

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра «Информационная
безопасность систем и технологий»

Специальность 10.05.03 –

Информационная безопасность
автоматизированных систем

Специализация –

Защищенные автоматизированные
системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

УСТРОЙСТВО ДЛЯ ВВОДА КЛЮЧЕВОЙ ИНФОРМАЦИИ С КОМПАКТ
ДИСКА И РОССИЙСКОЙ ИНТЕЛЛЕКТУАЛЬНОЙ КАРТЫ

Студент

Привалова Ирина Андреевна

Руководитель

Родионов Е.Ф.

Нормоконтролёр

Иванов А.П.

Рецензент начальник НИО «АО ПНИЭИ»

Оськин Р.С.

Работа допущена к защите (протокол заседания кафедры от 21.06.19 № 16)

Заведующий кафедрой

С.Л. Зефирова

Работа защищена с отметкой

хорошо

(протокол заседания ГЭК

от 25.06.19 № 25)

Секретарь ГЭК

А.П. Иванов

Пенза 2019

Проверка (предзащита)

10 баллов б.с.

21.06.19.

Оглавление

Введение.....	5
1 Анализ состояния рассматриваемой технической проблемы.....	10
1.1 Актуальность разработки устройства ввода ключевой информации.....	10
1.2 Требования, предъявляемые к разрабатываемому средству ввода ключевой информации.....	10
2 Изучение протокола взаимодействия с портативным приводом для чтения компакт- дисков по USB интерфейсу.....	12
2.1 Изучение строения CD диска и устройств для считывания информации с оптического носителя.....	12
2.2 Изучение протокола взаимодействия с портативным приводом для чтения компакт-дисков по USB интерфейсу.....	15
2.3 Изучение файловой системы CDFS (ISO 9660).....	17
3 Изучение протокола взаимодействия с российской интеллектуальной картой.....	20
3.1 История создания РИК.....	20
3.2 Операционная система РИК.....	24
3.3 Основные характеристики РИК-2.....	26
4 Файловая система российской интеллектуальной карты.....	28
5 Разработка схемы электрической структурной устройства ввода ключевой информации	32
6 Выбор и обоснование элементной базы для построения устройства ввода ключевой информации.....	35

7	Разработка алгоритма работы устройства ввода ключевой информации	38
7.1	Алгоритм работы устройства ввода ключевой информации.....	38
7.2	Программный модуль реализующий ППК.....	39
7.3	Программный модуль инициализации аппаратной части.....	40
7.4	Модуль UART.....	40
7.5	Модуль для работы по USB интерфейсу.....	41
7.6	Программный модуль, реализующий взаимодействие с РИК.....	43
7.7	Программный модуль, реализующий взаимодействие с головным устройством.....	43
8	Разработка протокола взаимодействия с устройством ввода ключевой информации.....	45
9	Разработка схемы электрической принципиальной устройства ввода ключевой информации.....	54
10	Разработка программного обеспечения устройства ввода ключевой информации.....	55
10.1	Описание разработки программного кода.....	55
10.2	Описание файлов проекта.....	56
11	Разработка методики тестирования устройства при его изготовлении, а также его контроля ОТК предприятия-изготовителя и представителем заказчика на предприятии.....	58
11.1	Требования к контейнеру.....	58
12	Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....	66
	Заключение.....	71
	Список используемых источников.....	72

Приложение А.....	73
Приложение Б.	75
Приложение В.	78

Введение

Проблема защиты информации путем ее изменения, исключаящего ее прочтение посторонним лицом долгое время была проблемой для человеческого разума. История криптографии совпадает с историей человеческого языка. Кроме того, сам оригинальный текст представлял собой форму криптографической системы, поскольку в древних обществах она принадлежала только избранным.

Первый период (приблизительно с 3-го тысячелетия до н.э.) характеризуется господством моноалфавитных шифров (основной принцип - замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами).

Второй период (хронологические рамки - с IX века на Ближнем Востоке (Ал-Кинди) и с XV века в Европе (Леон Баттиста Альберти) - до начала XX века) ознаменовался применением полиалфавитных шифров.

Третий период (с начала и до середины XX века) характеризуется внедрением электромеханических устройств в работу шифровальщиков. При этом продолжалось использование полиалфавитных шифров.

Четвёртый период - с середины до 70-х годов XX века - период перехода к математической криптографии. В работе Клода Шеннона появляются строгие математические определения количества информации, передачи данных, энтропии, функций шифрования. Обязательным этапом создания шифра считается изучение его уязвимости к различным известным атакам - линейному и дифференциальному криптоанализу. Однако до 1975 года криптография оставалась «классической», или же, более корректно, криптографией с секретным ключом.

Современная эра развития криптографии (с конца 1970-х годов до настоящего времени) характеризуется появлением и развитием новых направлений - криптографии, криптография с открытым ключом. Его внешний вид проявляется не только в новых технических возможностях, но и в

использовании криптографии для использования частными лицами (в прежние времена использование криптографии было единственным подходящим для правительства). Правовой контроль за использованием криптографии и частных лиц в разных странах очень отличается - от разрешения до полного запрета.

В криптосистеме, в которой применяется симметричная криптография (Американский и Российский стандарты шифрования DES и ГОСТ28.147-89), отправитель и получатель используют два экземпляра одного и того же ключа для зашифрования и расшифрования информации. Таким образом, ключ имеет двойную функциональность и применяется как в процессе зашифрования, так и в процессе расшифрования. [1]

Симметричные ключи также называют секретными ключами, потому что этот тип шифрования считает, что каждый пользователь хранит ключ в секрете и хорошо его защищает. Если злоумышленник получит этот ключ, он сможет расшифровать с его помощью любое перехваченное зашифрованное на нем сообщение.

При использовании алгоритмов синхронизации отправитель и получатель используют один и тот же ключ зашифрования и расшифрования.

Безопасность таких алгоритмов зависит от того, как пользователи должны защищать ключи. В этом случае безопасность полностью зависит от работников, которые должны скрывать свои ключи. Если ключ скомпрометирован, все сообщения, скрытые в этом ключе, могут быть расшифрованы и прочитаны злоумышленником. На самом деле, это более сложно, потому что ключи необходимо безопасно распространять и обновлять при необходимости. Процесс распределения симметричных ключей может быть очень сложной задачей.

Поскольку все пользователи используют один и тот же ключ для зашифрования и расшифрования сообщений, симметричные криптосистемы могут обеспечить конфиденциальность, но не аутентификацию или неотказуемость. Этот алгоритм не позволит вам проверить, кто на самом деле

отправил сообщение, поскольку два пользователя используют один и тот же ключ.

Система симметричных алгоритмов быстрее, чем асимметричная. Они могут быстро зашифровывать и расшифровывать большие объемы данных. Кроме того, данные, зашифрованные симметричным алгоритмом с использованием длинного ключа, очень сложно вскрыть.

Необходимость разработки систем с использованием современных информационных технологий на основе микропроцессорных пластиковых карт сегодня ни у кого не вызывает сомнений. Интеллектуальные карты (смарт-карты) и большой потенциал эффективно используются не только для хранения важной информации, но также широко используются в электронных платежных системах, в интегрированных решениях для медицины, транспорта, связи, образования и т. д.

Компакт - диски представляют наиболее распространенный тип носителя ключевой информации. Применение оптического диска в качестве носителя ключа позволяет реализовать необходимое свойство отчуждаемости носителя ключа от защищенной информационной системы, т.е. осуществлять временное изъятие диска из состава технических средств компьютерной системы. Для предотвращения возможности перехвата ключевой информации в процессе ее чтения с диска применяется хранение ключевой информации в зашифрованном виде.

Таким образом целью данной работы является анализ решений для разработки устройства для ввода ключевой информации с компакт-диска и российской интеллектуальной карты.

Для выпускной квалификационной работы была выбрана тема «Устройство для ввода ключевой информации с компакт диска и российской интеллектуальной карты». Сведения, составляющие государственную тайну, в пояснительной записке к дипломному проекту отсутствуют.

Первый раздел дипломного проекта посвящен анализу состояния рассматриваемой технической проблемы.

Второй раздел содержит изучение протокола взаимодействия с портативным приводом для чтения компакт- дисков по USB интерфейсу

В третьем разделе проанализирована файловая система CDFS (ISO 9660).

Четвертый раздел посвящен изучению протокола взаимодействия с российской интеллектуальной картой.

Пятый раздел содержит посвящен файловой системе российской интеллектуальной карты.

Шестой раздел посвящен разработке схемы электрической структурной устройства ввода ключевой информации.

Седьмой раздел содержит выбор и обоснование элементной базы для построения устройства ввода ключевой информации.

Восьмой раздел посвящен разработке алгоритма работы устройства ввода ключевой информации.

Девятый раздел содержит разработку протокола взаимодействия с устройством ввода ключевой информации.

Десятый раздел посвящен разработке схемы электрической принципиальной устройства передачи зашифрованной информации.

Одиннадцатый раздел содержит разработку программного обеспечения устройства ввода ключевой информации.

В двенадцатом разделе описана методики тестирования устройства при его изготовлении, а также его контроля ОТК предприятия-изготовителя и представителем заказчика на предприятии.

Тринадцатый раздел включает в себя вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.

1 Анализ состояния рассматриваемой технической проблемы

1.1 Актуальность разработки устройства ввода ключевой информации.

Развитие информационных технологий привело к появлению проблемы хранения закрытой информации. Та же ситуация возникает при авторизации пользователя на компьютере. Незащищенный пароль может попасть к злоумышленнику, и вся система будет скомпрометированной.

В настоящее время ввод ключевой информации в аппаратуру выполняется через ПЭВМ под управлением ОС Windows. В данной работе предлагается разработать устройство для ввода ключей на базе микроконтроллера. Данное устройство позволит обеспечить доверенную среду для ввода ключевой информации и исключить из состава аппаратуры ПЭВМ.

1.2 Требования, предъявляемые к разрабатываемому средству ввода ключевой информации

Технические требования:

- устройство должно обеспечивать ввод ключевой информации с компакт диска с файловой системой ISO 9660 и контроль ее целостности при передаче;
- устройство должно обеспечивать ввод ключевой информации с РИК и контроль ее целостности при передаче;
- взаимодействие с устройством должно выполняться по интерфейсам USB и UART;
- для работы по протоколу USB в устройстве должны быть реализованы драйверы для работы по профилям VCP (фирменный профиль ф. FTDI) и CDC (стандартный профиль виртуального COM-порта);
- работа по интерфейсу по UART порту должна выполняться на скорости 115200 кбит/с;

- исходный код программного обеспечения устройства должен быть полностью доступен для проведения его анализа на отсутствие недокументированных возможностей;
- в программном обеспечении устройства должен быть реализован предпусковой контроль, включающий в себя тестирование ОЗУ и проверку целостности программного обеспечения криптографическим способом по ГОСТ Р 34.13-2015;
- устройство должно обладать автономным источником питания, обеспечивающим питание устройства и подключаемого к нему привода для чтения компакт дисков и РИК;
- должны быть проработаны требования для контейнера, используемого при транспортировке и хранении устройства;
- должна быть разработана методика тестирования устройства при его изготовлении, а также его контроля ОТК предприятия-изготовителя и представителем заказчика на предприятии.

2 Изучение протокола взаимодействия с портативным приводом для чтения компакт- дисков по USB интерфейсу

2.1 Изучение строения CD диска и устройств для считывания информации с оптического носителя

Компакт-диск (Compact Disk, CD) представляет собой диск диаметром 120 мм (4,75 дюйма) или 80 мм (3,1 дюйма) и толщиной 1,2 мм.

Для считывания информации с компакт-диска используется лазерная головка (ЛГ), расположенная в приводе для чтения компакт дисков. В корпусе ЛГ установлены лазерный диод, внутренняя оптическая система (дифракционная решетка, цилиндрическая, коллиматорная и другие линзы, призма), катушки фокусировки и трекинга с фокусирующей линзой, лазерный диод. Конструкция лазерной головки представлена на рисунке 1.

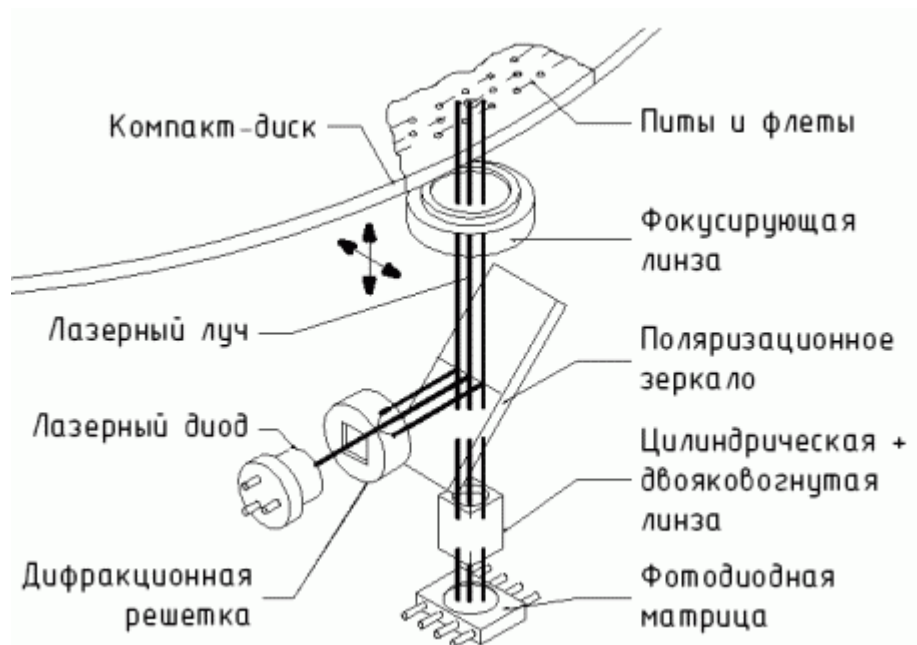


Рисунок 1 - Конструкция лазерной головки

При подаче напряжения питания полупроводниковый лазерный диод генерирует когерентный (разность фаз волн постоянна во времени) луч, который с помощью дифракционной решетки разделяется на основной луч и два дополнительных. Пройдя через элементы оптической системы и

фокусирующую линзу, эти лучи попадают на компакт-диск. Точную фокусировку лучей на диске осуществляют катушки фокусировки, устанавливающие нужное положение линзы. Отразившись от диска, лучи снова попадают на фокусирующую линзу и дальше в оптическую систему. При этом отраженные лучи отделяются от падающих благодаря их разной поляризации.

Далее отраженные лучи попадают на фотодатчики, где декодируются встроенным микроконтроллером в поток данных, пригодный для дальнейшей обработки. Считанные данные передаются в различные устройства через внешний интерфейс привода компакт диска.

В настоящее время приводы для чтения компакт дисков можно разделить на внутренние и внешние.

Внутренние приводы подключаются к устройствам через IDE, SCSI и SATA интерфейсы.

IDE — параллельный интерфейс подключения накопителей (жёстких дисков (HDD), приводов (CD/DVD-ROM)). Разработан фирмой Western Digital, позднее стал именоваться ATA или PATA. Для подключения жёстких дисков с интерфейсом IDE обычно используется 40- или 80-проводный кабель (шлейф). Максимальная пропускная способность 150 МБ/с.

SATA (Serial ATA) - интерфейс обмена данными и устройства хранения данных (жесткий диск (HDD), привод (CD / DVD-ROM)), является развитием параллельного интерфейса ATA (IDE), который после появления SATA был назван PATA (Parallel ATA). Основным преимуществом SATA на PATA является использование последовательной шины вместо параллельной. Несмотря на то, что метод последовательного преобразования медленнее соответствующего, в этом случае он компенсируется способностью работать на высокой частоте из-за большей защиты кабеля. Это успешно с небольшим количеством проводников в де витые пары, экранированные заземленными проводниками. [2]

SCSI - это интерфейс, разработанный для объединения устройств различного назначения, таких как жесткие диски, магнитооптические

накопители, ленточные накопители и т. Д. Интерфейс предназначен для интеграции мультиклассовых устройств: памяти прямого и последовательного доступа, CD-ROM, оптических дисков однократной и многократной записи, устройств автоматической смены носителей информации, принтеров, сканеров, коммуникационных устройств и процессоров. Он используется в различных архитектурах компьютерных систем, а не только на ПК. Стандарт определяет не только физическую связь, но и систему команд, управляющих оборудованием SCSI. За время существования стандарт активно развивался.

На данный момент USB является основным интерфейсом подключения внешних накопителей.

Спецификация шины USB позволяет подключать периферийные устройства с автоматической установкой, когда физическое устройство подключено к шине. Нет необходимости перезагружать или устанавливать компьютер, а также запускать программы установки и настройки. Для исправления одной ошибки на линии используется циклический код CRC. В настоящее время большинство внешних приводов CD-дисков работают в соответствии с настройками USB2.0. [3]

На основании анализа приведённой выше информации можно рассмотреть несколько вариантов решения задачи по считыванию информации с компакт диска:

- 1) разработка собственного привода чтения компакт-дисков;
- 2) разработка устройства со встроенным приводом с одним из описанных интерфейсов;
- 3) разработка устройства, к которому будет подключаться внешний привод по USB интерфейсу;
- 4) использование ПЭВМ с установленным приводом.

Первый вариант не подходит по причине своей технической сложности. Второй вариант проигрывает третьему и четвёртому из-за необходимости вносить в устройство дополнительный контроллер управления интерфейсом.

При использовании USB интерфейса может быть использован один микроконтроллер, который обеспечит как работу по USB интерфейсу, так и выполнение других функций устройства. При использовании ПЭВМ для чтения информации с компакт-диска может использоваться ПО, установленное в ОС.

2.2 Изучение протокола взаимодействия с портативным приводом для чтения компакт-дисков по USB интерфейсу

В соответствии со спецификацией USB 2.0 устройства для чтения компакт-дисков относятся к Mass Storage Class (дословно классу массового хранения). К данному классу относятся устройства обеспечивающие передачу файлов в одном или двух направлениях.

Помимо устройств чтения компакт-дисков к данному классу так же относятся внешние жёсткие диски и USB-флэшки. Рассмотрим более подробно принципы работы устройств по USB шине.

USB-шина содержит четыре проводника: два — витая пара, питание 5 В и общий провод.

Таким образом, устройства подключенные к интерфейсу разделяют одну сигнальную линию.

USB протокол обеспечивает обмен данными между хост-устройством и множеством периферийных устройств. В момент подключения хост запрашивает у устройства ряд стандартизованных сведений (дескрипторов), на основании которых принимает решение, как с этим устройством работать. Дескрипторы содержат сведения о производителе и классе устройства, на основании которых хост подбирает программный драйвер. Так же при этом каждому периферийному устройству хост назначает свой адрес, через который выполняется дальнейшее обращение к устройству со стороны хоста. Так же хост выполняет при подключении процедуру согласования скоростей с устройством.

Обмен данными происходит так называемыми транзакциями — неразрывными последовательностями из нескольких пакетов. Инициатором обмена всегда является хост.

Он передаёт короткий пакет (token), уведомляющий о начале новой транзакции. В этом пакете-токене хост указывает направление транзакции (IN или OUT), адрес устройства и номер конечной точки. Пакетов с данными может быть несколько в одной транзакции, если каждый из них имеет максимально допустимую для этого устройства длину данных.

Окончание пересылки данных определяется по длине пакета, не равной максимальной.

Как только приходит укороченный пакет, устройство немедленно передаёт ответный пакет-подтверждение (handshake), например ACK (всё успешно принято), NACK (не смог принять: например, переполнен входной буфер), STALL (данные адресованы отключённому endpoint).

Аналогично происходит передача данных от устройства к хосту. Хост инициирует передачу токеном IN. Если устройство не имеет готовых данных для передачи, то отвечает NACK и транзакция заканчивается. Если данные готовы, устройство начинает передавать пакеты. Принцип окончания передачи аналогичен: неполная длина пакета с данными. Получив неполный пакет, хост отвечает устройству пакетом-подтверждением ACK.

Транзакция с токеном SETUP полностью аналогична транзакции OUT, отличия лишь в логике восприятия данных устройством: это параметры соединения, которые управляют работой USB стека устройства.

Спецификация USB предоставляет несколько методов обмена данными.

Метод bulk позволяет хосту свободно обмениваться данными с устройством по своему усмотрению.

Метод control аналогичен bulk, но обменивается с устройством только специальными данными, управляющими работой USB-протокола в соответствии со спецификацией (в рамках транзакций типа SETUP). Поскольку

периферийные устройства не могут инициировать обмен, то для передачи внезапно возникающих у устройства данных придумали метод interrupt, который позволяет опрашивать устройство с заданным периодом. Метод interrupt широко применяется для опроса клавиатур и мышек.

Особняком стоит метод isochronous, позволяющий зарезервировать часть полосы пропускания USB-шины для таких данных, как аудио или видео. Isochronous не поддерживает контроля целостности передачи (пакеты ACK и NACK не передаются), а значит, не предусмотрены повторы в случае ошибок: неверно принятые данные пропадают. [4]

Устройство чтения компакт дисков используют метод bulk. При использовании данного метода USB хост может посылать команды и получать ответы используя передачу массивов данных, определенную в спецификации USB. В протоколе передачи только массивов данных каждый обмен информацией требует 2 или 3 USB передач данных. В первой передаче хост посылает команду в структуре, называемой CBW (Command Block Wrapper). За множеством CBW следует передача, которая содержит данные, посылаемые хостом или устройством. В последней передаче устройство возвращает статус в структуре, называемой CSW (Command Status Wrapper). Формат структур команд описан в стандарте SCSI Multi-Media Commands – 5 (MMC-5).

2.3 Изучение файловой системы CDFS (ISO 9660)

Международный стандарт ISO 9660 описывает файловую систему на компакт- дисках . ISO 9660 первого уровня напоминает файловую систему MS-DOS: имена файлов могут содержать до восьми символов, расширение имени файла (состоящее из трех символов) отделяется от имени файла точкой. Имена файлов не могут содержать специальных символов (" ", "~", "=", "+"). При именовании файлов используются символы только верхнего регистра, цифры и символ "_". Имена каталогов не могут иметь расширений. Каждый файл имеет версию - номер версии отделяется от расширения символом ";". Каталоги могут

иметь глубину вложенности 8. Стандарт ISO 9660 второго уровня позволяет использовать в именах файлов до 32 символов, накладывая описанные выше ограничения. Диски, созданные с использованием такого стандарта, не могут использоваться в ряде операционных систем, включая и MS-DOS.

Отметим, что для большинства компакт-дисков вся хранимая впоследствии на них информация заносится за один технологический цикл, или сеанс (single session).

Основными элементами файловой структуры CD-ROM являются:

- первичный дескриптор тома (PVD - Primary Volume Descriptor); он всегда находится в шестнадцатом секторе сеанса и содержит ссылки на таблицу путей (PT — Path Table) и корневой каталог (RD - Root Directory);
- таблица путей (PT) содержит адреса каталогов (DF - Directory Files).

Если файловая структура охватывает более одного сеанса, то ссылки из корневого каталога последующих сеансов включают в себя ссылки на каталоги предыдущих сеансов и таким образом каталоги предшествующих сеансов становятся доступными в последующих сеансах. На этом базируется возможность обновления файлов. Несмотря на невозможность стирания, эффект "перезаписи" сохраняется для пользователя: это достигается путем перезаписи в последующем сеансе каталогов, содержащих ссылки на замещаемый файл. Файл, разумеется, также записывается в последующем сеансе, и в новую редакцию каталога включается ссылка на него. При стандартном доступе к файлам будут использоваться ссылки из корневого каталога последнего сеанса, и файл будет выглядеть обновленным, хотя возможность доступа к предшествующей версии при помощи специальной ссылки сохранится. [5]

Возможен также вариант, когда записываемый позже сеанс является независимым, в этом случае ссылки на сеансы будут аналогичны ссылкам на различные разделы физического диска. Для нормальной работы файловой системы с CD-R весьма желателен накопитель, "понимающий" многосеансовые

диски. Проверить, обладает ли накопитель такими способностями, легко - достаточно посмотреть каталог многосеансового диска: примитивный проигрыватель "увидит" только каталоги и файлы первого сеанса.

3 Изучение протокола взаимодействия с российской интеллектуальной картой.

3.1 История создания РИК

Необходимость разработки систем с использованием современных информационных технологий на основе микропроцессорных пластиковых карт сегодня не вызывает сомнений. В течение ряда лет специалистами ФАПСи (ФСБ) проводились работы с целым рядом западных фирм – производителей микропроцессоров и карт, такими, как Gemplus Card International, Siemens AG, Motorola, Giesecke&Devrient, по созданию российского варианта интеллектуальных карт с использованием зарубежных кристаллов с отечественными криптографическими алгоритмами. Следует отметить, что иностранные компании выпускают кристаллы и карты, подробно публикуют список потребительских характеристик, однако отдельные особенности классифицируются как конфиденциальная информация. Важная часть специфических функций, таких как правила, не раскрывается, что делает невозможным проверку надежности кредитных карт и их сертификатов для конкретных требований.

Таким образом, государственная политика в сфере информатизации потребовала создания и организации серийного выпуска российских интеллектуальных карт, обеспеченных надежной защитой и криптографической компонентой на основе отечественных стандартов. Возникла необходимость в создании карты, которую можно было бы применять в прикладных системах различного уровня, начиная с локальных и кончая общенациональными системами.

Разработанный RIC имеет технические и достаточные функции для многих приложений. Он построен на основе оригинальной архитектурной обработки RISC, производительность которой обеспечивает доступ к скорости шифрования до 5 кБ / с при реализации алгоритма шифрования ГОСТ 28147-89

в сохраненной версии. Микроконтроллер имеет 2 КБ энергонезависимой памяти (EEPROM), 8 КБ постоянной памяти (ПЗУ) и 256 байт ОЗУ (RAM).

Система информационной безопасности РИК основывается на системе физической безопасности кристалла микроконтроллера и дополняется программно-алгоритмическими мерами защиты, реализованными в составе криптографического модуля и операционной системы.

Средствами операционной системы РИК реализуются алгоритмические меры защиты, такие, как тестовые проверки при включении питания карты, криптографическая защита данных, контроль их целостности, и др.

Криптографическая компонента операционной системы помимо ГОСТ 28147-89 включает также алгоритмы DES и Triple-DES. В карте имеется встроенный программно-аппаратный датчик случайных чисел, обеспечивающий поддержку со стороны РИК надежных криптографических протоколов взаимной аутентификации и выработку разовых сеансовых ключей шифрования данных для взаимодействия с терминальным оборудованием.

По своим функциональным возможностям и уровню защиты от несанкционированного доступа к хранимой информации РИК в целом не уступает своим зарубежным аналогам. Технические характеристики российской карты обуславливают весьма широкий спектр областей ее возможного использования. Кратко рассмотрим перспективы применения РИК в системах для решения задач по защите информации.

Интеграция РИК в качестве носителя идентификационной информации в средства разграничения доступа к ресурсам информационных систем (в дополнение или вместо пароля, вводимого с клавиатуры терминала) позволит существенно повысить уровень защиты ресурсов, так как в отличие от пароля хранящаяся в РИК информация надежно защищена от несанкционированного доступа при случайных или злоумышленных действиях индивида, использующего РИК. При этом программно-аппаратные средства РИК гарантируют передачу идентификационной информации из РИК в терминал

(режим offline) или на удаленный сервер системы (режим online) только в случае положительного результата их взаимной аутентификации в соответствии с поддерживаемыми операционной системой РИК надежными криптографическими протоколами. Применение персональных карточек для доступа к ресурсам позволяет осуществлять динамический контроль работы пользователя и в случае его отсутствия или перерыва в работе (т.е. когда карточка вынимается пользователем из приемного устройства) блокировать доступ.

Применение микропроцессорных карт позволяет в числе других обеспечить следующие существенные возможности:

- взаимную достоверную аутентификацию (опознавание) пользователя карточки и контрольного устройства (электронного замка, пропускного терминала или турникета и т.п.);
- шифрование информации, передаваемой между карточкой и контрольным устройством, так, что наиболее конфиденциальная часть данных никогда не покидает памяти карты в открытом виде и не может быть перехвачена злоумышленником;
- абсолютно достоверную регистрацию администратором безопасности системы всех входов-выходов на охраняемую территорию, при этом в контрольные журналы (файлы или память устройства) записываются все данные пользователя карточки, точное время прохода и т.п.;
- автоматическую подачу сигналов “тревога” при попытках несанкционированного проникновения на охраняемые территории;
- режим скрытой сигнализации о “проходе под контролем”, который означает, что лицо, обладающее правом доступа, действует по приказу злоумышленника;
- режим скрытой дистанционной блокировки (вывода из действия) карточки пользователя, лишённого полномочий доступа;

- системы контроля доступа на основе интеллектуальных карт дают возможность вводить различные иерархии доступа к охраняемым объектам и территориям, позволяя выделенным группам пользователей проходить только в разрешенные им зоны и только в определенные интервалы времени в течение заданного периода (сутки, недели, месяцы, праздничные дни, годы и т.д.);
- защищенное хранение паролей и секретных ключей на карте, что делает безопасной для системы в целом утерю пользовательской карточки.

Реализация указанных возможностей путем применения других средств контроля (не интеллектуальных карт) требует наличия существенно более дорогих и сложных электронных устройств и линий связи.

Использование РИК в качестве носителя ключевой информации связано с развитием сетевых и телекоммуникационных технологий. В настоящее время в системах передачи данных наблюдается тенденция к переходу на принцип абонентского засекречивания или “точка-точка”, при котором шифратор и ключевые носители находятся непосредственно в распоряжении абонента. В этих условиях существенно расширяется круг людей, допущенных к ключевым документам, и использование незащищенных ключевых носителей типа магнитных дисков или карт с магнитной полосой может привести к компрометации конфиденциальной информации за счет утраты таких ключей или их незаконного копирования. Одним из решений проблемы является применение алгоритмически и физически защищенных от НСД ключевых носителей.

Проведенные специалистами исследования показали, что разработанные и интегрированные в программно-аппаратную среду РИК меры защиты, а также специальные свойства кристалла позволяют обеспечить надежную защиту ключевых носителей на базе РИК.

Использование новых документов-пропусков, созданных на основе пластиковых карт со встроенным микроконтроллером, позволяет применить современные информационные криптографические технологии,

обеспечивающие высокий уровень защиты от подделки таких пропусков и дополнительные охранные функции, в частности создание зон различного уровня доступа и мониторинга находящихся в них лиц.

На карту полиграфически наносятся реквизиты владельца пропуска, права доступа, его фотография. В память карты также заносятся реквизиты, права доступа и цифровая фотография, подписанные электронной цифровой подписью.

Требования в части информационной безопасности РИК, используемых в качестве электронных документов, аналогичны применению РИК в качестве платежного средства.

При этом в ходе разработки конкретных систем, использующих электронные документы, должны быть предприняты организационные меры безопасности, аналогичные тем, что применяются в платежных системах.

Перспективы развития РИК в настоящее время связаны с развитием технологии производства микроэлектроники в Ангстреме. Особое место занимает эффективная работа по внедрению программного обеспечения и оборудования в микроконтроллере РИК, что позволяет реализовать эффективные алгоритмы асимметричных алгоритмов, в частности, цифровую подпись ГОСТ Р-34.10. Использование маленьких детей может стать одним из технических решений проблемы создания частных средств массовой информации для системы цифровой сертификации по данным внутренней криптографии, позволит повысить безопасность обмена информацией в Интернете и обеспечить надежное решение в области электронной коммерции.

3.2 Операционная система РИК

Ядром интеллектуальной карты является операционная система (ОС).

Операционная система РИК-2 обеспечивает:

- возможность односторонней и взаимной аутентификации карты и внешнего устройства на основе методов симметричной криптографии;

- возможность идентификации владельца карты на основе секретного кода функции шифрования/дешифрования данных с использованием российского криптоалгоритма ГОСТ 28147-89;
- функцию выработки имитовставки;
- функцию диверсификации ключей;
- возможность проверки целостности масочного ПЗУ программ микроконтроллера криптографическими методами;
- структурированный доступ к информации, хранящейся в энергонезависимой памяти карты;
- возможность криптографически защищенного обмена информацией между картой и терминальным оборудованием;
- возможность использования карты в качестве шифратора данных.

Свои функции ОС РИК-2 реализует посредством выполнения команд, подаваемых карте внешним устройством (ВУ). ОС обеспечивает обмен карты с внешним устройством с использованием протокола передачи данных T0 в соответствии с ISO 7816-3.

Допускается передача блоков данных размером до 64 байт в обоих направлениях. Тип обмена (тип кодировки) – прямой.

Логический интерфейс обмена данными карты с ВУ, реализованный в ОС РИК-2, соответствуют международному стандарту ISO 7816-4. В ОС РИК-2 реализован принцип обеспечения разграничения доступа внешнего устройства к файлам. ОС РИК-2 поддерживает следующие типы файлов:

- DF – управляющие файлы, объединяющие файлы одного приложения;
- EF – бинарные файлы, предназначенные для хранения данных;
- KF – специализированные файлы для хранения ключей и паролей.

Для каждого файла на карте могут быть индивидуально определены виды доступа.

Карта может содержать несколько приложений. ОС РИК-2, используемая в качестве программной компоненты серийно выпускаемых микроконтроллеров типа КБ5004ВЕ1, соответствует утвержденным ФАПСИ “Тактико-техническим требованиям к РИК в качестве интеллектуального носителя ключевой и идентификационной информации”. [6]

3.3 Основные характеристики РИК-2

Базовая российская интеллектуальная карта выполнена на основе микроконтроллера КБ5004ВЕ1 с операционной системой UniCOS.

Операционная система обеспечивает платформу, которая позволяет реализовать на РИК весь спектр приложений для осуществления безналичных расчетов с использованием платежных карт, в том числе: электронный кошелек, электронный чек, дебетовая карта, карта продавца, телефонная карта и другие.

В части специального применения на основе РИК можно строить системы доступа к объектам и помещениям, аутентификации пользователей для ограничения доступа к информационно-телекоммуникационным ресурсам, использовать РИК в качестве носителя ключевой информации, а также персонального средства шифрования и электронной подписи документов.

Система разграничения доступа ОС UniCOS РИК позволяет:

- создавать файлы с однократной записью;
- разрешать чтение файла только после предъявления пароля и/или осуществления криптографической аутентификации;
- разрешать добавление данных в файл только после предъявления пароля и/или осуществления криптографической аутентификации;
- разрешать модификацию данных в файле только после предъявления пароля и/или осуществления криптографической аутентификации;
- зашифровывать передаваемые и дешифровать получаемые данные на ключе, записанном в карту;

- обеспечивать защищенный обмен данными между терминалом и картой с помощью шифрования (дешифрования) на сеансовом ключе, вычисляемом в результате проведения криптографической аутентификации;
- снабжать передаваемые данные криптографической имитовставкой, обеспечивающей контроль целостности, при этом имитовставка может быть выработана как на ключе, записанном в карту, так и на сеансовом ключе.

В смарт-картах могут быть использованы только стандартизированные файловые структуры. Определяемая стандартом ISO/IEC 7816-4 файловая система является сравнительно простой иерархической структурой, включающей в себя элементы трех категорий:

- главный файл MF (Master File);
- файл каталога DF (Dedicated File);
- элементарный файл EF (Elementary File).

Главный файл MF является корневым каталогом в иерархической структуре файлов. На языке общепринятых файловых систем главный файл MF является контейнером, который содержит все другие каталоги DF и все элементарные файлы EF. Главный файл должен присутствовать в каждой смарт-карте, причем в смарт-карте может быть только один MF.

Файл каталога DF действует как картотека файлов, которая содержит другие файлы DF или EF более низкого уровня, логически связанные между собой. В принципе, нет ограничения на число уровней DE. Однако обычно число уровней DF не превышает двух из-за ограниченного объема памяти в смарт-картах. Файлу DF может быть присвоено имя, уникальное в пределах содержащего его DF (или MF). Это позволяет однозначно определить путь к файлу (то есть путь представляет собой простое сочленение имени нужного файла с именами всех каталогов DF между этим файлом и содержащим его каталогом DF или MF). Соглашения по правилам именования файлов содержатся в стандарте ISO/IEC 7816-5.

Элементарный файл EF содержит фактические полезные данные, используемые операционной системой или приложением. В пределах файла каталога DF файл EF может иметь короткое (5-разрядное) имя. В зависимости от назначения файлы EF делятся на внутренние файлы EF и рабочие файлы EF.

Внутренние файлы EF хранят данные для самой операционной системы,

данные для исполнения приложения, секретные ключи или программный код.

Доступ к этим данным надежно защищается операционной системой.

Все данные приложения, которые должны быть считаны или записаны из терминала, или, иными словами, все данные, которые предназначены для внешнего мира, располагаются в рабочих файлах EF. Данные, содержащиеся в таких файлах, не используются операционной системой. Все файлы EF, содержащие полезные данные для конкретного приложения, всегда группируются вместе в одном каталоге DF. Это прием создает понятную структуру и облегчает ввод нового приложения в смарт-карту путем создания соответствующего DF. В смарт-карте с одним приложением все файлы EF могут быть помещены либо прямо под главным файлом MF либо в отдельном каталоге DF. Смарт-карты с несколькими приложениями имеют соответствующее число каталогов DF, в которые помещаются файлы EF, принадлежащие конкретным приложениям.

Такая структура файлов способствует обеспечению безопасности данных.

В отличие от файлов в системах DOS, файлы EF в смарт-картах обладают внутренней структурой. Эту структуру можно индивидуально подобрать для каждого EF в соответствии с намеченным использованием. Выбранная структура файла позволяет построить элементы данных таким образом, чтобы обеспечить к ним прямой и быстрый доступ. Различают следующие основные варианты внутренней структуры файлов EF:

- простой бинарный файл;
- линейный файл с записями фиксированной длины;
- линейный файл с записями переменной длины;
- циклический файл с записями фиксированной длины.

Простые бинарные файлы являются едиными неструктурированными блоками памяти смарт-карты, структуру которых программа приложения может задавать удобным для нее образом. Простой бинарный файл можно рассматривать как строку байтов. Когда выполняется команда чтения или

записи информации в простом бинарном файле, необходимо устанавливать смещение в байтах (от начала файла) до определенного байта (в пределах простого бинарного файла), с которого будет начинаться чтение или запись.

Команда чтения или записи информации в простом бинарном файле также должна содержать счетчик или длину байтовой строки, читаемой из файла или записываемой в него.

Линейные файлы с записями являются файлами, содержащими более мелкие части, называемые записи. Записи в пределах файлов нумеруются последовательно. Доступ к записям может осуществляться по их номерам или при выполнении операций последовательного чтения в прямом или обратном направлении. В файле с записями фиксированной длины все записи содержат одно и то же количество байтов. В файле с записями переменной длины каждая запись может содержать различное количество байтов. Файл с записями переменной длины требует большего времени доступа для операции чтения/записи и затрат на администрирование. Некоторые операционные системы смарт-карт поддерживают ограниченную функциональность поиска в линейных файлах.

Циклические файлы являются линейными файлами, циклически возвращающимися к первой записи, когда читается или вносится запись, следующая за последней записью. Циклический файл удобно представить как кольцо записей. Каждая последующая операция записи в файл выполняется над следующей физической записью в кольце. Операции чтения выполняются над последней физической записью.

Операционные системы смарт-карт поддерживают обычный набор операций со всеми файлами, таких как создание, удаление, чтение, запись и обновление. Для работы с файловой системой смарт-карт определен протокол прикладного уровня в виде набора функций для выбора, чтения файлов и записи в них. С каждым файлом смарт-карты связан список управления доступом. В этом списке указано, какие операции каждому из объектов,

получившему доступ к карте, разрешено выполнять с файлом. Например, объект А может читать конкретный файл, но не может его обновлять, в то время как объект В может выполнять в файле операции чтения, записи и даже изменять список управления доступом.

5 Разработка схемы электрической структурной устройства ввода ключевой информации

Разработанная электрическая структурная схема приведена в приложении А.

Выделим основные требования к разрабатываемому устройству:

- работа с приводом для чтения компакт дисков;
- считывание информации с РИК карты;
- получение управляющих команд через UART и USB порты;
- доступность исходного кода ПО устройства для анализа на отсутствие недокументированных возможностей;
- наличие автономного источника питания.

Для реализации устройства ввода ключевой информации с компакт диска и РИК можно рассмотреть несколько вариантов:

- 1 Реализация устройства на базе ПЭВМ типа notebook;
- 2 Реализация устройства на базе покупной макетной платы;
- 3 Реализация устройства на базе микроконтроллера с разработкой собственной платы и корпуса устройства.

С точки зрения материальных затрат наиболее простым и дешёвым является вариант использования покупного ноутбука с приводом для чтения компакт дисков и подключаемого к нему смарт-кард ридера. Но у данного решения есть существенный недостаток — это невозможность проведения анализа на отсутствие недокументированных возможностей в разрабатываемом программном обеспечении. Так как ПЭВМ управляется либо ОС с недоступными исходными текстами для ПО (семейство windows, mac), либо может быть ОС с доступными исходными кодами (семейство linux), но при этом данный код будет иметь значительный объём и как следствие становится очень сложным его анализ. Так же при использовании полноценной ОС практически невозможно выполнить криптографический контроль целостности

используемого ПО, в которое входят помимо пользовательской программы различные драйвера, службы и утилиты самой ОС.

При использовании покупной макетной платы возникают проблемы с тем, что на рынке очень сложно найти плату с достаточным функционалом, в этом случае придётся использовать две или даже три платы что приведёт к увеличению габаритов устройства и его стоимости. Так же необходимо учитывать, что при использовании покупной платы сложнее становится изготовление корпуса устройства.

Исходя из сказанного выше наиболее оптимальным и правильным является третий вариант. В настоящее время на рынке представлено множество микроконтроллеров, которые могут обеспечить заданный в ТЗ функционал. Микроконтроллер - это специальная микросхема, предназначенная для управления различными электронными устройствами. Микроконтроллеры впервые появились в том же году, что и микропроцессоры общего назначения (1971).

Разработчики микроконтроллеров придумали идею - объединять процессор, память, ПЗУ и периферию в одном корпусе, который выглядит как обычная микросхема. С тех пор производство небольших регуляторов с каждым годом чаще, чем производство процессоров, и их потребность не уменьшается.

Микроконтроллеры выпускают несколько компаний, причем не только 32-битный микроконтроллеры, но и 16-ти, и даже 8-битные (как у i8051 и аналогов). Внутри каждого семейства часто можно найти практически идентичные модели, отличающиеся скоростью процессора и объемом памяти.

Дело в том, что микроконтроллеры используются в основном во встраиваемых системах, в игрушках, в машинном оборудовании, в бытовой технике, в домашней автоматизации - там, где требуется не мощность процессора, а баланс между ценой и адекватной производительностью.

Вот почему старшее поколение микроконтроллеров еще в ходу: они могут многое: открыть дверь и изменить орошение почвы посредством

сотрудничества в домашней интеллектуальной системе. В то же время существуют небольшие регуляторы, которые способны совершать сотни миллионов транзакций в секунду и связаны с вводом «до зубов». Поэтому сначала производитель оценивает задачу, затем выбирает соответствующее оборудование.

Исходя из требований к устройству можно сформулировать основные минимальные требования к периферии микроконтроллера:

- наличие двух USB портов, имеющих возможность работы в HOST режиме;
- наличие одного UART порта;
- наличие порта, работающего по стандарту ГОСТ Р ИСО/МЭК 7816-3-2006.

Исходя из требований к разрабатываемому устройству была разработана структурная схема устройства, представленная в приложении А, основным элементом которой является управляющий микроконтроллер. На данной структурной схеме можно выделить несколько основных элементов:

- управляющий микроконтроллер;
- блок питания;
- блок индикации;
- разъемы для подключения внешних носителей ключевой информации;
- разъемы для подключения к устройству, в которое должна вводиться ключевая информация (головному устройству);
- микросхемы согласования.

6 Выбор и обоснование элементной базы для построения устройства ввода ключевой информации

Основным элементом устройства является управляющий микроконтроллер. Помимо описанных выше требований, так же при выборе микроконтроллера необходимо обращать внимание на наличие технической поддержки со стороны производителя. Данная поддержка заключается в предоставлении библиотек для работы с различной периферией микроконтроллера, наличием документации по различным вопросам связанным с функционированием микроконтроллера.

Одним из ведущих производителей микроконтроллеров является фирма STMicroelectronics, производящая 32 разрядные микроконтроллеры. Для использования при разработке устройства был выбран микроконтроллер STM32F415RGT. Данный микроконтроллер имеет два USB порта, 4 UART порта (с возможностью работы по стандарту ГОСТ Р ИСО/МЭК 7816-3-2006 и аппаратным потоком данных при работе в режиме порта RS232). [8]

Основные характеристики микроконтроллера представлены в таблице 1
Таблица 1 — Основные характеристики микроконтроллера

Характеристика	Значение
Максимальная рабочая частота, МГц	168
Корпус	LQFP64
Объём флэш памяти	1 Мбайт
Объём оперативной памяти	192 Кбайт
Количество входов/выходов	51
Интерфейсы	CAN, I ² C, IrDA, LIN, SPI, UART/USART, USB OTG, I2S
Диапазон рабочих температур	от минус 40...до плюс 85
Напряжение питания	от 1.8 — до 3,6 В

Блок питания предназначен для формирования из первичного питания, поступающего либо от внешнего устройства, либо от портативного аккумулятора из состава устройства вторичного питания, напряжением 3.3В и 5В для элементов схемы. Основными критериями при выборе источника питания является диапазон изменения входного напряжения и выходное напряжение и ток, которые должны обеспечить источники питания. В нашем случае входное напряжение изменяется в диапазоне от 3.4В до 5.2 В (питание от оборудования или от внешнего портативного аккумулятора), а выходное напряжение 3.3 В при максимальном токе 200 мА и 5 В при максимальном токе 140 мА. Для формирования напряжения 5 в была выбрана микросхема TPS60150DRV, для формирования напряжения питания 3.3 В была выбрана микросхема TPS78233DDC. Для коммутации первичного была выбрана микросхема TPS2115A-Q1.

Разъёмы для подключения внешних в данной схеме служат для подключения смарт-карты и внешнего привода для чтения компакт дисков через USB разъём.

Микросхемы согласования предназначены для обеспечения корректной работы устройств с различными уровнями логических сигналов. В таблице 2 представлены физические уровни для логических сигналов 0 и 1 различных интерфейсов.

Таблица 2 - Физические уровни

Интерфейс	Уровень логической 1	Уровень логического 0
UART	от минус 3В до минус 12В	от плюс 3В до плюс 12.
Смарт-карта	плюс 5В	0В
USB	плюс 3.3В	0В

Учитывая тот факт, что для микроконтроллера уровень логической 1 равен плюс 3,3В а уровень логического нуля равен 0В, в схеме необходимо

установить микросхемы для согласования логических сигналов между микроконтроллером и стыком RS-232 и микроконтроллером и смарт-картой.

Для согласования уровней при работе по стыку RS-232 была выбрана микросхема MAX3241, а для согласования стыка подключения смарт карты специализированная микросхема ST8024. В приложении В представлены перечни элементов.

7 Разработка алгоритма работы устройства ввода ключевой информации

7.1 Алгоритм работы устройства ввода ключевой информации

На рисунке 2 представлен общий алгоритм работы устройства. После запуска устройства выполняется предпусковой контроль функционирования.

После того, как он успешно выполнен происходит инициализация различных периферийных модулей, а затем начинается выполнение основной фоновый процесс программы, в котором выполняются следующие процедуры:

- подпрограммы работы с UART;
- подпрограмма работы с USB;
- подпрограмма работы с USB хостом;
- подпрограмма работы с файловой системой ISO 9660;
- подпрограмма работы с РИК;
- подпрограмма обработки команд.

Исходя из общего алгоритма работы устройства программное обеспечение для разрабатываемого устройства можно разделить на следующие части:

- программный модуль реализующий предпусковой контроль (ППК);
- программный модуль инициализации аппаратной части;
- программный модуль для работы с UART портом;
- программный модуль для работы по USB интерфейсу;
- модуль для работы с файловой системой ISO 9660 через контроллер MMC команд;
- программный модуль управления смарт-картой РИК;
- модуль, реализующий прокол взаимодействия с головным устройством.

На рисунке 3 представлена общая схема программного обеспечения.



Рисунок 2 - Алгоритм работы программы

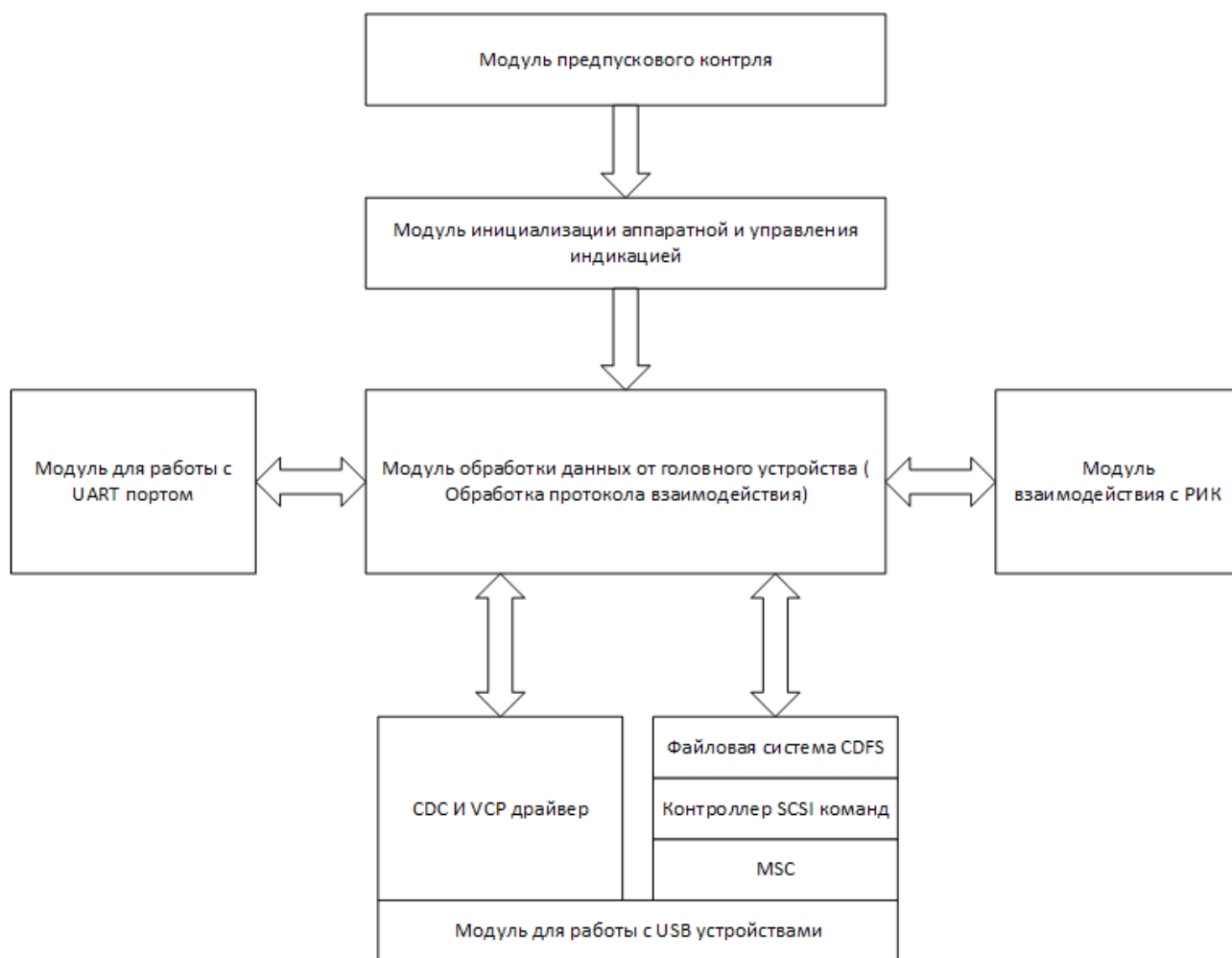


Рисунок 3 — Общая схема программного обеспечения

Далее остановимся подробнее на каждом из этих модулей.

7.2 Программный модуль реализующий ППК

Функции данного модуля вызываются при подачи питания на устройство. Функции данного модуля выполняют тестирование ОЗУ управляющего микроконтроллера, контроль целостности программного обеспечения микроконтроллера. Тестирование ОЗУ выполняется путём последовательной записи 0xFF, 0xAA, 0x55, 0x00 и контроль правильности записи данных значений. Контроль целостности ПО выполняется путём подсчёта имитозащитной вставки на ПО по алгоритму из ГОСТ 3413-2015 и сравнение её с эталонным значением. Также перед выполнением контроля целостности выполняется проверка криптоалгоритма на эталонном контрольном примере.

Так же в данном модуле выполняется контроль напряжения первичного питания устройства. Оно должно быть не менее 3,5 В для обеспечения надёжной работы устройства. При успешном выполнении ППК устройство продолжает свою работу. При возникновении ошибки устройство прекращает свою работу и включает индикатор «АВАРИЯ» (светодиод постоянно светится красным цветом).

7.3 Программный модуль инициализации аппаратной части

Функции данного модуля выполняют инициализацию аппаратной части микроконтроллера управления. Функции данного модуля программируют управляющие регистры различных периферийных устройств микроконтроллера.

7.4 Модуль UART

Модуль UART порта состоит из двух частей. Первая часть выполняется в прерывании а вторая в основной фоновой программе. При приёме данных выполняется их считывание из приёмного регистра UART порта и запись в приёмный буфер откуда они затем считываются в фоновой программе. При передаче данных в UART порт они сначала в фоновой программе записываются в буфер передачи откуда затем считываются в регистр передачи UART порта .

На рисунке 4 представлена структурная схема драйвера UART порта.

7.5 Модуль для работы по USB интерфейсу

Модуль для работы по USB интерфейсу состоит из нескольких частей. Первая часть, работающая в прерывании, обеспечивает взаимодействие с различными регистрами микроконтроллера, обеспечивающими работу по USB интерфейсу. Вторая часть обеспечивает функционирование ядра host-контроллера USB устройств. Оно обеспечивает контроль подключения устройств, их идентификацию и подключения соответствующего драйвера для

взаимодействия с устройством. Третья часть состоит из драйверов, обеспечивающих взаимодействие с устройствами в соответствии с алгоритмом описанном в профиле. В нашем случае необходимо обеспечить поддержку работы USB устройств работающих по профилю CDC, VCP и MSC. На рисунке 5 представлена структурная схема программного обеспечения, обеспечивающего работу по USB портам.

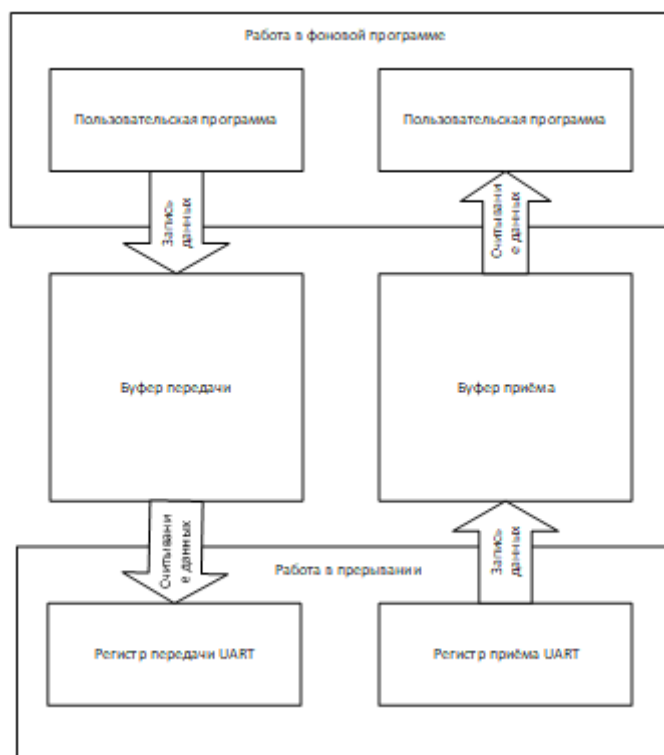


Рисунок 4 - Модуль для работы с UART

Профили VCP и CDC используются для реализации так называемого виртуального COM порта. В разрабатываемом устройстве они используются для получения управляющих команд передачи обратно результата их выполнения.

Профиль MSC (Mass Storage Class) предназначен для работы с различными устройства хранения информации в том числе и с портативным устройством чтения компакт дисков. После подключения привода с установленным компакт диском считывание данных выполняется через соответствующие запросы, которые выполняет контроллер MMC команд.

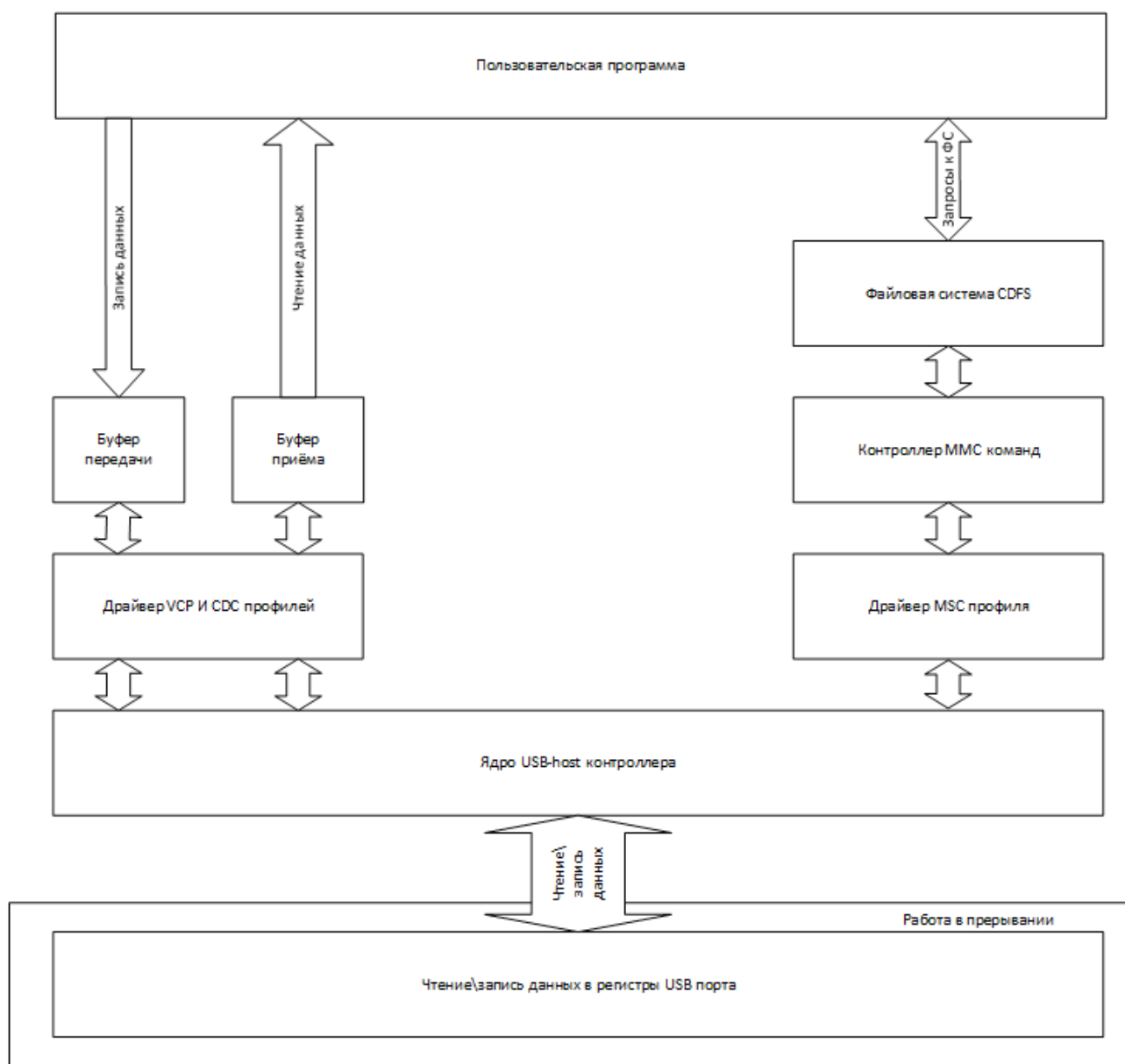


Рисунок 5 — Структурная схема

Пользовательская программа взаимодействует с файловой системой CDFS, которая предоставляет пользователю интерфейс для работы с файлами на диске. Файловая система в свою очередь взаимодействует с контроллером MMC команд.

7.6 Программный модуль, реализующий взаимодействие с РИК

Взаимодействие с РИК выполняется через передачу запросов к смарт карте и получения результата выполнения данных запросов. Программный модуль состоит из двух частей. Первая часть выполняется в прерывание и

обеспечивает непосредственное взаимодействие с аппаратным портом к которому подключена смарт карта, вторая часть выполняется в основном фоне программы и обеспечивает формирование запросов к РИК и обработку ответов получаемых от неё.

7.7 Программный модуль, реализующий взаимодействие с головным устройством

Данный модуль выполняет обработку потока управляющих данных, поступающих от головного устройства через USB порт, либо через UART порт. Взаимодействие с головным устройством выполняется в соответствии с разработанным в данной работе протоколом. При получении управляющей команды от головного устройства модуль выполняет её и при необходимости формирует запросы либо к файловой системе, либо к РИК. Общая структура программного модуля представлена на рисунке 6.

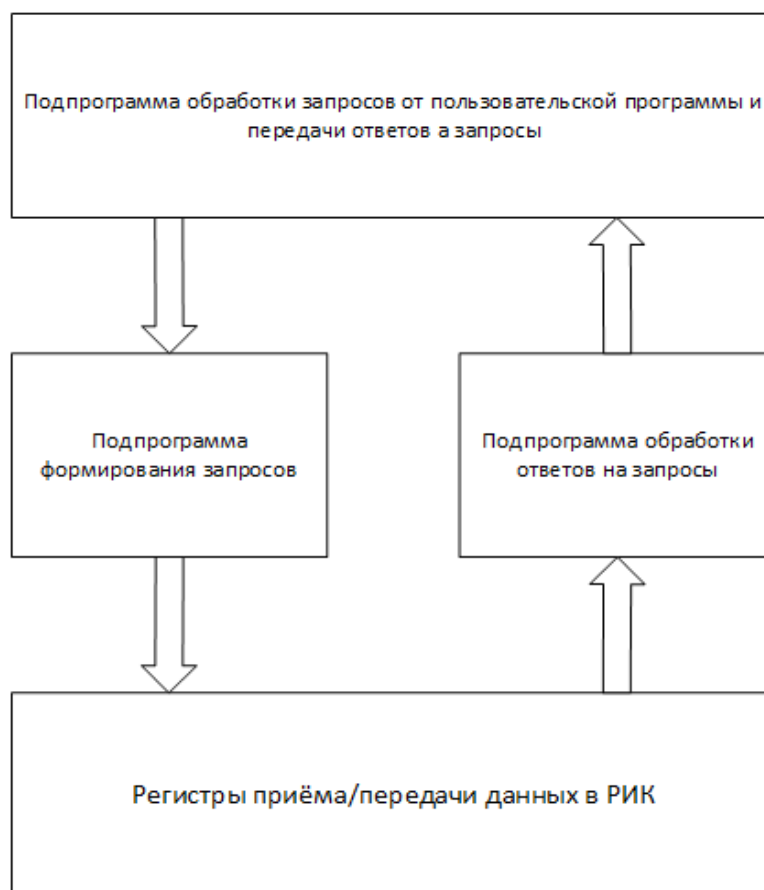


Рисунок 6— Общая структура модуля

8 Разработка протокола взаимодействия с устройством ввода ключевой информации

Первым этапом разработки протокола взаимодействия с устройством является выбор формата кадра для обмена, следующим этим является разработка перечня команд и на заключительном этапе выполняется проработка сценариев взаимодействия головного устройства и разрабатываемого устройства.

В соответствии с требованием ТЗ на ВКР при обмене с устройством должен обеспечиваться контроль целостности передаваемых данных. На основании данного требования был разработан формат кадра для обмена с устройством, представленный в таблице 2.

Таблица 2 — Формат кадра

Номер поля	1	2	3	4	5	6
Название поля	Стартовый байт	Код команды	Длина информационной части	Инверсная длина информационной части	Информационная часть	Контрольная сумма
Длина поля (байт)	1	1	1	1	0-255	2
Значение	0xEB	Любое из допустимых	0 -255	255-0	Любое	CRC16 на поля 2-5

Кадр состоит из 6 полей:

- стартовый байт – 1 байт 0xEB;
- код команды – любой допустимый код команды в соответствии с протоколом. Допустимые коды команд представлены в таблицах 1 и 2;
- длина информационной части;
- инверсная длина информационной части;

— информационная часть – данные передаваемые вместе с командой. Длина информационной части ограничивается 255 байтами. Данное поле может отсутствовать.

— контрольная сумма. Младший байт от арифметической суммы байт полей 2, 3, 4, 5.

После разработки формата кадра был проработан список управляющих команд для устройства и список ответных команд от устройства. В таблице 3 представлен перечень команд, передаваемых в устройство.

Таблица 3 — Перечень команд

Код команды	Длина информационной части(байт)	Описание
0x10	0	Запрос номера версии ПО устройства и контрольной суммы на его ПО
0x11	0	Выполнить инициализацию взаимодействия с РИК
0x12	n	Передать запрос к РИК. В информационной части передаётся запрос к РИК (в соответствии с протоколом взаимодействия с РИК)
0x13	0	Завершить работу с РИК
0x14	0	Выполнить инициализацию взаимодействия с приводом чтения компакт-дисков
0x15	n	Открыть каталог
0x16	n	Сменить каталог
0x17	0	Считать очередную запись каталога
0x18	n	Открыть файл для чтения
0x19	N	Считать блок данных из открытого файла
0x1A	n	Закрыть файл
0x1B	0	Завершить работу с приводом чтения компакт-диском

При получении команды устройство выполняет требуемое действие и передаёт результат выполнения команды. В таблице 4 представлен перечень команд поступающих от устройства.

Таблица 4 — Перечень команд поступающих от устройства

Код команды	Длина информационной части	Описание
0x40	n	Передача номера версии ПО устройства и его контрольной суммы
0x41	n	Передача ATR, полученного от РИК
0x42	n	Передача ответа на запрос со стороны РИК
0x43	0	Работа с РИК завершена
0x44	1	Диск, установленный в привод чтения компакт-дисков готов для работы. В информационной части передаётся идентификатор корневого каталога
0x45	1	Каталог открыт успешно. В информационной части передаётся идентификатор открытого каталога
0x46	0	Смена каталога выполнена успешно.
0x47	n	Передача очередной записи каталога
0x48	1	Файл открыт успешно. В информационной части передаётся идентификатор открытого файла.
0x49	n	Передача блока данных, считанного из файла
0x4A	0	Файл закрыт успешно
0x4B	0	Работа с приводом завершена
0x50	1	Ошибка взаимодействия с устройством

На рисунке 7 представлены сценарий взаимодействия с устройством при чтении информации с РИК.

При чтении данных с РИК головное устройство сначала инициализирует обмен передачей команды 0x11. При получении данной команды УВК запускает драйвер для взаимодействия с РИК и ожидает установки карточки в разъём. После установки карточки в разъём, драйвер выполняет так называемый холодный запуск и получает от неё Answer To Reset (дословно ответ на сброс) (ATR), который передаётся в головное устройство с командой 0x41. После этого головное устройство начинает передавать различные запросы к РИК в информационной части команды 0x12. Структура запросов к РИК представлена в таблице 5.

Таблица 5 — Структура запросов к РИК

Заголовок	Поле, Lc	Поле данных	Поле, Lc
4 байта	1 байт	0-60 байт	1 байт

Заголовок является обязательной частью и состоит из четырёх байт:

- CLA – класс. Для РИК всегда 0;
- INS – команда;
- P1 – параметр 1;
- P2 – параметр 2

Поле Lc определяет длину поля данных, передаваемых в РИК. В случае отсутствия данных поле исключается из запроса. Поле Le определяет количество байт, запрашиваемых с РИК. При отсутствии запрашиваемых байт данное поле исключается из запроса. В ответ на запрос РИК передаёт ответ, структура которого представлена в таблице 6.

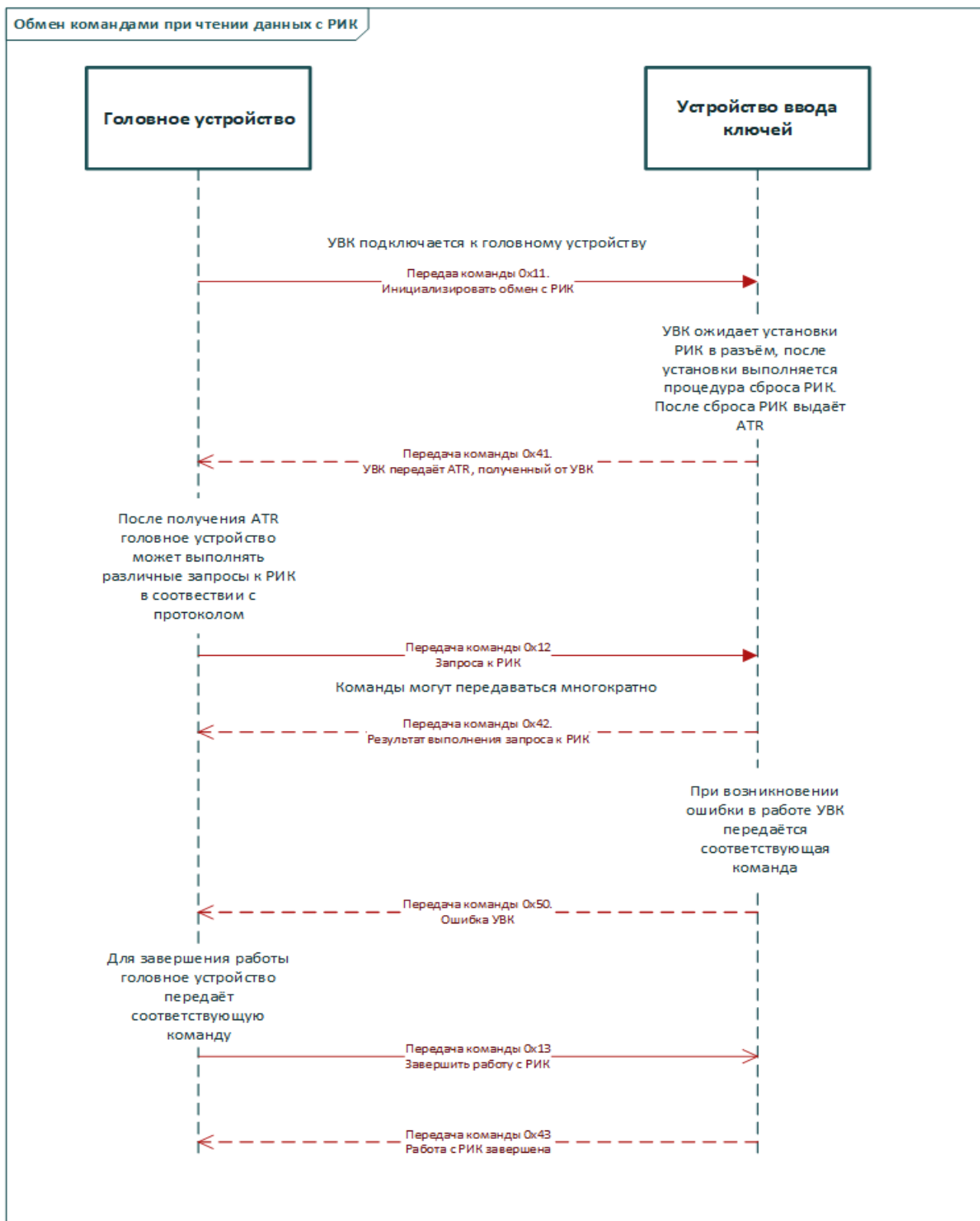


Рисунок 7 — Сценарии взаимодействия с устройством

Таблица 6 — Структура ответа от РИК

Поле SW1	Поле SW2	Поле данных
1 байт	1 байт	0-64 байт

Поле SW1 представляет собой состояние обработки команды, поле SW2 представляет собой квалификатор обработки команды. Поле данных переменной длины, которая определяется полем Lc запроса к РИК. Ответы от РИК передаётся в информационной части команды 0x42. В таблице 7 представлены основные запросы, передаваемые в РИК.

Таблица 7 — Запросы, передаваемые в РИК

Описание запроса	Запрос						Ответ			
	Команда	P1	P2	Lc	Поле данных	Lc	SW1	SW2	Поле данных	Примечание
Выбор файла	0x A4	0x 00	0x 00	2	Идентификатор файла	-	0x 90	0x 00	-	Если SW1 и SW2 другие, то ошибка.
Верификация	0x2 0	0x 00	0x 00	N	N байт, для которых выполняется верификация	-	0x 90	0x 00	-	Если SW1 = 0x63, то SW2 = 0xCn, где n оставшееся число попыток верификации. Если SW1 = 0x69, SW2 = 0x83, то верификация заблокирована
Чтение файла	0x B0	0x 00	0x 00	-	-	N	0x 90	0x 00	N байт	Если SW1 и SW2 другие, то ошибка.

Продолжение таблицы 7

Описание запроса	Запрос						Ответ			
	Команда	P1	P2	Lc	Поле данных	Lc	S W 1	S W 2	Поле данных	Примечание
Запись файла	0x D6	0x 00	0x 00	N	N байт, записываемых на РИК	-	0x 90	0x 00	--	Если SW1 и SW2 другие, то ошибка.

После завершения работы с РИК головное устройство передаёт в УБК команду 0x13. При получении данной команды УБК завершает работу с РИК и выдаёт команду 0x43. При возникновении ошибки УБК выдаёт команду 0x50 с информацией об ошибке.

На рисунке 8 представлен сценарий обмена командами при вводе информации с компакт-диска. Для начала считывания информации с диска головное устройство передаёт в УБК команду 0x14. По этой команде УБК запускает драйвер для работы с USB CD-ROM и ожидает его подключения и установки в него диска с ключевой информацией.

После установки диска УБК выполняет инициализацию работы с файловой системой диска, затем в головное устройство передаётся команда 0x44 с идентификатором корневого каталога. В дальнейшем головное устройство по этому идентификатору может выполнять обзор содержимого корневого каталога, передавая команду 0x17.

Для открытия нового каталога головное устройство передаёт команду 0x15 с именем открываемого каталога. Для смены текущего каталога используется команда 0x16. Для открытия файла используется команда 0x18.

Получив данную команду УБК выполняет поиск выбранного файла в текущем каталоге и передаёт уникальный идентификатор файла в головное устройство с командой 0x48. Далее по этому уникальному идентификатору

головное устройство может выполнить чтение данных из файла с помощью команды 0x19. После завершения работы с файлом головное устройство закрывает файл, передав команду 0x1A. Для завершения работы с диском головное устройство передаёт в УВК команду 0x1B. По этой команде УВК завершает работу с компакт диском и предаёт команду приводу на извлечение диска.

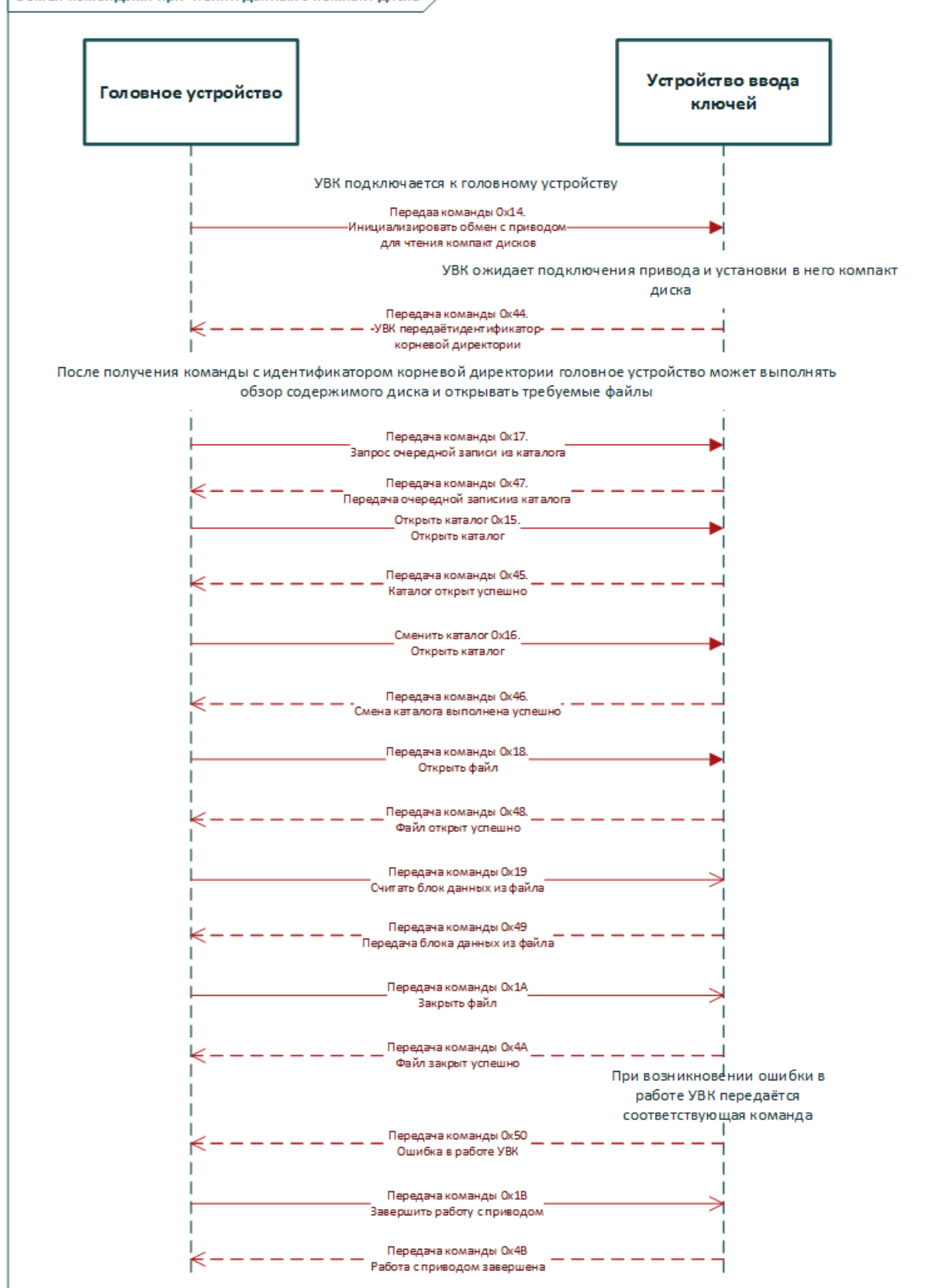


Рисунок 8 — Сценарии взаимодействия с устройством при чтении данных с компакт диска

9 Разработка схемы электрической принципиальной устройства ввода ключевой информации

В соответствии с разработанной электрической структурной схемой была разработана схема электрическая принципиальная устройства передачи зашифрованной информации. Схема электрическая принципиальная и перечень элементов устройства передачи ключевой информации приведены в приложении Б.

10 Разработка программного обеспечения устройства ввода ключевой информации

10.1 Описание разработки программного кода

Для разработки рабочего проекта была использована программная среда IAR Embedded Workbench v 7.8 for ARM. Программная среда включает в себя:

1 C/C++ компилятор – один из самых эффективных в своем роде. В нем также присутствует полная поддержка ANSI C.

2 Транслятор ассемблера, включающий в себя макроассемблер для программ реального времени и препроцессор для C/C++компилятора.

3 компоновщик, поддерживающий более тридцати различных выходных форматов для совместного использования с внутрисхемными эмуляторами.

4 Текстовый редактор, настроенный на синтаксис языка Си и имеющий удобный пользовательский интерфейс, автоматическое выделение ошибок программного кода, настраиваемую инструментальную панель, подсветку блоков, а также удобную навигацию по именам подпрограмм, макросов и переменных.

5 Симулятор и отладчик в кодах Си и ассемблера. Отладчик позволяет просматривать области EEPROM, DATA, CODE, а также регистры ввода/вывода, устанавливать точки останова и аппаратные флаги, обрабатывать прерывания с предсказанием. Кроме этого предусмотрен контроль стека и любых локальных переменных, режим пошагового выполнения программы. Тип отладчика и его настройки устанавливаются в свойствах проекта. Если отладчик отсутствует, то на помощь приходит симулятор, который, однако, не имеет возможности эмулировать работу процессора.

6 Менеджер проектов, облегчающий контроль и управление рабочими модулями.

7 Дополнительные утилиты для работы с оптимизированной CLIB/DLIB библиотекой .

Также при создании проекта был использован созданный компанией STMicroelectronics программный пакет STM32CubeMX. Данный пакет представляет собой настоящее автоматизированное рабочее место для разработчиков систем на базе 32-битных микроконтроллеров STM32, выполненных на основе ядер ARM Cortex. Это удобная среда для полноценной настройки конфигурации МК с выдачей пакета файлов инициализации, пригодных для дальнейшего использования в ряде систем разработки и отладки управляющего кода МК. STM32CubeMX значительно упрощает создание встраиваемого ПО, ускоряет этот процесс, не требует от начинающих специалистов досконального знания документации на МК, позволяет обойтись начальными сведениями об аппаратной и программной архитектуре контроллера, о возможностях библиотек ПО. STM32CubeMX отчасти позволяет эффективно совместить работу над своими первыми проектами с изучением возможностей МК.

10.2 Описание файлов проекта

В таблице 8 приведено описание файлов проекта.

Таблица 8 — Описание файлов проекта

Название файла	Назначение
Файлы для работы с периферией.	
stm32f4xx_ll_usb.c	Работа с USB портом
stm32f4xx_hal_uart.c	Работа с UART портом
stm32f4xx_hal_tim_ex.c stm32f4xx_hal_tim.c	Работа с таймерами микроконтроллера
stm32f4xx_hal_smartcard.c	Управление интерфейсом работы со смарт-картой
stm32f4xx_hal_rcc.c stm32f4xx_hal_rcc_ex.c	Управление тактированием микроконтроллера
stm32f4xx_hal_hcd.c	Управление и контроль состояния подключенных по USB порту устройств

Продолжение таблицы 8

Название файла	Назначение
Файлы для реализации драйверов USB устройств	
stm32f4xx_hal_pwr.c stm32f4xx_hal_pwr_ex.c	Управление питанием микроконтроллера
stm32f4xx_hal_hcd.c	Управление и контроль состояния подключенных по USB порту устройств
stm32f4xx_hal_gpio.c	Управление портами ввода/вывода
stm32f4xx_it.c	Файл с функциями, реализующими прерывания микроконтроллера
usbh_pipes.c	Файлы для обеспечения работы ядра USB хоста
usbh_ioreq.c	
usbh_core.c	
usbh_ctlreq.c	
usbh_cdc.c	Драйвер для работы с VCP и CDC устройствами
usbh_msc.c	Файлы реализуют драйвер для работы с компакт диском
usbh_msc_bot.c	
usbh_msc_scsi.c	
Пользовательские файлы	
MAIN_fone.c	Функции для реализации основного фонового процесса устройства
MESSAGE_lib.c	Функции для реализации очередей сообщений между различными блоками программы
UARTAM_lib.c	Функции для реализации работы с UART портом
RIK_lib.c smartcard.c	Функции для реализации работы с РИК
usb_host.c	Функции для обеспечения интерфейса между основной программой и USB хостом
PPK.c	Функции для реализации ППК микроконтроллера
main.c	Содержит функцию main.c
GOST34132015_Izv.c	Содержит реализацию функции контроля целостности по ГОСТ 3413-2015
CRC_lib.c	Реализация вычисления контрольной суммы по алгоритму CRC16
CDROM_lib.c	Содержит файлы для работы с файловой системой ISO9660

11 Разработка методики тестирования устройства при его изготовлении, а также его контроля ОТК предприятия-изготовителя и представителем заказчика на предприятии

11.1 Методика тестирования устройства

Методика проверки устройства ввода ключевой информации состоит из нескольких этапов.

- изготовление печатных плат и контроль качества их изготовления;
- монтаж электронных компонентов на печатные платы и контроль качества монтажа;
- настройка смонтированных плат и контроль электрических характеристик плат;
- сборка устройства ввода ключевой информации и контроль электрических характеристик устройства.

После изготовления печатных плат выполняется контроль качества изготовления службой ОТК предприятия изготовителя и службой представителя заказчика на предприятии. После прохождения контроля выполняется монтаж электронных компонентов на платы. Качество монтажа так же контролируется службой ОТК и службой представителя заказчика. Следующим этапом является настройка смонтированной платы. Настройка платы выполняется техническим персоналом предприятия-изготовителя. Настройка платы заключается в контроле различных характеристик платы. Далее будет проведена методика контроля смонтированной платы.

Из анализа принципиальной схемы устройства можно выделить несколько основных контролируемых узлов устройства:

- блок питания;
- микроконтроллер УУ STM32F415;
- порт для подключения USB CD-ROM;
- порт для подключения РИК;

- порт RS-232 для подключения к головному устройству;
- USB порт для подключения к головному устройству;
- узел индикации.

Для выполнения тестирования всех вышеперечисленных узлов должно быть организовано рабочее место, структурная схема которого представлена на рисунке 9.

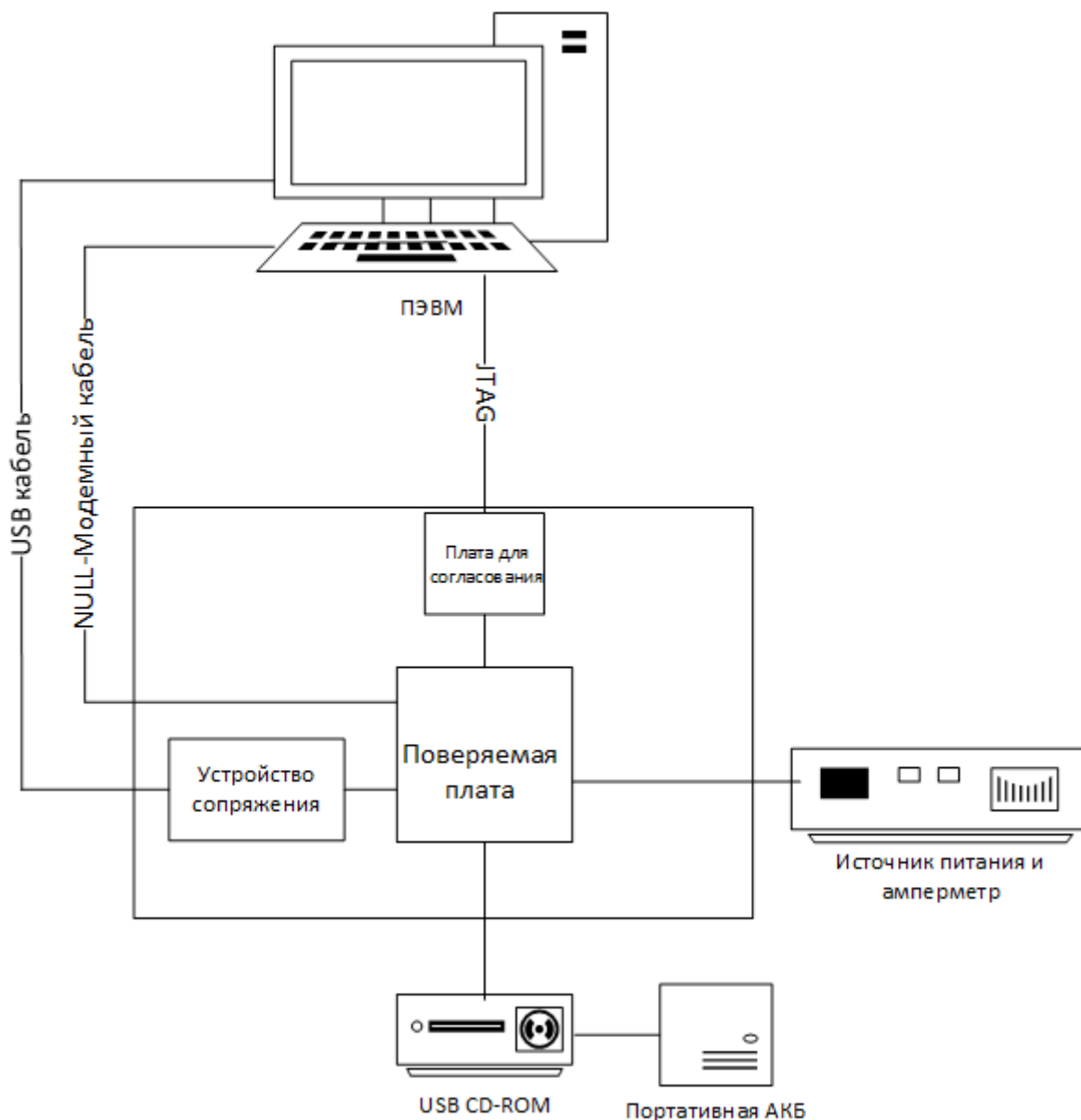


Рисунок 9 - Структурная схема рабочего места

В состав рабочего места входит ПЭВМ с ОС Windows, источник питания, USB CD-ROM, устройство сопряжения для подключения USB хоста устройства к ПЭВМ, JTAG для записи ПО в микроконтроллер.

Перед подключением к источнику питания выполняется контроль цепей питания на отсутствие из короткого замыкания на 0 В. В таблице 9 представлен перечень контролируемых цепей.

Таблица 9 — Перечень контролируемых цепей

Название цепи
D2:31 – C11
D2:47 – C12
D2:32 – C7
D2:48 – C8
D2:64 – C9
D2:19 – C10
X1:1 – U1:6
X4:1 – U1:8
U7:7 – D4:2
D3:8 – C20
D4:3 – C32
D5:5 – C31

После этого собирается схема проверки платы. При первом включении в плату необходима записать рабочее программное обеспечение. Для этой цели используется интерфейс JTAG, подключаемый через шлейфовый разъём X3. Запись рабочего программного обеспечения в микроконтроллер управления выполняется через ПЭВМ с использованием программы ST Visual Programmer. После записи программного обеспечения выполняется перезапуск питания проверяемой ячейки, при этом светодиод на плате сначала должен светиться красным цветом, а затем зелёным. После включения ячейки на ПЭВМ запускается программа для тестирования. Данная программа выполняет роль головного устройства и формирует команды управления для проверяемой ячейки. Интерфейс рабочего окна программы представлен на рисунке 10.

Программа проверки УВК

Статус подключения устройства:	Устройство подключено
Контрольная сумма на ПО:	0x11223344
Контрольная сумма на ВПО:	0x11223344
Версия ПО:	1.0
Номер COM-порта	COM1

Выполнить тестирование устройства

Окно вывода результатов тестирования устройства:

```

Начало тестирования устройства
Тестирование обмена через USB порт - НОРМА
Тестирование обмена через UART порт - НОРМА
Тестирование обмена РИК - НОРМА
Тестирование обмена с USB CD-ROM - НОРМА
Тестирование устройства завершено
  
```

Рисунок 10 - Интерфейс рабочего окна

При обнаружении подключенной ячейки в поле «Статус подключения устройства» появится статус «Устройство подключено». После этого в полях «Контрольная сумма на ПО», «Контрольная сумма на ВПО» и «Версия ПО» должны отобразиться значения которые соответствуют эталонным для записываемого программного обеспечения. Далее в поле «Номер COM-порта» необходимо ввести имя порта RS232 у ПЭВМ, к которой подключена проверяемая ячейка. После этого необходимо нажать кнопку «Выполнить тестирование ячейки». Программа тестирования выполняет последовательное тестирование всех узлов, а результат тестирования выводится в информационное окно программы тестирования на ПЭВМ. После завершения тестирования в информационном окне появится сообщение «Тестирование устройства завершено». Если при тестировании какого либо узла возникла ошибка, то в окне сообщение вместо слова «НОРМА» появится надпись «АВАРИЯ», при этом дальнейшая проверка устройства приостанавливается, а сотрудник предприятия изготовителя, выполняющий проверку ячейки, начинает

выполнять поиск неисправности ячейки в соответствии с таблицей 10, представленной ниже.

Таблица 10 - Проверка неисправности ячеек

Неисправность	Контролируемые цепи
При записи ячейки программа на ПЭВМ выдаёт ошибку	Проверьте правильность подключения JTAG к плате. Выполните проверку наличия связей между X3 и D2 в соответствии со схемой. Проверьте наличие питания на микросхеме D2.
После подключения платы к ПЭВМ не появляется сообщение о готовности	Проверьте наличие цепей между D2 и X4. Проверьте правильность монтажа R11 и R12, C16 и C17.
Контрольные суммы на ПО не совпадают с эталонными	Выполните повторную прошивку программного обеспечения
Тестирование обмена через USB порт завершилось аварией	Проверьте наличие цепей между D2 и X4. Проверьте правильность монтажа R11 и R12, C16 и C17.
Тестирование обмена через UART порт завершилось аварией	Проверьте наличие связей между D1 и D2 в соответствии со схемой Проверьте наличие питания на микросхеме D2 Проверьте наличие связей между D1 и X2 в соответствии со схемой
Тестирование обмена с РИК завершилось аварией	1 Проверьте наличие связей между D2 и D3 в соответствии со схемой 2 Проверьте наличие питания на микросхеме D3 3 Проверьте наличие связей между D3 и X5 в соответствии со схемой
Тестирование обмена с CD-ROM завершилось аварией	1 Проверьте наличие цепей между D2 и X1. 2 Проверьте правильность монтажа R5 и R6, C1 и C2.

После выполнения первичной проверки ячейки выполняется её гидроизоляция путем нанесения на её поверхность специального покрытия. Затем плата повторно проверяется в соответствии с описанной ранее методикой.

После этого плата предъявляется сотруднику ОТК предприятия-изготовителя. Сотрудник ОТК контролирует ячейку так же по описанной выше методике. Затем сотрудник ОТК предъявляет ячейку представителю заказчика на предприятии. Таким образом обеспечивается полный контроль качества изготовления ячейки. После приёмки ячейки всеми службами она поступает на сборку готового устройства (помещается в корпус). Процесс сборки так же контролируется сотрудником ОТК и представителем заказчика.

После сборки устройство также проверяется на работоспособность. Для проверки работоспособности собирается схема, представленная на рисунке 10. Для контроля работоспособности УВК используется та программа на ПЭВМ что и для проверки ячейки. Выполняется контроль тех же параметров. При возникновении аварии в процессе тестирования ячейка из состава устройства должна пройти повторную проверку. УВК прошедшее проверку предъявляется сотруднику ОТК предприятия-изготовителя, а затем представителю заказчика.

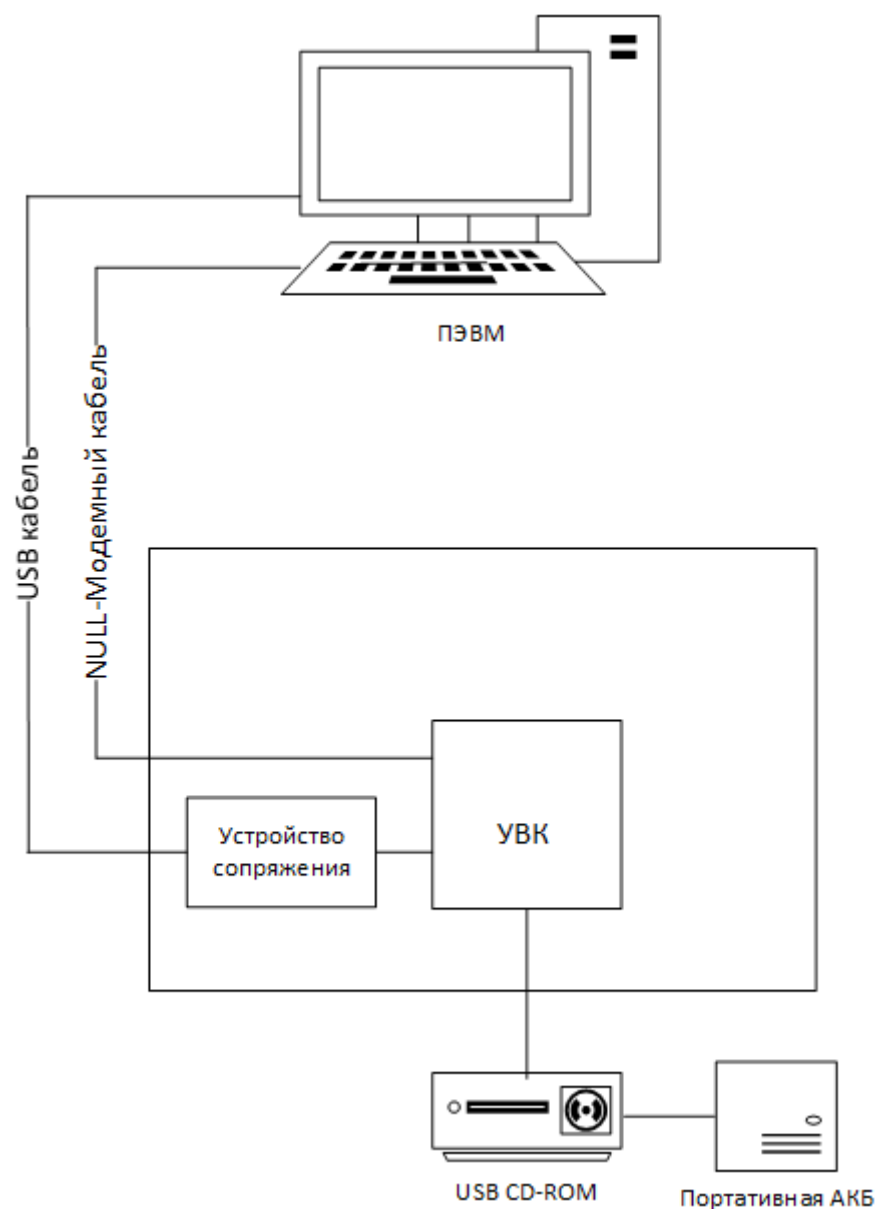


Рисунок 10 — Схема

11.2 Требования для контейнера, используемого при транспортировке и хранении устройства

Требования к разрабатываемому контейнеру:

- контейнер должен обеспечивать хранение составных частей УВК, представленных в таблице 11;
- в конструкции контейнера должны быть предусмотрены места для опечатывания, обеспечивающие невозможность вскрытия без нарушения печатей;

- на внешней поверхности контейнера должен быть размещён заводской номер контейнера;
- внутри контейнера должна размещаться опись хранящихся в нем компонентов;
- конструкция контейнера должна обеспечивать целостность размещённых в нём составных частей при транспортировании и обеспечивать герметичность в закрытом состоянии;
- контейнер должен иметь минимально возможные размеры;
- все элементы в контейнере должны размещаться в отдельных отсеках.

Таблица 11 — Перечень составных частей УБК

Наименование	Количество
Портативный CD-ROM TS8XDVDS-K фирмы Transcend + кабель из состава	1
Внешний аккумулятор ZenPower ABTU005 10050mAh (черный) фирмы ASUS + кабель из состава	1
Разрабатываемое УБК	1
Устройство зарядное сетевое СЗУ USB 2.1 А, черное фирмы Ri-tech Company	1

12 Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

К причинам психологических вредных факторов, влияющих на сердечно-сосудистую систему специалистов по защите информации, относятся нервно-психические и физические перегрузки. Работа специалистов по информационной безопасности связана с многочасовой работой, небольшой активностью и малоподвижным образом жизни. Это положение создает большую нагрузку на мышцы, включая ноги, плечи, шею и руки. В результате возникают болевые ощущения, уменьшается кровообращение, уменьшается количество потребляемого кислорода тканями организма.

Малоподвижный образ жизни также способствует различным заболеваниям сосудов сердца и крови. Было установлено, что у представителей умственного труда чаще встречаются сердечно-сосудистые заболевания, чем у людей, которые работают физически.

Например, при инфаркте миокарда наблюдается в два три раза реже у работников физического труда, чем у работников умственного труда. Если человек умственного труда больше двигался, было бы меньше пациентов с атеросклерозом и меньше случаев инфаркта миокарда.

Физическая активность в профилактике заболеваний сердца

Влияние физической деятельности на предупреждение заболеваний сердечно-сосудистой системы в настоящее время очень важно. С учетом работы двигательной системы снижается скорость атеросклеротического процесса.

Для людей, ведущих правильный образ жизни и ориентирующихся на необходимый минимум двигательной активности, повышается стабильность сердечно-сосудистой системы к заболеваниям, а клинические проявления во время его болезни снижаются.

Каждый человек, страдающий сердечно-сосудистыми заболеваниями, с помощью специалиста-физиотерапевта может заниматься самотренировками в зависимости от состояния здоровья, профессии, возраста. [8]

Недостатком является совокупность временных изменений в психологическом состоянии человека, которые появляются из-за длительной работы или стресса, что может привести к ухудшению таких показателей, как качественных так и количественных. Основными показателями утомления являются уровень утомляемости, изменения в структуре крови, артериальное давление. Развитие усталости и переутомления может привести к плохой координации движений, потере контроля. Из-за этих симптомов работник делает много ошибок в своей работе, и более того, переутомление и усталость могут вызвать кислородную недостаточность.

Развитие усталости и переутомления могут привести к головным болям, а также способствуют усилению таких заболеваний, как сосудистая дистония, болезни сердца, гипертония. При появлении симптомов усталости или утомления работника снижается координация, снижаются мыслительные процессы, повышается раздражение, увеличивается время реакции и снижается эффективность профессиональных знаний. Усталость сопровождается состоянием, в которой работник совершает много ошибок на работе, что может привести к опасной ситуации и даже несчастному случаю. Неблагоприятные нарушения в организме работника часто не ликвидируются полностью, а могут перейти в хроническую стадию. Борьба с неблагоприятными психофизическими изменениями работника сводится к улучшению гигиены и санитарии труда и использование конкретных методов, которые восстанавливают функцию костно-мышечной системы, увеличить приток крови к мозгу. В особом смысле это физическая культура, которая направлена на повышение успеваемости. Физическая культура помогает уменьшить усталость и ускорить процесс восстановления.

Специалисты рекомендуют начинать свой день с введения гимнастики, которая выполняется в течение времени от 5 до 7 минут и активизирует деятельность органов, играющих главную роль в работе и профессиональной деятельности. Или, если это невозможно, необходимо делать физкультурные паузы каждые 2 часа. Упражнения должны выполняться таким образом, чтобы органы, которые не участвуют в рабочем процессе, также получали нагрузку.

В этом случае упражнения необходимо практиковать, которые регулирует кровообращение. Как правило, упражнения выбираются независимо, а их воздействие направлено на усталость какой либо из частей тела. В целях улучшения кровообращения к таким упражнениям можно отнести ходьбу и дыхательные упражнения. Другие упражнения - это вращение головы, плеч, тела. Если во время обеденного перерыва есть свободное время, то избавьтесь от нагрузки на организм, необходимо спокойно ходить, занимаясь дыханием, для лучшего это следует делать не в комнате, а на свежем воздухе. В конце рабочего дня важно практиковать восстановительную гимнастику, в которой используются только упражнения, которые помогают уменьшить усталость более чувствительных систем организма.

Для работников с малоподвижным трудом, небольшой физической нагрузкой упражнения, улучшающие работу сердечно-сосудистой системы, имеют особое значение. Эти упражнения повышают выносливость организма к работе, помогают противостоять усталости. Эти упражнения должны быть низкой интенсивности, но достаточно длинными, например ходьба. Выбор возможности практиковаться зависит от ситуации и способностей каждого. [9]

Упражнения расслабляющие мышцы, успокаивающие дыхательные упражнения. Это уменьшает дискомфорт тела, напряжение мышц, наделает функции сердечно-сосудистой системы и дыхания. Специалисты рекомендуют физическую паузу, когда начинает развиваться усталость, для умственных работников - через три часа. Физические упражнения занимают от 1 до 2 минут и 4 упражнений для уменьшения мышечной усталости и зрения. Небольшая

пауза - это короткая форма производственной гимнастики, ее время составляет всего две или три секунды, обычно на рабочем месте: небольшой массаж, упражнения для глаз, кистей рук. В течение рабочего дня рекомендуется использовать каждую возможность для простой гимнастики. После работы, если возможно, гуляйте. Говоря о здоровой жизни, одной из ведущих областей является питание, которое особенно важно при занятиях физкультурой и спортом. Снаружи стресс возникает у разных людей по-разному, у одного болит голова, у другого создается впечатление, что он почти опустошен, у третьего болит спина в области грудины.

Поэтому вывод: узнать свое проявление на стресс. Причины проблем различны: сильное волнение, внезапные изменения погоды, умственная и физическая усталость и т.д. [10]

Заключение

В ходе выполнения выпускной квалификационной работы были разработаны структурная и принципиальная электрические схемы устройства ввода ключевой информации с компакт диска и российской интеллектуальной карты.

В процессе работы был проведен анализ протокола взаимодействия с портативным приводом для чтения компакт - дисков по USB интерфейсу, файловой системы CDFS (ISO 9660), протокола взаимодействия с российской интеллектуальной картой, файловой системы российской интеллектуальной карты.

Был разработан алгоритм работы устройства ввода ключевой информации, протокол взаимодействия с устройством ввода ключевой информации. А также разработаны программное обеспечение устройства ввода ключевой информации и методика тестирования устройства при его изготовлении, его контроля ОТК предприятия-изготовителя и представителем заказчика на предприятии.

Таким образом, задание на выпускную квалификационную работу выполнено в полном объеме.

Список используемых источников

- 1 Криптографическая защит информации [электронный ресурс] - <https://studfiles.net/preview/6210714/> режим доступа свободный — дата последнего обращения — 01.03.2019.
- 2 SATA [электронный ресурс] - <https://ru.wikipedia.org/wiki/SATA> режим доступа свободный — дата последнего обращения — 01.03.2019.
- 3 Применение USB [электронный ресурс] - <http://perscom.ru/usb/105-usb-primeneniye/674-usb36> режим доступа свободный — дата последнего обращения — 01.03.2019.
- 4 USB [электронный ресурс] - <https://ru.wikipedia.org/wiki/USB> режим доступа свободный — дата последнего обращения — 01.03.2019.
- 5 Стандарт ISO 9660 [электронный ресурс] - https://ru.wikipedia.org/wiki/ISO_9660 режим доступа свободный — дата последнего обращения — 02.05.2019.
- 6 Способы защиты объектов информатизации от утечки информации по техническим каналам: защита цепей электропитания средств вычислительной техники [электронный ресурс] - <http://www.bnti.ru/showart.asp?aid=739&lvl=04.03.07>. режим доступа свободный — дата последнего обращения — 03.03.2019.
- 7 STM32: эпоха 32-битных микроконтроллеров наступила [электронный ресурс] - <https://www.compel.ru/lib/ne/2011/2/3-stm32-epoha-32-bitnyih-mikrokontrollerov-nastupila> режим доступа свободный — дата последнего обращения — 20.04.2019
- 8 Сердечно-сосудистые заболевания и образ жизни [Электронный ресурс]. – Режим доступа: <https://jesuslove.ru/13235-serdechno-sosudistye-zabolevaniya-i-obraz-zhizni.html>, свободный — дата последнего обращения — 10.05.2019.

9 Общие характеристики ЧСС и АД. [Электронный ресурс]. – Режим доступа: <https://studfiles.net/preview/4496816/page:3/>, свободный — дата последнего обращения — 14.05.2019.

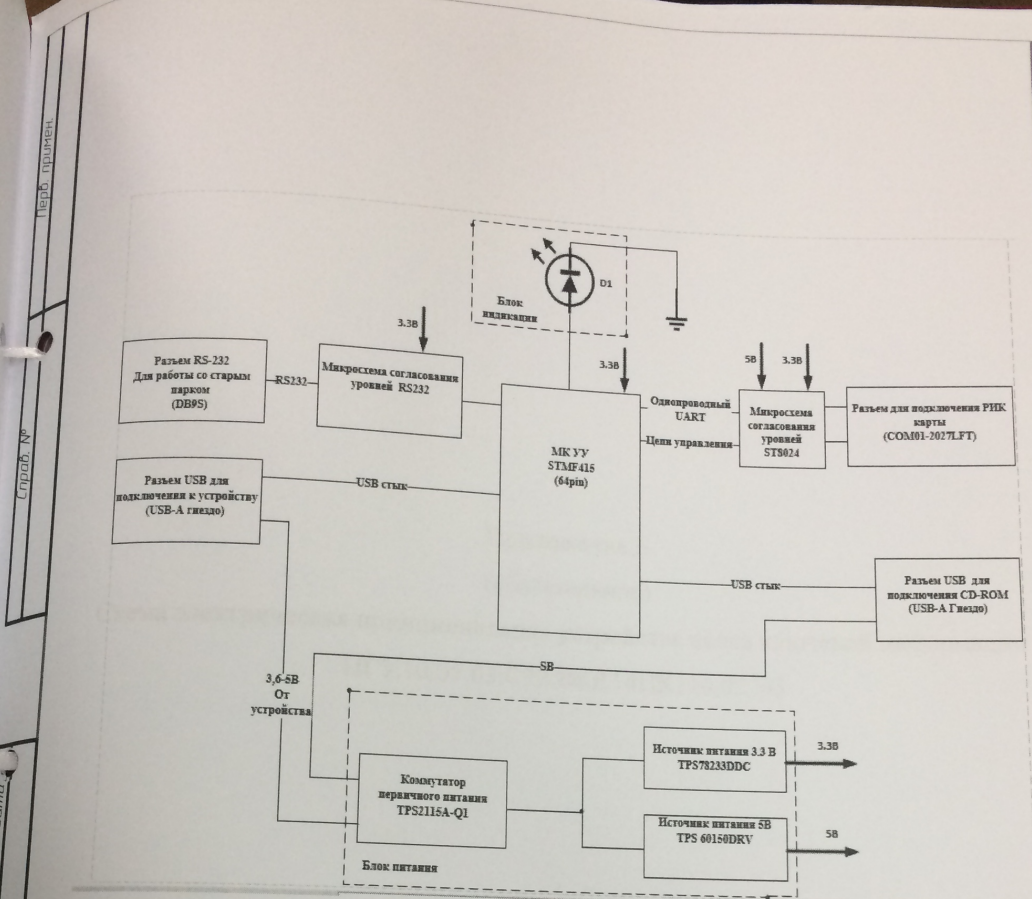
10 Физическая культура работников умственного труда [Электронный ресурс]. – Режим доступа: <https://pglu.ru/upload/iblock/75f/16.pdf>, свободный — дата последнего обращения — 22.05.2019.

Приложение А

(обязательное)

Схема электрическая структурная устройства ввода ключевой информации

ПГУ.10.05.03.С32.ВКР.14ПК116.01 Э1



ПГУ.100503.С32.14ПК116.01 Э1					Лист		
Изм.	Лист	№ докум.	Подп.	Дата	Лист	Лист	Листов
Разраб.	Придолова И.А.						1
Проверил	Родионов Е.Ф.						
Н. контр.	Иванов А.П.				Гр. 14ПИ1		
Утв.							

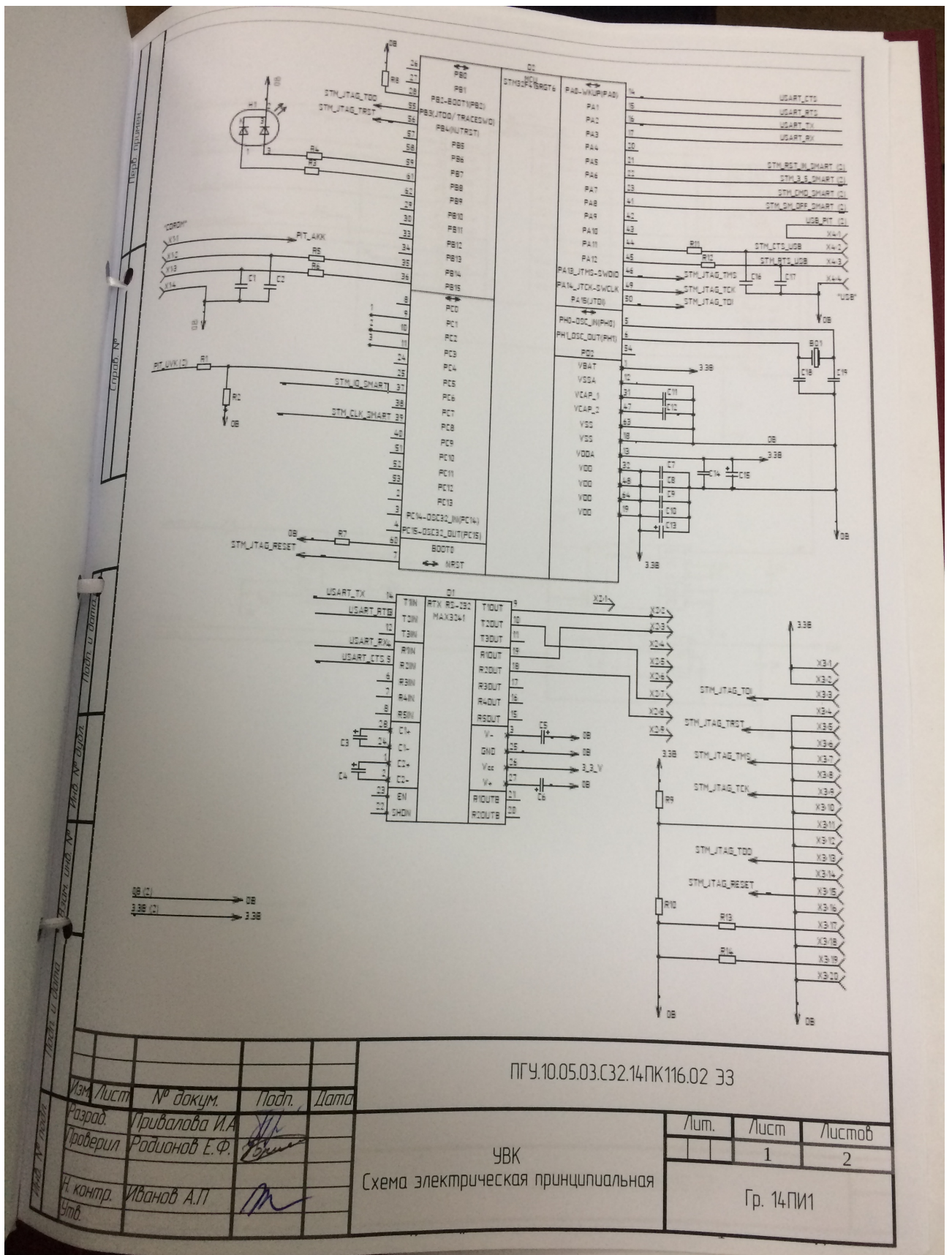
УВК
Схема электрическая структурная

Приложение Б

(обязательное)

Схема электрическая принципиальная устройства ввода ключевой информации

ПГУ.10.05.03.С32.ВКР.14ПК116.02 ЭЗ



Приложение В
(обязательное)
Перечень элементов
ПГУ.10.05.03.С32.ВКР.14ПК116.02 ПЭЗ

Поз.обозначение	Наименование	Кол.	Примечание
BQ1	Резонатор ABM8G- 1 2 . 0 0 0MHz - 1 8 -D2Y	1	Abrakon Corporation
C1,C2	Конденсатор GRM1 5 5 C1H4 7 0GA0 1	2	Murata
C3...C6	Конденсатор GRM1 5 5 R6 1A1 0 4KA0 1	2	Murata
C7..C10	Конденсатор GRM1 8 8 R7 1A2 2 5KE1 5	4	Murata
C11 ,C12	Конденсатор танталовый TAJA4 7 5K0 1 0R	2	AVX
C13	Конденсатор GRM1 5 5 R6 1A1 0 4KA0 1	1	Murata
C14	Конденсатор танталовый TAJA1 0 5K0 2 0R	1	AVX
C15	Конденсатор GRM1 5 5 C1H4 7 0GA0 1	2	Murata
C16,C17	Конденсатор GRM1 8 8 5C2A1 6 0 JA0 1	2	Murata
C18,C19	Конденсатор GRM1 5 5 R6 1A1 0 4KA0 1	1	Murata
C20	Конденсатор GRM1 8 8 R6 0 J 2 2 5KE1 9	1	Murata
C21	Конденсатор GRM1 5 5 R6 1A1 0 4KA0 1	1	Murata
C22	Конденсатор GRM1 8 8 R6 0 J 2 2 5KE1 9	1	Murata
C23,C24	Конденсатор GRM1 5 5 R6 1A1 0 5KA0 1	1	Murata
C25	Конденсатор GRM1 5 5 R6 1A1 0 4KA0 1	1	Murata
C26	Конденсатор GRM1 8 8 R6 0 J 2 2 5KE1 9	1	Murata
C27,C28	Конденсатор танталовый TAJA4 7 6M0 0 2R	2	AVX
C29,C30	Конденсатор GRM1 8 8 R6 0 J 2 2 5KE1 9	2	Murata
C30,C31	Микросхема MAX3 2 4 1	1	MAXIM
D1	Микросхема STM3 2 F4 1 5RGT 6	1	STMicroelectronics
D2	Микросхема ST 8 0 2 4CTR	1	STMicroelectronics
D3	Микросхема TPS6 0 1 5 0DRV	1	Texas Instruments
D4	Микросхема TPS7 8 2 3 3DDC	1	Texas Instruments
D5	Индикатор единичный L - 3VEGW	1	Kingbright
H1			

ПГЧ.10.05.03.С32.14ПК116.02 ПЭЗ

Изм. Лист № докум. Подп. Дата

Разраб. Придолова И.А.

Проверил Родионов Е.Ф.

Н. контр. Иванов А.П.

Утв.

УВК
Перечень элементов

Лист Лист Листов

2

Гр. 14ПИ1

Поз.обозначение	Наименование	Кол.	Примечание
R1 ,R2	Резистор CR0 4 0 2 - FX- 6 8 0 0GL F	2	Bourns
R3 ,R4	Резистор CR0 4 0 2 - FX- 3 9 0 0GL F	2	Bourns
R5 ,R6	Резистор CR0 4 0 2 - FX- 2 7R0GL F	2	Bourns
R7...R10	Резистор CR0 4 0 2 - J / - 0 0 0GL F	4	Bourns
R11 ,R12	Резистор CR0 4 0 2 - FX- 2 7R0GL F	2	Bourns
R13... R15	Резистор CR0 4 0 2 - J / - 0 0 0GL	3	Bourns
R16	Резистор CR0 4 0 2 - FX- 3 9 0 0GL F	2	Bourns
R17	Резистор CR0 4 0 2 - FX- 1 5 0 3GL F	1	Bourns
R18	Резистор CR0 4 0 2 - FX- 6 8 0 3GL F	1	Bourns
R19	Резистор CR0 4 0 2 - FX- 4 7 0 3GL F	1	Bourns
R20	Резистор CR0 4 0 2 - FX- 1 0 0 3GL F	1	Bourns
U1	Микросхема TPS2 1 1 5A	1	Texas Instruments
X1	Розетка USBA- 1 J	1	
X2	Вилка DBR- 9M	1	
X3	Соединитель FH3 4SRJ - 2 0S- 0 . 5SH	1	Hirose
X4	Розетка USBA- 1 J	1	
X5	Соединитель CCM0 1 - 2 0 2 7 L FT	2	C&K Components

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Изм.	Лист	№ докум.	Подп.	Дата

ПГЧ.10.05.03.С32.14ПК116.02 ПЭЗ

Лист

Копировал

Формат А4