ДОКЛАД

Уважаемый председатель, уважаемые члены комиссии, вашему вниманию предлагается дипломный проект на тему “Система защиты и контроля доступа в помещения”.

На сегодняшний день для многих государственных и частных предприятий и организаций стала актуальной проблема обеспечения безопасности сотрудников и материальных ценностей этой организации. Эта проблема во многом зависит от уровня управления доступа на объекте защиты и определяется комплексом предпринятых мер защиты и контроля доступа в помещения.

Система защиты и контроля доступа в помещения представляет из себя централизованную систему. На верхнем уровне — пульт управления; на нижнем — контролируемые пункты (показать плакат).Число контpолиpуемых пунктов зависит от количества входов подлежащих контролю на охpаняемом объекте. Проектируемая система способна обслуживать не менее 200 контролируемых пунктов.

Пульт управления выполненный на базе компьютера совместимого с IBM PC и контролируемые пункты соеденены между собой в локальную сеть. Локальная сеть содержит пульт управления и ряд удаленных контроллеров, каждый из которых соединен с одним шлюзом. В проектируемой системе выбран магистральный тип интерфейса, с "шинной" топологией системы обмена. Режим обмена информацией — полудуплексный. В полудуплексном режиме любой из контроллеров может начать передачу, если на вход его последовательного интерфейса поступил запрос с пульта управления, то есть его сетевой адрес.Для уменьшения вероятности наложений контроллер перед выдачей сообщения прослушивает канал и начинают выдачу только при поступлении запроса от компьютера на его адрес. По режиму организации передачи, данная СЗКДП относится к сети с асинхронной передачей (момент считывания данных приемником определяется по сигналам запуска от передатчика; по окончании пересылки приемник выдает передатчику сигнал об окончании цикла передачи).

В следствии того что, система представляет из себя средство управления доступом, коды идентификации пользователя и другая информация обеспечения безопасности должны хранится в таблице авторизации. Таблица авторизации находится в защищенной зоне основной памяти компьютера или хранится как файл данных на дополнительном устройстве. Каждый пользователь имеет свою запись в таблице. Если кода идентификации пользователя нет в таблице авторизации, то доступ запрещается.

Кроме того, пульт управления автоматически тестирует состояние системы и ведет протокол функционирования всего компекса защиты. Автоматически ведет жуpнал:

проходов пользователей с указанием даты, времени и направления прохода;

несанкционированных действий пользователей с указанием даты и времени нарушений;

работы операторов и администраторов системы.

Доступ к компьютеру возможен только при помощи электронного идентификатора принадлежащего администратору безопасности. Администратор безопасности с помощи мастер-карты регистрирует и удаляет коды пользователей и проводит операции по изменению прав пользователей.

Теперь покажем, что из себя представляет контролируемый пункт объекта защиты. Конструктивно контролируемый пункт представляет из себя шлюзовую систему, с двумя сдвижными дверями (показать плакат). Каждой сдвижной дверью управляет электромотор блокировки дверей. При подаче управляющего напряжения от устройства управления (показывать чертеж) на электромотор двери соответственно открываются или закрываются. В закрытом положении двери блокированы. Внутри шлюза установлен датчик массы, служащий для подтверждения подлиности пользователя.

В предлагаемой системе процедура управления доступом сводится к опознаванию пользователя системой на основе личных электронных идентификаторов. в качестве надежного сpедства pаспознавания пользователей в настоящее время служат электpонные идентификатоpы Touch Memory производства фирмы Dallas Semiconductor, Inc. Благодаря гарантированной производителем неповторяемости ключа обеспечивается высокий уровень защищенности объекта защиты.

Идентификация пользователя систимой защиты происходит следующим образом. Пользователь прикасается личным идентификатором считывателя кода (показать на чертеже); микроконтроллер прерывает рабочую программу и считывает с идентификатора 64-ех битный код. Далее код передается на ПУ, где происходит сравнение кода с кодами хранящимися в таблице авторизации. В случае совпадения идет ответный сигнал на микроконтроллер приказывающий открыть 1-ые двери шлюза. МК подает сигнал на устройство управления. УУ включает электромотор и открывает 1-ые двери приглашая тем самым пользователя войти.

В шлюзе происходит установление подлиности пользователя, то есть его аутентификация. Подлиность определяется массой пользователя. Код соответствующий массе пользователя также как и код идентификатора хранится в памяти компьютера в таблице авторизации.

СОДЕРЖАНИЕ

Введение

1. Обзор аналогичных технических решений

2. Выбор и обоснование технических требований к системе

3. Разработка архитектуры системы

4. Разработка принципиальной схемы

5. Разработка алгоритма управляющей программы

6. Разработка конструкции печатной платы

7. Технико–экономическое обоснование

8. Охрана труда и экологическая безопасность

Заключение

Список использованной литературы

Приложение 1. Характеристики радиомодемов

Приложение 2. Перечень элементов контроллера шлюза

Приложение 3. Текст основных управляющих подпрограмм

Ппиложение 4. Технические характеристики ОМЭВМ

AT89C51-20PI

 Введение

В настоящее время для многих органиэаций и частных лиц стало характерным то, что увеличилось количество краж личного и общественного имущества. Особенно эта проблема стала актуальной для крупных организаций где нарушение безопасности может нанести огромный материальный ущерб, как самим организациям, так и их клиентам. Поэтому эти организации вынуждены особое внимание уделять гарантиям безопасности. В следствие чего возникла проблема защиты и контроля доступа в помещения. И сейчас данная проблема представляет собой совокупность тесно связанных подпроблем в областях права, организации, управления, разработки технических средств, программирования и математики. Одна из центральных задач проектирования системы защиты состоит в надежном и эффективном управлении доступом на объект защиты.

Процедура управления доступом сводится к взаимному опознаванию пользователя и системы и установления факта допустимости использования ресурсов конкретным пользователем в соответствии с его запросом. Средства управления доступом обеспечивают защиту охраняемого объекта как от неавторизованного использования, так и от несанкционированного обслуживания системой. Защита реализуется процедурами идентификации, установления подлиности и регистрации обращений.

Процедура идентификации реализует задачу присвоения каждому пользователю конкретного кода с целью последующего опознавания и учета обращения. Принятая система идентификации служит исходной предпосылкой для последующего контроля подлиности доступа.

В настоящее время существует много вариантов систем защиты и контроля доступа в помещения. Но как правило, они являются дорогими, сложными, имеют недостаточное количество функциональных возможностей и используют устаревшую элементную базу. Это не позволяет решать проблему массовой тотальной охраны квартир и служебных помещений. Для расширения функциональных возможностей и для снижения стоимости при разработке охранных систем необходимо использовать микропроцессоры, что позволит реализовать аппаратуру с улучшенными техническими и потребительскими характеристиками.

Сейчас начинают получать распространание интегрированые системы обеспечения безопасности, которые позволяют осуществлять полный спектр электронного управления всеми процессами, происходящими в структуре объекта.

В случае организации системы контроля доступа при помощи электронного оборудования каждому из пользователей (сотрудники предприятия, охрана, гости и т. д.) выдается электронный идентификатор: магнитная карта, получившая наибольшее распространение в последние годы, но, к сожалению, уже не позволяющая избежать подделок и достаточно быстро изнашивающаяся, индуктивная карта или ключ, имеющие более высокую устойчивость к копированию и значительно больший срок жизни или специальный ключ (брелок) со встроенным микрочипом, срок жизни которых практически равен времени жизни системы, а попытка взлома приводит к разрушению носителя информации.

Система защиты и контроля доступа в помещения позволяет при помощи центрального микропроцессора производить сбор информации со всех опознающих устройств (считывателей), обрабатывать ее и управлять исполнительными устройствами, начиная с автоматических ворот на КПП объекта и, заканчивая тяжелыми дверьми банковских хранилищ.

1. Обзор аналогичных технических решений

Существует большое множество типов электронных систем защиты и контроля доступа в помещения. Все они отличаются друг от друга как степенью сложности и надежности, так и удобством обслуживания, что в свою очередь отражается на стоимости системы.

Как правило все системы защиты сводятся к следующим функциям: обнаружение, опознавание, управление, контроль. Приведенная ниже блок-схема часто приводится в литературе и хорошо отражает функции систе защиты.

Рис.1.1

где 1—выявление подлежащих анализу пpизнаков воздействия;

2—сравнение выявленных признаков с эталонными;

3—выработка запроса статистики опасных воздействий;

4—сбор и хранение опасных признаков воздействий;

5—выработка управляющих воздействий;

6—контроль;

7—исполнительный блок;

Выполняемые функции: 1—обнаружение, 2—опознавание 3,5—управление, 4,6—контроль, 7—коммутация доступа (или его ограничение).

При выработке подходов к решению проблем безопасности предприятия-призводители как правило исходят из того, что конечной целью любых мер противодействия угрозам является защита владельца и законных пользователей системы от нанесения им материального или морального ущерба в результате случайных или преднамеренных воздействий на нее. И здесь нужно решить три основные задачи. Это:

1) идентификация—пpоцес pаспознания опpеделенных компонентов системы, обычно с помощью уникальных, воспpинимаемых системой имен (идентификатоpов).

2) аутентификация—пpовеpка идентификации пользователя, устpойства или дpугого компонента в системе, обычно для пpинятия pешения о pазpешении доступа к pесуpсам системы.

3) автоpизация—пpедоставление доступа пользователю, пpогpамме или пpоцессу.

До сих поp основным сpедством идентификации являются или магнитные каpточки или механические ключи, котоpые сейчас удачно подделываются и не обеслечивают надежной безопасности объекта защиты. Сейчас начинают получать pаспpостpанение электpонные ключи защиты. Как показывает мировой опыт в качестве надежного сpедства pаспознавания пользователей в настоящее время служат электpонные идентификатоpы Touch Memory производства фирмы Dallas Semiconductor, Inc. Благодаря гарантированной производителем неповторяемости ключа обеспечивается высокий уровень защищенности объекта защиты.

Анализ литературы и результаты посещений выстовок (“Безопасность-96” Минск,”TIBO-96” Минск) приводят к выводу, что для обеспечения эффективной системы защиты и контроля доступа в помещения важно организовать комплексную систему безопасности. Один из лидеров в организации обеспечения систем безопасности фирма “Advance Sucurity Systems” предлагают различное оборудование для ограничения прохода людей и перемещения ценностей. Туда могут входить:

— оборудование систем контроля доступа— считыватели, различные типы идентификаторов, сетевые контроллеры, подстанции управления, подстанции сбора информации с датчиков,компьютерные платы и программное обеспечение;

— оконечные исполнительные устройства— электромагнитные замки, электрозащелки, электромоторы блокировки дверей;

— датчики охраны и сигнализации—инфракрасные датчики (принцип действия—регистрация изменения уровня теплового излучения людей и животных, передвигающихся в охраняемой зоне), вибрационные датчики, ультразвуковые датчики изменения объема, датчики массы и др., сирены, громкоговорители, всеразличные индикаторы.

— системы видеонаблюдения—мониторы, видеокамеры, объективы, коммутаторы, устройства цифровой обработки видеосигнала, знакоге-нераторы, системы сканирования.

— контрольно-пропускное оборудование—турникеты, шлюзы, шлагбаумы, ворота и т.д.

— охранно-пожарные системы—извещатели охранные, приборы приемо контрольные, аппаратура пожарной сигнализации и др.

— системы персонального вызова (пейджеры).

— бронированные двери для хранилищ.

— центральные пульты-концентраторы и пульты управления.

Перечисленые элементы системы безопасности предлагаемые этой фирмой, а также аналогичными фирмами такими как “BAUER”(Германия-Швейцария), “INTERNATIONAL ELECTRONICS”(США) соответствуют европейским и мировым стандартам, имеют высокую степень надежности, но являются очень дорогими. Поэтому средние и мелкие организации вынуждены искать менее дорогие системы защиты, имеющие невысокую степень надежности.

Исходя из вышесказанного можно сделать вывод, что комплексная система безопасности позволяет при помощи мощной центральной процессорной станции осуществлять высоконадежную защиту и эффективный контроль доступа на объект защиты.

2.Выбор и обоснование технических требований

Структура технических средств системы защиты и контроля доступа в помещения (СЗКДП) должна представлять собой двухуровневую централизованную систему, работающую в реальном времени. На верхнем уровне — пульт управления (ЭВМ, совместимая с IBM PC), с блоком связи и локальной сетью передачи данных. На нижнем уровне — N контролируемых пунктов ( КП ). КП — контролируемый пункт, в задачу которого входит защита и контроль контролируемого пункта

Обоснование:

На верхнем уровне пультом управления выполняются функции:

сбора, документирования, архивирования, представления на видеотерминал информации. А для этих целей лучше всего подходит ПЭВМ совместимая с IBM PC. Применение ПЭВМ по сравнению со специализированным пультом удобнее тем, что ПЭВМ обеспечивает широкие функциональные возможности и гарантирует гибкость и удобство в эксплуатации. Кроме того при дальнейшей модернизации системы или ее расширения не потребуется дополнительных аппаратных затрат на пульт управления, а нужно изменить только управляющую программу.

На нижнем уровне выполняются функции сигнализации, управления, регулирования и контроля. Функцию контроллера выполняет однокристальный микропроцессор, который имеет физическую и логическую разделенность памяти программ и памяти данных. Структурная организация, набор команд и аппаратурно-программные средства ввода/вывода информации такого микропроцессора очень хорошо приспособлены для решения задач управления и регулирования в приборах, устройствах и системах автоматики, а не для решения задач обработки данных. Кроме того, массовый выпуск однокристальных микропроцессорных наборов БИС с их широкими функциональными возможностями, их низкая стоимость, гибкость и точность цифровых методов обработки информации превратили МП в системные элементы, на основе которых создаются системы промышленной автоматики, связи, измерительной техники и т.д.

Можно сказать, что назначение системы, это обеспечение безопасности. Под безопасностью СЗКДП будем понимать ее свойство, выражающееся в попытках нанесения ущерба владельцам и пользователям системы при различных возмущающих (умышленных и неумышленных) воздействиях на нее. Обеспечение безопасности СЗКДП в целом предполагает создание препятствий для любого несанкционированного вмешательства в процесс ее функционирования, а также попыток хищения, модификации, выведения из строя или разрушения ее компонентов, то есть защиту всех компонентов системы: оборудования, программного обеспечения, данных и персонала.

По мере развития и расширения применения средств вычислительной техники острота проблемы обеспечения безопасности систем и хранящейся в них информации от различных угроз все возрастает.Основная из них — возросший уровень доверия к автоматизированным системам обработки данных. То есть система помимо выполнения функции защиты и контроля должна быть сама защищена, как на нижнем уровне, так и на верхнем. Доступ к ресурсам системы, а особенно к ПЭВМ должен быть максимально ограничен и надежно защищен. Вероятность подбора индивидуального кода должна быть не менее 10-6. Как показывает мировой опыт при такой вероятности подбора, система, в плане подбора идентификационного номера пользователя, практически надежна. Такую вероятность может обеспечить электронный идентификатор.

Требования к электропитанию.

Первичным источником электропитания пульта управления и контролируемого пункта должна быть однофазная сеть переменного тока напряжением 220 вольт и частотой 50 герц. При кратковременных авариях в системе энергоснабжения должен быть обеспечен перезапуск и восстановление предаварийного состояния пульта управления и контролируемого пункта.

Требования к системе персонального вызова. Так как СЗКДП предусматривает персональный вызов (ситуация — к пользователю пришел гость который не идентифицируется системой), то система должна обеспечить надежную радиосвязь и работоспособность между передатчиком на входе КПП и пейджерами установленными в удаленных помещениях. Максимальное удаление охраняемых помещений где установлены пейджеры от передатчика должно быть не менее 200 метров.

Требования к защите от влияний от внешних воздействий.

Электрическая составляющая электромагнитного поля помех в помещениях не должна превышать 0.3В на 1 метр согласно ГОСТ 16325-88.

Должна быть предусмотрена автономная шина заземления технических средств для подключения корпусов устройств, экранов, кабелей. Контур заземления должен быть автономным, то есть несвязанным гальванически с контуром заземления каких-либо промышленных помещений. Сопротивление заземляющего устройства между клеммой земли контроллируемого пункта, пульта управления и землей (грунтом) не должно превышать 4-ех ом в любое время года.

В линиях связи должны использоваться приемники с высоким входным сопротивлением, малой входной емкостью и предпочтительно с гистерезисной передаточной характеристикой для увеличения помехозащищенности. Шины питания и земли должны обладать минимальной индуктивностью. Кроме того линия связи должна быть защищена от паразитных импульсных токов в оплетке кабеля из-за связи с источником помех через паразитную емкость между источником помех и оплеткой.

В проектируемой системе компьютер должен взаимодействовать с внешними устройствами (контроллерами). Для этой цели в мировой практике [ ] используется несколько стандартов и множество устройств, которые работают со стандартными интерфейсными схемами. Один из наиболее распространенных интерфейсных стандартов называется RS-232C (Reference Standart N232 Revision C), сигналы которого приведены в приложении. Благодаря очень небольшому расстоянию (несколько сантиметров) между различными узлами внутри контроллера шлюза уровни сигналов, используемых для предоставления двоичных данных, зачастую весьма малы. Например, распространенным логическим семейством, используемым в контроллере шлюза, является транзисторно-транзисторная логика (ТТЛ), в которой для представления двоичной единицы используется сигнал напряжением от 2 до 5 В, а для представления двоичного нуля — сигнал напряжением от 0,2 до 0,8 В. Напряжения вне этих диапазонов порождают неопределенное состояние: в худшем случае, если уровень напряжения близок к одному из этих пределов, то воздействие даже небольшого понижения сигнала или небольшой электрической помехи может привести к ошибке. Поэтому при подключении контроллеров к компьютеру уровни напряжений обычно выше тех, которые используются для соединения отдельных элементов внутри некоторого узла. На практике фактически [ ] используемые уровни зависят от источников напряжений, подаваемых на схемы интерфейса; в проектируемой системе предполагается использовать напряжения +12 В. Схемы передачи преобразуют низкие уровни сигналов в более высокие, тем самым обеспечивая связь по моноканалу между компьютером и контроллерами шлюзов. Приемные схемы выполняют обратную функцию. Схемы согласования интерфейса также выполняют необходимые преобразования напряжений.

Относительно высокие уровни напряжений в интерфейсе значительно уменьшают влияние электрических помех по сравнению с их воздействием на уровни ТТЛ.

Предполагается использовать стандартную скорость передачи в стандарте RS-232C равную 9600 бит/сек.

3. Разработка архитектуры системы

Обеспечение безопасности и сохранность информации в СЗКДП обеспечивается прежде всего выполнением общих процедур защиты, которые являются составной частью большинства защитных мероприятий. Прежде, чем раскрыть архитектуру системы, отобразим общие процедуры безопасности (см. рис.3.1 ) для лучшего понимания проектируемой СЗКДП.

ОБЩИЕ ПРОЦЕДУРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

 Управление доступом Контроль угроз Управление надежностью

 Идентификация Прекращение Контроль

 работы работы аппаратуры

 Установление

 подлиности Протоколирование Контроль за

 попыток работой персонала

 Регистрация проникновения

сообщений

 Преобразования информации

 и передача информации

Рис.3.1

В дальнейшем при описании архитектуры системы и ее структурной схемы будем исходить из показанной выше блок-схемы "Общей процедуры безопасности". Но в начале опишем основные блоки, устройства, узлы и элементы входящие в СЗКДП (см. чертеж “Структурная схема”)

Идентификаторы. В качестве основного средства распознавания пользователей служат электронные идентификаторы Touch Memory подгруппы DS1990A. В частном случае идентификатор имеет вид таблетки, размером с небольшую монету, хотя могут быть и другие варианты. В корпус "таблетки" встроена литиевая батарейка, срок службы которой не менее 10-ти лет и имеет встроенный микропроцессор с ПЗУ. В ПЗУ содержится резидентная программа обслуживающая идентификатор и кроме того там хранится неповторимый идентификационный номер объемом 64 бита. Выход ключа электрически совместим со схемами ТТЛ. Идентификатор имеет два контакта, через которые считывается 64-ый битный код. Или как его еще называют — идентификационный номер, который раз и навсегда заносится фирмой-производителем. Благодаря гарантированной производителем неповторяемости ключа (число уникальных 64-ех битовых комбинаций составляет более 280 триллионов) обеспечивается высокий уровень защиты. Коснувшись идентификатором считывателя, информация с него (т. е. его 64-битный код) считывается за микросекунды. Это делает его весьма удобным в обpащении, а его малые pазмеpы позволяют его использовать даже как бpелок. Код каждого идентификатора заносится в базу данных компьютера. Описание и назначение узлов (блоков) контроллера шлюза (см.чертеж “Структурная схема”):

1)Микроконтроллер (МК). Микроконтроллер предназначен для контроля и управления шлюзом. МК путем периодического опроса осведомительных слов генерирует в соответствии с алгоритмом управления последовательности управляющих слов []. Осведомительные слова это сигналы состояния шлюза, сформированные датчиками объекта управления. Выходные сигналы датчиков вследствие их различной физической природы могут потребовать промежуточного преобразования на аналого-цифровых преобразователях или на схемах формирователей сигналов, которые выполняют функции гальванической развязки и формирования уровней двоичных сигналов стандарта ТТЛ.

Микроконтроллер с требуемой периодичностью (см. раздел “Разработка алгоритма управляющей программы”) обновляет управляющие слова на своих выходных портах. Некоторая часть управляющего слова интерпретируется как совокупность прямых двоичных сигналов управления, которые через схемы формирователей сигналов (усилители мощности, реле, оптроны и т. п.) поступают на исполнительные механизмы и устройства индикации. МК постоянно снимает информацию с датчиков контроля дверей и датчика массы; выдает управляющие сигналы на схему управления, на индикаторы и на звуковой сигнализатор; управляет считывателем кода при считывании идентификационного номера с электронного идентификатора; обменивается информацией с компьютером.

2)Считыватель кода. Считыватель кода представляет из себя схему для считывания 64-ех битного кода с идентификатора и дальнейшей передачи этого кода микроконтроллеру. Его назначение состоит в том, чтобы согласовывать выходные импедансы и уровни напряжений между контроллером и идентификатором. Кроме того, считыватель защищает микроконтроллер от возможных коротких замыканий на входе считывателя. Конструктивно считыватель выполнен в виде корпуса с двумя выходными контактами к которым прикасается пользователь персональным идентификатором при доступе на объект защиты.

3)Схема управления. Схема предназначена для автоматического управления открытия и закрытия сдвижных дверей для входа на объект защиты. Выход схемы подключается к электрозащелке и к электромотору блокировки дверей, которые непосредственно управляют открыванием и закрыванием сдвижных дверей объекта защиты. При опознавании системой пользователя, схема управления включает электромотор на открывание дверей для входа пользователя в шлюз. Двери автоматически закрываются после выхода пользователя из шлюза, при условии что аутентификация прошла удачно. Если система не опознала пользователя или пользователь не аутентифицирован, двери шлюза остаются в блокирующем положении (то есть в закрытом).

4)Датчики контроля дверей. Они предназначены для контроля положения дверей. Датчики всегда находятся в двух положениях — включено или выключено. Конструктивно они могут быть выполнены в двух видах, это кнопка с самовозвратом или герконовый датчик, в зависимости от конструкции дверей. Датчики крепятся непосредственно на дверях или возле них и в зависимости от положения дверей находятся во включенном или выключенном состоянии. На одни сдвижные двери предусматривается по четыре датчика. Контроллер периодически опрашивает датчики и в зависимости от их положения переходит на соответствующую подпрограмму обслуживания, с тем чтобы принять решение открывания (закрывания) дверей.

5)Индикаторы. Индикаторы служат для сигнализации пользователю о приглашении или запрещении входа (выхода) на объект защиты. Они устанавливаются рядом со считывателем кода и сигнализируют пользователю: когда можно вставить идентификатор в считыватель кода; когда можно идти; когда вход запрещен. Конструктивно индикаторы представлены в виде обычных светодиодов, которые подсвечивают соответствующие надписи или знаки. Во включенном состоянии один из двух индикаторов будет сигнализировать:

красный светодиод — вход запрещен;

зеленый светодиод — можно идти.

Третье состояние, когда оба светодиода выключено, означает ждущий режим, то есть пользователь может прикоснутся идентификатором к считывателю кода.

6)Датчик массы. Служит для проверки подлинности пользователя, то есть его аутентификации. Конструктивно он представляет из себя электронные весы, для измерения массы человека. Аналоговый сигнал снимаемый с датчика обрабатывается аналого-цифровым преобразователем в цифровой код. Полученный код, содержащий информацию о весе пользователя передается на контроллер для последующей его обработки и передаче его на пульт управления. Вес каждого пользователя занесен в базу данных, в таблицу авторизации компьютера (пульта управления).

7)Звуковой сигнализатор. Его назначение следующее. Если пользователь не идентифицирован системой или он не прошел проверку на подлинность, или обнаружена попытка саботажа системы включается звуковая сигнализация. Сигнализатор устанавливается внутри шлюза или непосредственно рядом с ним.

8)Схема связи с пультом управления. Схема предназначена для связи микроконтроллера с пультом управления. Она устанавливает нужный размах сигнала при передачи его в линию связи и выделяет сигналы из линии связи когда микроконтроллер находится в режиме приема информации от компьютера. То есть схема связи выполняет необходимые преобразования напряжений и кроме того выполняет согласование интерфейса с линией связи.

Как уже упоминалось в технических требованиях, СЗКДП представляет из себя централизованную систему, работающую в реальном времени. На верхнем уровне — пульт управления; на нижнем — контролируемые пункты. Упомянутые выше узлы и элементы входят в контролируемый пункт, т. е. они находятся на нижнем уpовне системы. Число контpолиpуемых пунктов зависит от количества входов подлежащих контролю на охpаняемом объекте.

На веpхнем уpовне находится пульт упpавления выполненный на базе ПЭВМ, совместимой с IBM PC. Пульт управления и контролируемые пункты соеденены между собой в локальную сеть. На рис.3.2 изображена блок-схема локальной сети.

Рис.3.2

Локальная сеть содержит пульт управления (ПУ) выполненный на базе ПЭВМ и ряд удаленных контроллеров (кшn), каждый из которых соединен с одним шлюзом(Шn).

Передача информации между пультом управления и удаленным контроллером шлюза требует представления ее в виде последовательного потока бит, характеристики которого зависят от особенностей конкретной системы. Определим эти особенности локальной сети.

Прежде всего локальная сеть определяется топологией связей и режимом обмена по линиям связи. В проектируемой системе выбран магистральный тип интерфейса, с "шинной" топологией системы обмена. Режим обмена информацией — полудуплексный. В полудуплексном режиме любой из контроллеров может начать передачу, если на вход его последовательного интерфейса поступил запрос с пульта управления, то есть его сетевой адрес. Можно сказать, что по управлению передачи информации в каналах, локальная сеть является централизованной. Компьютер в протокольном режиме “широковещательной” передачи (всем ведомым контроллерам) выдает в моноканал байт-идентификатор абонента (код адреса контроллера-получателя), который отличается от байтов данных только тем, что в его девятом бите содержится **1**. После того как компьютер выставил адрес, он в течение 2 милисекунд ожидает ответа от контроллера. Если ответ в течении этого времени не получен, компьютер выставляет в моноканал следующий адрес.Для уменьшения вероятности наложений контроллер перед выдачей сообщения прослушивает канал и начинают выдачу только при поступлении запроса от компьютера на его адрес. По режиму организации передачи, данная СЗКДП относится к сети с асинхронной передачей (момент считывания данных приемником определяется по сигналам оповещения или запуска от передатчика; по окончании пересылки приемник выдает передатчику сигнал об окончании цикла передачи). По способу представления сигналов выбран униполярный код.

В качестве физической среды распространения сигналов каналов межмодульного обмена используется витая пара, заключенная в оплетку. Применение витой пары повышает помехоустойчивость. Всякое внешнее воздействие влияет на оба провода, и поэтому искажение разности сигналов снижается. Более того, так как витая пара заключена в оплетку, то это еще более ослабляет воздействие, вызванное взаимными наводками.

Центральный пульт управления выполнен на базе IBM PC совместимого компьютера со следующей конфигурацией:

640 Кбайт ОЗУ.

EGA монитор.

20 МБ винчестер.

MS-DOS версия не ниже 3.30

2 последовательных порта.

Для связи компьютера с контроллерами используется стандартный интерфейс RS-232C (см. приложение). Основным преимуществом последовательной передачи является возможность пересылки данных на большие расстояния, как правило около 30 метров. Ипользуя дополнительный блок приема-передачи это расстояние можно увеличить до 200 метров. В этот блок входит такая же схема, которая рассчитана для контроллера шлюза (имеется в виду схема связи с ПУ). Данные передаются и принимаются с использованием аппаратного последовательного интерфейса, который работает в режиме прерывания. Система работает в фоновом режиме.

Так как передаваемые данные в контроллерах генерируются в случайные моменты времени, то предполагается использовать асинхронный режим обмена данных между пультом управления и контроллерами. Из-за отсутствия синхронизации, показывающей начало и конец каждого байта, байт данных приходится обрамлять стоповыми и стартовыми битами, чтобы приемные устройства могли распознать начало и конец передачи байта данных (см. чертеж “Форматы данных”). Как видно стартовый и стоп-биты имеют различные полярности. Это обеспечивает наличие, как минимум, одного перехода (1—0—1) между каждыми двумя последовательными символами, причем независимо от последовательности битов в передаваемых символах. Поэтому первый после периода бездействия переход 1—0 используется получающим устройством для определения начала каждого нового символа. Каждый символ состоит из 8-ми бит данных, стартового и стопового битов и бита паритета. В проектируемой системе бит паритета используется для идентификации символа как символа-идентификатора адреса контроллера шлюза. При передаче данных бит паритета принимает значение логического нуля. Система работает в полудуплексном режиме и инициатором связи всегда является пульт управления (то есть компьютер). Выставив адрес в моноканал компьютер, переходит в режим ожидания. Если в течение двух милисекунд (см. расчет ниже) компьютер не получает подтверждение запроса, он выставляет новый адрес в моноканал. Если же получено подтверждение запроса, компьютер переходит в режим приема данных от микроконтроллера. Данные могут содержать информацию:

код идентификатора (8 символов или 88 бит);

код физической массы пользователя, то есть код аутентификации(1 сим вол или 11 бит);

код содержащий информацию о саботаже системы (1 символ или 11 бит)

После получения данных и соответствующей обработки компьютер сообщает микроконтроллеру о том прошел или не прошел пользователь идентификацию и аутентификацию (2 символа или 22 бита).

Предполагается использовать стандартные скорости обмена данных по моноканалу, которые поддерживаются интерфейсом RS-232. Произведем расчет для скорости приема-передачи равной 9600 бит/с.

Один бит передается за время:

1/9600=0,104 мсек.

Тогда скорость передачи слова или 11 бит равна:

0,104\*11=1,145 мсек.

Рассчитаем максимальное время обмена информацией между пультом управления и адресуемым микроконтроллером. Для этого подсчитаем максимальное количество битов в формате обмена. Оно будет максимальным при передаче в сообщении идентификационного номера и кода аутентификации. Туда войдут:

адрес контроллера (1 слово)=1,145 мсек;

подтверждение запроса контроллером (1 слово)=1,145 мсек;

подтверждение ответа компьютером (1слово)=1,145мсек;

передача данных — код идентификации (8 слов), подтверждение идентификации (1 слово)=8+1=9 слов. Тогда

9\*1,145=10,305 мсек;

конец связи (1 слово)=1,145 мсек.

Кроме того в формат сообщения войдет время задержки, которое максимально равно 2 мсек. Время 2 мсек выбрано из следующих соображений. Так как время передачи одного слова по моноканалу составляет 1,145 мсек, то 2 мсек будет вполне достаточно для обнаружения компьютером сигнала от контроллера (имеется в виду подтверждение запроса контроллером). Следовательно, общее максимальное время связи между компьютером и микроконтроллером будет равно:

1,145+1,145+1,145+10,305+1,145+2= 14,885 мсек.

Сюда не вошло время обработки данных компьютером и микроконтроллером которое составляет единицы микросекунд.

Исходя из того, что количество обслуживаемых помещений или количество обслуживаемых шлюзов входящих в одну локальную должно быть не менее 200, определим максимальное время обслуживания всех контроллеров: 14,885\*200=2,997 сек.

В следствии того что, СЗКДП представляет из себя средство управления доступом, коды идентификации пользователя и другая информация обеспечения безопасности должны хранится в таблице авторизации. Таблица авторизации находится в защищенной зоне основной памяти компьютера или хранится как файл данных на дополнительном устройстве. Каждый авторизованный пользователь имеет свою запись в таблице авторизации.

Код идентификации пользователя представляет индекс в таблице авторизации. Если кода идентификации пользователя нет в таблице авторизации, то доступ запрещается.

Кроме того, пульт управления автоматически тестирует состояние системы и ведет протокол функционирования всего комплекса защиты. Автоматически ведет жуpнал:

проходов пользователей с указанием даты, времени и направления прохода;

несанкционированных действий пользователей с указанием даты и времени нарушений;

работы операторов и администраторов системы.

Доступ к ПУ возможен только при помощи электронного идентификатора принадлежащего администратору безопасности. Администратор безопасности с помощи мастер-карты регистрирует и удаляет коды пользователей и проводит операции по изменению прав пользователей. Теперь покажем, что из себя представляет контролируемый пункт (КП) объекта защиты. Конструктивно КП представляет из себя шлюзовую систему, с двумя сдвижными дверями (см. рис.3.3 )

**Открытое положение двери**

**Закрытое положение двери**

Рис.3.3 Шлюз(вид сверху)

Шлюз имеет следующие размеры (эти размеры выбраны произвольно, но я считаю их оптимальными):длинна=1,5 м; ширина=1 м; высота=2 м. Каждой сдвижной дверью управляет электромотор блокировки дверей. При подаче управляющего напряжения от устройства управления на электромотор двери соответственно открываются или закрываются. В закрытом положении двери блокированы.

Внутри шлюза устанавливаются три датчика массы, которые покрывают всю нижнюю площадь шлюза (см. рис.3.5). В системе применены именно три датчика массы для установления подлинности пользователя.

**Три**

**датчика масс**

Рис.3.5 Шлюз с датчиками массы (вид сверху)

Кроме того на каждую сдвижную дверь закрепляются 4 датчика контроля открывания и закрывания дверей (см. рис.3.6). Датчики должны быть установлены внутpи шлюза таким обpазом, чтобы исключить всякую возможность доступа к ним лиц не имеющих права обслуживать систему. В случае саботажа pаботы шлюза, датчики устанавливаются в соответствующее положение. Контроллер обрабатывает информацию снимаемую с датчиков и на пульт управления идет соответствующий сигнал тpевоги.

|  |  |
| --- | --- |
|  | положение дверей |
|  | закрыто |  нейтрально |  открыто |
| д1.1 | 1 | 0 | 1 |
| д1.2 | 1 | 0 | 0 |
| д1.3 | 1 | 0 | 0 |
| д1.4 | 1 | 0 | 1 |

Устройство управления

Электро­мотор

**датчики**

Устройство управления

Электро­мотор

 д1.4 д1.3 д1.2 д1.1

 д1.4 д1.3 д1.2 д1.1

Рис.3.6 Шлюз с датчиками контроля положения дверей

При анализе структурной схемы (см. рис.3.7) будем исходить из общих процедур обеспечения безопасности (структура процедур отражена в начале раздела "Архитектура системы"). То есть описание структурной схемы будет происходить в соответствии со структурой общих процедур безопасности, сверху-вниз.

где Ш — шлюз;

ШЛЮЗ

 ск

 ск

  **И**

 **И**

 **эл / мот.**

 **эл / мот.**

 **УУ**

 **УУ**

МК

ПУ

 **АС**

 радиомодем

 от МК

 к МК

 ЭИ

от МК

от МК

сигналы с датчиков

контроля положения

дверей (д.1.1, д1.2,

д1.3, д1.4, д2.1, д2.2,

д2.3, д2.4) к МК

от МК

к МК

 ЭИ

 мастер-карта

контроллируемый

пункт 1

к другим КП

Рис.3.7

 сигнал с датчика

 массы к АЦП

 **зс**

**АЦП**

АС— адаптер сети;

И — индикаторы;

эл/мот — электромотор блокировки дверей;

УУ — устройство управления электромотором;

ЭИ — электронный идентификатор;

МК — микроконтроллер;

СК — считыватель кода;

КП — контролируемый пункт;

ПУ — пульт управления (компьютер);

ЗС — звуковой сигнализатор;

АЦП — аналого-цифровой преобразователь.

1.1)Управление доступом. Идентификация.

Идентификация пользователя системой защиты происходит следующим образом. Пользователь прикасается личным идентификатором адаптера; микроконтроллер прерывает рабочую программу и считывает с идентификатора 64-ех битный код. Далее код передается на ПУ, где происходит сравнение кода с кодами хранящимися в таблице авторизации. В случае совпадения идет ответный сигнал на микроконтроллер приказывающий открыть 1-ые двери шлюза. МК "зажигает" зеленый индикатор и подает сигнал на устройство управления. УУ включает электромотор и открывает 1-ые двери приглашая тем самым пользователя войти. Пользователь входит в шлюз двери за ним закрываются и зеленый индикатор гаснет. Зажигается красный индикатор с обеих стоpон шлюза, тем самым запpещая вход и выход остальным пользователям, котоpые могут находится в этот момент с двух стоpон шлюза.

1.2) Упpавление доступом. Установление подлинности.

В шлюзе происходит установление подлинности пользователя, то есть его аутентификация. Подлинность определяется массой пользователя. Код соответствующий массе пользователя также как и код идентификатора хранится в памяти компьютера в таблице авторизации.

В шлюзе установлено три датчика массы. Пользователь становится на центральный датчик. Закодированный сигнал содержащий информацию о массе пользователя снимается микроконтроллером и передается на пульт управления, где он сверяется с кодом хранящимся в таблице авторизации. В случае совпадения кодов или есть небольшая погрешность не более 20 кг. (человек вошел с сумкой), МК подает сигнал на 2-ое УУ, которое включает электромотор. Вторые двери шлюза открываются и пользователю предлагается выйти. Пользователь выходит, 2-ая дверь закрывается и одновременно гаснут красные индикаторы. Система переходит в режим ожидания.

В шлюзе устанавливается три датчика массы: во первых для улучшения точностных характеристик датчика, во вторых для того чтобы гарантировать присутствие в шлюзе только одного человека. Если за пользователем в шлюз зайдет еще один человек, сработает один из дополнительных датчиков или информационный код с центрального датчика не совпадет с кодом из таблицы авторизации (если человек стал вместе с пользователем на центральный датчик). В обоих случаях с микроконтроллера идет сигнал тревоги на звуковой сигнализатор, а 1-ая дверь остается открытой и нарушителю предлагается выйти.

1.3)Управление доступом. Регистрация сообщений.

Когда пользователь проходит через шлюз, то на ПУ регистрируются: время, дата и направление прохода пользователя. Вся эта информация записывается и хранится в базе данных компьютера.

2.1)Контроль угроз. Прекращение работы.

В СЗКДП предусмотрен аварийный режим работы. В случае пожара, срабатывает пожарный датчик с которого поступает сигнал на МК. Микроконтроллер подает сигнал на оба устройства управления, которые включают электромоторы и все двери шлюза открываются. Одновременно сигнал тревоги поступает на ПУ. При создании на СЗКДП какой-либо экстремальной ситуации, оператор ПУ по своей инициативе может открыть шлюз. Кроме того предусматривается автономный режим работы контроллеров в следующих ситуациях: перерезан кабель локальной сети или нет ответа от компьютера; отключено электропитание. В обоих ситуациях двери шлюза блокируются и микроконтроллер переходит в режим ожидания до тех пор, пока не будет получен ответ от компьютера или восстановлено электропитание.

2.2)Контроль угроз. Протоколирование попыток проникновения.

СЗКДП работает таким образом, что при нарушении графика рабо-ты системы, происходит активизация процедур обнаружения. То есть при попытке открыть вручную двери или саботировать работу датчиков на микроконтроллере запускаются подпрограммы обнаружения, которые определяют класс нарушения и сообщают об этом на ПУ. Все попытки проникновения контролируются МК. Если все же нарушитель проник в шлюз, все двери системы блокируются, до прихода службы безопасности или администратора.

Любая попытка несанкционированого доступа на объект защиты через СЗКДП фиксируется на ПУ. В память компьютера записывается и заносится в архив базы данных: время, число и вид нарушения регламента работы системы. Если нарушение произошло по вине авторизованного пользователя, то информация о нарушении регистрируется на имя пользователя.

3)Преобразование и передача информации.

3.1.)Преобразование и передача информации электронного идентификатора.

Считывание информации с электронного идентификатора происходит следующим образом. После прикосновения идентификатором к считывателю, идентификатор формирует стартовый бит (логический ноль) длительностью не более 240 мксек, а микроконтроллер отвечает импульсом сброса длительностью не менее 480 мксек (см. рис.3.8 и чертеж “Форматы команд”).

 trsth

 Vpullup

 0 V

 trstl

 tpdl

 480мксек < trstl <

 480мксек < trsth <

 60мксек < tpdl < 240мксек

резистор

микроконтроллер

идентификатор

Рис.3.8 Сброс и старт-бит.

В следствии чего в микроконтроллере происходит прерывание рабочей программы и переход на подпрограмму обслуживания идентификатора. Далее инициатором считывания каждого бита информации, является микроконтроллер. То есть: контроллер каждые мсек сбрасывает напряжение в логический ноль и переходит в режим ожидания ( мсек), в течение которого идентификатор формирует бит данных. Запись логического нуля и единицы показана на рис. Если идентификатор передает “0” , то он держит напряжение логического нуля в течении ожидания; если передает “1”, то он “отпускает” напряжение до прихода нового запроса от микроконтроллера. Общее время считывания составит:

После того, как код ключа считан в резидентную память данных микроконтроллера, он (контроллер) переходит в режим ожидания запроса от компьютера.

Vpullup

0 V

trdv

резистор

микроконтроллер

идентификатор

trelease

tslot

 trec

tlowr

60мксек< tslot <120мксек

1мксек< tlowr <15мксек

0< trelease <45мксек

1мксек< trec <

trdv=15мксек

Рис.3.9 Чтение данных из идентификатора.

Произведем расчет времени считывания идентификационного кода микроконтроллером с электронного ключа.

Как видно из рисунков максимальное время записи и чтения одного бита равно 120мксек. Тогда зная общее количество бит (64 бита ПЗУ и 8 командных бит контроллера) общее время обмена информацией равно:

(64+8)\*120=8,64 мсек.

3.2)Передача информации на компьютер.

Информация на пульт управления передается в униполярном коде. Система обеспечивает двусторонний обмен данными между компьютером и выбранным контроллером. Выбор абонента производится посылкой из компьютера в магистраль адресного кода, который распознается этим абонентом. После передачи адресного кода производится обмен данными между компьютером и контроллером (см. стр. ). Скорость передачи данных в стандарте RS-232C составляет 9600 бит/сек. Такая скорость является наиболее приемлемой, так как увеличение скорости до 19200 бит/сек может привести к потере информации в микроконтроллере, так как при такой скорости возрастает погрешность до 49% [ ].

В качестве кабеля предлагается использовать экранированную витую пару по следующим соображениям: сравнительно маленькая скорость передачи данных, значительно лучшая защита от емкостных наводок. Кроме того витая пара обеспечивает защиту от низкочастотных магнитных полей. В этом случае ЭДС, наводимые внешним магнитным полем на составляющих витую пару проводах, полностью компенсируют друг друга как по знаку, так и по абсолютной величине.

В проектируемой системе предусматривается ситуация: к пользователю пришел гость у которого нет санкционированного доступа в систему. Для этого случая предусмотрена пейджинговая связь между ПУ и пользователем. На объекте защиты, в помещении у каждого авторизованного пользователя есть свой пейджер или один пейджер на несколько пользователей, но разными мелодиями вызова. Гость приходит на ПУ, где оператор по просьбе гостя на компьютере проверяет присутствие пользователя на объекте. Если пользователь присутствует, оператор с компьютера запускает передатчик и сообщение отправляется в эфир. Пользователь принимает сообщение на свой пейджер, в виде тонального вызова.

В качестве передатчика предполагается использовать готовый радиомодуль TXM433F работающий в новом европейском стандарте телекоммуникаций I-ETS 300 220 (см. приложение ). Он предназначен для передачи цифровой информации и представляет собой готовое изделие. Радиомодем подключается к последовательному порту компьютера и передает информацию в эфир в стандарте RS-232C со скоростью 4800 бит/сек. В передатчике используется ЧМ несущей частоты 433,9 Мгц. Генератор несущей стабилизирован фильтром на ПАВ. Этот радиомодем обладает размерами со спичечную коробку и излучает мощность не более 10 мВт (см. рис.3.10 )

 полосовой

 фильтр

 433,9МГц

 генератор

с фильтром

 на ПАВ

 ЧМ

модулятор

 ФНЧ

 RF OUT

 GND

 Vcc 3\_4V

 DATA

0 VOLT

Рис.3.10

Формат передаваемых данных такой же, как при передаче по моноканалу. Каждое передаваемое слово в себя включает старт-бит, 8 бит данных,

бит паритета, стоп-бит (см. рис.3.11)

 старт

бит

 D7

 D6

 D5

 D4

 D3

 D2

 D1

 D0

 бит

 паритет

 стоп

 бит

Рис.3.11

В начале каждой передачи 1-ое передаваемое слово будет содержать сплошные единицы, за исключением стартового бита. Это делается для того, чтобы приемник-радиомодем мог надежно фиксировать прием несущей. Второе и третье слова содержат адрес пейджера. Итого в проектируемой системе можно адресовать 216=65536 пейджеров. В целях экономии денежных затрат можно предложить другой вариант. Во втором слове и первых четырех битах третьего слова передается адрес пейджера. В оставшихся четырех битах передавать код определенной мелодии. Каждая мелодия “принадлежит” конкретному пользователю. То есть если в одном помещении часто находятся одни и те же люди (оптимально 5 человек), то за каждым из них “закрепляется” определенная мелодия вызова. В этом случае можно адресоваться к 212=4096 пейджерам и на каждом из них вызвать 16 мелодий. Итого: формат передаваемых данных содержит три слова или 33 бита; скорость передачи данных 4800 бит/сек; используется прямая ЧМ несущей частоты 433,9 Мгц; выходная мощность не более 10 мВт (расчет см. ниже).

Пейджер представляет из себя устройство состоящее из радиомодема,

контроллера адреса и вызова, динамика со схемой согласования (рис.3.12)

 контроллер

 адреса и

 вызова

 радиомодем

 схема

согласования

Рис.3.12

Приемник-радиомодем представляет собой готовое изделие SILRX433A и предназначено для приема цифровой информации и работает в стандарте I-ETS 300 220. Радиомодем построен по типичной для всех модулей супергетеродинной схеме с двойным преобразованием частоты, что позволяет достигать чувствительности в 0,5 мкВ при отношении с/ш 20дБ (см. рис. ). Скважность включения (отношение выкл/вкл) может достигать 100. Радиомодем-приемник SILRX433A работает в паре с радиомодемом-передатчиком TXM433F на частоте 433,92 Мгц. Скорость приема данных в соответствии со скоростью передачи составляет 4800 бит/сек.

полосовой

фильтр

433,9 МГц

 УВЧ

 2 смеситель

 УПЧ,

ЧМ демод.

 ФНЧ 3-го

 порядка

(0\_5кГц)

 УНЧ

 1 гетеродин

с фильтром

на ПАВ

 2 гетеродин

15,9 МГц

 +

 -

 GND

0 VOLT

DATA

 AF

DETECT

Vcc 4\_9V

 REIN

формирователь

 1 смесит.

Рис.3.13

|  |
| --- |
| Краткие характеристики радиомодемов |
|  |  | Uпит,В | Iпотр,мА | Скоростьпередачи | Типоваядальность,м | Размеры,мм |
| TXM433F | передатчик |  3\_4 |  10 | 10000 |  200 | 30х20х6 |
| SILRX433A | приемник |  4\_9 |  14 | 5000 |  200 | 48х28х6 |

Функции контроллера адреса и вызова выполняет микроконтроллер AT89C51-20PI серии 80С51 (такой микроконтроллер предполагается использовать в контроллере шлюза). Каждый микроконтроллер имеет свой адрес, который зашит в резидентной памяти программ. Радиомодем обнаружив несущую, выделяет информацию из несущей и передает ее на микроконтроллер. Микроконтроллер “сверяет” полученный адрес со своим адресом и в случае совпадения переходит на подпрограмму вызова адресата.

4.1)Управление надежностью. Контpоль pаботы аппаpатуpы.

Работа системы защиты и контpоля доступа в помещения постpоена таким обpазом, что каждый микpоконтpоллеp полностью обслуживает свой контpоллиpуемый пункт. Постоянно ведется опpос всех датчиков, индикатоpов, переключателей не только с целью обнаружения и контроля доступа на объект, но и с целью обнаружения сбоя или какой-либо поломки в системе. И в случае сбоя в системе микроконтроллер посылает сообщение на ПУ: где, в каком месте и какого вида произошла поломка или сбой в системе. Эта информация фиксируется и идет в архив памяти компьютера.

4.2)Управление надежностью. Контроль за работой персонала.

Одной из важнейших функций СЗКДП является функция контроля. То есть контролируется не только регламент работы аппаратуры, но и работа обслуживающего персонала. В этот контроль входят ( с архивированием в памяти компьютера): время и дата просмотра оператором базы данных; вpемя и дата входа в ПО, таблицы аpхивов(пpи наличии соответствующих полномочий, т. е. идентификатоpа или мастеp-каpты); время и дата внесений изменений в систему. В проектируемой системе предусматривается, что доступ к компьютеру возможен только при наличии мастер-карты. Мастер-карта представляет из себя электронный идентификатор применяемый в качестве идентификации пользователя, с тем отличием в том, что мастер-карта имеет более высокий приоритет, чем обычный идентификатор. Идентификатор и мастер-карта могут иметь одинаковое корпусное исполнение. То есть доступ к базам данных возможен только при наличии мастер-карты.

Произведем системный расчет.

В начале произведем стойкость шифра электронного идентификатора. Стойкость шифра определяется по формуле:

W=V\*T/2

где

W — время стойкости шифра

V — количество комбинаций, чтобы раскрыть код

Т — время одной операции или время набора одного кода

Шифр считается стойким если W>10 лет.

Пусть время одной операции будет равно максимальному времени передачи кода от идентификатора к микроконтроллеру, то есть 8,64 мсек. Количество комбинаций определим как 264=1,84\*1019. Тогда

W=1,84\*1019\*0,00864/2=7,9\*1016 лет.

Следовательно можно с уверенностью сказать, что шифр является вполне стойким.

Теперь определим вероятность подбора кода, при заданной 10-6. Вероятность подбора вычисляется по формуле

P=1/(n+1-i)

где

Р — вероятность подбора

n — количество комбинаций ( 264=1,84\*1019)

i — число попыток раскрытия кода

Предполагается, что число пользователей обслуживаемых системой будет в среднем около 1000 человек. Но возьмем предполагаемый максимум 10000 пользователей (хотя может быть и больше). Тогда количество комбинаций соответственно уменьшается в 10000 раз. То есть n равно

n/10000=1,84\*1015

Число попыток (i) будет равно 1. Так как после того как система считает идентификационный код и проверит его по базе данных и не найдет кода в таблице авторизации, сработает сигнализация. Тогда

Р=1/(1,84\*1015+1-1)=5,42\*10-16

Следовательно в плане подбора кода проектируемая система достаточно устойчива.

Рассчитаем дальность радиосвязи при известной чувствительности радиомодема-приемника и максимальной мощности радиомодема-передатчика по следующей формуле [ ].

 Pu\*Gu\*Gпрм\*l2

R= P0\*(4П)2

где R — дальность непосредственной радиосвязи;

Pu — мощность излучения радиомодема;

Gu — КНД излучающей антенны. Предполагается использовать штырьевую антенну с КНД=0,5;

Gпрм — КНД приемной антенны;

l — длинна волны несущей;

P0 — мощность сигнала на входе радиомодема-приемника.

Тогда

 0,01\*0,5\*0,5\*0,692

R= = 1565 м

 2,5-13\*42\*3,142

При условии, что система будет эксплуатироваться в зданиях, что внесет затухание сигнала, радиосявзь будет надежной в радиусе 500 метров. Это вполне достаточно для проектируемой системы.

4.Разработка принципиальной схемы

При проектировании системы защиты и контроля доступа в помещения разрабатывалась принципиальная схема контроллера шлюза (см. чертеж “Принципиальная схема”). Она построена в соответствии со структурной схемой. Дальнейшее описание будет происходить с сылками на структурную схему.

Микроконтpоллеp. В качестве контpоллеpа выбpан однокpистальный микpопpоцессоp AT89C51-20PI серии 80С51 (наш аналог КМ1816ВЕ51). Этот микpоконтpоллеp обладает значительными функционально-логическими возможностями и пpедставляет собой эффективное сpедство автоматизации и контpоля доступа на объект. Так как для управления объектами часто применяются алгоритмы, содержащие операции над входными и выходными булевскими переменными (истина/ложь), реализация которых средствами обычных микропроцессоров сопряжена с определенными трудностями, то очень важной особенностью МК51 является его способность опеpиpовать не только байтами, но и битами. Отдельные пpогpаммно-доступные биты могут быть установлены, сброшены, инвертированы, переданы, проверены и использованы в логических операциях.

Основу структурной схемы микроконтроллера образует внутренняя двунаправленная 8-битная шина, которая связывает между собой все основные узлы и устройств: резидентную память, арифметико-логическое устройство, блок регистров специальных функций, устройство управления и порты ввода/вывода (см. приложение ).

Цоколёвка корпуса AT98C51–20PI и наименования выводов показаны на рис.4.1.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Р1.0 | — | 1 |  | 40 | — | VCC |
| Р1.1 | — | 2 |  | 39 | — | Р0.0 |
| Р1.2 | — | 3 |  | 38 | — | Р0.1 |
| Р1.3 | — | 4 |  | 37 | — | Р0.2 |
| Р1.4 | — | 5 |  | 36 | — | Р0.3 |
| Р1.5 | — | 6 |  | 35 | — | Р0.4 |
| Р1.6 | — | 7 |  | 34 | — | Р0.5 |
| Р1.7 | — | 8 |  | 33 | — | Р0.6 |
| RST | — | 9 |  | 32 | — | Р0.7 |
| RXD | — | 10 |  | 31 | — | ЕА/VPP |
| TXD | — | 11 |  | 30 | — | ALE |
| INT0 | — | 12 |  | 29 | — | PSEN |
| INT1 | — | 13 |  | 28 | — | Р2.7 |
| T0 | — | 14 |  | 27 | — | Р2.6 |
| T1 | — | 15 |  | 26 | — | Р2.5 |
| WR | — | 16 |  | 25 | — | Р2.4 |
| RD | — | 17 |  | 24 | — | Р2.3 |
| XTAL2 | — | 18 |  | 23 | — | Р2.2 |
| XTAL1 | — | 19 |  | 22 | — | Р2.1 |
| VSS | — | 20 |  | 21 | — | Р2.0 |

Рис. 4.1. Цоколёвка корпуса AT98C51–20PI

AT98C51–20PI выполнен на основе высокоуровневой n–МОП технологии и выпускается в корпусе БИС, имеющим 40 внешних выводов. Для работы микроконтроллера требуется один источник электропитания +5 В. Через четыре программируемых порта ввода/вывода AT98C51–20PI взаимодействует со средой в стандарте ТТЛ–схем с тремя состояниями выхода.

Корпус микроконтроллера (МК) имеет два вывода для подключения кварцевого резонатора, четыре вывода для сигналов, управляющих режимом работы МК, и восемь линий порта 3, которые могут быть запрограмированны на выполнение специализированных функций обмена информацией со средой.

Синхронизация МК. Опорную частоту синхронизации определяет кварцевый резонатор РГ–05 с типом корпуса М, добротностью 2000х103, статической ёмкостью менее 9пФ, допустимым отклонением рабочей частоты 10х10–6. Кварцевый резонатор имеет гибкий тип выводов, предназначенные для соединений пайкой, миниатюрный плоский корпус, хорошо компонуется в современной аппаратуре. Он подключается к выводам XTAL1 и XTAL2 (рис.4.2). По рекомендации изготовителей микроконтроллера конденсаторы C9 и С10: КД–1 ёмкостью 20пФ каждый.

ZQ

C9

C10

Рис.4.2

XTAL1

XTAL2

Системный сброс AT98C51–20PI по рекомендации изготовителей осуществляется путём подачи на вход RST сигнала 1. Для уверенного сброса этот сигнал должен быть удержан на входе RST по меньшей мере в течение двух машинных циклов (24 периода резонатора). Время, необходимое для полного заряда ёмкости, обеспечивает уверенный запуск резонатора и его работу в течение более чем двух машинных циклов.

Связь микроконтроллера с датчиками и исполнительными механизмами обеспечивается через все имеющиеся выходные порты. Из-за низкой нагрузочной способности выходов МК для всех исполнительных механизмов и датчиков потребуются усилители мощности и согласователи уровней напряжений. Произведем их расчет.

Расчет индикаторов. В качестве светодиодов VD1, VD2 применим светоизлучающий диод АЛ336К красного цвета свечения с силой света не менее 40 мкд, а в качестве VD3, VD4 светоизлучающий диод АЛ336Г зеленого цвета свечения с силой света не менее 15 мкд. Для задания тока через светодиоды, последовательно с ними включим резисторы R1,R2,R3,R4. Для согласования микроконтроллера со светодиодами и его защиты будем подключать их через буферные формирователи. Выберем микросхему ТТЛ К155ЛП9 (DD1). Она содержит шесть буферных формирователей с открытым коллектором и повышенным коллекторным напряжением. Ее параметры:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| U0вых, не более  | U1вых, не менее | I0вх, не более | I1вх, не более | Iпот, не более |
|  В |  В |  мА |  мА |  мА |
|  0,4 |  2,4 |  -1,6 |  0,04 |  50 |

Определим номиналы резисторов.

При прямом падении напряжении на светодиоде 2 В и токе свечения 10 мА сопротивление каждого резистора:

R = [Uпит - Uпр]/Iпр =[5-2]/0,01=300 Ом. (4.1)

Рассеиваемая мощность резистора определяется исходя из тока, протекаемого через него по формуле

P = RI2 = 300х0,012 = 0,03 Вт. (4.2)

Таким образом сопротивление резисторов R1,R2,R3,R4 равно по 300 Ом каждый. В качестве номиналов выберем C2-33H–0,125–300Ом–10%.

Рассчитаем схему связи микроконтроллера с компьютером, которая включает в себя приемник и передатчик. Схема представляет из себя традиционную схему включения транзисторных ключей с буферными элементами [ ].Узел сопряжения с локальной сетью при передаче собран на DD4.2 и транзисторе VT2 совместно с портом Р3.1 (выход TXD — используется как универсальный асинхронный приемопередатчик). Резистор R9 выбирается исходя из тока в линии связи. Приемный узел сопряжения собран на DD4.1 и VT1 с использованием порта Р3.0 (вход RXD — вход данных универсального асинхронного приемопередатчика). Конденсаторы С1,С2,С3,С4 используются для повышения помехоустойчивости. Резисторы R6 и R7 задают рабочую точку ключа , собранного на транзисторе VT1. Нагрузкой каскада является резистор R5.

В качестве буферных элементов используется интегральная микросхема К1533ЛН5, которая представляет из себя шесть буферных логических элементов НЕ. Причем выходы с открытыми коллекторами. Параметры микросхемы:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| U0вых, не более  | U1вых, не менее | I0вх, не более | I1вх, не более | Iпот, не более |
|  В |  В |  мА |  мА |  мА |
|  0,7  |  2,4 |  -1,6 |  0,04 |  77 |

Проведем расчет элементов узла.

Задаемся током линии в передающем каскаде Iл = 20 мА [ ] и Eп = 12В, находим Rк (Rк=R9).

Rк = Eп / Iл = 12/0,02=600 Ом ; ( )

Определим мощность выделяемую на резисторе.

Р=I2\*Rк=0,022\*600=0,24 Вт; ( )

Rб = В х Rк =100х600=60 кОм ; ( )

где В = 100 - коэффициент усиления транзистора в ключевом режиме.

Задаемся током коллектора транзистора в приемном каскаде Iк = 1 мА и Eп = 5 В , определяем Rк(Rк=R5)в приемном каскаде.

R к = Eп / Iк = 5/0,001=5 кОм ; ( )

Резистор Rб (Rб=R6) в базе находим через В.

Rб = В х Rк = 50 кОм. ( )

Резистор R7 задает рабочую точку транзистора в каскаде , так чтобы он не уходил в область глубокого насыщения и находился на границах активного режима . Он рассчитывается исходя из Uбэ = 0.7 В , Uпор = 6 В.

Iб = Uпор / Rб =6/50000= 0.12 мА ; (4.7)

R7 = Uбэ / Iб =0,7/0,00012= 5.8 кОм.

По цепям питания ставим помехоподавляющие конденсаторы. C1 и С3 выбираются 10n [ ]. Они служат для подавления ВЧ составляющих помех. Конденсаторы С2,С4 выбираются равными 100мк х 16В [ ]. Они служат для подавления НЧ-компонент по питанию. Тогда выберем из [ ] номиналы конденсаторов:

С1,С3 — К10-17 10n+20%

C2,C4 — К50-16 100мк х16В

Выберем номиналы резисторов. Так как при самом большем токе мощность выделяемая на резисторе R9 (R9=Rк) равна 0,24 Вт, тогда R9 выбираем МЛТ- 0,25-5,1кОм10%. На остальных резисторах выделяется мощность меньше 0,125Вт. Тогда выберем [ ]:

R5 — C2-33H–0,125–5,1кОм–10%;

R6 — C2-33H –0,125–51кОм–10%;

R7 — C2-33H –0,125–5,6кОм–10%;

R8 — C2-33H –0,125–56кОм–10%;

В качестве транзисторов VT1,VT2 выберем мощный переключающий транзистор КТ972 [ ]. Кроме того в схеме предполагается применить импульсные диоды с малым временем переключения VD5,VD6 — КД521А. Диоды служат для защиты входных каскадов от высоких статических напряжений и импульсных выбросов.

Для питания схемы используются два стабилизированных источника напряжения : + 5 В , + 12 В.

Рассчитаем схему звукового сигнализатора.

На транзисторе VT4 собран блок выдачи сигнала тревоги ,представляющий собой электронный транзисторный ключ , подключенный к порту Р.3.4. Элементы ключа рассчитываются исходя из следующих параметров :

Uбэ = 0.7 В , U1= 3.5 В , Iб = 1 мА.

R14 = Uбэ / Iб = 750 Ом ;

R13 = U1 - Uбэ / Iб = 2,7 кОм.

Нагрузкой каскада является динамическая головка В1 типа 2ГДШ - 4.

Опишем схему считывателя кода идентификатора. Эта схема включения рекомендуется предприятием-изготовителем электронного идентификатора.

На логических элементах DD4.3 и DD4.4 , а также транзисторе VT3 собрано приемно - передающее устройство электронного ключа . Параметры каскада и элементов , рекомендуются изготовителем ключа фирмой “ Touch memory “. Приемная часть передает сигнал на порт Р.3.2 , а передаются управляющие команды с порта Р.3.5. Конденсаторы С5 и С6 служат фильтрами по питанию : С6 - по низким частотам , а С5 - по высоким частотам. Резистор R11 предназначен для защиты схемы от короткого замыкания на входном гнезде. Диоды VD7 и VD8 предназначены для защиты входного каскада от электростатических разрядов. Будем использовать диоды КД521 , как диоды с большим быстродействием , основанным на эффекте Шотки.

Такая же схема применена во втором считывателе кода идентификатора, с тем отличием, что второй считыватель кода подключается к портам Р3.3 и Р3.7 соответственно.

Рассчитаем схему подключения датчиков контроля положения дверей. В схеме используется описанная выше микросхема К1533ЛП9 выполняющая роль буферных элементов (DD2, DD3.1, DD3.2). В качестве датчиков предлагается использовать кнопочные выключатели с самовозвратом. Рассчитаем резисторы R18\_R25. Нагрузочный ток выберем равным 5 мА. Тогда

R=U/ I=5/ 0,005=1 кОм. ( )

Мощность рассеиваемая резистором будет равна:

Р=I2\*R=0,0052\*1000=0,025 Ом.

Из [ ] выберем для R18\_R25 следующие номиналы: C2-33H - 0,125 - 1кОм +10%.

Теперь произведем расчет для схемы управления электродвигателем. Так как микроконтроллер должен быть связан с мощным потребителем энергии, нужно предусмотреть в схеме управления гальваническую развязку между микроконтроллером и электродвигателем. Электромотор включается подачей логической единицы на порт Р1.6.(выключается нулем). В связи с этим предлагается применить оптронную развязку со схемой рекомендуемой предприятием-изготовителем. Оптрон типа — твердотельное реле 5П19Т. Его параметры: Iвх=25мА; Uком=+400В; tcраб,max=0,01мс; Iвх и=10мА; Iвых=1 А; тип корпуса 37х24х11 мм. Оптрон связан с микроконтроллером через буферный элемент НЕ и резистор R26 сопротивлением 360 Ом. Такая же схема включения идет на второй электродвигатель(порт Р1.7).

Для задания направления вращения электродвигателя предлагается использовать электромагнит(“1”-- вращение по часовой стрелке; “0”--вращение против часовой стрелки).Электромагнитный замок собран на транзисторе VT6 и подключен на порт Р.1.4. Резистор в базе рассчитывается исходя из тока коллектора транзистора. Диод VD11 предназначен для защиты транзистора во время включения и выключения , так как катушка электромагнита является индуктивной нагрузкой. Из [ ] выбираем диод КД226.

Расчет схемы контроля датчика физической массы пользователя. Так как для контроля массы в шлюзе предполагается использовать в качестве датчика массы обычные весы с аналоговым сигналом на выходе, то необходимо применить аналого-цифровой преобразователь. Для оцифровки этого напряжения необходимо использовать АЦП, который должен удовлетворять следующим требованиям: легко сопрягаться с микроконтроллером и требовать минимум внешних элементов для сиоей работы. Таким требованиям удовлетворяет микросхема К1113ПВ1 [ ]. Это функционально-законченный АЦП, основные технические характеристики которого следующие:

диапазон изменения входных напряжений — от -5 до +5 вольт;

разрядность — 10 бит;

время преобразования — 30мксек;

логические выходные сигналы — ТТЛ.

Работает схема следующим образом. При поступлении на вход “Запуск” АЦП сигнала низкого уровня запускается его внутренний генератор, и начинается процесс преобразования величины напряжения, присутствующего на выводе 13, в цифровую форму. Через 30 мксек. этот процесс заканчивается и на выходы D1\_D10 выдается цифровой код. О том, что данные поступили на выход, АЦП сообщает выдачей сигнала низкого уровня на выводе 17 (“Готовность”). Во время преобразования выходные линии данных находятся в Z-состоянии. Уровень логического нуля на выводе 15 определяет работу АЦП в режиме преобразования однополярного входного напряжения. Питается схема двуполярным напряжением +5В и -15В.

Так как высокой точности определения положения R29 не требуется, то ограничимся разбиением всего диапазона положений на 128 уровней. Тогда для представления номера каждого уровня потребуется log2128=7 двоичных разрядов. Поэтому задействованы будут выходы D1\_D7 АЦП. Определим теперь диапазон входных напряжений, которые необходимо снимать с датчика для получения на выходе АЦП кодов от 0 до 128 (от 0000000 до 1111111 в двоичном представлении). При работе с однополярными входными сигналами диапазон входных напряжений составляет от 0 до 10 вольт. Им соответствует выходные двоичные коды от 0 до 1023 ( т. е. от 0000000000 до 1111111111). Таким образом, вес младшего разряда составляет 10/1023 В - т.е. приблизительно 10мВ. Тогда для получения кода “1111111” необходимо подать входное напряжение 10\*128=1,28 В. При перемещении движка реостатного датчика R29 в верхнее по схеме положение, напряжение на входе АЦП составит:

U=5\*R29/(R29+R28) ( )

Приравнивая его к 1,28 , находим требуемое сопротивление резистора шкалы R28:

R28=3,9\*R29

Резистор R28 выбран переменным для возможности подстройки под конкретный тип датчика. Итак, для обработки сигналов от датчика массы потребуется девять линий связи с микроконтроллером: семь линий данных и две линии управления (запуска и готовности).

5.Разработка алгоритма управляющей программы

При проектировании системы в основу данной разработки блок-схемы алгоритма (БСА) была положена та же процедура модульного проектирования, которая традиционно используется разработчиками аппаратурных средств. Алгоритм управляющей программы составлен для контроллера шлюза и ориентирован на микроконтроллер AT89C51-20PI (см. чертеж “Блок схема алгоритма”).

Алгоритм имеет разветвленную структуру и дальнейшее его описание будет происходить в строгом соответствии с каждым символом-блоком действий.

Запрос прерывания. Алгоритм начинается с проверки условий запроса прерывания. Имеется в виду прерывание по портам P3.2 (INT0) и P3.3(INT1). Инициатором прерывания являются электронные идентификаторы. Регистор масок прерываний устанавливается в “разрешение внешних прерываний”. От внешних прерываний (если пользователь прикоснулся идентификатором считывателя кода) устанавливаются флаги IE0 или IE1 в регистре TCON, которые инициируют вызов соответствующей подпрограммы обслуживания прерывания. Флаги опрашиваются аппаратно в каждом машинном цикле. Внешние прерывания INT0 и INT1 вызываются переходом сигнала из 1 в 0 на входах МК51. То есть проверка запроса прерывания заключается в проверке условий: установлен флаг IE0 (или IE1) или нет. Если флаг установлен, значит есть запрос прерывания и программа переходит к обслуживанию ввода 64-ех битного кода идентификатора пользователя. Если флаг не установлен (то есть нет запроса прерывания), тогда программа переходит к блоку обработки — “Опрос датчиков”.

Ввод кода. После того как обнаружено прерывание, происходит переход к вводу идентификационного кода, который заключается в комбинациях минизадержек и опросов порта P3.2 (или P3.3). Задержка организуется запуском таймера (105 мксек), в течении которой опрашиваются входные порты. Инициатором запуска таймера выступает микроконтроллер, который выдает “стробирующие импульсы” на выход порта P3.5( или Р3.7) и переходит в режим ожидания ответа от идентификатора в течении задержки. Считывая код, микроконтроллер каждый бит заносит в резидентную память данных. Программа считывания кода с идентификатора приведена в приложении 3.

ИК1=1; ИК2=1. После того как код считан и занесен в РПД, программа переходит к следующему блоку. В данном случае блок индикации. Контроллер настраивает порты Р1.0 и Р1.1 на вывод логических нулей, для того чтобы “зажечь” красные светодиоды на обеих сторонах шлюза. Красные светодиоды сигнализируют пользователю, что код считан и система обрабатывает полученные данные, причем внешние прерывания от идентификаторов игнорируются. Затем программа переходит к блоку передачи кода в моноканал.

4) Вывод кода. Вывод кода в моноканал для передачи его на пульт управления происходит следующим образом. МК51 переходит в режим ожидания запроса от пульта управления. Имеется в виду следующее.

В регистре специальных функций SCON микроконтроллера имеется управляющий бит SM2, который в режиме 3 УАПП позволяет относительно простыми средствами реализовать обмен информацией в локальной сети между контроллерами и пультом управления (компьютером). Механизм обмена информацией через последовательный порт МК51 построен на том, что в режиме 3 программируемый девятый бит данных при приеме фиксируется в бите RB8. УАПП программируется таким образом, что при получении стоп-бита прерывание от приемника будет возможно только при условии RB8=1. Это выполняется установкой управляющего бита SM2 в регистре SCON. Компьютер в протокольном режиме “широковещательной” передачи (всем ведомым контроллерам) выдает в моноканал слово-адрес микроконтроллера, которое отличается от слов-данных только тем, что в его девятом бите содержится 1. Программа реализации протокола сетевого обмена информацией построена таким образом, что при получении слова-адреса, МК51 сверяет полученный адрес со своим адресом и в случае совпадения выдает в моноканал слово подтверждающее запрос адреса. Затем сбрасывает свой управляющий бит SM2 и готовится к подтверждению ответа от компьютера. После подтверждения микроконтроллер переходит к передаче кода-идентификатора в моноканал и заканчивает передачей кода “конец связи”. Передача ведется в режиме 3 УАПП.

Ожидание1. “Ожидание1” является подпрограммой обслуживающей обмен данными между компьютером и контроллером. Когда МК51 передает данные в моноканал он затем переходит в режим ожидания от компьютера. Это реализуется аппаратурной реализацией временного интервала на основе таймера задержки длительностью 2мсек.

В задачу ожидания также входит определение момента прихода ответа от компьютера. Для этого каждые два цикла микроконтроллера опрашивается регистор SCON.0( или бит RI). Бит RI устанавливается аппаратно в единичное состояние для фиксации приема байта в регистре SBUF. (Флаг прерывания приемника RI устанавливается аппаратурно в середине периода стоп-бита в режиме 3. Подпрограмма обслуживания прерывания должна сбрасывать бит RI). То есть если обнаружено, что в течении ожидания RI=1, значит пришел ответ от компьютера.

Ввод ответа. В течении ожидания приходит ответ от компьютера, который заносится в РПД. А в резидентной памяти программ (РПП) хранятся коды правильных и неправильных кодов-ответов (см. Таблицу5.1)

Таблица 5.1

|  |  |  |
| --- | --- | --- |
| адрес РПП | информационный код | назначение |
| 0CH | 00001111 | пользователь идентифицирован |
| 0DH | 11110000 | пользователь неидентифицирован |
| 0EH | 00011111 | подлиность подтверждена |
| 0FH | 11100000 | подлиность неподтверждена |

Сверяя полученные ответы с хранящимися кодами, МК51 принимает соответствующее решение о переходе на ту или иную подпрограмму.

Опрос датчиков. Контроллер обрабатывает информацию снимаемую с датчиков. Эта задача реализуется обращением к порту P.0 и сравнении снятого кода с таблицей кодов положения дверей хранящихся в РПП (см. таблицу 5.2)

Таблица 5.2

|  |  |
| --- | --- |
|  | положение дверей |
|  | закрыто |  нейтрально |  открыто |
| д1.1 | 1 | 0 | 1 |
| д1.2 | 1 | 0 | 0 |
| д1.3 | 1 | 0 | 0 |
| д1.4 | 1 | 0 | 1 |
| д2.1 | 1 | 0 | 1 |
| д2.2 | 1 | 0 | 0 |
| д2.3 | 1 | 0 | 0 |
| д2.4 | 1 | 0 | 1 |

Таблица 5.3

|  |  |  |
| --- | --- | --- |
| адрес РПП | информационный код | назначение |
| 05H | 00001001 | двери1 открыты |
| 06H | 00001111 | двери1 закрыты |
| 07H | 10010000 | двери2 открыты |
| 08H | 11110000 | двери2 закрыты |

В таблице 5.3 хранятся коды соответствующие возможным положениям дверей шлюза. В нейтральном положении на входе порта Р.0 присутствуют все нули (т. е. 00000000). В зависимости от считанного кода порта Р.0 принимается соответствующее решение о переходе на соответствующую подпрограмму.

Кроме того опрашивается порт Р.2 , который предназначен для считывания кода с АЦП, в котором содержится информация о физической массе. Если масса равна нулю и двери закрыты происходит переход на начало программы. В случае не выполнения этих условий запускается подпрограмма инициализации запуска тревоги, которая заключается в передаче соответствующего кода на пульт управления.

Микроконтроллер переходит в режим ожидания запроса адреса от компьютера (См. блок “Вывод кода”). Установив связь с компьютером МК сбрасывает в регистр SBUF байт соответствующей определенному виду тревоги. Т.е. если масса не равна нулю то в SBUF записывается 01011000 (что говорит о присутствии в шлюзе нарушителя), если двери открыты, то в SBUF записывается 00001001 или 10010000 (что говорит о саботаже работы дверей). Запись в SBUF означает автоматическую передачу кода в моноканал.

Звуковая сигнализация. После выдачи в моноканал кода-тревоги, МК инициирует подпрограмму включения звуковой сигнализации, которая предупреждает нарушителя о саботаже работы системы. Длительность звуковой сигнализации — 5 секунд. После чего программа снова возвращается к опросу датчиков. Еще раз опросив датчики и если условие m=0, d=0 (т.е. масса =0, двери закрыты) программа возвращается в начало.

ИК1=0, ИЗ1=1. Если пользователь идентифицирован программа переходит к следующей операции: погасить красный светодиод на входе в шлюз (на выходе красный остается включенный), включить зеленый. Для этого на порт P.1.0. подается 1, на порт Р.1.2 подается 0. Если пользователь не идентифицирован происходит переход на подпрограмму запуска звуковой сигнализации, а затем в начало программы.

После того как пользователь идентифицировался запускается подпрограмма открывания сдвижных дверей (см. приложение 3) и переход в режим ожидания. Ожидание заключается в аппаратно-программной задержке на 10 секунд для того, чтобы дать пользователю время войти в шлюз. Если по истечении этого времени он не войдет, двери автоматически закрываются. В течении задержки программа постоянно (каждые 10 циклов) опрашивает датчик массы. Как только не выполняется условие m=0, происходит переход к следующему блоку программы. А именно — закрытие дверей1. Закрытие дверей заключается не только в подаче кода-закрытия на Р.1.6. и Р.1.4. Попутно с запуском подпрограммы задержки (на время закрытия двери) происходит опрос датчиков для обнаружения возможного факта нарушения регламента работы сдвижных дверей. Т.е. если во время задержки двери не будут закрыты, поступит команда на их повторное открывание (ситуация — пользователь не спел войти в шлюз). Если по истечении одной минуты конфликтная ситуация не разрешится с компьютера поступит код-сигнал блокировки дверей до прихода службы безопасности. Если пользователь находится в шлюзе (m не равна 0, т.е. код на порте Р.2.1-Р2.7 не равен 0) программа переходит к ожиданию кода своего сетевого адреса на входе УАПП (см. ввод кода). После установки связи контроллер выдает в моноканал код соответствующий массе пользователя после чего переходит в режим ожидания1 (см. приложение 3) ответа от компьютера. Полученный код сверяется с адресом 0СН в случае совпадения — переход к подпрограме “открытия двери”.

Основные подпрограммы приведены в приложении 3

6.Разработка конструкции печатной платы

Под конструктивным расчетом печатной платы понимается расчет геометрических размеров платы, компоновка радиодеталей на плате, выбор материала платы и др.

В данном дипломном проекте необходимо произвести расчет платы контроллера шлюза. В начале произведем расчет предполагаемой площади и геометрических размеров, затем выберем материал печатной платы, и произведем трассировку. Для расчета площади платы необходимо подсчитать количество компонентов каждого класса, определить геометрические размеры этой платы.

По размещению проводящего рисунка печатные платы делятся на односторонние, двусторонние и многослойные.

Односторонняя печатная плата проста по конструкции и несложна в изготовлении, но при существующих системах трассировки на ней практически невозможно выполнить сложные схемы. Поэтому была произведена автоматическая трассировка платы в системе PCCARDS на две стороны. Высокая плотность проводников, полученная при трассировке, позволяет выполнить монтаж платы с высокой плотностью, что экономит материал платы.

В качестве основного материала для печатных плат используется фольгированные и нефольгированные листовые диэлектрики. Исходными для изготовления фольгированных диэлектриков могут быть бумага или стеклоткань, пропитанные синтетическими смолами или полимерные пленки из лавсана, фторопласта. На поверхность этих материалов приклеивается металлическая фольга.

В качестве материала для печатной платы выберем стеклотекстолит фольгированный СТФ - 2 со следующими параметрами: толщина фольги 35 мкм, толщина материала с фольгой 2 мм, прочность сцепления 450 гс/3 мм.

Размещение элементов конструкции печатной платы регламентируется условной координатной сеткой из двух взаимно перпендикулярных систем параллельных линий, расположенных на одинаковом ( 2.5 мм или 1.25 мм) расстоянии друг от друга. Центры монтажных отверстий и контактных площадок под выводы навесных радиоэлементов располагают в узлах координатной сетки.

Расчет размеров печатной платы произведем по формуле:

Sэ = k\*(S1 + S2) (6.1)

где Sэ-суммарная площадь элементов;

S1-площадь малых элементов;

S2-площадь больших элементов; k - коэффициент плотности.

Для определения суммарной площади определим количество элементов.

Таблица 6.1.

|  |  |  |
| --- | --- | --- |
| НАИМЕНОВАНИЕ | КОЛ-ВО ЭЛЕМЕНТОВ | ПЛОЩАДЬ ЭЛЕМЕНТА |
| РЕЗИСТОРЫ | 31 | 0.7 |
| КОНДЕНСАТОРЫ | 10 | 0.3 |
| ДИОДЫ | 8 | 0.4 |
| КВАРЦ | 1 | 5.5 |
| ТРАНЗИСТОРЫ | 54 | 0.80.6 |
| ОПТРОНЫ | 2 | 3.8 |
| МИКРОСХЕМЫ | 511 | 1.54.62.1 |

S1 = Sк + Sд = 10\*0,3 + 8\*0,4 = 6,2 см2

S2= Sр + Sмс + Sкв + Sтр + Sоп = 0,7\*31+5,5\*1+0,8\*5+0,6\*4+3,8\*2+1,5\*5+4,6\*1+2,1\*1 = 58.7 см2

К=8 , (Монтаж двухсторонний при средней плотности)

Sэ = 8\*(6,2 + 58,7) = 519,2 см2

Печатная плата разведена автоматически, элементы размещались на площади 150:150 мм. Соотношение сторон выбрано 1:1. После разводки элементы удалось разместить более компактно получили 140х140 мм соответственно.

В результате конструктивного расчета получили, что контроллер шлюза будет располагаться на двухсторонней стеклотекстолитовой фольгированной плате размерами 130х140 мм.

Вид печатной платы со стороны деталей изображен на чертеже “Конструкция печатной платы”.

Печатная плата разведена при помощи пакета PCAD (Personal CAD System) версии 4.50. Расстановка элементов на печатной плате и трассировка электрических связей производилась автоматически при помощи интеллектуального графического редактора PCCARDS. Использовались также программы автоматического размещения элементов (PCPLACE) и трассировки электрических связей (PCROUTE) в виду относительной сложности схемы и, соответственно, печатной платы.

7 Технико–экономическое обоснование

Характеристика проекта

В качестве основного аргумента при проектировании системы защиты и контроля доступа в помещения является экономическая целесообразность проекта. Реализация системы поможет в пресечении противоправных действий, уменьшит причиняемый гражданам вред.

В виду того, что для развертывания системы не требуется какихлибо дорогих и дефицитных комплектующих деталей, предполагается, что производство изделия будет носить массовый характер.

На начальном этапе в г.Минске может быть установлено в одних только административных зданиях около 1500 систем. Можно сказать, что для развертывания производства потребуется сравнительно небольшие затраты (оборудование, комплектующие, кадры). Исходя из этого, предполагаем физический объем выпуска 2000 систем в год. В качестве расчетного периода берем срок три года. Вследствии того, что система состоит из нескольких блоков и способна к наращиванию, произведем расчет для одного блока — контроллера.

Выбор методики расчета годового экономического эффекта

В мировой практике по вопросам инженерной экономики рассматриваются многочисленные методы инвестиционных расчётов, среди которых выделяются как наиболее широко применяемые:

чистая приведённая величина дохода;

срок окупаемости капиталовложений;

“внутренняя” норма доходности;

рентабельность;

безубыточность.

Указанные показатели отражают один и тот же процесс сопоставления распределенных во времени выгод от инвестиций и самих инвестиций.

Чистая приведенная величина дохода характеризует конечный эффект инвестиционной деятельности. В отечественной практике под чистой приведенной величиной дохода понимают экономический эффект за расчетный период времени (Э):

Э = Р – З , (7.2.1)

где:

Р — стоимостная оценка результата от внедрения мероприятия за расчётный период, руб.

З — стоимостная оценка затрат на реализацию мероприятия, руб.

Определение себестоимости товара и оптовой цены проектируемого изделия

В радиоэлектронных отраслях промышленности все затраты, включаемые в себестоимость продукции принято делить на прямые и косвенные. К прямым статьям относятся такие затраты как:

* сырьё и основные материалы (за вычетом отходов);
* комплектующие изделия и покупные полуфабрикаты;
* основная заработная плата производственных рабочих.

Остальные статьи затрат являются косвенными и рассчитываются по нормативам, установленным в процентах либо к основной заработной плате производственных рабочих, либо к производственной себестоимости продукции.

В статье “Комплектующие изделия и покупные полуфабрикаты” учитываются затраты, связанные с приобретением со стороны готовых комплектующих изделий и полуфабрикатов, подвергающихся на предприятии монтажу и обработке, транспортно заготовительные расходы на их приобретение и доставку сторонним транспортом.

Одним из важнейших показателей, характеризующих изделие как объект производства, является его себестоимость. Она включает сумму затрат в сфере производства на его изготовление.

Расчёт себестоимости единицы проектируемой техники (С) производится по всем статьям затрат в соответствии с “Основными положениями по планированию, учёту, калькулированию себестоимости на промышленных предприятиях”. Расчёт затрат на комплектующие изделия и покупные полуфабрикаты сведён в таблицу 7.1.

Таблица 7.1 — Расчёт затрат на комплектующие изделия и покупные полуфабрикаты (руб.).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ¹ | Наименование комплектующих изделий и полуфабрикатов | Количество на единицу изделия, шт. | Цена за единицу,руб. | Сумма затрат,руб.  |
| 1 | Микросхемы:AT89С51-20PI155ЛП9155ЛН5К1113ПВ1 | 1321 | 600002000150015000 | 600006000300015000 |
| 2 | Резисторы:МЛТ– 0,125  | 31 | 100 | 31000 |
| 3 | Конденсаторы:К73–16К50-35 | 67 | 1000800 | 60005600 |
| 4 | Диоды:КД521ВД226 | 62 | 10004000 | 6008000 |
| 5 | Светодиоды:АЛ336ГАЛ336К | 22 | 30003000 | 60006000 |
| 6 | Динамическиеголовки: 2ГДШ4 | 2 | 40000 | 80000 |
| 7 | Оптронный5П19T  | 2 | 30000 | 60000 |
| 8 | ВыключателиКМ2-I | 8 | 5000 | 40000 |
| 9 | Кварцевый резонатор | 1 | 13000 | 13000 |
| 10 | Плата | 1 | 14300 | 14300 |
| 11 | Транзисторы:КТ814АКТ972АКТ315А | 142 | 300030002000 | 3000120004000 |
| 13 | Соединители | 3 | 3000 | 9000 |
| Итого: | 410000 |
| Расходы на транспортировку 2% | 8000 |
|  Итого: | 418000 |

Определив величину затрат по какой-либо одной из статей прямых затрат (в данном случае это статья “Комплектующие изделия и полуфабрикаты”) можно рассчитать затраты по всем остальным статьям проектируемого изделия, а затем определить себестоимость.

Величину по статье “Сырье и основные материалы” можно рассчитать по формуле:

М = Мк , руб, (7.3.1)

где Ум – удельный вес затрат на сырье и материалы в полной себе

стоимости, Ум = 1%;

Ук – удельный вес затрат на комплектующие изделия и покупные

полуфабрикаты, Ук = 48%.

Отсюда: М= руб.

Величина затрат по статье “Основная заработная плата производственных рабочих” определяется по формуле.

ЗО= МК х(УЗ/УК),руб, (7.3.2)

где:

УЗ – удельный вес затрат по статье “Основная зарплата производственных рабочих” в полной себестоимости продукции: УЗ =1%,

ЗО=418000х1/48 = 88000 руб.

Выше рассчитаны прямые статьи затрат. Косвенные статьи затрат рассчитываются по нормативам, установленным в %, либо к основной зарплате производственных рабочих, либо к производственной себестоимости продукции.

Таблица 7.2.-- Проценты косвенных расходов.

|  |  |  |  |
| --- | --- | --- | --- |
| № | Наименование статей | Условное обозначение | Величина, % |
| 1 | Возмещение износа специнструмента | НИЗ | 20 |
| 2 | Расходы на эксплуатацию инструмента | НСЭ | 50 |
| 3 | Цеховые расходы | НЦ | 50 |

Таблица 7.3 — Расчет себестоимости и оптовой цены единицы продукции (руб.).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Наименование статей затрат | Услов- ное обозна-чение | Методика расчета | Сумма |
| 1 | Материалы (за вычетом стоимости возвратных отходов) | М | смотри формулу 7.3.1. | 8700 |
| 2 | Покупные полуфабрикаты и комплектующие изделия | МК | смотри таблицу 7.2. | 418000 |
| 3 | Основная заработная плата основных производственных рабочих | ЗО | смотри формулу 7.3.2. | 8700 |
| 4 | Дополнительная заработная плата основных производственных рабочих | ЗД | ЗД=НД – процент дополнительной заработной платы(10%) | 870 |
| 5 | Заработная плата (основная и дополнитель­ная) остальных категорий ППП | ЗПК | ЗПК=(ЗО+ЗД)КЗПКЗП – коэффициент заработной платы остальных категорий ППП (0,2) | 1910 |
| 6 | Отчисления в фонд социальной защиты населения | ЗФС | ЗФС=НФС –процент отчисления в фонд социальной защиты населения (36%) | 4200 |
| 7 | Износ специнструментов и приспособлений целевого назначения | РИЗ | РИЗ= | 1740 |
| 8 | Расходы на эксплуатацию инструмента | РСЗ | РСЗ= | 4350 |
| 9 | Цеховые расходы | РЦД | РЦ= | 4350 |
| Итого цеховая себестоимость изделия:СЦ=М+МК+ЗО+ЗД+ЗПК+ЗФС+РИЗ+РСЭ+РЦ | 453000 |
| 10 | Общезаводские расходы | РОЗ | РОЗ=НОЗ=100% | 8700 |
| 11 | Отчисления в бюджет и во внебюджетные фонды, включаемые в себестоимость:-чрезвычайный налог в фонд Чернобыля – 8%-на финанси-рование расходов по содержанию вневедомственных дошкольных учреждений (ДДУ)– 5% | РБВ | РБВ=НБВ=13% | 15000 |
| 12 | Прочие производственные расходы | РПР | РПР=НПР=1%С\*ПР — производственная себестоимость без учета прочих производственных расходовС\*ПР=СЦ+РОЗ+РБВ=4908500. | 4632 |
| Итого производственная себестоимость изделия | СПР | СПР=С\*ПР+РПР | 467830 |
| 13 | Внепроизвод­ственные рас­ходы | РВ | РВ=НВН=0.3% | 14000 |
| Итого полная себестоимость изделия | СП | СП=СПР+РВ | 481864 |
| 14 | Нормативная прибыль на единицу изделия | П | П=УРИ–уровень рентабель­ности изделий (20%) | 96373 |
| 15 | Добавленная стоимость | ДС | ДС=ЗО+ЗД+ЗПК+ЗФС++АО+ПАО–амортизационные отчисления на полное восстановление ОПФ предприятияАО=НАО–процент амортизационных отчислений на полное восстановление ОПФ предприятия (12%) | 113000 |
| 16 | Налог на добавленную стоимость | РДС | РДС=НДС=20% | 22600 |
| 17 | Отчисления в спецфонды (на содержание дорог, ведомственного жилого фонда, в фонд поддержки производителей сельскохозяиствен-ной продукции) | ОСФ | ОСФ=НСФ-процент отчислений в спецфонды (2,5%) | 15020 |
| 18 | Свободная отпускная цена | Ц | Ц=СП+П+РДС+ОСФ | 615800 |

Определение сметной стоимости НИОКР

Сначала определим основную заработную плату сотрудников, учавствующих в НИОКР:

Таблица 7.4 — Расчёт основной заработной платы.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Исполнители | Количество | Количество человеко–дней | Средняя заработная плата в день, руб. | Сумма основной заработной платы, уб. |
| Научный сотрудник | 1 | 20 | 100000 | 2000000 |
| Инженер | 1 | 20 | 60000 | 1200000 |
| Итого | 3200000 |

Теперь определим затраты на приобретение спецоборудования для НИОКР:

Таблица 7.5 — Затраты на приобретение оборудования.

|  |  |  |  |
| --- | --- | --- | --- |
| Показатели | Количество,шт. | Отпускная цена, руб. | Затраты,руб. |
| Осцилограф | 1  | 3000000 | 3000000 |
| Транспортно–заготовительные расходы (5%) | 150000 |
| Итого | 3150000 |

Определим затраты, необходимые для разработки программного обеспечения системы (табл 7.6.).

Таблица 7.6 — Стоимость программного средства.

|  |  |  |
| --- | --- | --- |
| Показатель | Единицы | Значение |
| Трудоёмкость разработки ПС | чел.—дн. | 40 |
| Тарифная стоимоисть одного часа машинного времени | руб./час. | 2000 |
| Итого стоимость: | руб. | 40х8х2000=640000 |

Смета затрат на проведение научно-исследовательской работы включает несколько статей. Произведем расчёты в табличной форме (табл. 7.7.).

Таблица 7.7 — Смета затрат на проведение НИОКР (руб.).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Наименование статей затрат | Условное обозначение | Методика расчета | Сумма |
| 1 | Покупные полуфабрикаты и комплектующие изделия | МК | смотри таблицу 7.1. | 418000 |
| 2 | Основная заработная плата сотрудников НИОКР | ЗО | смотри таблицу7.4. | 3200000 |
| 3 | Затраты на спецобору­дование | ЗСО | Смотри таблицу 7.5. | 3150000 |
| 4 | Дополнитель­ная заработная плата сотрудников НИОКР | ЗД | ЗД=НД – процент дополнительной заработной платы(10%) | 320000 |
| 5 | Отчисления в фонд социальной защиты населения | ЗФС | ЗФС=НФС — процент отчисления в фонд социальной защиты населения (36%) | 1267200 |
| 6 | Отчисления в бюджет и во внебюджетные фонды. |  РБВ |  РБВ=НБВ=13% | 457600 |
| 7 | Стоимость машинного времени  | УСТ | Смотри табл. 7.6. | 640000 |
| 8 | Итого SНИОКР: | 9453000 |

Расчёт единовременных затрат

Единовременные затраты в сфере производства включают предпроизводственные затраты (КППЗ), капитальные вложения в производственные фонды завода – производителя (КПФ):

КП= КППЗ+КПФ . (7.5.1)

Предпроизводственные затраты определяются по формуле:

КППЗ= SНИОКР+КОСВ, (7.5.2)

КОСВ — затраты на освоение производства.

Капитальные вложения в сфере производства новой техники определяются следующим образом:

КПФ = ЦОБ + КТР + КМ + КЗД + КОС + КПР . (7.5.3)

Пусть оборудование, необходимое для изготовления новой техники, уже является нашей собственностью (внесено в уставный фонд или безвозмездно передано в пределах одного собственника) и не требует особых капиталовложений. Тогда ценой оборудования ( ЦОБ ), затратами на транспортировку и монтаж (КТР,КМ) можно пренебречь.

При условии предоплаты на сумму начисленной годовой арендной платы (расходы будущих периодов), исходя из стоимости 2000000 руб./мес., можно найти стоимость переданной в аренду без права выкупа производственной площади:

К’ЗД = 2000000х12 =24000000 руб.

Но так как в течение срока аренды вся сумма начисленной арендной платы включается в себестоимость изделия, то:

КЗД = 0.

Капитальные вложения в оборотные фонды определяются по формуле:

КОС = КОСМ + КОСПРИС + КОСД, (7.5.4)

где КОСМ – капитальные вложения в образование постоянных нормативных запасов основных и вспомогательных материалов, полуфабрикатов и комплектующих изделий в расчёте на годовую программу, руб.;

КОСПРИС – капитальные вложения в образование постоянного запаса малоценных приспособлений и инструментов в расчете на годовую программу, руб.;

КОСД – капитальные вложения в образование постоянных заделов деталей и узлов в расчете на годовую программу, руб.

Можно пренебречь расчётом КОСПРИС и КОСД ввиду их незначительной величины и ограничиться расчётом КОСМ по следующей формуле:

КОСМ = , (7.5.5)

где Sмi – цена едницы материала i – го вида, руб./над.ед.;

Nмi – годовая потребность в материале i – го вида, нат.ед./год;

ТН – количество дней работы предприятия в год, дн./год;

ТНЗ – норма запасов материалов, дней.

В нашем случае:

КОСМ = 418000х2000х0.1/300 = 280000 руб.

Итак, пренебрегая прочими капитальными вложениями КПР:

КПФ = 280000 руб.

Затратами на освоение производства КОСВ можно пренебречь, т. к. при изготовлении, наладке и испытании изделия не требуется специальной техники и высококвалифицированных кадров. Итак, единовременные затраты:

КП = 9453000 + 280000 = 1225000 руб.

Расчёт экономического эффекта

На основе расчётов, приведённых ранее, определим целесообразность внедрения инженерного проекта. Теперь у нас есть все данные для

расчёта ЭЭ. Определение экономического эффекта удобно провести в табличной форме (таблица 7.8.).

Таблица 7.8 — Расчёт экономического эффекта по годам.

|  |  |  |
| --- | --- | --- |
| Показатели | Единицыизмерения | Расчетный период |
| 1997 | 1998 | 1999 |
| РЕЗУЛЬТАТ:1.Прогнозируемый физический объём производства | шт. | 2000 | 2000 | 2000 |
| 2.Прогнозируемый объём продаж | млн.руб. | 1231,5 | 1231,5 | 1231,5 |
| 3.Полная себестоимость продукции | млн. руб. | 963,7 | 963,7 | 963,7 |
| 4.Чистая прибыль | млн. руб. | 192,75 | 192,75 | 192,75 |
| 5.То же с учётом фактора времени | млн.руб. | 192,75 | 289,125 | 433,68 |
| ЗАТРАТЫ:6.Предпроизводственные затраты | млн.руб. | 9,453 |  |  |
| 7.Капитальные вложения | млн. руб. | 0,28 |  |  |
| 8.Итого единовременных затрат | млн. руб. | 1,225 |  |  |
| 9.То же с учётом фактора времени | млн. руб. | 1,225 | 1,837 | 2,756 |
| ЭКОНОМИЧЕСКИЙ ЭФФЕКТ:10.Превышение результата над затратами (п.5 – п.9) | млн. руб. | 181,792 | 287,28 | 430,924 |
| 11.Экономический эффект нарастающим итогом | млн. руб. | 181,792 | 352,688 | 883,569 |
| 12.Коэффициент приведения к расчётному году |  | 0,44 | 0,66 | 1 |

###### ВЫВОДЫ:

При данном объёме выпуска изделия (2000 шт./год) мы уже в первом году получим прибыль, при условии продажи всей партии. Конкурентноспособность изделия обеспечивается широкими функциональными возможностями и более низкой ценой, по сравнению с аналогами.

Экономический эффект от внедрения и изготовления проектируемого изделия составит: (1999г.) 883,569млн. руб.

8.Охрана труда и экологическая безопасность

Оценка электробезопасности:

В проектируемой системе с точки зрения экологической безопасности одним из самых опасных факторов влияющих на жизнедеятельность человека, является опасность поражения электрическим током.

Оценка опасности поражения заключается в расчёте протекающего тока через человека или напряжения прикосновения UПР и сравнения этих величин с предельно допустимыми в зависимости от продолжительности воздействия тока. Эта оценка проводится как в нормальном режиме работы электроустановки, так и в аварийном. Оценка опасности электропоражения позволяет определить необходимость применения способов и средств защиты, а фактические и предельно допустимые значения UПР и IК служат исходными данными для их проектирования и расчёта.

Ввиду того, что проектируемая система может иметь различную конфигурацию по количеству контролируемых пунктов, месту их размещения и расстояния между ними и центральным пультом управления, будем исходить из следующего. СЗКДП пусть будет иметь пять контролируемых пунктов и один центральный пульт управления, расположенные в одну линию, (рис.8.1).

КП

КП

КП

КП

ЦПУ

КП

заземлитель

Рис.8.1 Заземлители

Контролируемый пункт представляет собой систему шлюза с двумя сдвижными дверями которые управляются электродвигателем питающимся от однофазной сети. Электродвигателем управляет микропроцесорное устройство. Работу контроллируемых пунктов (КП) контролирует центральный пульт управления (ЦПУ) выполненный на базе IBM PC совместимого компьютера. Каждый КП и ЦПУ запитываются от однофазной сети переменного тока. Расстояние между контролируемыми пунктами выбирается равным 10 метрам.

Исходя из выше сказанного ясно, как важно оценить потенциальную опасность электропоражения. В системе предполагается использовать заземляющие устройства на базе искусственных и естественных заземлителей, о чем будет описано ниже. Но прежде производится расчет возможных токов поражения. Фактические значения напряженияприкосновения Uпр и протекающего тока через человека Iк могут быть определены расчетным путем или эксперементально.

При расчете Iк необходимо знать сопротивление в цепи человека Rск, которое включает в себя сумму сопртивлений тела человека Rк, обуви Rоб и основания Rос, на котором стоит человек, то есть

Rск = Rк + Rоб + Rос (8.1)

Сопротивление тела человека Rк принимается равным 1кОм. Сопротивление обуви принимается равным 1,5кОм [ ].

Электрическое сопротивление основания Rос зависит от материала и степени влажности пола. Так как очень часто в качестве материала для пола используется бетон, будем сопротивление считать для бетона, считая, что пол мокрый (худший случай). Тогда из таблицы [ ] ,берем:

Rос=0,1кОм

Следовательно сопротивление в цепи человека

Rск=1+1,5+0,1=2,6кОм

Расчитаем Iк для случая с заземленным проводом (прикосновение к незаземленному проводу)

Iк=U/(Rск+r0) , (8.2)

где U — напряжение сети, равное 220В;

г0 — сопротивление заземления провода, равное 10 Ом.

Тогда

Iк=220/(2600+10)=0,0843А

Теперь рассчитаем Iк для случая с заземленным проводом (прикосновение к заземленному проводу). При прикосновении к заземленному проводу человек оказывается под воздействием напряжения Uпр, равного потере напряжения в заземленном проводе на участке от места его заземления **а** до места касания **в**:

Uпр= Iнг\* rав (8.3)

где Iнг — ток нагрузки;

rав ---- сопротивление провода на участке *ав*.

В нормальных условиях Uпр невелико. Наибольшее его значение соответствует прикосновению человека к точке в непосредственной близости с нагрузкой и составляет не более 5% напряжения сети. То есть

Uпр=220\*0,05=11В (худший случай),

тогда

Iк=Uпр/Rск=11/2600=0,0042А

При коротком замыкании между проводами ток резко возрастает и потеря напряжения в проводах достигает почти 100%U. Напряжение прикосновения возрастает практически пропорционально увеличению тока в проводе и при коротких замыканиях может достигать опасных для человека значений, особенно вблизи нагрузки, тогда

Iк=220/2600=0,085А

Подведя итоги можно сделать вывод, что наиболее опасный случай для человека возникает при прикосновении к проводу при коротком замыкании, когда ток равен 85мА. Неопасным для человека является ток равный 4,2мА [ ] при прикосновении к заземленному проводу при нормальном режиме работы.

При выборе средств защиты работающих от электропоражения необходимо учитывать особенности производства и условия эксплуатации оборудования, потребляющего электрическую энергию. Согласно правилам и условиям электробезопасности для обеспечения электробезопасности объекта в случае повреждения изоляции следует применять, по крайней мере, один из следующих способов защиты: защитное заземление, зануление, защитное отключение, разделительный трансформатор и другие.

В проектируемой системе в качестве основного способа защиты выбираем защитное заземление. Оно применяется в электроустановках, питающихся изолированными от земли выводами источника однофазного тока, что применительно к нашему случаю.

В системе предусматривается автономная шина заземления технических средств для подключения корпусрв устройств, экранов кабелей и подключения логических нулей цепей элементов схем. Основным требованием к автономному заземлению является то, чтобы сопротивление заземляющего устройства между клемой земли контролируемых пунктов, центрального пульта управления и землей (грунтом) не превышало 4 Ом в любое время года [ ].

Расчет заземлителей в проектируемой системе с напряжением до 1кВ выполняют методом коэффицента использования по допустимому сопротивлению заземлителя растеканию тока.

Вначале определим допустимое сопротивление заземляющего устройства Rз.доп. Согласно ПУЭ значение Rз.доп устанавливается в зависимости от напряжения сети и суммарной мощности трансформаторов, питающих эту сеть, а именно: при напряжении до 1000В и мощности менее 1000 кВ\*А допустимое заземляющее сопротивление Rз.доп=4Ом. Возможно на территории где будет эксплуатироваться СЗКДП будут присутствовать естественные заземлители, которые можно использовать. Поэтому общее сопротивление заземляющего устройства Rз.у будет складываться из сопротивления естественных и искусственных заземлителей, т.е.

1/ Rз.у=1/Rест + 1/Rиск < Rз.доп (8.4)

Так как требуемое значение Rз.доп может быть обеспечено только естественнымизаземлителями, то сначала необходимо выполнить расчет сопротивления естественных заземлителей и полученный результат сравнить с требуемым значением Rз.доп.В виду того, что отсутствуют исходные данные для расчета сопротивления естественных заземлителей, произведем расчет искусственных заземлителей.

Для заземления стационарных установок наибольшее распространение получили групповые искусственные заземлители, размещенные в грунте на определенной глубине. Они представляют собой систему вертикальных электродов, параллельно соединенных горизонтальным проводником связи. Расстояние (Q) между соседними вертикальными электродами рекомендуется выбирать не менее 2,5 м. Для заземлителей, расположенных в ряд отношение Q к длине (L) вертикального электрода предпочтительно выбирать равным около 2, а при расположении электродов по контуру — равным 3.

В начале определим сопротивление одиночного вертикального электрода. Предполагается использовать заземлитель стержневой круглого сечения или уголковый у поверхности земли (рис.8.2).

 d

 L

 Рис.8.2 Заземлитель

Rв=р/(6,28\*L)\*ln(4\*L/d) (8.5)

где Rв - сопротивление одиночного заземлителя;

p - удельное сопротивление земли;

L - длина стержня;

d - ширина стержня.

Удельное сопротивление земли (p) определяется эксперементально и зависит от типа грунта. Из таблицы [ ] выбираем наиболее распространенный вид грунта — почва. Рекомендуемое значение p для почвы равно 200 Ом\*м. С учетом коэффицента сезонности (*y*) из таблицы определим рассчетное сопротивление грунта,

pp=p\**y* (8.6)

Коэффицент сезонности *y* исходя из таблицы для вертикального электрода длиной 3 метра равен 1,5. Тогда

pp=200\*1,5=300 Ом\*м

Ширину заземлителя (d) выберем равной 0,05 метров. Теперь найдем сопротивление одиночного заземлителя,

Rв=300/(6,28\*2)\*ln(4\*2/0,1)=20 Ом

Далее определим ориентировочное количество вертикальных электродов (n) с некоторым избытком. Для этого находят произведение коэффицента использования вертикальных электродов (*n*в) на их количество (n) по формуле

n\**n*в=Rв/Rз (8.7)

n\**n*в=20/4=5

Для нахождения числа электродов используем таблицу [ ].

Из таблицы видно, что при размещении в ряд получим:

*n*в=0,77 ; n=6

Далее, зная ориентировочное количество электродов, с учетом их размещения в грунте, найдем длину горизонтального проводника связи при расположении в ряд,

l=1,05\*(n- 1)\*a=1,05\*(6-1)\*10=52,5 м.

Рассчитаем сопротивление растекания тока горизонтального проводника связи (в виде стальной полосы шириной (b)), соединяющего верхние концы вертикальных электродов из выражения,

Rr=рр/(6,28\*L)\*ln(2\*l2/b) , Ом (8.8)

Тогда

Rr=300/(6,28\*3)\*ln(2\*52,52/0,05)=84 Ом.

Результирующее сопротивление искусственного группового заземлителя будет равно,

Rи=Rв\*Rr/ (Rв\**n*г+Rr\**n*в\*n), Ом (8.9)

Тогда

Rи=20\*84/(20\*0,84+84\*0,77\*6)=4,14 Ом

При использовании естественного заземлителя параллельно с искусственным даст нужный результат и сопротивление заземляющих проводников не превысит требуемого значения.

Итак: проектируемый заземлитель состоит из 6 вертикальных стержневых электродов длиной по 2 метра и диаметром 10мм и горизонтального электрода в виде стальной полосы длиной 52 метра углубленных в землю (грунт). При таких условиях Rи искусственного заземлителя в самое неблагоприятное время года не превышает 4,14 Ом, при требуемом сопротивлении 4 Ом. Можно сказать, что проектируемый заземлитель соответствует требованиям электробезопасности.

Заключение

В заключении можно отметить, что проектируемая автоматизированная система защиты и контроля доступа в помещения позволяет решить все возникающие вопросы при организации ограниченного доступа на объект подлежащий защите. Она может применятся как в административных зданиях, так и на крупных предприятиях, везде где требуется организация высокого пропускного режима.

Применение таких мощных электронных средств как: электронный идентификатор, микроконтроллер серии 80С51, радиомодем TXM433F, компьютер позволяют создать мощную локальную сеть по обеспечению безопасности людей на контролируемой системой объекте.

Система производит не только идентификацию и аутентификацию пользователей, но и контроль доступа к ресурсам системы. СЗКДП постоянно производит регистрацию и анализ событий происходящих внутри системы, ведет протокол функционирования всего комплекса защиты.

Обеспечение комплексной безопасности на объекте подлежащем защите на основе проектируемой СЗКДП, позволяет создавать препятствия для любого несанкционированного вмешательства в процесс ее функционирования, а также попыток выведения или разрушения ее компонентов. То есть защиту всех компонентов системы оборудования, программного обеспечения, данных и персонала.

Cписок литературы

1. Хвощ С.Т. Организация последовательных мультиплексных каналов систем автоматического управления - Л.:Машиностроение,1989
2. Сташин В.В. Проектирование цифровых устройств на однокристальных микроконтроллерах - М.:Энергоатомиздат,1990
3. Лебедев О.Н. Изделия электронной техники. Цифровые микросхемы. Микросхемы памяти. Микросхемы ЦАП и АЦП: Справочник - М.: Радио и связь, 1994
4. Апорович А.Ф. Проектирование радиотехнических систем: Учебное пособие. - Мн.: Выш. шк., 1988
5. Халсалл Ф. Передача данных, сети компьютеров и взаимосвязь открытых систем: Пер. с англ. - М.: Радио и связь, 1995
6. Бергхаузер Т. Система автоматизированого проектирования AutoCAD: Справочник: Пер с англ. - М.: Радио и связь, 1989
7. Долин П. А. Основы техники безопасности в электроустановках: Учебное пособие для вузов. - М. Энергоатомиздат, 1984
8. Михнюк Т.Ф. Задачи и расчеты по охране труда по курсу “Охрана труда” для студентов радиотехнических и приборостроительных специальностей. В двух частях. Защита от электрического тока. - БГУИР, 1994
9. Каган Б.М. Основы проектирования микропроцессорных устройств автоматики. - М.: Энергоатомиздат, 1987
10. Гольденберг Л.М. Цифровые устройства и микропроцессорные системы: Учебное пособие для вузов. - М.: Радио и связь, 1992
11. Фролкин В.Т. Импульсные и цифровые устройства: Учубное пособие для вузов. - М.: Радио и связь, 1992
12. Ходасевич Р. Г. Методическое пособие по дипломному проектированию. - Минск , 1980.
13. ГалкинВ.И. , Булычев А.Л. , Прохоренко В.А. Полупроводниковые приборы : Справочник - Минск `` Беларусь `` , 1987.
14. Общесоюзные нормы технологического проектирования ОНТП 24-86.
15. ГОСТ 12.2.006-87. ( МЭК 65-85 ) Безопасность аппаратуры электронной сетевой и сходных с ней устройств , предназначенных для бытового и аналогичного общего применения. Общие требования и методы испытаний.
16. ГОСТ 12.2.007.0-75. ССБТ. Радиопомехи индустриальные. Методы испытаний источников индустриальных радиопомех.
17. ГОСТ 2.144-70. ТУ. Правила построения , изложения и оформления.
18. ГОСТ 29037-91. Совместимость технических средств электромагнитная. Сертификационные испытания. Общие положения.
19. ГОСТ 27570.0-87. Безопасность бытовых и аналогичных электроприборов. Общие требования и методы испытаний.
20. Селиванов Н.Р. Электроника в криминалистике.-- Москва, 1979.
21. Touch Memory Standards.-- Dallas Semiconductor Corporation , Dallas, Texas , USA , 1994.
22. Афитов Э.А. Учебное пособие : Организация и планирование производства. - Мн. : МРТИ , 1992.
23. Варламов Р.Г. Справочник конструктора РЭА. - М. : Радио и связь , 1987.
24. Рафикузаман М. Микропроцессоры и машинное проектирование микропроцессорных систем : В 2-х кн. - М. : Мир , 1988.
25. Шевкопляс Б.В. Микропроцессорные структуры. Инженерные решения : Справочник. М. : Радио и связь , 1990.
26. Хоровиц П. , Хилл У. Искусство схемотехники : В 3-х томах. - 4-е изд. перераб. и доп. - М. : Мир , 1993.
27. Кобылинский А.В. , Сабадаш Н.Г. , Тесленко А.К. Система автоматизации программирования однокристальной микроЭВМ. - Микропроцессорные средства и системы, 1986, №3.
28. Кушнир В.Е. , Панфилов Д.И. , Шаронин С.Г. - Учебная микроЭВМ на основе однокристальной ЭВМ КМ1816ВЕ48. - Микропроцессорные средства и системы , 1986 , №6.
29. Р 50-34.119-90. Рекомендации.Информационная технология. Комплекс стандартов на автоматизированные системы. Архитектура локальных вычислительных сетей в системах промышленной автоматизации. Общие положения.
30. ГОСТ 34.602-89. Информационная технология. Техниеское задание на создание автоматизированной системы.
31. РД 50-682-89. Методические указания. Информационная технология. Общие положения.
32. ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные ситемы. Автоматизированные системы.
33. Общеотраслевые руководящие методические материалы по созданию и применению автоматизированных систем управления. (ОРММ-3АСУ ТП). М.: Государственный комитет СССР по науке и технике. 1986
34. ГОСТ 34.003-90.Информационная технология. Комплекс стандартов на автоматизированные ситемы. Автоматизированные системы. Термины и положения.
35. Р 50-34.119-90. Рекомендации.Информационная технология. Комплекс стандартов на автоматизированные системы. Архитектура локальных вычислительных сетей в системах промышленной автоматизации. Общие положения.
36. ГОСТ 26342-84. Средства охранной, пожарной и охраннопожарной-сигнализации. Типы, основные параметры и размеры.
37. 5. ГОСТ 12.2.006-87. (МЭК 65-85). Безопасность аппаратуры
38. электронной сетевой и сходных с ней устройств, предназначенных для бытового и аналогичного общего применения. Общие требования и методы испытаний.
39. 6. ГОСТ 12.2.007.0-75. ССБТ. Радиопомехи индустриальные. Методы испытаний источников индустриальных радиопомех.
40. ГОСТ Р50009-92. Совместимость технических средств охранно-пожарной сигнализации электромагнитная. Нормы и методы испытаний.
41. ГОСТ 4.188-85. СПКП. Средства охранно-пожарной сигнализации. Номенклатура показателей.
42. ГОСТ 2.144-70. ТУ. Правила построения, изложения и оформления.
43. ГОСТ 29037-91. Совместимость технических средств электромагнитная. Сертификационные испытания. Общие положения.
44. 11.ГОСТ 27570.0-87. Безопасность бытовых и аналогичных электроприборов. Общие требования и методы испытаний.
45. ГОСТ 251099-83. Средства пожарной, охранной сигнализацииОбщие технические требования и методы испытаний.
46. ГОСТ 16325-88. Машины вычислительные цифрового общего назначения. Общие технические требования.
47. СНиП 3.05.07-85. Системы автоматизации.
48. ГОСТ 24.602-86. Надежность автоматизированых систем управления. Основные положения.

Приложение 1

СТАНДАРТ I-ETS 300 220

В 1993 году Технический Комитет по Радиооборудованию и Системам европейского Института Телекоммуникационных Стандартов разработал и провел утверждение Временного Европейского Стандарта Телекоммуникаций (Interim European Telecommunication Standard, I-ETS).

Данный стандарт, получивший обозначение I-ETS 300 220, регламентирует технические характеристики и способы их измерения для радиооборудования, работающего в диапазоне частот от 25 до 1000 Мгц со всеми видами модуляции, исключая системы множественного доступа с кодовым разделением, и имеющего мощность до 500 мВт,

На работу приборов класса 1.а стандарт I-ETS 300 220 накладывает следующие ограничения:

- максимальная эффективная излучаемая мощность.........10 мВт

- тип используемой антенны**......................................**.встроенная

- уровень внеполосных излучений передатчика:

- в диапазонах 47...74 МГц, 87.5...118 МГц, 174...230 МГц, 470...862 МГц..........................................................4 нВт

- в других диапазонах до 1000 МГц...............**............**...250 нВт

- на частотах свыше 1000 МГц...**...............**.......................1 мкВт

- температурный диапазон проведения тестов........-25...+55 о С