

И.Л. Орлова

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет 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

ЗАЩИЩЕННОЕ УСТРОЙСТВО ВВОДА КЛЮЧЕВОЙ ИНФОРМАЦИИ

Студент _____ Полянская Ульяна Павловна

Руководитель _____ Миндалев Р.В.

Нормоконтролер _____ Иванов А.П.

Рецензент _____ Сомкин С.А.

Работа допущена к защите (протокол заседания кафедры от _____ № ____)

Заведующий кафедрой _____ Зефилов С.Л.

Работа защищена с отметкой _____ (протокол заседания ГЭК от
_____ № ____)

Секретарь ГЭК _____ Иванов А.П.

Пенза 2022

Оглавление

Обозначения и сокращения.....	5
Введение.....	6
1 Обзор носителей ключевой информации.....	7
1.1 Что такое ключевая информация.....	7
1.2 Бумажные блокноты.....	7
1.3 Оптические диски.....	8
1.4 Смарт-карты.....	8
1.5 Комбинированный подход.....	8
2 Анализ методов защиты тракта ввода ключевой информации устройства криптографической защиты информации.....	9
2.1 Устройство криптографической защиты информации.....	9
2.2 Механические методы защиты.....	9
2.3 Методы защиты от утечки в электромагнитных полях.....	10
2.4 Информационно-логические методы защиты.....	10
2.5 Требования к устройству ввода ключевой информации.....	11
3 Определение перечня угроз и методов защиты.....	12
3.1 Список угроз.....	12
3.2 Описание угроз.....	12
4 Обоснование конструкции с учетом специальных требований.....	16
4.1 Внешний вид устройства.....	16
5 Описание структурной схемы устройства.....	19
5.1 Состав устройства.....	19
6 Подбор покупных узлов.....	20
6.1 Выбор привода чтения оптических дисков.....	20
6.2 Выбор преобразователя USB-SATA.....	21
6.3 Выбор соединителя смарт-карт.....	22
6.4 Выбор дисплея.....	22
6.5 Выбор клавиатуры.....	23
7 Описание функциональных схем устройства.....	25
7.1 Описание функциональной схемы платы индикации.....	25
7.2 Описание функциональной схемы платы управления.....	25
8 Выбор элементной базы.....	26
8.1 Порядок выбора.....	26

8.2 Выбор элементной базы платы индикации.....	26
8.3 Выбор элементной базы платы управления.....	26
8.4 Оценка подсистемы питания.....	29
9 Описание принципиальных схем устройства.....	33
9.1 Принципы проектирования систем на основе микроконтроллеров.....	33
9.2 Описание принципиальной схемы платы индикации.....	34
9.3 Описание принципиальной схемы платы управления.....	38
10 Выбор и описание программной реализации.....	51
10.1 Сравнение средств разработки.....	51
10.2 Подготовка системы на базе GNU/Linux.....	51
10.3 Библиотека libopencm3.....	51
10.4 Библиотека libusbhost.....	52
10.5 Абстракции USB.....	52
10.6 Предпусковой контроль.....	53
10.7 Периодический контроль.....	54
10.8 Протоколирование событий.....	56
10.9 Описание программы контроллера карты.....	56
10.10 Описание программы контроллера управления.....	58
11 Разработка протокола обмена с учетом специальных требований.....	62
11.1 Активирующие последовательности.....	62
11.1 Прореживание информации.....	62
11.2 Маскирование информации.....	63
11.3 Контроль целостности информации.....	63
11.4 Контроль целостности программного обеспечения.....	64
11.5 Описание протокола.....	64
11.6 Порядок работы с устройством.....	67
12 Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....	70
Заключение.....	71
Список использованных источников.....	72
Приложение А Угрозы безопасности и соответствующие им методы защиты.....	75
Приложение Б Схема электрическая структурная устройства.....	76
Приложение В Схема электрическая функциональная устройства.....	77

Приложение Г Схема питания устройства.....	78
Приложение Д Схема электрическая принципиальная платы индикации.....	79
Приложение Е Схема электрическая принципиальная платы управления.....	80
Приложение Ж Алгоритм работы предпускового контроля.....	81
Приложение И Перечень протоколируемых событий.....	82
Приложение К Обработка данных с использованием протокола обмена.....	83

Обозначения и сокращения

GPIO – General-purpose input/output

SATA – Serial ATA

UART – Universal asynchronous receiver-transmitter

ULPI – UTMI+ low pin interface

USART – Universal synchronous and asynchronous receiver-transmitter

USB – Universal Serial Bus

Введение

Чем ценнее информация (и чем выше возможный ущерб в случае ее раскрытия), тем больше внимания (и средств) уделяется ее закрытию. При хранении, поддержании и предоставлении доступа к любому информационному объекту его владелец, либо уполномоченное им лицо, составляет набор правил по работе с ней. Умышленное нарушение этих правил классифицируется как атака на информацию.

Шифрование подразумевает процесс обратимого преобразования данных в целях их сокрытия от посторонних лиц, но предоставления доступа авторизованным пользователям. Основная задача шифрования — обеспечение конфиденциальности данных, которые передаются по какому-либо каналу. В наше время шифрование информации производится с использованием электронных устройств, построенных на основе цифровых микросхем. Так как для разработки используются импортные элементные базы, разработчику приходится дополнительно продумывать методы, позволяющие обеспечить защиту от уязвимостей, вероятно встроенных в эту импортную элементную базу.

Поскольку для работы устройства шифрования требуется ключевая информация, которую нужно в него вводить, то в комплекте с устройством шифрования должно использоваться устройство ввода ключевой информации, спроектированное по схожим с устройством шифрования принципам.

Проектирование такого устройства (защищенного как от эксплуатации возможных уязвимостей в элементной базе, так и от утечки ключевой и криптографически опасной информации в электромагнитных полях) и является целью данной работы.

Актуальность проекта обусловлена участвовавшими информационными атаками, а разрабатываемое устройство будет защищено от воздействия злоумышленников. В рамках проекта были поставлены следующие задачи: выполнить обзор носителей ключевой информации; произвести анализ методов защиты тракта ввода ключевой информации; разработать структурную и функциональную схемы устройства; произвести разработку программного обеспечения; произвести разработку протокола обмена данными между устройством и УКЗИ с учетом специальных требований; определить вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации.

1 Обзор носителей ключевой информации

1.1 Что такое ключевая информация

Для проведения операций кодирования/декодирования в общем случае нужны только данные, обратимо преобразуемые по некоторому алгоритму. Например, в электронной почте прикрепляемые файлы кодируются по алгоритму Base64 [1], где 8-битные данные преобразуются в печатные символы (латинского алфавита, цифры и некоторые другие). Это увеличивает размер передаваемой информации примерно на 35%, зато позволяет передавать бинарные файлы без потери содержимого по каналам, которые не предназначены для передачи 8-битных данных (но до начала 90-х многие каналы связи были символьно-ориентированными [2])

Однако закодированный подобным образом файл может быть прочитан кем угодно на пути от отправителя к получателю. Можно провести аналогию с почтовой открыткой, пересылаемой без конверта. В тех случаях, когда это неприемлемо, файл можно предварительно зашифровать. При шифровании кроме самого алгоритма шифрования нужен также ключ. Если алгоритм надежный и ключ известен только отправителю и получателю, то содержимое файла третьим лицам в процессе передачи не раскрывается.

На первый взгляд может показаться, что ничего не изменилось – и с шифрованием, и без шифрования все также нужно передавать данные в открытом виде между отправителем и получателем, однако если размер ключа (ключевой информации) меньше, чем размер информации, подвергаемой зашифровке, то передать ключевую информацию проще.

Однако возникает задача предоставления ключа получателю и отправителю таким образом, чтобы он не попал в руки посторонним лицам.

1.2 Бумажные блокноты

Наиболее простой и понятный способ — распечатать ключевую информацию на бумаге и отправить курьером. Данное действие не требует никаких специальных устройств. Однако вводить эту последовательность в аппаратуру вручную долго. Также с такого носителя ключевой информации просто снять копию. А курьер должен быть доверенным человеком.

1.3 Оптические диски

Следующий носитель – оптический диск. Обладает большой емкостью и долговечностью (более десятка лет [3]), есть варианты с однократной (R) и многократной (RW) записью. Информация на диске хранится в виде последовательности ямок, используются преобразование NRZ [4], модуляция 8-в-14 [5] и коды коррекции ошибок Рида-Соломона [6]. Минусом такого носителя является легкость копирования при помощи обычного компьютера (хотя во времена низкоскоростного Интернета были распространены компьютерные игры на дисках, защищенных от копирования [7]).

1.4 Смарт-карты

Электронные носители, защищённые от копирования - смарт-карты [8], применяемые повсеместно: это и банковские платежные карты, и SIM-карты операторов сотовой связи. Физический размер карты (который различен для симки и кредитки) здесь не важен – расположение контактных площадок и протокол обмена стандартизированы в ISO 7816 [9]. Внутри карты находится чип, на котором хранится конфиденциальная информация и который осуществляет процедуру аутентификации для доступа к этой информации. При нескольких попытках неверного ввода PIN [10], а затем PUK [11] карта блокируется. (Возможно извлечение информации и с заблокированной карты, однако для этого требуются специальное оборудование и навыки [12]). Однако емкость смарт-карты значительно меньше емкости оптического диска.

1.5 Комбинированный подход

Но также возможно использовать сразу три носителя ключевой информации, комбинируя их достоинства – большую по объему часть ключевой информации в зашифрованном виде поместить на оптический диск, ключ для расшифровки ключевой информации с диска – на смарт-карте, доступ к которому возможен только при предъявлении PIN (или PUK), а сами PIN (и PUK) распечатывать на бумажном носителе.

2 Анализ методов защиты тракта ввода ключевой информации устройства криптографической защиты информации

2.1 Устройство криптографической защиты информации

Устройство криптографической защиты информации будет представлено как «черный ящик», имеющий следующие стыки сопряжения:

- входной информации (аналоговой или цифровой);
- выходной информации (аналоговой или цифровой);
- управления;
- ввода ключевой информации.

Информация, поступающая на вход устройства, подвергается преобразованию в соответствии с режимом, задаваемым по стыку управления, и подается на выход устройства.

Устройство размещено на объекте эксплуатации и постоянно включено. В таком случае при случайном или злонамеренном обрыве кабелей на трех стыках (вход, выход и управление) персонал оперативно способен выявить такую внештатную ситуацию.

Ввод же ключевой информации происходит периодически, и большую часть времени стык ввода ключевой информации не используется. Поэтому существует вероятность того, что злоумышленник может скрытно подключиться к устройству криптографической защиты информации и вмешаться в его работу.

Возникает задача защиты тракта ввода ключевой информации.

2.2 Механические методы защиты

Если разъем для ввода ключевой информации находится на корпусе устройства, то имеющий физический доступ к устройству злоумышленник может подключить к нему свое оборудование. Для защиты от такого рода атаки следует предусмотреть закрытие разъема отдельной крышкой, прилегающей к корпусу устройства. Крышка должна пломбироваться. Конструкция крышки должна быть разработана так, чтобы при попытке доступа к разъему пломба повреждалась и это могло быть выявлено персоналом на объекте эксплуатации.

Также следует предусмотреть наличие отдельных электрических цепей, замыкаемых при подключении кабеля и открытии крышки, сигналы на которых должны анализироваться устройством для выявления факта несанкционированного доступа с

записью события в журнал безопасности и активацией режима аварийной блокировки работы устройства.

2.3 Методы защиты от утечки в электромагнитных полях

Поскольку информация в устройстве передается при помощи электрических сигналов, при работе устройство излучает электромагнитные волны. Злоумышленник, не имеющий физического доступа к устройству, может удаленно детектировать эти волны и получить доступ к криптографически опасной информации. Для защиты от атаки такого рода следует поместить устройство в цельнометаллический корпус. Крышка, закрывающая разъем ввода ключевой информации, должна плотно прилегать к корпусу устройства, чтобы исключить излучение через щели.

Этого достаточно для защиты тракта ввода ключевой информации во время его неиспользования. Однако при вводе ключевой информации крышка открыта и к разъему ввода ключевой информации подключен кабель, соединяющий устройство криптографической защиты информации с устройством ввода ключевой информации. При передаче ключевой информации в устройство криптографической защиты информации по цепям кабеля также излучаются электромагнитные волны.

Их можно ослабить, уменьшив уровень электрических сигналов и поместив кабель в сплошную металлическую оплетку, соединенную с корпусом устройства. В идеале, кабель также должен иметь цельнометаллический корпус.

2.4 Информационно-логические методы защиты

Если злоумышленник не имеет физического доступа к устройству и не может детектировать электромагнитные волны, но может получить доступ к носителю ключевой информации и произвести его модификацию, например, внедрить в состав информации, передаваемой в устройства криптографической защиты информации, кодовую последовательность, активирующую аппаратный эксплоит в устройстве, то для защиты от атаки такого рода следует предусмотреть специальный протокол обмена между устройством криптографической защиты информации и устройством ввода ключевой информации, который будет модифицировать информацию, считываемую с носителя ключевой информации. Так активирующая кодовая последовательность будет разбиваться на отрезки, неспособные активировать аппаратный эксплоит.

2.5 Требования к устройству ввода ключевой информации

Однако защиты одного только устройства криптографической защиты информации недостаточно. Устройство ввода ключевой информации также должно быть спроектировано таким образом, чтобы исключить возможность утечки ключевой информации и криптографически опасной информации. Те же требования по наличию цельнометаллического корпуса и плотно прилегающих крышек актуальны и для него.

Кроме того, для исключения возможности модификации злоумышленником устройства ввода ключевой информации (например, внесения изменений в электрическую схему или программное обеспечение) корпус устройства должен пломбироваться.

Дополнительно следует предусмотреть контроль целостности программного обеспечения устройства ввода ключевой информации устройством криптографической защиты информации. Для проведения контроля программное обеспечение устройства ввода ключевой информации должно передаваться в устройства криптографической защиты информации, которое должно производить подсчет контрольной суммы криптографическим методом и выдавать по стыку управления результат, отображаемый персоналу на объекте эксплуатации. Контроль целостности должен происходить перед каждым вводом ключевой информации. При неуспешном исходе контроля ввод ключевой информации производиться не должен.

3 Определение перечня угроз и методов защиты

3.1 Список угроз

В банке данных угроз безопасности информации ФСТЭК [13] был приведен поиск угроз, которые могут воздействовать на разрабатываемое устройство. Составлен список, для каждого из элементов которого определены методы защиты. Угрозы безопасности и соответствующие им методы защиты занесены в таблицу 1.

Таблица 1 – Угрозы безопасности и соответствующие им методы защиты

Идентификатор угрозы	Описание угрозы	Методы защиты
УБИ.139	Угроза преодоления физической защиты	Пломбирование винтов, скручивающих корпус устройства и крышку. Организационные меры, препятствующие попаданию устройства к посторонним лицам Контроль целостности программного обеспечения
УБИ.124	Угроза подделки записей журнала регистрации событий	
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Прореживание передаваемой информации Маскирование передаваемой информации Контроль целостности передаваемой информации
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Контроль целостности передаваемой информации
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	Выбор дисплея с пониженной яркостью Маскирование отображения кодов доступа на дисплее устройства
УБИ.111	Угроза передачи данных по скрытым каналам	Тщательное экранирование устройства

3.2 Описание угроз

УБИ 139. Угроза заключается в возможности осуществления нарушителем практически любых деструктивных действий в отношении дискредитируемой информационной системы при получении им физического доступа к аппаратным средствам вычислительной техники системы путём преодоления системы контроля физического доступа, организованной в здании предприятия.

Данная угроза обусловлена уязвимостями в системе контроля физического доступа (отсутствием замков в помещении, ошибками персонала и т.п.).

Реализация данной угрозы возможна при условии успешного применения нарушителем любого из методов проникновения на объект (обман персонала, взлом замков и др.)

Последствия реализации угрозы: нарушение конфиденциальности, целостности и доступности.

Меры защиты: Пломбирование винтов, скручивающих корпус устройства и крышку, организационные меры, препятствующие попаданию устройства к посторонним лицам, контроль целостности программного обеспечения.

УБИ 124. Угроза заключается в возможности внесения нарушителем изменений в журналы регистрации событий безопасности дискредитируемой системы (удаление компрометирующих нарушителя записей или подделка записей о не произошедших событиях) для введения в заблуждение её администраторов или сокрытия следов реализации других угроз.

Данная угроза обусловлена недостаточностью мер по разграничению доступа к журналу регистрации событий безопасности. Реализация данной угрозы возможна в одном из следующих случаев: технология ведения журналов регистрации событий безопасности предполагает возможность их редактирования и нарушитель обладает необходимыми для этого привилегиями; технология ведения журналов регистрации событий безопасности не предполагает возможность их редактирования, но нарушитель обладает привилегиями, необходимыми для осуществления записи в файлы журналов, а также специальными программными средствами, способными обрабатывать файлы журналов используемого в дискредитируемой системе формата

Последствия реализации угрозы: нарушение целостности.

Меры защиты: Пломбирование винтов, скручивающих корпус устройства и крышку, организационные меры, препятствующие попаданию устройства к посторонним лицам, контроль целостности программного обеспечения.

УБИ 115. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информации, вводимой и выводимой на периферийные устройства, путём перехвата данных, обрабатываемых контроллерами периферийных устройств. Данная угроза обусловлена недостаточностью мер защиты информации от утечки и контроля потоков данных, а также невозможностью осуществления защиты вводимой и выводимой на периферийные устройства информации с помощью криптографических средств (т.к. представление пользователям системы информации должно осуществляться в доступном для понимания виде). Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на

установку и запуск специализированных вредоносных программ, реализующих функции «клавиатурных шпионов» (для получения нарушителем паролей пользователей), виртуальных драйверов принтеров (перехват документов, содержащих защищаемую информацию) и др.

Последствия реализации угрозы: нарушение конфиденциальности.

Методы защиты: Прореживание передаваемой информации, Маскирование передаваемой информации, контроль целостности передаваемой информации

УБИ 027. Угроза заключается в возможности дезинформирования пользователей или автоматических систем управления путём подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации, а также подмены или искажения информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства. Данная угроза обусловлена слабостями мер антивирусной защиты и контроля достоверности входных и выходных данных, а также ошибками, допущенными в ходе проведения специальных проверок аппаратных средств вычислительной техники. Реализация данной угрозы возможна при условии наличия в дискредитируемой информационной системе вредоносного программного обеспечения (например, виртуальных драйверов устройств) или аппаратных закладок

Последствия реализации угрозы: нарушение целостности.

Методы защиты: Контроль целостности передаваемой информации.

УБИ 067. Угроза заключается в возможности неправомерного случайного или преднамеренного ознакомления пользователя с информацией, которая для него не предназначена, и дальнейшего её использования для достижения своих или заданных ему другими лицами (организациями) деструктивных целей. Данная угроза обусловлена уязвимостями средств контроля доступа, ошибками в параметрах конфигурации данных средств или отсутствием указанных средств. Реализация данной угрозы не подразумевает установку и использование нарушителем специального вредоносного программного обеспечения. При этом ознакомление может быть проведено путём просмотра информации с экранов мониторов других пользователей, с отпечатанных документов, путём подслушивания разговоров и др.

Последствия реализации угрозы: нарушение конфиденциальности.

Методы защиты: Выбор дисплея с пониженной яркостью, Маскирование отображения кодов доступа на дисплее устройства.

УБИ 111. Угроза заключается в возможности осуществления нарушителем неправомерного вывода защищаемой информации из системы, а также передаче

управляющих команд путём её нестандартного (незаметного, скрытого) размещения в легитимно передаваемых по сети (или сохраняемых на отчуждаемые носители) открытых данных путём её маскирования под служебные протоколы, сокрытия в потоке других данных (стеганография), использования скрытых пикселей («пикселей отслеживания») и т.п.

Данная угроза обусловлена недостаточностью мер защиты информации от утечки, а также контроля потоков данных. Реализация данной угрозы возможна при: наличии у нарушителя прав в дискредитируемой системе на установку специализированного программного обеспечения, реализующего функции внедрения в пакеты данных, формируемых для передачи в системе, собственной информации; доступа к каналам передачи данных; посещении пользователем сайтов в сети Интернет и открытия электронных писем, содержащих скрытые пиксели.

Последствия реализации угрозы: нарушение конфиденциальности.

Методы защиты: Тщательное экранирование устройства

В дальнейшем при разработке устройства описанные меры защиты будут реализованы.

4 Обоснование конструкции с учетом специальных требований

4.1 Внешний вид устройства

Требуется разработать комбинированное устройство ввода ключевой информации, позволяющее вводить ключевую информацию как с оптического диска, так и со смарт-карты. Следует определить, как оно может выглядеть.

Поскольку применяются обычные оптические диски, то имеет смысл использовать и обычный привод для их считывания. Можно взять внешний привод, подключаемый по USB – он легкий и компактный. Но у него есть один сильный недостаток – у него пластиковый корпус. А значит при работе будут излучаться электромагнитные поля, из которых может быть извлечена хранящаяся на диске информация. Поэтому нужно поместить этот привод в металлический корпус.

Чтобы обеспечить устойчивую механическую фиксацию гладкой пластиковой поверхности, нужно использовать внутренний привод чтения оптических дисков. Используемый в настольных компьютерах привод имеет большую высоту, поэтому выбор падает на используемый в ноутбуках. Он тонкий и у него есть отверстия для крепления при помощи винтов.

Считыватель смарт-карт следует разработать самостоятельно – достаточно обеспечить механический контакт, а напряжение питания, сила тока и скорость работы электрического интерфейса по сравнению с диском незначительны. Соединитель для установки карты можно монтировать на печатную плату.

Итак, корпус устройства должен быть металлический и в нем должны быть установлены соединитель для установки смарт-карты и привод для чтения оптического диска. На случай необходимости записи журнала безопасности на внешней носитель следует предусмотреть также разъем для подключения USB флеш накопителя.

Со всеми этими тремя элементами конструкции пользователь непосредственно обращается, поэтому нужно расположить их на передней панели. А чтобы исключить излучение электромагнитных полей через переднюю панель, предусмотреть открывающуюся металлическую крышку, плотно прилегающую к корпусу при закрывании.

В случае, если оператор забудет закрыть крышку, должен быть предусмотрен механизм надежной механической фиксации при помощи пружины и информирование электроники устройства о факте закрытия. При открытой дверце ввод ключевой информации должен блокироваться.

На задней панели нужно расположить разъем питания и разъем для подключения к внешнему устройству криптографической защиты информации, в который будет вводиться ключевая информация. Разъемы следует выбрать металлические завинчивающиеся, обеспечивающие экранировку электромагнитных излучений. В режимах работы устройства, не требующих подключения кабелей к разъемам, на них должны быть установлены металлические крышки. Также потребуется тумблер питания.

Устройство получается имеющим вид параллелепипеда, с невысокими передней и задней панелями. На верхней стороне устройства будет помещен жидкокристаллический дисплей и клавиатура для отображения пользовательского меню и навигации по нему. Верхняя сторона устройства будет съемной.

Клавиатуру лучше применить пленочную, подключаемую к плате гибким шлейфом, тогда щель, в которую будет проходить шлейф, будет минимальной ширины. Дисплей нужно прикрепить к печатной плате, а плату прикрепить к верхней (съемной) стороне устройства. Поскольку экран является дырой в экранировке, потребуется предусмотреть сплошную металлизацию на верхней стороны платы, а также спроектировать отдельный изолированный отсек внутри корпуса устройства.

В устройстве получается две платы – индикации (поля от которой будут выходить наружу через дисплей) и управления (на которой размещен соединитель для подключения смарт-карт и к которой подключается привод чтения оптических дисков). Для изоляции плат друг от друга необходимо соединить цепи питания и данных между ними через проходные фильтры, ввинчиваемые в стенку отсека, в который помещается плата индикации после закрывания крышки.

Так как обеспечить идеально точную подгонку двух металлических частей (основная часть корпуса и передняя дверца, основная часть корпуса и верхняя крышка) невозможно, то потребуются экранирующие прокладки в местах соприкосновения.

Приняв во внимание величину тока, потребляемого оптическим приводом при раскручивании диска, и общие соображения по размещению на объекте эксплуатации, следует питать устройство от внешнего источника постоянного тока напряжением 12 В. Устройство при своей работе создает в цепях питания и земли помехи, анализ которых может быть предпринят злоумышленником, поэтому питание требуется фильтровать (относительно корпуса), и в схеме устройства появляется фильтр питания из двух звеньев, которые должны быть размещены в изолированных отсеках и соединяться через проходные фильтры, ввинчиваемые в стенки отсеков. В отдельном отсеке нужно

разместить тумблер питания (так как он пластиковый, и через него возможно излучение электромагнитных полей).

Также необходимо поместить в отдельный отсек корпуса устройства привод чтения оптических дисков.

В основной части корпуса устройства должно находиться шесть изолированных отсеков:

- тумблера питания;
- звена 1 фильтра питания;
- звена 2 фильтра питания;
- основной платы;
- привода чтения оптических дисков;
- дисплея.

А крышка с установленной на ней платой индикации, дисплеем и клавиатурой опускается на основную часть корпуса так, что плата индикации помещается в изолированный объем дисплея основной части корпуса.

Корпус — фрезерованный металлический. Выбранный металл — алюминий. Подсоединяемые к устройству внешние кабели (питания и данных) должны удовлетворять требованию непрерывности электромагнитной экранировки (иметь сплошную металлическую оплетку).

Применяемые в устройстве проходные фильтры (данных и питания) должны быть подобраны таким образом, чтобы максимально «срезать» избыточные частотные составляющие сигналов и в то же время не нарушать работы устройства (так как данные передаются при перепаде напряжений на некоторой частоте, то если срезать слишком сильно — они не пройдут). При этом следует учесть, что чем большую полосу спектра «режет» фильтр, тем он габаритнее и массивнее.

Также есть и технологические особенности — например, радиус закругления стенки зависят от диаметра фрезы, что накладывает ограничение на минимальный размер отсека, а для сверления отверстий в стенках внутренних отсеков могут потребоваться технологические отверстия во внешних стенках (которые затем закрываются металлическими пробками). Также винты, при помощи которых устройство сворачивается, имеют ненулевой диаметр (поскольку должны обеспечивать механическую прочность).

5 Описание структурной схемы устройства

5.1 Состав устройства

В состав устройства входят следующие основные узлы:

- дисплей;
- клавиатура;
- плата индикации;
- привод чтения оптических дисков;
- плата управления;
- фильтр питания.

Дисплей подключается к плате индикации и принимает данные для вывода пользователю. Клавиатура подключается к плате индикации и передает данные от пользователя. Плата индикации связана цепями питания и данных с платой управления через фильтры. Дисплей, клавиатура и плата индикации размещены в отсеке 1.

Привод чтения оптических дисков подключается к плате управления цепями питания и данных. Привод чтения оптических дисков размещен в отсеке 2.

Смарт-карта вставляется в соединитель, расположенный на плате управления и связана с ней цепями питания и данных. USB флеш накопитель вставляется в соединитель, расположенный на плате управления и связан с ней цепями питания и данных. Внешнее устройство криптографической защиты информации подключается к плате управления через разъем на корпусе устройства и связано с платой управления цепями питания и данных. Плата управления размещена в отсеке 3, смарт-карта и USB флеш накопитель размещены в отсеке 4.

Фильтр питания подключен к плате управления и связан с ней цепями питания. Подача питания осуществляется через разъем на корпусе устройства. Фильтр питания размещен в отсеке 5.

6 Подбор покупных узлов

6.1 Выбор привода чтения оптических дисков

Для поиска привода чтения оптических дисков для ноутбуков использовался сайт компьютерного магазина «НИКС». На дату написания данного текста в его ассортименте было представлено всего три привода – два фирмы Hitachi-LG Data Storage (HLDS) и один фирмы ASUS. Данные о них представлены в таблице 2.

Таблица 2 – Параметры приводов чтения оптических дисков для ноутбуков

Параметр	HLDS		ASUS
	GTC2N	BU40N	SDRW-08U1MT
Интерфейс	SATA		
Размеры, мм	128x12.7x129	128x11x128	128x10x127
Напряжение питания, В	5		
Потребляемый ток, А	1.8	1.5	1.8
Чтение CD	да	да	да
Чтение DVD	да	да	да
Чтение BD	нет	да	нет
Цена, руб	2225	10320	3406

Чтения Blu-Ray дисков для наших задач не требуется. Потребляемый ток и напряжение питания у двух DVD моделей одинаковы. Исходя из цены был выбран привод GTC2N.



Рис. 1 – Выбранный привод чтения оптических дисков

В компьютерах аппаратная поддержка этого интерфейса встроена в чипсет, а за программную поддержку отвечает операционная система. Но аппаратные платформы от Intel/AMD уже давно нельзя считать доверенными из-за наличия в составе чипсетов/процессоров отдельных «сопроцессоров безопасности» со своими операционными системами и закрытыми прошивками (Intel ME [14] и AMD PSP [15]), имеющих привилегированный доступ к ресурсам системы. В мобильных устройствах

используются системы на кристалле [16], которые можно считать более безопасными, и поддержка SATA редко, но встречается (например, в [17]). Однако аппаратная конфигурация для работы операционной системы (пусть и хорошо оптимизированной версии Linux) достаточно сложная – требуется минимум три микросхемы:

- процессора – с частотой минимум 100 МГц;
- оперативной памяти – размером от 16 Мб;
- флеш памяти – размером хотя бы 8 Мб.

Причем соединяться процессор и оперативная память должны по параллельной шине (с повышенными требованиями к конструкции печатной платы). Из сложных высокоскоростных интерфейсов повсеместно встречаются Ethernet и USB.

6.2 Выбор преобразователя USB-SATA

Для выбора преобразователя был использован сайт «OZON» – там много моделей разной цены и качества, из них для сравнения были выбраны 4 и их параметры описаны в таблице 3.

Таблица 3 – Параметры преобразователей USB-SATA

Параметр	Espada	PALMEXX	VCOM	KS-is
	PA023U3	USB2.0-SATA	USB3.0-SATA	USB2.0-SATA
Версия интерфейса USB	3.0	2.0	3.0	2.0
Длина кабеля, см	20	нет данных	40	40
Цена, руб	359	590	520	499

Для привода чтения оптических дисков интерфейс USB 3.0 явно избыточен по пропускной способности, поэтому выбираем среди имеющих интерфейс USB 2.0. И по критерию минимизации цены выбираем преобразователь фирмы KS-is.



Рисунок 2 – Выбранный преобразователь USB-SATA

6.3 Выбор соединителя смарт-карт

Для поиска соединителей смарт-карт использовался сайт электронных компонентов «Компэл». Был выбран раздел «Держатели карт памяти», в нем тип «Smart Card» и произведен поиск в примечаниях (Surface Mount, Push In, Pull Out). Было найдено несколько десятков результатов.

С учетом того, что смарт карты (и, соответственно, соединители для них) бывают разных физических размеров [18], дальнейший поиск происходил вручную по фотографиям. Нам требовался соединитель для Full-size (1FF) карты (имеющей габариты 85.6 x 53.98 x 0.76 мм) с позолоченными контактами.

В качестве такового была выбрана модель CCM01-2027 LFT фирмы C&K Components с функцией определения наличия карты и диапазоном рабочих температур от минус 40 до 85 градусов Цельсия.



Рисунок 3 – Выбранный соединитель смарт-карт

6.4 Выбор дисплея

Дисплей устройства должен иметь малые габариты и напряжение питания, желательно также наличие металлического корпуса и надежных креплений. Количество пикселей особого значения не имеет. Количество цветов также не важно.

По этим параметрам достаточно простого и механически прочного монохромного дисплея с высокой контрастностью. По этим параметрам был выбран дисплей MT-12864A-3FLG-3V0-T фирмы «МЭЛТ» на базе микросхем российского производства. Он обладает разрешением 128 x 64 точки, желто-зеленой подсветкой, имеет физические размеры 93 x 70 x 13 мм и работает в диапазоне температур от минус 30 до 70 градусов Цельсия. Напряжение питания логики – 3 В, напряжение питания подсветки – 5 В.

Экран закрыт прочным стеклом и по краям металлической крышкой, крепится к плате из стеклотекстолита, имеющей четыре крепежных отверстия диаметром 2.7 мм. Сигнальные цепи, цепи земли и питания выведены на ряд из двадцати отверстий диаметром 1 мм, в которые могут быть запаяны провода.

Интерфейс обмена с микроконтроллером – параллельный восьмиразрядный, описание команд и пример программы приведены на сайте производителя.



Рисунок 4 – Выбранный дисплей

6.5 Выбор клавиатуры

Клавиатура устройства используется для перемещения по пунктам меню и ввода числовых значений. То есть должны присутствовать цифровые клавиши и стрелки. Желательна работоспособность в широком диапазоне температур.

По этим параметрам была выбрана гибкая пленочная клавиатура ТЕСТА СК-24 с антибликовым устойчивым к воздействиям агрессивных сред покрытием лицевой стороны. Обратной стороной клавиатура приклеивается к корпусу устройства.

Клавиатура содержит 18 клавиш с нанесенными изображениями «1», «2», «3», «4», «5», «6», «7», «8», «9», «0», «.», «F», «ESC», «ENTER», «←», «→», «↑», «↓», имеет физические размеры: 68 x 87 мм при толщине около 2 мм и работоспособна в диапазоне температур от минус 20 до 50 градусов Цельсия. Соединяется с «внешним миром» при помощи гибкого десятиконтактного шлейфа (один контакт не задействован) длиной 90 мм, выходящим из ее нижней стороны. Клавиатура позволяет коммутировать напряжения не более 36 В и имеет сопротивление замкнутых цепей не более 100 Ом.

С программной точки зрения клавиатура представляет собой матрицу из колонок и столбцов, подавая сигналы с логическими уровнями «0» и «1» на которые, и считывая с которых, можно определить нажатую клавишу.



Рисунок 5 – Выбранная клавиатура

7 Описание функциональных схем устройства

7.1 Описание функциональной схемы платы индикации

Экран требует напряжения питания 5 В для подсветки и 3.3 В. Клавиатура отдельных выводов питания не имеет (она представляет из себя матрицу соединений с замыкающимися цепями). Микроконтроллеру необходимо питание 3.3 В.

Напряжение питания 5 В поступает на плату индикации с платы управления. Далее оно поступает на подсветку дисплея и преобразователь напряжения. Преобразователь напряжения формирует напряжение 3.3 В, от которого питаются микроконтроллер и логическая часть дисплея.

Микроконтроллер платы индикации обменивается данными с дисплеем и клавиатурой по интерфейсу GPIO с уровнем сигналов 3.3 В, и с микроконтроллером платы управления по интерфейсу UART с уровнем сигналов 3.3 В.

7.2 Описание функциональной схемы платы управления

Привод чтения оптических дисков требует напряжения питания 5 В, а входным для устройства является напряжение 12 В. Значит потребуются преобразователь с минимальной выходной мощностью 10 Вт (5В x 1.8А для привода). Смарт-карты разных поколений работают с разными напряжениями питания (5В/3.3В/1.8В), поэтому может потребоваться дополнительный преобразователь напряжения. Для USB флеш накопителя нужно питание 5В. Микроконтроллеру необходимо питание 3.3 В.

Напряжение питания 12 В поступает на плату управления с фильтра питания. Далее оно преобразовывается в напряжение питания 5 В. Напряжение 5 В используется для питания USB флеш накопителя и привода чтения оптических дисков. Также оно подается на плату индикации и преобразователь напряжения. Преобразователь напряжения формирует напряжение 3.3 В, от которого питается микроконтроллер.

Микроконтроллер платы управления обменивается информацией с микроконтроллером платы индикации по интерфейсу UART с уровнем сигналов 3.3 В и со смарт-картой по интерфейсу USART с уровнем сигналов 3.3 В. Микроконтроллер обменивается информацией по интерфейсу USB с приводом чтения оптических дисков через адаптер USB-SATA. Также микроконтроллер обменивается данными с USB флеш накопителем по интерфейсу USB и с внешним устройством криптографической защиты информации по интерфейсу USB.

8 Выбор элементной базы

8.1 Порядок выбора

Элементы будут подбираться от сложного к простому – то есть сначала следует выбрать микроконтроллеры, потом вспомогательные микросхемы, которые к ним подходит, и наконец пассивные элементы – резисторы, конденсаторы и т.д. Для начала следует определиться, какие интерфейсы для подключения покупных блоков, внешнего устройства и между платами внутри устройства необходимы.

8.2 Выбор элементной базы платы индикации

К плате индикации должны подключаться:

- клавиатура (по интерфейсу GPIO [19]);
- дисплей (по интерфейсу GPIO);
- плата управления (по интерфейсу UART [20]).

Подключать их нужно к микроконтроллеру. Особых требований к скорости его работы нет, и выбрать можно в принципе любой – но из соображений срока поддержки и энергопотребления имеет смысл выбрать более новый, например STM32L471RET6 [21] фирмы STMicroelectronics. Его параметры:

- ядро ARM Cortex-M4;
- частота работы до 80 МГц;
- 128 Кб оперативной памяти;
- 512 Кб флеш-памяти;
- напряжение питания от 1.71 В до 3.6 В.

На случай отладки можно также предусмотреть наличие преобразователя UART - RS-232 с одним приемником и одним передатчиком – например, MAX3221EAE+ [22] фирмы Maxim Integrated. Микроконтроллер питается от напряжения 3.3 В, поэтому был установлен преобразователь из напряжения 5 В, поступающего на вход платы индикации от платы управления, в напряжение 3.3 В. В качестве преобразователя была применена микросхема LP2985AIM5-3.3/NOPB [23] фирмы Texas Instruments.

8.3 Выбор элементной базы платы управления

К плате управления должны подключаться:

- привод чтения оптических дисков через преобразователь (в режиме USB device);
- флеш накопитель (в режиме USB device);

- внешнее устройство (в режиме USB device);
- смарт-карта (по интерфейсу USART);
- плата индикации (по интерфейсу UART).

В топовом STM32H743XIH6 [24] от STMicroelectronics (микроконтроллер с частотой 480 МГц) таких интерфейсов всего 2. в микроконтроллере STM32L151VBT6A [25] начального уровня – и вовсе 1. Разнести внешнее оборудование и внутреннее оборудование по разным портам USB имеет смысл даже с точки зрения производительности (не говоря уже о безопасности), а внутреннее оборудование можно повесить на один порт через хаб.

Обмен информацией с картой и диском одновременно происходить не должен, поэтому можно подключить карту через промежуточный контроллер, а его подключить к основному опять же по USB. Такое решение усложняет и удорожает разработку и изготовление устройства, но является более универсальным. Например, можно отлаживать работу с картой непосредственно с компьютера (предусмотрев резисторы на цепях USB между контроллерами, которые можно снять и припаяться к контактам), или использовать отлаженную программно-аппаратную комбинацию в другом проекте. А на тот случай, если потребуется оптимизировать по цене и ограничиться одним контроллером, имеет смысл оба контроллера выбрать одинаковыми.

С оглядкой на планируемые к применению программные решения для использования в качестве контроллеров управления и карты была выбрана микросхема STM32F415RGT6 [26] фирмы STMicroelectronics со следующими характеристиками:

- ядро ARM Cortex-M4;
- частота работы до 168 МГц;
- 192+4 Кб оперативной памяти;
- 1 Мб флеш памяти;
- USB 2.0 full-speed контроллер;
- USB 2.0 high-speed контроллер (с поддержкой ULPI [27]);
- напряжение питания от 1.8 В до 3.6 В.

Контроллеров USB в этой микросхеме два, и они имеют разные параметры.

Контроллер USB_FS:

- буфер на прием+передачу объемом 320x35 бит;
- количество endpoints: 4;
- встроенный FS OTG PHY [28].

Контроллер USB_HS:

- буфер на прием+передачу объемом 1024x35 бит;
- количество endpoints: 6;
- встроенный FS OTG PHY;
- поддерживается также внешний ULPI приемопередатчик.

Первый контроллер USB попроще, и поддерживает режимы low-speed (1.5 Мбит/с) и full-speed (12 Мбит/с), а второй поддерживает еще и режим high-speed (480 Мбит/с), но через внешнюю микросхему. Контроллер HS OTG PHY не был интегрирован внутрь, чтобы не увеличивать площадь кристалла и энергопотребление.

В качестве приемопередатчика ULPI можно бы использовать микросхему STULPI01 от все той же STMicroelectronics. У корпусов с шариковыми выводами ниже надежность крепления и теплоотдача, поэтому выбран был приемопередатчик USB3300-EZK-TR от фирмы Microchip Technology с планарными выводами [29] и теплоотводящей площадкой внизу корпуса.

Микроконтроллер подключается к приемопередатчику ULPI по 12 цепям (8 данных и 4 управления). Тактовую частоту можно также подать с микроконтроллера.

Дальше к приемопередатчику ULPI нужно подключить по дифференциальной паре [30] трехпортовый USB хаб. В качестве хаба была выбрана микросхема TUSB4041I [31] фирмы Texas Instruments. У нее четыре порта, задействованы будут три из них.

Чтобы информация с карты и информация с диска не могли перемешиваться, было предусмотрено аппаратное отключение диска. Дополнительно была произведена гальваническая развязка [32] цепей передачи данных при помощи микросхемы ADuM3160BRWZ [33] фирмы Analog Devices. Поскольку привод чтения оптических дисков потребляет значительный ток (1.8 А) от источника питания напряжением 5 В, а входное напряжение питания устройства 12 В, был установлен импульсный преобразователь [34] ST1S40IPUR [35] фирмы STMicroelectronics (у импульсных преобразователей эффективность выше, чем у линейных [36], но выше и уровень шумов).

Питание платы управления будет формироваться из входного при помощи гальванически развязанного преобразователя напряжения TMR 6-1211 [37] фирмы Traco Electronic. Формируемое им напряжение 5 В будет направляться также на плату индикации и питать USB порт съемного флеш накопителя. Основное питание для применяемых на плате микросхем – 3.3 В, будет формироваться из 5 В при помощи еще одного преобразователя ST1S40IPUR.

Микросхема USB3300 имеет вход VBUS, измеряя уровень напряжения на котором определяет, подключено ли к ней USB устройство (в данном случае хаб). Можно

предусмотреть возможность подавать напряжение 5 В на этот вход под управлением сигнала микроконтроллера при помощи переключателя TPS2069CDG NR-2 [38] фирмы Texas Instruments.

Управлять подачей питания на съемный флеш накопитель будет хаб (у него есть соответствующие выводы) при помощи переключателя TPS2553QDBVRQ1 [39] фирмы Texas Instruments. Хаб одного только напряжения 3.3 В недостаточно, нужно еще 1.1 В, которое можно сформировать микросхемой линейного преобразователя напряжения TLV71211DBV [40] фирмы Texas Instruments.

Вместо того, чтобы подключить напрямую к микроконтроллеру смарт-карту, проще выполнить сопряжение по примеру [41] STMicroelectronics при помощи микросхемы ST8024CTR [42], которая будет выполнять функции защиты и управления картой.

Для защиты USB порта микроконтроллера, к которому подключается внешнее устройство, от разрядов статического электричества, будет использована микросхема USBLC6-2P6 [43] фирмы STMicroelectronics.

Для возможности использования платы совместно с внешним устройством, подключаемым по интерфейсу RS-232 на плате были предусмотрены площадки под установку преобразователя USB-UART FT231XQ [44] фирмы FTDI и преобразователя UART-RS232 MAX3221EAE+ фирмы Maxim Integrated, но устанавливаться эти микросхемы и относящиеся к ним конденсаторы сейчас не будут. Так появляется второй вариант платы.

Обмен по цепочке микроконтроллер – преобразователь USB-UART – преобразователь UART-RS232 может показаться странным (у контроллера есть свободный UART), поэтому можно предусмотреть третий вариант платы, где микроконтроллер соединяется напрямую с преобразователем UART-RS232. Отличия между вторым вариантом и третьим будет в резисторах нулевого сопротивления на цепях к преобразователю UART – RS-232.

8.4 Оценка подсистемы питания

Далее требуется посчитать, смогут ли выбранные преобразователи напряжения пропустить достаточный для работы устройства в максимально нагруженном режиме ток. Значения для элементов были взяты из таблиц и графиков, приведенных в документации к ним. Для одних элементов (например, постоянно включенных светодиодов) эти цифры могут быть достаточно точными, а для других (например, приемопередатчика) варьироваться от условий применения.

Плата индикации. Дисплей потребляет 3 мА от напряжения 3.3 В (логика) и 150 мА от напряжения 5 В (подсветка). Приемопередатчик RS-232 при работе на скорости 120 Кбит/с на нулевую емкость потребляет 5 мА от напряжения 3.3 В, но уже 20 мА при работе на емкость 5 нФ. Максимальный ток по всем цепям питания микроконтроллера – 150 мА, он растет с ростом тактовой частоты и температуры. Например, на 1 МГц при 25 °С – 0.27 мА, а при 125 °С – уже 1.57 мА, на 80 МГц при 25 °С – 11.22 мА, а при 125 °С – уже 13.3 мА. И еще следует учесть зависимость тока потребления от емкости нагрузки.

Оценка потребляемого платой индикации тока от источника напряжения 3.3 В:

- дисплей – 3 мА;
- микроконтроллер – 14 мА;
- приемопередатчик – 20 мА.

Всего – 37 мА. Преобразователь напряжения LP2985 может обеспечить 150 мА. Проверка по 3.3 В прошла.

Поскольку преобразователь напряжения линейный, то они будут потреблять эти же 37 мА от входного напряжения 5 В, а разница $((5 - 3.3) * 37 = 62.9 \text{ мВт})$ будет рассеиваться в виде тепла.

Оценка потребляемого платой индикации тока от источника напряжения 5 В:

- дисплей – 150 мА;
- преобразователь 5 В в 3.3 В – 37 мА.

Всего – 187 мА.

Привод чтения оптических дисков потребляет 1.8 А от источника напряжения 5 В. В качестве источника выступает импульсный преобразователь из 12 В в 5 В. Его эффективность (исходя из документации) при данных токе и напряжениях около 92%. То есть привод чтения оптических дисков будет потреблять $(5 / 12) * 1.8 * (100 / 92) = 0.82 \text{ А}$ от источника питания напряжением 12 В.

Микроконтроллер платы управления, работая на частоте 168 МГц, потребляет 87 мА при температуре 25 °С от источника напряжения 3.3 В и 109 мА при температуре 125 °С. Таких микроконтроллеров на плате управления два. Приемопередатчик ULPI при передаче в режиме high-speed потребляет 29 мА от источника питания напряжения 3.3 В, хаб при наличии четырех подключенных устройств в режиме high-speed – 76 мА от источника напряжения 3.3 В и 86 мА от источника напряжения 1.1 В.

Преобразователь TLV71211 из 3.3 В в 1.1 В может обеспечить ток 300 мА. Раз он линейный, то будет потреблять от 3.3 В те же 86 мА, а остальное $((3.3 - 1.1) * 86 = 189.2 \text{ мВт})$ рассеивать в виде тепла.

Максимальный потребляемый микросхемой ST8024 ток от источника напряжения 3.3 В – 1.5 мА, и от источника напряжения 5 В – 200 мА.

Если на плате будет установлен преобразователь USB в UART, то дополнительно потребуется еще 8.4 мА от источника напряжения 3.3 В, а при наличии преобразователя из UART в RS-232, работающего на скорости 235 кбит/с на нагрузку емкостью 5 нФ – еще 35 мА.

Оценка тока потребления платы управления от источника напряжения 3.3 В:

- микроконтроллеры – $109 * 2 = 218$ мА;
- приемопередатчик ULPI – 29 мА;
- хаб – $76 + 86 = 162$ мА;
- микросхема ST8024 – 2 мА;
- преобразователь USB в UART – 9 мА;
- преобразователь UART в RS-232 – 35 мА.

Всего – 455 мА. Преобразователь ST1S40 при входном напряжении 5 В, выходном напряжении 3.3 В и токе 0.5 А имеет ориентировочную эффективность 94%, поэтому от источника 5 В будет потреблять $(3.3 / 5) * 0.455 * (100 / 94) = 0.32$ А.

Микросхема гальванической развязки ADuM3160 имеет двухстороннее питание и с каждой стороны потребляет 8 мА. С учетом ее и микросхемы ST8024 ток от источника напряжением 5 В будет составлять $0.32 + 0.2 + 0.008 = 0.528$ А. Если учесть плату индикации, также питающуюся от напряжения 5 В (0.187 А), подается итоговое значение 0.715 А. Преобразователь TMR 6-1211 обеспечивает максимальный выходной ток 1.2 А при эффективности 83%, то есть от напряжения 12 В будет потреблять $(5 / 12) * 0.715 * (100 / 83) = 0.36$ А.

Обе платы и привод чтения оптических дисков будут потреблять от источника питания с напряжением 12 В: $0.36 + 0.82 = 1.18$ А.

Если же использовать еще и USB флеш накопитель, то потребуется дополнительный ток. Заранее сказать, какой накопитель подключит пользователь, невозможно, но согласно спецификации USB 2.0 устройство может потреблять ток 0.5 А. В этом случае ток потребления от источника питания с напряжением 5 В составит $0.715 + 0.5 = 1.215$ А, что на 15 мА превышает максимально допустимый для преобразователя TMR 6-1211. При условии, что преобразователь выдержит, ток потребления от напряжения 12 В будет составлять в этом случае $(5 / 12) * 1.215 * (100 / 83) = 0.61$ А, а обе платы и привод чтения оптических дисков будут потреблять от источника питания с напряжением 12 В: $0.61 + 0.82 = 1.43$ А.

В случае применения основного исполнения платы управления преобразователь USB в UART и преобразователь UART в RS-232 на плате не устанавливаются, и 44 мА от источника питания 3.3 В экономятся, и от источника питания 5 В устройство будет потреблять на $(3.3 / 5) * 0.044 * (100 / 94) = 31$ мА меньше, то есть преобразователь TMR 6-1211 будет работать на пределе, но не превышать его. Можно предположить, что при работе в широком диапазоне температур и входных напряжений при работе устройства с флеш накопителем, картой и оптическим диском одновременно будут наблюдаться сбои. Поэтому в следующей модификации устройства желательно рассмотреть возможность замены преобразователя напряжения TMR 6-1211 на более мощный.

Однако поскольку одновременная работа всех трех устройств сразу (флеш накопитель, карта и оптический диск) нежелательна с точки зрения безопасности, можно считать вышеописанную схему допустимой.

Составленная схема питания приведена в приложении Г.

9 Описание принципиальных схем устройства

9.1 Принципы проектирования систем на основе микроконтроллеров

Микроконтроллер – это устройство, которое содержит в своем составе:

- процессор (т.е. арифметическо-логическое устройство);
- оперативную память;
- постоянную память;
- модули внешних интерфейсов.

Все это размещается на одном кристалле и упаковывается в один корпус. Количество выводов у корпуса может отличаться, для одного и того же микроконтроллера как правило есть несколько вариантов. Чем больше выводов – тем больше модулей внешних интерфейсов будет доступно. Для одного и того же интерфейса обычно есть возможность вывода на разные контакты. Выбор того, что и куда выводить определяется программно. Если программа никак не настраивает контакт, то он по умолчанию находится в состоянии логического входа (то есть не выдает ничего), но никаких действий при изменении уровня сигнала на этом входе не производится. Часть контактов, (например, применяемых для программирования микроконтроллера) в начале работы программы жестко заданы, остальные задаются в ходе работы программы. Варианты корпусов с выводами питания и земли в пределах семейства обычно унифицируются.

При разработке электрической схемы вначале определяется, какие внешние микросхемы нужны для выполнения заданных функций, а затем подсчитывается, сколько выводов микроконтроллера и в каком режиме требуется задействовать. На основе параметров энергопотребления, производительности и наличия интерфейсов выбирается семейство и микроконтроллер внутри семейства. Далее просматривается таблица выводов для разных корпусов и устанавливается, на какие из них можно назначить требуемые интерфейсы. Выбирается корпус с минимальным количеством контактов, на которые можно (с небольшим запасом) разместить все, что нужно.

Для программирования и отладки микроконтроллера обычно применяется интерфейс JTAG, имеющий 5 контактов:

- TMS – Test Mode Select;
- TCK – Test Clock;
- TDI – Test Data Input;
- TDO – Test Data Output;
- TRST – Test Reset.

Также обычно на разъем программирования выводятся цепь RESET микроконтроллера, цепи питания и земли – всего получается 8 контактов.

Как правило, начинает работу микроконтроллер на частоте в единицы мегагерц, тактируясь от встроенного генератора. Его нестабильность в диапазоне температур не позволяет использовать микроконтроллер для работы с высокоскоростными интерфейсами, поэтому требуется подключение внешнего кварцевого резонатора/генератора на несколько мегагерц. В случае необходимости точного отслеживания времени дополнительно подключается низкочастотный кварцевый резонатор (обычно на 32768 Гц). Рекомендуемые частоты генераторов и емкости соответствующих им конденсаторов приводятся в документации на микроконтроллер.

После сброса микроконтроллер начинает работу в активном режиме (и, соответственно, потребляет максимальное количество энергии на такт), далее под управлением программы он может перейти в один из нескольких низкопотребляющих режимов (каждому соответствует свой диапазон рабочих частот, набор доступных периферийных устройств и уровень энергопотребления). Переход обратно в активный режим возможен по внешнему (для арифметически-логического устройства) событию, например срабатывание таймера или перепаду уровня сигнала на одном из входов.

Загрузка микроконтроллера возможна не только из основной постоянной памяти (программируемой пользователем), но также из встроенной памяти загрузчика (программируемого на заводе, изготовившим микроконтроллер), и даже из оперативной памяти. Выбор режима загрузки определяется контактом с зарезервированной для этого функцией и битами параметров в специальной области постоянной памяти.

9.2 Описание принципиальной схемы платы индикации

Дисплей подключается к микроконтроллеру по 14 цепям, клавиатура — по 9 цепям. Микросхема преобразования уровней RS-232 (MAX3221) имеет 4 контакта управления, будут задействованы 3 из них. Таким образом, требуется 26 контактов, переназначаемых как входы/выходы.

Данные на плату управления и отладочный интерфейс RS-232 передаются по UART, то есть их потребуется два (каждый использует две цепи – на прием и на передачу). Интерфейс программирования JTAG, входы и выходы кварцевых резонаторов (основного и низкопотребляющего), вход выбора режима загрузки и сброса расположены на выделенных контактах – вот еще 11 контактов.

Итого, требуется 41 сигнальных контактов. Микроконтроллер STM32L471 выпускается в следующих корпусах:

- LQFP144 – пластиковый корпус 20 x 20 x 1.6 мм, выводы с четырех сторон;
- UFBGA132 – пластиковый корпус 7 x 7 x 0.6 мм, выводы снизу;
- LQFP100 – пластиковый корпус 14 x 14 x 1.6 мм, выводы с четырех сторон;
- LQFP64 – пластиковый корпус 10 x 10 x 1.6 мм, выводы с четырех сторон.

Будет достаточно минимального 64-х контактного корпуса. Также в этом корпусе 11 контактов земли и питания.

Контакты занесены таблицу 4.

Таблица 4 – Контакты контроллера индикации

Номер контакта	Название контакта	Назначение
1	VBAT	Батарейное питание
2	PC13	Цепь E дисплея
3	PC14-OSC32_IN	Цепь от часовому кварцевому резонатору
4	PC15-OSC32_OUT	Цепь к часовому кварцевому резонатору
5	PH0-OSC_IN	Цепь от основного кварцевому резонатору
6	PH0-OSC_OUT	Цепь к основному кварцевому резонатору
7	NRST	Цепь сброса
8	PC0	Цепь D0 дисплея
9	PC1	Цепь D1 дисплея
10	PC2	Цепь D2 дисплея
11	PC3	Цепь D3 дисплея
12	VSSA/VREF-	Аналоговая земля
13	VDDA/VREF+	Аналоговое питание
14	PA0	Цепь ROW1 дисплея
15	PA1	Цепь ROW2 дисплея
16	PA2	Цепь ROW3 дисплея
17	PA3	Цепь ROW4 дисплея
18	VSS	Земля
19	VDD	Питание
20	PA4	Цепь ROW5 дисплея
21	PA5	Цепь COL1 дисплея
22	PA6	Цепь COL2 дисплея
23	PA7	Цепь COL3 дисплея
24	PC4	Цепь D4 дисплея
25	PC5	Цепь D5 дисплея
26	PB0	Цепь RES дисплея
27	PB1	Цепь RW дисплея
28	PB2	-
29	PB10	-

Продолжение таблицы 4

Номер контакта	Название контакта	Назначение
30	PB11	-
31	VSS	Земля
32	VDD	Питание
33	PB12	-
34	PB13	-
35	PB14	-
36	PB15	-
37	PC6	Цепь D6 дисплея
38	PC7	Цепь D7 дисплея
39	PC8	Цепь E1 дисплея
40	PC9	Цепь E2 дисплея
41	PA8	Цепь COL4 дисплея
42	PA9	Цепь INVALID приемопередатчика RS-232
43	PA10	Цепь FORCE_OFF приемопередатчика RS-232
44	PA11	Цепь ENABLE приемопередатчика RS-232
45	PA12	-
46	TMS	Цепь JTAG
47	VSS	Земля
48	VDD	Питание
49	TCK	Цепь JTAG
50	TDI	Цепь JTAG
51	PC10	Данные на основную плату (USART3_TX)
52	PC11	Данные с основной платы (USART3_RX)
53	PC12	Данные на отладочный RS-232 (UART5_TX)
54	PD2	Данные с отладочного RS-232 (UART5_RX)
55	TDO	Цепь JTAG
56	TRST	Цепь JTAG
57	PB5	Цепь A0 дисплея
58	PB6	-
59	PB7	-
60	BOOT0	Выбор режима загрузки
61	PB8	-
62	PB9	-
63	VSS	Земля
64	VDD	Питание

Условное графическое изображение микроконтроллера занимает много места, поэтому схему следует рисовать на листах формата A1. На первом листе схемы будет размещен микроконтроллер D1 (главный), разъемы программирования и клавиатуры. На

втором листе – точки для подключения дисплея, приемопередатчик RS-232 и преобразователь напряжения LP2985 из 5В в 3.3В.

Для сглаживания пульсаций входного напряжения к каждому контакту питания контроллера требуется подключить по керамическому конденсатору емкостью 100 нФ, и один танталовый конденсатор емкостью 4.7 мкФ.

На вход сброса (также подключаемый к разъему программирования) был подключен конденсатор 100 нФ, используемый для формирования совместно с подтягивающим резистором внутри микроконтроллера линии задержки, что заставит программу микроконтроллера начать выполнения только после стабилизации напряжения питания.

Вход выбора режима загрузки был подключен к земле через резистор сопротивлением 10 кОм. Загрузка будет происходить из основной постоянной памяти, а при необходимости выбора других режимов можно будет установить перемычку между контактом микроконтроллера и цепью питания.

В качестве основного кварцевого резонатора был выбран резонатор FA-238 24.0000МВ-К фирмы Seiko Epson, подходящий для поверхностного монтажа с погрешностью частоты $\pm 50 \times 10^{-6}$, с рабочей температурой от минус 40 до 85 градусов Цельсия и физическими размерами 3.2 x 2.5 x 0.7 мм.

В качестве часового кварцевого резонатора был выбран резонатор FC-12M 32.7680КА-А фирмы Seiko Epson, подходящий для поверхностного монтажа, с рабочей температурой от минус 40 до 85 градусов Цельсия и физическими размерами 2.05 x 1.2 x 0.6 мм и погрешностью частоты $\pm 30 \times 10^{-6}$.

На контакты колонок клавиатуры (по умолчанию) подается логическая единица, поэтому они подключены к цепи питания через резисторы сопротивлением 150 кОм, а с контактов рядов – считываются значения, поэтому они подключены через диоды.

Сигнальные цепи дисплея подключены к микроконтроллеру напрямую, цепи питания логики и земли тоже, а цепь питания подсветки через резистор с малым сопротивлением (чтобы возможное короткое замыкание в цепи подсветки не привело к короткому замыканию на плате). Также установлен переменный резистор для регулировки контрастности дисплея.

К приемопередатчику RS-232 в соответствии с документацией на него подключено пять керамических конденсаторов емкостью 100 нФ.

К преобразователю напряжения подключены по паре конденсаторов (керамический на 100 нФ и танталовый на 10 мкФ) на вход и выход, а также конденсатор на 10 нФ для снижения уровня шумов к специальному контакту.

Получившаяся принципиальная схема платы индикации приведена в приложении Д.

9.3 Описание принципиальной схемы платы управления

На плате управления размещены два микроконтроллера. К основному (далее – контроллер управления) подключается приемопередатчик ULPI по 12 цепям данных и цепь частоты (частота подается с микроконтроллера). Данные на внешнее устройство (в которое будет вводиться ключевая информация) в базовом исполнении подключается по двум цепям USB (в дополнительном – по двум цепям UART), данные на плату индикации передаются по интерфейсу USART (2 цепи). Для управления приемопередатчиком RS-232, используемого в дополнительных исполнениях платы, были предусмотрены три цепи.

Для дополнительного взаимодействия с микроконтроллером, к которому подключается смарт-карта (далее – контроллер карты), предусмотрено наличие трех цепей.

Также потребуются цепи для обеспечения возможностей:

- сброса внешней подсистемы USB;
- отключения привода чтения оптических дисков;
- контроля состояния дверцы корпуса (открыта/закрыта);
- сброса преобразователя USB – UART (в дополнительном исполнении).

Три контакта подключаются к контрольным точкам (при необходимости на них можно вывести сигналы Start Of Frame, USB_DM и USB_DP узла работы с USB микроконтроллера).

Кварцевого резонатора достаточно одного (2 контакта), входов выбора режима загрузки у микроконтроллера STM32F415 два. Они (а также вход сброса и цепи программирования интерфейса JTAG) расположены на выделенных контактах – всего 10 контактов.

Итого задействованы 42 контакта. Микроконтроллер STM32F415 выпускается в следующих корпусах:

- LQFP176 – пластиковый корпус 24 x 24 x 1.6 мм, выводы с четырех сторон;
- UFBGA176+25 – пластиковый корпус 10 x 10 x 0.6 мм, выводы снизу;
- LQFP144 – пластиковый корпус 20 x 20 x 1.6 мм, выводы с четырех сторон;

- LQFP100 – пластиковый корпус 14 x 14 x 1.6 мм, выводы с четырех сторон;
- WLCSP90– пластиковый корпус 4.223 x 3.969 x 0.57 мм, выводы снизу;
- LQFP64 – пластиковый корпус 10 x 10 x 1.6 мм, выводы с четырех сторон.

Будет достаточно минимального 64-х контактного корпуса. Также в этом корпусе 11 контактов земли и питания.

Контакты занесены в таблицу 5.

Таблица 5 – Контакты контроллера управления

Номер контакта	Название контакта	Назначение
1	VBAT	Батарейное питание
2	PC13	-
3	PC14-OSC32_IN	-
4	PC15-OSC32_OUT	-
5	PH0-OSC_IN	Цепь от основного кварцевого резонатора
6	PH0-OSC_OUT	Цепь к основному кварцевому резонатору
7	NRST	Цепь сброса
8	PC0	Цепь STP приемопередатчика ULPI
9	PC1	-
10	PC2	Цепь DIR приемопередатчика ULPI
11	PC3	Цепь NXP приемопередатчика ULPI
12	VSSA	Аналоговая земля
13	VDDA	Аналоговое питание
14	PA0	-
15	PA1	Цепь контроля дверцы
16	PA2	-
17	PA3	Цепь D0 приемопередатчика ULPI
18	VSS	Земля
19	VDD	Питание
20	PA4	Контрольная точка OTG_HS_SOF
21	PA5	Цепь СК приемопередатчика ULPI
22	PA6	Цепь отключения привода чтения дисков
23	PA7	Цепь сброса внешней подсистемы USB
24	PC4	-
25	PC5	-
26	PB0	Цепь D1 приемопередатчика ULPI
27	PB1	Цепь D2 приемопередатчика ULPI
28	BOOT1	Цепь №2 выбора режима загрузки
29	PB10	Цепь D3 приемопередатчика ULPI
30	PB11	Цепь D4 приемопередатчика ULPI
31	VCAP_1	Контакт внутреннего регулятора питания
32	VDD	Питание
33	PB12	Цепь D5 приемопередатчика ULPI

Продолжение таблицы 5

Номер контакта	Название контакта	Назначение
34	PB13	Цепь D6 приемопередатчика ULPI
35	PB14	Контрольная точка OTG_HS_DM
36	PB15	Контрольная точка OTG_HS_DP
37	PC6	Цепь управления контроллера карты №1
38	PC7	Цепь управления контроллера карты №2
39	PC8	Цепь управления контроллера карты №3
40	PC9	-
41	PA8	Цепь подачи частоты на приемопередатчик ULPI
42	PA9	Цепь сброса преобразователя USB - UART
43	PA10	-
44	PA11	Цепь USB на внешнее устройство
45	PA12	Цепь USB на внешнее устройство
46	TMS	Цепь JTAG
47	VCAP_2	Контакт внутреннего регулятора питания
48	VDD	Питание
49	TCK	Цепь JTAG
50	TDI	Цепь JTAG
51	PC10	Данные на плату индикации (USART3_TX)
52	PC11	Данные от платы индикации (USART3_RX)
53	PC12	Данные на внешнее устройство (UART5_TX)
54	PD2	Данные от внешнего устройства (UART5_RX)
55	TDO	Цепь JTAG
56	TRST	Цепь JTAG
57	PB5	Цепь D7 приемопередатчика ULPI
58	PB6	-
59	PB7	Цепь INVALID приемопередатчика RS-232
60	BOOT0	Цепь №1 выбора режима загрузки
61	PB8	Цепь FORCE_OFF приемопередатчика RS-232
62	PB9	Цепь ENABLE приемопередатчика RS-232
63	VSS	Земля
64	VDD	Питание

Условное графическое изображение микроконтроллера занимает много места, поэтому схему будет нарисована на листах формата A1. На первом листе схемы размещен микроконтроллер управления D1 (главный), разъемы программирования и подключения внешнего устройства, приемопередатчик RS-232 и преобразователь USB - UART (для дополнительных исполнений). Чтобы разобраться, какие элементы в каком исполнении устанавливать, на первом листе также размещена таблица (в перечне элементов на схему

сперва будут перечисляться общие для всех исполнений элементы, а затем – уникальные для каждого исполнения).

К каждому входу питания микроконтроллера подключено по керамическому конденсатору емкостью 100 нФ для сглаживания высокочастотных помех, и один общий танталовый емкостью 4.7 мкФ. К контактам внутреннего регулятора питания подключено по танталовому конденсатору емкостью 2.2 мкФ.

На вход сброса (также подключаемый к разъему программирования) подключен конденсатор 100 нФ, который будет использоваться для формирования совместно с подтягивающим резистором внутри микроконтроллера линии задержки, что заставит программу микроконтроллера начать выполнения только после стабилизации напряжения питания.

Входы выбора режима загрузки подключены к земле через резисторы сопротивлением 10 кОм. Загрузка будет происходить из основной постоянной памяти, а при необходимости выбора других режимов можно будет установить перемычки между контактами микроконтроллера и цепью питания.

В качестве основного кварцевого резонатора выбран резонатор FA-238 24.0000MB-K фирмы Seiko Epson, подходящий для поверхностного монтажа с погрешностью частоты $\pm 50 \times 10^{-6}$, с рабочей температурой от минус 40 до 85 градусов Цельсия и физическими размерами 3.2 x 2.5 x 0.7 мм.

К приемопередатчику RS-232 в соответствии с документацией на него подключено пять керамических конденсаторов емкостью 100 нФ, к преобразователю USB – UART – три керамических конденсатора емкостью 100 нФ и один танталовый конденсатор емкостью 4.7 мкФ, а также (для фильтрации цепей USB) – два конденсатора емкостью 47 пФ. Для защиты цепей USB от электростатических разрядов применена микросхема USBLC6-2 фирмы STMicroelectronics, содержащая в корпусе размером 1.6 x 1.6 мм пять защитных диодов – эта микросхема должна располагаться в непосредственной близости от разъема и оснащаться конденсатором емкостью 100 нФ.

Основное исполнение платы управления отличается от дополнительных способом подключения внешнего устройства к контроллеру управления:

- в основном исполнении внешнее устройство подключается к микроконтроллеру по интерфейсу USB;
- в первом дополнительном исполнении внешнее устройство подключается по интерфейсу RS-232 к приемопередатчику RS-232, приемопередатчик RS-232 – к

преобразователю USB – UART, а преобразователь USB – UART – к микроконтроллеру по интерфейсу USB;

- во втором дополнительном исполнении внешнее устройство подключается по интерфейсу RS-232 к приемопередатчику RS-232, а приемопередатчик RS-232 – к контроллеру по интерфейсу UART.

Таким образом, можно изготовить платы, имеющие возможность работы как с внешними устройствами с интерфейсом USB, так и с внешними устройствами с интерфейсом RS-232, причем в случаях основного и первого дополнительного исполнений программное обеспечение микроконтроллера будет одним и тем же, а в случае второго дополнительного исполнения – отличаться (исходя из предположения, что во внешнем устройстве установлен тот же преобразователь FT231, что и на плате управления).

На втором листе схемы размещен приемопередатчик ULPI и микросхема гальванической развязки с сопутствующими им вспомогательными элементами.

Приемопередатчик ULPI связан по параллельному интерфейсу ULPI с контроллером управления с одной стороны и по последовательному интерфейсу USB с хабом USB с другой стороны. Приемопередатчик имеет контакт CPEN для управления подачей питанием на разъем USB, он не используется, но выведен (на всякий случай) на контрольную точку. Также приемопередатчик имеет контакт VBUS для определения наличия подключения USB устройства, в данном устройстве фиксированное (хаб), но возможность имитации подключения была предусмотрим подачей на этот контакт (и одноименный контакт хаба) напряжения 5 В через переключатель TPS2069, управляемый контроллером управления.

Приемопередатчик ULPI может питаться как от одного напряжения (3.3 В), так и от двух (3.3 В и 1.8 В) при условии использования внутреннего преобразователя напряжения. Здесь он используется, поэтому контакт REG_EN соединен с землей. Соединен с землей через резистор 12 кОм контакт RBIAS. К контактам питания подключены керамические конденсаторы на 100 нФ и танталовые на 4.7 мкФ (целых три – для входного напряжения 3.3 В и для формируемых микросхемой аналогового и цифрового напряжений 1.8 В).

Ко входу и выходу переключателя TPS2069 подключено по одному керамическому конденсатору на 100 нФ, цепь управления подтянута к логической единице резистором на 10 кОм.

Микросхема гальванической развязки USB интерфейса ADuM3160 изображена расположенной на границе отсеков (основного и отсека привода чтения оптических дисков). Задается ее режим работы full-speed (12 Мбит/с) подачей логических единиц на

входы SPU и SPD. Следует учесть, что эта микросхема имеет независимое питание (и землю) с каждой стороны, поэтому пропустить питание напрямую из одного отсека в другой нельзя – поэтому цепь питания пропущена через фильтры, а земля в отсеке привода чтения оптических дисков своя (объединенная с корпусной).

Также на границе отсеков расположена оптопара PRAB37S, которая будет включать преобразователь напряжения в отсеке привода чтения оптических дисков.

Цепь включения преобразователя напряжения, цепи питания и земли для ADuM3160, а также цепи USB пропущены через фильтры.

В качестве фильтров цепей USB применены трехконтактные фильтры для сигнальных цепей MEM2012F50R0T001 фирмы TDK, имеющие частоту среза 50 МГц и рабочее напряжение до 12 В при физических размерах 2 x 1.25 x 0.8 мм.

В качестве фильтра цепи управления преобразователем напряжения применен комбинированный индуктивно-емкостный фильтр с ферритовым сердечником NFE61PT472C1H9 фирмы Murata, имеющий частоту среза 1 МГц и рабочее напряжение до 50 В при физических размерах 6.8 x 1.6 x 1.6 мм.

В качестве фильтров цепей питания применены трехконтактные конденсаторные фильтры NFM41PC155B1E3 фирмы Murata, имеющие емкость 1.5 мкФ и рабочее напряжение до 25 В при физических размерах 4.5 x 1.6 x 1.0 мм.

Выбранный преобразователь USB – SATA имеет два соединителя USB, поэтому в отсеке привода чтения оптических дисков размещены два разъема USB, к одному из которых подключены цепи данных от фильтров цепей USB, землю и питание, а к другому – только земля и питание. К каждому разъему подключены по одному керамическому конденсатору емкостью 100 нФ и по одному танталовому емкостью 47 мкФ. Цепи данных перед подачей на разъем USB дополнительно пропущены через фильтр дифференциальных сигналов ACM2012H-900-2P фирмы TDK с волновым сопротивлением 90 Ом и рабочим напряжением до 20 В при физических размерах 2.0 x 1.2 x 1.2 мм.

На третьем листе схемы размещен хаб с сопутствующими элементами и узел преобразователя напряжения из 12 В в 5 В для отсека привода чтения оптических дисков.

К хабу подключен кварцевый резонатор FA-238 24.0000MB-K фирмы Seiko Epson (тот же, что используется совместно с контроллером управления) и резисторы для задания параметров работы хаба, выбранные согласно документации на микросхему. Предусмотрена возможность имитации подключения USB хоста использованием контакта USB_VBUS микросхемы. Хаб питается от двух напряжений: 3.3 В и 1.1 В.

Напряжение 3.3 В для питания хаба получено из основного напряжения 3.3 В после прохождения через дроссель BLM18EG221SN1 фирмы Murata, имеющий индуктивность 220 Ом на частоте 100 МГц и рабочий ток 2 А при физических размерах 1.6 x 0.8 x 0.8 мм.

Напряжение 1.1 В для питания хаба получено из основного напряжения 3.3 В при помощи линейного преобразователя напряжения TLV71211DBV фирмы Texas Instruments с выходным током 300 мА и точностью выходного напряжения 2% при физических размерах 2.9 x 2.8 x 1.45 мм. К его входу и выходу подключены по керамическому конденсатору емкостью 1 мкФ, выход дополнительно пропущен через дроссель BLM18EG221SN1 фирмы Murata.

На каждый контакт питания хаба подключено по керамическому конденсатору емкостью 100 нФ, и по танталовому емкостью 10 мкФ на каждое напряжение питания (1.1 В и 3.3 В). К контакту GRSTZ микросхемы подключен конденсатор емкостью 1 мкФ для формирования сигнала сброса после стабилизации напряжения питания микросхемы.

Микросхема хаба может управлять подачей питания на устройства, подключенные к своим четырем портам. Управление питанием привода чтения оптических дисков не требуется (для этого имеется есть отдельная цепь на контроллере управления), управление питанием контроллера карты тоже (контроллер карты уже связан с контроллерам управления тремя цепями управления), остается съемный USB флеш накопитель.

Управляется подача питания на разъем для подключения съемного USB флеш накопителя при помощи микросхемы переключателя TPS2553QDBVRQ1 фирмы Texas Instruments со встроенным настраиваемым ограничителем на ток до 1.7 А в корпусе с физическими размерами 2.9 x 2.8 x 1.45 мм. В данном случае он настроен на ток в 1.3 А подключением резистора на 20 кОм между контактом ILIM и землей. На входе переключателя установлен керамический конденсатор на 100 нФ, на выходе – керамический конденсатор на 22 мкФ. Выход далее пропускается через дроссель BLM18EG221SN1 фирмы Murata и подключим к USB разъему, у которого установлен керамический конденсатор на 100 нФ и танталовый – на 47 мкФ.

Узел преобразователя напряжения из 12 В в 5 В для отсека привода чтения оптических дисков построен на основе микросхемы понижающего импульсного преобразователя напряжения ST1S40IPUR фирмы STMicroelectronics с физическими размерами 4 x 4 x 0.9 мм. Этот преобразователь с настраиваемым выходным напряжением работает на частоте 850 кГц и обеспечивает выходной ток 3 А при входном напряжении от 4 до 18 В. При помощи резисторного делителя, состоящего из резистором на 20 кОм и

107 кОм, подключенного к цепи обратной связи, преобразователь настроен на формирование напряжения 5 В.

Для работы импульсного преобразователя напряжения необходима катушка индуктивности, выбрана была В82477Р2332М000 фирмы TDK с ферритовым сердечником и магнитной экранировкой с физическими размерами 12.5 x 12.5 x 6 мм. Она имеет индуктивность 3.3 мкГн и может выдерживать ток до 6.7 А.

На входе преобразователя установлены керамические конденсаторы емкостью 1 мкФ и 10 мкФ с номинальным напряжением 50 В, на выходе – керамический конденсатор емкостью 22 мкФ с номинальным напряжением 16 В.

В качестве земли преобразователя будет использоваться корпус устройства. У привода металлический корпус, он соединен с сигнальной землей USB разъема и крепится к металлическому корпусу устройства. Поэтому ключевая информация на оптическом диске должна храниться только в закрытом виде, а во время ввода ключевой информации со смарт-карты привод чтения оптических дисков должен обесточиваться. Основная же часть платы развязана по земле с отсеком привода чтения оптических дисков.

На четвертом листе схемы размещен контроллер карты, разъем для его программирования по интерфейсу JTAG и, раз уж осталось свободное место, разъем для подключения к плате индикации и контрольные точки, к которым будут припаиваться провода от тумблера, срабатывающего при открытии дверцы устройства.

К контроллеру карты подключим:

- три цепи управления от контроллера управления;
- две цепи USART на микросхему взаимодействия со смарт-картами;
- четыре цепи GPIO на микросхему взаимодействия со смарт-картами;
- две цепи USB на хаб.

Также предусмотрена контрольную точку для вывода отладочной информации (по интерфейсу UART) и две контрольные точки для вывода второго USB интерфейса микроконтроллера (могут пригодиться для отладки программного обеспечения микроконтроллера совместно с компьютером, без участия хаба, приемопередатчика ULPI и основного контроллера).

Два выделенных контакта будут задействованы для выбора режима загрузки микроконтроллера, один для сброса и два – для подключения кварцевого резонатора. Также необходимо подключить пятиконтактный интерфейс программирования JTAG.

Итого потребуется задействовать 24 контакта микроконтроллера. Применен тот же микроконтроллер, что и в случае с контроллером управления, с минимальным 64-х контактным корпусом.

Контакты занесены в таблицу 6.

Таблица 6 – Контакты контроллера карты

Номер контакта	Название контакта	Назначение
1	VBAT	Батарейное питание
2	PC13	-
3	PC14-OSC32_IN	-
4	PC15-OSC32_OUT	-
5	PH0-OSC_IN	Цепь от основного кварцевого резонатора
6	PH0-OSC_OUT	Цепь к основному кварцевому резонатору
7	NRST	Цепь сброса
8	PC0	-
9	PC1	-
10	PC2	-
11	PC3	-
12	VSSA	Аналоговая земля
13	VDDA	Аналоговое питание
14	PA0	Контрольная точка UART (UART4_TX)
15	PA1	-
16	PA2	Цепь на ST8024 (USART2_TX)
17	PA3	-
18	VSS	Земля
19	VDD	Питание
20	PA4	Цепь на ST8024 (USART2_CK)
21	PA5	Цепь на ST8024 (GPIO)
22	PA6	Цепь на ST8024 (GPIO)
23	PA7	Цепь на ST8024 (GPIO)
24	PC4	-
25	PC5	Цепь управления контроллера карты №3
26	PB0	-
27	PB1	-
28	BOOT1	Цепь №2 выбора режима загрузки
29	PB10	-
30	PB11	-
31	VCAP_1	Контакт внутреннего регулятора питания
32	VDD	Питание
33	PB12	Цепь управления контроллера карты №1
34	PB13	Цепь управления контроллера карты №2
35	PB14	Контрольная точка OTG_HS_DM

Продолжение таблицы 6

Номер контакта	Название контакта	Назначение
36	PB15	Контрольная точка OTG_HS_DP
37	PC6	-
38	PC7	-
39	PC8	-
40	PC9	-
41	PA8	Цепь на ST8024 (GPIO)
42	PA9	-
43	PA10	-
44	PA11	Цепь USB на хаб
45	PA12	Цепь USB на хаб
46	TMS	Цепь JTAG
47	VCAP_2	Контакт внутреннего регулятора питания
48	VDD	Питание
49	TCK	Цепь JTAG
50	TDI	Цепь JTAG
51	PC10	-
52	PC11	-
53	PC12	-
54	PD2	-
55	TDO	Цепь JTAG
56	TRST	Цепь JTAG
57	PB5	-
58	PB6	-
59	PB7	-
60	BOOT0	Выбор режима загрузки
61	PB8	-
62	PB9	-
63	VSS	Земля
64	VDD	Питание

К каждому входу питания микроконтроллера подключено по керамическому конденсатору емкостью 100 нФ для сглаживания высокочастотных помех, и один общий танталовый емкостью 4.7 мкФ. К контактам внутреннего регулятора питания подключено по танталовому конденсатору емкостью 2.2 мкФ.

На вход сброса (также подключаемый к разъему программирования) подключен конденсатор 100 нФ, который будет использоваться для формирования совместно с подтягивающим резистором внутри микроконтроллера линии задержки, что заставит

программу микроконтроллера начать выполнения только после стабилизации напряжения питания.

Входы выбора режима загрузки подключены к земле через резисторы сопротивлением 10 кОм. Загрузка будет происходить из основной постоянной памяти, а при необходимости выбора других режимов можно будет установить перемычки между контактами микроконтроллера и цепью питания.

В качестве основного кварцевого резонатора выбран резонатор ABM8G-12.000MHz-18-D2Y фирмы Abracon Corporation, подходящий для поверхностного монтажа с погрешностью частоты $\pm 20 \times 10^{-6}$, с рабочей температурой от минус 40 до 85 градусов Цельсия и физическими размерами 3.2 x 2.5 x 1.0 мм.

На пятом листе схемы размещена микросхема сопряжения со смарт-картой, соединитель для подключения смарт-карты и оставшаяся часть схемы питания: преобразователь напряжения из 12 В в 5 В и преобразователь напряжения из 5 В в 3.3 В.

Микросхема взаимодействия со смарт-картой ST8024CTR фирмы STMicroelectronics подключается по 6 цепям к контроллеру карты и по 7 цепям к соединителю смарт-карт, выполняя следующие функции:

- защита от короткого замыкания на контактах карты;
- определение наличия карты с устранением дребезга контактов;
- выдача стартовой последовательности для карты;
- подача на карту напряжения 3 В или 5 В.

Благодаря этой микросхеме контроллер, работающий с трехвольтовыми уровнями сигналов, может взаимодействовать с картой, работающей с пятивольтовыми уровнями сигналов.

Когда карта оказывается вставленной, замыкаются контакты SW соединителя. Подключив один к земле, а другой – к микросхеме взаимодействия, можно обеспечить определение присутствия карты. Так как на смарт-карте хранится ключевая информация в открытом виде, и ввод ее с открытой дверцей устройства недопустим (из-за утечки в электромагнитных полях), контакт SW соединителя соединен с землей не напрямую, а через геркон, а в дверце установлен магнит. При закрытии дверцы магнит приближается к геркону, и геркон замыкает контакт SW соединителя на землю. Тогда, в случае если карта вставлена, микросхема взаимодействия со смарт-картами передаст контроллеру карты о том, что карта вставлена. А так как первичная настройка платы будет происходить без корпуса, параллельно геркону установлен двухконтактный соединитель, устанавливая джампер на который можно имитировать закрытие дверцы.

Схема подключения микросхемы преобразователя заимствована из примера STMicroelectronics.

На плату управления питание подается по четырехконтактному соединителю KLS1-XL5-2.50-04-S фирмы KLS Electronic с рабочим диапазоном температур от минус 40 до 105 градусов Цельсия. Контакты из фосфористой бронзы диаметром 0.6 мм способны выдержать ток в 3 А каждый, в данном случае соединены их по два, увеличивая общий максимальный ток до 6 А (и заодно уменьшаем сопротивление соединения).

Объединенная цепь питания подается на самовосстанавливающийся предохранитель MF-R110 фирмы Bourns, который в случае аномально высокого тока, потребляемого схемой (например, короткого замыкания), разорвет цепь.

Далее установлен защитный диод SMAJ18A фирмы STMicroelectronics с пиковой мощностью рассеивания электростатического разряда 400 Вт и номинальным рабочим напряжением 18 В в корпусе с физическими размерами 5.1 x 2.6 x 2.2 мм.

Далее установлен танталовый конденсатор TAJE476K035RNJ фирмы AVX с емкостью 47 мкФ и номинальным напряжением 35 В при физических размерах 7.3 x 4.3 x 4.1 мм, и керамический – CC0603KRX7R9BB105 фирмы Yageo с емкостью 1 мкФ и номинальным напряжением 50 В при физических размерах 1.6 x 0.8 x 0.8 мм.

Затем установлен изолированный импульсный преобразователь напряжения TMR 6-1211, преобразующий входное напряжение в диапазоне от 9 до 18 В в выходное напряжение 5 В, обеспечивающий выходной ток до 1200 мА с типовой эффективностью 83% и работоспособный при температуре от минус 40 до 70 градусов Цельсия в семивыводном пластиковом корпусе с физическими размерами 21.8 x 9.1 x 11.2 мм.

И если на вход преобразователя подается корпусная земля, то на выходе получается уже гальванически развязанная сигнальную землю, которая будет использоваться во всех вторичных преобразователях на плате. А соединяться сигнальная земля с корпусной будет лишь при подаче питания на отсек привода чтения оптических дисков.

Конденсаторы на выходе TMR той же емкости что и на входе, но рассчитанные на напряжение 16 В.

Также на листе 5 схемы изображен инвертор, выполненный на транзисторе, для цепи управления подачей питания на отсек привода чтения оптических дисков. Его необходимость обусловлена применением оптопары PRAB37S, для управления которой требуется ток порядка миллиампер. Так обеспечивается защита от возможного выгорания входа контроллера, которое могло бы произойти при прямом подключении оптопары к нему.

Преобразование из 5 В в 3.3 В производится при помощи узла, похожего на узел преобразователя напряжения из 12 В в 5 В для отсека привода чтения оптических дисков. Микросхема понижающего импульсного преобразователя напряжения ST1S40IPUR фирмы STMicroelectronics с резисторным делителем, состоящим из резистором на 20 кОм и 63.4 кОм позволит получить выходное напряжение 3.3 В. Согласно документации, максимальная эффективность (на уровне 94%) достигается при токе нагрузки 0.5 А, затем медленно убывает, и достигает значения 88% при токе 3 А.

Нулевой резистор на выходе узла преобразователя напряжения – это не случайность, он установлен намеренно для устранения возможной ошибки в построении преобразователя напряжения, могущей привести к выгоранию большого количества микросхем и логических элементов. При монтаже элементов на плату (который обычно происходит на автоматической линии) этот резистор не устанавливается, и при первой настройке платы проверяется корректность работы преобразователя. А затем, если напряжение на выходе преобразователя соответствует желаемому, этот резистор устанавливается (уже вручную).

Получившаяся принципиальная схема платы управления приведена в приложении Е.

10 Выбор и описание программной реализации

10.1 Сравнение средств разработки

К популярным средствам разработки для микроконтроллеров фирмы STMicroelectronics относятся Atollic TrueSTUDIO, IAR Embedded Workbench, Keil MDK. Данные о них сведены в таблицу 7.

Таблица 7 – Коммерческие средства разработки

Название	Atollic TrueSTUDIO	IAR Embedded Workbench	Keil MDK
Владелец	STMicroelectronics	IAR Systems	ARM
Страна	Швейцария	Швеция	Великобритания
Ограничения бесплатной версии	Необходимость регистрации	Размер исполняемого файла не более 32Кб, исходный код библиотек не включен	Размер исполняемого файла не более 32Кб,, дизассемблирование недоступно
Компилятор	открытый	собственный	собственный

Из этой тройки лучшей средой является TrueSTUDIO, собранная из проектов с открытым исходным кодом с коммерческими расширениями. В качестве библиотек предлагается использовать CMSIS (от ARM) и STM32Cube.

10.2 Подготовка системы на базе GNU/Linux

В качестве операционной системы был использован свободно распространяемый дистрибутив Debian GNU/Linux [45] (коммерческая модификация которого под названием Astra Linux [46] сертифицирована для работы с гостайной), в качестве компилятора – GCC [47] (он же используется в STM32CubeIDE), в качестве отладчика – GDB [48]. Взаимодействие с микроконтроллером по интерфейсу JTAG (для загрузки и отладки программного обеспечения) будет производиться при помощи OpenOCD [49]. Правила сборки будут задаваться в Makefile.

10.3 Библиотека libopencm3

Библиотека с открытым исходным кодом для микроконтроллеров с ядром ARM Cortex существует – это libopencm3. Поддерживается ряд микроконтроллеров от фирм Microchip, NXP, Silicon Laboratories, STMicroelectronics и Texas Instruments. Библиотека написана полностью с нуля с использованием документации производителей на

микросхемы. Предполагается использование совместно со средствами разработки GNU [50]. Библиотека распространяется под лицензией GPL [51] версии 3 или выше.

Поддержка USB в режиме device есть для микроконтроллеров семейств EFM32 (Silicon Laboratories), STM32 (STMicroelectronics) и LM4F (Texas Instruments).

10.4 Библиотека libusbhost

Преимущества библиотеки libusbhost:

- распространяется под лицензией LGPL версии 3;
- не использует блокирующих задержек;
- не использует динамическую аллокацию памяти;
- не зависит ни от какой операционной системы.

В списке поддерживаемого оборудования указана демонстрационная плата stm32f4discovery на базе микроконтроллера STM32F407VGT6.

В состав библиотеки включены драйверы hub, gamepad, hid и midi, которые можно использовать в качестве примеров для написания собственных драйверов.

10.5 Абстракции USB

Драйвер – это часть системного программного обеспечения, обеспечивающая поддержку определенного оборудования или функции операционной системы (например, файловой системы). Может распространяться в виде исходных текстов (обычно в Linux) или в бинарном виде (обычно в Windows).

Для удобства использования при разработке современных интерфейсов предусматривается функция автоопределения устройств. В таком случае операционная система сама определяет, какой драйвер нужен тому или иному устройству и использует его.

При разработке шины USB были предусмотрены дескрипторы, в которых устройство передает информацию о себе. Пользуясь этой информацией, драйвер ядра USB операционной системы производит поиск подходящего драйвера USB устройства.

Задача device:

- сообщить host свои параметры;
- получить адреса для своих endpoints;
- обрабатывать информацию по этим адресам.

Задача host:

- регулярно опрашивать шину;
- осуществлять поиск драйверов для устройств USB;

- назначать адреса для подключенных device;
- обрабатывать информацию по этим адресам.

Режимы работы устройств могут отличаться для достижения различных уровней энергопотребления системы, этим тоже занимается host.

Все эти понятия (host, device, endpoints), механические и электрические характеристики, протокол и программная модель, строение и принципы работы хаба – подробно разобраны в спецификации USB.

10.6 Предпусковой контроль

Согласно спецификации USB 2.0, данные по шине передаются кадрами (*frames*) в режимах low-speed (1.5 Мбит/с) и full-speed (12 Мбит/с), и микрокадрами (*micro-frames*) в режиме high-speed (480 Мбит/с). Каждый кадр начинается с маркера *Start Of Frame*, который повторяется на шине через 1 мс (T_{FRAME} в случае low-speed/full-speed) или через 125 нс ($T_{HSFRAME}$ в случае high-speed).

Для настройки приемника на начало пакета в режимах low-speed/full-speed применяется синхропосылка (*SYNC pattern*) длительностью 8 бит (10101000), в режиме high-speed – длительностью 32 бита (10101010101010101010101010101000), для устранения необходимости использования отдельного тактового сигнала используется метод кодирования NRZI с бит-стаффингом (добавляется ноль после каждых шести последовательных единиц).

Используемые в разрабатываемом устройстве контроллеры (управления и карты) содержат в своем составе блоки, реализующие функционал приемопередатчика USB, и вышеописанные операции кодирования/декодирования выполняются аппаратно. Однако от программы требуется обеспечить настройку умножителя частоты для получения 48 МГц, необходимых для работы блоков обработки USB и производить обмен с ними посредством чтения/записей в выделенные для этих целей регистры каждые 1 мс (в случае low-speed/full-speed).

Для формирования временных меток для USB host был применен таймер (*basic timer*), настроенный на частоту 10 кГц. Этот (точный) таймер нужен для host (в данном случае – контроллер управления), для device (в данном случае – контроллер карты) его наличие необязательно. Но в обоих случаях для реализации подсистемы отложенного выполнения функций (*delayed call*) используется системный таймер (*SysTick timer*), настроенный на частоту 1 кГц.

Получается, что в первом случае (исключительно для USB host) применен таймер с разрешением 16 бит, который может задавать промежутки времени до $2^{16} = 65536$ мс ≈ 65 с, а во втором – таймер с разрешением 24 бита, который может задавать промежутки времени до $2^{24} = 16777216$ мс ≈ 4.7 ч.

В начале работы программы будет проверяться корректность функционирования таймеров. В случае, если таймеры работают неправильно – дальнейшую работу программы можно и не начинать, а подразумевать что устройство неработоспособно.

Таким образом, в программе контроллера карты будет проверяться один таймер (системный), а в программе контроллера управления – два таймера (системный и базовый), и дополнительно сравниваться различия в их показаниях.

Каждая проверка будет состоять из замеров показаний таймеров до выполнения миллиона «пустых» тактов арифметическо-логического устройства микроконтроллера и после. При частоте работы в 168 МГц продолжительность такта работы равна интервалу времени в $1 / 168000000$ с ≈ 5.95 нс, но так как выполнения происходит в цикле, и проверка достижения заданного значения и выполнения перехода тоже занимают время (фактически цикл состоит из 7 команд), а пока программа крутится в цикле, происходит выполнение незапрещенных прерываний, то общее время выполнения цикла из миллиона «пустых» тактов составляет 48 мс.

Эти действия выполняются многократно для получения последовательности из десяти значений (в случае контроллера карты – интервалов системного таймера, в случае контроллера управления – разниц интервалов системного и базового таймеров), для которой вычисляются среднее, максимальное и минимальное значения. Пока максимальное значение в последовательности не перестанет сильно отклоняться от среднего значения в последовательности, проверка завершена не будет.

Таким образом осуществляется предпусковой контроль в контроллерах карты и управления. Если он пройден, происходит инициализация подсистемы USB и драйверов используемых устройств USB и затем устройство переходит в нормальный режим работы.

Алгоритм работы предпускового контроля приведен в приложении К.

10.7 Периодический контроль

При помощи предпускового контроля проверяется, что таймеры работают стабильно и микроконтроллер может выдавать кадры по интерфейсу USB с требуемой частотой. Однако выдает ли он их на самом деле и корректно ли происходит обработка информации – в предпусковом контроле (занимающим в норме 0.5 с) не проверяется.

Для более глубоких проверок должен использоваться периодический (по команде оператора) контроль работоспособности устройства.

Проверкам подвергаются:

- обмен данными по интерфейсу USB между контроллером управления и контроллером карты (Контроль 1);
- обмен данными по интерфейсу USB между контроллером управления и хабом с подключенными к нему устройствами (Контроль 2);
- обмен данными по интерфейсу USB между контроллером управления и внешним устройством (Контроль 3).

В режиме «Контроль 1» контроллер управления отправляет тестовую последовательность данных контроллеру карты, тот ее получает и сразу же отправляет обратно. Если отправленная и полученная последовательности совпадают, данный тест считается выполненным.

В режиме «Контроль 2» контроллер управления запускает параллельно три теста:

- запрос контроллера карты о состоянии карты;
- запрос привода чтения оптических дисков о наличии файла на диске;
- попытка записи на съемный флеш накопитель.

Раскрутка оптического диска занимает более десятка секунд, поэтому этот тест самый длительный.

Режим «Контроль 3» похож на режим «Контроль 1», но контроллер управления отправляет тестовую последовательность данных на внешнее устройство. Внешнее устройство ее получает и сразу же отправляет обратно. Если отправленная и полученная последовательности совпадают, данный тест считается выполненным.

Так как выбор режима работы устройства происходит с клавиатуры устройства, подключенного к контроллеру индикации, то заодно происходит проверка работоспособности обмена между контроллером индикации и контроллером управления. Результаты выполнения тестов отображаются на дисплее устройства.

Чтение собственно информации с карты и диска при прохождении тестов в режиме «Контроль 2» не выполняется, поэтому даже при использовании носителей с рабочей ключевой информацией утечки этой информации не происходит.

10.8 Протоколирование событий

Контроллер индикации производит протоколирование происходящих с устройством событий, важных с точки зрения безопасности, с записью в журнал безопасности, хранящийся во внутренней флеш-памяти контроллера индикации.

Регистрации подвергаются следующие события:

- результат ввода ключевой информации с диска;
- результат ввода ключевой информации с карты;
- результат проведение контроля целостности программного обеспечения;
- результат проведения периодического контроля;
- факт смены кода доступа к устройству;
- факт переполнения журнала безопасности;
- факт перемещении журнала безопасности на съемный носитель.

Ввод ключевой информации происходит по правилу двух лиц – один оператор вводит первую часть ключевой информации с карты №1, второй – вторую часть ключевой информации с карты №2.. Перед вводом оператор проходит идентификацию с вводом своего кода доступа к устройству.

Журнал безопасности недоступен операторам, а доступен только администратору устройства после предъявления его кода доступа. Администратор имеет право просматривать журнал безопасности. Но даже администратор не может бесследно провести очистку журнала, а может лишь переместить его на съемный носитель, при этом факт перемещения журнала фиксируется.

Коды доступа хранятся во внутренней флеш-памяти контроллера индикации, на заводе-изготовителе устанавливаются нулевыми, а на объекте эксплуатации задаются в соответствии с правилами пользования устройством.

10.9 Описание программы контроллера карты

Работа программы начинается с выполнения функции *main* (файл *main.c*), где происходит инициализация системы тактирования, таймера и предпусковой контроль. Затем происходит инициализация драйвера USB и подсистемы USB device, после чего планируется вызов функции *main_tick* (файл *main.c*) опроса подсистемы USB с периодичностью 1 мс, происходит вызов функции *smart_process* (файл *smart.c*) обработки событий от смарт-карты и вызов функции *usart2_idle* (файл *usart2.c*) обработки данных от карты, далее следует переход в бесконечный цикл, где происходит опрос подсистемы отложенного выполнения функций *defer_process* (файл *defer.c*).

Подсистема отложенного выполнения функций представляет из себя примитивный планировщик задач, которому может быть поручено выполнить какую-либо функцию через некоторый промежуток времени. Управление к функции *defer_tick* (файл *defer.c*) планировщика переходит при каждом срабатывании системного таймера (то есть с частотой 1 кГц).

Инициализация драйвера USB происходит в функции *cdcacm_init* (файл *cdcacm.c*), где вызывается функция *usbd_init* (файл *usb.c*) высокоуровневого драйвера для работы с USB библиотеки *libopenm3*, вызывающая функцию *stm32f107_usbd_init* (файл *usb_f107.c*) низкоуровневого драйвера для работы с USB библиотеки *libopenm3*, которая производит выполнение последовательности операций для настройки подсистемы USB в режиме *device*. Также производится передача в подсистему USB функций драйвера, вызываемых после записи либо чтения пакета данных USB. Выполняется инициализация обработчика протокола взаимодействия с контроллером управления *sp_init* (файл *sp.c*).

Обмен данными между контроллерами в составе разрабатываемого устройства и внешнего устройства с разрабатываемым устройством происходит по унифицированному протоколу с кодированием и подсчетом контрольных сумм (о нем подробно описано в следующем разделе), поэтому требуется промежуточная обработка данных.

Периодический опрос состояния подсистемы USB происходит в функции *main_tick* (файл *main.c*), вызывающей функцию *usbd_poll* (файл *usb.c*) высокоуровневого драйвера USB, которая вызывает функцию *dwc_poll* (файл *usb_dwc_common.c*) низкоуровневого драйвера USB, где производится работа с регистрами блока USB микроконтроллера. При обнаружении завершения записи пакета USB происходит вызов запомненной подсистемой USB функции *cdcacm_data_tx_cb* (файл *cdcacm.c*) написанного драйвера, при обнаружении завершения чтения пакета USB происходит вызов запомненной подсистемой USB функции *cdcacm_data_rx_cb* (файл *cdcacm.c*) нашего драйвера.

В функции *cdcacm_data_rx_cb* (файл *cdcacm.c*) драйвера происходит чтения пакета USB путем вызова функции *usbd_ep_read_packet* (файл *usb.c*) высокоуровневого драйвера USB, которая вызывает функцию *dwc_ep_read_packet* (файл *usb_dwc_common.c*) низкоуровневого драйвера USB, где производится чтение данных из регистров блока USB микроконтроллера. Затем эти данные передаются на обработку в функцию *sp_rx* (файл *sp.c*), где происходит снятия байт-стаффинга, проверки длины и контрольной суммы пакета. В случае успешного завершения проверок вызывается функция *sp_cmd* (файл *sp.c*), где происходит обработка команд от контроллера управления.

При необходимости записи данных драйвер `cdcacm` вызывает функцию `usb_ep_write_packet` (файл `usb.c`) высокоуровневого драйвера USB, которая вызывает функцию `dwc_ep_write_packet` (файл `usb_dwc_common.c`) низкоуровневого драйвера USB, где производится запись данных в регистры блока USB микроконтроллера. Когда запись будет завершена, подсистема USB вызовет функцию `cdcacm_data_tx_cb` (файл `cdcacm.c`) написанного драйвера, которая проверяет успешность записи, и, при необходимости вызывает функцию `sp_send_next` (файл `sp.c`) для отправки следующей порции данных.

При поступлении байта данных от смарт-карты по прерыванию происходит вызов функции `usart2_isr` (файл `usart2.c`), где производится запись в циклический буфер. Чтение из этого буфера происходит в функции `usart2_idle` (файл `usart2.c`), вызываемой с периодичностью 10 мс. Прочитанная информация передается на обработку в функцию `ric_rx` (файл `ric.c`), где производится анализ ответов от карты и их предварительная обработка, подготовка к отправке в функции `ric_prepare_sp` (файл `ric.c`) и вызов функции `sp_pack_and_send` (файл `sp.c`) для упаковки и отправки во внешнее устройство в соответствии с протоколом обмена. Собственно отправка происходит в функции `sp_sending` путем вызова вышеописанной функции `usb_ep_write_packet` (файл `usb.c`).

Отправка данных к карте производится при получении соответствующей команды от внешнего устройства в функции `sp_cmd` (файл `sp.c`), где производится вызов функции `ric_tx` (файл `ric.c`), производящей проверку команд, оценку времени их выполнения и передачу для отправки по USART в функцию `usart2_txs` (файл `usart2.c`). В функции `usart2_txs` происходит запись в циклический буфер. Чтение из буфера производится по готовности USART при вызове по прерыванию функции `usart2_isr` (файл `usart2.c`).

10.10 Описание программы контроллера управления

Работа программы начинается с выполнения функции `main` (файл `usb.c`), где происходит инициализация системы тактирования, таймеров и предпусковой контроль. Затем происходит инициализация драйверов USB и подсистемы USB host, после чего планируется вызов функции `main_loop` (файл `usb.c`) опроса подсистемы USB с периодичностью 1 мс и функции `work_process` (файл `work.c`) обработки рабочих событий с периодичностью 1 с, далее следует переход в бесконечный цикл, где происходит опрос подсистемы отложенного выполнения функций `defer_process` (файл `defer.c`) и обработка полученных по USART данных от контроллера индикации.

При получении данных от контроллера индикации эти данные по прерыванию записываются в буфер в функции `usart3_isr` (файл `usart3.c`). В функции `usart3_idle` (файл

usart3.c) происходит чтение из этого буфера и декодирование данных при помощи функции *dp_rx* (файл *dp.c*), заключающееся в снятии байт-стаффинга, проверки длины и контрольной суммы. В случае успеха в функции *dp_cmd* (файл *dp.c*) происходит обработка команд от контроллера индикации.

Подсистема отложенного выполнения функций аналогична реализованный в программе для контроллера карты.

Низкоуровневая работа с USB (выполнение последовательности операций для настройки подсистемы USB, запись в регистры и чтение из регистров для передачи и приема данных) с учетом специфики микроконтроллеров ST реализована в файле *usbh_ild_stm32f4.c* библиотеки *libusbhost*, высокоуровневая платформонезависимая работа (поиск устройств на шине, поиск и регистрация драйверов) – в файле *usbh_core.c*.

Каждое управляемое (*device*) устройство USB при подключении «представляется», передавая управляющему (*host*) устройству путем передачи *дескрипторов* разнообразную информацию о себе, включая:

- код класса;
- код подкласса;
- код протокола;
- код производителя;
- код продукта;
- код класса интерфейса;
- код подкласса интерфейса;
- код протокола интерфейса.

Получив эту информацию, ядро подсистемы USB подбирает наиболее подходящий для устройства драйвер из имеющихся в наличии и «привязывает» устройство к драйверу, который в дальнейшем будет использоваться для взаимодействия с этим устройством.

Драйверов в разработанной программе пять:

- для работы с контроллером карты (*usbh_driver_acm.c*);
- для работы с внешним устройством (*usbh_driver_cdc.c*);
- для работы с приводом чтения оптических дисков (*usbh_driver_cdr.c*);
- для работы с хабом (*usbh_driver_hub.c*);
- для работы с флеш накопителем (*usbh_driver_msc.c*).

Каждый драйвер содержит в своем составе четыре обязательные функции, вызываемые ядром подсистемы USB:

- *init* – выполняет инициализацию переменных для устройства;

- *analyze_descriptor* – выполняет анализ дескриптора устройства;
- *poll* – выполняет периодическую обработку данных;
- *remove* – выполняет очистку переменных для устройства.

Также каждый драйвер содержит в своем составе структуру *driver_info* с заданными в ней кодами поддерживаемых устройств.

Функция *init* драйвера вызывается функцией *find_driver* (файл *usbh_core.c*) ядра подсистемы USB в случае успешной проверки соответствия кодов структуры *driver_info* драйвера соответствующим кодам подключенного устройства.

Функция *analyze_descriptor* драйвера вызывается функцией *device_register* (файл *usbh_core.c*) ядра подсистемы USB для каждого дескриптора устройства после успешного вызова функции *find_driver*.

Функция *poll* драйвера вызывается функцией *usbh_poll* (файл *usbh_core.c*) ядра подсистемы USB, а та – функцией *main_loop* (файл *usb.c*) с периодичностью 1 мс.

Функция *remove* драйвера вызывается функцией *device_remove* (файл *usbh_core.c*) ядра подсистемы USB при обнаружении в функции *usbh_poll* отключения устройства.

Для осуществления отправки данных устройству, основная программа должна произвести запись в буфер, известный драйверу и установить флаг, периодически проверяемый драйвером, а тот, во время периодического опроса в функции *poll* должен произвести действия по подготовке данных для отправки и вызвать функцию *usbh_write* ядра подсистемы USB, которая вызовет функцию *write* (файл *usbh_llt_stm32f4.c*) низкоуровневого драйвера работы с USB, где и произойдет непосредственная запись данных в регистры.

Чтение данных от устройства происходит примерно в той же последовательности – драйвер вызывает функцию *usbh_read* ядра подсистемы USB, которая вызывает функцию *read* (файл *usbh_llt_stm32f4.c*) низкоуровневого драйвера работы с USB, где происходит запись в регистры информации о необходимости чтения данных.

Периодический опрос в низкоуровневом драйвере работы с USB происходит в функции *poll*, которая может производить инициализацию и сброс блока работы с USB микроконтроллера, а также производить опрос блока работы с USB микроконтроллера о произошедших событиях. Когда опрос показывает завершение записи, то вызывается функция обратного вызова (*callback*) драйвера, запомненная для вызова после записи. Таким образом драйвер узнает об успешной/неуспешной записи своих данных и может предпринять дальнейшие действия (например, повторить запись). Когда опрос показывает завершение чтения, то вызывается функция обратного вызова (*callback*) драйвера,

запомненная для вызова после чтения. Таким образом драйвер узнает об успешном/неуспешном чтении своих данных и может предпринять дальнейшие действия (например, повторить чтение).

Узнав об успешном чтении, драйвер может или произвести запись в буфер, известный основной программе и установить флаг, периодически проверяемый основной программой, или вызвать функцию основной программы для обработки принятых данных (в разных наших драйверов это делается по-разному).

В основной программе обработка данных от внешнего устройства происходит в функции *mp_rx* (файл *mp.c*), где происходит снятии байт-стаффинга, проверки длины и контрольной суммы пакета. В случае успешного завершения проверок вызывается функция *mp_cmd* (файл *mp.c*), где происходит обработка команд от внешнего устройства.

В основной программе обработка данных от контроллера карты происходит в функции *sp_rx* (файл *sp.c*), где происходит снятии байт-стаффинга, проверки длины и контрольной суммы пакета. В случае успешного завершения проверок вызывается функция *sp_cmd* (файл *sp.c*), где происходит обработка команд от контроллера карты.

В функции *work_process* (файл *work.c*) происходит анализ состояния дверцы и отправка информации о произошедших событиях контроллеру индикации путем вызова функции *dp_send_events* (файл *dp.c*).

11 Разработка протокола обмена с учетом специальных требований

11.1 Активирующие последовательности

Разрабатываемое устройство построено на импортной элементной базе. Поэтому возможно, микросхемы содержат некоторые дополнительные (недокументированные) функции, исполняемые при поступлении на свои входы (или при появлении в оперативной памяти) некоторых последовательностей (активирующих).

Злоумышленник, знающий про такие дополнительные функции, может их использовать в своих целях. Например, вставить в устройство специально подготовленный оптический диск или смарт-карту и запустить ввод ключевой информации. Считанная с диска или карты активирующая последовательность, проходя по микросхемам, переключит их в особый режим функционирования (например, записи всей последующей информации во флеш память). После чего ключевая информация, считанная с корректных носителей, будет сохраняться внутри устройства. А затем злоумышленник сможет (например, используя другой подготовленный носитель) инициировать вывод этой информации. При реализации этого (пусть и маловероятного) сценария произойдет хищение ключевой информации.

11.1 Прореживание информации

Считанная с носителя информация должна передаваться в устройстве не в том виде в каком хранится. Например, можно после каждого байта, считанного с носителя, добавлять пустой байт. Таким образом, считанная информация будет порезана на кусочки и возможная активирующая последовательность будет обезврежена.

Но если разработчики дополнительной функции микросхемы учли возможность игнорирования монотонно изменяющихся байт, нужно менять байты по еще более сложной схеме.

Данной меры будет достаточно, если пустой байт имеет одно и то же значение (например, нулевое). Если же разработчики заложили возможность такой защиты, как игнорирование нулей, то вместо нулей нужно добавлять какое-то значение от байта к байту.

11.2 Маскирование информации

Наиболее хорошую защиту обеспечат случайные изменения байт. Передатчик накладывает случайную последовательность, приемник ее снимает. Возникает проблема осуществления обмена случайной последовательности между приёмником и передатчиком.

Внешнее устройство криптографической защиты информации, в которое производится ввод ключевой информации, содержит в своем составе генератор псевдослучайной последовательности, и при каждом вводе будет присылать ее в разрабатываемое устройство.

Лучше, если наложение будет происходить не только на пустые байты, но и на саму считанную информацию. Тогда можно защититься от утечки этой информации при прохождении по каналу связи (например, в виде электромагнитного излучения). Даже если электромагнитное излучение выйдет за пределы устройства, все, что злоумышленник сможет получить – случайную последовательность. И, если генератор последовательности идеальный, то закрываемая информация не сможет быть выделена [52].

Последовательность следует передавать по отдельному проводу, но это создает дополнительные сложности при проектировании – например, из-за того, что интерфейс USB передает данные пакетами, и пакеты могут теряться, потребуется как-то согласовывать размер выдаваемой случайной последовательности.

Поэтому было принято решение запрашивать случайную последовательность однократно – перед вводом, и накладывать ее на считываемую информацию по кругу.

11.3 Контроль целостности информации

По интерфейсу USB информация передается пакетами. Для каждого пакета происходит вычисление контрольной суммы с выявлением 100% одиночных и двойных ошибок. Также разрабатываемое устройство может работать и по интерфейсу RS-232 (при монтаже платы управления в дополнительном исполнении), поэтому в протокол был заложен свой собственный блочный обмен с выявлением ошибок.

Поскольку вычисление контрольной суммы производится программно, то эта операция будет отнимать часть вычислительных мощностей, поэтому был выбран простой алгоритмом – Флетчера [53]. Его можно представить в виде следующей последовательности операций, выполняемых над каждым байтом данных:

$$sum1 = (sum1 + байт) \% 0xff;$$
$$sum2 = (sum2 + sum1) \% 0xff;$$

В начале вычисления контрольной суммы переменные *sum1* и *sum2*, имеющие разрядность 8 бит, обнуляются. В конце вычисления переменная *sum2* содержит старшую половину контрольной суммы, а переменная *sum1* – младшую. На каждый пакет данных таким образом будет приходиться по 16 бит контрольной суммы.

Данные на оптическом диске хранятся в виде файлов в составе файловой системы iso8660 [54] и представляют из себя последовательность блоков. Считывание возможно лишь поблочно, но не побайтно. Размер блока на диске (2048 байт) больше, чем размер блока в написанных драйверах для работы с USB, поэтому при передаче придется дополнительно делить его (файловый блок) на части. Из соображений деления на кратное количество частей размер блока в протоколе принят равным 256 байт.

Поскольку внешнее устройство криптографической защиты информации не знает заранее о размере файла, то потребуется команда запроса размера. Поэтому внешнее устройство будет сначала запрашивать количество блоков, а затем запрашивать сами блоки.

11.4 Контроль целостности программного обеспечения

В разрабатываемом устройстве содержатся три контроллера с записанными в их постоянную память программами управления. Загрузка программ управления в постоянную память контроллеров происходит после изготовления устройства на заводе-изготовителе. Но если при эксплуатации произойдет случайное или намеренное искажение в постоянной памяти контроллера, корректная работа устройства может нарушиться. Поэтому содержимое постоянной памяти контроллеров нужно контролировать.

При работе происходит подключение к устройству криптографической защиты информации, которое специализируется на шифровании и подсчете контрольных сумм. Нужно передать содержимое постоянной памяти контроллеров в устройство криптографической защиты информации.

11.5 Описание протокола

Разрабатываемое устройство содержит три контроллера, обменивающихся между собой данными. Протокол обмена между ними и между разрабатываемым устройством и внешним устройством криптографической защиты информации нужно сделать унифицированным. Следует учесть также вышеописанные механизмы контроля и защиты от возможных активирующих последовательностей.

При передаче информации выполняется следующая последовательность операций:

- прореживание – добавление каждого второго байта с монотонно возрастающим значением;
- маскирование – наложение случайной последовательности на прореженные данные;
- добавление контрольной суммы – вычисляемой на прореженные и замаскированные данные;
- байт стаффинг – с добавлением маркеров начала и конца пакета, предназначенный для возможности выделения пакета из потока данных на приеме.

При приеме информации производится обратная последовательность операций. Если какая-либо из операций выполняется unsuccessfully, то приемник не получает предназначенную ему информацию и обмен останавливается. В таком случае ведущее устройство, при отсутствии ответа в течении заданного промежутка времени (которое в принципе может быть разным для разных команд) инициирует перезапрос..

Для контроллера индикации и контроллера карты ведущим является контроллер управления, для контроллера управления ведущим является внешнее устройство криптографической защиты информации.

С точки зрения внешнего устройства криптографической защиты информации команды протокола можно разделить на три категории:

- команды для работы с контроллером управления;
- команды для работы с контроллером карты;
- команды для работы с контроллером индикации.

Составленный список команд для работы с контроллером управления:

- запрос статуса контроллера управления;
- передача маски контроллеру управления;
- запрос размера основной флеш памяти контроллера управления;
- запрос размера флеш памяти загрузчика контроллера управления;
- запрос блока основной флеш памяти контроллера управления;
- запрос блока флеш памяти загрузчика контроллера управления;
- запрос размера файла на диске;
- запрос блока файла на диске.

Составленный список команд для работы с контроллером карты:

- запрос статуса контроллера карты;
- передача маски контроллеру карты;

- запрос размера основной флеш памяти контроллера карты;
- запрос размера флеш памяти загрузчика контроллера карты;
- запрос блока основной флеш памяти контроллера карты;
- запрос блока флеш памяти загрузчика контроллера карты;
- запрос к карте.

Составленный список команд для работы с контроллером индикации:

- запрос статуса контроллера индикации;
- запрос маски контроллера индикации;
- запрос размера основной флеш памяти контроллера индикации;
- запрос размера флеш памяти загрузчика контроллера индикации;
- запрос блока основной флеш памяти контроллера индикации;
- запрос блока флеш памяти загрузчика контроллера индикации;
- передача результата выполнения операции.

Используя команду «передача результата выполнения операции», внешнее устройство криптографической защиты информации может отобразить на дисплее разрабатываемого устройства информацию о состоянии процесса ввода и результате процесса ввода.

С точки зрения контроллера управления команды протокола также можно разделить на три категории:

- собственные команды;
- команды для работы с контроллером карты;
- команды для работы с контроллером индикации.

Составленный список команд для работы с контроллером карты:

- запрос статуса контроллера карты;
- передача маски контроллеру карты;
- запрос размера основной флеш памяти контроллера карты;
- запрос размера флеш памяти загрузчика контроллера карты;
- запрос блока основной флеш памяти контроллера карты;
- запрос блока флеш памяти загрузчика контроллера карты;
- запрос к карте.

Составленный список команд для работы с контроллером индикации:

- запрос статуса контроллера индикации;
- передача маски контроллеру индикации;
- запрос размера основной флеш памяти контроллера индикации;

- запрос размера флеш памяти загрузчика контроллера индикации;
- запрос блока основной флеш памяти контроллера индикации;
- запрос блока флеш памяти загрузчика контроллера индикации;
- передача событий контроллеру индикации.
- прием команд от контроллера индикации.

Используя команду «прием команд от контроллера индикации», контроллер индикации сообщает контроллеру управления о выборе режимов и других действиях оператора, а используя команду «передача событий контроллеру индикации» контроллер управления сообщает контроллеру индикации о произошедших событиях, таких как завершение выполнения тестов или результат выполнения операции ввода ключевой информации, о которых должен быть проинформирован оператор.

11.6 Порядок работы с устройством

Для внешнего устройства карта является подчиненным устройством. Если оно хочет произвести к ней обращение, то кодирует запрос в соответствии с протоколом обмена с разрабатываемым устройством и производит отправку этого закодированного запроса разрабатываемому устройству. Запрос получает контроллер управления, перекодирует в соответствии с протоколом обмена и отправляет контроллеру карты. Контроллер карты раскодирует запрос в соответствии с протоколом обмена, проверяет корректность запроса и отправляет карте. Затем (зная, сколько времени в норме занимает обработка той или иной команды) ждет, проверяет корректность полученного ответа, кодирует в соответствии с протоколом обмена и передает контроллеру управления. Тот перекодирует в соответствии с протоколом обмена и отправляет во внешнее устройство. Если внешнее устройство не получает ответа в течении ожидаемого промежутка времени, то может или повторить запрос или сообщить оператору об ошибке при работе с картой.

Последовательность работы с диском для внешнего устройства несколько отличается от последовательности работы с картой. Также требуется вначале запросить состояние носителя, а потом (при наличии и готовности носителя) дополнительно запросить размер файла. Внутри же разрабатываемого устройства последовательность более простая, потому что контроллер карты в этом случае не задействован. При необходимости чтения файла внешнее устройство кодирует номер запрашиваемого блока в соответствии с протоколом обмена и отправляет разрабатываемому устройству. Запрос получает контроллер управления и производит опрос привода чтения оптических дисков. Тот производит передачу блока данных, который получает контроллер управления.

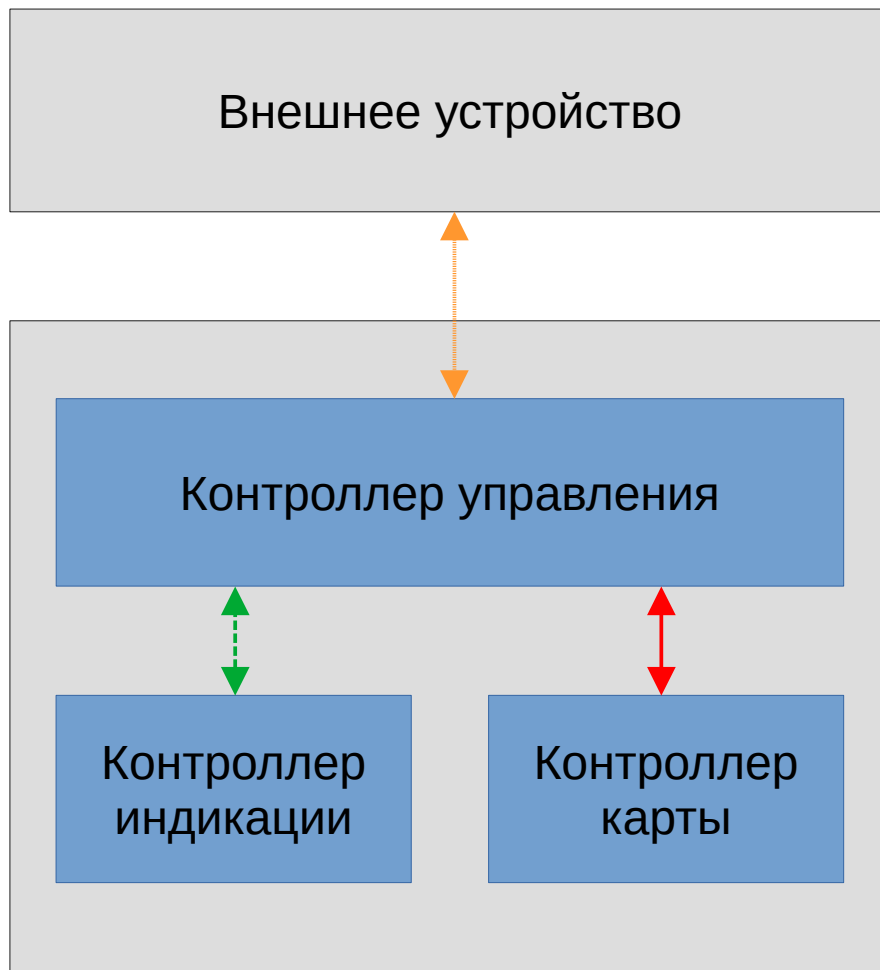
Контроллер управления кодирует блок данных в соответствии с протоколом обмена и отправляет во внешнее устройство. Если внешнее устройство не получает ответа в течении ожидаемого промежутка времени, то может или повторить запрос или сообщить оператору об ошибке при работе с диском.

Хотя и контроллер управления, и контроллер карты обмениваются данными по унифицированному протоколу, перекодирование в контроллере управления при передаче от внешнего устройства к карте требуется, поскольку маски на отрезках «внешнее устройство – контроллер управления» и «контроллер управления – контроллер карты» в общем случае используются разные.

Для ввода ключевой информации с диска оператор должен выбрать соответствующий пункт меню, открыть дверцу устройства, нажать на кнопку извлечения диска на приводе, установить диск на шпиндель выдвинувшегося лотка привода, задвинуть лоток, закрыть дверцу устройства и ожидать завершения процесса ввода.

При вводе с карты оператор должен выбрать соответствующий пункт меню, открыть дверцу устройства, вставить карту до упора, закрыть дверцу устройства и ожидать завершения процесса ввода. В процессе ввода дополнительно требуется ввести PIN (или PUK, если число попыток ввода PIN превышено). Ввод PIN/PUK в текущей версии программного обеспечения происходит на клавиатуре внешнего устройства (именно оно является управляющим и формирует запросы к карте/диску).

Данные с карты (и на карту) проходят от внешнего устройства до контроллера управления разрабатываемого устройства под одной маской, а от контроллера управления до контроллера карты – под другой. Интерфейс используется в обоих случаях одинаковый – USB, и частота его работы – тоже одинаковая, поэтому при наличии электромагнитных излучений от устройства они будут накладываться, что дополнительно усложнит задачу съема информации для потенциального злоумышленника.



- Маска 1 – между внешним устройством и контроллером управления
- Маска 2 – между контроллером управления и контроллером карты
- Маска 3 – между контроллером управления и контроллером индикации

Рисунок 6 – Схема обмена данными между контроллерами

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

В результате обследования людей, работающих в условиях постоянного воздействия электромагнитных излучений от компьютера, было доказано, что наиболее чувствительны к данному влиянию нервная и сердечно-сосудистая системы. Кроме того, у респондентов описаны изменения кровотока, нарушения со стороны эндокринной системы, метаболических процессов и заболевания органов зрения. Иммунная система уменьшает выброс в кровь специальных ферментов, выполняющих защитную функцию, из-за чего происходит ослабление системы клеточного иммунитета. Эндокринная система, напротив, начинает выбрасывать в кровь большее количество адреналина и, как следствие, увеличивает нагрузку на сердце. Происходит сгущение крови, в результате чего клетки не получают достаточное количество кислорода [55].

Среди мероприятий, направленных на повышение умственной работоспособности, на преодоление и профилактику психоэмоционального и функционального состояния можно рекомендовать следующие [56]:

- ритмичную и системную организацию умственного труда;
- постоянное поддержание эмоции, интереса;
- совершенствование межличностных отношений работников между собой;
- организацию рационального режима труда, питания, сна и отдыха;
- отказ от вредных привычек: употребление алкоголя и наркотиков, курения и токсикомании;
- двигательную активность и физическую тренировку, постоянное поддержание организма в состоянии оптимальной физической тренированности.

Для поддержания здоровья и работоспособности на соответствующем уровне одинаково необходимы четыре элемента: физическая нагрузка, рациональное питание, закаливание и умение отдыхать.

Заключение

В ходе выполнения дипломного проектирования было пояснено понятие ключевой информации, выполнен обзор носителей ключевой информации и обосновано применение выбранных, проведен анализ методов защиты тракта ввода ключевой информации устройства криптографической защиты информации, определены угрозы безопасности информации и подобраны методы защиты для устранения этих угроз, высказаны соображения о принципах конструирования устройства, способного взаимодействовать с носителями ключевой информации выбранных типов.

Составлена и описана структурная схема разрабатываемого устройства, подобраны покупные узлы, на основе которых будет строиться разрабатываемое устройство, составлена и описана функциональная схема с учетом применения подобранных покупных узлов.

Произведен выбор элементной базы, на которой будет строиться устройство с акцентом на надежность в широком диапазоне температур, рассмотрены принципы проектирования систем на основе микроконтроллеров, составлены и описаны электрические схемы для входящих в состав устройства плат и составлены перечни элементов.

Произведен выбор средств разработки программного обеспечения для входящих в состав платы управления микроконтроллеров, подобраны библиотеки с открытым исходным кодом для использования при написании программного обеспечения, настроена среда для разработки и отладки программного обеспечения.

Разработан протокол взаимодействия между контроллерами в составе устройства и внешним устройством, способный противостоять возможным активирующим последовательностям, которые могут быть считаны с носителей ключевой информации.

Написано программное обеспечение для входящих в состав устройства микроконтроллеров, реализующее выполнение устройством требуемых функций с функциями контроля состояния устройства и возможностью проверки целостности программного обеспечения при помощи внешнего устройства.

Описаны вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации, а также методы и средства физической культуры, снижающие их воздействие.

Разработанное в результате выполнения дипломного проекта защищенное устройство ввода ключевой информации соответствует требованиям технического задания и может изготавливаться серийно.

Список использованных источников

- 1 Base64 – URL: <https://ru.wikipedia.org/wiki/Base64>
- 2 8-bit clean – URL: https://ru.wikipedia.org/wiki/8-bit_clean
- 3 Compact disc – URL: https://ru.wikipedia.org/wiki/Compact_disc
- 4 Non-return-to-zero – URL: <https://ru.wikipedia.org/wiki/Non-return-to-zero>
- 5 Eight-to-fourteen modulation – URL: https://ru.wikipedia.org/wiki/Eight-to-fourteen_modulation
- 6 Cross-interleaved Reed–Solomon coding – URL: https://ru.wikipedia.org/wiki/Cross-interleaved_Reed–Solomon_coding
- 7 Compact Disc and DVD copy protection – URL:
https://en.wikipedia.org/wiki/Compact_Disc_and_DVD_copy_protection
- 8 Smart card – URL: https://ru.wikipedia.org/wiki/Smart_card
- 9 IEC 7816 – URL: https://ru.wikipedia.org/wiki/ISO/IEC_7816
- 10 Personal identification number – URL:
https://ru.wikipedia.org/wiki/Personal_identification_number
- 11 Personal unblocking key – URL:
https://ru.wikipedia.org/wiki/Personal_unblocking_key
- 12 Hagai Bar-El Known Attacks Against Smartcards – URL:
http://www.infosecwriters.com/text_resources/pdf/Known_Attacks_Against_Smartcards.pdf
- 13 Банк данных угроз безопасности информации <https://bdu.fstec.ru/threat>
- 14 Intel Management Engine – URL:
https://en.wikipedia.org/wiki/Intel_Management_Engine
- 15 AMD Platform Security Processor – URL:
https://en.wikipedia.org/wiki/AMD_Platform_Security_Processor
- 16 System on a chip – URL: https://en.wikipedia.org/wiki/System_on_a_chip
- 17 i.MX 6Quad Applications Processors – URL: <https://www.nxp.com/imx6q>
- 18 SIM card – URL: https://ru.wikipedia.org/wiki/SIM_card
- 19 General-purpose input/output – URL: https://en.wikipedia.org/wiki/General-purpose_input/output
- 20 Universal asynchronous receiver-transmitter – URL:
https://en.wikipedia.org/wiki/Universal_asynchronous_receiver-transmitter
- 21 STM32L471RE Ultra-low-power with FPU Arm Cortex-M4 MCU 80 MHz with 512 Kbytes of Flash memory, DFSDM – URL: <https://www.st.com/en/microcontrollers-microprocessors/stm32l471re.html>

22 MAX3221 +3V to +5.5V RS-232 Transceivers with AutoShutdown – URL:
<https://www.maximintegrated.com/en/products/interface/transceivers/MAX3221.html>

23 LP2985 150-mA, 16-V, low-dropout voltage regulator with enable – URL:
<https://www.ti.com/product/LP2985>

24 STM32H743XI High-performance and DSP with DP-FPU, Arm Cortex-M7 MCU with 2MBytes of Flash memory, 1MB RAM, 480 MHz CPU, Art Accelerator, L1 cache, external memory interface, large set of peripherals – URL: <https://www.st.com/en/microcontrollers-microprocessors/stm32h743xi.html>

25 STM32L151VB-A Ultra-low-power Arm Cortex-M3 MCU with 128 Kbytes of Flash memory, 32 MHz CPU, USB – URL:
<https://www.st.com/en/microcontrollers-microprocessors/stm32l151vb-a.html>

26 STM32F415RG High-performance foundation line, Arm Cortex-M4 core with DSP and FPU, 1 Mbyte of Flash memory, 168 MHz CPU, ART Accelerator, HW crypto – URL:
<https://www.st.com/en/microcontrollers-microprocessors/stm32f415rg.html>

27 USB 2.0 Transceiver Macrocell Interface (UTMI) Specification – URL:
<https://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/usb2-transceiver-macrocell-interface-specifications.pdf>

28 Physical layer – URL: https://en.wikipedia.org/wiki/Physical_layer#PHY

29 Quad flat package – URL: https://en.wikipedia.org/wiki/Quad_flat_package

30 Differential signalling – URL: https://en.wikipedia.org/wiki/Differential_signalling

31 TUSB4041I 4-port high-speed 480-Mbps USB 2.0 hub – URL:
<https://www.ti.com/product/TUSB4041I>

32 Galvanic isolation – URL: https://en.wikipedia.org/wiki/Galvanic_isolation

33 ADUM3160 Datasheet and Product Info – URL:
<https://www.analog.com/en/products/adum3160.html>

34 DC-to-DC converter – URL: https://en.wikipedia.org/wiki/DC-to-DC_converter

35 ST1S40 3 A DC step-down switching regulator – URL: <https://www.st.com/en/power-management/st1s40.html>

36 Linear regulator – URL: https://en.wikipedia.org/wiki/Linear_regulator

37 TMR 6-1211 – URL: <https://www.tracopower.com/int/en/model/tmr-6-1211>

38 TPS2069 1.5A loading, 2.7-5.5V, 70mΩ USB power switch, active-high, reverse blocking – URL: <https://www.ti.com/product/TPS2069>

39 TPS2553 0.075-1.7A adj. ILIMIT, 2.5-6.5V, 85mΩ USB power switch, active-high, reverse blocking – URL: <https://www.ti.com/product/TPS2553>

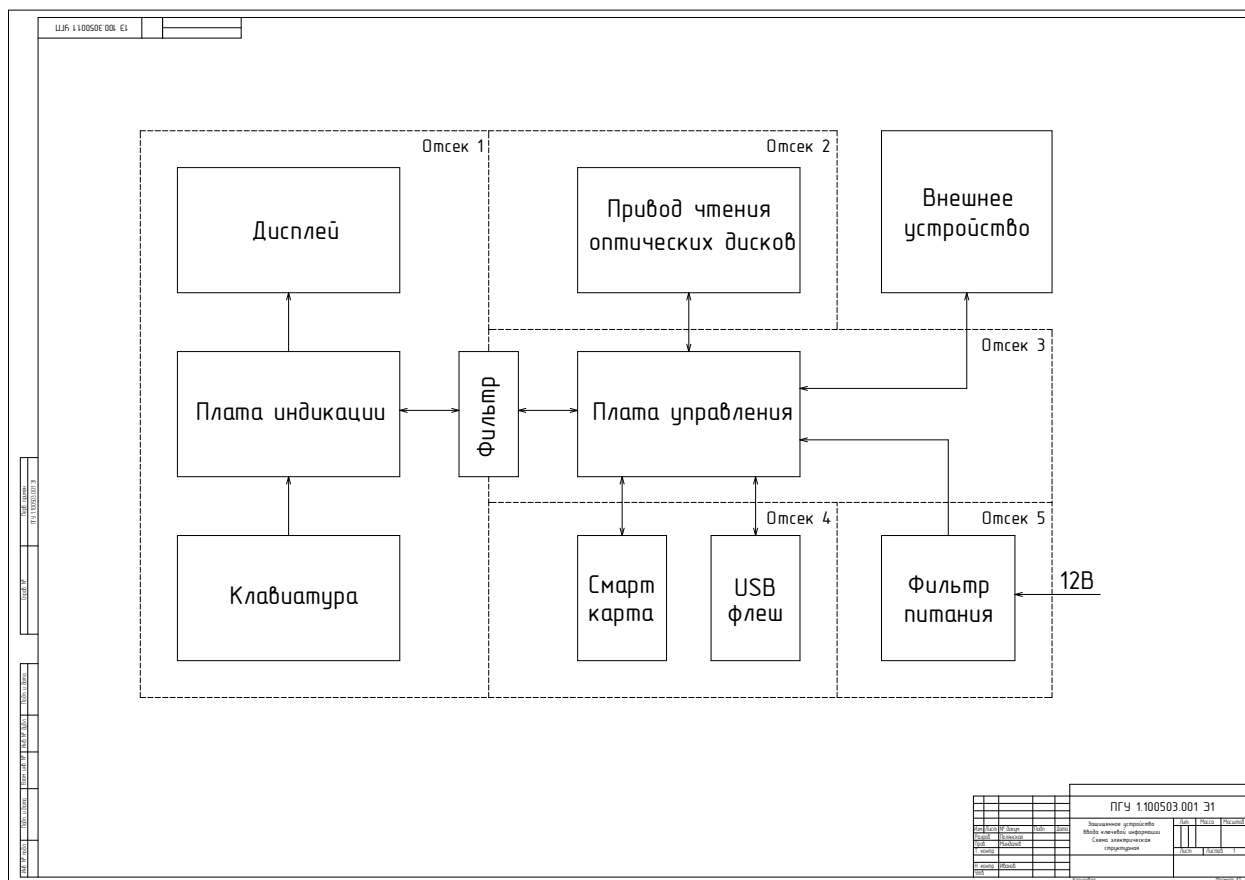
- 40 TLV7211 Micropower, high-voltage, single comparator – URL:
<https://www.ti.com/product/TLV7211>
- 41 Smartcard interface with STM32F10x and STM32L1xx microcontrollers – URL:
https://www.st.com/resource/en/application_note/an2598-smartcard-interface-with-stm32f10x-and-stm32l1xx-microcontrollers-stmicroelectronics.pdf
- 42 ST8024 Smartcard interface – URL: <https://www.st.com/en/interfaces-and-transceivers/st8024.html>
- 43 USBLC6-2 ESD Protection for USB 2.0 High Speed – URL:
<https://www.st.com/en/protectoins-and-emi-filters/usblc6-2.html>
- 44 FT231XQ USB Full Speed to Full Handshake UART with USB Charger Detection, QFN-20 – URL: <https://ftdichip.com/products/ft231xq/>
- 45 Debian – URL: <https://en.wikipedia.org/wiki/Debian>
- 46 Astra Linux – URL: https://en.wikipedia.org/wiki/Astra_Linux
- 47 GNU Compiler Collection – URL:
https://en.wikipedia.org/wiki/GNU_Compiler_Collection
- 48 GNU Debugger – URL: https://en.wikipedia.org/wiki/GNU_Debugger
- 49 Open On-Chip Debugger – URL: <https://openocd.org>
- 50 GNU – URL: <https://en.wikipedia.org/wiki/GNU>
- 51 GNU General Public License – URL:
https://en.wikipedia.org/wiki/GNU_General_Public_License
- 52] XOR cipher – URL: https://en.wikipedia.org/wiki/XOR_cipher
- 53 Fletcher's checksum – URL: https://en.wikipedia.org/wiki/Fletcher%27s_checksum#Fletcher-16
- 54 ISO 9660 – URL: https://en.wikipedia.org/wiki/ISO_9660
- 55 Как компьютер влияет на сердце – URL: <https://med-info.ru/content/view/2332>
- 56 Физическое воспитание студентов в техническом вузе – URL:
<https://core.ac.uk/download/pdf/42049582.pdf>

Приложение А Угрозы безопасности и соответствующие им методы защиты

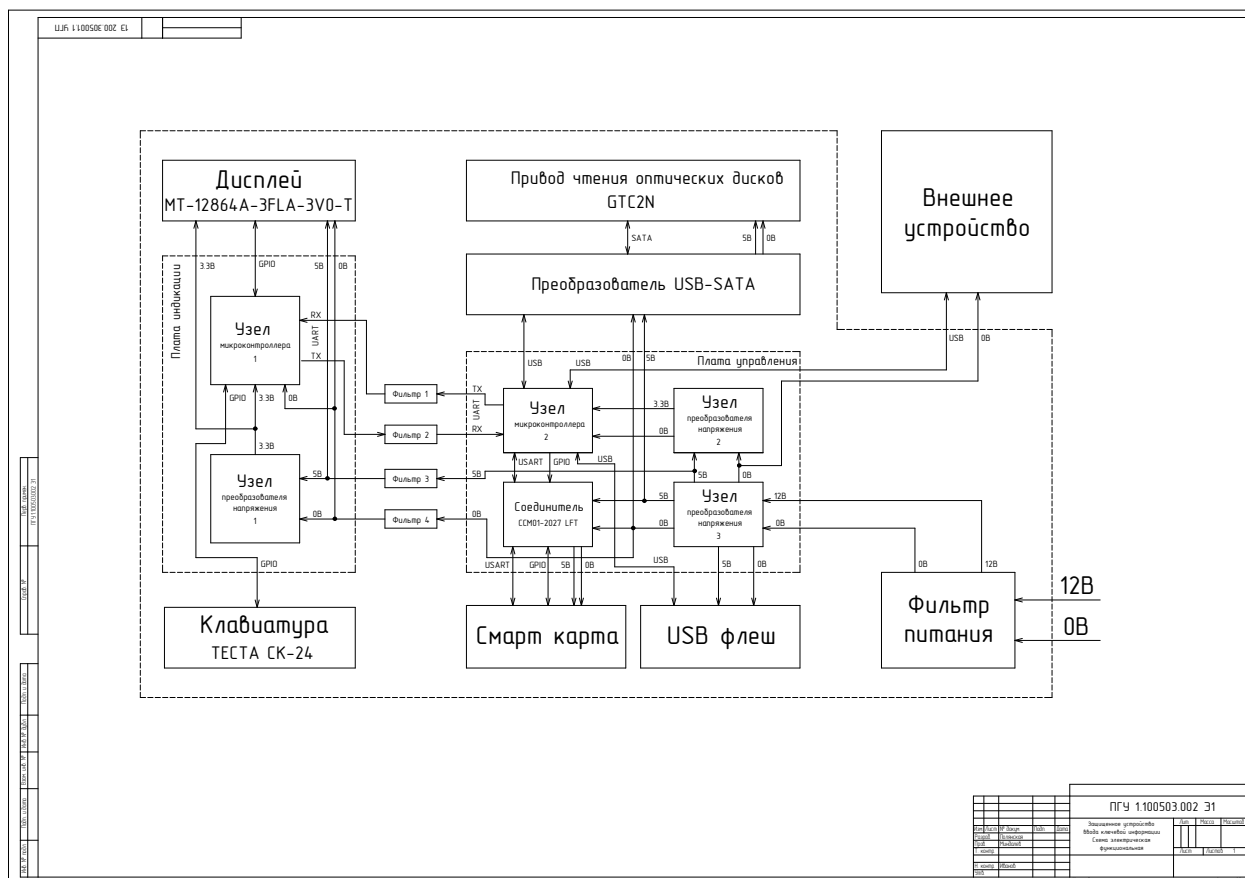
Защищенное устройство ввода ключевой информации
Угрозы безопасности и соответствующие им методы защиты

Идентификатор угрозы	Описание угрозы	Методы защиты
УБИ.139	Угроза преодоления физической защиты	Пломбирование винтов, скручивающих корпус устройства и крышку Организационные меры, препятствующие попаданию устройства к посторонним лицам Контроль целостности программного обеспечения
УБИ.124	Угроза подделки записей журнала безопасности	
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Прореживание передаваемой информации Маскирование передаваемой информации Контроль целостности передаваемой информации
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Контроль целостности передаваемой информации
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	Выбор дисплея с пониженной яркостью Маскирование отображения кодов доступа на дисплее устройства
УБИ.111	Угроза передачи данных по скрытым каналам	Тщательное экранирование устройства

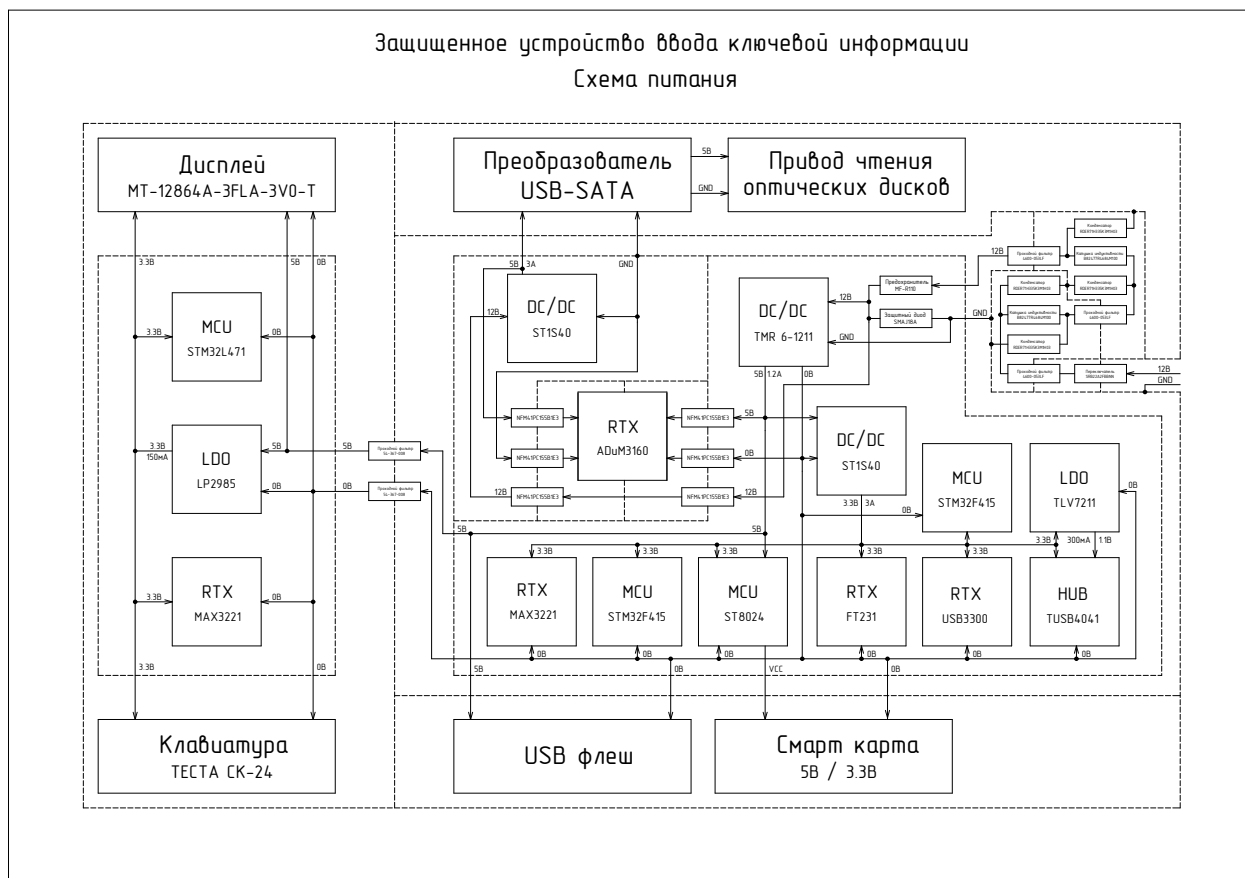
Приложение Б Схема электрическая структурная устройства



Приложение В Схема электрическая функциональная устройства

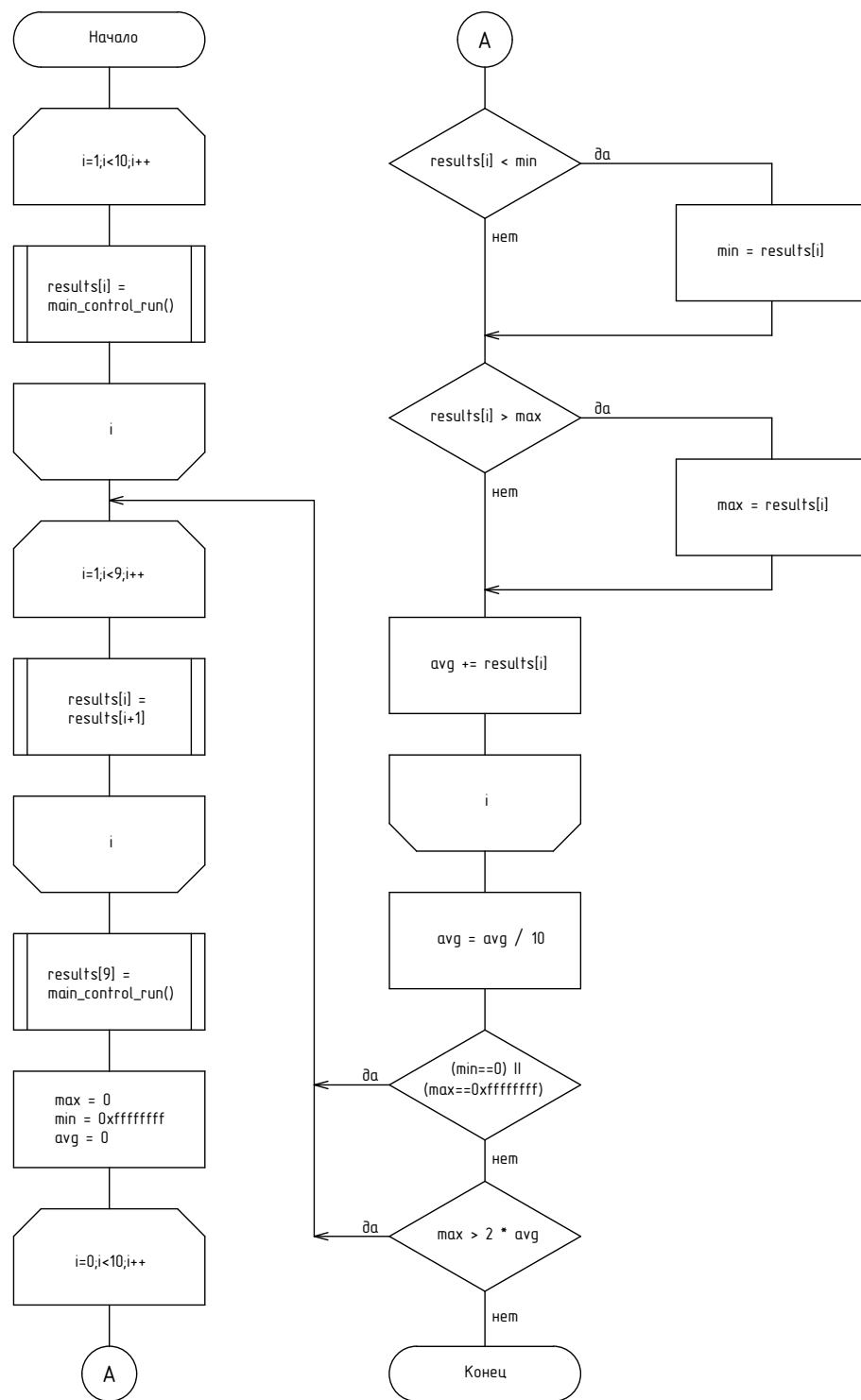


Приложение Г Схема питания устройства



Пр
ил
ож
ен
ие
Ж

Защищенное устройство ввода ключевой информации
Алгоритм работы предпускового контроля
Функция main_control()



Приложение И Перечень протоколируемых событий

Защищенное устройство ввода ключевой информации
Перечень протоколируемых событий

Результат ввода ключевой информации с диска

Результат ввода ключевой информации с карты

Результат проведения контроля целостности программного обеспечения

Результат проведения периодического контроля

Факт смены кода доступа к устройству

Факт переполнения журнала безопасности

Факт перемещения журнала безопасности на съемный носитель

Приложение К Обработка данных с использованием протокола обмена

Защищенное устройство ввода ключевой информации
Обработка данных с использованием протокола обмена

