнализация может выполняться как с помощью проводных, так и беспроводных извещателей (радиокнопок, брелоков и т.п.). На объектах, на которых ведутся операции с деньгами, могут устанавливаться автоматические тревожные извещатели (извещатель наличия последней купюры и т.п.).

Тревожная сигнализация должна обеспечивать удобство скрытного (от преступника) использования пользователем для вызова милиции или службы безопасности предприятия. При невозможности скрытного использования ручных тревожных извещателей (кнопок) необходимо использовать ножные (педали), беспроводные тревожные извещатели (радиокнопки, брелоки). При использовании тревожной сигнализации должно быть обеспечено отсутствие звукового сигнала в помещении, где она была использована.

Выбираемые для оснащения объекта технические средства охранной сигнализации и способ их монтажа должны обеспечивать пожаро - и взрывобезопасность охраняемого объекта.

При оснащении крупных объектов системами охранной сигнализации по возможности должны использоваться ПКП одного типа или одного производителя для удобства обслуживания. Однотипные ПКП позволяют снизить расходы на создание обменного фонда, закупку запасных частей, обучение персонала и т.п. .

При оснащении объекта охранно-пожарной сигнализацией обязательна установка светозвуковых оповещателей, независимо от способа охраны объекта, причем характер звучания звукового оповещателя при срабатывании пожарных извещателей должен отличаться от характера звучания при срабатывании охранных извещателей.

Телевизионные системы видеонаблюдения и системы контроля и управления доступом не могут использоваться в качестве дополнительного рубежа охранной сигнализации.

При оснащении объектов системами охранной сигнализации должны предусматриваться организационные или технические способы резервирования системы в случае выхода из строя отдельных её элементов и прежде всего приемно-контрольных приборов.

Для этих целей может использоваться метод подключения 21 и более шлейфов сигнализации не на один многошлейфный ПКП, а на два, или прокладываться дополнительный (не задействуемый) резервный кабель до места, где установлен еще один ПКП, который может быть использован для обеспечения контроля за шлейфами сигнализации вышедшего из строя прибора.

Порядок выбора систем сигнализации для охраны объекта

Выбор варианта охраны объекта следует начинать с определения подгруппы, к которой он относится, количества помещений, подлежащих охране, характера и структуры размещения ценностей. Вначале производится анализ основных уязвимых мест по периметру объекта: окон, дверей, иолов. Указанные уязвимые места оборудуются охранной сигнализацией. Однако, для некоторых объектов такой защиты недостаточно. На особо важных объектах ряд помещений оснащаются дополнительными рубежами сигнализации. Они подключаются по линиям городских телефонов на отдельные номера СПИ, а при их отсутствии - на отдельные номера ПКП.

На промышленных предприятиях, базах, складах, учреждениях банков и других объектах необходимо создавать внешний рубеж сигнализации по периметру ограждения.

Методика выбора варианта охраны

Варианты охраны объектов должны выбираться по следующей методике:

Первый этап. Определение характеристики объекта.

1. Тип объекта и его важность или ценность, характер имеющихся ценностей, место их расположения и концентрация.

2. Структура объекта:

- количество помещений, типы и размеры, расположение;
- количество уязвимых мест, их конструктивные особенности и размеры.

3. Телефонизация и характеристика сети питания.

Второй этап. Определение тактики охраны.

1. Выбор вида сигнализации:

- автономная;
- с выводом сигнала на пост охраны;
- с выводом сигнала на пульты централизованного наблюдения подразделений Департамента охраны МВД Республики Казахстан.

2. Выбор структуры охраны:

- количество рубежей сигнализации на объекте;
- количество пультовых номеров на ПЦН.

3. Определение структуры и значимости рубежей сигнализации:

- определение количества охранных и пожарных шлейфов;
- разделение охранных и пожарных шлейфов на самостоятельные блокируемые участки, определение блокируемых участков;
- определение способа блокировки уязвимых участков (открытие, пролом, комбинация и иные способы: объем, зона, ловушка);
- размеры блокируемых участков.

4. Выбор технических средств обнаружения:

контролируемого признака (точечный, линейный, поверхностный, объемный, комбинированный);

способа обнаружения (электроконтактный, магнитоконтактный, ударноконтактный, пьезоэлектрический, емкостной, радиоволновой, ультразвуковой, оптикоэлектронный, комбинированный);

извещателей с конкретными тактико-техническими характеристиками (надежность, сложность установки и монтажа, удобство технического обслуживания (ТО) и ремонт, маскирующие средства).

5. Выбор типа приемно-контрольных приборов:

- тип ПКП (надежность, сложность установки и монтажа, удобство ТО и ремонта, маскирующие средства);
- элементов индикации, контроля и сигнализации нарушения;
- определения и реализации порядка согласования с системами централизованной охраны;
- определение структуры размещения ПКП, оконечного устройства, источников питания (основного и резервного).

При оборудовании объектов сигнализацией, подключенной на ПЦН, пожарные и охранные шлейфы должны быть разделены, иметь самостоятельные ПКП и пультовые номера.

При наличии на объекте постов охраны реализация раздельной структуры решается установкой ПКП с подключением пожарных и охранных шлейфов на отдельные номера.

Охранная сигнализация включает в себя центральный модуль, который принимает и анализирует информацию, получаемую от охранных датчиков. После чего этот модуль выполняет запрограммированные функции, при срабатывании охранных датчиков. Постановка/снятие с

охраны осуществляется с помощью пульта управления. Для работы охранной системе еще необходим источник бесперебойного питания. Ну и конечно систему нужно оснастить охранными датчиками.

Датчики существуют различных видов. Самые распространенные – датчики движения (инфракрасные датчики), датчики открытия (геркон), разбития стекла (акустические).

Часто кроме охранных функций охранная сигнализация выполняет и функции контроля за различными технологическими процессами. В таком случае, охранная сигнализация оснащается сервисными датчиками. Такие датчики могут отслеживать утечку газа, воды, контролировать температуру в помещении, а так же наличие электроэнергии на охраняемом объекте. При нарушении заранее установленных параметров подается сигнал тревоги.

К охранной сигнализации возможно подключить пожарные датчики. С помощью такой системы можно защитить свое имущество вдобавок еще и от пожара. Неприятности, от которого, как правило, на много значительнее, чем от проникновения.

Системы охранной сигнализации условно можно разделить на два типа:

- Первый тип – автономная система охранной сигнализации. Такая система оснащена мощной сиреной, которая включается при проникновении на охраняемый объект. В тоже время сигнал тревоги не будет передаваться на пост охраны и не будет сообщения хозяину о проникновении. Такие охранные системы оказывают чисто психологическое воздействие на злоумышленника. Чаще всего этого бывает более чем достаточно.

- Второй тип – активные охранные системы. В таких системах сигнал о проникновении на объект передается на пост охраны. При получении сигнала тревоги охранная структура обязана прибыть на охраняемый объект незамедлительно. Еще их называют пультовая система охранной сигнализации. В данной охранной сигнализации имеется тревожная кнопка. В случае нажатия которой, тоже должна прибыть охрана.

Клиенту, решившему установить охранную сигнализацию, нужно обращаться в специализированную фирму, занимающуюся установкой охранных систем сигнализаций. Это подразумевает выезд специалиста и составление проекта установки. Установкой занимаются монтажники охранных систем.

С развитием техники появилась альтернатива выше приведенным охранным системам – это беспроводная GSM сигнализация. Она включает в себя лучшие аспекты стандартных охранных сигнализаций. Ее можно установить самостоятельно. При это сделать это можно за считанные минуты. С появлением на рынке беспроводной GSM сигнализации охрана имущества стала более доступной простой в использовании. Основные плюсы беспроводной GSM сигнализации:

- работает через GSM канал (нет необходимости в наличие стационарного телефона), что позволяет использовать GSM сигнализацию на даче, в гараже, сарае и т.д.
- беспроводные охранные датчики – не будет кабель-каналов нарушающих интерьер
- наличие мощной сирены
- не требуется проект установки
- возможность самостоятельной установки без знания особых навыков
- поступление сигнала тревоги о проникновении на Ваш мобильный телефон
- нет платы за обслуживание сигнализации (абонентской платы)
- работа на случай отключенной электроэнергии от встроенного аккумулятора.

1.1.1 Технические средства

Все внешние воздействия можно разделить на климатические, механические и радиационные.

К климатическим воздействиям относятся температура окружающей среды, влажность, атмосферное давление и наличие в атмосфере активных веществ.

К механическим воздействиям относятся вибрация, удары, линейное ускорение, невесомость (для данной системы механические воздействия не допускаются).

К радиационным воздействиям относятся космическое излучение, излучение от атомных двигателей, реакторов и др.

По условиям эксплуатации различают аппаратуру, работающую в нормальных условиях, наземную и бортовую.

На данную сигнализационную систему будут оказывать большое влияние климатические воздействия, и применение данной системы может осуществляться только в нормальных условиях.

Для нормальных условии, обеспечиваемых в закрытых отапливаемых помещениях, характерно поддержание определенного узкого диапазона изменения температуры, влажности, давления, отсутствие газов, кислот, микроорганизмов, пыли, механических воздействий, излучения выше допустимого.

Наибольшее влияние на работу аппаратуры оказывает температура окружающей среды, так как от номинала температуры или ее изменения в разной степени зависят свойства всех материалов и элементов.

Повышение температуры окружающей среды вызывает нестабильность работы полупроводниковых приборов и микро электронных

устройств, увеличение сопротивления проводниковых материалов и ухудшение параметров изоляции, вплоть до полного отказа аппаратуры.

Понижение температуры отрицательно влияет на работу электромеханических устройств и радиоэлектронной аппаратуры, особенно при значительных перепадах температуры — термоударах.

Повышенная относительная влажность воздуха и непосредственное воздействие атмосферных осадков приводит к ухудшению характеристик изоляционных материалов, появлению коррозии металлов.

1.1.2 Организационные меры

Организация охраны — составная часть общей системы защиты конфиденциальной информации предприятия. Вопросы обеспечения надежной охраны территории предприятия и его объектов неразрывно связаны с задачами организации пропускного режима на предприятии. Силы и средства, участвующие в решении этих задач, являются составными элементами системы охраны предприятия.

От эффективности функционирования системы охраны в полной мере зависят возможность и уровень решения задач пропускного и внутри-объектоного режимов. Системы пропускного и внутриобъектового режимов образуют следующие после системы охраны рубежи безопасности, предотвращающие доступ злоумышленника к охраняемой предприятием информации.

Главные цели охраны предприятия следующие:

- предотвращение попыток проникновения посторонних лиц (злоумышленников) на территорию (объекты) предприятия;
- своевременное обнаружение и задержание лиц, противоправно проникших (пытающихся проникнуть) на охраняемую территорию;
- обеспечение сохранности находящихся на охраняемой территории носителей конфиденциальной информации и материальных средств и исключение, таким образом, нанесения ущерба предприятию;
- предупреждение происшествий на охраняемом объекте и ликвидация их последствий.

К основным объектам охраны относятся:

- территория предприятия;
- расположенные на территории предприятия объекты (здания, сооружения);
- Носители конфиденциальной информации (документы, изделия);
- материальные ценности (грузы).

Особыми объектами охраны являются руководство предприятия персонал, допущенный к конфиденциальной информации. Организация охраны руководства и персонала предприятия регулируются отдельным положением (инструкцией), которое утверждается руководителем

предприятия, и, в необходимых случаях согласовывается с территориальными органами внутренних дел и органами безопасности. Основные цели охраны руководства и перевала предприятия — обеспечение их личной безопасности в повседневных условиях и при возникновении чрезвычайных ситуаций, предотвращение возможных попыток завладения злоумышленниками защищаемой информацией путем физического и иного насильственного воздействия на этих лиц, выработка рекомендаций охраняемым лицам по особенностям поведения в различных ситуациях.

Указанные цели достигаются в тесном взаимодействии с подразделениями внутренних дел, органами безопасности, а также подразделениями охраны (безопасности) других предприятий.

Основные задачи охраны перечисленных объектов следующие:

- контроль объекта и охраняемой территории, в том числе территории с особым режимом пропуска, в целях обнаружения и предотвращения попыток несанкционированного проникновения на них посторонних лиц (злоумышленников);
- обеспечение конфиденциальности и сохранения в тайне фактов проведения закрытых мероприятий на предприятии (его объектах), обсуждаемых или рассматриваемых на них вопросов;
- сопровождение и охрана носителей конфиденциальной информации, в том числе служебных документов предприятия, материальных ценностей и грузов при их транспортировке и перевозке (доставке);
- защита объектов и территорий с особым режимом пропуска т насильственных действий и вооруженных нападений, которые могут нанести ущерб предприятию;
- выполнение в необходимых случаях специальных задач по обеспечению личной охраны руководства предприятия и персонала предприятия, допущенного к конфиденциальной информации;
- участие в обеспечении пропускного режима для посетителей, транспортных средств и грузов на охраняемой территории (объектах предприятия) в целях установления личности и учета посетителей, контроля за ввозом, вывозом носителей конфиденциальной информации, грузов, материальных ценностей, предотвращения их несанкционированного перемещения, а также фиксации следов скрытых и открытых попыток хищения иного имущества предприятия;
- систематический анализ эффективности системы охраны, принимаемых должностными лицами мер по охране объектов предприятия и обеспечению сохранности носителей конфиденциальной информации, материальных ценностей и грузов, и выработка предложений по совершенствованию системы охраны.

Для реализации главных целей и основных задач охраны предприятия (его объектов) создается система охраны. Система охраны предприятия — совокупность используемых для охраны предприятия сил и средств, а также способов и методов охраны предприятия и его объектов.

1.2 Механизмы взаимодействия аппаратных модулей системы

COM port (Communication port, последовательный порт, Serial Port) – это стандартный двунаправленный последовательный порт компьютера, используется для передачи данных согласно протоколу RS-232.

На рисунке 1 представлен COM port.

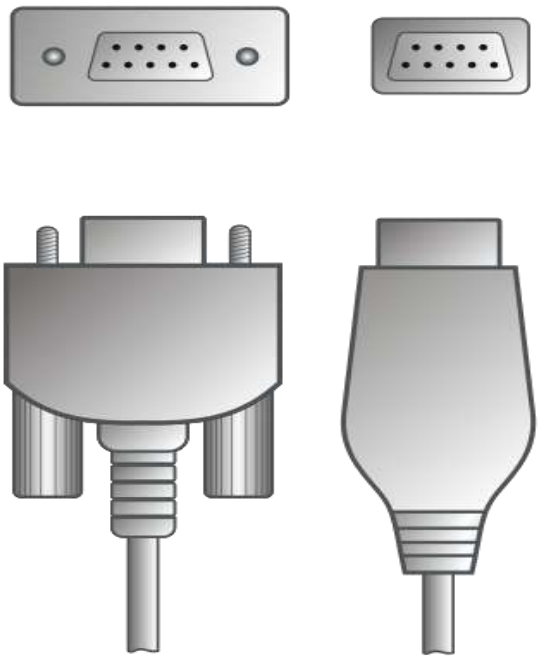


Рисунок 1 – Строение COM порта

Наиболее часто для последовательного порта персональных компьютеров используется стандарт RS-232C. Ранее последовательный порт использовался для подключения терминала, позже для модема или мыши. Сейчас он используется для соединения с источниками бесперебойного питания, для связи с аппаратными средствами разработки встраиваемых вычислительных систем, спутниковыми ресиверами, кассовыми аппаратами, с приборами систем безопасности объектов, а также с многими прочими устройствами.

С помощью COM-порта можно соединить два компьютера, используя так называемый «нуль-модемный кабель» (см. ниже). Использовался со времен MS-DOS для перекачки файлов с одного компьютера на другой, в UNIX для терминального доступа к другой машине, а в Windows (даже современной) — для отладчика уровня ядра.

Достоинством технологии является крайняя простота оборудования. Недостатком является низкая скорость, крупные размеры разъемов, а также зачастую высокие требования ко времени отклика ОС и драйвера и большое количество прерываний (одно на половину аппаратной очереди, то есть 8 байт).

Широко распространённый в IBM PC-совместимых компьютерах, последовательный порт в настоящее время морально устарел (Спецификация PC99 — один из примеров попытки избавиться в современных материнских платах от наследия старых интерфейсов), но ещё нередко присутствует на современных компьютерах и используется в промышленном и узкоспециализированном оборудовании. В настоящее время в IBM PC-совместимых компьютерах практически вытеснен интерфейсом USB.

Существуют стандарты на эмуляцию последовательного порта над USB и над Bluetooth (эта технология в значительной степени и проектировалась как «беспроводной последовательный порт»).

Тем не менее программная эмуляция данного порта широко используется и сегодня. Так, например, практически все мобильные телефоны эмулируют внутри себя классический COM-порт и модем для реализации тетеринга — доступа компьютера в Интернет через GPRS/EDGE/3G оборудование телефона. При этом для физического подключения к компьютеру используется USB, Bluetooth или Wi-Fi[2].

Также программная эмуляция данного порта предоставляется «гостям» виртуальных машин VMWare и Microsoft Hyper-V, основная цель при этом — подключение отладчика уровня ядра Windows к «гостю».

В виде UART, отличающегося уровнями напряжения и отсутствием дополнительных сигналов, присутствует практически во всех микроконтроллерах, кроме самых-самых маленьких, SoC, платах разработчиков, а также присутствует на платах большей части устройств, но не выведен разъем на корпус. Такая популярность связана с простотой этого интерфейса, как с физической точки зрения, так и с легкостью доступа к порту со стороны ПО по сравнению с другими интерфейсами.

Пример кросировки COM порта представлен на рисунке 2.

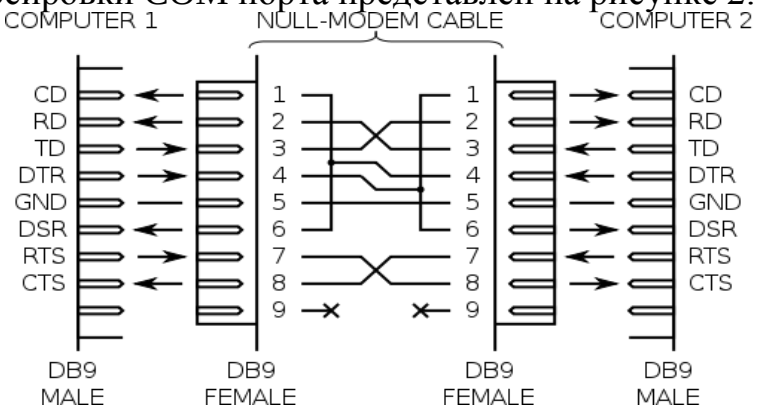


Рисунок 2 - Кроссировка кабеля

Стандарт Ethernet

Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, формат кадров и протоколы управления доступом к среде — на канальном уровне модели OSI. Ethernet в основном описывается стандартами IEEE группы 802.3. Ethernet стал самой распространённой технологией ЛВС в середине 1990-х годов, вытеснив такие устаревшие технологии, как ARCNET и Token ring.

Название «Ethernet» (буквально «эфирная сеть» или «среда сети») отражает первоначальный принцип работы этой технологии: всё, передаваемое одним узлом, одновременно принимается всеми остальными (то есть имеется некое сходство с радиовещанием). В настоящее время практически всегда подключение происходит через коммутаторы (switch), так что кадры, отправляемые одним узлом, доходят лишь до адресата (исключение составляют передачи на широковещательный адрес) — это повышает скорость работы и безопасность сети.

Преимущества использования витой пары по сравнению с коаксиальным кабелем:

- возможность работы в дуплексном режиме;
- низкая стоимость кабеля витой пары;
- более высокая надёжность сетей: при использовании витой пары сеть строится по топологии «звезда», поэтому обрыв кабеля приводит лишь к нарушению связи между двумя объектами сети, соединёнными этим кабелем (при использовании коаксиального кабеля сеть строится по топологии «общая шина», для которой требуется наличие терминальных резисторов на концах кабеля, поэтому обрыв кабеля приводит к неисправности сегмента сети);
- уменьшен минимально допустимый радиус изгиба кабеля;
- большая помехоустойчивость из-за использования дифференциального сигнала;
- возможность питания по кабелю маломощных узлов, например, IP-телефонов (стандарт Power over Ethernet, PoE);
- гальваническая развязка трансформаторного типа. В условиях СНГ, где, как правило, отсутствует заземление компьютеров, применение коаксиального кабеля часто приводило к выходу из строя сетевых карт в результате электрического пробоя.

Причиной перехода на оптический кабель была необходимость увеличить длину сегмента без повторителей.

Выводы по первой главе

Не закрытые протоколы и наборы файлов для open-source сред разработки позволяют объединить огромный ассортимент аппаратных

сенсоров. Организовать передачу данных на верхние уровни представления информации. Распределение полученной информации с использованием SQL сервер открывает новые горизонты. Вплоть до организации распределённого доступа посредствам глобальной сети.

2 Подбор аппаратной и программной части, необходимой для реализации системы безопасности

2.1 Подбор программных модулей для построения комплексной системы

Так как одна из концепций open source решений подразумевает под собой использование не только самостоятельно разработанных программных, но и библиотек сторонних разработчиков, за время исследования был проведён подбор и настройка соответствующих библиотек в соответствии с требованиями к производительности вычислительной системы.

В качестве ядра системы был выбран Windows 7 —операционная система семейства Windows NT получившая широкое распространение. Программное обеспечение, необходимое для графического интерфейса выполнено в среде разработки Processing . Processing 1.0 — это бесплатное, открытое, кроссплатформенное ПО. Исходный архив включает в себя java-машину, сам интерпретатор, мини-IDE. Позволяющий в короткие сроки создать готовый программный комплекс – нацеленный на решение узко специализированной задачи.

Основным связующим звеном между элементами системы и аппаратной частью является библиотека processing.serial. Используя эту библиотеку можно организовать собственный протокол, функционирующий только в рамках этого продукта или семейства продуктов. Это позволяет быстро расширить функционал устройства. Ярким примером является TLV (type – length – value) модель кодирования данных применённая в ISIS протоколе. Такая модель оказалась очень эффективной при переходе с IPv4 на IPv6.

За хранение данных отвечает MySQL server. MySQL — система управления базами данных (СУБД) для работы с БД SQL. СУБД – система управления базой данных. Она предназначена для изменения, поиска, добавления и удаления информации в БД. Есть множество СУБД, разработанных для похожих целей с разными особенностями. Одна из самых популярных – СУБД MySQL.

В роли WEB сервера выступает Xampp. Кроссплатформенная сборка веб-сервера (развитие LAMP), содержащая Apache, MySQL, интерпретатор скриптов PHP, язык программирования Perl и большое количество дополнительных библиотек, позволяющих запустить полноценный веб-

сервер. Изначально XAMPP создавался как инструмент для разработчиков, позволяя веб-дизайнерам и программистам тестировать свою работу, не используя Интернет. Для упрощения работы некоторые возможности и настройки безопасности отключены по умолчанию, и в целом XAMPP рекомендуется к использованию только в очень дружественном окружении. Однако XAMPP иногда используется и во всемирной паутине. Также программа поддерживает создание и управление базами данных MySQL и SQLite.

2.2 Основные аспекты выбора оборудования для построения распределённой вычислительной системы

Выделение ключевых требований к разрабатываемой системе является самой важной частью исследования. На данном этапе моделируется отказоустойчивость модулей и компонентов, разрабатывается ПО, организующее правильную работу системы в целом при минимальном использовании памяти устройства. Как следствие, при должном выполнении указанных требований достигается максимальная производительность всех компонентов.

2.2.1 Arduino MEGA

Подбор модулей основывается на выделении основных критериев и требований:

Размер устанавливаемой платы должен быть пропорционален общему форм-фактору устройства. Питающие уровни должны соответствовать стандартным значениям . Например TTL 5В.

Центральным узлом аппаратной части выступает Arduino Mrga.

Внешний вид платы представлен на рисунках 3 и 4.

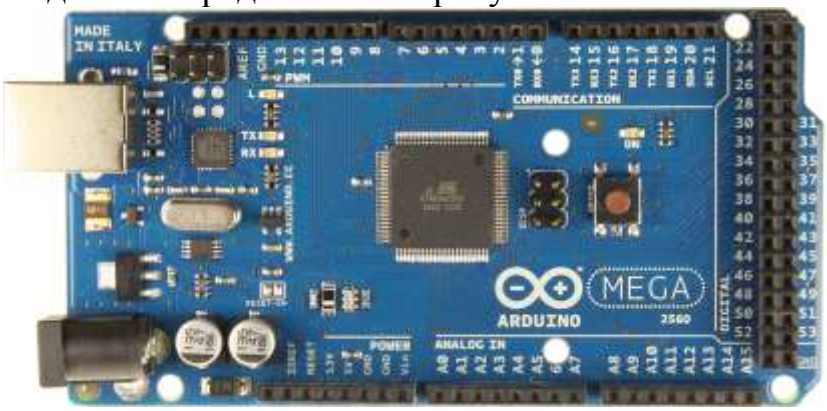


Рисунок 3 – Плата Arduino. Вид спереди

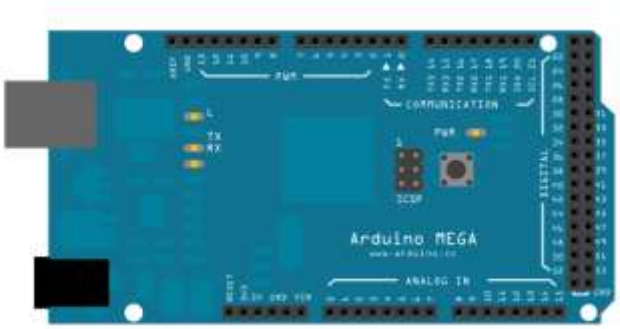


Рисунок 4 – Плата Arduino. Вид сзади

Arduino Mega построена на микроконтроллере ATmega1280 (техническое описание). Платформа содержит 54 цифровых входа/выходов (14 из которых могут использоваться как выходы ШИМ), 16 аналоговых входов,4 последовательных порта UART, кварцевый генератор 16 МГц, разъем USB, силовой разъем, разъем ICSP и кнопку перезагрузки. Для работы необходимо подключить платформу к компьютеру посредством кабеля USB или подать питание при помощи адаптера AC/DC, или аккумуляторной батареей. Arduino Mega совместима со всеми платами расширения, разработанными для платформ Duemilanove или Diecimila.

Краткие характеристики:

- Микроконтроллер ATmega1280
- Рабочее напряжение 5В
- Входное напряжение (рекомендуемое) 7-12В
- Входное напряжение (предельное) 6-20В
- Цифровые Входы/Выходы 54 (14 из которых могут использоваться как выходы ШИМ)
- Аналоговые входы 16
- Постоянный ток через вход/выход 40 mA
- Постоянный ток для вывода 3.3 В 50 mA
- Флеш-память 128 KB (4 используются для загрузчика)
- ОЗУ 8 KB
- Энергонезависимая память 4 KB
- Тактовая частота 16 MHz
- Питание
- Arduino Mega может получать питание через подключение USB или от внешнего источника питания. Источник питания выбирается автоматически.

Внешнее питание (не USB) может подаваться через преобразователь напряжения AC/DC (блок питания) или аккумуляторной батареей. Преобразователь напряжения подключается посредством разъема 2.1 мм с центральным положительным полюсом. Провода от батареи подключаются к выводам Gnd и Vin разъема питания.

Платформа может работать при внешнем питании от 6 В до 20 В. При напряжении питания ниже 7 В, вывод 5V может выдавать менее 5 В, при этом платформа может работать нестабильно. При использовании напряжения выше 12 В регулятор напряжения может перегреться и повредить плату. Рекомендуемый диапазон от 7 В до 12 В.

Выводы питания:

VIN. Вход используется для подачи питания от внешнего источника (в отсутствие 5 В от разъема USB или другого регулируемого источника питания). Подача напряжения питания происходит через данный вывод.

5V. Регулируемый источник напряжения, используемый для питания микроконтроллера и компонентов на плате. Питание может подаваться от вывода VIN через регулятор напряжения, или от разъема USB, или другого регулируемого источника напряжения 5 В.

3V3. Напряжение на выводе 3.3 В генерируемое микросхемой FTDI на платформе. Максимальное потребление тока 50 мА.

GND. Выводы заземления.

Память

Микроконтроллер ATmega1280 имеет: 128 кБ флеш-памяти для хранения кода программы (4 кБ используется для хранения загрузчика), 8 кБ ОЗУ и 4 Кб EEPROM (которая читается и записывается с помощью библиотеки EEPROM).

Входы и Выходы

Каждый из 54 цифровых выводов Mega, используя функции pinMode(), digitalWrite(), и digitalRead(), может настраиваться как вход или выход. Выводы работают при напряжении 5 В. Каждый вывод имеет нагрузочный резистор (стандартно отключен) 20-50 кОм и может пропускать до 40 мА. Некоторые выводы имеют особые функции:

Последовательная шина: 0 (RX) и 1 (TX); Последовательная шина 1: 19 (RX) и 18 (TX); Последовательная шина 2: 17 (RX) и 16 (TX); Последовательная шина 3: 15 (RX) и 14 (TX). Выводы используются для получения (RX) и передачи (TX) данных TTL. Выводы 0 и 1 подключены к соответствующим выводам микросхемы последовательной шины FTDI USB-to-TTL.

Внешнее прерывание: 2 (прерывание 0), 3 (прерывание 1), 18 (прерывание 5), 19 (прерывание 4), 20 (прерывание 3), и 21 (прерывание 2). Данные выводы могут быть сконфигурированы на вызов прерывания либо на младшем значении, либо на переднем или заднем фронте, или при изменении значения. Подробная информация находится в описании функции attachInterrupt().

PWM: 0 до 13. Любой из выводов обеспечивает ШИМ с разрешением 8 бит при помощи функции analogWrite().

SPI: 50 (MISO), 51 (MOSI), 52 (SCK), 53 (SS). Посредством данных выводов осуществляется связь SPI, которая, хотя и поддерживается аппаратной частью, не включена в язык Arduino. Также выводы SPI могут быть выведены на блоке ICSP, который совместим с платформами Duemilanove и Diecimila.

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

I2C: 20 (SDA) и 21 (SCL). Посредством выводов осуществляется связь I2C (TWI). Для создания используется библиотека Wire (информация на сайте Wiring). Расположение выводов на платформе Mega не соответствует расположению Duemilanove или Diecimila.

На платформе Mega установлены 16 аналоговых входов, каждый разрешением 10 бит (т.е. может принимать 1024 различных значения). Стандартно выводы имеют диапазон измерения до 5 В относительно земли, тем не менее имеется возможность изменить верхний предел посредством вывода AREF и функции analogReference().

Дополнительная пара выводов платформы:

- AREF. Опорное напряжение для аналоговых входов. Используется с функцией analogReference().
- Reset. Низкий уровень сигнала на выводе перезагружает микроконтроллер. Обычно применяется для подключения кнопки перезагрузки на плате расширения, закрывающей доступ к кнопке на самой плате Arduino.

Связь

На платформе Arduino Mega установлено несколько устройств для осуществления связи с компьютером, другими устройствами Arduino или микроконтроллерами. ATmega1280 поддерживает 4 порта последовательной передачи данных UART для TTL. Установленная на плате микросхема FTDI FT232RL направляет один из интерфейсов через USB, а драйверы FTDI (включены в программу Arduino) предоставляют виртуальный COM порт программе на компьютере. Мониторинг последовательной шины (Serial Monitor) программы Arduino позволяет посылать и получать текстовые данные при подключении к платформе. Светодиоды RX и TX на платформе будут мигать при передаче данных через микросхему FTDI или USB подключение (но не при использовании последовательной передачи через выводы 0 и 1).

Библиотекой SoftwareSerial возможно создать последовательную передачу данных через любой из цифровых выводов Mega.

ATmega1280 поддерживает интерфейсы I2C (TWI) и SPI. В Arduino включена библиотека Wire для удобства использования шины I2C. Более подробная информация находится на сайте Wiring. Для использования интерфейса SPI обратитесь к техническим данным микроконтроллера ATmega1280.

Программирование

Платформа программируется посредством ПО Arduino. Подробная информация находится в справочнике и инструкциях.

Микроконтроллер ATmega1280 поставляется с записанным загрузчиком, облегчающим запись новых программ без использования внешних программаторов. Связь осуществляется оригинальным протоколом STK500.

Имеется возможность не использовать загрузчик и запрограммировать микроконтроллер через выводы блока ICSP (внутрисхемное программирование). Подробная информация находится в данной инструкции.

Автоматическая (программная) перезагрузка

Mega разработана таким образом, чтобы перед записью нового кода перезагрузка осуществлялась самой программой, а не нажатием кнопки на платформе. Одна из линий FT232RL, управляющих потоком данных (DTR), подключена к выводу перезагрузки микроконтроллера ATmega1280 через конденсатор 100 нФ. Активация данной линии, т.е. подача сигнала низкого уровня, перезагружает микроконтроллер. Программа Arduino, используя данную функцию, загружает код одним нажатием кнопки Upload в самой среде программирования. Подача сигнала низкого уровня по линии DTR скоординирована с началом записи кода, что сокращает таймаут загрузчика.

Функция имеет еще одно применение. Перезагрузка Mega происходит каждый раз при подключении к программе Arduino на компьютере с ОС Mac X или Linux (через USB). Следующие полсекунды после перезагрузки работает загрузчик. Во время программирования происходит задержка нескольких первых байтов кода во избежание получения платформой некорректных данных (всех, кроме кода новой программы). Если производится разовая отладка скетча, записанного в платформу, или ввод каких-либо других данных при первом запуске, необходимо убедиться, что программа на компьютере ожидает в течение секунды перед передачей данных.

На Mega имеется возможность отключить линию автоматической перезагрузки разрывом соответствующей линии. Контакты микросхем с обоих концов линии затем могут быть соединены с целью восстановления. Линия маркирована «RESET-EN». Отключить автоматическую перезагрузку также возможно подключив резистор 110 Ом между источником 5 В и данной линие

Токовая защита разъема USB

В Arduino Mega встроена перезагружаемая плавкая вставка, защищающая порт USB компьютера от токов короткого замыкания и сверхтоков. Хотя практически все компьютеры имеют подобную защиту, тем не менее, данный предохранитель обеспечивает дополнительный барьер. Предохранитель автоматически прерывает обмен данных при прохождении тока более 500 мА через USB порт.

Физические характеристики и совместимость с платами расширения

Длинна и ширина печатной платы Mega составляют 10,2 и 5.3 см соответственно. Разъем USB и силовой разъем выходят за границы данных размеров. Три отверстия в плате позволяют закрепить ее на поверхности. Расстояние между цифровыми выводами 7 и 8 равняется 0,4 см, хотя между другими выводами оно составляет 0,25 см.

Arduino Mega совместима со всеми платами расширения, разработанными для платформ Duemilanove или Diecimila. Расположение выводов 0 – 13 (и примыкающих AREF и GND), аналоговых входов 0 – 5, силового разъема, блока ICSP, порта последовательной передачи UART (выводы 0 и 1) и внешнего прерывания 0 и 1 (выводы 2 и 3) на Mega соответствует расположению на вышеприведенных платформах. Связь SPI может осуществляться через блок ICSP, как на платформах Duemilanove / Diecimila, так и на Mega. Однако расположение выводов (20 и 21) связи I2C на платформе Mega не соответствуют расположению тех же выводов (аналоговые входы 4 и 5) на Duemilanove / Diecimila.

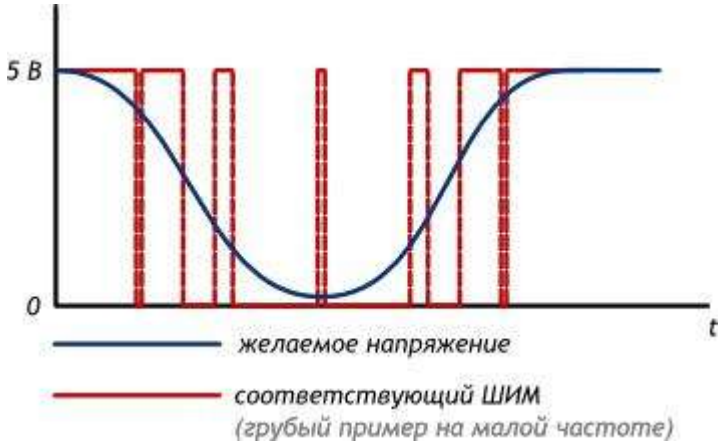


Рисунок 5 – Пример работы ШИМ

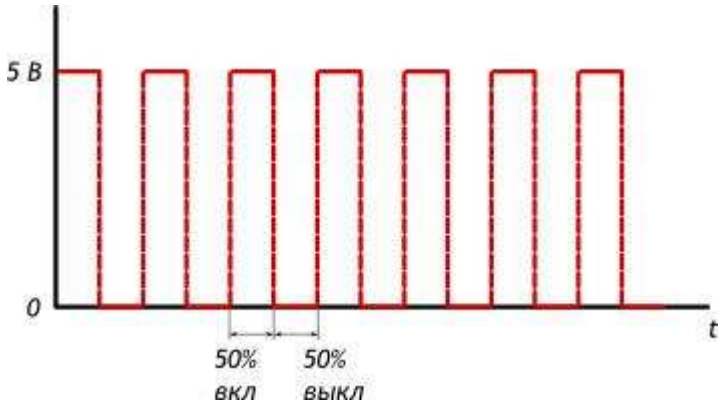


Рисунок 6 – Скважность при 2,5 В

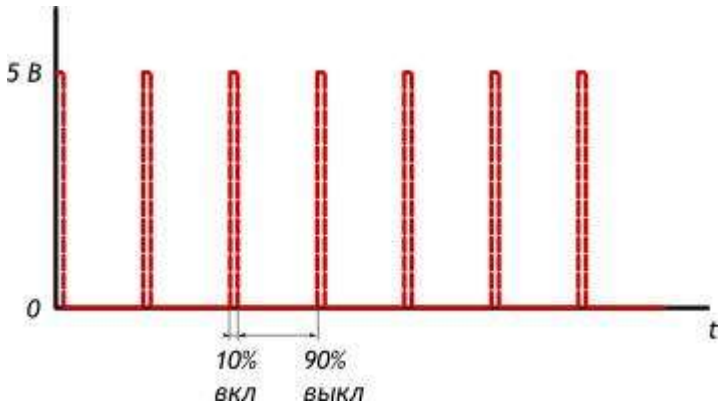


Рисунок 7 - Скважность при 0,5 В

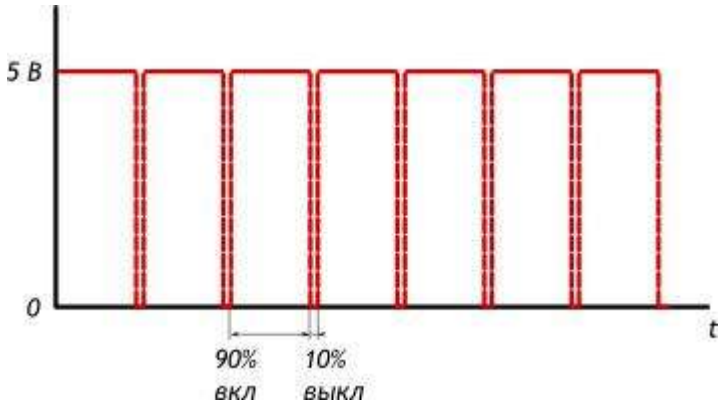


Рисунок 8 - Скважность при 4,5 В

2.2.2 Сервоприводы

Под сервоприводом чаще всего понимают механизм с электромотором, который можно попросить повернуться в заданный угол и удерживать это положение. Однако, это не совсем полное определение.

Если сказать полнее, сервопривод — это привод с управлением через отрицательную обратную связь, позволяющую точно управлять параметрами движения. Сервоприводом является любой тип механического привода, имеющий в составе датчик (положения, скорости, усилия и т.п.) и блок управления приводом, автоматически поддерживающий необходимые параметры на датчике и устройстве согласно заданному внешнему значению.

Иными словами:

Сервопривод получает на вход значение управляющего параметра. Например, угол поворота

Блок управления сравнивает это значение со значением на своём датчике

На основе результата сравнения привод производит некоторое действие, например: поворот, ускорение или замедление так, чтобы значение с внутреннего датчика стало как можно ближе к значению внешнего управляющего параметра

Наиболее распространены сервоприводы, которые удерживают заданный угол и сервоприводы, поддерживающие заданную скорость вращения.

Типичный сервопривод изображён на рисунке 9.

Рисунок 9 – Типовой серво привод

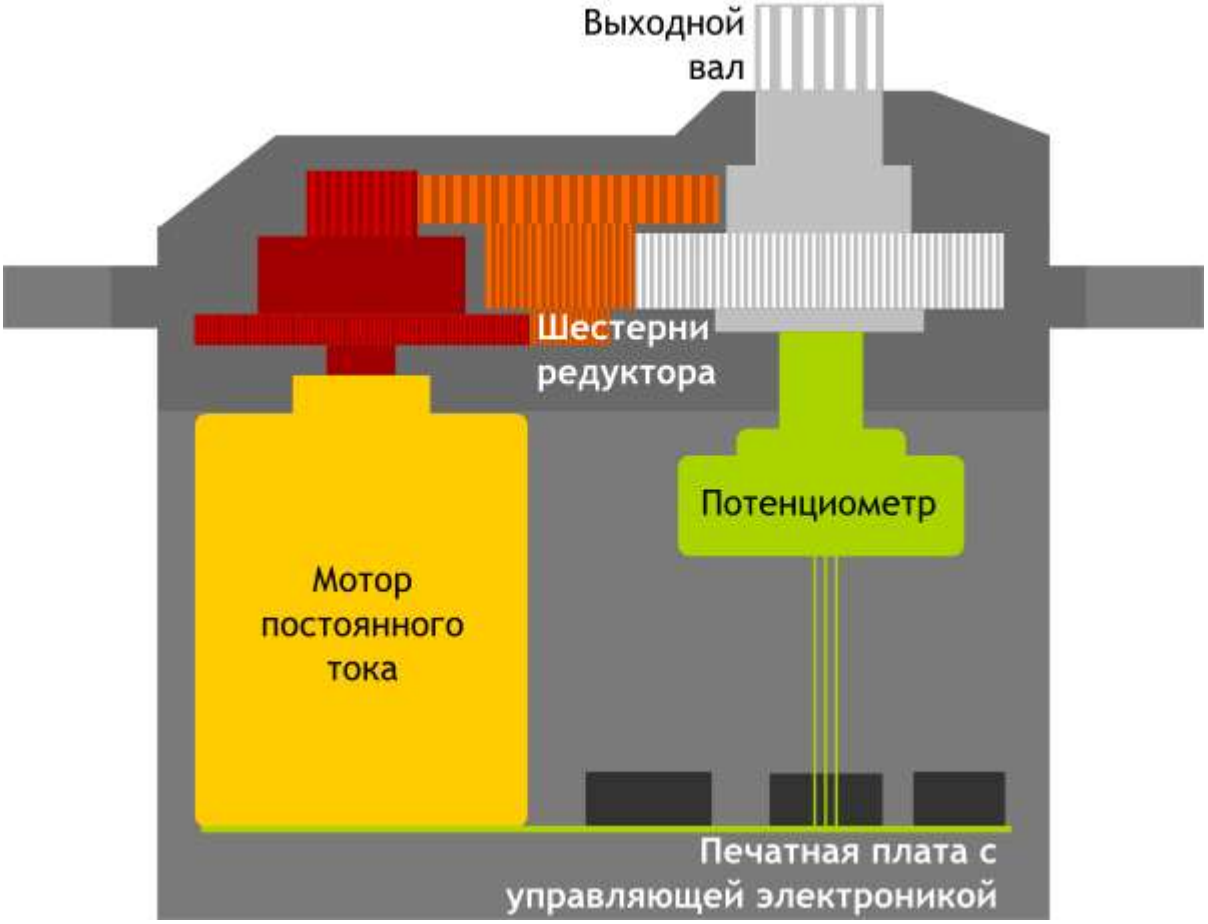


Рисунок 10 – Строение сервопривода

Привод — электромотор с редуктором. Чтобы преобразовать электричество в механический поворот, необходим *электромотор*. Однако зачастую скорость вращения мотора бывает слишком большой для практического использования. Для понижения скорости используется *редуктор*: механизм из шестерней, передающий и преобразующий крутящий момент.

Включая и выключая электромотор, можно вращать выходной вал — конечную шестерню сервопривода, к которой можно прикрепить нечто, чем мы хотим управлять. Однако, для того чтобы положение контролировалось устройством, необходим *датчик обратной связи — энкодер*, который будет преобразовывать угол поворота обратно в электрический сигнал. Для этого часто используется потенциометр. При повороте бегунка потенциометра происходит изменение его сопротивления, пропорциональное углу поворота. Таким образом, с его помощью можно установить текущее положение механизма.

Кроме электромотора, редуктора и потенциометра в сервоприводе имеется электронная начинка, которая отвечает за приём внешнего параметра, считывание значений с потенциометра, их сравнение и включение/выключение мотора. Она-то и отвечает за поддержание отрицательной обратной связи.

К сервоприводу тянется три провода. Два из них отвечают за питание мотора, третий доставляет управляющий сигнал, который используется для выставления положения устройства.

Управление сервоприводом. Интерфейс управляющих сигналов

Чтобы указать сервоприводу желаемое положение, по предназначенному для этого проводу необходимо посылать управляющий сигнал. Управляющий сигнал — импульсы постоянной частоты и переменной ширины.

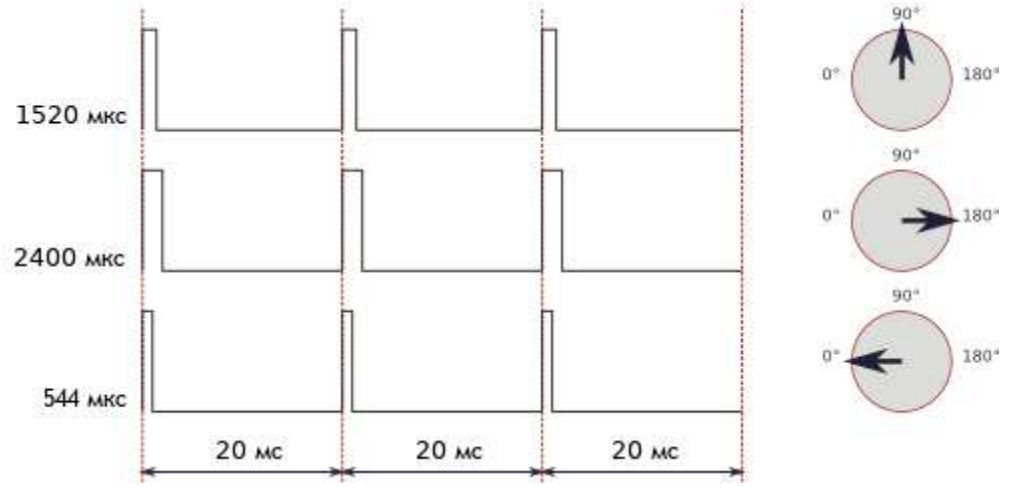


Рисунок 11 – Пример зависимости угла поворота от скважности

То, какое положение должен занять сервопривод, зависит от длины импульсов. Когда сигнал поступает в управляющую схему, имеющийся в ней генератор импульсов производит свой импульс, длительность которого определяется через потенциометр. Другая часть схемы сравнивает длительность двух импульсов. Если длительность разная, включается электромотор. Направление вращения определяется тем, какой из импульсов короче. Если длины импульсов равны, электромотор останавливается.

Чаще всего в серво-приводах импульсы производятся с частотой 50 Гц. Это значит, что импульс испускается и принимается раз в 20 мс. Обычно при этом длительность импульса в 1520 мкс означает, что сервопривод должен занять среднее положение. Увеличение или уменьшение длины импульса заставит сервопривод повернуться по часовой или против часовой стрелки соответственно. При этом существуют верхняя и нижняя границы длительности импульса. В библиотеке Servo для Arduino по умолчанию выставлены следующие значения длин импульса: 544 мкс — для 0° и 2400 мкс — для 180°.

Обратите внимание, что на вашем конкретном устройстве заводские настройки могут оказаться отличными от стандартных. Некоторые сервоприводы используют ширину импульса 760 мкс. Среднее положение при этом соответствует 760 мкс, аналогично тому, как в обычных сервоприводах среднему положению соответствует 1520 мкс.

Также стоит отметить, что это всего лишь общепринятые длины. Даже в рамках одной и той же модели сервопривода может существовать погрешность, допускаемая при производстве, которая приводит к тому, что рабочий диапазон длин импульсов немного отличается. Для точной работы каждый конкретный сервопривод должен быть откалиброван: путём экспериментов необходимо подобрать корректный диапазон, характерный именно для него.

На что ещё стоит обратить внимание, так это на путаницу в терминологии. Часто способ управления сервоприводами называют PWM/ШИМ (Pulse Width Modulation) или PPM (Pulse Position Modulation). Это не так, и использование этих способов может даже повредить привод. Корректный термин — PDM (Pulse Duration Modulation). В нём крайне важна длина импульсов и не так важна частота их появления. 50 Гц — это норма, но сервопривод будет работать корректно и при 40, и при 60 Гц. Единственное, что нужно при этом иметь в виду — это то, что при сильном уменьшении частоты он может работать рывками и на пониженной мощности, а при сильном завышении частоты (например, 100 Гц) может перегреться и выйти из строя.

Характеристики сервоприводов

Крутящий момент и скорость поворота

Сначала поговорим о двух очень важных характеристиках сервопривода: о *крутящем моменте* и о *скорости поворота*.

Момент силы, или крутящий момент — векторная физическая величина, равная произведению радиус-вектора, проведенного от оси вращения к точке приложения силы, на вектор этой силы. Характеризует вращательное действие силы на твёрдое тело.

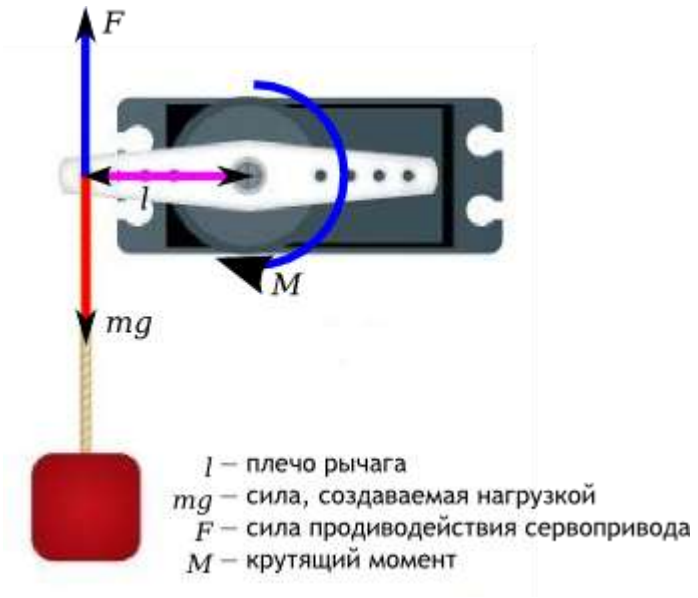


Рисунок 12 – Физические характеристики серво привода

Стоит отметить, что иногда приходится искать компромисс между этими двумя характеристиками, так как если мы хотим надёжный, выдерживающий большой вес сервопривод, то мы должны быть готовы, что эта могучая установка будет медленно поворачиваться. А если мы хотим очень быстрый привод, то его будет относительно легко вывести из положения равновесия. При использовании одного и того же мотора баланс определяет конфигурация шестерней в редукторе.

Конечно, мы всегда можем взять установку, потребляющую большую мощность, главное, чтобы её характеристики удовлетворяли нашим потребностям.

Форм-фактор

Сервоприводы различаются по размерам. И хотя официальной классификации не существует, производители давно придерживаются нескольких размеров с общепринятым расположением крепёжных элементов. Их можно разделить на:

- маленькие
- стандартные
- большие

Эти проблемы можно решать за счёт увеличения частоты приёма, обработки сигнала и управления электромотором. Цифровые сервприводы используют специальный процессор, который получает управляющие импульсы, обрабатывает их и посылает сигналы на мотор с частотой 200 Гц и более. Получается, что цифровой сервопривод способен быстрее реагировать на внешние воздействия, быстрее развивать необходимые скорость и крутящий момент, а значит, лучше удерживать заданную позицию, что хорошо. Конечно, при этом он потребляет больше электроэнергии. Также цифровые сервоприводы сложнее в производстве, а потому стоят заметно дороже. Собственно, эти два недостатка — все минусы, которые есть у цифровых сервоприводов. В техническом плане они безоговорочно побеждают аналоговые сервоприводы.

2.2.3 Сонар

Внедрение ультразвуковых датчиков обусловлено возможностью организации динамической карты помещения. И дублирующей системой определения проникновения.

Ультразвуковой дальномер HC-SR04 предназначен для измерения расстояния от устройства до объекта. Сенсор дальномера работает по принципу сонара, а точнее — посылает ультразвуковой пучок и по задержке отражённого от объекта сигнала определяет расстояние до цели.

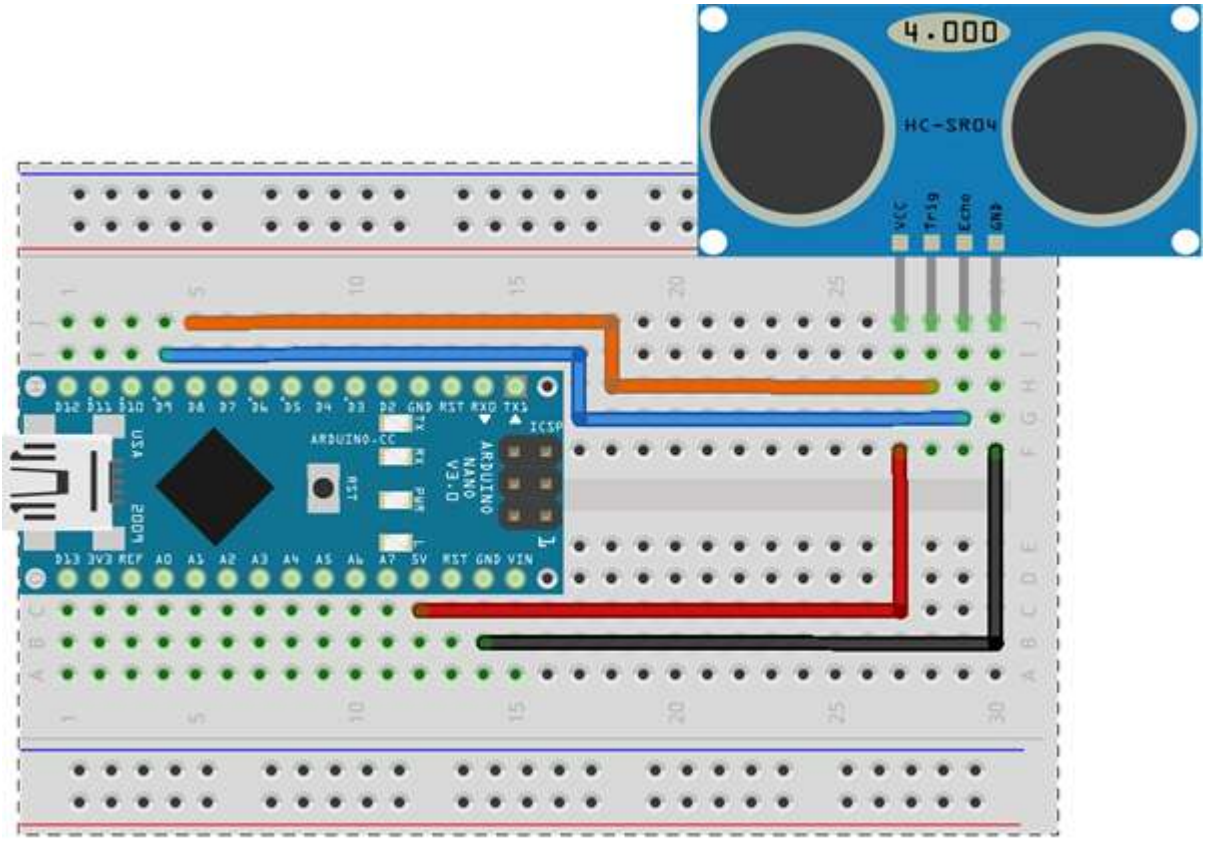


Рисунок 13 – Схема подключения сонара

Рисунок 14 – Принцип работы сонара

Примером использования такой технологии могут стать небольшие автозалы контейнерного типа, получившие широкое распространение в удалённых районах.

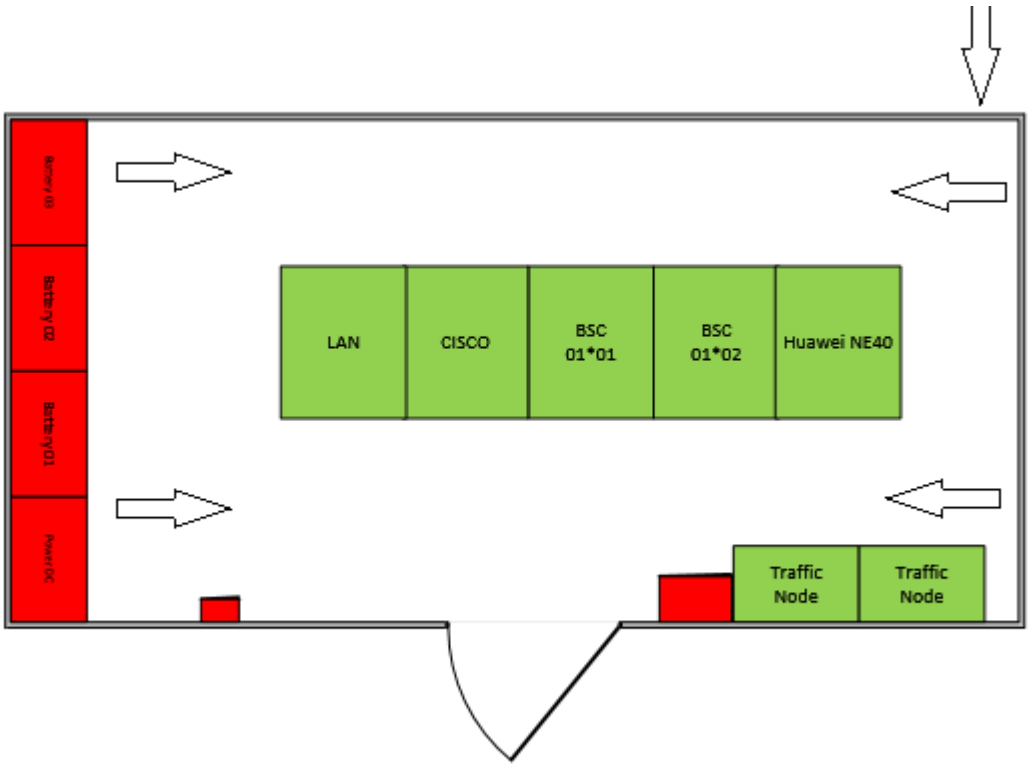


Рисунок 15 – Схема внедрения детектирования по средствам сонара

2.2.4 Инфракрасный датчик

PIR (пассивные инфракрасные датчики) сенсоры позволяют улавливать движение. Очень часто используются в системах сигнализации. Эти датчики малые по габаритам, недорогие, потребляют мало энергии, легки в эксплуатации, практически не подвержены износу. Кроме PIR, подобные датчики называют пироэлектрическими и инфракрасными датчиками движения.

Рисунок 16 – Внешний вид инфракрасного сенсора

ПИР датчики движения по сути состоят из пироэлектрического чувствительного элемента (цилиндрическая деталь с прямоугольным кристаллом в центре), который улавливает уровень инфракрасного излучения. Все вокруг излучает небольшой уровень радиации. Чем больше температура, тем выше уровень излучения. Датчик фактически разделен на две части. Это обусловлено тем, что нам важен не уровень излучения, а непосредственно наличие движение в пределах его зоны чувствительности. Две части датчика установлены таким образом, что если одна половина улавливает больший уровень излучения, чем другая, выходной сигнал будет генерировать значение высокого уровня или низкого уровня.

Пироэлектрический датчик движения состоит из двух основных частей. Каждая из частей включает в себя специальный материал, чувствительный к инфракрасному излучению. В данном случае линзы особо не влияют на работу датчика, так что мы видим два участка чувствительности всего модуля. Когда датчик находится в состоянии покоя, оба сенсора определяют одинаковое количество излучения. Например, это может быть излучение помещения или окружающей среды на улице. Когда теплокровный объект (человек или животное), проходит мимо, он пересекает зону чувствительности первого сенсора, в результате чего на модуле ПИР датчика генерируются два различных значения излучения. Когда человек покидает зону чувствительности первого сенсора, значения выравниваются. Именно изменения в показаниях двух датчиков регистрируются и генерируют импульсы HIGH или LOW на выходе.

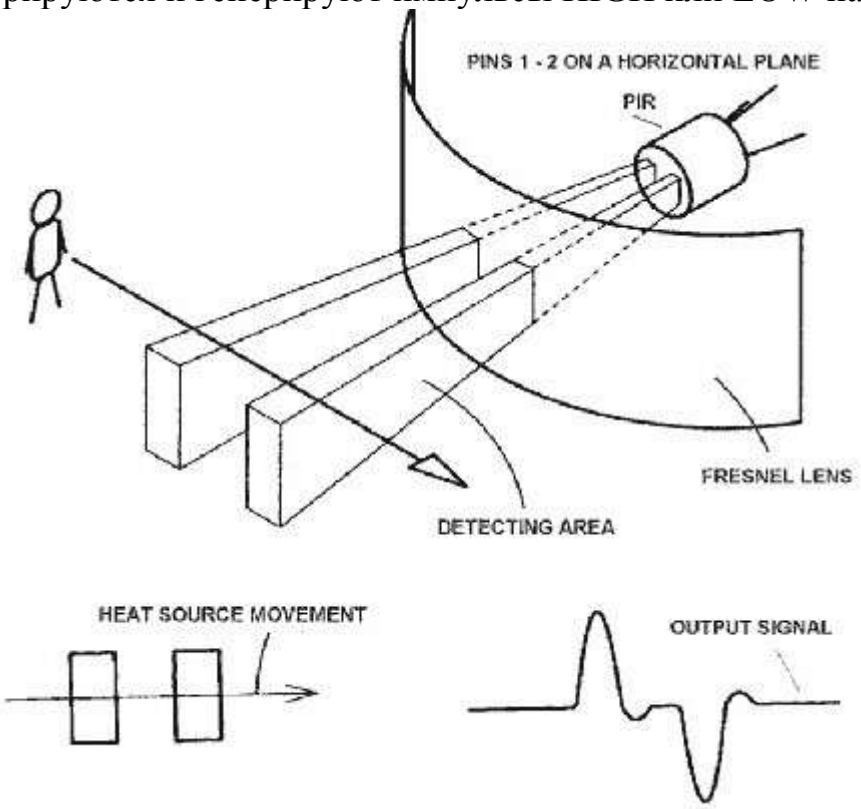


Рисунок 17 – Диаграмма направленности PIR датчика

Конструкция PIR датчика

Чувствительные элементы ПИР датчика устанавливается в металлический герметический корпус, который защищает от внешних шумов, перепадов температур и влажности. Прямоугольник в центре сделан из материала, который пропускает инфракрасное излучение (обычно это материал на основе силикона). За этой пластиной устанавливаются два чувствительных элемента.

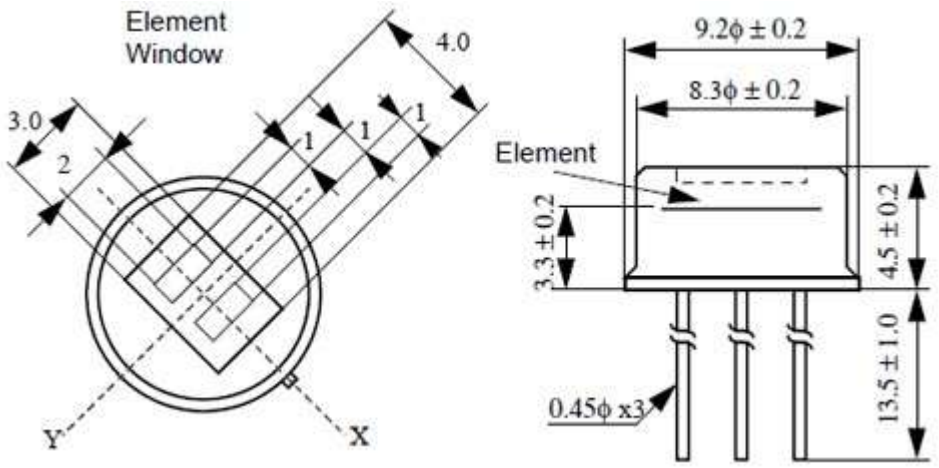


Рисунок 17 – Устройство PIR датчика

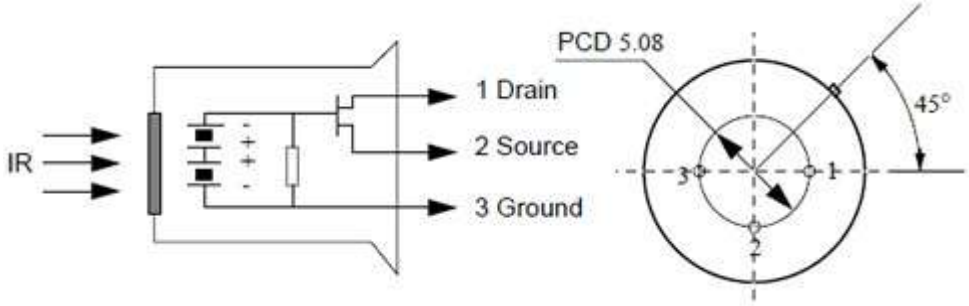


Рисунок 18 – Устройство PIR датчика

На рисунке выше приведена внутренняя схема подключения.

Инфракрасные датчики движения практически одинаковые по своей структуре. Основные отличия - чувствительность, которая зависит от качестве чувствительных элементов. При этом значительную роль играет оптика.

На рисунке выше приведен пример линзы из пластика. Это значит, что диапазон чувствительности датчика представляет из себя два прямоугольника. Но, как правило, нам нужно обеспечить большие углы обзора. Для этого можно использовать линзы, подобные тем, которые используются в фотоаппаратах. При этом линза для датчика движения должна быть маленькая, тонкая и изготавливаться из пластика, хотя он и добавляет шумы в измерения. Поэтому в большинстве PIR датчиков используются линзы Френеля.

Линзы Френеля концентрируют излучение, значительно расширяя диапазон чувствительности пиродатчиков

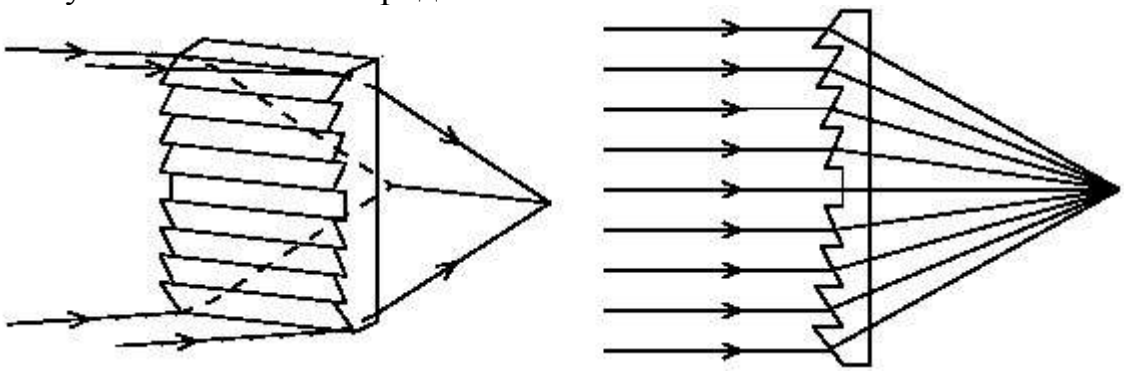


Рисунок 19 – Линза Френеля

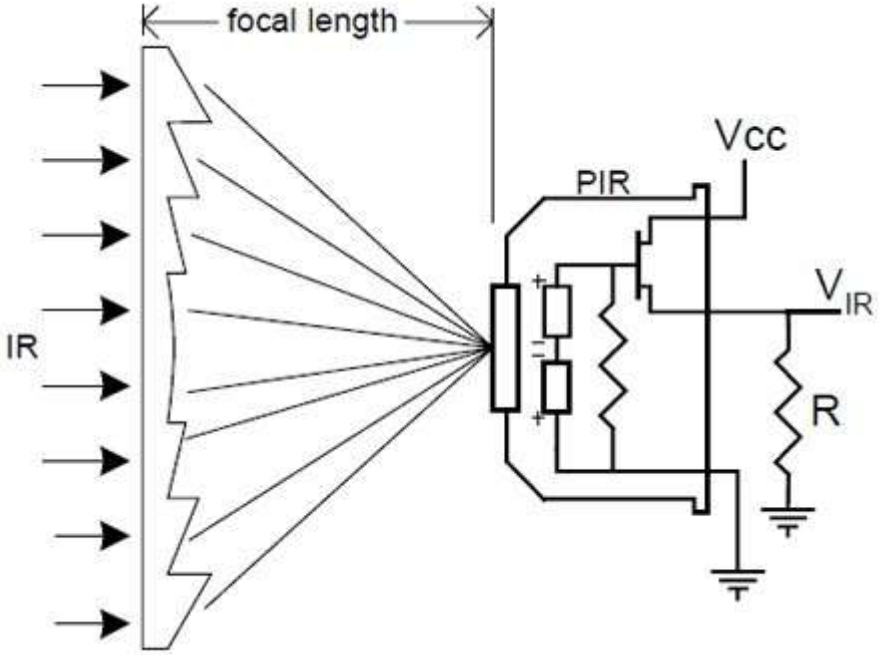


Рисунок 20 – Линза Френеля применимо к датчику

Теперь есть значительно больший диапазон чувствительности. При этом мы помним, что у нас два чувствительных элемента и нам нужны не столько два больших прямоугольника, сколько большое количество маленьких зон чувствительности. Для этого линза разделяется на несколько секций, каждая из которых представляет из себя отдельную линзу Френеля.

2.2.5 Прецизионный датчик температуры и влажности

DHT11 цифровой датчик температуры и влажности является составным датчиком, который содержит калиброванный цифровой выходной сигнал с показаниями температуры и влажности. Он имеет высокую надежность и превосходную долговременную стабильность работы. Датчик включает в себя резистивный сенсор влажности и измерения температуры.

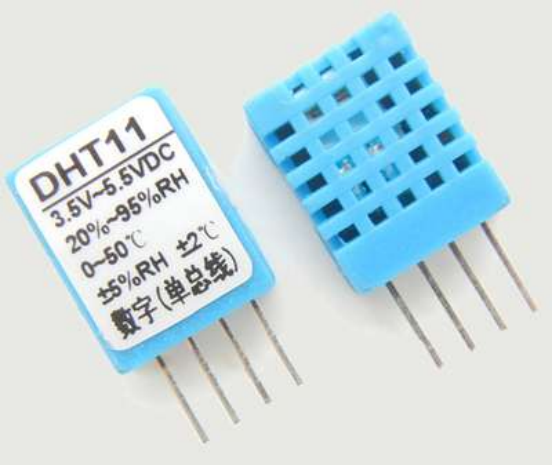


Рисунок 21 – Внешний вид DHT11

Фотография датчика DHT11 в разрезе представлена на рисунке 21.

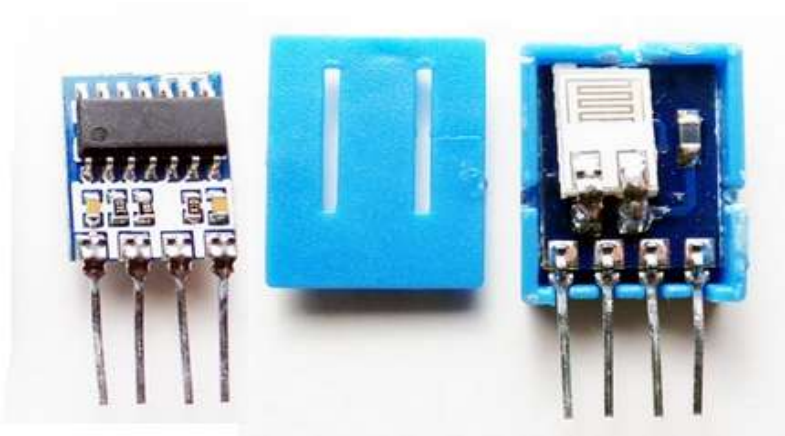
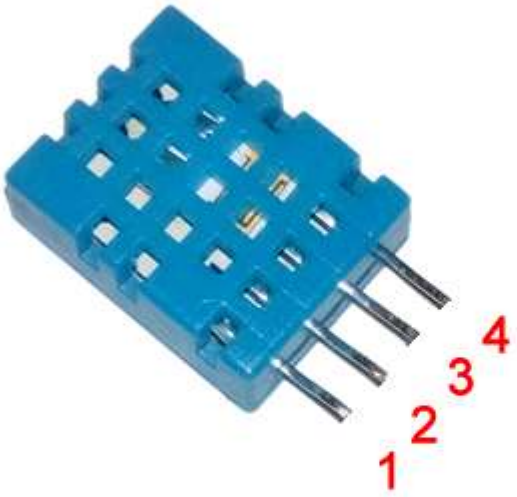


Рисунок 22 - Датчик DHT11 в разрезе



1 - Vcc 3 - NC
2 - Data 2 - GND

Рисунок 23 – Порты

Vcc — питание +3,5 ~ 5,5 В
Data — передача данных
NC — не используется
GND — отрицательное питание (-)

2.2.6 Фоторезистор

Фоторезистор – это датчик, электрическое сопротивление которого меняется в зависимости от интенсивности падающего на него света. Внешний вид представлен на рисунке 16.

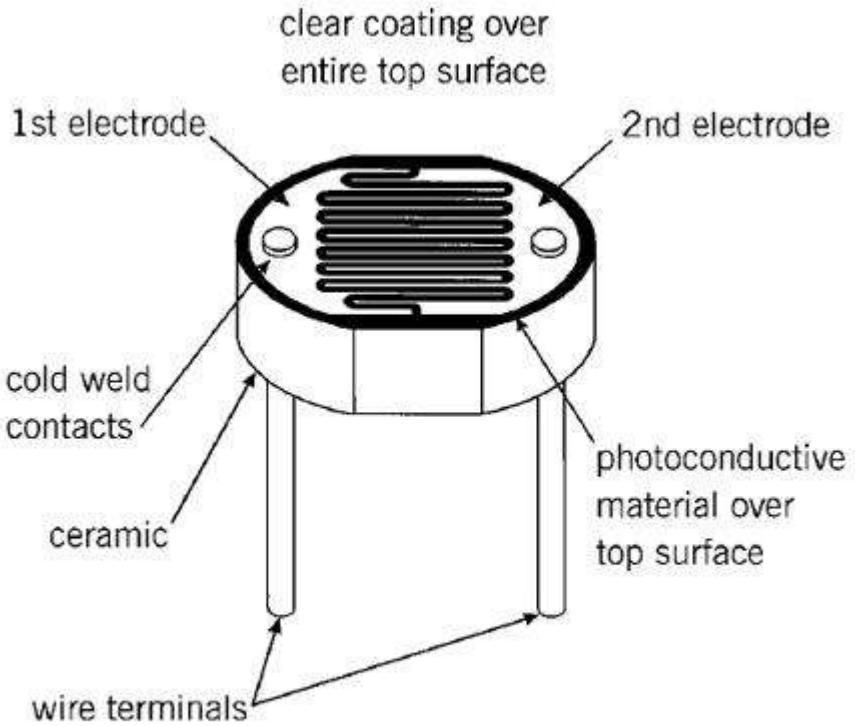


Figure 3
Typical Construction of a Plastic Coated Photocell

Рисунок 24 – Схема фоторезистора

Область применения фоторезистора в данном классе охранных комплексов охарактеризована необходимостью за контролем общего фона освещённости охраняемого объекта. Сопротивление фоторезистора изменяется в зависимости от уровня освещения. Когда темно, сопротивление резистора увеличивается до 10 МОм. С увеличением уровня освещенности сопротивление падает. Приведенный ниже график отображает приблизительное сопротивление сенсора при разных условиях освещения. Не забывайте, что характеристика каждого отдельного фоторезистора будет несколько отличаться, эти характеристики отображают только общую тенденцию. Применение фоторезисторов в связке с программно-аппаратным комплексом охранной сигнализации даёт возможность задать функциональную зависимость параметру освещённости индивидуально для каждого подключаемого фоторезистора. Либо вывести аппроксимированную функцию – которая в допустимых пределах погрешности позволит получить Люкс - Омную характеристику.

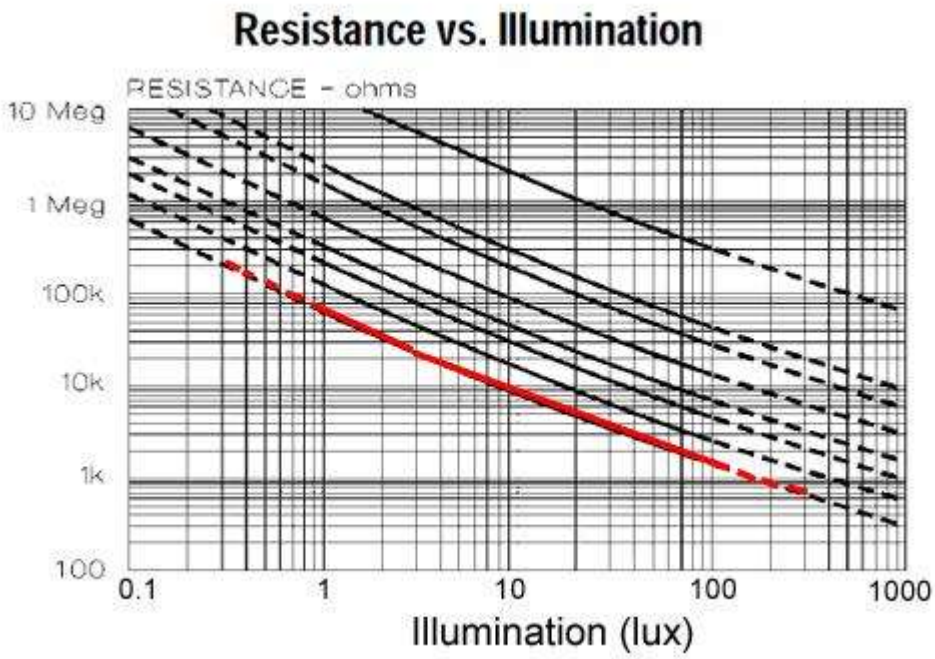


Рисунок 24 – Люкс Омная характеристика

Обратите внимание, что характеристика нелинейная, а имеет логарифмический характер.

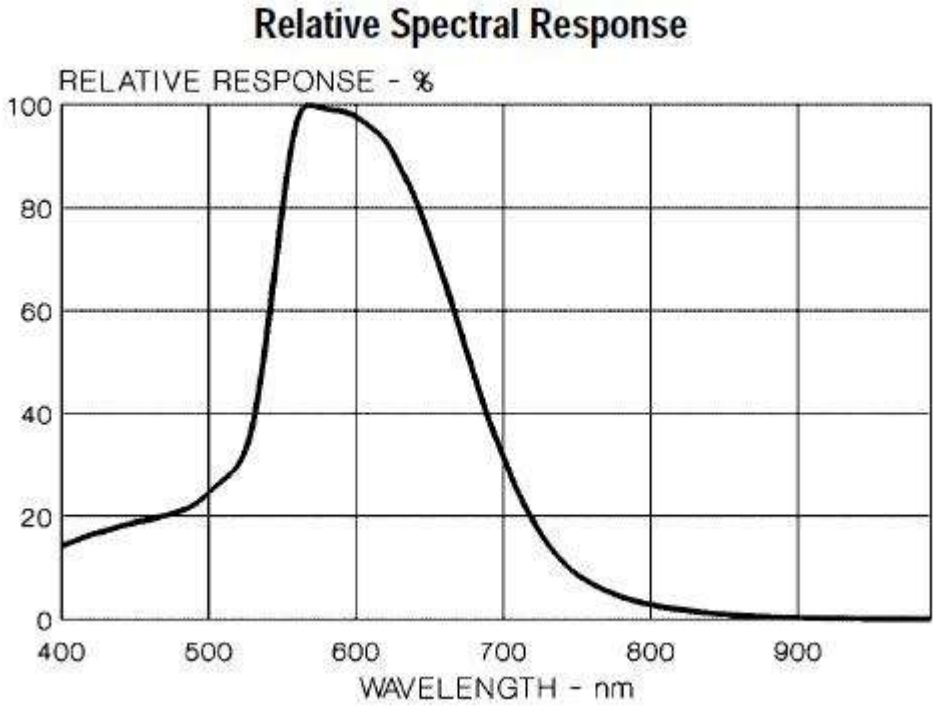


Рисунок 24 –характеристика чувствительности датчика

2.2.7 Датчик газа MQ2

Датчик можно использовать для обнаружения утечек промышленного газа и задымления. Выходным результатом является аналоговый сигнал, пропорциональный содержанию газов, к которым восприимчив газоанализатор. Чувствительность может быть настроена с помощью триммера на плате датчика. Применение данного датчика газа в связке с программно-аппаратным комплексом охранной сигнализации даёт возможность задать функциональную зависимость параметру освещённости индивидуально для каждого подключаемого сенсора. Либо вывести аппроксимированную функцию – которая в допустимых пределах погрешности позволит получить характеристику содержания газа. В силу дешевизны датчиков точную калибровку необходимо производить индивидуально для каждого датчика на эталонном оборудование.

В газоанализатор встроен нагревательный элемент, который необходим для химической реакции. Поэтому во время работы сенсор будет горячим, это нормально. Для получения стабильных показаний новый сенсор необходимо один раз прогреть (оставить включённым) в течение 24 часов. После этого стабилизация после включения будет занимать около минуты.

Показания сенсора подвержены влиянию температуры и влажности окружающего воздуха. Поэтому в случае использования датчика газа в изменяющейся среде, при необходимости получения точных показаний, понадобится реализовать компенсацию этих параметров.

Рисунок 25 – Сенсор CO2

Характеристики
Напряжение питания: 5 В
Потребляемый ток: 160 мА
Диапазон измерений
Пропан: 0,2 – 5 промилле
Бутан: 0,3 – 5 промилле
Метан: 5 – 20 промилле
Водород: 0,3 – 5 промилле

Выводы по второй главе

Использование открытых стандартов интерфейсов а так же гибкости исходного кода – достигается высокая надёжность и адаптивность конечного продукта. В аппаратной модели будет представлена функция определения нарушения безопасности объекта в первую на основе скорости изменения температуры воздушных масс. Также будут внедрены вспомогательные методы обнаружения проникновений и потенциальных угроз по прямым и косвенным признакам.

3 Разработка и исследование системы безопасности

Общий вид системы представлен на рисунке 18 и представляет собой комплексное решение по предоставлению защищённой зоны, как от внешних угроз, так и от внутренних. О принципах работы аппаратной части пойдёт речь в главе 3.1 - Разработка принципов взаимодействия частей аппаратной части. Непосредственно, стык между аппаратной и программной частями рассматривается в двух главах: в каждой со своей стороны. Способ реализации графического интерфейса, описание метода отправки данных в базу данных SQL, организация почтовых уведомлений и разработка WEB-интерфейса подробно представлены в главе 3.2 - Разработка принципов взаимодействия модулей системы.

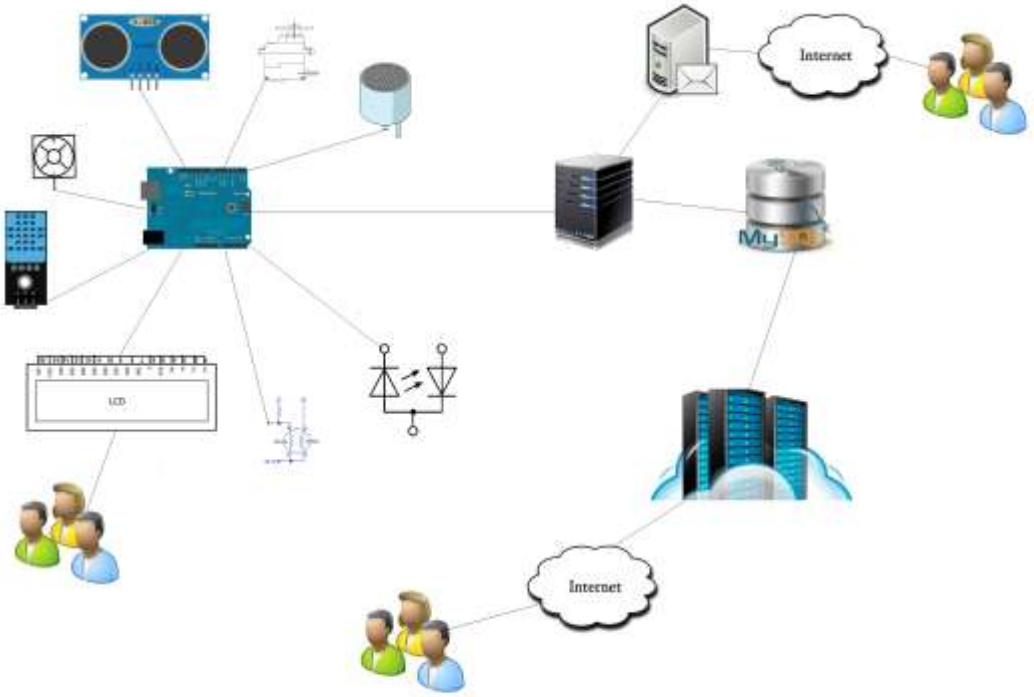


Рисунок 26 – Структурная схема системы безопасности

3.1 Разработка принципов взаимодействия модулей аппаратной части

Для обмена данными аппаратной и программной части применяется COM port на первом уровне.

Так же есть возможность организации поддержки TCP/IP протокола. Но это требует установки дополнительного модуля. И дальнейшей разработки системы. В силу строгих разграничений по модели OSI и наличию набора протоколов IP Sec (AH, ESP) – есть возможность внедрить шифрование на канальном уровне.

В случае установки дополнительного модуля появляется возможность развёртывания WEB сервера на базе контроллера.

3.1.1 Контроль температуры и влажности

Контроль температуры внутри и снаружи помещения даёт возможность косвенного обнаружения проникновения в охраняемую зону.

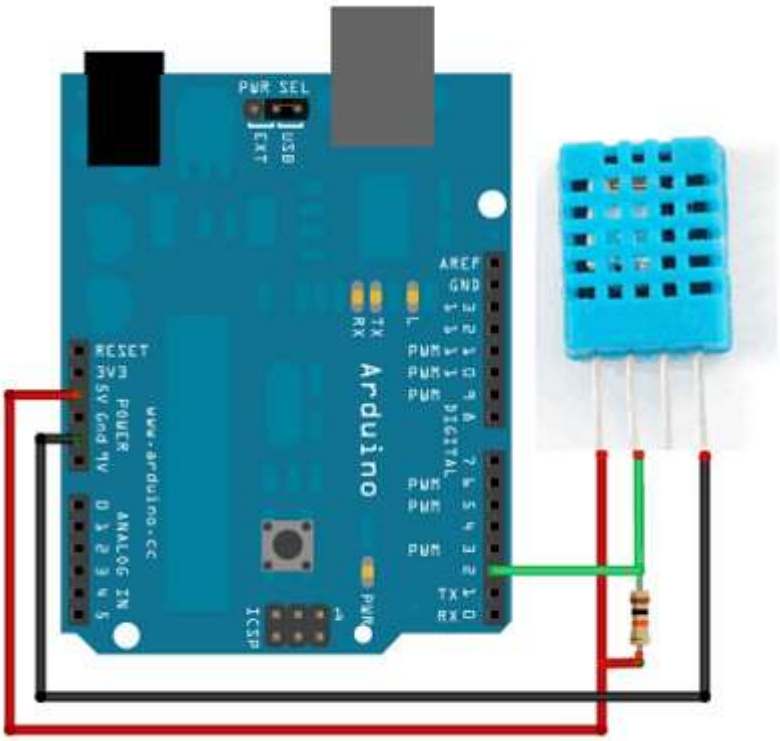


Рисунок 27 – Подключение сенсора температуры и влажности

Выбор пал на этот сенсор в силу высокой точности, экономии портов контроллера, низкого энергопотребления, отсутствия необходимости использования АЦП.

Коммуникация осуществляется при помощи библиотеки взаимодействия с датчиками семейства DHT. Библиотека оснащена обработчиком ошибок. Под процессом взаимодействия понимается считывание показаний температуры и влажности окружающей среды и передача этой информации на сервер графического интерфейса и ЖК экран.

Часть листинга взаимодействия приведена ниже.

```
#include <dht11.h>
 dhtRes = DHT.read(DHT11_PIN);    // Чтение данных с сенсора DHT11
        switch (dhtRes){
        case DHTLIB_OK: // Если всё хорошо то вывести данные
                LcdDht1Temp(DHT.temperature);
                LcdDhtRH1(DHT.humidity);
                Serial1.print(DHT.temperature);
                Serial1.print(" C,");
                Serial1.print(DHT.humidity);
                Serial1.print(" RH,");
        break;
        case DHTLIB_ERROR_CHECKSUM:
                Serial1.println("Checksum error, \t");
   break;
   case DHTLIB_ERROR_TIMEOUT:
                Serial1.println("Time out error, \t");
        break;
        default:
   Serial1.println("Unknown error, \t");
        break;
  }
```

3.2 Разработка принципов взаимодействия модулей программной части

3.2.1 Графический пользовательский интерфейс

Графический интерфейс реализован на компиляторе Processing на рисунке 26.

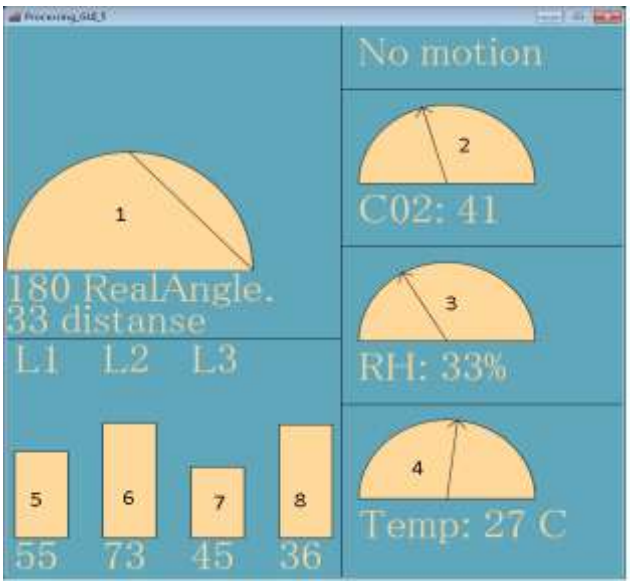


Рисунок 28 – Графический интерфейс написанный на Java

Анимированное меню состоит из следующих секций:

- индикатор положения лазера относительно горизонта;
- уровень CO2;
- относительная влажность воздуха;
- температура;
- уровень приёма первого сонара;
- уровень приёма второго сонара;
- уровень приёма третьего сонара;

Пороги срабатывания лазеров выставляются в контроллере и графическом интерфейсе отдельно. Пороги внутри контроллера отвечают за изменения на ЖК экране. В то время как пороги внутри кода графического интерфейса помимо дополнительной индикации принимают решение об отправке электронной почты. В теле письма содержится информация о имени сенсора – на котором было замечено проникновение и цифровым значением (при его наличии.

3.2.2 Хранение истории данных в MySQL

В силу необходимости ведения истории и возможности получения статистических данных об охране объекта, необходимо записывать историю состояний сенсоров. Данная система позволяет вести такую историю с периодом до 10 записей в секунду.

Для этих целей идеально подходит база данных SQL.

Настраивается интерфейс между графической оболочкой и SQL на основе подключаемой библиотеки , как на рисунке 27.

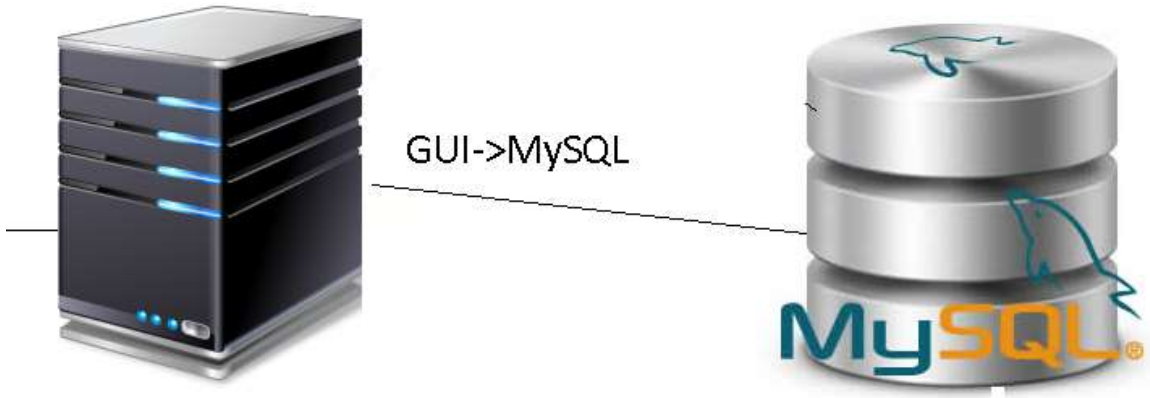


Рисунок 29 – Взаимодействие между графической оболочкой и базой данных

Взаимосвязь SQL и графическим интерфейсом происходит по средствам библиотеки import de.bezier.data.sql.*;

Данные узлы могут находиться на единой машине – что позволит экономить ресурсы, но приведёт к Single point of failure. Так применение географического разнесения позволит избежать данной проблемы – но приведёт к росту оперативных расходов. При таком используется среда Internet как сетевой уровень передачи данных и IP Sec туннели – для шифрования данных. Данный способ шифрования характерен сетевому уровню. При наличии специальных требований , могут быть внедрены SSL на транспортном и внутреннее шифрование на уровне приложений.

Принцип построения структуры базы данных:

Была написана функция, в аргументах содержащая имя таблицы и передаваемые туда данные.

Имя таблицы меняется в зависимости от характера данных.

Пример взаимодействия java оболочки и SQL server приведена ниже.

```
MySQL msql1; // Create object
String user     = "mainUser";
String pass     = "Changeme";
String database = "Security_DB";
String host = "localhost";
void Sql( String curTabl,String Column1,String Column2,String Column3, String Column4, String Column5) {
  if ( msql.connect() )
  {
```

```
msql.query( "INSERT INTO " + curTabl + "  VALUES(NULL, " + Column1 + ", "+ Column2 + ", "+ Column3 + ", "+ Column4 + ", "+ char(34)+ Column5 + char(34)+", NULL);");
//println("INSERT INTO " + curTabl + "  VALUES(NULL, " + Column1 + ", "+ Column2 + ", "+ Column3 + ", "+ Column4 + ", "+ Column5 +", NULL);");
}
}
```

3.3.3 Представление данных в WEB сервере

Бывают случаи, в которых требуется распределённый доступ к информации.

Примером может группа людей-операторов центра мониторинга, или же если требуется иметь возможность мониторинга, находясь в любой отдалённой точке планеты.

Рисунок 30 – WEB форма представления информации.

Для этих целей был использована сборка WEB сервиса на базе Xampp.

Стык между ним с базой данных был выполнен по средствам функции mysql_connect.

В следствии распределенности узлов системы, данные могут независимо обрабатываться на разных этапах следования.

WEB платформа является наиболее приемлемой, с точки зрения её унифицированности и кросс-платформенности. Давая возможность для просмотра информации как мобильным терминалами разных производителей , так и стационарным ПК с различными ОС.

Так же присутствует возможность внедрения протокола HTTPS. Как с доверенным сертификатом – выданным мировым центром сертификации (для внедрения продукта в большие компании), так и с лично сгенерированным ключом (во избежание ошибок необходимо добавить его в доверенные сертификаты каждой машины)

Выводы по третьей главе

При разработке сложных охранных комплексов с возможностью быстрого расширения функционала необходимо разделение процессов обработки информации. Не рационально нагружать один блок многими задачами, так как это создаст single point of failure. Перед выполнением проекта в аппаратной платформе необходимо сделать виртуальную модель , проверив её пригодность в идеальных условиях. На данном этапе важную роль играет программный пакет ISIS Proteus и Fritzing. Fritzing, бесплатное ПО нацеленное на макетирование из плат Arduino и Arduino-совместимых устройств.

Заключение

Проектирование и внедрение представленной системы безопасности телекоммуникационных объектов позволяет более детально рассмотреть мельчайшие детали организации охраны телекоммуникационных объектов. Учитывая научную новизну данного направления исследований и высокую потребность рынка связи в такого рода устройствах, можно сказать, что данная технология будет активно развиваться и дальнейшем, причём в самых разных областях: от разработки и поддержки комплексов операторского уровня до рынка мелкого и среднего бизнеса в сфере телекоммуникаций.

Базируясь на модульной конструкции и концепции взаимозаменяемости деталей, дополненной политикой открытого кода – достигается высокая надёжность и быстродействие системы при сохранении приемлемой стоимости. Достигается это тем, что минимизируется CAPEX и OPEX.

В данной работе было проведено исследование, посвященное возможности взаимодействия микроконтроллерной части охранной системы с уровнем приложений по средствам внутреннего протокола взаимодействия. Такой вид интеграции открывает новые горизонты в построении охранных систем. Так как появляется возможность наращивания функционала сенсоров, по мере их появления или по мере роста потребностей заказчика.

Перечень сокращений

В настоящей магистерской диссертации применяют следующие термины с соответствующими определениями:

IDE – Integrated Development Environment, интегрированная среда разработки

HTTP - Hypertext Transfer Protocol

PWM - Pulse Width Modulation, широтно-импульсная модуляция

UART - Universal Asynchronous Receiver-Transmitter

SQL - structured query language

WWW - world wide web

POP3 - Post Office Protocol Version 3

ИК - инфракрасный порт

СЗИ - средства защиты

Vcc - Collector supply voltage

ШИМ – широтно импульсная модуляция

IP Sec – Internet protocol security

Список литературы

1 Майк Шмидт. Arduino - 08.05.2014

2 Марголис М. Рецепты Arduino. Margolis M. – Arduino Cookbook – 2011

3 Долгий А. Разработка и отладка устройств на микроконтроллерах / Радио» – №5. – 2001.

4 Зайцев А.П., Шелупанов А.А. Технические средства и методы защиты информации / Машиностроение – 2009.

5 Р.Стюарт Болл – Аналоговые интерфейсы микроконтроллеров (Программируемые системы) 2007.

6 Кабатов Д.А. «Что такое облачные сервисы для небольших компаний?» URL: http://www.moysklad.ru/chto_takoe_oblachnye_servisy/ (Дата обращения: 21.02.2015)

7 Облачные технологии // Wikipedia.URL: https://ru.wikipedia.org/wiki/Облачные_вычисления / Дата обращения: 13.02.2015)

8 Оксер Дж., Блемингс Х. Практика для Arduino: Крутые проекты для доступных плат / Practical Arduino: Cool Projects for Open Source Hardware - Oxer J., Blemings H

9 Майк МакРобертс . Arduino для начинающих»// Arduino starter kit manual - Mike McRoberts

10 Улли Соммер. Программирование микроконтроллерных плат Arduino/Freeduino

11 Знакомство с Arduino (перевод книги "Getting Started with Arduino")

12 Чарльз Платт . Электроника для начинающих

13 В. Эванс . Ардуино Блокнот программиста

14 Полярная система координат. URL:https://ru.wikipedia.org/wiki/Полярная_система_координат (Дата обращения 5.04.2015)

Приложение А

Код микроконтроллера

```
/* Подключаем библиотеку для работы с LCD */
#include <LiquidCrystal.h>
#include <dht11.h>      // Добавляем библиотеку DHT11
//LCD
#define RS      22
#define RW      24
#define E       26
#define DB4     28
#define DB5     30
#define DB6     32
#define DB7     34
LiquidCrystal lcd(RS, E, DB4, DB5, DB6, DB7);

byte degree [8] = {
  B11000,
  B11000,
  B00111,
  B01000,
  B01000,
  B01000,
  B01000,
  B00111,
};
//4 relay module
#define RELAY1  36
#define RELAY2  38
#define RELAY3  40
#define RELAY4  42
//DHT11
dht11 DHT;      // Объявление переменной класса dht11
#define DHT11   44
int chk; // Переменная в которую записывается результат считывания с
датчика температуры.
//Servo
#define SERVO1  46
//Sonar
#define ECHO    31
#define TRIG    33
//PIR
#define PIR     35
//Main
void setup()
```

```
{
  //LCD
  pinMode(RW, OUTPUT);
  digitalWrite(RW, LOW);
  lcd.begin(16, 2);
  lcd.createChar(2, degree);
  //Serial
  Serial.begin(9600);   // Скорость работы порта
  Serial.println("DHT TEST PROGRAM "); // Выводим текст
  Serial.print("LIBRARY VERSION: ");   // Выводим текст
  Serial.println(DHT11LIB_VERSION);
  Serial.println();                    // Пустая строка
  //DHT

}

 void loop(){

  ;
  // Мониторинг ошибок
  chk = DHT.read(DHT11);    // Чтение данных
  switch (chk){
  case DHTLIB_OK:
    LcdDhtTemp(DHT.temperature);
    LcdDhtRH(DHT.humidity);
    break;
  case DHTLIB_ERROR_CHECKSUM:
    Serial.println("Checksum error, \t");
    break;
  case DHTLIB_ERROR_TIMEOUT:
    Serial.println("Time out error, \t");
    break;
  default:
    Serial.println("Unknown error, \t");
    break;
  }
  delay(1000);
}

//Блок под-программ
//LCD print  humidity  - ПП вывода влажности на LCD экран
void LcdDhtRH(unsigned int RH) {
    lcd.setCursor(0, 0); //Устанавливаем курсор в 1 столбец 1й строки.
```

Нумерация идёт с нуля

```
    lcd.print("RH    ");
    lcd.print(RH); // DHT.humidity
    lcd.print("%");
  }
void LcdDhtTemp(unsigned int Temp) {
    lcd.setCursor(0, 1); //Устанавливаем курсор в 1 столбец 1й строки.
Нумерация идёт с нуля
    lcd.print("Temp  ");
    lcd.print(Temp);  // DHT.temperature
    lcd.write(byte(2));
}
void setup()
{
  //LCD
  pinMode(RW, OUTPUT);
  digitalWrite(RW, LOW);
  lcd.begin(16, 2);
  lcd.createChar(2, degree);
  //Serial
  Serial.begin(9600);   // Скорость работы порта
  Serial.println("DHT TEST PROGRAM "); // Выводим текст
  Serial.print("LIBRARY VERSION: ");   // Выводим текст
  Serial.println(DHT11LIB_VERSION);
  Serial.println();                    // Пустая строка
  //Relay
  pinMode(RELAY1, OUTPUT);
  pinMode(RELAY2, OUTPUT);
  pinMode(RELAY3, OUTPUT);
  pinMode(RELAY4, OUTPUT);
  //Distance
  pinMode(TRIG, OUTPUT);
  pinMode(ECHO, INPUT);
  pinMode(LSR, OUTPUT);

}

void loop() {
digitalWrite(TRIG, HIGH); // Подаем сигнал на выход
микроконтроллера
delayMicroseconds(10); // Удерживаем 10 микросекунд
digitalWrite(TRIG, LOW); // Затем убираем
time_us=pulseIn(ECHO, HIGH); // Замеряем длину импульса
distance_sm=time_us/58; // Пересчитываем в сантиметры
Serial.println(distance_sm); // Выводим на порт
```

```
if (distance_sm<7) // Если расстояние менее 7 сантиметром
{
  digitalWrite(LSR, 1); // Зажигаем светодиод
}
else
{
  digitalWrite(LSR, 0); // иначе тушим
}

delay(100);
}

void loop() {
   PIR_value = digitalRead(PIR); //read state of the PIR
   if (PIR_value == LOW) {
     Serial.println("Net dvijenia"); //if the value read is low, there was no
motion
   }
   else {
     Serial.println("Dvijenie!"); //if the value read was high, there was motion
   }
   delay(1000);
}
//4 relay module
#define RELAY1  36
#define RELAY2  38
#define RELAY3  40
#define RELAY4  42

//Main
void setup()
{
// Initialise the Arduino data pins for OUTPUT
  pinMode(RELAY1, OUTPUT);
  pinMode(RELAY2, OUTPUT);
  pinMode(RELAY3, OUTPUT);
  pinMode(RELAY4, OUTPUT);
}

 void loop()
{
  digitalWrite(RELAY1,LOW);          // Turns ON Relays 1
  delay(2000);                       // Wait 2 seconds
```

```
digitalWrite(RELAY1,HIGH);        // Turns Relay Off

digitalWrite(RELAY2,LOW);         // Turns ON Relays 2
delay(2000);                      // Wait 2 seconds
digitalWrite(RELAY2,HIGH);        // Turns Relay Off

digitalWrite(RELAY3,LOW);         // Turns ON Relays 3
delay(2000);                      // Wait 2 seconds
digitalWrite(RELAY3,HIGH);        // Turns Relay Off

digitalWrite(RELAY4,LOW);         // Turns ON Relays 4
delay(2000);                      // Wait 2 seconds
digitalWrite(RELAY4,HIGH);        // Turns Relay Off
```